UNIVERZITET U BEOGRADU

FAKULTET ORGANIZACIONIH NAUKA

Saša R. Paunović

PRIMENA MULTIMODALNE BIOMETRIJE U SISTEMIMA ZA UTVRĐIVANJE IDENTITETA

doktorska disertacija

Beograd, 2013

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Saša R. Paunović

APPLYING MULTIMODAL BIOMETRICS IN IDENTITY DETERMINING SYSTEMS

Doctoral Dissertation

Belgrade, 2013

Primena multimodalne biometrije u sistemima za utvrđivanje identiteta

Mr Saša R. Paunović

Doktorska teza

Mentor:

Dr Dušan Starčević, redovan profesor,
Univerzitet u Beogradu, Fakultet organizacionih nauka

Članovi komisije :

Dr Nevenka Žarkić-Joksimović, redovan profesor,
Univerzitet u Beogradu, Fakultet organizacionih nauka

Dr Zoran Radojičić,vanredni profesor,
Univerzitet u Beogradu, Fakultet organizacionih nauka

Dr Velimir Štavljanin,vanredni profesor,
Univerzitet u Beogradu, Fakultet organizacionih nauka

Dr Rade Stankić, redovan profesor,
Univerzitet u Beogradu, Ekonomski fakultet

Datum odbrane: .....

Od cilja vodi hiljadu puteva, do cilja samo jedan (Mišel de Montenj).

Ovo je moto koji me je vodio ka cilju, a na čijem putu ostvarenja nisam bio sam.
Zato želim svoju doktorsku disertaciju da posvetim svojim roditeljima,
jer znam koliko bi bili ponosni.
Posvećujem ga i mojoj porodici, sinu Mateji i suprugi Ivi,
čije su me razumevanje i ljubav vodili ka cilju,
kao i bratu, Ivanu Jeriniću.
Zahvaljujem i svima koji su svojim savetima, strpljenjem i podrškom
doprineli izradi ove doktorske disertacije,
a pre svih mentoru profesoru dr Dušanu Starčeviću.

Abstract (Rezime)

Primena multimodalne biometrije u sistemima za utvrđivanje identiteta

U svetu čije su odrednice globalna ekonomija, Internet, česta i snažna migracija ljudi, regionalna politička nestabilnost i ukorenjen organizovan kriminal, pitanje svakodnevnog utvrđivanja identiteta ljudi u navedenim kontekstima je od ključnog značaja za bezbednost i efikasno funkcionisanje svakog društva. U važnim društvenim aktivnostima, na primer na polju bezbednosti, zdravstva ili finansija, tačnost zaključaka nekih unimodalnih biometrijskih sistema postaje problematična, jer pojedinačni propusti mogu da izazovu nesagledivu štetu pojedincu ili zajednici. Smanjenje neizvesnosti se traži u istovremenom kombinovanju više biometrijskih modaliteta, odnosno u multimodalnoj biometriji. Izvedena istraživanja su imala za cilj da doprinesu boljem sagledavanju mogućnosti i ograničenja primene multimodalnih biometrijskih sistema u postupcima identifikacije lica, kao neophodnog preduslova za uspostavljanje sistema menadžmenta identitetom. Sprovedeno je analitičko i eksperimentalno istraživanje u naučnom, organizacionom, tehničkom, tehnološkom, pravnom i finansijskom domenu, kako bi se izveli odgovarajući konkretni zaključci, zapažanja i preporuke potrebni za procenu mogućnosti primene multimodalnih biometrijskih sistema u sistemima identifikacije. Studija slučaja je korišćena kao najprikladniji metodološki okvir za proveru postavljenih hipoteza u oblasti primene multimodalne biometrije u procesu utvrđivanja identiteta. U studiji slučaja su istraživane mogućnosti i ograničenja rada biometrijskog sistema sa dva često korišćena biometrijska modaliteta, otiskom prsta i slikom lica. Nakon tako postavljenog problema, u radu je izložena i potom praktično primenjena metodologija za rešavanja problema koji se javljaju u sistemima multimodalne biometrije. Izložene su specifičnosti dve korišćene biometrijske baze podataka. Opisan je i eksperimentalan, ispitni multimodalni sistem za utvrđivanje identiteta sa datom specifikacijom arhitekture, odabranim režimima rada, kao i navođenjem

postupka ispitivanja performansi ovog sistema. Završni deo rada je posvećen analizi i interpretaciji dobijenih rezultata radi određivanja, kako performansi rada multimodalnog biometrijskog sistema, tako i oceni ispunjenja polaznih hipoteza. Rezultati istraživanja potvrdili su polaznu hipotezu da multimodalna biometrija podiže tačnosti postupka utvrđivanja identiteta, kao i da takvi sistemi poseduju inherentnu redudantnost koja im omogućava rad sa degradiranim performansa u slučaju nemogućnosti zahvatanja ili smeštaja nekog biometrijskog podataka. Posebno treba istaći nalaz da primena biometrije u nekim segmentima sistema bezbednosti dovodi do kontraproduktivnih efekata u drugim segmentima ovog sistema! Naime, širenje primene biometrije ugrožava normalan rad sistema za zaštitu svedoka, pa je potvrđena posebna hipoteza da nalaženje rešenja za ovaj problem treba tražiti u širem prostoru nego što je to samo prostor biometrije. U radu je predložen mogući sklop mera kao prostor rešenja.

Ključne reči: biometrija, biometrijski identitet, elektronski identifikacioni dokument, menadžment identiteta, multimodalna biometrija, bezbednost, zaštita svedoka

Naučna oblast: Menadžment informacionih tehnologija
Uža naučna oblast: Biometrijski informacioni sistemi
UDK 57.087.1:004

Abstract

Applying Multimodal Biometrics in Identity Determining Systems

In a world defined by Global economy, the Internet, mass migration, regional political instability and deeply rooted organized crime, the question of determining and verifying identities of individuals on a daily basis is of utmost significance for the security and efficient functioning of all social groups. The use of a single mode method for verifying identities has become an issue with potential for damaging consequences for individuals and organizations. This is especially true in highly sensitive fields such as banking, national security and the health sector. With the aim of minimizing risk and uncertainty, multiple identification metrics are being combined in multimodal systems. Research has been carried out with the aim of exploring the possibilities and limiting factors of applying multimodal biometric systems to the process of identifying persons, as a prerequisite for implementing an identity management system. Experimental and analytical research has been performed within the scientific, logistical, technical and technological, legal and financial domains in order to reach the appropriate, concrete conclusions, observations and recommendations required to assess the feasibility of using multimodal biometric systems, as part of an identification management system. A case study approach was used as the most suitable methodology framework for the analysis and verification of the above described hypothesis of applying multimodal biometric systems as a means of determining people's identities. In the case studies explore the capabilities and limiting factors of a multimodal system that uses two popular biometric identifiers, the fingerprint, and the facial image. With the challenge set, this paper presents a subsequently applied methodology for overcoming the challenges that occur in the use of multimodal biometric systems. Presented herein are the specific features and characteristics of two biometric databases. Also described is the architecture of the experimental multimodal biometric system, the chosen business processes as

well as the performance metrics used on the described system. The final sections of this paper presents the analysis and interpretation of the obtained performance results and describe the level of fulfillment of the afore set hypothesis. The results obtained confirm the initial hypothesis that a multimodal biometric identification system increases the level of accuracy in determining a person's identity. In addition the results show that such systems possess an inherent redundancy making them more robust and able to work with degraded biometric specimens or lack of specimen whereby the given specimen could not be obtained or appropriately stored. It is important to emphasize that applying biometric identity measures in certain segments of a security system has counterproductive effects on other parts of the overall security system. Namely, the use of such systems has a negative impact on the normal operations and functions of the witness protection process. As such we can confirm the hypothesis that the solution for the outlined problem must be sought across a wider range of fields, beyond biometric identification.

Key words: Biometrics, biometric identity, electronic identification document, identity management, multimodal biometrics, security, witness protection

Scientific discipline: Information Technology Management
Sub-field: Biometric Information Systems
UDK 57.087.1:004

SADRŽAJ

LISTA SLIKA, DIJAGRAMA, BLOK DIJAGRAMA I TABELA

1. UVOD

Živimo u veku u kojem su fenomeni Interneta i globalizacije obeležili sve aspekte života i rada ljudi. Početna primena Interneta u elektronskoj trgovini, prerasla je u sveobuhvatno elektronsko poslovanje. Poslovanje putem Interneta postalo je *de facto* standardan način poslovanja, a za ilustraciju možemo da navedemo samo nekoliko najčešće korišćenih modela poslovanja: poslovanje između preduzeća (*B2B*), poslovanje između građana i preduzeća (*B2C* ili *C2B*), poslovanje između preduzeća i države (*B2G*), poslovanje između građana i države (*C2G*) ili poslovanje između samih građana (*C2C*). U svakom od navedenih modela poslovanja važno je ustanoviti identitet partnera sa kojim se odvija elektronska komunikacija.[1]

Pored poslovanja preko Interneta, druga dva obeležja savremenog sveta, posledica procesa globalizacije, a od posebnog interesa u našem istraživanju, su mobilnost ljudi i terorizam. Mobilnost ljudi je neposredna posledica vladajuće paradigme globalne ekonomije. Ljudi putuju svetom bilo iz poslovnih razloga bilo privatno, na primer kao turisti. U masi onih koji svakodnevno prelaze granice, neki od njih putuju sa lažnim identitetom i pripadaju svetu kriminala ili terorizma. Zbog toga je poželjan postupak automatizovanog utvrđivanja identiteta pojedinaca, kako bi se podigla opšta bezbednost i omogućilo nesmetano kretanje ljudi.[2]

Ali, problem utvrđivanja identiteta je daleko širi i odnosi se na celokupan život ljudi, na okruženje u kojem se svakodnevno boravi i radi. Mnogi objekti kojima želimo pristupiti su obezbeđeni tako da je pristup omogućen samo licima sa *pravom* pristupa, pri čemu se to pravo ostvaruje u prethodnom postupku utvrđivanjem identiteta. Mnogi naši lični elektronski uređaji, poput mobilnog telefona i tableta, sadrže podatke koje ne želimo da

[1] H. Chan, R. Lee, Th. Dillon, E. Chang, *E-commerce: Fundamentals and Applications*, John Wiley & Sons (2001).
[2] S. Paunović, D. Starčević, *Multimodalna biometrija i menadžment identiteta*, Zbornik konferencije ITEO 2010, Banja Luka, Republika Srpska, BiH, (2010).

delimo sa drugim ljudima. U stvari, želimo da to ne bude moguće čak i u slučajevima kada su nam takvi uređaji ukradeni ili kada ih izgubimo.

Na poslu većina ljudi koristi neku vrstu računarske opreme, bilo da je reč o *ATM* mašini, *POS* terminalu ili računaru na kojem se obavlja aplikacija iz domena administrativno-kancelarijskog poslovanja. U svim slučajevima važno je utvrditi ko i pod kojim uslovima ima pravo pristupa nekom od takvih uređaja, ili, ko je i kada poslao neke elektronske dokumente, ili ako vas zaustavi saobraćajac tokom vožnje, da li vozite kola sa vašom vozačkom dozvolom.

Napretkom tehnologije, pre svega u oblasti računarstva i elektronskih senzora, u poslednjoj deceniji od tehničkih sredstava koja se koriste da bi se dobili odgovori na postavljena pitanja, u prvi plan su izbili biometrijski sistemi identifikacije. Danas su biometrijski sistemi za identifikaciju po svojoj veličini sve manji, precizniji, pouzdaniji i brži i nalaze sve veću primenu u drugim delatnostima, gde je neophodno nedvosmisleno utvrditi ili potvrditi identitet osobe.[3]

Prednost primene biometrije je što eliminiše potrebu za korišćenjem lozinki, jer biometrijski podatak postaje lozinka. Biometrija se danas koristi za poboljšanje bezbednosti rada računarskih mreža, za zaštitu finansijskih transakcija ili kontrolu pristupa zaštićenim radnim lokacijama, ali je od neprocenjive važnosti za efikasan rad službi bezbednosti. Biometrijski sistemi identifikacije i u našoj zemlji se koriste u pojedinim organima državne uprave i institucijama, odnosno firmama, prevashodno za identifikaciju zaposlenih. Može se reći da je masovnija upotreba biometrije i biometrijskog sistema identifikacije u Srbiji, započela uvođenjem *smart* kartica, biometrijskih ličnih karata i biometrijskih putnih isprava.

Danas u svetu dominira upotreba unimodalnih biometrijskih sistema, odnosno sistema identifikacije koji koriste samo jedan vid ili modalitet identifikacije osoba. Nažalost, u nekim oblastima primene, na primer

[3]A. K. Jain, A. Ross, S. Prabhakar, *An introduction to biometric recognition*, IEEE Trans. Circuits Systems Video Technol. 14 (1) (2004), str. 4–20.

bezbednosti, to nije dovoljno jer pojedinačni propusti mogu da izazovu nesagledivu štetu zajednici. Rešenja se poslednjih nekoliko godina traže u istovremenom kombinovanju više biometrijskih modaliteta, odnosno u *multimodalnoj* biometriji.[4] Biometrijska identifikacija postaje sofisticirana, jer se kombinuju različiti biometrijski modaliteti i tehnike, ali se zauzvrat dobija veća tačnost ili se bitno smanjuje napor korisnika u procesu identifikacije.[5] U literaturi se poslednjih godina može naći više podataka o istraživanjima u oblasti multimodalne biometrije, ali nije značajnije analiziran uticaj određene kombinacije biometrijskih modaliteta, raspoloživih metoda obrade biometrijskih podataka i veličine baze biometrijskih podataka na performanse sistema.

U svim pomenutim slučajevima uočava se društvena potreba da se u nekom trenutku utvrdi identitet određene osobe. Na osnovu izloženog možemo reći da je naše istraživanje obuhvatilo analizu rada i mogućnosti primene multimodalnih biometrijskih sistema u uspostavljanju efikasnog i efektivnog sistema menadžmenta identitetom posredstvom elektronskih identiteta. U najopštijem smislu, sistem menadžmenta identitetom se može definisati kao „*Integrisani sistem poslovnih procesa, skupa pravila i tehnologija koje omogućavaju organizaciji da uspostavi i upravlja pristupom korisnika kritičnim resursima koje nadzire organizacija, pri čemu sistem štiti poverljive informacije od neautorizovanih korisnika*“.[6] Sistem menadžmenta identitetom je odgovoran za kreiranje, korišćenje i okončavanje elektronskih identiteta.

U ovom radu dat je prikaz sopstvenih rezultata istraživanja o mogućnostima, ali i ograničenjima, primene multimodalnih biometrijskih sistema u implementaciji sistema menadžmenta identitetom u odnosu na konkurentne unimodalne biometrijske sisteme.

---

[4] D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 154–159.

[5] A. K. Jain, Patrick Flynn, A. A. Ross, Eds., *Handbook of Biometrics*, Springer, (2008).

[6] http://www.nist.gov/itl/idms/, pristupljeno 14.10.2012.

Imajući u vidu dubinu zadiranja biometrijskih sistema sa menadžment identitetom u sve pore društvenog života pojedinaca, kao i kontroverze koje se pritom pojavljuju, u drugom poglavlju ovog rada, nakon definisanja pojma biometrije, analizirane su društvene i pravne konotacije primene biometrije sa stanovišta društvene opravdanosti. Dat je prikaz pravnih aspekata biometrije i pravno regulisanje zaštite biometrijskih podataka, kako u svetu, tako i kod nas.

Treće poglavlje rada posvećeno je menadžmentu identiteta, odnosno tehničko-tehnološkim pogledima na proces implementacije sistema menadžmenta identitetom. Izložena je materija koja pokriva identitet i važnost identiteta, specifičnosti biometrijskog identiteta i pregled elektronskih dokumenata zasnovanih na biometrijskom identitetu. Posebna pažnja je data prikazu *smart* tehnologije, kao dominantne tehnologije u domenu biometrijskih elektronskih dokumenata. Kako je proces globalizacije snažno povezan sa pitanjem bezbednosti, posebna pažnja je posvećena problemu međunarodnog povezivanja bezbednosnih mehanizama, koji koriste biometrijske sisteme. Ovo poglavlje sadrži pregled odgovarajućih međunarodnih standarda, koja se odnose na biometrijska elektronska dokumenta, kao i pregled stanja u Srbiji u oblasti elektronskih identifikacionih dokumenata.

Četvrto poglavlje rada, pod nazivom Menadžment identiteta i zaštita svedoka, posebno elaborira problem koji se pojavio, nakon primene biometrijskih sistema identifikacije, u važnom odbrambenom segmentu društva (Programu zaštite svedoka), kao mehanizmu zaštite od organizovanog kriminala i međunarodnog terorizma. Treba istaći da jačanje odbrambenih mehanizma društva uz pomoć biometrijskih tehnika istovremeno ugrožava normalan rad učesnika u Programu zaštite svedoka. Poglavlje sadrži mogući pristup merama unapređenja zaštite u slučaju široke primene biometrijskih sistema za utvrđivanje identiteta.

Peto poglavlje rada detaljno obrađuje pitanja vezana za utvrđivanje identiteta pomoću biometrijskih sistema. Opisane su sistemske prednosti i nedostaci takvih sistema, a izloženi su i mogući pristupi njihovoj

implementaciji. Sa više tehničkih detalja je elaborirano pitanje privatnosti u kontekstu biometrijskih sistema menadžmenta identitetom. Data je i jedna moguća klasifikacija biometrijskih sistema identifikacije.

Šesto poglavlje predstavlja tehničko-tehnološko produbljivanje u opisu rada tipičnih biometrijskih sistema za utvrđivanje identiteta na osnovu samo jedne biometrijske osobine čoveka. Imajući u vidu dominantnu upotrebu otisaka prstiju i slike lica u međunarodnim elektronskim identifikacionim dokumentima, kao i činjenicu da i nacionalna elektronska identifikaciona dokumenta koriste ove biometrijske modalitete, u ovom poglavlju su sa više pažnje opisani biometrijski sistemi identifikacije koji rade sa otiskom prsta, odnosno sa slikom lica. Uzimajući u obzir sve šire korišćenje glasovnih zapisa ljudi u postupcima identifikacije prilikom elektronskog poslovanja i pristupa obezbeđenim objektima ili uređajima, u ovom delu rada su detaljnije prikazani i biometrijski sistemi sa glasovnim zapisom. Za sva tri opisana biometrijska sistema identifikacije dat je pregled praktične primene, kao i pregled njihovih prednosti i nedostataka.

Sedmo poglavlje rada posvećeno je analizi rada i korišćenja multibiometrijskih sistema za utvrđivanje identiteta. Posebno su analizirani jednostavniji multibiometrijski sistemi koji rade sa više instanci jednog biometrijskog modaliteta, sa osvrtom na njihova ograničenja u praktičnom radu, ali i potrebom da ta ograničenja budu prevaziđena. Potom su analizirani multibiometrijski sistemi za utvrđivanje identiteta koji u svom istovremeno koriste više biometrijskih modaliteta. Izložena je opšta arhitektura takvih sistema i opisani mogući režimi njihovog rada. Posebna pažnja je data načinima povezivanja biometrijskih podataka u multimodalnim sistema, jer od načina njihovog povezivanja zavise i performanse sistema u realnim uslovima korišćenja.

Osmo poglavlje rada sadrži prikaz studije slučaja Multimodalni biometrijski sistem za utvrđivanje identiteta u slučajevima kada se koriste dva česta biometrijska modaliteta, otisak prsta i slika lica. Istraživanja obuhvaćena

studijom su realizovana u okviru Laboratorije za multimedijalne komunikacije pri Fakultetu organizacionih nauka, kao deo odgovarajućeg šireg Projekta.[7] Nakon postavke rešavanog problema, u ovom poglavlju je izložena primenjena metodologija rešavanja problema, kao i dobijeni rezultati. Najpre su opisani razlozi i načini formiranja dve korišćene biometrijske baze podataka, a potom je sa više detalja dat prikaz eksperimentalnog, ispitnog multimodalnog sistema za utvrđivanje identiteta. Izložena je njegova arhitektura, odabrani režimi rada, kao i postupak ispitivanja performansi ovog sistema. Posebno treba istaći deo ovog poglavlja u kojem su prezentovani rezultati ispitivanja. Završni deo osmog poglavlja je posvećen analizi i interpretaciji dobijenih rezultata radi određivanja performansi rada multimodalnog biometrijskog sistema.

Deveto poglavlje, Zaključak, sadrži kratak sumaran prikaz sprovedenih istraživanja i dobijenih rezultata.

Poslednje poglavlje sadrži listu korišćene literature u toku istraživanja.

[7] Projekat *Primena multimodalne biometrije u menadžmentu identiteta*, finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, pod zavodnim brojem TR-32013.

2. BIOMETRIJA I DRUŠTVENI IZAZOVI

2.1. Pojam biometrije

U literaturi postoji više definicija biometrije, ali se sve svode na činjenicu da biometrija predstavlja metod identifikacije, koji je zasnovan na fizičkim karakteristikama ili karakteristikama ponašanja osobe. Međutim, pojedini eksperti iz ove oblasti zastupaju još formalniju definiciju, tako što biometriju definišu kao naučnu disciplinu, koja se bavi identifikacijom pojedinaca statističkim metodama u slučajevima kada se koriste njihove biološke karakteristike ili karakteristike ponašanja. Svrha ovakvog naučnog istraživanja je uspostavljanje svojevrsne metodologije za rešavanje problema utvrđivanja identiteta prema navedenim kriterijumima. Da bi biološke karakteristike kvalifikovali kao biometrijske, one moraju biti *univerzalne* (svaka osoba mora posedovati datu karakteristiku), *jedinstvene* (karakteristika mora biti različita za sve članove populacije), *nepromenljive* (karakteristika ne sme da se menja pri različitim uslovima prikupljanja ili tokom vremena) i na kraju, karakteristika mora biti takva da joj se može *pristupiti* i mora biti *merljiva*.[8] Prednost korišćenja biometrijskih karakteristika se ogleda u tome što eliminišu potrebu za korišćenjem lozinki u situacijama kada se traži pristup privilegovanim resursima u našem okruženju, jer biometrijski podatak (otisak prsta, glas, geometrija lica...), koji se tom prilikom koristi može da zameni lozinku. Biometrijske karakteristike, za razliku od lozinki ili ID kartica, ne mogu biti izgubljene ili zaboravljene. Biometrija se oslanja na ono *što jesi* ili *kako se ponašaš*, umesto na ono *što znaš* (npr. šifra) ili *šta poseduješ* (npr. *ID* kartica). Sa stanovišta tehnologija koje se koriste u ostvarivanju prava pristupa zaštićenim resursima, biometriju susrećemo u tehnikama provere prava pristupa pri čemu se radi automatske provere identiteta koriste merljive fizičke karakteristike osobe.[9]

[8] Perry R. Cook, *Human Computer Interface Technology*, Biometrics Introduction and Issues, Princeton University, Princeton, New Jersey, USA, October 21, (2002).
[9] Jain, A.K.,A.Ross, S.Prabhakar. *An introduction to biometric recognition*. T.14.IEEE Trans. On Circuits and Systems of Video Technology, Jan (2004).

Ako pođemo od pojma identifikacije[10], koji u savremenom društvu odražava povezanost određenog podatka o ličnosti sa njom samom, može se slobodno reći da iz navedenog proizilazi da su biometrijske metode identifikacije građana bazirane na merenju određenih svojstava organizma specifičnih za svakog čoveka, u cilju potvrđivanja njegovog identiteta u društveno-institucionalnom smislu.

Sistemi koji u svom radu koriste biometrijske tehnike i tehnologije mogu se međusobno upoređivati na osnovu više kriterijuma. Jedan od vodećih svetskih naučnika u ovoj oblasti *Yau Wei Yun*, navodi upotrebu različitih tipova biometrije kroz sedam kriterijuma:

1. *Opštost* – opisuje koliko je česta data biometrijska karakteristika pojedinca u posmatranoj populaciji. Svaki pojedinac koji pristupa biometrijskoj aplikaciji mora imati datu biometrijsku karakteristiku. Problem može postojati ako osoba izgubi deo tela potreban za identifikaciju (prst, ruka, glasne žice..);
2. *Jedinstvenost* - pokazuje koliko precizno biometrijska karakteristika razlikuje jednog pojedinca od drugog. Mogući problem je kod jednojajčanih blizanaca, koji imaju isti DNK i otisak prsta;
3. *Trajnost* – biometrijska karakteristika se ne bi smela menjati prilikom različitih uslova prikupljanja i u toku određenog perioda u odnosu na posmatrani algoritam. Karakteristika podložna promenama nije podobna da bude biometrijska karakteristika. Problem nastaje ako dođe do fizičkih (anatomskih i strukturalnih) i funkcionalnih (fizioloških) oštećenja pojedinih delova tela (izmena lica, prsta, glas);
4. *Pristupačnost* – pokazuje jednostavnost odnosno stepen kompleksnosti prikupljanja i beleženja jedne biometrijske osobine. Biometrijski sistem treba da bude takav da ima mogućnost da digitalizuje prikupljenu biometrijsku karakteristiku koristeći

[10] Od latinske reči *identificare* -ustanovljenje identičnosti, istovetnosti.

odgovarajuće uređaje. Prikupljeni podaci moraju da budu podložni za obradu kako bi se izvukao skup reprezentativnih podataka;

5. *Performanse* – ovaj kriterijum obuhvata traženu preciznost, kako bi se prevazišla polazna ograničenja i zadovoljile potrebe aplikacije, kao i sredstva potrebna za postizanje takve preciznosti. Pošto je reč o višekriterijumskoj optimizaciji, problem je koji sistem izdvojiti kao optimalan;
6. *Prihvatljivost* – uređaji kojima se zahvataju biometrijski podaci treba da budu prihvatljivi sa stanovišta pojedinca, jer tada će da koriste i razvijene aplikacije. Dva aspekta uzimanja podataka za datu biometrijsku karakteristiku su posebno važna, jednostavnost postupka akvizicije i stepen narušavanja privatnosti;
7. *Zloupotreba* – ovaj kriterijum se odnosi na lakoću imitiranja određene biometrijske karakteristike od strane neovlašćenog lica, kao što su recimo lažni otisci prstiju, čime se kompromituje ceo sistem i stvara mogućnost za niz negativnih posledica;
8. *Pouzdanost* – pošto je reč o statističkom metodama rada, ni jedan biometrijski sistem nije sto odsto pouzdan, tako da uvek postoji mogućnost poboljšanja pouzdanosti;
9. *Cena* – važan kriterijum koji u praksi određuje rasprostranjenost upotrebe biometrijskog sistema. U potpunosti se sagledava i analizira ekonomska opravdanost takvog sistema: vrednost potrebne opreme, implementacije rešenja, instalacije, obuke, eksploatacije i pogonskog održavanja sistema.

2.2. Biometrija sa aspekta društvene opravdanosti

Razvoj informacionih tehnologija, u sadejstvu sa biometrijskim tehnologijama, stvara priliku za unapređenje nekih važnih procesa u informacionom društvu, ali u isto vreme iskustvo u primeni ovih tehnologija proteklih decenija nas upozorava na neophodnu opreznost. Primena

biometrijskih sistema poslednjih godina pored očiglednih poboljšanja otvara i nova pitanja, koja su složenija od tehničke izvodljivosti i implementacije same biometrije.

Da bi se biometrijski sistemi na najbolji način implementirali u društvu, neophodno je da postoji pozitivna relacija između građana i države, bazirana na principu dobrovoljnosti u primeni biometrije. Biometrijski sistemi su novi sistemi i ukoliko se polazi od činjenice da ljudi imaju različite stavove ka nepoznatom, onda je i očekivano da postoje barijere, odnosno otpor u primeni biometrijskih sistema u društvenom životu. Manji ili veći otpor ljudi, ili bar delova populacije, ka svemu što je novo, ili se bar na drugačiji način primenjuje, je poznat sociološki fenomen i o njemu se uvek mora voditi računa prilikom uvođenja novih tehnologija. Pravovremeno informatičko obrazovanje najšireg dela populacije stvoriće bolje uslove za uspešnu primenu biometrije, jer će se samo na taj način kod mnogih građana stvoriti realna slika o prednostima koje ona nudi, ali i mogućim slabostima o kojima zato pravovremeno treba voditi računa, u podizanju ukupnog nivoa bezbednosti savremenog društva.

Ako se osvrnemo na fenomen globalizacije i primenu biometrije kao mehanizma podrške ovom fenomenu, već na početku treba istaći da postojeće *kulturološke barijere*, koje se ispoljavaju u različitim religijskim načelima ili različitim običajima ljudi u jednom društvu, snažno utiču na opseg i dubinu njene primenu. Naime, određene grupe ljudi zbog religijskih uverenja neće prihvatiti biometrijske sisteme i na te grupe se biometrijske metode neće moći primeniti. Recimo, kod Hindusa postoji verovanje da fotografisanje uzima dušu osobe. Mnogobrojne islamske države, pak, primenjuju stroge verske zakone koji obavezuju žene da nose veo preko lica, skrivajući tako celo lice osim očiju. Drugi vid prepreka primeni biometrije može da se pojavi i u visoko razvijenim državama, na primer u Japanu, gde se ljudi pozdravljaju naklonom, dakle bezkontaktno. Pitanje je kako bi bila prihvaćena, recimo, kontrola pristupa objektu, u kojem bi postojala potreba za stalnim dodirivanjem ruku ljudi od

strane ovlašćenog lica kako bi se skener za otisak prsta adekvatno usmerio i uspešno uzeo otisak.

U takvim slučajevima, pred organizovanim društvom nije jednostavan zadatak jer, sa jedne strane, mora da nađe način da omogući primenu biometrijskih metoda, a sa druge da poštuje religijska uverenja ili običaje određenih grupa u društvu. Zbog toga, najcelishodnije je davati prednost onim rešenjima koja se zasnivaju na dobrovoljnoj osnovi.[11]

Čak i u društvima u kojima ne susrećemo navedene vidova ograničenja primeni biometrije, prosečan građanin se često neprijatno oseća zbog činjenice da neko o njemu prikuplja podatke, posebno ako su oni ličnog karaktera. Međutim, ukoliko bi se građanima na adekvatan način predočile prednosti biometrijskih sistema, praćene postojanjem adekvatne pravne regulative i institucionalizovanih mehanizama kontrole, a koje se odnosi na zaštitu privatnosti i zaštitu podataka, ta barijera bi se mogla prevazići.

Psihološka barijera postoji i kod uzimanja DNK uzorka kao biometrijskog podatka, s obzirom da DNK kao biometrijski identifikator omogućava uvid u informacije, ne samo o rasnoj i etničkoj pripadnosti, već i o postojanju nekih bolesti ili nedostataka. Treba napomenuti da su istraživanja u oblasti molekularne biologije i njene primene u domenu biometrije još uvek u ranoj fazi razvoja i da neće biti začuđujuće ukoliko u budućnosti iskrsnu i drugi problemi.

Navedeni problema stvaraju ograničenja u primeni biometrije i neminovno dovode do društvene diskriminacije pri implementaciji biometrijskih sistema. Do diskriminacije dolazi i zbog činjenice da nije moguće na isti način sakupiti sve biometrijske podatke pojedinaca. Dakle, odmah treba da se istaknemo važan stav da nema mogućnosti za ostvarivanje apsolutne unificiranosti i standardizacije u domenu rada sa biometrijskim podacima. Manji procenat ljudi u svakom društvu se rađa sa određenim nedostacima ili anomalijama, bilo fizičkim ili mentalnim, ili ih u životu nesrećnim slučajem

[11] http://collopy.case.edu/mbac423f05/projects/biometrics.pdf, pristupljeno 13.03.2013.

stiču, pa od takvih osoba nije uvek moguće prikupiti željene podatke standardnim metodama. Osobi koja nema kažiprst, otisak prsta nije moguće uzeti ustanovljenom metodom, kao što je slučaj i kod lica koje boluje od autizma i nije u stanju da razume način davanja podataka.

Takođe, kod nekih građana se javlja uznemirenost i negodovanje zbog mogućnosti da se društvo zasniva prevashodno na njima nerazumljivim visokim tehnologijama, i vodi tehnokratskim metodima, a ne demokratskim postulatima. To u društvu može stvoriti bojazan da sve to vodi svođenju građana na proste numeričke instance, pri čemu se pojedincima pruža značajna mogućnost manipulacije masama.

Veliki broj građana je zabrinut i zbog potencijalnog narušavanja njihovog zdravlja, koje se može desiti u procesu uzimanja biometrijskih podataka, na primer, primenom laserske tehnologije. Građanima se oduvek predočavalo kada je nešto zaista štetno, naročito ako se radi o jonizujućem zračenju koje je postalo i stereotip za štetnost po ljudsko zdravlje. Naročito je važno građanima objasniti da je najveći broj biometrijskih metoda potpuno neškodljiv za ljudsko zdravlje, ili su pak posledice toliko male, ili nemerljive, da su stoga zanemarljive. Neophodno naglasiti da, recimo, skener za uzimanje biometrijskih podataka oka nije nekakav laserski snop velike jačine, intenziteta i talasne dužine koja šteti biološkom tkivu i organizmu, već je takav snop daleko bezbedniji od, recimo, prosečnog ksenonskog bljeska blica fotoaparata ili „strob“ ili „laserskog“ svetla u mnogim klubovima ili diskotekama. Takođe, u slučaju kvara takvog uređaja, ne postoji ni jedan moguć scenario da se bezazlena svetlost određene talasne dužine naprasno transformiše u lasersku, recimo onu kojom oftamolozi smanjuju dioptriju na oku.

Još jedna u nizu barijera pri implementaciji biometrijskih sistema, ali ništa manje značajna, jeste i političke prirode. Pasivnost ili saradnja sa državom? Zanimljivo je istaći da je 2002. godine Američki statistički biro ministarstva pravde, *U.S. Bureau of Justice Statistic,* sproveo anketu *SEARCH* (*ORC-2002*) među ispitanicima koji su prošli neku vrstu biometrijske

identifikacije. Nakon sprovedene ankete, 88% ispitanika bilo je zabrinuto zbog postojanja mogućnosti zloupotrebe podataka o ličnosti, dok je na drugo pitanje da li ispitanik želi da sarađuje sa državom u primeni biometrije, kako bi se smanjio procenat krivičnih dela 80% ispitanika iskazalo da želi.[12] Dakle, postoji kontradiktornost među ispitanicima i njihovim stavovima po pitanju biometrijskih sistema i metoda, jer se stavovi anketiranih građana mogu okarakterisati kao odobravanje biometrijskih metoda, ali ako oni sami nisu u pitanju!

U vezi sa upotrebom biometrije, važno je sagledati pravni i politički aspekt problematike. Bitno je razjasniti odnos između države i građana kada je u pitanju odluka o primeni biometrije, kao i prepreke koje država treba da prevaziđe kako bi se ovaj sistem nesmetano primenjivao. Najvažnije je uvažavanje stavova građana, s obzirom da je za kvalitetnu implementaciju bilo kog sistema u društvu, u ovom slučaju biometrijskog sistema, neophodna njihova podrška. Naročito je bitno da država uvaži i preporuke eksperata iz oblasti gde se istražuje da li biometrijski sistemi menjaju politiku u određenom društvu i da li narušavaju odnose između države i građana.[13] Država mora preduzeti i sve potrebne mere kako ne bi došlo do povrede prava na privatnost i učiniti sve da jača poverenje građana u institucije javnog i privatnog sektora. To se postiže propisivanjem adekvatnih mera za zaštitu podataka o ličnosti i pružanjem informacija građanima o njihovim pravima i obavezama.[14]

Nivo *obrazovanja* društvene populacije u celini utiče na stepen prihvatanja ili neprihvatanja biometrije i biometrijskih sistema. Naime, manje obrazovani ljudi često imaju predrasude, otpor i teško shvataju i prihvataju novine, naročito nove i savremene sisteme. Takođe, nivo *tehnološke razvijenosti* jedne države utiče na stepen primene biometrijskih rešenja. Neka društva nemaju ekonomske mogućnosti za razvoj i primenu biometrijskih sistema.

[12] Nalini K. Ratha, Venu Govindaraju, *Advances in Biometrics: Sensors, Algorithms and Systems*, Springer, London, (2008), str. 423-425.
[13] Oliver Subotić, *Biometrijski sistemi identifikacije: (kritička studija),* Beograd, (2007).
[14] Strategija zaštite podataka o ličnosti, (Službeni glasnik RS, br. 58/2010 od 20.08.2010. godine).

Primena biometrijskih metoda i sistema na nivou države zahteva i znatna ulaganja, a to može da izazove nezadovoljstvo kod dodatno oporezovanih građana. Troškovi početnog investiranja koji se odnose na instalaciju biometrijskih sistema se mere milionima evra. U Srbiji su za instalaciju i primenu sistema za uvođenje biometrijskih ličnih karata i putnih isprava iz budžeta izdvojena značajna finansijska sredstava.[15]

Uzimajući u obzir predočene činjenice, može se zaključiti da su najbolji načini za prevazilaženje pomenutih barijera adekvatna informisanost i obrazovanje građana i potpuno pravno regulisanje te oblasti odgovarajućim zakonom i podzakonskim aktima, a da su stepen i načini uvođenja biometrije u upotrebu u bitnoj meri predodređeni ekonomskim i finansijskim kapacitetima države, kao i njenih građana, te da svaka krajnost, pre ili kasnije, dovodi do problema pri implementaciji biometrijskih sistema na nivou jedne države.

2.3. Pravni aspekti biometrije

Sa sigurnošću se može zaključiti da su nova dostignuća iz oblasti informacionih i komunikacionih tehnologija, pored brojnih koristi, donele i nove izazove, od kojih treba naglasiti one koji se odnose na korišćenje i upotrebu ličnih podataka. Brzina primena novih tehnologija, kao na primer Internet tehnologije, predstavlja poseban izazov u domenu prava, koje zahteva pažljivo i svestrano proučavanje problematike u određenoj oblasti primene tehnoloških inovacija, pre donošenja odgovarajuće pravne regulative. To se posebno odnosi na pravnu regulativu zaštite podataka, koja se neprekidno izgrađuje kako se širi primena biometrijskih tehnologija u identifikaciji i verifikaciji ličnosti. Regulisanje biometrije u jednom pravnom okviru veliki je izazov i nimalo jednostavan zadatak, budući da je neophodno uspostaviti ravnotežu između slobodnog protoka podataka i zaštite privatnosti. Nažalost, danas sve češće dolazi do zloupotrebe ličnih podataka. Zbog toga je neophodno

[15] Saša Paunović, *Primena specijalizovanih biometrijskih sistema za identifikaciju*, Magistarska teza, Fakultet organizacionih nauka, Univerzitet u Beogradu, Beograd, (2009).

obezbediti adekvatne pravne mere zaštite i informisati građane o njihovim pravima i interesima.

Kada je o evropskom zakonodavstvu reč, može se zaključiti da su sve članice Evropske unije i države kandidati uspostavile sisteme zaštite ličnih podataka, koji čine jedinstveni zakonski i institucionalni mehanizmi. Zakon o zaštiti ličnih podataka Republike Srbije iz 2008. godine većim delom je usaglašen sa pravom Evropske unije.

Novom strategijom zaštite podataka o ličnosti, koju je usvojila Vlada Republike Srbije, predloženo je da se nastavi usklađivanje domaće pravne regulative u oblasti zaštite ličnih podataka u skladu sa evropskom pravnom regulativom. Predloženo je i da se razgraniči upotreba biometrijskih podataka u javnom i privatnom sektoru, po uzoru na čl. 79 i čl. 80 slovenačkog zakona.[16]

Biometrijske tehnologije konstantno se unapređuju i usavršavaju, te je potrebno neprekidno pratiti postojeću pravnu regulativu u toj oblasti i po potrebi je menjati i dopunjavati, kako bi se obezbedila sigurnost prikupljenih podataka i ostvarila zaštita prava na privatnost.

2.3.1. Pravo na privatnost

Danas je sve češća primena biometrijskih metoda u poslovanju ili komunikaciji sa organima državne uprave, budući da one omogućavaju veću sigurnost u oblasti pristupa određenim podacima, dobra su preventivna mera kod zloupotrebe identiteta, olakšavaju transakcije podataka kod elektronske kupovine i imaju veliki značaj pri identifikaciji kriminalaca. Međutim, tako široka primena dovodi i do zabrinutosti pojedinaca zbog mogućnosti povrede prava na privatnost, te je iz tog razloga neophodno ovu oblast normativno regulisati. Način da se to uradi jeste da se sa jedne strane zaštiti poštovanje tog prava, a da se sa druge strane omogući nesmetana implementacija biometrijskih metoda. To nije jednostavan zadatak, imajući u vidu da je reč o osetljivim ličnim

[16] Strategija zaštite podataka o ličnosti, (Službeni glasnik RS, br. 58/2010 od 20.08.2010. godine)

podacima. U ovom momentu ne postoji zakonska definicija upotrebe biometrije niti u Evropi, niti na drugim kontinentima.[17]

Pravo na privatan život je jedno od osnovnih ljudskih prava zajemčenih Evropskom konvencijom o zaštiti ljudskih prava i osnovnih sloboda.[18] Ovo pravo, između ostalog, podrazumeva i zaštitu bilo kojih osetljivih ličnih podataka, kao što je slučaj i sa biometrijskim. Prema tome, zaštita biometrijskih podataka je pre svega bazirana na zaštiti privatnosti. Iz tog razloga, većina zemalja se oslanja se na zakonsku zaštitu podataka o ličnosti. Pravo na privatnost, između ostalog, znači „*mogućnost da svoj život vodite slobodno, bez instrukcija, autonomno i da kontrolišete pristup vašim ličnim podacima*". Elegantna definicija privatnosti jeste da je to kontrola nad tim kako i kada smo predstavljeni (prikazani) drugima.

Pravni akti kojima je zagarantovano pomenuto pravo na privatnost su Univerzalna deklaracija o pravima čoveka, Pakt o građanskim i političkim pravima i Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda. Univerzalnom deklaracijom o pravima čoveka iz 1948. godine zajemčena su građanska, politička, ekonomska, socijalna i kulturna prava. Iz čl. 12 pomenute Univerzalne deklaracije proizilazi da „*niko ne sme biti izložen proizvoljnom mešanju u njegovu privatnost, porodicu, dom ili prepisku, niti napadima na čast ili ugled. Svako ima pravo na zaštitu zakona protiv ovakvog mešanja ili napada*".[19]

Iz Pakta o građanskim i političkim proizilazi da „*niko ne može biti predmet samovoljnih ili nezakonitih mešanja u njegov privatni život, njegovu porodicu, u njegov stan ili njegovu prepisku, niti nezakonitih povreda nanesenih njegovoj časti ili njegovom ugledu*".[20]

---

[17] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 43–47.

[18] Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda, Rim, 4. novembar 1950. godine.

[19] http://www.sostelefon.org.rs/zakoni/12.%20Univerzalna%20deklaracija%20o%20ljudskim%20pravima.pdf, pristupljeno 11.03.2013.

[20] http://www.mhrr.gov.ba/PDF/MedunarodniPakt%20B.pdf, pristupljeno 11.03.2013.

Najvažniji dokument o zaštiti ljudskih prava u Evropi je Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda. Taj međunarodni ugovor potpisan je u Rimu 1950. godine. Srbija je ratifikovala ovu Konvenciju 2004. godine i od tog momenta građani naše zemlje mogu se obraćati Evropskom sudu za ljudska prava i podnositi individualne predstavke, ukoliko smatraju da su organi naše zemlje povredili njihova prava zajemčena Konvencijom. Građani se mogu direktno obratiti Sudu podnošenjem predstavke. Konvencija u svom materijalno-pravnom delu, između ostalog, u članu 8 reguliše zaštitu prava na privatnost i poštovanje porodičnog života, doma i prepiske. Iz tog člana proizilazi obaveza država da se, ne samo uzdrže od mešanja u privatnu sferu pojedinaca, već i da preduzmu pozitivne korake kako bi se pravo na privatnost zaštitilo. Evropski sud za ljudska prava je stalni Sud koji je ustanovljen 1959. godine. Njegovo sedište je u Savetu Evrope u Strazburu.[21]

2.3.2. Biometrijski podaci kao osetljivi lični podaci

Biometrijski podaci predstavljaju specifičnu kategoriju ličnih podataka, te iz tog razloga mogu biti korišćeni samo za određene, jasne i zakonom definisane svrhe uz primenu adekvatnih mera zaštite. Znači, pojedincima je potrebno pružiti zaštitu i sigurnost da njihov identitet neće biti ukraden i zloupotrebljen. Nedavni izveštaj Saveta Evrope govori o tome da odgovarajuća arhitektura biometrijskog sistema treba da bude izabrana u zavisnosti od njegove svrhe. Taj izveštaj preporučuje da kompletne informacije o svrsi ovog sistema moraju biti dostupne osobama čiji se biometrijski podaci i uzimaju. Te osobe moraju imati pravo uvida ispravke podataka o njima. Neophodna je kompletna transparentnost biometrijskog sistema, posebno ukoliko je sistem dizajniran za raznovrsnu upotrebu.[22]

[21] M. Paunović i S. Carić, *Evropski sud za ljudska prava nadležnost i postupak*, Centar za publikacije Pravnog fakulteta univerziteta u Beogradu, (2007).

[22]S.Paunović, D.Starčević, I.Milenković, *Menadžment identiteta i pitanja privatnosti*, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011).

Međunarodna biometrijska grupa podelila je rizik za privatnost na dve osnovne kategorije: ličnu privatnost, koja se odnosi na to da biometrijski postupci mogu ljudima biti neprijatni, i informacionu privatnost, koja podrazumeva mogućnost zloupotreba (neovlašćeno prikupljanje, upotreba, zadržavanje i otkrivanje) biometrijskih podataka. Činjenica, da se za vreme akvizicije biometrijskih podataka koristi deo nečega što je deo ljudskog bića ili sastavni deo interakcije sa okruženjem, vodi ka zaključku da je biometrijska transakcija "davanje informacija o sebi". Građani hoće da znaju posledice po njihov privatni život kada je u pitanju primena biometrije. Pored toga, biometrijska tehnologija je relativno nova, i prilično nepoznata širem krugu ljudi, pa zato ljudi prema njoj mogu imati unapred negativan stav i da sa rezervom prilaze njenom uvođenju.

Priliv novih tehnologija utiče na postojeću zakonsku regulativu. Zaista, sa pojavom novih tehnologija postojeći zakonski okvir biva prevaziđen i javlja se potreba da se osmisli drugi, usklađen sa novom stvarnošću, i da se postave društveno prihvatljive granice za njihovu upotrebu. To je upravo ono što se danas dešava sa uvođenjem biometrije u svakodnevne aktivnosti i njene implementacije u razne identifikacione dokumente. Pravni stručnjaci treba da istraže sa svog aspekta „šta je neophodno kako bi se zaštitio javni interes i obezbedili optimalni rezultati za društvo", jer objektivno postoji opasnost od zloupotreba.[23] Glavna opasnost jeste u tome što se biometrijske informacije, bilo da se koriste sa ili bez dozvole, mogu zloupotrebiti, na primer, radi neovlašćenog pristupa određenim podacima ili aplikacijama. Ono što posebno zabrinjava u pogledu korišćenja biometrije je sledeće: [24]

- biometrijski podaci se koriste u druge svrhe sem naznačenih prilikom skupljanja,
- biometrijski podaci se mogu skupljati bez dozvole,

[23] http://www.sostelefon.org.rs/zakoni/12.%20Univerzalna%20deklaracija%20o%20ljudskim%20pravima.pdf, pristupljeno 13.04.2013.

[24] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 43–47.

- biometrijski podaci se mogu prenositi bez dozvole,
- biometrijski podaci se mogu kombinovati sa drugim podacima o ličnosti radi dobijanja potpunije predstave o ličnosti,
- biometrijski podaci omogućavaju stvarni nadzor i profilisanje ličnosti.

Sa druge strane, uvođenje biometrije može ojačati zaštitu, bezbednost i efikasnost bilo koje transakcije. U prilog tome ide i činjenica da je pametno korišćenje biometrije jedan od najboljih načina za dokazivanje identiteta. U pogledu načina jačanja bezbednosti zajednice korišćenjem ovakvih sistema, postavlja se pitanje da li korišćenje biometrije može naneti štetu ljudskoj slobodi i privatnosti i da li treba menjati slobodu pojedinca za bezbednost zajednice. U modernom društvu posledice primene biometrije kada je u pitanju pravo na privatnost je veoma važno i osetljivo pitanje i zbog toga ga treba rešiti primenom, kako moralnih, tako i pravnih standarda.

2.4. Pravno regulisanje zaštite biometrijskih podataka

Pravno regulisanje zaštite podataka o ličnosti je složeno pitanje. Cilj pravnog regulisanja te materije jeste da se primena biometrijskih metoda zakonski uokviri, odnosno da se nacionalna zakonodavstva usaglase sa međunarodno pravnim principima i obavezama. Važnost dobre pravne regulative u toj oblasti ogleda se i u tome što je neophodno obezbediti i poštovanje načela zabrane diskriminacije. Neke zemlje u kojima se ne poštuje načelo vladavine prava mogu zloupotrebiti ove podatke, odnosno različito postupati u odnosu na određena lica ili grupe.

Za zaštitu prava na privatnost i zaštitu podataka o ličnosti, od velikog je značaja za ovu oblast razvijanje i prilagođavanje odgovarajućih informacionih tehnologija. Zakonodavac je zakonom regulisao pitanje obezbeđenja podataka i evidencije, kao i organizacione i tehničke mere za zaštitu podataka o ličnosti od zloupotrebe, uništenja, gubitka, neovlašćene promene ili pristupa. Kako bi pojedinci imali poverenja u te sisteme, uputno im je predočiti da nema neograničenog pristupa podacima, već da je pristup omogućen samo na osnovu

izričitih ovlašćenja za vođenje određenih upravnih, sudskih ili drugih postupaka.[25]

2.4.1. Međunarodna pravna regulativa

Na 25. Međunarodnoj konferenciji o zaštiti podataka i poverenicima za zaštitu privatnosti, održanoj u Sidneju septembra 2003. godine, usvojeno je pet rezolucija koje su tretirale problematiku zaštite privatnosti i jačanje zaštite podataka, od kojih se neke mogu primeniti i na slučajeve biometrijskog dokumentovanja identiteta, to su:[26]

- Rezolucija o unapređenju veze između zaštite podataka i razmene ličnih podataka. Cilj je da se postigne saglasnost o potrebi, kako privatnog, tako i javnog sektora, o boljoj razmeni informacija o načinu prikupljanja i obrade ličnih podataka. Uprkos trendu rasta broja različitih evidencija o ljudima, pojedinci nisu adekvatno informisani o tome kako mogu imati uvid u te podatke, u kojoj formi i sa kojim sadržajem.
- Rezolucija o transferu podataka o putnicima (u svetlu borbe protiv terorizma i organizovanog kriminala uz poštovanje određenih principa zaštite podataka o ličnosti).
- Rezolucija o zaštiti podataka i međunarodnim organizacijama. Mnoge međunarodne organizacije i njihova tela inicirale su uvođenje novih standarda u oblast zaštite ličnih podataka pri njihovoj razmeni na međunarodnom nivou. Na primer, inicijativa za dodavanje biometrijskih podataka u pasoše je potekla od Međunarodne organizacije za civilno vazduhoplovstvo.
- Predlog rezolucije o softveru za automatsko ažuriranje podataka sa ciljem da podstakne razvoj i implementacija tehnologija za ažuriranje softvera na način koji poštuje privatnost i autonomiju korisnika računara.

[25] Oliver Subotić, *Biometrijski sistemi identifikacije: (kritička studija)*, Beograd, (2007).

[26] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 43–47.

- Rezolucija o radiofrekvencijskim (*RF*) tehnologijama, s obzirom da ova tehnologija može omogućiti praćenje lica i povezivanje prikupljenih informacija sa postojećim bazama podataka.

Stavovi iz navedenih rezolucija služe nacionalnim zakonodavnim telima da definišu nacionalnu politiku u oblasti zaštite privatnosti podataka o ljudima. Na primer, u Švajcarskoj, poverenik za zaštitu podataka duže vremena je razmišljao pre nego što je doneo odluku o uvođenju biometrijskih podataka u identifikaciona dokumenta. Međutim, mnogo manje vremena mu je trebalo da zauzme stav da je uzimanja otisaka prsta u cilju identifikacije pri dolasku i odlasku sa posla, koji je potom pohranjen u smart karticu, u skladu sa zakonskim propisima o zaštiti podataka.

Na 26. međunarodnoj konferenciji o zaštiti podataka o ličnosti, održanoj septembra 2004. godine u Poljskoj, istaknuto je da prikupljanje i obrada biometrijskih podataka mora da zadovolji nekoliko osnovnih principa, i to:[27]

Princip zakonitosti - u privatnom sektoru, biometrijski podaci, u principu, mogu biti korišćeni samo uz odobrenje osobe na koju se odnose, a odobrenje mora biti dato slobodno, mora biti određeno i pojedinac mora biti upoznat sa razlogom davanja ličnih podataka.

Princip „dobre vere" - proces prikupljanja i obrade biometrijskih podataka mora biti transparentan i ne sme biti sproveden bez znanja osobe na koju se odnose.

Princip svrhe - ukoliko se isti cilj (npr. upravljanje pristupom zaštićenim resursima) može ostvariti na manje osetljiv način u smislu zadiranja u privatnost, kao što je verifikacija umesto identifikacije, onda ta tehnika treba da bude upotrebljena.

Princip proporcionalnosti - lični podaci se mogu prikupljati samo ako je to neophodno uz uvažavanje svrhe za koju se inače mogu prikupljati i obrađivati.

[27] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167, (2007), str. 43–47.

Princip zaštite - sigurnost biometrijskih podataka je primarna, pa mere obezbeđenja treba uključiti već u procesu akvizicije.

Najvažniji evropski i međunarodno prihvaćeni standardi značajni za normativno regulisanje ove oblasti su: [28]

- Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (1950), koja u članu 8. garantuje pravo na poštovanje privatnog i porodičnog života;
- Evropska konvencija o zaštiti lica u pogledu automatske obrade ličnih podataka Saveta Evrope, broj 108, usvojena 28. januara 1981. u Strazburu i Dodatni protokol uz Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka, u vezi sa nadzornim organima i prekograničnim protokom podataka, usvojen u Strazburu 2001. godine;
- Konvencija o sprovođenju Šengenskog sporazuma od 14. juna 1985. između vlada Privredne unije Beneluks, Savezne Republike Nemačke i Francuske Republike o postupnom uklanjanju kontrole na zajedničkim granicama (koju moraju poštovati sve države članice Šengenskog graničnog režima). Podneti podaci se mogu koristiti samo za svrhu koja je predviđena Konvencijom SE iz 1981. godine i to jedino od strane ovlašćenih organa. Upotreba u druge svrhe se može odobriti samo ukoliko nacionalni propisi država članica koje su podatak poslale to odobravaju. Konvencija takođe, propisuje da je država članica koja je poslala podatak odgovorna za njegovu tačnost i da strana koja prenosi netačne podatke može biti obavezana da nadoknadi eventualnu štetu. Istom Konvencijom regulisano je i uspostavljanje nezavisnog organa od strane ugovornica, koji je nadležan za sprovođenje nadzora nad zbirkom podataka nacionalnog dela Šengenskog informacionog sistema kao i za proveru zakonitosti obrade podataka koji su uneti u Šengenski informacioni sistem;

[28] www.poverenik.org.rs/index.php/sr/javna-rasprava.html i Strategija zaštite podataka o ličnosti, (Službeni glasnik RS, br. 58/2010 od 20.08 2010. godine).

- Direktiva Evropskog parlamenta i Saveta, o zaštiti građana u vezi sa obradom ličnih podataka i slobodnom kretanju tih podataka (95/46 od 24. oktobra 1995);
- Direktiva Evropskog parlamenta i Saveta, u vezi obrade ličnih podataka i zaštite privatnosti u elektronskom komunikacionom sektoru (2002/58 FC od 12. jula 2002);
- Direktiva Evropskog parlamenta i Saveta o zadržavanju generisanih ili obrađenih podataka u vezi sa odredbom u javnosti raspoloživih elektronskih komunikacionih servisa ili javne komunikacione mreže i dopune (2002/58/ES) i (2006/24) EU od 15. marta 2006;
- Direktiva 99/93/EC od 13. XII 99. godine koja reguliše standarde za digitalni potpis;
- Direktiva 00/31/EC od 08. VI 00. koja reguliše pravne okvire za elektronsku trgovinu;
- Direktiva 01/45/EC koja reguliše standarde za elektronsku administraciju, odnosno elektronske transakcije sa državnim institucijama i organima;
- Odluka 01/497/EC koja reguliše standarde za zaštitu ličnih podataka u transakcijama van EU.

Evropska konvencija o zaštiti lica u pogledu automatske obrade ličnih podataka Saveta Evrope značajna je, ne samo za države članice Evropske unije, već i za ostale države evropskog kontinenta. Ona predstavlja osnov za mnoge druge kako međunarodne, tako i nacionalne propise, koji regulišu pitanje ove zaštite. Cilj Konvencije jeste da dovede u sklad vrednosti, kao što su poštovanje privatnosti, s jedne strane i potreba slobode protoka informacija među narodima, sa druge strane.

Evropski savet zatim je doneo Direktivu za zaštitu podataka 95/46/EC. Pomenuta Direktiva reguliše zaštitu lica u odnosu na obradu ličnih podataka i njihovo slobodno korišćenje. Osnovni principi ove direktive su sledeći:

- Svođenje prikupljanja ličnih podataka na neophodnu (optimalnu) meru;

- Održavanje transparentnosti na najvišem nivou;
- Efikasna institucionalna i individualna kontrola obrade ličnih podataka na što efikasnijem nivou.

Cilj Direktive je usklađivanje zakonodavstva država članica i omogućavanje slobodne cirkulacije podataka i informacija unutar Evropske zajednice. Domen njene primene je širi od Konvencije jer se odnosi, kako na javni, tako i na privatni sektor. Direktivom je uspostavljena i ravnoteža između osiguranja zaštite, kao i slobodnog prometa podataka o ličnosti. Ona utvrđuje granice prikupljanja i rukovanja ličnim podacima, tako što zahteva od država članica da uspostave jedno ili više nadzornih tela čiji će zadatak biti zaštita podataka i praćenje primene zakonskih odredbi.

Direktive o privatnosti i elektronskim komunikacijama, regulišu zaštitu osnovnih prava i sloboda svakog pojedinaca, a posebno prava na privatnost, kao i zaštita legitimnih interesa pravnih lica u vezi sa obradom podataka o ličnosti u sektoru elektronskih komunikacija. Zanimljivo je istaći da ova Direktiva takođe predviđa još i mere praćenja usluga elektronskih komunikacija, s tim što propisuje da one moraju biti zasnovane na nacionalnim zakonima i neophodne radi zaštite javne i državne bezbednosti, odbrane i aktivnosti država u oblasti krivičnih postupaka ili ispunjenja ciljeva i potreba demokratskog društva. Direktiva takođe propisuje da podaci o telekomunikacionom saobraćaju određenog korisnika moraju biti, nakon izvesnog vremena, obrisani *ili anonimni* ukoliko više nisu neophodni za prenos komunikacija.

U skladu sa načelom proporcionalnosti, odnosno kako bi bezbednost mreža i usluga bila proporcionalna procenjenom riziku, posrednici u pristupu javno dostupnim mrežama i uslugama elektronskih komunikacija moraju da preduzmu sve potrebne tehničke i organizacione mere. U obavezi su i da korisnike informišu o mogućim rizicima i šteti koja može da nastane tokom, kao i o načinima zaštite komunikacija ukoliko nije u mogućnosti da pruži potrebnu bezbednost. Pojedina udruženja, kako u Evropi, tako i u Americi, takođe su

izradila kodekse ponašanja koja, zapravo, predstavljaju samoregulativu. S tim u vezi, treba pomenuti i Deklaraciju o prekograničnim tokovima podataka koja je vrlo kratka, sadrži samo četiri tačke osnovnih principa i tri tačke koje se odnose na dalje oblike rada vezane za određene kategorije prekograničnih tokova podataka.[29]

Iako nije donet poseban zakon koji bi se bavio problematikom biometrije, švajcarski Ustav, na primer, štiti pravo na privatnost i štiti od zloupotreba ličnih podataka. Takođe, švajcarski Zakon o zaštiti podataka za osnovni zaštitni objekat ima zaštitu ličnosti i osnovnih prava ličnosti, čiji se podaci obrađuju. Poverenik za zaštitu podataka u Švajcarskoj upozorio je na potencijalne probleme uvođenjem biometrijskog sistema. On je istakao da implementacija tog sistema mora da prati, između ostalog, poštovanje principa proporcionalnosti i konkretna primena propisa koji uređuju tu oblast.[30]

U Francuskoj je korišćenje biometrije dozvoljeno u skladu sa Zakonom o zaštiti podataka. Važnu ulogu u regulisanju te oblasti ima Savet za zaštitu podataka Francuske, koji je dao preporuke za zaštitu privatnosti prilikom korišćenja biometrijske tehnologije, tako što preporučuje korišćenje decentralizovanih baza podataka, uvažavanje principa proporcionalnosti i strogo poštovanje propisanih procedura.

Prvi poseban zakon u oblasti zaštite podataka donet je u Nemačkoj još 1970. godine. To je Savezni zakon o zaštiti podataka koji štiti pojedinca i njegovo pravo na privatnost. Međutim, kao i ostale evropske zemlje i Nemačka treba da implementira u svoj federalni zakon Direktivu o zaštiti podataka 95/46 EU. U oblasti zaštite podataka značajnu ulogu ima i Nemački ured za bezbednost informacija.

Kada je o Sloveniji reč, Zakon o zaštiti podataka o ličnosti reguliše pitanje biometrijskih podataka. Iz odredaba čl. 79 i čl. 80 tog zakona proizilazi da je odvojeno regulisana upotreba biometrijskih podataka u privatnom i

[29] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents,* Forensic Science International 167 (2007), str. 43–47.
[30] *Ibid.*

javnom sektoru.[31] Naime, prema članu 79 biometrijske mere u javnom sektoru mogu se predvideti zakonom ukoliko su neophodne radi bezbednosti ljudi i imovine, kao i radi zaštite poverljivih podataka i poslovnih tajni, odnosno kada se ti ciljevi ne mogu ostvariti manje nametljivim sredstvima. Prema članu 80 istog zakona proizilazi da privatni sektor može koristiti biometrijske postupke samo ukoliko su neophodni radi sprovođenja svojih aktivnosti, zaštite lica i imovine ili zaštite poverljivih podataka i poslovnih tajni. Takođe, iz istog člana proizilazi da lice koje prikuplja i radi sa biometrijskim podacima zaposlenih može da podnese pismeni zahtev nadzornom organu kojim zahteva uvođenje biometrijskih mera iz nekog drugog razloga.

U nekim zemljama kao što je Japan, ne postoji Zakon o zaštiti podataka već zaštitu sprovodi svako ministarstvo pojedinačno.

U anglosaksonskim zemljama (Sjedinjene Američke Države i Kanada), regulisanje pravne regulative polazi od "privatnopravne" zaštite ličnih prava i sloboda pojedinaca. To znači da se zaštita prava ostvaruje preko sudova na osnovu lične inicijative.

Sjedinjene Američke Države nemaju zakon o zaštiti podataka, već samo preporuke, a termin „privatnost" ne postoji u Ustavu Sjedinjenih Američkih Država. Još od 2001. godine Sjedinjene Američke Države teže normativnom regulisanju ove oblasti sa ciljem da se ojača nadzor nad građanima radi zaštite zemlje, posebno su značajni sledeći zakoni:[32]

US Patriot Act ima za cilj, između ostalog, da odvrati i kazni terorističke akte usmerene protiv Sjedinjenih Američkih Država, bilo da su izvršeni na teritoriji SAD-a ili širom sveta, kao i da ojača zakonske mehanizme istrage.

The US Public Law 107-71 (Zakon o zaštiti avionskog saobraćaja i transporta) reguliše upotrebu novih tehnologija u zaštiti avio saobraćaja, kao što je sistem za kontrolu pristupa zaposlenih na aerodromima.

---

[31] http://www.privatnost-srbija.com/skup2011/Resanovic.pdf, pristupljeno 17.12.2012.

[32] Flynn, A. A. Ross, Eds., *Handbook of Biometrics*, Springer, (Legal framework, privacy and social factors), (2008), str. 357-379.

The US Public Law 107-173 ima za cilj jačanje zaštite granica Sjedinjenih Američkih Država, kao što je uvođenje biometrijskih informacija u putne isprave.

US National Intelligence Reform Act (Nacionalni zakon o reformi obaveštajnog rada iz 2004). U ovom propisu upotreba biometrijske tehnologije se pominje kao način da se poveća bezbednost Sjedinjenih Američkih Država. Predviđa se upotreba biometrijskog ulaznog i izlaznog sistema za verifikaciju identiteta putnika na aerodromima i za prikupljanje biometrijskih podataka pri izlazu iz Sjedinjenih Američkih Država; razvoj integrisanog biometrijskog sistema proveravanja; upotreba biometrije za unapređenje zaštite putnih isprava i pilotskih licenci; uspostavljanje odgovarajućeg centra u nacionalnoj laboratoriji za biometriju i promociju istraživanja i razvoja biometrijskih tehnologija primenljivih u zaštiti avio saobraćaja.

US-VISIT program spada u mere zaštite za jačanje kontrole granica Sjedinjenih Američkih Država i treba da obezbedi verifikaciju identiteta posetilaca sa vizama i to prikupljanjem njihovih biometrijskih karakteristika, uzimanjem otiska dva prsta i fotografisanjem lica posetilaca.

Cilj akta *The US Real Act*, iz februara 2005. godine, jeste uspostavljanje i ubrzana primena regulative o vozačkim dozvolama i standardima zaštite identifikacionih dokumenata. Saglasno ovom pravnom aktu, koristiće se tehnologija za mašinsko čitanje svih vrsta, kako vozačkih dozvola, tako i ostalih kartica za identifikaciju. Iz navedenog akta proizilazi da se elektronski otisak prsta i fotografije uzimaju i čuvaju u elektronskim bazama za sve vozače, a takođe i za sve primaoce socijalne pomoći u Sjedinjenim Američkim Državama. Pored toga, *FBI* poseduje baze podataka otisaka prstiju svih osuđenih lica i svih prijavljenih izvršilaca krivičnih dela.

Zakon o zaštiti podataka u Velikoj Britaniji predviđa registar za zaštitu podataka i nadležnog registratora za vođenje evidencija o zaštiti podataka. U Velikoj Britaniji predložen je projekat stvaranja baze DNK profila čitave populacije. Današnja britanska baza najveća je na svetu i sadrži više od 4,5

miliona uzoraka, kako osuđenih, tako i osumnjičenih za izvršenje krivičnih dela. Britanski pravni sistem dozvoljava i čuvanje uzoraka DNK lica koja su optužena i oslobođena krivice za određeno krivično delo.

Na međunarodnoj konferenciji komesara za informacije i zaštitu podataka koja je održana u Madridu 5. Novembra 2009. godine usvojena je Madridska konvencija koja sadrži zajednički predlog Nacrta međunarodnih standarda zaštite privatnosti u pogledu obrade podataka o ličnosti. Rezolucija sadrži principe, prava, obaveze i postupke koje bi svaki sisteme zaštite podataka i privatnosti u savremenom svetu trebalo da obuhvati.[33]

2.4.2. Pravna regulativa u Srbiji

U Srbiji, do pred kraj 2008. godine, nije postojao zakon koji je definisao i određivao način prikupljanja, korišćenja, obrade i čuvanja podataka o ličnosti. Primarni uslov da se ostvari odgovarajuća zaštita podataka o ličnosti u Republici Srbiji jeste da nacionalno zakonodavstvo bude u potpunosti usaglašeno sa odredbama Direktive 95/46/EZ.[34]

Pravni okvir koji reguliše zaštitu ličnih podataka podrazumeva ratifikovane međunarodne ugovore i opšte prihvaćena pravila međunarodnog prava, koja su deo unutrašnjeg pravnog poretka, kao i postulate domaćeg zakonodavstva.

Ustav Republike Srbije članom 42. garantuje zaštitu ličnih podataka, pa se prikupljanje, držanje, obrada i korišćenje ličnih podataka uređuje zakonom. Zabranjena je i kažnjiva upotreba ličnih podataka izvan svrhe za koju su prikupljeni. Svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti u skladu sa zakonom kao i pravo na sudsku zaštitu u slučaju eventualne zloupotrebe. Republika Srbija potpisala je i ratifikovala Konvenciju Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti, koja je stupila na snagu 1. januara 2006. godine. U oktobru 2008.

[33] E. Miletić., S. Lilić,. D. Vitkauskas, *Podrška instituciji poverinika za informacije od javnog značaja i Zaštitu podataka o ličnosti*, IBF International Consulting, (2010).
[34] Nataša Pirc Musar, *Vodič kroz Zakon o zaštiti podataka o ličnosti,* Beograd, (2009).

godine, usvojen je Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka u vezi sa nadzornim organima i prekograničnim protokom podataka. Tokom procesa evropskih integracija, Srbija je zaključila Sporazum o stabilizaciji i pridruživanju sa EU, a koji obuhvata i obavezu da usaglasi svoje zakonodavstvo o zaštiti podataka o ličnosti sa pravom Evropske unije i drugim relevantnim evropskim i međunarodnim standardima.

U oblasti zaštite podataka o ličnosti, prvi korak je učinjen 2008. godine kada je donet danas važeći Zakon o zaštiti podataka o ličnosti, a koji je počeo da se primenjuje od 1. januara 2009. godine. Međutim, ni on nije u celosti usklađen sa Direktivom 95/46/EZ.[35]

Važno je napomenuti da je Vlada Republike Srbije avgusta 2010. usvojila Strategiju zaštite podataka o ličnosti, a kojom su utvrđeni ciljevi, mere i aktivnosti, uloga i odgovornost izvršne vlasti, nadzornog organa i drugih subjekata u ostvarivanju ovog prava.[36] Zakon o zaštiti podataka o ličnosti je opšti zakon koji reguliše prikupljanje, obradu i prenošenje podataka o ličnosti.

Cilj zakona jeste da u vezi sa obradom podataka o ličnosti, svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda. Taj zakon primenjuje se na svaku automatizovanu obradu, ali i na obradu sadržanu u zbirci podataka koja se vodi manuelno.

Jedno od važnih načela tog zakona je načelo zabrane diskriminacije što znači da zakon obezbeđuje zaštitu podataka o ličnosti svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva.

U smislu načela tačnosti i ažurnosti, obrada podataka o ličnosti nije dozvoljena ako je podatak neistinit ili nepotpun, odnosno kada nije zasnovan

[35] *Ibid.*
[36] Zakon o zaštiti podataka o ličnosti, (Službeni glasnik RS, br. 97/2008, 104/2009).

na verodostojnom izvoru ili kada je zastareo. To znači da obrađeni podaci o ličnosti moraju odgovarati stvarnim, najnovijim podacima i da su tačni. Zakonodavac je pojedincu dao mogućnost da se uveri da li su prikupljeni podaci tačni i ažurni. U slučaju da nisu, pokreću se odgovarajući postupci predviđeni zakonom.

Obrada podataka nije dozvoljena ukoliko nema pravnog osnova, a to može biti zakon ili pojedinac koji daje saglasnost. Pristanak se može opozvati pismeno ili usmeno na zapisniku. Naime, fizička lica imaju pravo da daju ili odbiju pristanak za obradu podataka, pravo na obaveštenje o obradi, pravo na uvid, kopiju kao i pravo povodom izvršenog uvida. Zakonodavac je takođe predvideo i slučajeve kada se može vršiti obrada ličnih podataka i bez pristanka lica na koje se ti podaci odnose, s tim što se prema tim izuzecima treba odnositi restriktivno. Kada je reč o obradi podataka osetljivog karaktera, podaci moraju biti posebno označeni i moraju biti obezbeđene odgovarajuće mere zaštite. Poverenik ima pravo uvida u te podatke i pravo provere zakonitosti obrade po službenoj dužnosti ili po zahtevu lica na koje se ti podaci i odnose.

U okvirima načela srazmernosti, dozvoljeno je obrađivati samo one podatke koji su očigledno potrebni i primereni za postizanje zakonske namene. Svrha mora biti precizno opredeljena, nepromenjena i dozvoljena. Zabranjena je i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije.

Zakonom je takođe propisano da lice čiji se podaci obrađuju mora biti obavešteno o obradi i o tome da ima pravo da traži ispravku ili brisanje nezakonitih ili pogrešno unetih podataka. Zakonom je regulisano i pravo na žalbu u slučaju povrede prava na zakonitu obradu podataka. U slučaju nepoštovanja prava na obaveštenje, uvid, kopiju, ispravku ili brisanje podataka, pojedinac ima pravo na žalbu.

Saglasno načelu zaštite, podaci moraju biti odgovarajuće zaštićeni od zloupotreba, uništenja, gubitka, neovlašćenih promena ili pristupa. Rukovalac i obrađivač dužni su da preduzmu tehničke, kadrovske i organizacione mere

zaštite podataka, u skladu sa utvrđenim standardima i postupcima, a koje su potrebne da bi se podaci zaštitili od gubitka, uništenja, nedopuštenog pristupa, promene, objavljivanja i svake druge zloupotrebe, kao i da utvrde obavezu lica, koja su zaposlena na obradi, da čuvaju tajnost podataka. Obezbeđenje podataka je jedan od ključnih elemenata zaštite podataka o ličnosti. Naime, obezbeđenje podataka je deo šireg pojma zaštite podataka. Poslove zaštite podataka o ličnosti obavlja Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. On je samostalan i nezavisni organ koji vrši nadzor nad sprovođenjem zaštite i obezbeđenja podataka o ličnosti, odlučuje po žalbi u slučajevima koji su ovim zakonom predviđeni i daje mišljenja o propisima.

Poseban akcenat treba staviti na odredbe Zakona kojima je regulisano pitanje zaštite zbirki podataka, imajući u vidu da su sve češće pojave krađe identiteta. Zbirka podataka je skup podataka koji se vodi automatizovano ili neautomatizovano i podaci mogu biti dostupni po ličnom, predmetnom ili drugom osnovu. Centralni registar omogućava da se zainteresovano lice upozna sa zbirkama podataka o ličnosti i tako lakše dođe do informacija o podacima koji su mu potrebni.[37]

Doneti su i propisi koji se neposredno ili posredno odnose na zaštitu podataka o ličnosti. Takvi su, na primer, propisi koji regulišu: slobodan pristup informacijama od javnog značaja, bankarski sektor, sektor penzijsko-invalidskog i zdravstvenog osiguranja, medicinsku dokumentaciju, sektor bezbednosti, sektor telekomunikacija, evidencije u oblasti rada, sektor oglašavanja i reklamiranja, arhivske građe, sektor tržišta hartija od vrednosti itd.

Zakon o zaštiti podataka o ličnosti je opšti zakon. Pored tog opšteg zakona postoje i posebni zakoni, odnosno zakoni kojima se regulišu pitanja iz tačno određenih oblasti, kao što su Zakon o ličnoj karti i Zakon o putnoj ispravi. Ovi zakoni su i u neposrednoj vezi sa zaštitom podataka o ličnosti.[38] U vezi sa

[37] Nataša Pirc Musar, *Vodič kroz Zakon o zaštiti podataka o ličnosti,* Beograd (2009).

[38]Strategija zaštite podataka o ličnosti, (Službeni glasnik RS, br. 58/2010 od 20.08.2010.godine).

tim zakonima urađeni su i podzakonski akti, odnosno Pravilnik o ličnoj karti i Pravilnik o putnoj ispravi. Kada je o podzakonskim aktima reč, njima se mogu urediti samo tehnički aspekti obrade podataka. Tu spadaju Uredba o obrascu za vođenje evidencije i načinu vođenja evidencije o obradi podataka o ličnosti (2009), Pravilnik o načinu prethodne provere radnji obrade podataka o ličnosti (2009) i Pravilnik o obrascu legitimacije ovlašćenog lica za vršenje nadzora po Zakonu o zaštiti podataka (2009). U pripremi je i nacrt Uredbe o načinu arhiviranja i merama zaštite naročito osetljivih podataka. Imajući u vidu da je tek 2008. godine u Republici Srbiji počelo normativno regulisanje oblasti zaštite podataka o ličnosti, nije začuđujuće što trenutno postoje veoma važne oblasti (marketing, video nadzor, upotreba biometrijskih podataka i dr.) u kojima još uvek nisu doneti odgovarajući pravni propisi.[39]

Zakon o ličnoj karti građanima Srbije dao je mogućnost da koriste lične karte sa čipom ili bez čipa, čime je Zakonom precizirana opcija izbora dokumenta sa biometrijskim podacima ili dokumenta bez biometrijskih podataka. Za razliku od Zakona o ličnoj karti, Zakon o putnoj ispravi, između ostalog, predviđa i obavezno unošenje biometrijskih podataka u putnu ispravu. Kod biometrijskih ličnih dokumenata (lična karta, pasoš) način unošenja biometrijskih podataka regulisan je Pravilnikom o ličnoj karti i Pravilnikom o putnoj ispravi.

Lična karta, u smislu Zakona o ličnoj karti, predstavlja javnu ispravu na osnovu koje građani Srbije dokazuju identitet.[40] Pored osnovnih podataka, lična karta sadrži i biometrijske podatke u elektronskom obliku. Zakonodavac u pomenutom zakonu, između ostalog, reguliše i sadržinu obrasca na kome se izdaje lična karta. Iz zakona proizilazi da obrazac na kome se izdaje lična karta sadrži podatke koji se odnose na određeno lice, (prezime, ime, pol, dan, mesec i godinu rođenja, mesto, opštinu i državu rođenja kao i jedinstveni matični broj), biometrijske podatke, prostor koji se odnosi na mikroelektronsku komponentu -

[39] www.poverenik.org.rs/index.php/sr/javna-rasprava.html, pristupljeno 19.12.2012.
[40] Zakon o ličnoj karti, (Službeni glasnik RS br. 62/2006 i 36/2011).

čip, prostor za mašinski čitljivu zonu za potrebe automatskog očitavanja podataka, kao i zaštitne elemente, zasnovane na PKI tehnologiji.

Način uzimanja biometrijskih podataka regulisan je Pravilnikom o ličnoj karti.[41] U skladu sa tim Pravilnikom, prilikom izdavanja lične karte, kao biometrijski podaci uzimaju se fotografija, otisak prsta i potpis. Ti podaci se uzimaju pomoću odgovarajućih tehničkih sredstava, a nakon toga se prevode u elektronski oblik.

Kada je o uzimanju fotografije reč, propisano je da se slika digitalnom kamerom ili se skenira fotografija koja je priložena uz zahtev. Zakonodavac je propisao i uslove koje mora da ispunjava digitalna fotografija građana:

1. veličina 50x50 mm, koja pokazuje prirodnu boju kože, sa pozadinom koja je jednobojna siva, na kojoj se ne vide druge osobe, delovi nameštaja i drugi predmeti;
2. 70-80% fotografije mora da zauzima slika lica;
3. fotografija mora biti visokog kvaliteta, oštra i jasna, bez mrlja i ogrebotina;
4. lice treba da gleda direktno u kameru, oči otvorene i jasno vidljive (bez kose preko očiju), usta zatvorena, da se jasno vide obe ivice lica, bez osmeha i grimasa;
5. za lice sa naočarima: da su oči jasno vidljive, da ram ne zaklanja bilo koji deo oka i da je bez refleksije.

Kao i u svakom društvu, tako i kod nas postoje određene grupe ljudi koji zbog nacionalne pripadnosti, veroispovesti ili narodnih običaja nose kapu ili maramu kao sastavni deo kulturne nošnje. Iz zakona proizilazi da u tom slučaju lice može biti fotografisano sa kapom ili maramom, a u skladu sa propisom o načinu uzimanja biometrijskih podataka.

Drugi biometrijski podatak koji se unosi u lične karte je otisak prsta. Uzimanje otiska prsta vrši se skenerom za otiske i podrazumeva uzimanje

[41] Pravilnik o ličnoj karti (Službeni glasnik RS br.11/2007 I 9/2007).

otiska levog i desnog kažiprsta, tehnologijom na dodir, valjanjem prsta u jednom pravcu od jedne do druge ivice nokta.

Međutim, postoje i situacije u kojima nije moguća primena te biometrijske metode. To je recimo slučaj kada lice nema kažiprst, ukoliko otisak skenerom iz bilo kog razloga nije moguć ili ukoliko lice nema prste. U slučajevima kada lice nema kažiprst, službeno lice dužno je da unese tu činjenicu na zahtev za izdavanje lične karte. Obavezno je i da upiše sa kojih prstiju su uzeti otisci i da sve to potvrdi svojim potpisom. Važno je istaći da se u takvim slučajevima otisak uzima sa narednog prsta i to sledećim redosledom: palac, srednji prst, domali i mali. Kada uzimanje otiska prsta skenerom nije moguće, kao i kada otiske nije moguće biometrijski obraditi, otisci se uzimaju na klasičan način, odnosno mehaničkim otiskom na kartonu, s tim što se u zahtevu za izdavanje lične karte obavezno unese napomena da je otisak uzet na klasičan način.

Treća situacija je situacija kada lice nema prste. U takvim slučajevima se na mestu za sliku otiska prsta upisuje oznaka ND (nije dostupno).

Pored fotografije i otiska prsta, uzimanje potpisa je treći biometrijski metod koji se primenjuje kod lične karte. On se uzima pomoću tabele za digitalizaciju potpisa. Potpis mora biti čitak, ispisan pisanim slovima i veran originalu. Do problema u takvim slučajevima može doći kada je reč o nepismenim licima ili kada iz drugih objektivnih razloga uzimanje potpisa nije moguće. Iz Pravilnika proizilazi da u takvim situacijama mesto za potpis u obrascu lične karte ostaje prazno. Za putne isprave kao ličnom dokumentu, postoji Zakon o putnoj ispravi.[42] Putna isprava, saglasno zakonu, predstavlja javnu ispravu koja našem državljaninu služi za prelazak državne granice, radi putovanja i boravka u inostranstvu, kao i za povratak u zemlju. Ona vlasniku služi za dokazivanje identiteta i državljanstva za vreme boravka u inostranstvu. Pod putnim ispravama podrazumeva se pasoš, diplomatski pasoš, službeni pasoš, putni list,

[42] Zakon o putnoj ispravi, (Službeni glasnik br. br. 90/2007, 116/2008, 104/2009 и 76/2010).

putne isprave koje se izdaju na osnovu međunarodnog dokumenta, kao i brodska i pomorska knjižica ukoliko je u nju uneta viza.

Ovim Zakonom je, između ostalog, regulisan i obrazac putne isprave. On sadrži prostor za upis podataka - prezime i ime, dan, mesec i godinu rođenja, mesto i državu rođenja, pol, državljanstvo, jedinstveni matični broj, kao i stranu državu u kojoj žive državljani Srbije bez prebivališta na teritoriji Republike Srbije. Iz istog zakona proizilazi da obrazac pasoša, diplomatskog pasoša i službenog pasoša sadrži i prostor za potrebe automatskog očitavanja podataka u koji se unose vidljivi alfanumerički podaci, kao i zaštitne elemente. Lice kojem je izdata putna isprava ima pravo da izvrši uvid u automatsko očitavanje podataka koje sadrži njegova putna isprava. Uzimanje napred pomenutih biometrijskih podataka regulisano je na sličan način, kao i uzimanje biometrijskih podataka za ličnu kartu, i to Pravilnikom o putnim ispravama.[43]

Na čip koji se nalazi u zakonskoj ispravi, i na kome postoje zaštitni mehanizmi za rad sa infrastrukturom javnih ključeva, PKI, unose se svi vidljivi podaci na biometrijskim dokumentima, a to su podaci o državljanstvu, prebivalištu odnosno boravištu, adresa kao i ime jednog roditelja. Na zahtev vlasnika lične karte, može se uneti i matični broj roditelja vlasnika lične karte, kao i kvalifikovani elektronski sertifikat vlasnika i odgovarajući podaci za formiranje kvalifikovanog elektronskog potpisa. Na taj način, biometrijski dokument postaje i sredstvo za formiranje kvalifikovanog elektronskog potpisa.

Imajući u vidu karakter biometrijskih podataka, zakonodavac je propisao obavezno neposredno prisustvo lica kome se uzimaju biometrijski podaci i izdaju biometrijska dokumenta.

[43] Pravilnik o putnim ispravama, (Službeni glasnik RS br. 54/2008 i 34/2010).

3. MENADŽMENT IDENTITETA

3.1. Identitet i važnost identiteta

Geopolitičke promene u poslednje dve decenije odrazile su se na sve aspekte privrede, politike, zabave i života ljudi uopšte. Proces globalizacije prati ne samo kretanje roba i kapitala, već i ljudi. Mobilnost ljudi je direktna posledica vladajuće paradigme globalne ekonomije. Ljudi putuju svetom bilo iz poslovnih razloga bilo privatno, na primer kao turisti. U masi onih koji svakodnevno prelaze granice ima i ljudi koji pripadaju svetu kriminala ili terorizma. Neki od njih putuju sa lažnim identitetom.[44]

Pod identitetom ličnosti podrazumevamo zbir opštih i ličnih znakova karakterističnih za jednu osobu po kojima se ona razlikuje od ostalih osoba i po kojima se sigurno može prepoznati, odnosno identifikovati.[45] To su nepromenljiva obeležja jedne osobe.

Na osnovu toga, identitet jedne osobe obuhvata sledeće elemente:

- *lični identitet* - čine podaci koji se dodeljuju svakoj novorođenoj osobi (ime, prezime, datum i mesto rođenja, podaci o roditeljima). Lični identitet takođe, podrazumeva i posedovanje jedinstvenog matičnog broja građana /JMBG/, koji je uveden u upotrebu sredinom sedamdesetih godina prošlog veka.
- *biografski identitet* – identitet koji osoba stiče tokom života, na primer, školovanjem, radom i iskustvima u različitim životnim okolnostima (lekarski kartoni, školske diplome, radna knjižica i mnoga druga zvanična dokumenta).
- *biometrijski identitet* u najširem smislu reči predstavlja skup podataka o biološkim, fiziološkim, anatomskim i ponašajnim karakteristika individue, specifičnim za tu osobu, i po kojima se ona može razlikovati

[44] S. Paunović, D. Starčević, *Multimodalna biometrija i menadžment identiteta*, Zbornik konferencije ITEO 2010, Banja Luka, Republika Srpska, BiH (2010).

[45] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.

od bilo koje druge. Preciznost ove kategorije identiteta se bitno uvećava korišćenjem više pojedinačnih biometrijskih komponenti, kao što su otisak prsta, otisak dlana, analiza fotografije lica osobe, skeniranje irisa i mrežnjače oka, analiza DNK uzorka, analiza glasa, analiza hoda i drugo.

Mogućnost dokazivanja identiteta je od ključnog značaja za uključivanje pojedinca u društveni život, a utvrđivanje identiteta je danas polazna tačka prilikom obavljanja raznih administrativnih aktivnosti. Moderno doba, akcentovano globalizacijom u kojoj lokalnost svih učesnika interakcije prestaje da bude osnova života i rada, povlači za sobom veliku potrebu za identifikacijom pojedinca, bilo da je reč o svakodnevnim, rutinskim stvarima ili pak ključnim bezbednosnim rizicima. Skoro svaka bezgotovinska transakcija zahteva potvrdu identiteta u određenom stepenu, te u zavisnosti od pouzdanosti utvrđivanja identiteta učesnika, zavisi i nivo poverenja u odvijanje ovakvih transakcija.

Sredstva pomoću kojih osoba dokazuje identitet mogu biti raznovrsna i razlikuju se prema mestu i načinu odvijanja transakcije. Kako bi se postigao viši nivo poverenja učesnika u ovom procesu potrebno je da postoji viši i pouzdaniji nivo provere identiteta.

Važnost biometrije i utvrđivanja identiteta posebno dobija na značaju pri upotrebi informaciono-komunikacionih tehnologija. Na primer, prilikom kupovine ili poslovne transakcije na Internetu, gde ne postoji neposredan kontakt osoba u interakciji, potreban je viši nivo provere identiteta korisnika. Taj nivo može biti baziran na tehnologiji *smart* kartica, digitalnim sertifikatima ili čak biometrijskim tehnikama pomoću otiska prsta ili digitalne fotografije.

Identifikacija učesnika u transakciji se u opštem slučaju može izvršiti na dva načina, proverom identiteta ili utvrđivanjem identiteta. Provera identiteta predstavlja postupak koji se sprovodi uvidom u javna dokumenta učesnika i zakonske isprave predviđene za tu svrhu, dok utvrđivanje identiteta

predstavlja složeniji postupak, koji se vrši posebnim metodama i tehnikama. Provera identiteta određene osobe vrši se, između ostalog i uvidom u ličnu kartu, pasoš ili vozačku dozvolu, jer ovi dokumenti sadrže i sliku osobe kojoj su izdati. Poređenjem detalja fotografije iz isprave i lica neke osobe uživo, možemo proveriti njen identitet.

Kompleksnost i potencijalni problemi pri utvrđivanju identiteta u savremenom svetu u žiži su interesovanja ne samo državnih organa i institucija, već i poslovnih organizacija, udruženja i pojedinaca. Nećemo pogrešiti ako tvrdimo da je problem utvrđivanja identiteta daleko širi od naznačenog i da se odnosi na celokupan život ljudi, na okruženje u kojem svakodnevno boravi i radi.[46] Na primer, na poslu većina ljudi koristi neku vrstu računarske opreme, bilo da je reč o *ATM* mašini, *POS* terminalu ili računaru na kojem se obavlja aplikacija iz domena administrativno-kancelarijskog poslovanja. Važno je utvrditi ko i pod kojim uslovima ima pravo pristupa nekom od takvih uređaja. Pitanje koje traži precizan i pouzdan odgovor u realnom životu može biti i ko je, i kada, poslao neke elektronske dokumente?

Većina ljudi koristi neku vrstu računarske opreme i Internet, preko kojih se obavljaju korisničke aplikacije. Danas još uvek u tim aplikacijama preovladava postupak identifikacije slanjem korisničkog imena i lozinke korespondentu u procesu komunikacije. Ovakvom vrstom identifikacije ne može se pouzdano utvrditi identitet osobe, odnosno da je zaista u pitanju osoba za koju se predstavlja, što je jedan od bitnih nedostataka ovakvog načina identifikacije. Jednostavne lozinke se lako pamte, ali i lako otkrivaju! Složenije lozinke se lakše zaboravljaju. U oba slučaja, neko ih može saznati i zloupotrebiti. Da bi se izbeglo zaboravljanje kompleksnih lozinki većina ljudi zapisuje lozinke, pri čemu one dobijaju fizičku realizaciju, pa mogu biti predmet krađe. Takođe, lična dokumenta, kao što su pasoši i kartice, mogu se

[46] A.K. Jain, A. Ross, S. Prabhakar, *An introduction to biometric recognition*, IEEE Trans. Circuits Systems Video Technol. 14 (1) (2004), str. 4–20.

izgubiti ili mogu biti klonirani ili ukradeni, što obično vodi ka zloupotrebi tuđeg identiteta.

Nažalost, podaci pokazuju da je zloupotreba identiteta krivično delo koje je sve češće u svetu, sa tendencijom porasta. Ova vrsta krivičnog dela je često u sprezi i sa drugim vrstama kriminalnih aktivnosti, kao što su pranje novca, trgovina ljudima, lažno predstavljanje i prikrivanje identiteta. Značaj prevencije krađe i zloupotrebe identiteta je najlakše predstaviti preko ekonomskih pokazatelja koji na egzaktan način, preko matematičkog modela, prikazuju ogromnu finansijsku uštedu u svim društvenim sferama, ako se koriste adekvatne bezbednosne tehnike i tehnologije, i primene najsavremenija naučna dostignuća, u borbi protiv zloupotrebe identiteta.[26]

Vodeće države, pre svih Sjedinjene Države, ulažu sve više finansijskih sredstava u prevenciju zloupotrebe i krađe identiteta, i na taj način zapravo štede ogromna finansijska sredstva kako svojih, državnih institucija, agencija i raznih organizacija, tako i svih njenih državljana. Korist od prevencije je, dakle, apsolutna i sveobuhvatna.[47]

Kada se analizira šteta nastala krađom identiteta, kloniranjem bankovnih kartica i telefonskih brojeva, dolazi se do iznosa od više milijardi dolara godišnje. Prema izveštaju Savezne trgovinske komisije Vlade Sjedinjenih Američkih Država iz februara 2013. godine samo od prevara nastalih krađom identiteta je pričinjena šteta od blizu jedne i po milijarde dolara!

U Velikoj Britaniji, prema podacima državne agencije za sprečavanje prevara, šteta od prevara nastalih zbog korišćenja tuđeg identiteta iznosila je sredinom prošle decenije 1,7 milijardi funti godišnje.[48]

Vrtoglav razvoj informacionih tehnologija i bitno pojeftinjenje hardvera specijalnih namena utiču na sve važniju primenu tehniko-tehnoloških sredstava u prevenciji zloupotrebe i efikasnog utvrđivanja identiteta osobe. Uređaji za biometrijsku identifikaciju nikada nisu bili dostupniji, tako da se već nekoliko

[47] A.K.Jain, A. Ross, S. Pankanti, *Biometric Identification*, CACM (2008).

[48] http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf, pristupljeno, juni (2013).

godina u nazad mogu naći u slobodnoj prodaji po relativno niskim cenama čak i za krajnje korisnike. Sve to mora dodatno ohrabriti vlade zemalja širom planete ka što efikasnijoj primeni nauke i tehnologije radi efikasnog utvrđivanja, kontrole i borbe protiv zloupotrebe i krađe identiteta na globalnom nivou.

3.2. Biometrijski identitet

Ako pođemo od pojma identifikacija, čija etimologija reči potiče od latinske reči *identificare*, a što znači utvrđivanje istovetnosti, identifikacija predstavlja povezanost određenog podatka o ličnosti sa njom samom. Iz napred navedenog proizilazi da su biometrijske metode identifikacije građana, bazirane na merenju određenih svojstava organizma specifičnih za svakog čoveka, a radi potvrđivanja njegovog identiteta u društveno institucionalnom smislu.[49]

Svaka osoba je jedinstvena i po svojim biometrijskim karakteristikama se razlikuje od drugih. Kriterijumi na osnovu kojih se razlikuje od drugih nazivaju se identifikacijska obeležja. Ako ih svaka osoba poseduje, onda su ta obeležja univerzalna. Obeležja su individualna - jedinstvena, ako su različita za svaku osobu. Da bi se praktično mogla iskoristiti, identifikacijska obeležja trebaju biti trajna i vremenski nepromenljiva. Takođe, bitno je da su dostupna u procesu akvizicije, kao i da nisu zahtevna i neprijatna tokom tog procesa. Biometrijski identitet je zasnovan na jedinstvenim biološkim (anatomskim[50] i fiziološkim[51]) i ponašajnim[52] karakteristikama. U anatomske karakteristike se, između ostalih, ubrajaju: otisak prstiju i dlana, mrežnjača i dužica oka, oblik i crte lica na specifičnim mestima, razmak među očima (ključan identifikacioni element kada je reč o prepoznavanju lica!), dok u ponašajne ili bihejvioralne karakteristike ubrajamo: svojeručni potpis, način i dinamiku hoda i slično. Pojedine

[49] Oliver Subotić, *Biometrijski sistemi identifikacije (kritička studija),* Beograd (2007), str. 17-21.
[50] Opis građe organa
[51] Opis funkcije organa
[52] Opis ponašanja pojedinca u datoj situaciji

karakteristike je teško svrstati u samo jednu kategoriju, kao što je to slučaj sa glasom.[53] Oprečna su mišljenja gde spadaju osobenosti glasa kao identifikacione komponente.

Opšte je mišljenje da će biometrijski identitet imati sve veću primenu širenjem upotrebe informacionih tehnologija, a posebno u elektronskim komunikacijama. Kod laptopova je kamera već standardna oprema (preko 90% prenosnih računara stiže sa integrisanom kamerom dobrog kvaliteta), dok je nešto slabija situacija sa integrisanim modulom za čitanje otiska prsta koji još uvek dolazi uz kvalitetnije serije prenosnih računara. Slična je situacija i sa najnovijom generacijom "tablet" uređaja (engl. *Tablet PC)*, kao i kod „pametnih" telefona (engl. *Smartphones*).

Pitanja u vezi sa identitetom su važna pitanja u modernom društvu i poslednjih godina je dosta uloženo napora da se biometrijski identitet iskoristi, kao pouzdano sredstvo u identifikaciji osoba. Ključna osobenost biometrijskog identiteta u celini, a i svih njegovih činilaca pojedinačno, pod uslovom da se pri evidentiranju biometrijskih karakteristika ispoštuje svaka procedura i norma, je originalnost i jedinstvenost identiteta bez mogućnosti falsifikovanja ili kopiranja.[54]

Upotreba biometrijskog identiteta sve više postaje svakodnevna realnost, kako na nacionalnom, tako i na globalnom nivou. Naime, građani se sreću sa biometrijskim aplikacijama u mnogim situacijama, a posebno u vezi sa međunarodnim putovanjima. Pored toga, primenu biometrijskog identiteta srećemo u mnogim društvenim aktivnostima kao što su putni dokumenti (vize, pasoši), kod pogranične kontrole, policijske službe, kontrole pristupa određenim objektima, elektronskog bankarstva.

Progresivna inovativnost specijalizovanih naučno-istraživačkih i komercijalnih institucija u primeni dostignuća na polju biometrije i zaštite

[53] D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents,* Forensic Science International 167 (2007), str. 154–159.
[54] A.K.Jain, A. Ross, S. Pankanti, *Biometric Identification*, CACM (2008).

identiteta deluje ohrabrujuće u stalnoj borbi na suzbijanju zloupotreba i falsifikovanja ličnog identiteta, a sve u vezi sa ostalim krivičnim delima u cilju podizanja nivoa bezbednosti svakog pojedinca, institucije i na kraju države u celini.

3.3. Menadžment identiteta i elektronska dokumenta zasnovana na biometrijskom identitetu

3.3.1. Menadžment identiteta

Protekle dve decenije smo svedoci rapidnog napretka informacionih tehnologija, tako da već sada živimo u zreloj eri digitalnog doba. Ali, ogroman rast udela informacionih tehnologija na tržištu razvijenih zemalja u novim poslovima ili novim načinima obavljanja postojećih poslova, otvara i nove mogućnosti za zloupotrebe i kriminalne radnje. Postojeći oblici borbe protiv visokotehnološkog kriminala nisu dovoljni, već se moraju razvijati nove, specifične protivmere. Raspoloživost novih računarskih tehnologija i novih proizvoda na bazi ovih tehnologija, omogućava kriminalcima razvijanje sofisticiranih sistema za kompromitovanje sistema za upravljanje pristupom zaštićenim resursima, i postupkom identifikacije kao njegovim sastavnim delom, pa se i takvi sistemi moraju kontinuirano unapređivati.

Problem upravljanja pristupom zaštićenim resursima na osnovu identifikacije korisnika računarskog sistema posebno je eskalirao pojavom Interneta. Razvoj Interneta i elektronskog poslovanja, permanentno su uticali na povećanje krivičnih dela izazvanih zloupotrebom identiteta. Ovakvi i slični problemi se mogu prevazići primenim menadžmenta identiteta, sistemom koji podržava korišćenje ličnih informacija prilikom pristupa podacima.

U najopštijem smislu, sistem menadžmenta identitetom se prema Nacionalnom institutu za standarde i tehnologiju Sjedinjenih Američkih Država (*NIST*) može definisati kao „*Integrisani sistem poslovnih procesa, skupa pravila i tehnologija koje omogućavaju organizaciji da uspostavi i upravlja pristupom korisnika kritičnim resursima koje nadzire organizacija, pri čemu sistem štiti poverljive*

informacije od neautorizovanih korisnika". Sistem menadžmenta identiteta je odgovoran za kreiranje, korišćenje i okončavanje elektronskih identiteta. Menadžment identiteta je sastavni deo savremenog multidisciplinarnog pristupa problemu komunikacije, koji daje kompletno rešenje u oblasti digitalnog prikupljanja podataka, odnosno akvizicije identifikacionih podataka (alfanumeričkih i biometrijskih), obrade navedenih podataka, njihove integracije sa postojećim bazama podatka i formiranja novih baza podataka.[55]

Savremena tehnologija doprinosi uspostavljanju pouzdanog menadžmenta identiteta, tako što visoko pozicionira upotrebu biometrijskih karakteristika u formiranju, održavanju i korišćenju elektronskog identiteta, koji će prirodno povećati njegovu upotrebljivost i efikasnost u svetu elektronskih komunikacija, te dalje doprineti smanjenju zloupotreba.[56]

Tipična prvobitna primena menadžmenta identiteta se može sagledati navođenjem sledećih slučajeva:

- Logička kontrola pristupa (pristup podacima u personalnom računaru, pristup računarskim mrežama, pristup bazama podataka, pristup mobilnim uređajima),
- Evidentiranje i kontrola fizičkog pristupa (pristup sefovima u bankama, kontrola celokupne državne granice),
- Evidentiranje vremena dolaska i prisustva (na primer, radnika zaposlenih u poslovnim organizacijama i ustanovama),
- Utvrđivanje autentičnosti učesnika u elektronskim transakcijama (postupci kojima se utvrđuje identitet i održava integritet transakcija),
- Elektronska identifikaciona dokumenta za građane.

[55] Saša Paunović, *Menadžment identiteta i elektronska dokumenta zasnovana na biometrijskom identitetu,* Simpozijum o operacionim istraživanjima, Zbornik radova SYMOPIS 2011, Ekonomski fakultet, Beograd, (2011).

[56] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.

Ubrzani razvoj menadžmenta identiteta doveo je do širenja njegove primene u mnogim područjima:

- Primena u oblasti državne uprave (elektronska identifikaciona dokumenta, putne isprave, vozačke dozvole, saobraćajne dozvole, dozvole za nošenje oružja, kartice za socijalnu zaštitu, socijalnu pomoć i penzije, kartice za zdravstveno osiguranje, *e-government*...)
- Komercijalna primena (kreditne i debitne kartice u bankarstvu, elektronsko bankarstvo, elektronsko poslovanje, elektronska trgovina, mobilna telefonija sa naprednim *SIM* karticama, vozne karte u gradskom transportu, TV pretplata za satelitske i kablovske sisteme, članske karte i druge elektronske kartice...)
- Lična primena (zaštita stanova, zaštita automobila, zaštita u većem broju ličnih prenosnih elektronskih uređaja- *gedžeta*)

Treba naglasiti da se u digitalnom svetu uobičajeni metod identifikacije još uvek zasniva na principu da korisnik *nešto zna* što predstavlja zajedničku tajnu sa drugim učesnikom u komunikaciji, odnosno da se korisnik predstavlja sistemu pomoću korisničkog imena i lozinke. U pogledu postupka identifikacije, identifikacioni dokument baziran na *smart* kartici sa integralnim kolom, čipom, ima višestruke prednosti u poređenju sa drugim rešenjima. Ugrađeni memorijski čip može sadržati znatno više podataka nego bilo koje drugo sredstvo za zapis podataka (na primer, bar kod, magnetna traka, optička traka). Sem toga, veoma precizni, zaštitni mehanizmi čuvaju podatke na *smart* kartici od nedozvoljenog pristupa i sprečavaju nedozvoljene obrade podataka. Zbog navedenih osobina *smart* kartice su više nego pogodne za smeštanje biometrijskih podataka vlasnika. Ugrađen čip može da pre zapisivanja u memoriju vrši šifrovanje unetih podataka.

Da bi se sa raspoloživim tehnologijama postigla veća pouzdanost, poželjno je istovremeno korišćenje više različitih metoda identifikacije. Na primer, korišćenje *smart* kartica sa ugrađenim kvalifikovanim sertifikatom za

digitalni potpis, otiskom prsta i standardnim sistemom identifikacije sa lozinkom bitno bi podiglo pouzdanost utvrđivanja identiteta.

3.3.2. Elektronska identifikaciona dokumenta zasnovana na biometrijskim karakteristikama

Pojava fenomena globalnog terorizma u protekloj deceniji i nemogućnost vodećih zemalja sveta da mu se konvencionalnim protivmerama društva efikasno suprotstave, u prvi plan je postavila zahteve za izgradnjom globalnog bezbedonosnog sistema. Takav „štit" bi, pre svega, funkcionisao preventivno, tako što bi pravovremeno otkrivao namere i planove grupa ekstremista, a potom efikasno pratio kretanje otkrivenih ekstremista i osujetio njihovo delovanje. Prvi deo bezbedonosnog sistema odnosi se na mogućnost praćenja svih vidova komunikacija na Internetu, fiksnoj i mobilnoj telefoniji, radiokomunikacija, poštanskog saobraćaja, novina,... Drugi deo ovog sistema odnosi se na globalni nadzor kretanja svih putnika u međunarodnom saobraćaju. Da bi se pravno uredio ovaj bezbedonosni sistem, ove zemlje su donele više već navedenih zakona, od kojih neki ozbiljno dovode u pitanje ustavne slobode građana, pa time i pravo na privatnost, ali koji se opravdavaju ugroženošću zemlje na osnovu trenutne situacije u pogledu ekstremizma. Upravo je strah od terorističkih napada uticao na pojavu svetskog trenda uvođenja obaveznih elektronskih identifikacionih dokumenata, kao i putnih isprava koje uključuju biometrijske pokazatelje (obavezno digitalnu sliku lica, a opciono otisak ili otiske prstiju, sliku dužice oka...).Uvođenje u upotrebu elektronskih dokumenata baziranih na biometrijskom identitetu u različitim državama ima i različite primarne ciljeve. U Republici Srbiji, koja ima složenu bezbednosno-političku situaciju, za biometrijski sistem identifikacije se ne može odrediti samo jedan primarni cilj, već je namena ovakve vrste dokumenata višestruka: efikasniji rad svih organa državne uprave, pružanje najrazličitijih vidova elektronskih usluga građanima, podrška elektronskom poslovanju,

suzbijanje krivičnih dela vezanih za zloupotrebu ili krađu identiteta, ali i najkompleksniji vid prevencije potencijalnog terorističkog delovanja.[57]

Prednosti elektronskih identifikacionih dokumenata su mnogobrojne, a nedostataka gotovo i da nemaju, ako se porede sa tradicionalnim dokumentima. Dugotrajnost, mogućnost recikliranja, visok stepen zaštite od falsifikovanja, pojednostavljen postupak u slučaju gubitka, krađe ili kvara, samo su neke u nizu prednosti.

Kombinacija *smart* kartice i biometrijskih tehnika, koja se ogleda u integrisanom smeštanju i ličnih i biometrijskih podataka na ovakvu karticu, predstavlja podesno i pouzdano rešenje za utvrđivanje identiteta lica, pa je to dovelo do opšteg trenda u svetu da se unaprede postojeća elektronska identifikaciona dokumenta dodavanjem biometrijskih podataka osoba (otiska prsta, otiska dlana, digitalne fotografije, slike dužice oka, čak i *DNK* markera).[58] Bitno unapređenje elektronskog identifikacionog dokumenta, snabdevenog biometrijskim karakteristikama vlasnika, postiže se proširivanjem funkcionalnosti *smart* kartice elementima koji podržavaju komuniciranje sa infrastrukturom javnih ključeva (engl. *Public Key Infrastructure, PKI)*. Danas *PKI* pruža značajnu zaštitu podataka na elektronskom dokumentu. Elektronska dokumenta zasnovana na biometrijskom identitetu zajedno sa *PKI*-om omogućavaju brzu i pouzdanu identifikaciju i autentifikaciju njenog vlasnika u elektronskoj komunikaciji.[59] Posebna pogodnost ovakvih dokumenata leži u činjenici da osoba svoje biometrijske podatke nosi "*sa sobom*" u računarski čitljivom obliku, tako da je moguća veoma brza lokalna provera identiteta i kada je *PKI* infrastruktura nedostupna. Ovlašćeno lice pomoću čitača elektronskog dokumenta vrši poređenje biometrijskih podataka upisanih na čipu, na primer otiska prsta, i onih uzetih na licu mesta, odnosno otiska uzetog pomoću lokalnog skenera otisaka. Elektronska lična isprava je multiaplikativna

[57] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.
[58] *Ibid.*
[59] Radna grupa, *„Osnovni koncepti novih elektronskih identifikacionih dokumenata“*, MUP, (2004).

PKI kontaktna *smart* kartica za rad sa različitim operativnim sistemima, softverskim i hardverskim mehanizmima za zaštitu (algoritmima sa kriptografskim ključevima, hardverskim generatorom ključeva na čipu...) i funkcijama bezbednog čuvanja podataka od neovlašćenog pristupa.[60]

3.3.2.1. Tehnologija smart kartica kao osnova za izradu biometrijskih elektronskih dokumenata

Tehnologija *smart* kartice pripada grupi specifičnih informacionih tehnologija. Zbog mnogih prednosti koje nudi u praktičnoj primeni, postala je široko primenljiva u mnogim oblastima ljudske delatnosti, a posebno u zadacima koji zahtevaju pouzdano utvrđivanje identiteta. Brzina rada, jednostavnost upotrebe i niska cena razvoja i implementacije su važne prednosti koje nudi ova tehnologija u slučajevima kada je reč o daljinskom, posrednom, preciznom, nedvosmislenom i blagovremenom utvrđivanju identiteta osobe uključene u neku transakciju. Posebno treba naglasiti da se sve to postiže uz podršku adekvatnih mehanizama zaštite podataka na *smart* kartici od zloupotrebe. *Smart* kartice su postale standardni element u elektronskim transakcijama u svetu, pa i u Republici Srbiji u vezi sa digitalnim skladištenjem ličnih podataka.

Smart kartice su u osnovi specifičan mikroprocesorski računarski sistem postavljen na jeftinu plastičnu podlogu. Svaki računarski sistem, pa tako i onaj na *smart* kartici, sadrži procesor sa određenom količinom *RAM* memorije za obradu podataka u digitalnom obliku, poznat pod kolokvijalnim nazivom *čip* (engl. *chip*). Pored *RAM* memorije čip sadrži i određenu količinu memorije koja obezbeđuje trajan zapis spolja unetog sadržaja. Prema načinu trajnog zapisivanja ovih podatka ove memorije mogu biti *ROM* tipa, u slučaju kada se podaci mogu upisati samo jednom, a potom čitati više puta, ili *EEPROM* tipa, što im omogućava da se zapamćen sadržaj povremeno ažurira. Zapamćeni

[60] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.

trajan sadržaj po svojoj prirodi može biti aplikativni program, koji određuje namenu *smart* kartice, ili podaci koje će ovi aplikativni programi koristiti.

Smart kartice mogu biti kontaktne i bezkontaktne. Kontaktna *smart* kartica zahteva da se pre upotrebe mehanički postavi u odgovarajuće podnožje elektronskog uređaja, čitač ili pisač. Bezkontaktna *smart* kartica razmenu podatka sa računarskim sistemom ostvaruje posredstvom posebnog antenskog sistema, a po tehnologiji može biti *RFID* ili *NFC*. *Smart* kartice nemaju bateriju, već električnu energiju potrebnu za rad procesora dobijaju iz spoljnjeg sveta, preko kontakata ili preko antenskog sistema. Čip koji je ugrađen u *smart* karticu je veoma složen i može da vrši hardversko i programsko šifrovanje i dešifrovanje podataka, što je posebno važno u finansijskim transakcijama ili u slučajevima kada se koristi infrastruktura javnih ključeva, *PKI*. *Smart* kartica memoriše podatke u šifrovanoj, zaštićenoj formi.[61] Velika prednost *smart* kartica je lokalno memorisanje podataka, što znači da nije neophodna veza sa centralizovanom bazom podataka, da bi se kartica mogla koristiti. Podaci su memorisani u samom elektronskom dokumentu koji je pohranjen na kartici, odnosno vlasnik je nosilac svojih ličnih podataka i to u zaštićenom - šifrovanom obliku. Dakle, eventualna zloupotreba nije na nivou celog sistema, što bi moglo da dovede do epidemijskih razmera, već se svodi na pojedinačnu zloupotrebu. Sistem je, kao celina, bezbedan. Navedene osobine čine *smart* karticu jednim od najboljih nosilaca ličnih i drugih poverljivih podataka, koji obezbeđuju veoma pouzdani dokaz identiteta njenog vlasnika, što je poznato ne samo mnogim vladama, već i poslovnim organizacijama. Ono što predstavlja posebnu prednost *smart* kartica u primeni, je činjenica da jedna *smart* kartica sa stanovišta korisnika može biti multifunkcionalna, odnosno da kombinuje funkciju elektronskog identifikacionog dokumenta - legitimacije sa funkcijom elektronske vozačke dozvole. Ugrađeni čip pouzdano će razdvajati različite

[61] *Ibid*.

aplikacije i pripadajuće podatke. Takođe, čip omogućava primenu različitih nivoa autorizacije za pristup različitim aplikacijama.[62]

U budućnosti će se verovatno naći još snažniji i bolji vidovi zaštite i načini čuvanja podataka, kao i rešenja za proveru i utvrđivanje identiteta, no trenutno su rešenja zasnovana na primeni tehnologije *smart* kartica najbolja. Posebna pogodnost koju nudi tehnologija *smart* kartice je njeno korišćenje u mrežnim transakcijama koje zahtevaju rad sa kvalifikovanim digitalnim sertifikatima i digitalnim potpisom, čime se pruža siguran pristup i rad sa brojnim elektronskim servisima. *Smart* kartice nude zaštitu podataka u prenosu baziranu na upotrebi jakih algoritama u kriptografiji, zasnovanih na upotrebi ne samo tehnike šifrovanja sa simetričnim ključem, već tehnike šifrovanja sa asimetričnim ključeva koju implementira infrastruktura javnih ključeva, *PKI*.

Elektronski identifikacioni dokument, *eID* baziran na *smart* kartici i *PKI* arhitekturi mora imati najmanje dva privatna ključa za vlasnika te kartice, a po potrebi i više. Privatni ključevi su zaštićeni od zloupotrebe, kako hardverskim i softverskim rešenjima kartice, tako i zahtevima za unosom lozinke za autentifikaciju, personalnog identifikacionog broja, *PIN* ili biometrijske karakteristike, pre samog korišćenja kartice.

Za potrebe identifikacije vlasnika u elektronskim transakcijama, identitet vlasnika kartice prethodno proverava ovlašćeni sertifikacioni autoritet, *CA* koji izdaje i garantuje kvalifikovane digitalne sertifikate. Digitalni sertifikat sa ličnim podacima vlasnika sadrži i odgovarajući javni ključ čime se utvrđuje pouzdana veza vlasnika i javnog ključa. Tako izdat i proverljiv digitalni sertifikat postaje dokaz elektronskog identiteta vlasnika jednako kao što je zakonska identifikaciona isprava građana sa fotografijom – legitimacija, dokaz identiteta vlasnika u svakodnevnom životu.[63] Elektronski identifikacioni dokument, *eID* je namenjen svom vlasniku prvenstveno za dokazivanje da je upravo on ta osoba čiji se identitet utvrđuje ili potvrđuje. *eID* sadrži privatan

[62] Radna grupa, *„Osnovni koncepti novih elektronskih identifikacionih dokumenata“*, MUP, (2004).
[63] *Ibid*.

ključ koji je na specifičan način uparen sa javnim ključem vlasnika, ali naravno ključevi nisu isti! Kao što samo ime kaže, javni ključ je dostupan radi provere identiteta vlasnika, a privatni ključ je tajan i može ga upotrebiti isključivo vlasnik *eID* dokumenta. Uloga privatnog i javnog ključa može se videti na sledećem primeru. Kada preko Interneta šaljemo nalog za finansijsku transakciju našoj banci, nalog ćemo, pre slanja šifrovati javnim ključem banke. Banka će nakon prijema takvog šifrovanog naloga isti i dešifrovati, odnosno učiniti čitljivim, korišćenjem svoga privatnog ključa. Iz ovoga primera vidimo na koji su način privatni i javni ključ upareni. Ako se tekst šifruje jednim ključem, može da se dešifruje samo onim drugim ključem!

U navedenom primeru ostaje problem poverenja banke u dobijen nalog za finansijsku transakciju, odnosno da li smo zaista mi dali platni nalog kojim će biti skinuta sredstva sa našeg računa ili je to uradio neki uljez umesto nas. Sumnja se otklanja tako što ćemo pre slanja na ranije opisan način šifrovanog platnog naloga našoj banci digitalno potpisati taj platni nalog. Za digitalni potpis koristi se kraći tekst, izveden poznatim načinom iz sadržaja platnog naloga u formi sažetka, ali sada šifrovan našim privatnim ključem, koji se takođe šalje banci. Banka će upotrebiti naš javni ključ, a za koji ima garanciju trećeg lica – sertifikacionog autoriteta, *CA*, da je to naš elektronski identitet, kako bi ponovo rekonstruisala sažetak platnog naloga. Kako je poznat način na koji se sažetak izvodi, banka će ponoviti izvođenje sažetka na osnovu dešifrovanog platnog naloga i samo će u slučaju kada su oba sažetka identična, prihvatiti će platni nalog.

Dakle, sertifikacioni autoritet izdaje digitalni sertifikat koji jedinstveno identifikuje potpisnika. Digitalni potpis takođe garantuje neporečivost poslate elektronske poruke. Treba još dodati da se moguća prevara slanjem ponovljene elektronske poruke sprečava uključivanjem u poruku jedinstvenog broja (engl. *nonce*) koji se više ne može ponovo koristiti u komunikaciji. Uobičajeno sastavni deo ovog jedinstvenog broja je i vreme slanja poruke. Opisani mehanizmi obezbeđuju tajnost poruke, njen integritet, autentičnost izvora poruke,

neporečivost zahtevane elektronske transakcije, kao i sprečavanje kompromitovanja sistema ponovnim slanjem prethodno snimljene originalne poruke.[64]

Iz praktičnih razloga, u memoriju čipa na *smart* kartici se smeštaju i sertifikati sa odgovarajućim privatnim ključevima za druge elektronske usluge. Ovo omogućava različitim aplikacijama dobijanje pripadajućih sertifikata sa parom ključeva, što sve doprinosi uspostavljanju pouzdane veze korisnik usluge - davalac usluge.[65]

3.3.2.2. Biometrijska elektronska dokumenta i međunarodni standardi

Osnovno obeležje svake lične karte, i koje je čini posebnim, je Jedinstveni Matični Broj Građana (JMBG). Taj podatak je ključan za identifikovanje svake osobe u Republici Srbiji. U Sjedinjenim Američkim Državama je poznata uloga broja *Social Security number*, jedinstveni broj socijalnog osiguranika i koji je u osnovi ekvivalent srpskom JMBG-u, jer je takođe jedinstven i ključan u postupku identifikacije lica. Javnost zapadnih država je najviše zabrinuta za zloupotrebu i krađu identiteta i postojanje centralizovanih baza podataka i razmene podataka o licima sa različitim vladinim službama, kao i evidentiranju mesta i vremena kada se neka identifikacija ili verifikacija desila. Problematika centralnih baza podataka u Velikoj Britaniji nije vezana samo za biometrijske projekte. Zbog činjenice da će milioni podataka o zdravstvenim korisnicima, van njihove volje, biti ubačeni u centralizovanu bazu kojoj će pristup imati oko 250 hiljada radnika britanskog nacionalnog zdravstvenog servisa, veliki broj organizacija, stručnjaka i službenika digao je glas protiv.[66] Zemlje članice EU nisu jedinstvene po pitanju upotrebe biometrijskih ličnih dokumenata i ne postoji opšteprihvaćen konsenzus po pitanju ovog problema. Većina pristalica biometrije kao glavni argument navodi potrebu za višim nivoom bezbednosti lica, no ipak je više protivnika ovog koncepta smatrajući ga pogubnim i štetnim

[64] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.
[65] Radna grupa, *„Osnovni koncepti novih elektronskih identifikacionih dokumenata“*, MUP, (2004).
[66] *United Kingdom Parlament, House of Commons Hansard Debates, November (2003).*

po privatnost građana i potencijalnim zloupotrebama u mnogim sferama svakodnevnog života.

Elektronski identifikacioni dokumenti su od strateškog značaja za budućnost upotrebe *smart* kartica u Evropi, jer se svakodnevno nalaze nova područja primene takvih dokumenata u svim sektorima društva. S tim u vezi, se može nedvosmisleno zaključiti da je Evropska Unija pobornik širokog korišćenja tehnologije *smart* kartica.

U decembru 1999. godine Evropska komisija, je pokrenula inicijativu za proširenje oblasti primene *smart* kartica među zemljama Evropske Unije, uz mogućnosti uključivanja i biometrijskih podataka radi poboljšanja postupka utvrđivanja i dokazivanja identiteta i unapređenja zaštite podataka u elektronskim transakcijama. Radno telo (*eEurope Smart Card Charter*) ima 12 radnih grupa koje su zadužene za sva polja primene *smart* kartica:[67]

1. javni identitet
2. identifikacija i autentifikacija
3. profili zaštite i sertifikati
4. čitači *smart* kartica
5. elektronska plaćanja
6. bezkontaktne *smart* kartice
7. višenamenske *smart* kartice
8. zahtevi korisnika
9. javni transport
10. servisi elektronske vlade
11. zdravstvene primene
12. elektronski potpis.

Bela knjiga (*White Paper*) je dokument nastao kao rezultat težnji i napora Evropske komisije, odnosno *eEurope Smart Card Charter*-a da, pored različite zakonodavne prakse mnogih zemalja **i** mnoštva međunarodnih standarda,

[67] *The e Europe SMART Card Charter, ELETRONIC IDENTITY WHITE PAPER, (2003).*

donese osnovne smernice za početak planiranja i uvođenja jedinstvene šeme elektronskog identifikacionog dokumenta, *eID*. Ciljna grupa ovog dokumenta su svi u lancu zahtevnog projekta, od vlada mnogih evropskih zemalja i njihovih zvaničnih institucija, predstavnika tehničko-tehnoloških organizacija i agencija, organa zaduženih za izdavanje ličnih dokumenata, pa do softverskih kompanija iz oblasti razvoja softvera i pružanja elektronskih usluga.

Navedeni dokument precizira obaveze koje bi svaka država trebala da ima u vidu prilikom implementacije elektronskih identifikacionih dokumenata baziranih na *smart* karticama i infrastrukturi javnih ključeva, *PKI*. Bela knjiga obuhvata sve aspekte izdavanja elektronskog identifikacionog dokumenta, počev od organizacije izdavanja (država, registracioni autoriteti, *RA* i sertifikacioni autoriteti, *CA*) i procedura koje su u nadležnosti registracionog i sertifikacionog autoriteta (registracija, izdavanje sertifikata, povlačenje sertifikata, produžavanje važnosti, ponovno izdavanje), do sadržaja sertifikata, ključeva, ugradnje drugih aplikacija i zaštite podataka.[68]

Shodno preporukama Evropske komisije, koje se odnose na primenu elektronskih identifikacionih dokumenata u Evropskoj Uniji, izrađene su identifikacione isprave, koje u sebi sadrže bezkontaktni čip sa svim osobinama putnih isprava. Ovo u praksi omogućava korišćenje *elektronske lične karte*, kao putne isprave u zemljama Evropske Unije, bez posedovanja pasoša kao posebnog dokumenta pri prelasku granica.[69]

Na osnovu toga, strategija primene elektronskog identifikacionog dokumenta u EU obuhvata procese standardizacije i harmonizacije primene *eID*-a širom njihove teritorije. Republika Srbija je jedna od država koja je prihvatila elektronsku identifikacionu ličnu karta i primena ovog dokumenta datira od 2008. godine.

---

[68] *A Smart Card Alliance White Paper "Secure Personal Identification Systems: Policy, process and Technology Choices for a Privacy-Sensitive Solution", February (2002).*
[69] *A.Smart Card Alliance, „Smart Card and Biometrics in Privacy –Sensitive Secure Personal Identification Systems", (2002).*

Elektronska lična karta sadrži biometrijske podatke koji se odnose na otisak prsta, dlana i digitalnu fotografiju.

U Nemačkoj se od 1. novembra 2005. godine, redovno izdaju nove, elektronske putne isprave. Time je Nemačka bila jedna od prvih zemalja članica EU koja je primenila preporuke EU. U to vreme u elektronskom pasošu, "*e-Pass-u*", na čipu su bili memorisani osnovni lični podaci (ime, prezime, mesto rođenja, državljanstvo) i biometrijski podaci, u prvom redu digitalna fotografija vlasnika pasoša, "*Basic Access Control*", sa propisanom veličinom lica od najmanje 32, a najviše 36 milimetara, bez ikakvog pokrivanja, kao i bez pozadine (*BAC*). Od marta 2007. godine, svi nemački pasoši imaju u čipu memorisane i otiske prstiju ("*Extended Access Control*", odnosno *EAC*).[70]

Stručnjaci u Nemačkoj tvrde da je "*e-Pass*" najbolja barijera u prevenciji falsifikovanja pasoša, kao i da je ovom merom smanjena mogućnost zloupotreba i krađe identiteta. Čip u "*e-Pass-u*" omogućava brze elektronske provere verodostojnosti dokumenta i njegove autentičnosti u odnosu na nosioca dokumenta.

Skup u Berlinu, pod pokroviteljstvom Evropske unije, na kojem su se okupili eksperti iz 38 država radi učestvovanja na raspravi o dostignućima novih e-pasoša, kao i njihovom testiranju, je pokazao da su Nemački elektronski pasoši položili test. Naglašen je i značaj dodatnog obezbeđenja podataka putem memorisanja podataka o otiscima prstiju (*EAC*). Glavna poruka skupa bila je, da bi za dalju sigurnost e-pasoša od velikog značaja bilo i uvođenje jedinstvenog standarda u svetu, kako za e-pasoše, tako i za uređaje, skenere koji sa njih očitavaju podatke.

Tehnička specifikacija svih evropskih putnih isprava je urađena na osnovu referenci *NTWG* (*New Technologies Working Group*), stručne radne grupe *ICAO*, to jest, Međunarodnih vlasti za civilni vazdušni saobraćaj (*International Civil Aviation Organization*). *ICAO* blisko sarađuje sa međunarodnim organizacijama za standardizaciju (*ISO*) i Komisijom EU. Ova tehnička

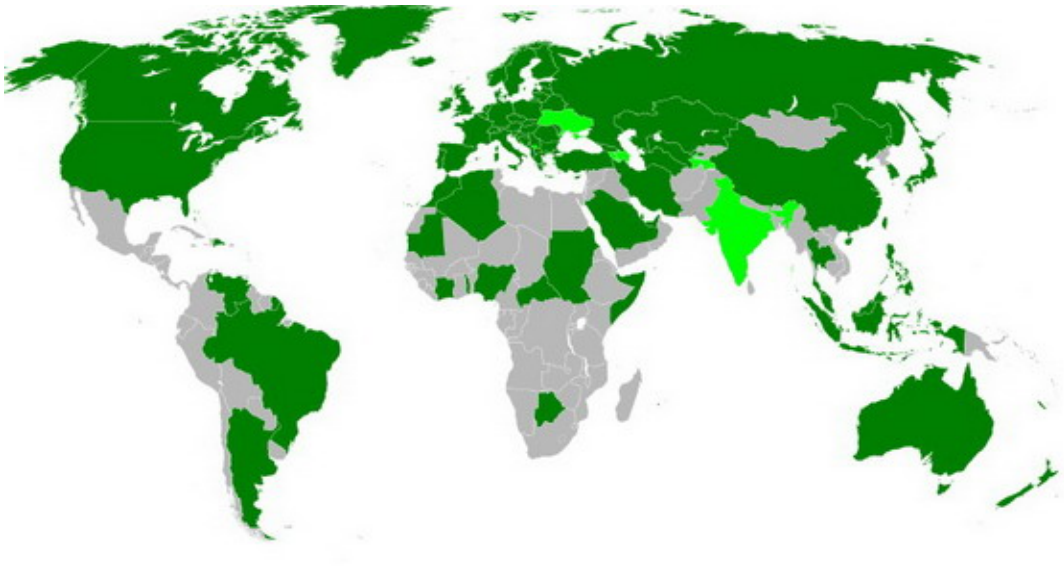
[70] Radna grupa, *„Projekat integrisanog rešenja obezbeđenja i kontrole prelaska državne granice“* (2003).

specifikacija predstavlja polaznu osnovu u procesu globalne standardizacije elektronskih dokumenata svih vrsta u celom svetu.

Glavni zagovornici uvođenja elektronskih pasoša bile su Sjedinjene Američke Države, i to nakon terorističkih napada u Njujorku od 11. septembra 2001. godine. Zagovornici daljeg tehničko-tehnološkog usavršavanja elektronskih putnih dokumenta, poručuju da će elektronski čipovi u pasošima uskoro imati, ne samo fotografiju i otiske prstiju nosioca isprave, već i mnoge druge fizičke podatke o vlasniku. To otvara vrata novim polemikama u javnosti o dodatnoj opasnosti od zloupotreba i kontrole, kao i o drastičnijem narušavanju privatnosti građana.

Sjedinjene Američke Države su 2002. godine izglasale kontroverzan zakon po kom su države koje su već imale bezvizni režim sa SAD-om bile u obavezi da počnu sa izdavanjem elektronskih pasoša najkasnije u roku od dve godine od izglasavanja istog zakona, ako žele da se takav bezvizni režim nastavi. U protivnom, SAD su bile spremne da svako odlaganje početka izdavanja e-pasoša sankcionišu uvođenjem viza građanima tih država. Ozbiljnost namera Sjedinjenih Američkih Država je bila potvrđena u praksi na primeru Italije, čiji su građani u jednom periodu morali da poseduju vizu za ulazak u SAD, jer Italija nije na vreme počela da izdaje nove e-pasoše.

Sjedinjene Američke Države, kao i pojedine evropske i azijske države su počele sa upotrebom biometrijskih pasoša 2005. godine. Trenutno, skoro sve evropske zemlje imaju u upotrebi nove, biometrijske pasoše. U svetu nove putne isprave trenutno koristi blizu sto zemalja, među kojima je i Republika Srbija. Na slici 1. tamno zelenom bojom su označene države u kojima se koriste elektronske putne isprave, dok su fluorescentnom zelenom bojom označene države u kojima će se biometrijske putne isprave primenjivati u budućnosti.



Slika 1 Karta zemalja koje koriste biometrijska dokumenta[71]

3.3.3. Elektronski identifikacioni dokumenti u Srbiji

Identifikacioni dokumenti se mogu klasifikovati na primarne identifikacione dokumente (lična karta) i sekundarne (pasoš, vozačka i saobraćajna dozvola, nekakva članska karta...). U specifičnim okolnostima se i sekundarni identifikacioni dokument može iskoristiti i kao primarni, kao što je slučaj sa upotrebom pasoša u inostranstvu, tako da navedena klasifikacija nije najpreciznija.

Elektronska identifikaciona dokumenta sadrže:

- vidljive (na površini same *smart* kartice) i nevidljive (memorisane u čipu *smart* kartice) alfanumeričke i biometrijske (digitalne i šifrovane) podatke nosioca *e-dokumenta*,
- asimetrične privatne ključeve (*Asymmetric Private Keys*, za digitalni potpis i digitalnu envelopu, *kovertu*) i dva digitalna sertifikata koji, naravno, odgovaraju tim ključevima, tj. njihovi su javni ekvivalenti,
- MRZ (*Machine Readable Zone*) mašinski čitljivu zonu.

Cilj koji se postiže ovim komponentama je neporeciva identifikacija vlasnika dokumenta i tačnosti podataka na ovom dokumentu. Dokumenta

[71] http://en.wikipedia.org/wiki/File:Map_of_countries_with_biometric_passports.svg, pristupljeno dana 14.03.2013. godine.

su rađena po ICAO 9303, ISO/IEC standardima, preporukama i direktivama EU, a u skladu sa domaćim i međunarodnim pravnim aktima.[72]

Suština svakog elektronskog identifikacionog dokumenta, *eID-a*, jeste pouzdana i tačna identifikacija nosioca dokumenta, pa je zato važno da svaki primerak takvog dokumenta po podacima bude jedinstven, što se postiže na dva načina:

- specijalnim tehnološkim procesima u proizvodnji blanko medijuma, takvim da je medijum praktično nemoguće kopirati, i
- unošenjem ličnih podataka za određenu osobu u takav blanko medijum.

O prednostima i neophodnosti novih biometrijskih e-dokumenata već je dosta rečeno, kao i o naprednim tehnologijama koje se koriste u tu svrhu. Jasno je da elektronski identifikacioni dokumenti zahtevaju posebne kontrolisane uslove za rad, pripremu i njihovu proizvodnju. Strogo se mora voditi računa o poštovanju predviđenih procedura koje obezbeđuju visokokvalitetan identifikacioni dokument sa potpuno tačnim unetim podacima od strane zaposlenih u autorizovanim ustanovama koje ih izdaju.

Kod izbora svake nove tehnologije u domenu identifikacionih dokumenata, uobičajeno se vode javne rasprave ne samo o mogućnostima, već i o bezbednosti i rizicima primene nove i u praksi nedovoljno proverene tehnologije. Tehnologija koja je primenjena kod čipova na ličnim dokumentima spada u najzaštićenije uređaje koji su ikada napravljeni i zadovoljava rigorozne svetske kriterijume (*CC EAL 5*+ standard - nekoliko elemenata kontrole pristupa čipu i kriptografske zaštite).

Da bi se osujetio svaki pokušaj krađe identiteta ili pojedinačnih podataka, kloniranja ili bilo koji drugi vid zloupotrebe *smart* kartica ma koje vrste, moralo se voditi računa o svakom detalju dizajna, tehnologije i tehnike proizvodnog procesa i stavljanja u upotrebu ovakvih dokumenata. Pored toga,

[72] Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP 2002-2004. godine.

neophodno je svaki element procesa proizvodnje držati pod kontrolom i u tajnosti, tako da se zadovolji osnovno pravilo da svako lice uključeno u proces proizvodnje ima pristup, i potrebno znanje, samo za one segmente procesa u koje je uključeno.

Dakle, da svako lice zna po nešto, a niko sve. Pojedini procesi u proizvodnji su potpuno automatizovani i ne zahtevaju prisustvo ljudi, tako da računar vrši dodelu serijskog broja novoizrađenoj kartici, a status i drugi podaci se automatizovano evidentiraju u posebnim bazama podataka sa najstrože kontrolisanim pravima pristupa i manipulacije.

3.3.3.1. Lična karta

Iz višegodišnjeg iskustva zemalja koje su bile pioniri na polju primene novih tehnologija i materijala za lična dokumenta, kao i ogromnog napretka u upotrebi novih, kompozitnih materijala, kao najbolji kandidat za podlogu *smart* kartice se pokazao polikarbonat. Polikarbonat je zadržao povoljne osobine različitih prirodnih materijala objedinjenih u jednom materijalu: čvrstoću i termičku stabilnost keramičkih kompozita, fleksibilnost i dugotrajnost plastičnih materijala, a što predstavlja osnovni preduslov za primenu polikarbonata u ličnim dokumentima, čime se obezbeđuje postojanost i dugotrajnost dokumenta.

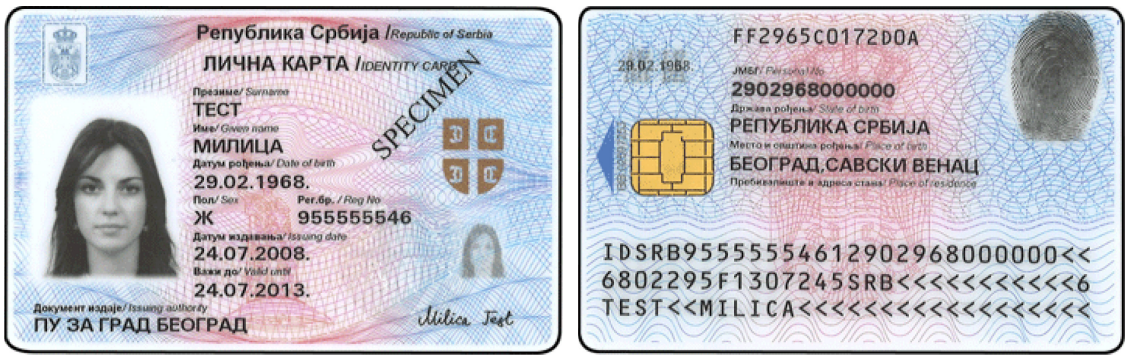
Moderna lična karta proizvedena primenom najsavremenijih tehnoloških procesa, sastavljena od preko dvadeset slojeva karbonata, pruža odlične mogućnosti za zaštitu od falsifikovanja i zloupotrebe. U slojeve se po potrebi ubacuje i čip što proizvodnju dodatno komplikuje. Kada je reč o verzijama dokumenta sa čipom, treba napomenuti da kod ovog dokumenta u Republici Srbiji nije predviđeno polje na kome se nalazi adresa prebivališta, tako da ustanove ili lica koja utvrđuju kompletne lične podatke nosioca dokumenta moraju posedovati i čitače kartica.

Konstantnim usavršavanjem metoda i načina za borbu protiv falsifikovanja i zloupotrebe ličnih dokumenata, iz godine u godinu se inovira i usavršava sve veći broj komponenti pasivne zaštite dokumenata.

Koordinacijom tehničkih, tehnoloških, naučnih, i naravno komercijalnih ustanova, države imaju više mogućnosti za adekvatan odabir i primenu najrazličitijih komponenti pasivne zaštite ličnih dokumenata.

Poleđina lične karte sadrži tzv. Mašinski čitljivu *MRZ* (engl. *Machine Readable Zone)* - mašinski čitljivu zonu, koja se skenira optičkom metodom prepoznavanja postavljenih alfanumeričkih znakova – *OCR* postupkom *(engl. Optical Character Recognition)*. OCR metoda predstavlja svojevrstan pomoćni, *backup* sistem, kada iz ma kog razloga nije moguće koristiti skener radi očitavanja podataka u memoriji čipa na biometrijskog dokumenta. Takođe, eliminiše se potreba za prekucavanjem teksta, što u nekim situacijama skraćuje vreme potrebno za utvrđivanje identiteta, npr. na graničnim prelazima.

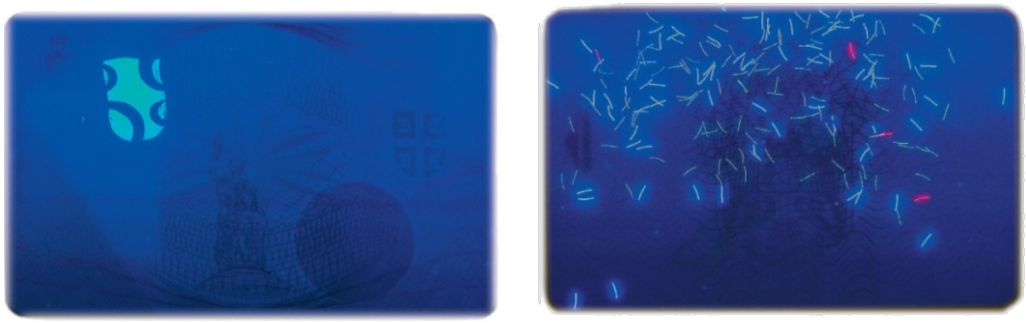
U Republici Srbiji, lične karte sa čipom su opcione, dakle nisu obavezne, a podaci o nosiocu lične karte sa čipom su nepromenjeni u odnosu na podatke koji su pre takvih dokumenata evidentirani, slika 2. Dakle, nema dodatnih vrsta podataka u novom sistemu.



Slika 2 Lična karta sa čipom

Nova lična karta je, u suštini, sastavljena od plastičnih kompozita i slična je platnim karticama, ali sa unapređenim merama zaštite od falsifikovanja i odsustvom magnetne trake koja je karakteristična za gotovo sve platne kartice. Činjenica da nova lična karta ima mnogo naprednih vidova zaštite je čini kvalitetnijom od sličnih kartica za druge namene.

Lične karte Republike Srbije sadrže desetak komponenti pasivne zaštite, od kojih su najznačajnije kinegram (posebna vrsta holograma), giljoš (niz sitnih krivih linija u širokom spektru boja koje zajedno daju kompleksnu sliku u pozadini, odštampanu u visokoj rezoluciji), *MLI - engl. Multi Laser Image* (višestruka laserska slika), *Ghost Image* (umanjena originalna slika nosioca, štampana u crno-beloj tehnici), itd. Na slici 3 je dat izgled lične karte pod ultravioletnom svetlošću, a na slici 4 su prikazani zaštitni elementi lične karte.



Slika 3 Lična karta pod UV svetlošću

Na biometrijskoj kartici je postavljen integrisan memorijski čip brenda *Infineon,* kapaciteta 32 kB (kilobajta). Očitavanje podataka uskladištenih u čipu se vrši kontaktnim prevlačenjem kroz čitač „pametnih" – *smart* kartica. U MUP-u Republike Srbije se u čip pohranjuju odgovarajući podaci, upisuju se lični podaci nosioca dokumenta (ime, prezime, JMBG, adresa i slično), a mogu se vršiti i naknadne izmene sadržaja na memorijskom čipu, recimo kod promene prebivališta lica kome se lični dokument izdaje. Za karticu kažemo da je biometrijska, i to multimodalna, jer po svojoj sadržini objedinjuje više jedinstvenih fizioloških i anatomskih karakteristika isključivo jedne osobe: digitalnu fotografiju lica osobe u JPEG formatu (engl. *Joint Photographers Expert Group*), snimljene u MUP-u, otiske prstiju (zapisane u standardnom formatu za tu namenu, koji sadrži izgled otiska, ali i „analiziran" i kompresovan izgled otiska). Na čip se ubacuje i slika potpisa nosioca dokumenta.

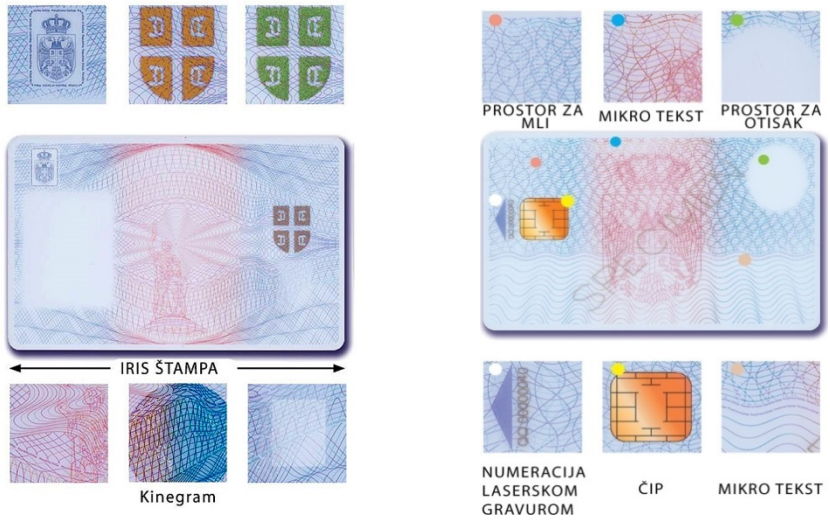
Na novoj ličnoj karti, u njenom memorijskom čipu, nalazi se i tzv. elektronski potpis nosioca lične karte. Svaki građanin se može odlučiti i za

izdavanje lične karte bez integrisanog čipa, ako tako želi. Na takvoj varijanti lične karte postoje određene razlike u odnosu na ličnu kartu sa čipom, kako bi se nadomestilo odsustvo čipa jednostavno se vrši doštampavanje nedostajućih podataka na površinu kartice.

Privatnost podataka koji se nalaze u memorijskom čipu je zagarantovana, jer se očitavanje i prenos podataka vrši isključivo u trenucima kada se uspostavi fizički kontakt između površine čipa i čitača-skenera, što predstavlja ekvivalent situacije, kod dokumenata starije generacije, kada se lična karta fizički preda licu koje ima pravo da čita sadržane podatke.

Dakle, samo zato što je neko u neposrednoj blizini lica koje poseduje biometrijsku ličnu kartu, ne znači da može bezkontaktnim putem očitati i zloupotrebiti podatke memorisane u čipu. Suština postojanja čipa je olakšavanje, pojednostavljenost i ubrzavanje procedure utvrđivanja identiteta nosioca lične isprave. To i za građane znači uštedu vremena jer očitavanje podatka traje kraće nego njihovo prepisivanje.

Upotreba novih tehnologija često prate i razne negativne priče u javnosti. Na primer, da lične karte sa čipom sadrže i neke dodatne podatke o nosiocu, a koje navodno ne postoje kod konvencionalnih ličnih karata, ali takve tvrdnje u javnosti nemaju nikakav osnov. Takođe, priče o potencijalnim zloupotrebama ličnih karata sa čipom, koje su se mogle čuti u elektronskim medijima, a naročito na nekim Internet forumima, su potpuno neosnovane i proističu pre svega iz neznanja i neupućenosti pojedinaca u načine primene savremenih informacionih tehnologija na polju čuvanja i obrade podataka. I pored medijskog komešanja koje je pratilo proces izdavanja novih ličnih karata, tek nešto više od 9% građana se opredelilo za lične karte bez integrisanog memorijskog čipa.



Slika 4 Zaštitni elementi na ličnoj karti

3.3.3.2. Pasoš

Kao i kod izdavanja novih ličnih karata, tako je i pojava novog biometrijskog pasoša sa integrisanim čipom, u formi elektronskog identifikacionog dokumenta, izazvala medijsku pažnju i različite komentare građana. Zagovornici tradicionalnih shvatanja i ljudi koji teže prihvataju promene koje moderno doba ubrzano nameće, stvorili su određenu dozu nepoverenja u nove pasoše, odnosno izrazili sumnju u bezbednost elektronskog identiteta, moguće narušavanje privatnosti i zloupotrebe takvog dokumenta. Akcenat na moguće kompromitovanje bezbednosti novih pasoša stavljen je na mogućnost reprogramiranja sadržaja memorije u čipu biometrijskog pasoša. Međutim, zanemaruje se činjenica da pored ugrađenih mera elektronske zaštite, svaki pasoš i dalje je osiguran konvencionalnim sistemima zaštite, kao što je to učinjeno na starim pasošima Republike Srbije (specijalni papir, serijski broj zumban na svim stranama putne isprave, stranice pokrivene slikama sastavljenim od kompleksnih spletova linija, i slično). Tehnološki napredak je omogućio još savremenije vidove zaštite, jer je i srpski pasoš jedan od "primamljivih" falsifikatorima i kriminalacima. Novi biometrijski pasoš Republike Srbije, prikazan na slici 5, je osmišljen, dizajniran i projektovan u skladu sa najvišim evropskim standardima pri izradi pasoša i karakteriše ga

prisustvo *Philips*-ovog integrisanog mikroprocesora, *čipa*, kapaciteta 82kB sa *RFID* karakteristikama (engl. *Radio Frequency Identification*). Kao što se iz *RFID* naziva može zaključiti, očitavanje podataka se vrši bezkontaktno, iz neposredne blizine, putem radio veze. Naglasak je na veoma kratkom rastojanju između *smart* kartice i uređaja koji vrši očitavanje, jer čip nema svoj izvor napajanja. Mora se naglasiti da je podatke sa čipa u pasošu nemoguće očitati bez našeg znanja, jer je bezkontaktno očitavanje moguće tek nakon što pasoš predate na očitavanje „*mašinski čitljive zone*". Dakle, biometrijski pasoš mora biti otvoren da bi skener dekodirao tekstualne informacije odštampane na stranici pasoša koje služe kao svojevrstan šifarnik za pristup informacijama u čipu.

Slika 5 Biometrijski pasoš Republike Srbije

Biometrijski pasoš Republike Srbije je funkcionalno i estetski savršeniji od svog prethodnika. Postignut je daleko viši nivo zaštite upotrebom najsavremenijih tehnika štampe i primene zaštitnih elemenata. Neki od zaštitnih elemenata su: lični podaci se upisuju laserom, višestruka laserska slika (*MLI*), hologram pozicioniran i preko crno-bele fotografije, mikro-tekst (koji takođe prelazi preko fotografije nosioca), giljoš linije površine koje se „osećaju" pod dodirom ruke, segmenti koji refleksijom menjaju boje iz spektra, segmente vidljive samo pod određenim uglom, polja osetljiva na *UV* (ultraljubičasti) i *IR* (infracrveni) spektar svetlosti, i mnogi drugi. Pojedini elementi zaštite nove putne isprave prikazani su na slici 6.

Slika 6 Unutrašnje stranice srpskog pasoša i stranica pod UV svetlom

Slika 7 Građa biometrijskih pasoša sa ugrađenim čipom

Važna osobina srpskih biometrijskih pasoša je postojanje dvoredne alfanumeričke zone koja služi za brzo očitavanje podataka koje je od neprocenjive koristi putnicima koji prolaze carinu i policijsku kontrolu. To znači bitno skraćivanje procedure i čekanja u redu.

Biometrijski pasoš Republike Srbije spada u red jednog od tehnološki najsavremenijeg dokumenta te vrste u Evropi i svetu uopšte, sa čak sedam

vidova zaštite. Osnovna stranica, izrađena od polikarbonata sadrži kinegram, optički varijabilne boje, a u procesu laminacije unose se mat i sjajni elementi. Ostale stranice, namenjene unosu raznih carinskih pečata, potvrda i viza sadrže grb Srbije, vodeni žig, zaštitne niti i druge skrivene elemente, koji pasoš štite od falsifikovanja. Na osmišljavanju i dizajniranju novog pasoša je, između ostalih, radila zajednička komisija MUP-a Republike Srbije i Zavod za izradu novčanica. Integrisano mikrokolo, čip, u novom srpskom pasošu nije opcija, kao kod ličnih karata, već je prisustvo čipa obavezno. Građa novog biometrijskog pasoša sa ugrađenim čipom prikazana je na slici 7.

Naš biometrijski pasoš je druga generacija pasoša koja u sebi sadrži *EAC* (*Extended Access Control*), što znači da se u čipu pored imena, prezimena, adrese i JMBG, nalazi i otisak prsta levog i desnog kažiprsta, kao i 2048-bitni ključ za otključavanje tog biometrijskog podatka. Taj ključ se, prilikom prelaska granica, razmenjuje sa drugim graničnim policijama u svetu, a nosilac putne isprave potvrđuje svoj identitet upoređivanjem svog otiska prsta sa skeniranim otiskom.[73]

Bezbednost podataka smeštenih u memorijskom čipu srpskog biometrijskog pasoša je na visokom nivou, jer se koriste tehnologije i metode zaštite proverene i potvrđene od strane vodećih zemalja i njihovih tehničkih institucija. Ne zalazeći predaleko u tehničke-tehnološke detalje, posebno iz domena kriptografije, ipak treba napomenuti da se u integrisanom mikroelektronskom kolu, čipu, nalazi i minijaturni radiopredajnik putem kojeg se vrši razmena podataka sa čitačem. Mogućnost zloupotrebe je minimizirana jer se za neovlašćeno čitanje podataka iz čipa mora zadovoljiti više potrebnih uslova, koje susrećemo, na primer, prilikom prelaska granice, a to podrazumeva: da se poseduje uređaj koji može očitati mašinski čitljivu zonu na stranici pasoša sa čipom; da se manipulacijom pročitanih podataka izračuna šifra za pristup podacima na čipu; da se šifra potom prosledi čipu radi

[73] Radna grupa, *„Projekat integrisanog rešenja obezbeđenja i kontrole prelaska državne granice“*, (2003).

postupka autentifikacije i da se potom izvrši dešifrovanje podataka postavljenih u memoriju čipa.

Otisak prsta je najsigurnije zaštićen, jer se taj podatak dobija isključivo nakon uspešnog poklapanja podataka iz mašinski čitljive zone pasoša i segmenta gde su podaci o otisku prsta zaštićeni 2048-bitnim ključem. Inače, analize su pokazale da je 2048-bitni asimetrični *RSA* ključ po procesorskom vremenu potrebnom za otkrivanje šifrovanog teksta približno ekvivalentan 112-bitnom simetričnom ključu! Skup podataka pohranjenih na pasošu nije moguće neprimetno izmeniti, jer ih je digitalno potpisalo odgovarajuće državno telo. Kao što je već naglašeno, kriptografija je matematički orijentisana, zahtevna naučna disciplina, pa ćemo se u ovom radu izlaganje ograničiti na tvrdnju da srpski biometrijski pasoš poseduje jaku enkripcijsku zaštitu. Argument za navedenu tvrdnju je i preporuka Američkog nacionalnog instituta za standarde i tehnologiju, *NIST*, da se postepeno do 2015. godine povuku iz upotrebe 80-bitni simetrični ključevi, jer će se nakon toga smatrati nebezbednim.

Čip sadrži i sve tekstualne podatke koji su odštampani na glavnoj strani pasoša (ime, prezime, adresa, broj, JMBG, rok važenja i drugo), uključujući i fotografiju nosioca. Ovi podaci su smešteni u tzv. *data* grupe, a ostavljen je prostor i za buduće definicije onoga šta će one čuvati. Dakle, ostavljeno je prostora za eventualno dodavanje podataka u budućnosti, ako tako nešto bude potrebno. To je vrlo korisno ako se, hipotetički, izmeni *Zakon o putnim ispravama* ili neke njegove odredbe, pa se ovakvom osobinom biometrijskog pasoša mogu bitno smanjiti troškovi zamene.

Identifikacija putem radio frekvencije, *RFID* je tehnologija koja datira iz osamdesetih godina prošlog veka, tako da osim u pasošu, *RFID* tehnologija je primenjena u mnogim drugim oblastima, kao što su kontrola pristupa i autorizacija. Dakle, da bi se sadržaj *smart* kartice mogao očitati, potrebno je raspolagati sa *RFID-čitačem*. Tek pošto očita karticu čitač utvrđuje da li je očitana kartica *njegova*. Ako jeste, on nastavlja da obrađuje podatke, a ako nije čitač zanemaruje dalji rad sa karticom. Čitač i prilikom zlonamernog pokušaja

očitavanja podataka iz njemu nepoznate kartice ne može da kompletira akciju, jer su podaci u kartici šifrovani.

Nakon ove analize, možemo zaključiti da je srpski biometrijski pasoš, kao i većina *digitalnih* pasoša drugih zemalja, adekvatno obezbeđen od moguće zloupotrebe i falsifikovanja i da mali broj ljudi, koji moraju raspolagati specifičnim visokotehnološkim znanjima, veštinama i opremom, može zloupotrebiti podatke iz takvog pasoša. Polazeći od najgoreg scenarija, zloupotreba jednog od milion biometrijskih pasoša, svakako je minorna stvar u odnosu na činjenicu da je ranije milione pasoša u staroj i prevaziđenoj tehnologiji bilo daleko jednostavnije zloupotrebiti. Ako svemu ovome dodamo i uštede u vremenu i novcu, pojednostavljenoj proceduri pri putovanjima, kvalitetu i trajnosti novog pasoša, kao i mnoge druge prednosti, možemo zaključiti da je biometrijski pasoš, u odnosu na ranije verzije, daleko superiorniji u većini slučajeva, posebno onih koji se tiču problema bezbednosti i zaštite od zloupotreba putne isprave.

3.3.3.3. Saobraćajna i vozačka dozvola

Saobraćajna dozvola za vozila registrovana u Republici Srbiji je osmišljena i dizajnirana prema primeru lične karte. Izrađena je od kvalitetnog polikarbonata, multilaminarna, odnosno sastavljena je iz više slojeva i sa istom vrstom zaštitnih elemenata kao i lična karta. Saobraćajna dozvola, takođe, obavezno sadrži i integrisano mikrokolo, čip odakle se podaci kontaktno očitavaju pomoću skenera, čitača kartica. U čipu se nalaze svi vidljivi podaci, odnosno podaci odštampani na samoj ispravi, kao i podaci koji nisu štampani, a to su: godina proizvodnje, vrsta vozila, broj motora, broj osovina, boja vozila, eventualni period zabrane otuđenja vozila, JMBG vlasnika, odnosno korisnika i nosivost vozila. Na slici 8 prikazane su obe strane saobraćajne dozvole sa čipom.

Slika 8 Saobraćajna dozvola sa čipom

Postojeće i potencijalne prednosti nove saobraćajne dozvole nije teško uočiti. Saobraćajna dozvola sa čipom skraćuje i pojednostavljuje proceduru prilikom registracije i tehničkog pregleda ili pri rutinskim kontrolama ovlašćenih lica; izdržljiva je, kompaktna i kvalitetna. Omogućava i funkcionalno proširenje ovog dokumenta, na primer, eventualno plaćanje parkinga ili putarine. Treba pomenuti da su u Srbiji u upotrebi i nove, potpuno drugačije vozačke dozvole u odnosu na stare. Iako je prvobitno bilo predviđeno da vozačke dozvole sadrže i čip, Pravilnikom je predviđeno da budu bez čipa, u obliku su kartice formata *ID1*, i sadrže niz podataka koji su u skladu sa direktivom EU. Izgled vozačke dozvole je prikazan na slici 9.

Slika 9 Izgled vozačke dozvole

Vozačke dozvole imaju iste vrste zaštitnih elemenata kao i nove lične karte. Prioritet i obaveza svake države, njene vlade i njenih drugih organa jesu nacionalna bezbednost i bezbednost svih građana. Važan preduslov za takve zadatke su upravo efikasno i pouzdano utvrđivanje identiteta, evidentiranje

stanovništva i efikasno upravljanje tako prikupljenim podacima, a sve uz visok stepen zaštite privatnosti i sprečavanja zloupotrebe podataka.

Razvoj i implementacija novih tehnologija u utvrđivanju i proveri identiteta lica, pre svega primena tehnologija *smart* kartica i biometrije, pružila je značajnu podršku realizaciji pouzdanih i bezbednih elektronskih servisa. Građani danas imaju privilegiju da brzo, jednostavno i bezbedno koriste prednosti koje im nude nova naučna i tehnološka dostignuća primenjena na mnogim poljima u svakodnevnom životu, kao što su Internet servisi organa državne uprave, bankarske transakcije, kupovina proizvoda ili elektronske usluge preko Interneta, prelasci granica,... Preduzeća su u prilici da omoguće svojim radnicima obavljanje poslova sa udaljenih mesta, sigurni da samo oni ti koji mogu pristupiti određenim poverljivim poslovnim podacima.

4. MENADŽMENT IDENTITETA I ZAŠTITA SVEDOKA

4.1. Potreba za zaštitom svedoka u krivičnom postupku

Nedvosmisleno je da su terorizam i organizovani kriminal prepoznati kao najveći izazovi savremenog doba, odnosno najozbiljniji rizici po bezbednost svake zemlje, s obzirom da podrivaju samu srž demokratije i osnovne civilizacijske vrednosti i nanose ogromnu štetu društvu i državi.[74]

Dodatnu ozbiljnost ovim oblicima kriminala, naročito u pogledu otkrivanja organizatora i nalogodavaca, daje najčešće transnacionalni karakter organizovanog kriminala i terorizma, koji ne poznaju geografske granice i nacionalne razlike, te i zahtevaju zajednički i organizovani pristup zemalja u regionu i svetu na njihovom efikasnom suprotstavljanju, jer u suprotnom lako izbegavaju odgovornost na teritoriji država u kojima deluju.

Sudska praksa je potvrdila, i to ne samo evropskih sudova, već i američkih, da su sudski postupci za organizovani kriminal, najefikasniji ako postoje svedoci iz te kriminalne organizacije, jer oni mogu da pomognu utvrđivanju funkcionisanja takve organizacije, ulogu članova, načina organizovanja i finansiranja i obezbeđenju neophodnih dokaza za vođenje krivičnog postupka.[75]

Zbog toga je neophodno uspostaviti odgovarajući mehanizam, koji će sadržati posebne mere za efikasnu zaštitu učesnika u krivičnom postupku i njima bliskih lica, koji će biti znatno efikasniji od dosadašnjih.

Na to su članice Ujedinjenih nacija obavezane i međunarodnim ratifikovanim dokumentima, a pre svega imajući u vidu odredbe Konvencije UN protiv transnacionalnog organizovanog kriminala i Rimskog statuta

[74]Douglas A. Kash, *Witness Protection Program is critical weapon in the war of crime*, The FBI Law Enforcement Bulletin, No.5, Vol 74, USA May (2004).
[75] US Marshal Service, *available on,* http://www.usmarshals.gov/witsec/index.html, pristupljeno 13.04.2012.

Međunarodnog krivičnog suda.[76] Nakon ratifikovanja navedenih dokumenata većina zemalja je donela odgovarajuću pravnu regulativu kojom su stvorene pravne pretpostavke za efikasnu realizaciju i primenu sistema zaštite svedoka.

U slučaju Republike Srbije, nakon donošenja Zakona o programu zaštite učesnika u krivičnom postupku u okviru Ministarstva unutrašnjih poslova R. Srbije formirana je specijalizovana Jedinica, koja na nacionalnom nivou sprovodi Program zaštite.

4.2. Program zaštite učesnika u krivičnom postupku i zakonska regulativa

Sa aspekta kriminalističke teorije i prakse, uvođenje Programa zaštite svedoka ima značajniji uticaj u suprotstavljanju organizovanom i transnacionalnom organizovanom kriminalu, naročito u domenu blagovremenog obezbeđenja dokaza. Međutim, ova oblast i način rada su sakriveni od javnosti, imajući u vidu specifičnu prirodu posla u ovoj oblasti, diskreciju i striktno poštovanje profesionalnih standarda koji su apsolutno najbitniji.

Poznato da se građani retko pojavljuju kao svedoci u postupku, upravo iz straha za svoju bezbednost i bezbednost članova svoje porodice, iako su mnogi od njih bili očevici kriminalnih delatnosti organizovanih kriminalnih grupa. Primena mera zaštite u okviru Programa zaštite svedoka, izaziva veće interesovanje građana da svedoče, budući da im je garantovana zaštita i lična bezbednost. [77]

Na međunarodnom nivou, pitanje zaštite svedoka regulisano je ugovorima i vanugovornim aktima na multilateralnom i bilateralnom nivou. U najvažnije akte Međunarodnog prava kojima se reguliše ova problematika spadaju:

[76] G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).

[77] US Marshal Service, *available on,* http://www.usmarshals.gov/duties/factsheets/witsec-2011.html, pristupljeno 13.04.2012.

- Konvencija UN protiv transnacionalnog organizovanog kriminala (*UNCATOC*), sa dopunskim protokolima , koja je stupila na snagu 29. 09.2003. godine [78],
- Statut međunarodnog krivičnog suda (ICC) koji je stupio na snagu 1. jula 2002. godine [79] i
- Statut međunarodnog krivičnog tribunala za bivšu Jugoslaviju (ICTY) koji je uspostavljen na osnovu rezolucije saveta bezbednosti UN br. 827 od 25. maja 1993. godine.[80]

Na evropskom nivou doneta je Evropska konvencija o međusobnoj pomoći u krivičnim stvarima[81] i Preporuka Saveta Evrope o zastrašivanju svedoka i pravo na odbranu.[82]

Takođe, Savet Evrope je doneo i sledeće odluke:

- Preporuka o nasilju u porodici;[83]
- Preporuka o zaštiti i pružanju pomoći žrtvama; [84]
- Preporuka u vezi seksualnog iskorišćavanja i izlaganja dece i omladine pornografiji, prostituciji i krijumčarenju; [85] i
- Preporuka o kaznenoj politici u Evropi za vreme promena[86] i
- Preporuka Rec. (2005) 9 o zaštiti svedoka i svedoka saradnika.[87]

Na regionalnom nivou postoje više regionalnih sporazuma kojima se reguliše saradnja na zaštiti svedoka i žrtava. Tako na primer postoji Baltički sporazum koji su potpisale Estonija, Litvanija i Letonija, kao i Balkanski

[78]Konvencija UN protiv transnacionalnog organizovanog kriminala (UNCATOC), sa dopunskim protokolima , koja je stupila na snagu 29. 09.2003. godine.

[79]Statut međunarodnog krivičnog suda (ICC) koji je stupio na snagu 1. jula 2002. godine.

[80]Međunarodni krivični sud za bivšu Jugoslaviju (ICTY) koji je uspostavljen na osnovu rezolucije saveta bezbednosti UN br. 827 od 25. maja 1993. godine.

[81]Krivičnopravna Konvencija o korupciji, od 27.01. 1999. godine.

[82]Preporuka sa oznakom N° R (97) 13 o zastrašivanju svedoka i prava odbrane, doneta na 600. zasedanju zamenika ministara 10. juna 1997. godine.

[83]Preporuka o nasilju u porodici, N° R(84) 4.

[84]Preporuka o zaštiti i pružanju pomoći žrtvama, N° R (87) 21.

[85]Preporuka u vezi seksualnog iskorišćavanja i izlaganja dece i omladine pornografiji, prostituciji i krijumčarenju, N° R (91) 11.

[86]Preporuka o kaznenoj politici u Evropi za vreme promena, N° R (96) 8.

[87] Preporuka Rec. (2005) 9 o zaštiti svedoka i svedoka saradnika, usvojena od strane Komiteta ministara 20 aprila 2005.godine.

sporazum, koji su potpisali Crna Gora, Makedonija, BiH, Bugarska i Srbija. Na nivou Istočne Evrope i Zapadnog Balkana su usvojene nove ili se usavršavaju postojeće postupke zaštite svedoka i uzajamne saradnje.

U Jugoistočnoj Evropi posebni značaj na ovom planu ima Savetodavna grupa tužilaca jugoistočne Evrope (*SEEPAG*) u okviru koje je Srbija koordinator radne grupe za zaštitu svedoka. Ova Grupa se u svojim aktivnostima oslanja na resurse Pakta za stabilnost zemalja Jugoistočne Evrope i *SECI* Centra za borbu protiv međunarodnog kriminala sa sedištem u Bukureštu. Inače, *SEEPAG*, čije su osnivanje 12. decembra 2003. godine inicirale Srbija i Crna Gora, čine predstavnici Srbije i Crne Gore, Albanije, BiH, Bugarske, Hrvatske, Makedonije, Grčke, Mađarske, Moldavije, Rumunije, Slovenije i Turske.

Treba napomenuti da u pojedinim državama, kao što je Kolumbija, postoji nekoliko nivoa u zaštiti svedoka, ali najozbiljniji je pod nadležnošću Kancelarije opšteg tužioca, sa svedocima koji su relocirani na teritoriji Kolumbije. U Brazilu je slučaj da se prilikom sprovođenja Programa zaštite uključuju i nevladine organizacije (*NGO*), imajući u vidu da postoji policijska korupcija i nedostatak poverenja u institucije.

U zemljama latinske Amerike (Gvatemala, El Salvador) u Program zaštite se uključuje veliki broj svedoka žrtava i svedoka iz domaćih slučajeva zlostavljanja.[88]

Evropski pristup zaštiti svedoka se razlikuje od pristupa koji se primenjuje u Sjedinjenim Američkim Državama i Južnoj Americi, jer je mnogo širi i često uključuje podršku (ekonomsku, socijalnu, zdravstvenu, psihološku...) svedocima, a ne samo mere zaštite.[89]

Zakonska regulativa koja se odnosi na zaštitu svedoka je različita i zavisi od zemlje do zemlje. Neke zemlje imaju vrlo detaljno iskazano zakonodavstvo za zaštitu svedoka (Slovačka, Srbija, Australija, Kanada), dok druge koriste

[88] *Principles of protection Tool 5.17 Witness protection, available on* http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_5-17.pdf.

[89] Yvon Dandurand, Kristin Farr, *A Review of Selected Witness Protection Programs*, Her Majesty the Queen in Right of Canada, Report No. 001, Canada, (2010).

opšte odredbe krivičnog zakonika i Zakona o krivičnom postupku (Engleska, Severna Irska, Francuska).

Takođe, ima slučajeva da neke zemlje tek sada usvajaju zakon o Programu zaštite, ali retko imaju lica koja bi se pojavila u ulozi svedoka (Finska, Norveška). Međutim, ima slučajeva da neke zemlje imaju svedoke, pa nemaju drugi izbor nego da štite svedoke, uprkos nedostatku zakonodavstva i drugih pravnih akata (Gvatemala, Španija).[90]

U većini istočnoevropskih zemalja zakoni o zaštiti svedoka na nacionalnom nivou su slični i vode poreklo iz Slovačkog zakonodavstva.[91] Zakon uglavnom uključuje nezavisno telo (odbor, komisiju), koja donosi odluku o pristupanju u Program zaštite, dok je Policijska jedinica odgovorna za primenu mera zaštite i procenu rizika pretnji.

Što se tiče srpskog zakonodavstva, Zakon o zaštiti učesnika u krivičnom postupku je stupio na snagu 01.01.2006. godine i uređuje uslove i postupak za pružanje zaštite i pomoći učesniku u krivičnom postupku i njima bliskim licima.[92] Zaštita po ovom Zakonu primenjuje se samo na ona lica čija je lična bezbednost ili bezbednost njihovih porodica izložena opasnosti zbog davanja iskaza u pretkrivičnom i krivičnom postupku, a obezbeđuje se primenom različitih mera predviđenih ovim zakonom.[93]

Saglasno odredbama ovog Zakona, posebne mere zaštite se primenjuju samo za ona lica čija je lična bezbednost ili bezbednost njihovih porodica izložena opasnosti zbog davanja iskaza u pretkrivičnom i krivičnom postupku.

Ovakva zaštita se može primeniti praktično na sva lica koja su učesnici u krivičnom postupku i koja su izložena realnoj opasnosti usled davanja iskaza ili pružanja značajnih informacija. Konkretnije, zaštita svedoka se primenjuje,

---

[90]United Nations Office on Drugs and Crime, /Vienna/, *Good practices for the protection of witnesses in criminal proceedings involving organized crime,* N.York, (2008).

[91]*Ibid*

[92]Zakon o programu zaštite učesnika u krivičnom postupku, (Službeni glasnik R. Srbije br. 85/2005).

[93]G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).

kako na svedoka, oštećenog i svedoka saradnika, tako i na osumnjičenog, odnosno okrivljenog, veštaka i stručno lice, a može se primeniti i na lica bliska pomenutim procesnim subjektima. Blisko lice je, svakako, član uže porodice (supružnik, dete, roditelj, brat, sestra), odnosno drugo lice koje zaštićeni svedok takvim označi, pod uslovom da je u konkretnom slučaju moguće da se njegovim ugrožavanjem izvrši ozbiljan pritisak na zaštićenog svedoka.[94] Podrazumeva se da će svedok, odnosno drugi odgovarajući procesni subjekat ili njemu blisko lice, uživati zaštitu samo pod uslovom da je usled davanja važnog iskaza, odnosno pružanja značajnih informacija, izloženo opasnosti po život, zdravlje, fizički integritet ili imovinu.[95]

Program zaštite svedoka treba razlikovati od programa pomoći žrtvama krivičnog dela, što znači da se oštećeni koji nisu značajni kao svedoci ne mogu uključiti u Program zaštite svedoka. Prema ovakvim licima primenjuju se proceduralne mere zaštite, koje određuje postupajuće sudsko veće, a obuhvataju svedočenje pod pseudonimom, svedočenje putem video linka, skremblovanje slike i distorzija glasa.

Sa druge strane, status zaštićenog lica po programu može dobiti isključivo ako je reč o iskazu, odnosno pružanju informacije, bez koje bi bilo onemogućeno ili znatno otežano dokazivanje u postupcima za krivična dela protiv ustavnog uređenja i bezbednosti, za dela protiv čovečnosti i međunarodnog prava i za dela sa elementima organizovanog kriminala.[96]

Zaštita se može primeniti prema zaštićenom licu pre, u toku i nakon pravosnažnog okončanja krivičnog postupka, a svi organi i lica koja u njemu učestvuju moraju postupati sa naročitom hitnošću. Podaci u vezi sa Programom zaštite predstavljaju službenu tajnu i ne sme ih otkrivati niko kome postanu dostupni.[97]

---

[94] *Ibid.*
[95] *Ibid.*
[96] Zakon o programu zaštite učesnika u krivičnom postupku, (Službeni glasnik R. Srbije br. 85/2005).
[97] *Ibid.*

4.3. Mere zaštite učesnika u krivičnom postupku

Prilikom određivanja mera zaštite mora biti osigurana srazmernost između prirode mera zaštite koje bi trebalo usvojiti i ozbiljnosti zastrašivanja kojem je svedok izložen. One moraju biti primenjene na svedoke i žrtve koji imaju potrebu za zaštitom duže od trajanja postupka u kojem moraju da svedoče. Mere se određuju zbog postojanja rizika po bezbednost navedenih lica ili članove njihove porodice.[98]

Mere zaštite koje se obezbeđuju Programom zaštite se razlikuju od države do države. Većina država nudi slične mere zaštite koje zavise od specifičnosti slučaja i utvrđene procene rizika.

Programi zaštite obuhvataju fizičku zaštitu, promenu identiteta, preseljenje, finansijsku podršku, kao i razne druge oblike podrške (psihološka, pravna, zdravstvena, ...). Neki programi zaštite imaju mogućnost da ponude novac (Italija) u zamenu za fizičku zaštitu, tako da zaštićeno lice mora koristiti sopstvene mere predostrožnosti.

U Srbiji na osnovu člana 14. Zakona o programu zaštite učesnika u krivičnom postupku primenjuju se sledeće mere: fizička zaštita ličnosti i imovine, promena prebivališta ili premeštanje u drugu zavodsku ustanovu, prikrivanje identiteta i podataka o vlasništvu, kao i promena identiteta.

Mera fizičke zaštite ličnosti i imovine sastoji se od sprečavanja protivpravnog ugrožavanja života, zdravlja, fizičkog integriteta, slobode ili imovine zaštićenog lica upotrebom fizičko-tehničkih mera.[99]

Mera promene prebivališta sastoji se od privremenog ili trajnog preseljenja zaštićenog lica iz mesta prebivališta ili boravišta u mesto koje odredi Jedinica za zaštitu. Mera premeštaja u drugu Zavodsku ustanovu sastoji se od upućivanja zaštićenog lica koje je lišeno slobode iz Zavodske ustanove u kojoj

[98] G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).
[99] *Ibid.*

se nalazi u Zavodsku ustanovu koju odredi Jedinica za zaštitu u dogovoru sa Ministarstvom pravde.[100]

Takođe je predviđeno da u toku sprovođenja Programa zaštite može primenjivati jedna ili više mera, što zavisi od bezbednosne procene i konkretne situacije. Poslednja u nizu mera zaštite, mera promene identiteta se primenjuje uz odobrenje Komisije, kao krajnja mera, kada se cilj Programa zaštite ne može ostvariti primenom drugih mera.

U daljem tekstu će biti više reči o merama prikrivanja identiteta i podataka o vlasništvu, meri promene identiteta, kao i polju primene biometrijskih metoda identifikacije u ovoj oblasti.

4.4. Specifičnosti menadžmenta identiteta u sistemima zaštite svedoka

4.4.1. Prikrivanje identiteta i podataka o vlasništvu

Mera prikrivanja identiteta i podataka o vlasništvu podrazumeva izradu i upotrebu identifikacionih dokumenata za zaštićena lica, ili dokumenta o vlasništvu, u kojima su privremeno izmenjeni lični podaci. Pomenuta mera se primenjuje kada je potrebno otkloniti opasnost za eventualne situacije u kojima bi se moglo naći zaštićeno lice.[101] Međutim, odmah je potrebno istaći da primena ove mere ne podrazumeva izmenu izvornih podataka o licu koji se vode u službenim evidencijama. U toku primene ove mere izvorni podaci o zaštićenom licu koji se vode u službenim evidencijama ostaju neizmenjeni. Reč je o ličnim podacima građana koji se odnose na privatnost, integritet ličnosti, lični i porodični život, kao i druga lična prava koja su u vezi sa identifikovanim licem ili licem koje se može identifikovati[102].

Dakle, primena ove mere podrazumeva stvaranje uslova za izradu i upotrebu izmenjene lične isprave ili isprave o vlasništvu, pri čemu zaštićeno lice ima ograničenu mogućnost da slobodno koristi isprave u kojima su

[100] *Ibid.*
[101] G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).
[102] *Ibid.*

privremeno izmenjeni lični podaci. Ograničenje obuhvata isključenje mogućnosti zaključivanja pravnih poslova koji mogu biti od uticaja na treća lica.

Osnovni problem koji se u praksi javlja jeste činjenica da zaštićeno lice može imati potrebu da zaključi neki pravni posao sa trećim licem, koji proizvodi pravno dejstvo i prema tom trećem licu. U tom slučaju je potrebno da dobije saglasnost Jedinice za zaštitu svedoka ili da svedok imenuje punomoćnika koji će u njegovo ime preduzimati radnje. Međutim, i u ovom drugom slučaju je potrebna saglasnost jedinice da bi opunomoćeno lice moglo da zaključi posao. Odabir rešenja zavisi od procene opasnosti kojoj bi moglo da bude izloženo zaštićeno lice u slučaju da određeni pravni posao bude zaključen upotrebom isprava koje sadrže njegove izvorne podatke[103].

4.4.2. Promena identiteta

Promena identiteta je posebna mera koja se primenjuje samo kada se drugim merama ne može obezbediti adekvatna zaštita svedoka. Ova mera se sastoji u kreiranju nove *životne legende* ili *istorije* svedoka, izrade novih identifikacionih dokumenata i preseljenje u novu životnu sredinu, čime se onemogućava trećim licima da uđu u trag njegovom izvornom identitetu.

U ovakvim situacijama mora se voditi računa da je svedoku pritom potrebno obezbediti uživanje svih njegovih atributa ličnog statusa, kao što je bračno stanje, zanimanje, verskih prava i drugih životnih aktivnosti i nakon promene identiteta. Jedan od osnovnih principa prilikom promene identiteta jeste da se zaštita i bezbednost svedoka mora ostvariti bez štetnih posledica za svedoka, kako sa aspekta zagarantovanih ljudskih prava, tako i sa aspekta moralnih vrednosti. Pored toga, klijentu se mora omogućiti ekonomska, socijalna, zdravstvena, pravna pomoć, kao i sva druga potrebna podrška

[103] *Ibid.*

prilikom njegove adaptacije na novi identitet, a sve u cilju zaštite od recidivizma ili ponovnog uključivanja u nedozvoljene aktivnosti.[104]

Kod promene identiteta broj ličnih podataka koji su predmet nove *životne legende* varira od zemlje do zemlje. U nekim zemljama, kao što su Holandija, Velika Britanija i SAD, menjaju se samo neophodni detalji, ime i prezime, dok se u drugim zemljama, na primer u Italiji, Nemačkoj, Slovačkoj i Austriji, menjaju i drugi podaci, kao što su mesto i datum rođenja, ime roditelja, ... Kod promene identiteta mora se voditi računa da treća lica ne mogu uočiti, niti uspostaviti, vezu između starog i novog identiteta, kako bi se štićenom klijentu obezbedila maksimalna bezbednost. Imajući u vidu činjenicu da se vrednosti fizičkih karakteristika osoba najviše koriste za identifikaciju, u nekim državama je dozvoljena i primena plastične hirurgije (Poljska, Srbija, Baltičke zemlje).

Znači, pored podataka koji se menjaju u dokumentima i drugim javnim ispravama, promena identiteta može da podrazumeva i promenu fizičkih, odnosno nekih biometrijskih osobina, što se postiže plastičnom operacijom lica ili uklanjanjem drugih fizičkih znakova raspoznavanja, kao što su mladeži, belezi i tetovaže. Primena mere promene fizičkih osobina se uglavnom odobrava nakon završetka sudskog postupka u kojima je svedok svedočio i kada su donete pravosnažne presude.

Prilikom promene identiteta, klijent je u obavezi da svu dokumentaciju koju poseduje o svom izvornom identitetu preda Jedinici koja sprovodi Program zaštite. To je neophodno, kako iz bezbednosnih razloga, radi sprečavanje pronalaženja izvornog, stvarnog identiteta, tako i zbog sprečavanja raznih zloupotreba korišćenja više identiteta. U postupku promene identiteta zaštićena lica dobijaju nova lična dokumenta, koja su regularno izdata u skladu sa zakonskim normama i sa svim stepenima zaštite, što znači da dokumenta sadrže fotografiju, potpis, biometrijske podatke,... Takođe, potrebo je istaći da se u nekim zemljama moraju promeniti sva dokumenta koja sadrže lične

[104] *United Nations Office on Drugs and Crime /Vienna/, Good practices for the protection of witnesses in criminal proceedings involving organized crime, N.York, (2008).*

podatke zaštićenog lica, dok se u drugima, pak, menjaju samo ona dokumenta koja su od suštinskog značaja za održavanje novog identiteta.

Vrsta i broj dokumenata, odnosno ličnih podataka, koja zaštićenim licima obezbeđuju novi identitet variraju od zemlje do zemlje, ali to su uglavnom:

1. Pasoš;
2. Lična karta;
3. Matični broj;
4. Medicinski karton ili zdravstvena knjižica;
5. Poreski broj;
6. Uverenje o državljanstvu;
7. Vozačka dozvola;
8. Saobraćajna dozvola;
9. Izvod iz matične knjige rođenih;
10. Izvod iz matične knjige državljana;
11. Dokaz o obrazovnoj kvalifikaciji;
12. Dokaz o završenim kursevima i stručnom usavršavanju.

Prilikom izdavanja novih dokumenata zaštićenom licu, potrebno je pažljivo voditi posebnu evidenciju o izdatim dokumentima, sa ograničenim pravom pristupa takvim evidencijama, kao i izvornim podacima. Zbog toga, nakon promene identiteta Jedinica za zaštitu čuva, odobrava i nadzire pristup izvornim podacima o identitetu zaštićenog lica i vodi računa o svim statusnim i drugim pravima i obavezama koja su u vezi sa izvornim identitetom zaštićenog lica[105].

U slučaju Republike Srbije, shodno Zakonu o zaštiti učesnika u krivičnom postupku, postupak izdavanja *legendirane* lične isprave ili dokumenta se ne razlikuje od postupka izdavanja originalne lične isprave ili dokumenta. Važno je naglasiti da podaci u *legendiranoj* ličnoj ispravi ili dokumentu ne smeju biti identična sa podacima nekog drugog lica! Potrebno je

[105]Zakon o programu zaštite učesnika u krivičnom postupku, (Službeni glasnik R. Srbije br. 85/2005).

posebno istaći da izrada i upotreba isprava i dokumenata izvršena u skladu sa ovim Zakonom u cilju primene mera prikrivanja identiteta i vlasništva, kao i promene identiteta zaštićenog lica ne predstavlja krivično delo.

Jedinica za zaštitu je jedini organ koji predstavlja zakonsku sponu između novog *legendiranog* identiteta i evidencija u kojima ostaju izvorni podaci zaštićenog lica, odnosno njegovog *stvarnog* identiteta[106].

U Republici Srbiji je odredbom člana 23. Zakona o zaštiti učesnika u krivičnom postupku, propisano da zaštićeno lice učestvuje u krivičnom postupku sa izvornim identitetom, ako je u svojstvu osumnjičenog, okrivljenog, svedoka saradnika, svedoka, oštećenog, veštaka ili stručnog lica pozvano pred sud povodom krivičnog dela učinjenog pre promene identiteta. Za druge postupke pred sudom ili državnim organom u kojem je neophodna upotreba izvornog identiteta, zaštićeno lice može učestvovati samo uz saglasnost Jedinice za zaštitu[107].

Ukoliko zaštićeno lice nakon promene identiteta učini krivično delo, Jedinica za zaštitu je u obavezi da o tome obavesti nadležnog javnog tužioca i Komisiju za sprovođenje Programa zaštite. Pozivanje zaštićenog lica vrši se preko Jedinice za zaštitu koja obezbeđuje njegov dolazak. U zavisnosti od toga o kojem krivičnom delu se radi, javni tužilac će odlučiti na koji način će da postupi (da odloži krivično gonjenje ili da podigne odgovarajući optužni akt). Učinjeno krivično delo može imati za posledicu i obustavu Programa zaštite [108].

4.5. Izazovi pred sistemom zaštite svedoka i menadžment identiteta

Program zaštite kao najuspešniji instrument u borbi protiv organizovanog kriminala i izvršilaca ratnih zločina se primenjuje samo kada se drugim načinom ne mogu zaštititi lica, koja su spremna da svedoče na sudu.

[106] *Ibid*.
[107] *Ibid.*
[108] G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).

Lica koja se uključe u Program zaštite u većini slučajeva dobijaju prikriveni ili novi, promenjeni identitet, koji koriste dok su u Programu zaštite.

Za zaštićena lica, promena lokacije i promena identiteta znači dobijanje mogućnosti za novi životni početak, sa jedne strane, ali sa druge strane to za njih znači promenu životnih navika, uz ograničenje osnovnih ličnih sloboda i individualnih prava u pogledu kretanja, komunikacije i rada. Međutim, ova mera ima i ozbiljne psihološke i socijalne posledice za zaštićeno lice budući da se očekuje da se to lice ne poziva na prošlost, da se nosi sa pritiskom novog okruženja, kao što su razna raspitivanja i ispitivanja, kao i da započne novi život. U vezi s tim, zaštićenim licima sa promenjenim identitetom se mora pružiti maksimalna psihološka podrška radi što lakšeg adaptiranja i socijalizacije. Zaštićeno lice mora prekinuti sa dotadašnjim načinom života, odnosno mora prekinuti sve navike, kontakte i komunikaciju sa poslovnim vezama, prijateljima i rođacima. To nije ni malo jednostavno imajući u vidu da je reč o licima sa kriminalnom prošlošću. Kod ovih lica poseban problem predstavlja napuštanje društvenog statusa i manifestacija finansijske moći stečene tokom godina bavljenja kriminalnim aktivnostima[109].

Mera promene identiteta mora biti izvedena u skladu sa zakonom, a zaštićenim licima je potrebno obezbediti da koriste stečeno obrazovanje, znanje i iskustvo, odnosno da ga primenjuju u *novom* životu. Međutim, ukoliko se radi o stručnjacima za određene oblasti rada, javnim ličnostima, sportistima, advokatima, to može dovesti do bezbedonosnog problema u sistemu zaštite, jer bavljenje starim profesijama može da dovede do otkrivanja izvornog identiteta. Zbog toga se zaštićenim licima ponekad mora obezbediti sticanje novog obrazovanja i veština radi promene karijere, ali bez falsifikovanja diploma. Dakle, u okviru programa zaštite takvim licima treba omogućiti dodatno obrazovanje i sticanje potrebnih kvalifikacija. Znači, zaštićenom licu se ne može

[109] *Principles of protection Tool 5.17 Witness protection, available on* http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_5-17.pdf, pristupljeno 15.01.2013.

dati diploma lekara, ako to nije njegova stvarna struka, ali može mu se omogućiti da studira medicinu, ako to želi, i da se u tom smeru razvija njegovo obrazovanje i karijera. Prilikom izbora budućeg obrazovanja mora se voditi računa o zanimanjima koja u datoj sredini obezbeđuju brže zasnivanje radnog odnosa, odnosno brže ekonomsko osamostaljivanje.

U sprovođenju Programa zaštite se može javiti i potreba da zaštićeno lice više puta promeni identitet. To je, uglavnom, slučaj kada zaštićeno lice ne može da se adaptira na novu sredinu i novi način života (jezička barijera, prekid komunikacije sa rodbinom i prijateljima, sociološke i kulturne barijere), pa donosi odluku da napusti Program zaštite kome je dobrovoljno pristupio. Nakon toga, može se dogoditi da se javi opasnost za njega i njemu bliska lica i da stoga ponovo zaželi da se uključi u Program zaštite. Nakon novog uključenja zaštićenom licu se ponovo dodeljuje novi identitet. Takođe, promena već promenjenog identiteta se mora izvršiti kada dođe i do *provale*, odnosno otkrivanja *legendiranog* identiteta. Program zaštite se može sprovoditi godinama i decenijama, tako da se promenjeni identitet može preneti i na sledeće generacije.

Razvoj nauke i tehnike, a posebno masovno uvođenje informaciono-komunikacionih tehnologija u svakodnevni život, stavili su programe sprovođenja zaštite svedoka pred velike izazove, posebno u delu Programa koji se odnosi na promenu identiteta i stvaranja *legendi* za zaštićena lica. Sa jedne strane, uvođenje informacionih i biometrijskih tehnologija u sisteme koji pripadaju delokrugu ministarstva unutrašnjih poslova, kako bi se društvo uspešnije suprotstavilo organizovanom kriminalu i ekstremističkim grupama, podiže nivo bezbednosti i efikasnost društva na segmentu ranog otkrivanja planova i namera kriminogenih elemenata društva, otkrivanja mesta boravka, praćenja njihovog rada i kretanja, kao i po potrebi lišavanja slobode.

Sa druge strane, navedene primene tih tehnologija znatno otežavaju rad i ugrožavaju efikasnost u drugom važnom segmentu društvene bezbednosti, a koje pripada domenu pravosuđa! Sudsko procesiranje kriminogenih i

ekstremističkim grupama postaje otežano, jer novi sistemi menadžmenta identiteta ugrožavaju osnovni princip rada sistema za zaštitu svedoka u takvim procesima.

Ranije, dok su se koristile i vodile ručne evidencije, koje nisu bile elektronske i multimedijalne, odnosno nisu sadržavale digitalne fotografije lica ili otisaka prstiju, bilo je jednostavno kreirati i realizovati promenu identiteta i uvođenje novog identiteta u jedinstvene registre i evidencije. Danas se svaka promena podataka u elektronskim bazama podataka automatski registruje i evidentira. Pored toga, činjenica da savremene tehnologije lako obezbeđuju automatski pregled multimedijalnih podataka, na primer fotografije lica, što može ukazati na vezu između starog i novog identiteta, a time i dovesti do otkrivanja pravog identiteta zaštićenog lica i kompromitovanje sistema zaštite svedoka. Pored toga, stvaranje centralizovanih baza dokumenata sa odgovarajućim visokim stepenima zaštite, na primer holografi, a koje se vode na svim nivoima državne uprave, od ministarstava do lokalnih samouprava, predstavljaju dodatno opterećenje sa kojim se suočava sistem zaštite svedoka.

Drugi značajan izazov koje savremene informaciono-komunikacione tehnologije stavljaju pred sistem zaštite svedoka, predstavlja masovna upotreba Interneta u savremenom načinu življenja. Naime, zaštićenim licima se ne može uskratiti korišćenje Interneta, imajući u vidu da se time ograničavaju principi osnovnih ličnih sloboda i individualnih prava. Međutim, zaštićeno lice korišćenjem raznih društvenih mreža, koje često kao svoj vitalan deo sadrže neki oblik menadžmenta identiteta, na primer *Facebook* i *Twitter*, pa i veb sajtova za *online* kupovinu, izlaže se potencijalnoj opasnost otkrivanja svoga *stvarnog* identiteta i time ugrožava svoju bezbednost. Korišćenje Interneta radi ostvarivanja bilo kojeg vida elektronskih komunikacija predstavlja još jedan u nizu izazova sa kojim se susreće sistem zaštite svedoka.

Posebno treba naglasiti opasnost za sistem zaštite svedoka koja dolazi od uvođenja biometrijskih podataka. Nesporna je korist od uvođenja biometrijskih podataka u lična dokumenta, kao jedne od efikasnih mera u borbi protiv

terorizma i organizovanog kriminala, ali uvođenje novih tehnoloških rešenja za identifikaciju lica zasnovanih na korišćenju biometrijskih podataka stvara ozbiljne probleme u sprovođenju Programa zaštite učesnika u krivičnom postupku, u delu promene i prikrivanja identiteta, kao jedne od često primenjenih i do sada efikasne mere zaštite.

Upotreba biometrijskih identifikacionih dokumenata predstavlja ozbiljan izazov u merama zaštite svedoka, pre svega zbog toga što se biometrijski podaci, za razliku od svih ostalih ličnih podataka, ne mogu izmeniti! Naime, ukoliko su određenom licu, pre ulaska u Program zaštite, već uzeti biometrijski podaci, na primer prilikom izdavanja lične karte ili putne isprave, oni ostaju sačuvani u odgovarajućim bazama podataka. Ako se tom licu po ulasku u program zaštite promeni identitet, javiće se sledeći problem: biometrijski podaci iz novog *legendiranog* identifikacionog dokumenta poklopiće se sa ranije uskladištenim biometrijskim uzorcima *stvarnog* identiteta lica i sistem zaštite svedoka biće kompromitovan!

Osim opisanog problema do kojih dolazi u vezi sa izradom novih biometrijskih dokumenata, zaštićenim licima je ograničena i mogućnost putovanja sa novim identifikacionim dokumentima. Naime, ukoliko je lice *pre* promene identiteta posećivalo države u kojima se prilikom izdavanja vize uzimaju biometrijski podaci, kao i na graničnim prelazima prilikom ulaska u tu zemlju, npr. SAD i Velika Britanija, jasno je da će veoma jednostavno biti razotkriven njegov novi identitet. Iz tog razloga se zaštićenom licu, po automatizmu, ograničava ulazak i kretanje u državama koje primenjuju ovakve mere. Treba napomenuti, da u ovom slučaju dolazi do povrede prava na slobodu kretanja, koje je inače zajamčeno Evropskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda.

Takođe, lica kojima je u Programu zaštite promenjen identitet na ovaj način, mogu imati i problema kod obavljanja finansijskih transakcija, podizanja novca i sličnih situacija u kojima se identitet utvrđuje ličnim dokumentima, što takođe dovodi do ograničavanja nekih osnovnih ljudskih prava.

U slučaju da izmena ličnih podataka zaštićenog lica nije dovoljna za uspešnu primenu mere promene identiteta, može se sprovesti i trajna promena fizičkih karakteristika zaštićenog lica. U ovom slučaju zaštićeno lice, pored novog identiteta, dobija i novi izgled. Za razliku od drugih mera koje se odlikuju opozivom prirodom, promena fizičkih karakteristika zaštićenog lica je trajnog karaktera, odnosno zaštićeno lice zadržava novi fizički izgled u slučaju da dođe do obustave ili prestanka sprovođenja Programa zaštite[110].

Ukoliko se licu, koje je u Programu zaštite, promene fizičke karakteristike, na primer crte lica putem plastične operacije, mogu da se pojave problemi druge vrste. Naime, zbog promenjenog fizičkog izgleda lice možda neće moći da ostvari neko svoje pravo koje je ranije ostvarivalo (finansijske transakcije).

Treba imati u vidu da izneti problemi sa kojima se susreće zaštićeno lice u odnosu na sisteme za menadžment identiteta nisu ograničeni samo na javni sektor. U privatnom sektoru takođe postoje baze podataka koje koriste biometriju za proveru identiteta, kao što su baze finansijskih institucija ili osiguravajućih kompanija. Na primer, prilikom obavljanja neke finansijske transakcije može se vršiti identifikacija lica putem fotografije lica. Nakon plastične operacije kojom se menjaju crte lica određene osobe, i tako joj se daje novi identitet, isto lice više neće biti u mogućnosti da ostvaruje finansijske transakcije koje je ranije obavljalo, s obzirom da se novi biometrijski podaci neće poklopiti sa podacima iz baze podataka[111]. Međutim, neka osiguravajuća društva idu i korak dalje pa traže da im se dostavi DNK određenog lica i odbijaju da izvrše isplatu ukoliko im se ne dostavi odgovarajući DNK uzorak.

Uprkos izloženim poteškoćama koje prate promenu identiteta zaštićenog lica u odnosu na savremene sisteme menadžmenta identiteta, ova mera, u

[110] G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd (2006).

[111] *United Nations Office on Drugs and Crime /Vienna/, Good practices for the protection of witnesses in criminal proceedings involving organized crime, N.York, (2008).*

određenim slučajevima, predstavlja jedini način za pružanje efikasne zaštite licu uključenom u Program zaštite. Ukoliko bi zaštićeno lice odbilo pomenutu meru, jedina alternativna mera bila bi dugotrajna izolacija iz okruženja i društva, što može prouzrokovati teške psihološke posledice.

Kako biometrija doživljava svoju sve veću primenu u društvu, i kako je sve više država koristi za utvrđivanje identiteta, Program zaštite svedoka ima sve više problema da efikasno sprovede svoje mere u domenu promena identiteta, a da pritom ne ograničava kretanje zaštićenih lica. Sve ovo ukazuje na ozbiljnu potrebu rešavanja ovih izazova koji stoje pred sistemom zaštite svedoka i savremenih sistema menadžmenta identiteta, kao posledica primene biometrijskih tehnologija u postupcima identifikacije. U profesionalnim krugovima u oblasti zaštite svedoka postoji opšta konstatacija o postojanju i važnosti ovog problema, ali nema saglasnosti o načinu rešavanja, što u budućnosti predstavlja jedan od najvećih izazova za sistem zaštite svedoka.

4.6. Moguća unapređenje mera zaštite u sistemima zaštite svedoka

U Programu zaštite svedoka za unapređenje sistema zaštite svedoka koristićemo multidisciplinaran pristup, koji pored informatičkih obuhvata organizacione, pravne, psihološke i sociološke discipline. Pošto je fokus našeg rada i istraživanja u oblasti informatičkog menadžmenta, u prvom delu izlaganja samo ćemo zbog sagledavanja celine problema ukratko navesti i moguće mere unapređenja u ostalim domenima.

Sve države koje se bave zaštitom svedoka trebalo bi da imaju zakonsku regulativu na nacionalnom nivou. Na nacionalnom nivou je veoma važna saradnja i komunikacija između svih organa koji se bave sistemom zaštite svedoka. U vezi toga, potrebno je ne samo u pravnom, već i organizacionom smislu, precizno definisati nadležnosti i delokrug rada državnih organa koji se nalaze u sistemu zaštite svedoka, kao i nadležnost nevladinih organizacija, koje ostvaruju kontakte sa svedocima pre uključenja u Program zaštite. Bilo bi

poželjno da je regulativa koja se odnosi na zaštitu svedoka na nacionalnom nivou bude usklađena sa evropskom i svetskom regulativom, ali takva dovoljno obuhvatna regulativa ne postoji. Treba istaći, da su međunarodna i regionalna saradnja veoma bitni faktori za uspešno sprovođenje Programa zaštite.

Što se tiče mera psihološke podrške u sistemima zaštite svedoka, važno je znati da su tokom sprovođenja Programa zaštite svedoci izloženi raznim vidovima psihološkog stresa. Svedoci iz oblasti organizovanog kriminala često imaju problem sa ograničenjem kretanja, promenom stila života, prekidom komunikacija sa prethodnim krugom ljudi.

Takođe, ovde dolaze i do izražaja njihove sklonosti ka vršenju krivičnih dela, zloupotrebe narkotika, alkohola i lekova i slično. Resocijalizacija se najčešće javlja i u slučajevima kada je svedok dislociran ili relociran, zbog poteškoća adaptiranja u novu sredinu, nove navike i novi identitet. Sve su to razlozi za uspostavljanje aktivne psihološke edukacije svedoka, ali i lica angažovanih na sprovođenju Programa zaštite. U vezi toga, svaka Jedinica koja se bavi zaštitom svedoka u svom sastavu treba da ima odgovarajuće saradnike, psihologa i kliničkog psihijatra.[112]

Pored navedenih mogućih pravnih, organizacionih i psiholoških unapređenja, posebnu pažnju zaslužuje tehnički aspekt uočenih problema u sistemu zaštite svedoka. Pomenuti tehnički aspekt prvenstveno se odnosi na posledice opšte upotrebe elektronskih komunikacija i informacionih sistema u današnjem svetu na sistem zaštite svedoka, a koji obuhvata promenu identiteta zaštićenog lica, kao i prikrivanje stvarnog identiteta i podataka o vlasništvu.

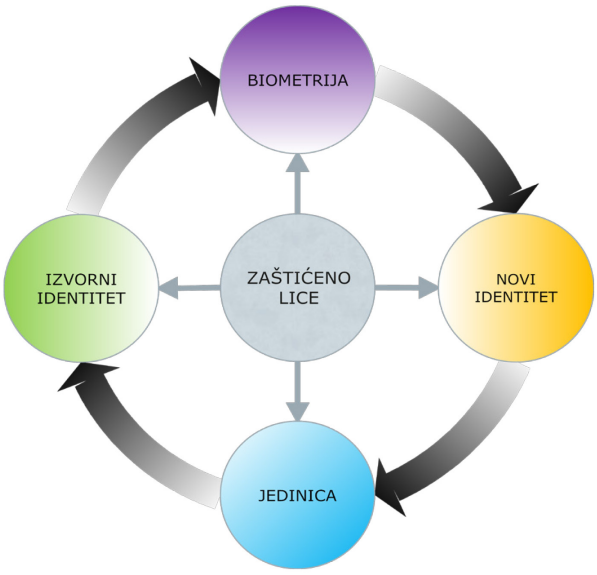
Pre upotrebe Interneta, i posebno korišćenja društvenih mreža, *legendiranom* zaštićenom licu sa se mora pružiti adekvatna obuka za bezbedno korišćenje Interneta na način koji neće kompromitovati sistem zaštite. Prilikom izdavanja novog *legendiranog* identiteta, odnosno novih dokumenata

[112] S. Paunović, D. Starčević, L. Nešić, *Identity Management and Witness Protection System,* Management – časopis za teoriju i praksu menadžmenta, Beograd, (2013).

zaštićenom licu, moraju se voditi posebne evidencije o izvornim dokumentima, koje će se čuvati u arhivama Jedinice za zaštitu.

Nakon promene identiteta zaštićenog lica Jedinica za zaštitu mora voditi računa i o svim drugim statusnim pravima i obavezama, koja su u vezi sa izvornim identitetom zaštićenog lica.

Jedinica za zaštitu je zadužena i za izradu novih biometrijskih dokumenta za zaštićeno lice, pa mora voditi računa i o digitalnom identitetu zaštićenih lica. Jedinica za zaštitu upravlja sa biometrijskim podacima svih lica koja su uključena u Program zaštite. Jedinica ovog tipa je jedini državni organ u sistemu zaštite svedoka koji predstavlja vezu između novog i izvornog identiteta, to jest vodi evidencije u kojoj ostaju izvorni podaci o zaštićenom licu, odnosno podaci o njegovom *stvarnom* identitetu. Međutim, treba imati u vidu da pored Jedinice za zaštitu, koja zakonski održava vezu između novog i izvornog identiteta zaštićenih lica, postoji i neželjena paralelna informatička veza. Ovu informatičku vezu, prikazanu na slici 10, održavaju ranije zabeleženi biometrijski podaci lica, jer su ovi podaci u suštini jedinstveni, nepromenljivi i trajni tokom našeg života, za razliku od drugih ličnih podataka, kao što su ime, prezime, matični broj itd.



Slika 10 Veze između izvornog i novog identiteta

Upravo imajući u vidu navedenu specifičnost biometrijskih podataka, izazovi sa kojima se susreću sistemi za zaštitu svedoka uvođenjem biometrijskih podataka u sisteme menadžmenta identiteta mogu se rešiti jedino primenom odgovarajućih pravnih, organizacionih i tehničkih mera.

Opšte organizaciono-tehničko rešenje navedenog problema bi se postiglo obavezujućim izdvajanjem svih podataka o zaštićenim licima iz postojećih relevantnih baza podataka o građanima i njihovo ažuriranje legendiranim podacima u slučajevima kada za to ima potrebe. Baze podataka sa vezom između *stvarnih* i *legendiranih* podataka zaštićenih lica imale bi i dalje poseban status pod nadležnošću Jedinica za zaštitu na nacionalnom nivou, kako bi se kontrolisano upravljalo i biometrijskom vezom između novog i izvornog identiteta zaštićenih lica. Ako bi isti pristup koristile i druge države, onda bi se mogao na osnovu međunarodnih bilateralnih ili multinacionalnih sporazuma uspostaviti regionalni, evropski, a možda i svetski sistem zaštite takvih lica, koji bi im obezbedio relokaciju u države potpisnice takvih sporazuma ili njihovo slobodno kretanje u okviru tih država. Realno je očekivati da bi se na taj način povećala efikasnost sistema zaštite svedoka saradnika, kvalitet njihovog života nakon *legendiranja* i motivisanost da insajder iz sveta organizovanog kriminala ili ekstremizma postane svedok saradnik.

Ovo je i sa pravnog aspekta na nacionalnom nivou već ostvarljivo, imajući u vidu činjenicu da Zakon o zaštititi učesnika u krivičnom postupku na nacionalnom nivou, daje mogućnost da se Jedinica obrati svim državnim organima za pomoć, tako da su svi državni organi dužni da joj izađu u susret prilikom sprovođenja Programa zaštite.

Sve napred izloženo ukazuje na ozbiljnu potrebu daljeg rešavanja menadžmenta identiteta sa aspekta sistema zaštite svedoka, jer još uvek postoji niz otvorenih pitanja o načinu prevazilaženja opisanih problema. Organizacioni i tehnički model kojim bi se prevazišli problemi iskrsli nakon masovne primene biometrijskih metoda u ovom trenutku predstavlja jedan od najvećih izazova za države i organe koji se bave pitanjem zaštite svedoka.

5. BIOMETRIJSKI SISTEMI ZA UTVRĐIVANJE IDENTITETA

5.1. Menadžment identiteta i biometrijski sistemi za utvrđivanje identiteta

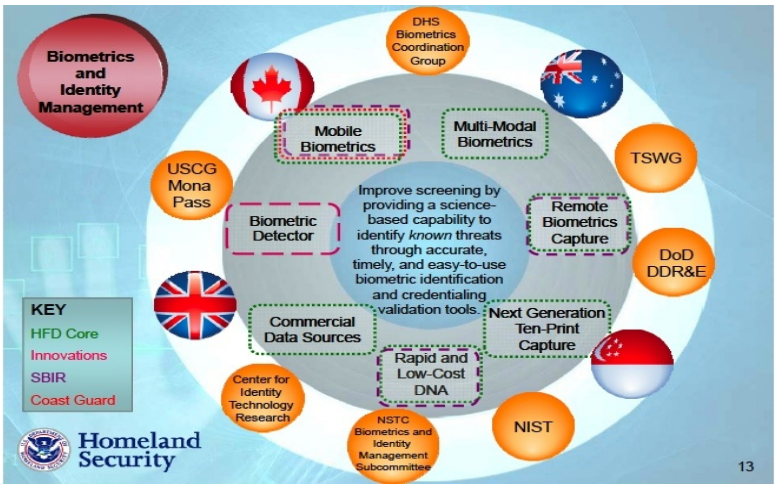
Veliki teroristički napadi obeležili su početak 21. veka (11. septembar 2001. godine u Sjedinjenim Američkim Državama, potom bombaški napadi u Londonu, Madridu, Bostonu, kidnapovanje u moskovskom pozorištu). Većina država je kao najozbiljnije negativne pojave i rizike po bezbednost definisala terorizam i međunarodni organizovani kriminal, jer nanose ogromne štetu kako društvu, tako i državi. Odgovor vodećih zemalja sveta na ove pretnje bio masovna primena informaciono-komunikacionih tehnologija u svim aspektima sistema bezbednosti. Težnja da se sve više takvih poslova automatizovano obavlja, kako bi se uticaj ljudskog faktora na sigurnost rada takvih sistema sveo na minimum ili potpuno uklonio, pospešio je razvoj i intenzivirao primenu biometrijskih sistema za utvrđivanje identiteta.[113] Naime, ozbiljni bezbednosni zahtevi naterali su stručnjake da istraže načine na koje se biometrijski podaci mogu iskoristiti u identifikaciji osoba, odnosno generalno u menadžmentu identiteta.

Danas se biometrijski sistemi koriste u svim oblastima života, od poboljšanja bezbednosti računarskih mreža, efikasnog komuniciranja sa vladinim servisima, zaštite finansijskih transakcija, kontrole pristupa zaštićenim radnim lokacijama, ali su ipak od neprocenjive važnosti za efikasan rad službi bezbednosti. Kao što je već rečeno metod biometrijske identifikacije predstavlja jedan od načina identifikacije osobe, a na osnovu njenih merljivih jedinstvenih bioloških osobina i na slici 11, preuzete sa sajta Departmana unutrašnje bezbednosti Sjedinjenih Američkih Država, prikazan je složen odnos između biometrije i menadžment identiteta.[114]

---

[113] *Report of the Defense Science Board Task Force on Defense Biometrics, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, March (2007).*

[114] Biometrija i menadžment identiteta, objavljeno http://www.Biometrics_and_identity_management_schematic, pristupljeno 13.04.2012.



Slika 11 Biometrija i menadžment identiteta

Biometrijski sistemi automatski identifikuju ili proveravaju identitet pojedinca na osnovu njegovih anatomskih i bihejvioralnih (fizioloških) karakteristika. Ovaj proces se vrši upotrebom računarske tehnologije, koja upoređuje šablone pojedinca u realnom vremenu sa ranije registrovanim podacima. Na primer, postoje uređaji služe pri identifikaciji pojedinca na osnovu njegovog lica, dlana, potpisa, irisa, glasa ili otisaka prstiju, slika 12.

Slika 12 Primeri biometrijskih sistema za utvrđivanje identiteta [115]

U zavisnosti od potreba, biometrijski sistem može da radi na dva režima rada:

Režim autentifikacije – U ovom režimu rada biometrijski sistem potvrđuje ili odbija da potvrdi identitet, koji je prezentovala osoba prilikom pristupa sistemu, tako što se porede trenutno uzete biometrijske karakteristike sa ranije

[115] Anil K. Jain and Arun Ross, *Introduction to Biometrics*, Handbook, (2008), str. 1-23.

u bazi zapisanim šablonom posmatrane karakteristike za osobu koja je registrovana u sistemu pod tim identitetom. To je poređenje *jedan prema jedan* (*engl*. *one–to–one*). Ako neko želi da predstavi svoj identitet i bude identifikovan, prilaže svoj biometrijski šablon sadržan na identifikacijskoj kartici čiju verodostojnost možemo proveriti. Sistem tada poredi podatke sa kartice, sa ranije snimljenim podacima osobe koja je priložila karticu. Ako se podaci podudaraju, ta osoba je primljena, u suprotnom je odbijena. Ova vrsta prepoznavanja se naziva i pozitivno prepoznavanje. Cilj je da se spreči da više ljudi koristi isti identitet.

Režim identifikacije – U ovom režimu rada biometrijski sistem vrši prepoznavanje identiteta, odnosno sistem upoređuje biometrijske karakteristike osobe sa svim šablonima sačuvanim u bazi da bi našao najveće poklapanje. Tom prilikom se izvodi upoređivanje tipa *jedan prema više* (*engl*. *one–to–many*). Za razliku od *autentifikacije*, ovde osoba ne treba da priloži svoje podatke. Sistem jednostavno skenira neku karakteristiku osobe. Potom proverava da li su njeni podaci upisani u sistem i ako jesu, da li joj je dozvoljen pristup. Ovaj način rada se još naziva i negativno prepoznavanje. Cilj je da se spreči da jedna osoba koristi više identiteta. Mada biometrijska tehnologija meri različite biometrijske karakteristike na različite načine, svi biometrijski sistemi, kao izlazni rezultat daju stepen podudaranja (*engl*. *matching score*) ulaznog podatka sa šablonom sačuvanim u bazi.

Biometrijski sistemi uglavnom se sastoje od dva tehnološka segmenta, od segmenta koji se koristi pri uzimanju i upisivanju biometrijske karakteristike, odnosno registraciji biometrijskih karakteristika, kao i od segmenta za utvrđivanje identiteta osobe.

Proces uzimanja podataka sastoji se od:

- Akvizicije biometrijskih podataka upotrebom biometrijskog skenera;
- Obrade uzetih podataka i pripreme za upis u bazu biometrijskih podataka;
- Upisa podataka u bazu podataka, neku centralnu bazu ili upisa na lokalni prenosni uređaj (*smart* kartica);

Proces prepoznavanja sastoji se od:

- Akvizicije biometrijskih podataka upotrebom biometrijskog skenera,
- Obrade biometrijskih podataka i pripreme za upoređivanje sa ranije uzetim i zapisanim podacima,
- Upoređivanja uzetih podataka sa podacima koji su ranije upisani radi određivanja stepena podudarnosti.

Kao što je već rečeno, proces prepoznavanja može da se koristi u dva režima rada uređaja, i to:

1. Režim identifikacije - „*Da li ja znam ko si ti?*". Uzeti biometrijski podaci se upoređuju sa podacima koji se nalaze u bazi podataka na računaru. Tip *1:n*.
2. Režim autentifikacije - „*Da li si ti onaj za koga se izdaješ?*". Zapisani biometrijski podaci se upoređuju sa podacima koje je korisnik doneo (npr., sa *smart* kartice). Tip *1:1*.

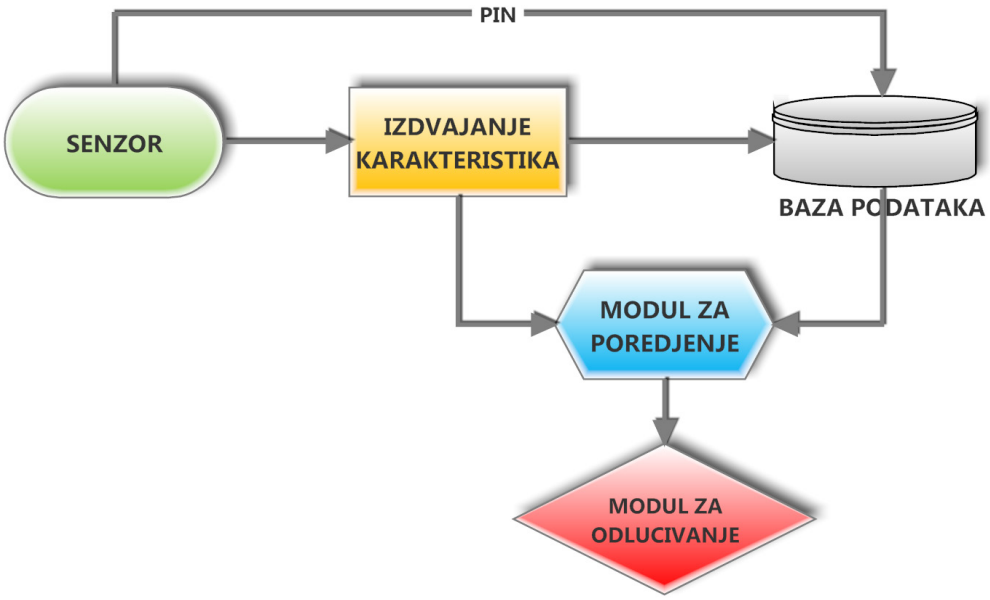
Rezultati upoređivanja se prosleđuju aplikaciji na dalju obradu i sa konačnim upisom događaja sa svim pratećim podacima.

Biometrijski sistem ima tipično pet sastavnih modula:[116]

1. ulazni uređaj - *senzor (engl. sensor module)* – koji uzima biometrijske podatke osobe i konvertuje ih u digitalni oblik (npr. skener za otiske prstiju);
2. modul za izdvajanje *karakteristika (engl. feature extraction module***) –** koji obrađuje digitalizovan ulazni podatak radi izdvajanja jedinstvene karakteristike i koja se može smestiti u šablon (*engl. template*) (npr. izdvajanje minucija iz slike otiska prsta);
3. modul za skladištenje podataka, *baza podataka*
4. modul za poređenje *(engl. matching module)* – služi za poređenje izdvojene karakteristike sa podacima iz šablona sačuvanog u bazi;
5. modul za donošenje odluke *(engl. decision-making module***) –** uz pomoć ljudskog faktora prihvata ili odbija identitet (verifikacija), ili utvrđuje identitet na osnovu skora poređenja (identifikacija).

[116] D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents,* Forensic Science International 167 (2007), 154–159.

Opšti model biometrijskog sistema prikazan je na blok dijagramu 1.



Blok dijagram 1 Opšti model biometrijskog sistema

Kao što je pomenuto, pored pozitivnih biometrijskih sistema, postoje i negativni biometrijski identifikacioni sistemi**.** Oni su dizajnirani tako da potvrđuju nepostojanje biometrijske osobine koja se želi identifikovati. Kod ovih sistema traži se nepodudaranje rezultata. Poređenjem biometrijskih podataka osobe koja se želi identifikovati sa podacima iz baze podataka sprečava se zloupotreba, odnosno onemogućava se toj osobi da se korišćenjem lažnih dokumenata registruje pod više identiteta. Drugi tip ovih sistema je nadzorna baza, na kojoj se nalaze biometrijski podaci sumnjivih osoba ili osoba sa specijalnim statusom. Te baze su dizajnirane tako da identifikuju osobe sa liste sumnjivih i upozore bezbednosne službe, radi preduzimanja potrebnih mera. Prilikom odabira biometrijskih sistema mora se voditi računa o pouzdanosti odluka koje donose takvi sistemi (odnosi se na tačnost, brzinu rada i faktore koji mogu uticati na njihov rad), prihvatljivosti (spremnost ljudi da prihvate korišćenje ovih sistema u svakodnevnom radu), kao i otpornosti (koliko je sistem otporan na zloupotrebu i na napade). U praksi, proces rada ovih sistema je potpuno automatizovan i za utvrđivanje identiteta potrebno je u proseku nekoliko sekundi, što ovaj proces čini brzim i efikasnim.

Biometrijski sistemi identifikacije su postali važan deo sistema za utvrđivanje identiteta. Uređaji na bazi biometrijske tehnologije koji se u praksi koriste za kontrolu pristupa (*engl. access control*) su:

- kamere i skeneri za snimanje slika ili merenje biometrijskih karakteristika, i
- računari (engl. *hardware)* sa odgovarajućim programom (*engl. software*) za komprimovanje, kodiranje i upoređivanje snimljenih ili izmerenih sa zapisanim karakteristikama.

Biometrijski sistemi za utvrđivanje identiteta se veoma brzo razvijaju. Primena biometrijskih sistema poboljšava opšti nivo bezbednosti građana, jer imaju potencijal za veću preciznost u utvrđivanju identiteta građana.

Zbog značaja utvrđivanja identiteta stalno se radi na usavršavanju sistema za preciznu identifikaciju, odnosno na poboljšavanju njihovih performansi.

5.2. Preciznost biometrijskih sistema identifikacije

Preciznost biometrijskih sistema zavisi od opsega i tipa podataka koje se uzimaju, kvaliteta opreme za analize biometrijskih uzoraka, kao i stanja ulaznog biometrijskog podatka. Nijedan biometrijski sistem identifikacije današnjice nije apsolutno precizan. Biometrijske karakteristike uzete od iste osobe mogu se razlikovati u zavisnosti od uslova i vremena njihovog uzimanja, pa se i ne može očekivati njihovo apsolutno poklapanje. Što je stepen podudaranja veći, to je sistem sigurniji da dva biometrijska uzorka dolaze od iste osobe. Ipak, odluku sistema određuje neka granica, sigurnosni prag, koju korisnik postavlja u skladu sa namenom sistema. Na osnovu raspoloživih tehnologija, odnosno osnovu dosadašnjih iskustava u radu sa tim tehnologijama, lako se može zaključiti da su precizniji biometrijski sistemi koji rade sa otiscima prstiju od sistema koji rade sa prepoznavanjem lica osoba.

Preciznost biometrijskih sistema, u kontekstu verovatnoće, se meri preko tri osnovna pokazatelja:

- Mera u kojoj se biometrijski podatak jednog čoveka povezuje sa biometrijskim podatkom drugog čoveka;
- Mera neprepoznavanja sadašnjeg biometrijskog podatka neke osobe sa ranije uzetim podacima te osobe;
- Mera nemogućnosti preciznog određivanja rezultata zbog slabog kvaliteta ulaznih podataka;

Sva tri pokazatelja su relevantna u slučaju režima rada tipa *1:n,* dok su druga dva relevantna kod režima rada tipa *1:1*.

Pre korišćenja biometrijskih sistema potrebno je detaljno proučiti njihove osobine, performanse, kao i ograničenja. Prilikom korišćenja biometrijskih sistema radi utvrđivanja identiteta mogu se pojaviti i sledeće greške:[117]

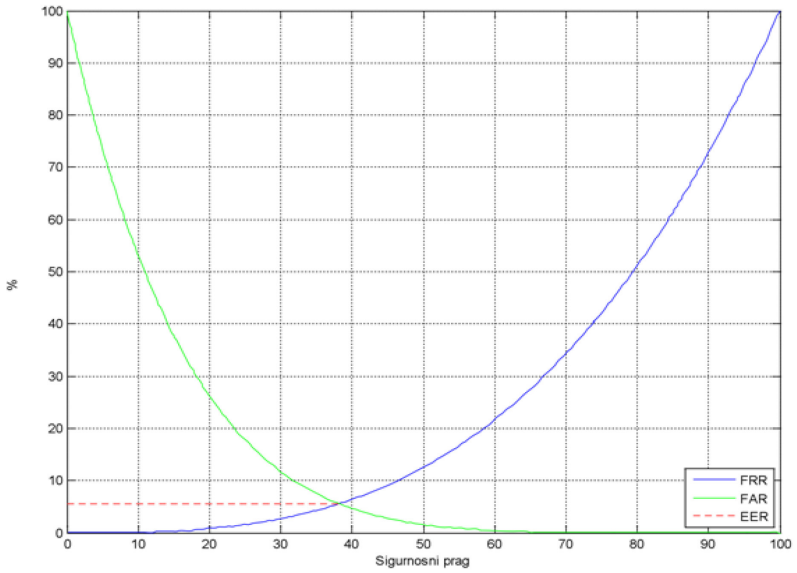
Pogrešno prihvatanje. Situacija u kojoj sistem prihvata lažnog korisnika, kao legitimnu osobu, imajući u vidu da je u bazi podataka pronašao biometrijski podatak sličan ulaznom podatku. Ova greška sistema može se pojaviti u slučaju postojanja visokog stepena sličnosti između biometrijskih karakteristika različitih osoba.

Pogrešno odbijanje. Situacija kada biometrijski sistem zbog nedovoljnog podudaranja ulaznih biometrijskih podataka sa podacima u bazi podataka ne prepoznaje legitimnog korisnika, pa odbija identifikaciju. Ovaj tip ograničenja rada sistema je ipak prihvatljiviji od prvog tipa pogrešnog rada sistema, jer korisnik može više puta ponoviti postupak identifikacije.

Da bi se bolje analizirao uticaj ovih grešaka na rad sistema u celini potrebno je izračunati odnos između broja pogrešnih prihvatanja i broja neovlašćenih pristupa, odnosno procenat pogrešnog prihvatanja (engl. *False Acceptance Rate*, ***FAR***). Takođe, je potrebno naći i odnos između broja pogrešnih odbijanja i broja ovlašćenih pristupa, odnosno procenat pogrešnog odbijanja *(*engl. *False Rejection Rate, **FRR**).* Prihvatljive vrednosti za *FAR* i *FRR* zavise od *sigurnosnog praga* nekog sistema (*engl. Security Threshold*). U aplikacijama u

[117] D. Dessimoz, J. Richiardi, *Multimodal Biometric for Identity Documents*, Research Report (2005).

kojima se zahteva viši nivo sigurnosti rada, na primer u kontroli pristupa strogo obezbeđenim resursima, sistem će rigoroznije raditi poređenje trenutno unesenih biometrijskih podataka sa podacima u bazi podataka, što će uticati na smanjenje pogrešnih prihvatanja, odnosno smanjenje *FAR*-a, ali po cenu povećanja broja pogrešnih odbijanja, odnosno povećanja *FRR*. Na osnovu navedenog se može zaključiti da su *FAR* i *FRR* obrnuto proporcionalne funkcije u zavisnosti od bezbedonosnog nivoa nekog sistema. Odluka o nivou bezbednosti nekog sistema zavisi od svrhe biometrijskog sistema i predstavlja kompromis između upotrebljivosti i sigurnosti rada. Sa druge strane, postoje komercijalne aplikacije u kojima odbijanje autorizovanog korisnika može naneti velike štete vlasnicima kontrole pristupa, pa se tu smanjuje *FRR* na račun povećanja *FAR*.[118] Na dijagramu 1 je prikazana tipična zavisnost parametara *FAR* i *FRR* od sigurnosnog praga za biometrijski sistem. Tačka gde *FAR* i *FRR* imaju istu vrednost je tačka sa jednakim procentima grešaka *FAR* I *FRR* (engl. *Equal Error Rate* – *EER*) i koristi se kao dobro merilo za procenu performansi sistema zajedno sa *FAR* i *FRR*.



Dijagram 1 Primer zavisnosti FAR-a i FRR-a od sigurnosnog praga

[118] D. Dessimoz, J. Richiardi, *Multimodal Biometric for Identity Documents*, Research Report (2005).

Iako se na osnovu dijagrama 1 može zaključiti da je biometrijski sistem koji ima vrednost *EER*-a od 5% pouzdaniji od sistema čija je vrednost *EER* od 10%, ipak u praksi se preporučuje poređenje kvaliteta sistema različitih proizvođača samo na osnovu *EER*, pogotovo ako se vrednosti neznatno razlikuju. Korisnik sistema ima mogućnost da se, u zavisnosti od namene sistema, opredeli za poželjnu vrednosti parametra *FAR*, odnosno *FRR*. U slučajevima kada tražimo veoma siguran sistem identifikacije, mogućnost neovlašćenog pristupa, određena parametrom *FAR*, se može svesti na minimum podešavanjem sigurnosnog praga koji to obezbeđuje. Naravno, sigurnosni prag koji pruža veću bezbednost rada istovremeno smanjuje upotrebljivost sistema, jer će više autorizovanih korisnika doći u situaciju da budu odbijeni. Nasuprot tome, manja kritična vrednost sigurnosnog praga kreira sistem pogodniji za korisnika, ali mu pritom snižava stepen bezbednosti.

Međutim treba napomenuti da pored navedenih grešaka u radu sistema postoji i ograničenje poznato pod imenom *stopa neprihvatanja unosa biometrijskog podatka*, (engl. *failure to enroll rate, FTE*). *FTE* meri verovatnoću da osoba neće moći predati svoje biometrijske karakteristike. Na primer, otisak prsta osobe koja obavlja fizički posao rukama možda se neće moći uzeti zbog deformacija i istrošenosti brazda na rukama. Veći procenat ljudi nije u mogućnosti da pruži tražene biometrijske karakteristike u pojedinim sistemima identifikacije i zbog tražene velike preciznosti sistema ili zbog kulturoloških ili verskih barijera. Hendikepirane osobe nisu u mogućnosti da imaju biometrijske podatke, na primer, ukoliko su nemi ili ukoliko su bez prstiju ili ruku. Urođene mane, izvršene operacije ili povrede mogu biti razlog nemogućnosti korišćenja biometrijskih sistema.

Pored brojnih prednosti i grešaka biometrijski sistemi imaju i neka druga ograničenja koja u praksi otežavaju njihovu primenu :[119]

[119] Sedma međunarodna konferencija o elektronskoj trgovini i elektronskom poslovanju, Zbornik radova, Palić (2007).

- Kvalitetni uređaji koji se koriste za biometrijsku identifikaciju i prateća softverska rešenja mogu biti skupi;
- Trajnost uređaja nije dovoljno proverena u praksi, jer se koristi relativno nova tehnologija;
- Pouzdanost rada pojedinih sistema je upitna;
- Traži se stručno osposobljavanje korisnika za rad sa ovakvim sistemima;
- Stalno otvoren problem privatnosti – mnogi korisnici smatraju da prikupljanje biometrijskih podataka ugrožava njihovo pravo na privatnost, pogotovo ako je reč o centralizovanim bazama podataka. Formiranje podataka za biometrijsku identifikaciju mora biti prethodno regulisano zakonom;
- Nedostatak standarda - proizvođači uređaja za biometrijsku identifikaciju često koriste vlasnička rešenja (*proprietary solutions*), koja nisu međusobno kompatibilna. Razvoj bez međusobne komunikacije dovodi do toga da biometrijski otisak sa jednog uređaja nije dovoljno sličan otisku na drugom, što će značajno povećati broj odbijenih pokušaja identifikacije i izazvati nezadovoljstvo korisnika;

5.3. Sistemske slabosti biometrijskih sistema

Zbog svoje prirode rada, a reč je o statističkoj obradi i interpretaciji rezultata zahvaćenih biometrijskih podatka, biometrijski sistemi se u jednom aspektu bitno razlikuju od većine tehničkih sistema koje susrećemo u svom okruženju. Naime, njihove radne performanse ne zavise samo od kvaliteta upotrebljenog sistema, već i od toga koja grupa ljudi ga koristi! Dakle, biometrijski sistemi nisu precizni u istom stepenu za sve grupe korisnike. Od biometrijskih osobina samih korisnika zavisi stepen njihove preciznosti. U jednoj grupi ljudi problem mogu imati oni sa autorizovanim pristupom, ali čiji identitet sistem ne potvrđuje. U drugoj grupi ljudi možemo imati problem zbog većeg broja grešaka u prihvatanju ljudi sa lažnim identitetima. Važno je

napomenuti da pojava lažnog prihvatanja ili odbacivanja nije ravnomerno raspoređena među različitim korisnicima biometrijskog sistema.

Postoji više uzroka koji dovode do opisanog fenomena ponašanja biometrijskog sistema. Pre svega, podsetimo se da osnova rada biometrijskih sistema leži na našem *uverenju* da se međusobno možemo razlikovati na osnovu fizičkih i ponašajnih osobina. Praksa, podržana statističkim rezultatima na velikom broju slučajeva, ide u prilog iznetoj tezi. Međutim, prvi problem koji treba rešiti pojavljuje se u načinu rada sa *sirovim* biometrijskim podacima, odnosno podacima koje generiše ulazni uređaj ili senzor, jedan oblik analogno-digitalnog konvertora. U zavisnosti od odabrane tehnologije rada, ovaj uređaj koristi princip prostornog i/ili vremenskog odabiranja, kako bi u opštem slučaju formirao n-dimenzionalnu matricu biometrijskih podataka koju prenosi računarskom sistemu. Već u ovom koraku se javlja proces aproksimacije, koji suštinski utiče na dalju obradu i donošenje zaključaka. Umesto da biometrijski sistem, u teorijskom pogledu, radi sa beskonačno mnogo podataka i sa neograničenom preciznošću za svaki zahvaćeni podatak, a čime bi se u potpunosti opisala posmatrana biometrijska osobina čoveka, uređaj aproksimira beskonačni skup podataka konačnim brojem podataka. *Verujemo* da ovaj skup podataka još uvek ne samo dovoljno precizno opisuje posmatranu osobinu čoveka, već i da se međusobno *razlikuje* od skupa podataka za nekog drugog korisnika.

Drugi, veoma značajan uzrok za pojavu fenomena zavisnosti performansi rada sistema od ulaznih biometrijskih podataka, leži u sledećom koraku, obradi biometrijskih podataka radi iznalaženja vrednosti *karakteristike* (engl. *feature extraction*). Naime, matrica sirovih podataka koju nam je dostavio senzor u procesorskom smislu može biti veoma zahtevna, pa se praktično u svim biometrijskim sistemima vrši *predobrada* (*pre-processing*), postupak kojim se ulazna matrica sa većim brojem podataka zamenjuje matricom sa mnogo manje podatka, a i sa manje dimenzija. Ako su poznata ograničenja koja mora zadovoljiti ciljna matrica, onda govorimo o *šablonu* ili *uzorku* (engl. *template*), pa

se predobrada svodi na određivanje vrednosti elementa u takvoj matrici. Tako dobijen skup biometrijskih podataka za dati ulaz se naziva *karakteristika* i tipično se smešta u bazu podatka. Ovaj proces je od ključnog značaja za rad biometrijskog sistema i sprovodi se na osnovu odgovarajućeg *algoritma za izdvajanje karakteristika*, kao rezultata prethodnog naučno-istraživačkog rada u oblasti biometrije. Algoritam za izdvajanje karakteristika treba da poseduje svojstva jakog diskriminacionog algoritma. U idealnom slučaju, očekujemo da će nakon njegovog rada, i formiranje baze uzoraka, svi uneti uzorci biometrijskih karakteristika jedne osobe biti vrednosno jedinstveni. Takođe, očekujemo da će od strane algoritma za upoređivanje svi uzorci jedne osobe biti prepoznati kao članovi jedne grupe podataka i da u toj grupi nećemo sresti uzorke drugih osoba. Nažalost, publikovani algoritmi to ne mogu ostvariti u svakom konkretnom slučaju, i to predstavlja sistemsku slabost biometrijskih sistema.

Dakle, u praksi se susrećemo sa problemom da će postojati različite anomalije u ponašanju nekog biometrijskog sistema, kao rezultat reakcije sistema na izvedenu biometrijsku karakteristiku posmatranog korisnika!

Studiju koja obuhvata opisane slabosti biometrijskih sistema uradili su *Doddington* i ostali, i poznata je pod nazivom *biometrijska menažerija*. Izvršena je kategorizacija biometrijskih korisnika na osnovu tih razlika koja se popularno naziva "*Doddington's zoo*". Podela korisnika je izvršena na ovce, koze, jagnjad i vukove. Ova kategorizacija se pokazala kao dobra u svim biometrijskim modalitetima. Novi okvir razvoja biometrije upravo je zasnovan na biometrijskoj menažeriji.[120]

1. *Ovce* predstavljaju većinu stanovništva. Klasteri uzoraka pojedinih osoba su međusobno dovoljno daleko udaljeni, a međusobna udaljenost uzoraka u klasteru je dovoljno mala. Za posledicu imamo prilično pouzdano utvrđivanje identiteta. Od ovaca očekujemo da doprinose

[120] N.Yager, T.Dunstone, *The Biometric Menagerie*, IEEE, (vol. 32 no. 2), February (2010), str. 220-230.

niskoj stopi, kako pogrešnog prihvatanja, *FAR*, tako i pogrešnog odbacivanja, *FRR*.

2. *Koze* predstavljaju grupu korisnika koji predstavljaju problem algoritmu korišćenom za poređenje uzoraka, odnosno određivanja stepena podudarnosti izvedenih karakteristika. Njihovi uzorci pokazuju velike varijacije *unutar* date klase, pa ih algoritam za utvrđivanje identiteta često pogrešno odbija. To su korisnici koji podižu vrednost stope pogrešnog odbijanja, *FRR*.
3. *Jagnjad* su grupa korisnika kod kojih se biometrijske karakteristike dosta poklapaju sa biometrijskim karakteristikama drugih pojedinaca. Možemo reći da problem potiče od slabosti algoritma za nalaženje vrednosti karakteristika, jer njihovu klasu pozicionira suviše blizu drugim klasama, tipično ovcama, i na takav način ostavlja nizak stepen varijacija *između* ovih klasa. Jagnjad su korisnici koji podižu stopu lažnog prihvatanja u sistemu, *FAR*.
4. *Vukovi* su grupa korisnika koji su uspešni u manipulaciji sa svojim biometrijskim karakteristikama, na primer oponašanje glasa ili potpisa, kako bi obmanuli i zloupotrebili biometrijski sistem. Ova grupa korisnika podiže stopu lažnog prihvatanja identiteta, *FAR*.

Ovce predstavljaju kategoriju većinu korisnika prema kojoj se sistem orijentisan, dok koze, jagnjad i vukovi predstavljaju manju, ali problematičnu kategoriju korisnika. Razlozi zbog kojih postoji razlika među korisnicima su različiti i složeni. Najvažniji, kao što su ulazni uređaji i kvalitet akviriranih podataka, algoritmi za izdvajanje karakteristika i poređenje uzoraka, su već navedeni, ali na navedene anomalije mogu uticati i drugi faktori, kao što je nepridržavanje procedure unosa podataka i nedovoljna obučenost ljudi koji rade na unosu podataka. Nije prihvatljivo shvatanje da postoje ljudi koji su sami po sebi nepodobni za biometrijsku identifikaciju. Opisani problemi predstavljaju izazov za ljude koji se bave biometrijom, a mogu se minimizirati

boljim procedurama rada, boljom obukom ljudi koji rade na poslovima zahvatanja podataka, kvalitetnijom opremom, ali pre svega pronalaženjem boljih algoritama za izdvajanje karakteristika i upoređenje karakteristika. U svojoj studiji autori su naveli i postojanje novih životinja u biometrijskom zoološkom vrtu, međutim broj korisnika toga tipa je zanemarljiv u odnosu na pomenute četiri kategorije. U ovoj studiji *Doddington* i ostali su koristili statističke postupke u procesu istraživanja kako bi se uočilo prisustvo ovih kategorija u biometrijskim sistemima. Svoju studiju su sproveli u biometrijskim sistemima koji identifikaciju vrše na osnovu biometrije glasa. Kombinacija *F-testa, Kruskal Wallis* testa i *Durbin* testa se koristi kako bi se utvrdila pojava ovih kategorija korisnika u 1998 *NIST* bazi podataka uzoraka glasa. Pored već navedenih grešaka biometrijskih sistema u postupku identifikacije, *FAR* i *FRR*, a koji bitno utiču na rad sistema, potrebno je osvrnuti i na još dva uzroka pogrešnog rada sistema. Jedan uzrok je greška koja potiče od loše akvizicije sirovog biometrijskog podatka, *FTA* (engl. *Failure to Acquire*), a drugi uzrok je greška koja proističe iz nemogućnosti algoritma za izvođenje karakteristike da na osnovu podatka dobijenih od senzora odredi vrednosti uzorka i da potom uzorak upiše u bazu uzoraka, *FTE* (engl. *Failure to Enroll*). Obe greške, *FTA* i *FTE*, izražavaju stopu tog tipa greške, odnosno predstavljaju odnos broja neuspešnih ishoda u odnosu na ukupan broj pokušaja. Tipičan slučaj *FTA* greške je nemogućnost uređaja da uspešno snimi datu biometrijsku karakteristiku, recimo, slučajevi kada osoba nema prst ili kada su brazde na prstu toliko neizražene da se ne mogu snimiti. *FTE* označava procenat korisnika koji ne može biti uspešno upisan u biometrijski sistem, jer je sistem tehnološki limitiran. Na primer, greške koje potiču od programa koji ne može da odredi vrednosti parametara karakteristike ili od sistema za upravljanje bazom podataka, jer ne može da upiše uzorak. *FTE, FTA, FAR, FRR* predstavljaju važne performanse u biometrijskim sistemima i uvek se moraju imati u vidu prilikom korišćenja biometrijskih sistema.[121]

[121] A.K.Jain, A.Ross, *Introduction to Biometric,* Handbook of biometrics, Springer, (2008), str. 6-12.

Izbor biometrije za određenu aplikaciju najviše je određen tolerisanim veličinama ovim greškama. Pored toga, na izbor utiču i ostali faktori kao što su troškovi sistema, brzina protoka, prihvatanje ovih sistema od strane društva, kao i lakoća prilikom upotrebe.

Kada se govori o bezbednosti računarskog sistema i podataka misli se na zaštitu od neautorizovanog korišćenja računarskog sistema i podataka koje on sadrži. Postizanje bezbednosti uz pomoć biometrijskih tehnologija predstavlja poseban izazov imajući u vidu izazove opisane pomoću biometrijske menadžerije. Svaki biometrijski sistem može biti zloupotrebljen, a to se meri stopom lažnog prihvatanja (*FAR*). Do toga može doći zbog recimo posekotina na prstu, bora na licu koje nastaju sa godinama, kao i zbog promena u okolini, kao što je promena osvetljenja kod biometrije crta lica ili prljav senzor kod biometrije otiska prsta. Izazov koji je stavljen pred biometriju je prevazilaženje problema koji se odnosi na lažno prihvatanje pojedinaca, pogrešno odbacivanje, uticaj grešaka *FTE, FTA, FAR i FRR* na preciznost i ukupne performanse sistema, kao i prevazilaženje različitih vidova zloupotrebe, kao što je krađa identiteta. Kao što je već rečeno, ključ uspeha bi bio dizajniranje biometrijskog algoritam koji će moći da se uhvati u koštac sa svim opisanim problemima.

Biometrijski sistemi mogu pokazivati slabosti prema različitim oblicima ugrožavanja njihove bezbednosti: [122]

- Napad na zaštićene tehničke resurse od kojih zavisi rad biometrijskih sistema,
- Zloupotreba biometrijskog podatka, kao što je korišćenje lažnog otiska prsta,
- Usporavanje i zaustavljanje sistema zbog preopterećenosti ili napad na performanse sistema,
- Odbijanje pristupa sistemu ovlašćenom korisniku.

[122] A.Adler, *Biometric System Security,* Handbook of biometrics, Springer (2008), str. 382-383.

Pored navedenih grupa slabosti koje vode ka kompromitaciji biometrijskih sistema, postoji i opasnost od krađe identiteta. Do krađe identiteta može doći iz sledećih razloga:[123]

- Biometrija pojedinca nije tajna, svako može doći do, recimo, nečije slike, glasa ili potpisa,
- Biometrijska karakteristika se ne može poništiti, ona je stalno povezana sa pojedincem, a jednom kompromitovan biometrijski podatak otvara mogućnost dalje zloupotrebe,
- Biometrijska karakteristika se može koristiti u različitim vrstama aplikacija, što može da dovede do različitih vidova zloupotrebe.

Slabe tačke biometrijskih sistema mogu se ispoljiti na više načina:[124]

1. U potvrđivanju identiteta, posebno kada su u pitanju lični dokumenti. Problem može biti maskiran visokom bezbednošću posmatranog dokumenta, kao što je pasoš, a on se izdaje na osnovu manje zaštićenih dokumenata, kao što je recimo izvod iz matične knjige rođenih.

2. Napad na biometrijski senzor dovodi do toga da se u biometrijski sistem unese lažan biometrijski podatak. Pored toga, može doći i do zavaravanja sistema uz korišćenje recimo šminke ili naočara, ako se snima biometrija crta lica. Mala rotacija glave može zbuniti algoritme kod biometrije irisa.

3. Biometrijska segmentacija - slučaj kada biometrijski sistem prethodno mora da automatski detektuje biometrijski objekat na posmatranoj sceni. Na primer kod sistema nadzora kod koga algoritmi za detekciju lica, prepoznaju lice sa dva oka. Ukoliko u ovom slučaju neko prekrije oko, sistem ga neće prepoznati.

4. Izdvajanje karakteristika - napad na ovaj deo sistema ima za cilj da izbegne detekciju ili stvori varalicu. Najbolji način za prevazilaženje ove

[123] G. Fahmy, D. E. M. Nassar, E. Haj-Said, H. Chen, O. Nomir, J. Zhou, R. Howell, H. H. Ammar, M. Abdel-Mottaleb, and A. K. Jain, *Toward an automated dental identification system,* Journal of Electronic Imaging, 14(4), 043018, (2005).
[124] *Ibid.*

slabosti je dizajniranje specijalnog algoritma. Pored toga postoje velike razlike među pojedincima u pogledu tačnosti i pouzdanosti biometrijskih podataka. To je predstavljeno u biometrijskoj menažeriji – ovce su dominantan tip i kada je u pitanju ova kategorija, biometrijski sistemi dobro rade. Koze je teško prepoznati. One nepovoljno utiču na performanse sistema iskazane pokazateljom *FRR*. Jagnjad pogoršava otpornost sistema na lažno predstavljanje. Vukovi lako manipulišu svojim biometrijskim karakteristikama. Postojanje jagnjadi i vukova unosi slabost u biometrijski sistem.

5. Procena i kontrola kvaliteta biometrijskog uzorka. Ovo je važno kako bi se obezbedila niska stopa greške, a postiže se primenom odgovarajućeg algoritma za validaciju uzorka.

6. Šabloni - slabost biometrijskih sistema se ogleda i u tome što se jedan biometrijski uzorak može koristiti u različitim aplikacijama, što može da dovede do zloupotrebe biometrijskih podataka. Zbog toga je potrebno ustanoviti zakonodavni okvir po kome će samo država moći da daje dozvolu za korišćenje jednog biometrijskog uzorka u različitim aplikacijama.

7. Skladištenje podataka – Uskladišteni biometrijski podaci se čuvaju radi verifikaciju ili identifikacije identiteta. Podaci se skladište u lokalne i centralne baze podataka. Slabe tačke ovog dela sistema se ogledaju u tome što može doći do kopiranja uzoraka, odnosno krađe identiteta.

8. U proceduri poređenja određuje se stepen verovatnoće podudaranja dva uzorka. Ovde samo u određenim slučajevima može doći do napada. Ovde se ogleda i jedna od prednosti multimodalnih sistema u odnosu na unimodalne sisteme, jer kod fuzije imamo više biometrijskih karakteristika, pa teško da će sve biti izložene napadu.

9. Odluka – u ovoj fazi rada sistema operator može da bude uzrok greške.

Biometrijski uzorak nosi najvažnije biometrijske podatke pa se iz tog razloga javlja zabrinutost, kako na polju prava na privatnost, tako i u pogledu bezbednosti sistema. Osnovna zabrinutost je mogućnost krađe identiteta. Navedene slabosti mogu biti prevaziđene primenom različitih organizacionih

mera, kao što je nadzor prilikom upisa i verifikacija rada, detekcija u realnom okruženju, kriptografsko skladištenje i zaštićeni transport. Ove protivmere se razlikuju prema trajanju, troškovima i ekonomičnosti.

Kako bi se umanjio značaj i efekti opisanih slabosti, mora se stalno raditi na usavršavanju biometrijskih sistema, kao što je biometrijsko šifrovanje, razvoj opozive biometrije ili de-identifikacije slike.[125]

Kod biometrijskog šifrovanja se nastoji koristiti biometrijski uzorak kao ključ za obavljanje kriptografskog protokola. Biometrijski uzorak bi bio vezan za tajni ključ koji bi bio dizajniran tako da se može koristiti samo za upisanog pojedinca.[126] Problem ovog šifrovanja je varijabilnost biometrijske slike između merenja, što znači da se biometrijska slika ne može predstaviti kao *kod* jer se menja sa svakom prezentacijom. Opoziva biometrija je kodirana šema koja zavisi od svake aplikacije. Jedan od načina na koji se takođe mogu prevazići ove slabosti je standardizacija. [127]

Standardi u biometriji imaju veoma važnu ulogu jer omogućavaju lakšu razmenu biometrijskih podataka između aplikacija i biometrijskog sistema. Postavljaju ih proizvođači biometrijskih proizvoda, krajnji korisnici i distributeri i mogu biti *de facto* standardi. Da bi se standard primenjivao mora da bude javno objavljen. Ovi standardi nisu obavezni već se primenjuju na dobrovoljnoj bazi. Veoma je važno međusobno usklađivanje standarda, jer na taj način proizvodi postaju dostupniji korisnicima, a proizvođačima se nameće potreba da stalno rade na poboljšanju proizvoda, kako bi ostali u tržišnoj "igri".

5.4. Implementacije biometrijskih sistema identifikacije

Šira upotreba automatizovanih biometrijskih sistema identifikacije prvo je našla svoju primenu u kriminalistici, za potrebe brzog pretraživanja baza kriminalističkih dosijea i upoređivanje tragova sa mesta zločina. U protekloj deceniji, pojavljuje se primena i u potvrdi identiteta autorizovanih učesnika u

[125] A.Adler, *Biometric System Security,* Handbook of biometrics, Springer (2008), str. 399.
[126] *Ibid*. str. 395.
[127] *Ibid*. str. 393.

krupnim ekonomskim transakcijama. Za identifikaciju zaposlenih ovaj koncept danas koristi jedan broj kompanija i organizacija, pogotovu prilikom korišćenja servisa koji zahtevaju stroga ovlašćenja (dobar primer su vojne institucije).

Pritisak kompanija koje proizvode biometrijske sisteme identifikacije u ogromnoj meri utiče i na političke strukture koje odlučuju o sprovođenju ovakvih mera na nacionalnom nivou. Ove kompanije u svojim prognozama očekuju veliki obrt kapitala u godinama koje dolaze, što je povratni impuls političkim strukturama, koje mnoge stvari mere novcem, često ne razmišljajući o drugoj strani medalje.

Brojni su akademski građani i svetski priznati stručnjaci iz oblasti informacionih tehnologija koji se protive korišćenju biometrijskih sistema identifikacije u obavezujućoj formi na nivou država i nadnacionalnih tela. Suštinski problem leži u činjenici da su zastupnici široke primene biometrijskih sistema ljudi sa direktnim finansijskim interesom ili pak političari koji žele da prošire moć državnog aparata nad građanima.

Danas su biometrijski sistemi za identifikaciju po svojoj veličini sve manji, precizniji, pouzdaniji, brži, finansijski dostupniji i nalaze sve širu primenu u slučajevima kada je neophodno nedvosmisleno utvrditi ili potvrditi identitet osobe. Sistemi poslednje generacije, oni najsavremeniji, mogu pružiti identifikaciju trodimenzionalnog modela lica, prepoznavanje rasporeda vena, analizu DNK strukture, detekciju mirisa i specifičnih hemijskih svojstava kože svakog čoveka. U poređenju sa starijim metodima identifikacije, biometrijska identifikacija se smatra sofisticiranim metodom identifikacije. Ovi sistemi su precizniji, brži i pogodniji za korišćenje, imaju manje troškove administracije, jeftiniji su za sprovođenje i upravljanje, i imaju viši nivo sigurnosti od tradicionalnih.

Biometrijski sistemi su postali presudni faktor u postizanju visoke pouzdanosti prilikom utvrđivanja identiteta. Biometrijski sistemi za utvrđivanje identiteta se danas koriste u sledećim oblastima:

1. *Fizički pristup* – za kontrolu pristupa sigurnosnim (zaštićenim) lokacijama (prostorijama ili zgradama). Nasuprot kontroli pristupa zasnovanoj na karticama koje se moraju proveravati i verifikovati posredstvom stražara, biometrija omogućava i dozvoljava kontrolu ulaska bez prisustva ljudi (obezbeđenja).
2. *Virtuelni pristup* – reč je primeni biometrije za kontrolu pristupa računarima, povezanim u mrežu. Fizičko zaključavanje može zaštiti hardver, a lozinke koje su trenutno najpopularniji način zaštite podataka u mreži, nisu i dovoljno pouzdane. Danas su u ovoj oblasti sve više prisutni sistemi zasnovani na identifikaciji preko otiska, fotografije lica i glasa.
3. *Aplikacije elektronske trgovine* – Elektronsko poslovanje je praktično nezamislivo bez pouzdanih metoda za proveru identiteta potencijalnog kupca, vlasnika odgovarajućeg računa. Sada se koriste biometrijski sistemi za zamenu običnih čitača kartica na POS (engl. *point-of-sales*) terminalima. U Srbiji je se trenutno u bankama i drugim organima državne uprave koriste čitači elektronski identifikacionih kartica na osnovu čega se pouzdano utvrđuje identitet korisnika.
4. *E-vlada* - Elektronska vlada (engl. *e-government*), po konceptu i realizaciji, je elektronski servis koji omogućava građanima obavljanje različitih upravnih poslova (poslova u vezi državljanstva, prijave i odjave boravišta, putnih isprava, produženja vozačke dozvole, registracije motornih vozila...) elektronskim putem. Te poslove građani tradicionalno obavljaju na šalterima što, po pravilu, oduzima puno vremena. Mnoge vlade u svetu gledaju na servise *e-vlade*, kao na način poboljšanje poslovanja sa stanovništvom. Pravilno uveden, informaciono-komunikacioni sistem e-vlade koristi svim učesnicima, jer s jedne strane organi državne uprave skraćuju vreme obrade dokumenata, dok s druge strane stanovništvo takođe štedi vreme, jer se elektronske transakcije mogu obaviti nezavisno od radnog vremena datih organa i njihovog mesta. Elektronska vlada, u suštini znači, da sada podaci "putuju" umesto građana.

5. *Zdravstvena zaštita i osiguranje* **-** U okviru zdravstvenog sektora biometrijski sistemi mogu biti primenjeni u oblasti zdravstvenog osiguranja i oblasti zdravstvene zaštite (zdravstveni kartoni i profesionalne kartice zaposlenih). U oba slučaja, značajno se unapređuje poslovanje, većom raspoloživošću i pokretljivošću podataka uz visok nivo njihove zaštite i strogo utvrđenu hijerarhiju pristupa ličnim i poverljivim podacima. Zdravstvene kartice zasnovane na *smart* karticama donose korist, kako sistemu zdravstvene zaštite jedne zemlje, tako i samim pacijentima. Primena elektronskih zdravstvenih kartona utiče na sniženje troškova smanjenjem broja nepotrebnih ispitivanja i testiranja pacijenata.
6. *Skriveno nadgledanje* – Jedna od najizazovnijih oblasti istraživanja jeste korišćenje biometrije za tajno nadgledanje. Korišćenjem tehnologija za prepoznavanje lica i tela, istraživači se nadaju da će uz pomoć biometrije automatski identifikovati poznatog osumnjičenog pri ulasku u zgradu ili prilikom prolaska kroz neku sigurnosnu oblast (na primer, aerodrom).

Biometrijski sistemi identifikacije u našoj zemlji koriste pojedini organi državne uprave i institucija, banke, privatne firme i mnogi objekti u kojima je neophodna identifikacija zaposlenih. Može se reći da je masovna upotreba biometrije i biometrijskog sistema identifikacije u Srbiji, počela uvođenjem multimedijalnih komunikacija, odnosno implementacijom *smart* kartica, biometrijskih ličnih karata i biometrijskih putnih isprava. Primena Interneta, multimedijalnih komunikacija i intraneta predstavlja potpunu modernizaciju i automatizaciju sadašnjeg sistema i procesa rada organa državne uprave. U Srbiji od 2009. godine efikasno funkcioniše informacioni sistem digitalnog prikupljanja, odnosno akvizicije identifikacionih podataka (alfanumeričkih i biometrijskih: fotografije lica, otiska prstiju, potpisa i dr.), obrade navedenih podataka, njihove integracije sa postojećim bazama podataka, formiranja novih baza podataka.

Iako se biometrijska identifikacija svakodnevno usavršava i sve više implementira u različite sisteme, postoji razlika u primeni biometrijskih sistema za utvrđivanje identiteta, kako sa stanovišta korisnika, tako i sa stanovišta sistema u koji se ugrađuju.

Sa korisničkog stanovišta važno je da takav sistem što manje ometa korisnika u izvršavanju pojedinih aktivnosti u postupku utvrđivanja identiteta. Takođe, za korisnika je veoma važno koliko dobro radi takav sistem identifikacije i koliki su troškovi nabavke i održavanja. Prilikom svakog korišćenja, odnosno implementacije ovakvih sistema veoma je važno doneti adekvatne odluke u odnosu na faktore ograničenja, kako bi se dobio funkcionalan i optimalan sistem za utvrđivanje identiteta. Na primer, prilikom korišćenja biometrijske metode geometrija lica korisnik ne ulaže puno napora kako bi se identifikovao (čak se može uraditi i identifikacija, a da to lice nije svesno), ali u tom slučaju preciznost sistema nije visoka. Sa druge strane, skeniranje i prepoznavanje mrežnjače je veoma pouzdano i precizno, ali može stvoriti neprijatan osećaj kod lica za koje se vrši verifikacija ili identifikacija. Pored toga korišćenje ovakvih sistema iziskuje i veće finansijske troškove.

5.5. Biometrijski sistemi i pitanja privatnosti

Privatnost tumačimo kao bitno određenje slobode, pravo i mogućnost da sami određujemo da li će, i pod kojim uslovima, ono što smatramo samo svojim biti dostupno i drugima. Imajući ovo u vidu, kao i činjenicu da su biometrijski podaci po definiciji deo našeg bića ili da suštinski opisuju naš odnos sa okruženjem, biometrijske sisteme identifikacije prevashodno treba proučavati u kontekstu njihovih društvenih implikacija, a ne samo kroz pitanja tehničke izvodljivosti i primenljivosti. To podrazumeva multidisciplinaran pristup koji pre svega obuhvata etičke, informatičke, pravne i sociološke discipline. Svaki redukcionizam i svođenje ove problematike na samo jedan od navedenih aspekata ne donosi dobre rezultate i vodi ka zaključcima koji mogu biti pogrešni i koji mogu imati dalekosežne posledice. Najveći problem je u

tome što se biometrijski podaci, kada su u pitanju javne računarske mreže, mogu upotrebiti i kada stvarni vlasnik nije fizički prisutan i tako biti zloupotrebljeni. Jednom kompromitovan biometrijski sistem ne može se izmeniti. Ovo je manje izražen problem kod zatvorenih mreža ili pojedinačnih sistema, ali kada se koristi Internet u procesu identifikacije, problem postaje izuzetno ozbiljan. Industrija koja se bavi biometrijskim metodama preporučuje standardan set principa za očuvanje privatnosti. To je obavezno šifrovanje biometrijskih podataka, pre bilo kakvog slanja, i stroga kontrola distribucije podataka.

U dostupnoj literaturi može se uočiti posmatranje problema privatnosti u tri različita konteksta: fizička privatnost, privatnost prilikom odlučivanja i privatnost u pogledu informacija. Fizička privatnost podrazumeva pravo građaninina da ne bude nadgledan tokom boravka na nekom mestu ili praćen tokom kretanja. Privatnost u pogledu odlučivanja podrazumeva slobodu građanina pri donošenju odluka. Privatnost u pogledu informacija podrazumeva slobodu građanina da ograniče pristup određenim ličnim podacima. Upravo navedeni konteksti privatnosti postaju problemi kada je reč o biometriji.[128]

Biometrijski podaci predstavljaju specifičnu kategoriju ličnih podataka te iz tog razloga mogu biti korišćeni samo za specifične, jasne i zakonom definisane svrhe uz primenu adekvatnih mera zaštite.

Zabrinutost građana je opravdana jer biometrijski podaci prikupljeni od strane sistema mogu biti povezani sa drugim podacima o ličnosti, što omogućava, na primer, neovlašćeno praćenje kretanja osobe. Ova tehnologija može da poveže osobu sa biometrijskim uzorkom i bilo kojim identifikacionim podatkom i ličnim atributom samo u vreme unosa u sistem i to garantuje autentifikaciju kada ni jedan drugi link nije moguć između biometrijskog podatka i informacije o ličnosti. Ukoliko ni jedna druga informacija o licu ne bi

[128] S Hoffman, Biometrics, *Retinal Scanning, and the Right to Privacy in the 21st Century*, Syracuse Science & Technology Law Reporter, Vo. 22, Article 2, (2010), str. 38.

bila sačuvana u vreme procesa unosa biometrijskih podataka, moglo bi se postaviti pitanje da li se uopšte radi o toj osobi koja je dala na uvid svoje biometrijske podatke. Konvencija 108 Saveta Evrope smatra da povezanost biometrije sa bilo kojom informacijom iz baze podataka jeste lični podatak. Analizom problema prava na privatnost u biometrijskim sistemima uočeno je da se treba imati u vidu sledeće aspekte neželjenih veza: [129]

1) Biometrijske karakteristike su i biološke karakteristike, pa se na osnovu biometrijskih podataka mogu dobiti dodatne informacije, na primer medicinske, koje se mogu iskoristiti za diskriminaciju pojedinca ili grupa. Slika irisa bi se mogla koristiti za dodatnu analizu u medicini, pa bi baza irisa bila od velikog značaja osiguravajućim društvima prilikom donošenja odluke o sklapanju ugovornih obaveza i određivanju iznosa premija.
2) U nekim slučajevima može doći do neželjene identifikacije, na primer, u slučajevima kada osoba zbog bezbednosti koristi drugi identitet (u postupku zaštite lica promena identiteta je jedna od korišćenih mera). Takođe, marketinške firme sa dodatnim ukrštanjem podataka koji se odnose za ponašanje, navike i sklonosti pojedinca, a koje dobijaju iz više različitih izvora ili aplikacija, mogu ostvariti veliku dobit, a u saradnji sa drugim subjektima društva, manipulacijom medija i veliku moć nad društvom.
3) Biometrijske karakteristike građanina jesu lične, ali današnja tehnologija omogućava njihovu dostupnost i bez saglasnosti građana, pa se u tom slučaju osobi uskraćuje pravo na privatnost i anonimnost.

Razvijeno je nekoliko metoda za ocenu povrede prava na privatnost korišćenjem biometrijskih sistema. Kako bi se ovaj problem bolje upoznao, *IBG* grupa je predložila pitanja kojima pomažu u sagledavanju rizika ugrožavanja privatnosti:[130]

---

[129] Marek Rejman-Greene, *Privacy Issues in the Application of Biometrics: a European Perspective*, Biometric Systems, (2005), str. 335-359.

[130] Terrance E. Boult and Robert Woodworth, *Privacy and Security Enhancements in Biometrics,* Advances in Biometrics, Springer-Verlag London Limited (2008).

- Da li je biometrijski sistem tajni ili otvoreni?
- Da li je sistem opcioni ili obavezan?
- Da li se koristi za verifikaciju ili identifikaciju?
- Da li je sistem razvijen za određeni period ili period nije definisan?
- Da li je razvijen u privatnom ili javnom sektoru?
- Ko poseduje biometrijske podatke? Ko je vlasnik, institucija ili ...?
- Koji tip biometrijske tehnologije se koristi, informacije o fizičkim karakteristikama osobe ili o njenom ponašanju?
- Gde su pohranjeni biometrijski podaci? Lično skladište ili zajednička baza podataka?
- Da li sistem koristi biometrijske templejte, biometrijske slike ili oba vida?

Na primer, u pogledu ugroženosti prava na privatnost manje je rizičan otvoreni verifikacioni sistem sa karticama, nego prikriveni identifikacioni sistem sa centralizovanim bazama podataka. Izveštaj sa „*RISE*"-ove konferencije sadrži nekoliko glavnih zaključaka izvedenih tokom same rasprave:[131]

- Treba da postoje jasna i proverljiva ograničenja oko upotrebe biometrije u okviru određenog sistema,
- Biometrijske aplikacije velikog obima treba da budu registrovane, overene i nadzirane,
- Vlasnici/operateri moraju da imaju otvoren i transparentan mehanizam za sprovođenje sistema „kočnica i ravnoteža" nad velikim biometrijskim sistemima.

Kako bi se zaštitilo pravo na privatnost, sa jedne strane, a sa druge strane omogućila sigurnost rada sistema identifikacije i verifikacije, potrebno je rukovoditi se, između ostalog, sledećim principima:[132]

- Okruženje treba da bude otvoreno umesto prikriveno,

---

[131] S.Brajušković, *Biometrijska identifikacija i pravo na privatnost*, jun (2011).
[132] Anil K. Jain, Flynn, A. A. Ross, Eds., *Handbook of Biometrics*, (*The Law and the Use of Biometrics*), Springer, (2008), str. 358-359.

- Poželjno je koristiti proces verifikacije umesto identifikacije,
- Sistem treba da koristi lokalno skladištenje umesto centralizovane baze podataka,
- Poželjno je da sistem dobrovoljan, a ne obavezan,
- Proces upoređivanja treba da bude baziran na uzorcima, odnosno na izvedenim podacima, umesto na originalnim artefaktima, na primer, sačuvanim slikama,
- Sistem treba da je dobro zaštićen od zloupotreba.

U literaturi se može naći stav da primena navedenih smernica i odgovorno korišćenje biometrijskih sistema u praksi može da zaštiti privatnost pojedinca. Zaštita biometrijskih podataka počinje u trenutku kada se od lica uzimaju podaci i za zaštitu biometrijskih dokumenata najodgovornija je sama država. Preporučuje se svakoj državi uspostavljanje nadzornog tela koje će nadzirati zaštitu biometrijskih baza, kao nezavisnog, samostalnog organa.

Upotreba biometrijskih sistema posmatrano sa stanovišta bezbednosti društva stvara mogućnosti koje ohrabruju građane, ali sa druge strane njihova primena može da povredi prava građana na privatnost i da podigne ozbiljnu zabrinutost u društvu. Dakle, prilikom korišćenja ovakvih sistema treba voditi računa o pravilu proporcionalnosti u odnosu na ishod. Nivo upotrebe biometrijskih sistema i opasnost od njihove moguće zloupotrebe moraju biti u proporcionalnom odnosu, odnosno takvom odnosu da šteta ne bude veća od koristi.

Dakle, sa sigurnošću možemo zaključiti da su nove informacione i komunikacione tehnologije, u sprezi sa biometrijskim tehnologijama, pored brojnih koristi, donele i nove društvene izazove, od kojih treba posebno naglasiti one koji se odnose na pitanje zaštite privatnosti građana, kao suštinskog atributa slobode. Navedeni problem zaštite privatnosti još više dobija na složenosti, ako se ima u vidu brzina primena novih tehnologija, na primer eksponencijalan rad broja Internet korisnika. Sa druge strane, društveni aparat koji treba da pravno reguliše ovu materiju, da formuliše odgovarajući

zakonski okvir za korišćenje novih informacionih tehnologija, pokazuje odgovarajuće kašnjenje, jer za ozbiljnu raspravu je potreban odgovarajući vremenski interval kako bi se izbegle brzoplete odluke i valjano sagledali svi elementi velikog društvenog izazova i nimalo jednostavnog zadatka, budući da je neophodno u informatičkoj eri uspostaviti ravnotežu između slobodnog protoka podataka i zaštite privatnosti građana.

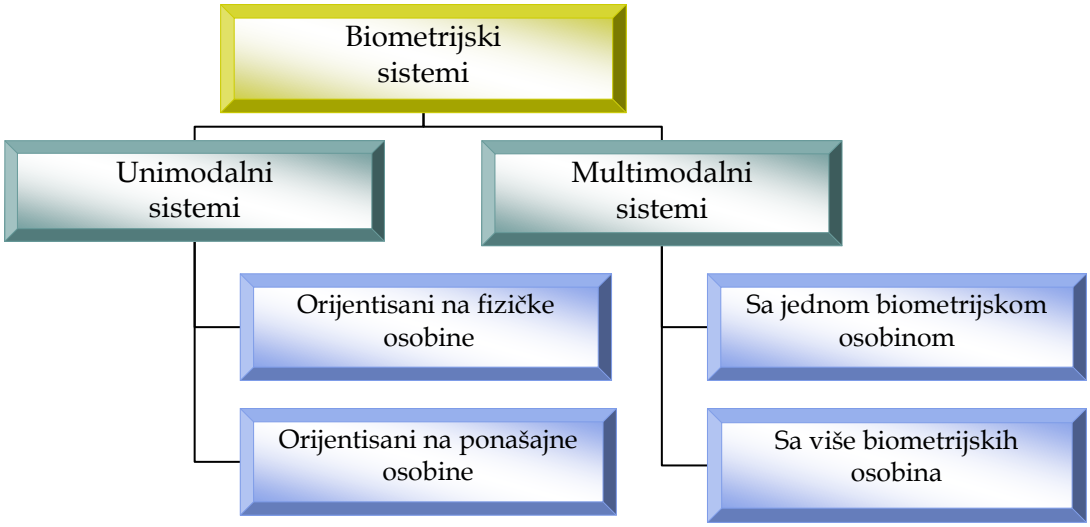
Takođe, jasno je da se posao pravnog uređenja ove problematike ne može svesti na jednokratan zadatak. Biometrijski sistemi se neprekidno tehnološki unapređuju i usavršavaju, te je potrebno u kontinuitetu pratiti postojeću pravnu regulativu u toj oblasti i po potrebi je menjati i dopunjavati, kako bi se obezbedila sigurnost prikupljenih podataka i ostvarila potrebna zaštita prava na privatnost.

5.6. Klasifikacija biometrijskih sistema identifikacije

U savremenom svetu, svetu koji je u svakom trenutku karakterisan ogromnim protocima informacija u računarsko-komunikacionim mrežama, ali i svetu u kojem zbog supremacije jedne supersile nema velikih ratova, ali zato postoji novi vid gerilskog ratovanja poznat pod nazivom međunarodni terorizam, kao i svet u kojem zbog procesa globalizacije organizovani kriminal postaje sve jači, jer više ne poznaje granice, sve više se javlja potreba za novim mehanizmima bezbednosti. Kako se od ovih vidova opasnosti državni aparati ne mogu uspešno boriti tradicionalnim odbrambenim mehanizmima, pokazalo se da uvođenje biometrijskih sistema predstavlja dobar vid bezbednosne preventive i od takvih sistema se očekuje da na vreme prepoznaju, lociraju i prate izvore bezbedonosnih pretnji. Korišćenje biometrijskih sistema je postalo presudni faktor kojim državni organi postižu najveći mogući stepen tačnosti prilikom provere i utvrđivanja identiteta lica, a time i podizanja nivoa društvene bezbednosti. Pokazali smo da se biometrijski sistemi za utvrđivanje identiteta zasnivaju na tehnologijama koje analiziraju fizičke karakteristike ljudi ili karakteristike njihovog ponašanja, i to može biti i osnov klasifikacije

biometrijskih sistema. Međutim, biometrijski sistemi se mogu klasifikovati na više načina. U ovom poglavlju ćemo kao osnov za klasifikaciju uzeti broj načina, *modova*, na koji se biometrijski uzorci za jednu osobu čuvaju u bazi podataka, pa ćemo biometrijske sisteme za utvrđivanje identiteta podeliti na sisteme koji za identifikaciju koriste samo jedan način zapisa biometrijskog uzorka po osobi – *unimodalni biometrijski sistemi*, i na sisteme koji koriste više načina zapisa biometrijskih uzoraka po osobi – *multimodalni biometrijski sistemi*.

Na slici 13 je data klasifikacija biometrijskih sistema prema uzorcima u bazi podataka.



Slika 13 Klasifikacija biometrijskih sistema prema uzorcima u bazi podataka

Unimodalne biometrijske sisteme ćemo dalje podeliti prema izvoru biometrijskog podatka na unimodalne biometrijske sisteme orijentisane na *fizičke* osobine osoba i na unimodalne biometrijske sisteme orijentisane na *ponašajne* osobine osoba.

Multimodalne biometrijske sistemi dalje ćemo prema broju izvornih biometrijskih osobina koje se za svaku osobu u procesu akvizicije prevode u računarski čitljiv oblik zapisa u bazi uzoraka, podeliti na multimodalne

biometrijske sisteme sa samo jednom biometrijskom osobinom i na multimodalne biometrijske sisteme sa više biometrijskih osobina.

U slučaju multimodalnih biometrijskih sistema formiranih na osnovu samo jedne biometrijske osobine do većeg broja uzoraka u bazi podataka, *modova*, za svaku osobu se može doći na više načine:

- koristi se veći broj tehnološki različitih ulaznih senzora za *ponovljeno* snimanje u kratkom vremenskom intervalu jedne biometrijske osobine, pa sledstveno tome i do većeg broja uzoraka u bazi karakteristika. Na primer, otisak istog prsta se uzima uz pomoć kapacitivnog i optičkog skenera, pa će *isti* algoritam za izdvajanje biometrijskih karakteristika u opštem slučaju generisati *različite* skupove podataka,
- koristi se tehnološki isti ulazni senzor za *ponovljeno* snimanje jedne biometrijske osobine u dužim vremenskim intervalima, pa sledstveno tome i do većeg broja uzoraka u bazi karakteristika (princip vremenskog odabiranja izvora podataka, engl. *sampling*). Na primer, isto lice snimljeno u *en face* poziciji fotoaparatom u razmacima od po šest meseci generisaće primenom *istog* algoritma za izdvajanje karakteristika različite setove podataka kao uzorke,
- koristi se isti tehnološki ulazni senzor za *ponovljeno* snimanje jedne biometrijske osobine u kratkom vremenskom intervalu, ali sa prostorno različitih delova tela iste osobe (princip prostornog odabiranja izvora podataka). Navedimo dva primera, prvi je snimanje otisaka dva odabrana prsta uz pomoć kapacitivnog skenera, a drugi je snimanje lica iste osobe fotoaparatom u pozicijama *en face* i poluprofila. U oba slučaja, algoritmi za izdvajanje biometrijskih karakteristika generisaće *različite* skupove podataka,
- koristi se ulazni senzor za snimak jedne biometrijske osobine, ali se primenjuju *različiti* algoritmi za izvođenje biometrijskih karakteristika. Na primer, na osnovu iste fotografije lice različiti algoritmi za izdvajanje biometrijskih karakteristika generisaće različite setove podataka.

Multimodalni biometrijski sistemi formirani na osnovu više biometrijskih osobina predstavljaju opšti slučaj biometrijskog sistema u kojem se svaka obuhvaćena biometrijska osobina osobe u bazi uzoraka opisuje bar sa jednim od gore navedenih modova.

U literaturi se može naći više načina klasifikacije sistema. Na primer, biometrijski sistem je multibiometrijski hibridni sistem, ako korišćeni modovi se predstavljaju kombinaciju fizičkih *i* ponašajnih osobina čoveka. Na primer, *Brunelli* i ostali su analizirali kombinaciju algoritama prepoznavanja lica i algoritama prepoznavanja govora. Postoje dve vrste ovih sistema, jedni sistemi koji koriste kombinaciju multialgoritama i multiuzoraka, dok drugi koriste kombinaciju biometrijskih identifikatora, kao što je otisak prsta sa drugim osobinama, na primer, sa polom, visinom, bojom očiju.[133]

Pored unimodalnih biometrijskih sistema, koji već imaju svoju praktičnu primenu, poslednjih godina se razvijaju biometrijski sistemi koji u svom radu koriste više biometrijskih osobina za utvrđivanje identiteta. Primenom multimodalnih biometrijskih sistema prevazilaze se nedostaci i ograničenja koje susrećemo kod unimodalnih biometrijskih sistema. Ovakvi sistemi sa stanovišta korisnika su fleksibilniji, imaju veći stepen preciznosti i pouzdanosti prilikom utvrđivanja identiteta. Posebnu pažnju biometrijskim sistemima, koji u postupku identifikacije ili verifikacije neke osobe koriste više nezavisnih merenja jedne ili više fizičkih osobina, anatomskih ili fizioloških, posvetićemo u sedmom i osmom poglavlju ovog rada. Međutim, prvo ćemo se upoznati sa detaljima rada unimodalnih biometrijskih sistema, upravo imajući u vidu da se biometrijski sistemi sa više podataka o nekoj osobi mogu posmatrati kao nadgradnja postojećih jednostavnijih biometrijskih sistema za utvrđivanje identiteta na osnovu jedne biometrijske osobine.

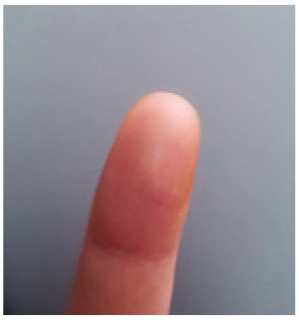
[133] A. Ross, *An introduction to multibiometrics*, West Virginia University, Morgantown, WV 26506 USA, (2007).

6. BIOMETRIJSKI SISTEMI ZA UTVRĐIVANJE IDENTITETA NA OSNOVU JEDNE BIOMETRIJSKE OSOBINE

6.1. Biometrijski sistemi identifikacije sa otiskom prsta

6.1.1. Razvoj sistema identifikacije na osnovu otiska prsta

Metoda prepoznavanja pomoću otiska prsta spada u metode prepoznavanja na osnovu fizičkih osobina. Sa fizičkog aspekta otisak prsta predstavlja konfiguraciju ispupčenja i udubljenja.[134] Linije koje formiraju ispupčenja nazivaju se papilarne linije i nalaze se na jagodici prsta, slika 14.



a) Jagodica prsta

b) Otisak prsta

Slika 14 Jagodica prsta i njen otisak

Anatomske karakteristike papilarnih linija su minucije, koje predstavljaju skup svih detalja koji se odnose na razne oblike pojavljivanja papilarnih linija. Za uspešnu identifikaciju je potrebno da se utvrdi određen broj minucija. Zahvaljujući njima otisak prsta predstavlja veoma atraktivan biometrijski identifikator na osnovu koga se može identifikovati svaki pojedinac. Danas je ova biometrijska metoda jedna od najrasprostranjenijih i najprihvaćenijih metoda u svetu koja se koristi u sistemima za identifikaciju.[135] U praćenju razvoja ovog tipa metode biometrijske identifikacije, na osnovu crteža papilarnih linija, prema dosadašnjim rezultatima istraživanja razlikujemo tri

[134] D. Maltoni, R. Cappelli, Fingerprint Recognition, *Handbook of Biometric* (eds. A.K.Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 23-43.
[135] *Fingerprint Recognition, available on,* http://www.biometrics.gov/Documents/FingerprintRec.pdf#page=1, pristupljeno 19.04.2012.

perioda: praistorijski, empirijski i naučni.[136] Čitav niz arheoloških istraživanja svedoči o tome da je postojanje papilarnih linija na prstima bilo zapaženo još u *praistorijskom periodu* u kome su otisci imali prevashodno umetnički značaj.

Kada pominjemo empirijsko doba, u istoriji starih zapadnih civilizacija nema pomena o korišćenju otisaka u druge svrhe osim u vidu ukrasa na grnčarijama. U isto vreme istočni i dalekoistočni narodi su koristili otiske papilarnih linija u različite svrhe. Tako se na glinenim pločicama Asiraca mogu naći otisci noktiju korišćeni u svrhu potpisa. U Rusiji, još u najstarije vreme, otisci prstiju korišćeni su kao znak za overavanje akata i ugovora. Istočni narodi i dan-danas umesto potpisa ili pečata upotrebljavaju otiske prstiju ili dlanova ruku umrljanih čađu ili mastilom.

Prvi naučni rad posvećen papilarnim linijama pripada italijanskom anatomu Marčelu Malpiđiju i datira iz XVII veka. Malpiđi je izučio sastav papila i pora, a uočio je postojanje kružnih i petljastih oblika papilarnih linija. U znak poštovanja prema njegovom delu najniži sloj epiderma nazvan je *Malpiđijev sloj*. Treba naglasiti da Malpiđi u svojim radovima nije razmatrao mogućnost identifikacije ljudi na osnovu crteža papilarnih linija.

Ivan Evanđelista Purkinje, češki lekar i anatom, objavio je 1823. godine rad iz oblasti anatomske analize papilarnih linija *Comentarii de examine phisiologico organi visus et sistematis cultanei*. U svom radu on je izvršio klasifikaciju papilarnih linija na devet vrsta. Međutim, njegovo bavljenje ovom problematikom završeno je sa tim radom, tako da ni on nije shvatio važnost papilarnih linija za raspoznavanje ljudi. Pa ipak, Malpiđi i Purkinje su bili pioniri koji su sa naučnog stanovišta proučavali papilarne linije, tako da ih je poznati francuski kriminalista Edmund Lokar nazvao tvorcima daktiloskopije. Pravi razvoj identifikacije ljudi na osnovu papilarnih linija započeo je radovima engleskih istraživača sredinom i krajem XIX veka. Po uverenju većine

[136] Z. Skakavac, M. Milivojević, *Neki teorijsko-istorijski i empirijski aspekti tragova papilarnih linija,* zbornik „Kriminalističko forenzička istraživanja“, Internacionalna Asocijacija Kriminalista, Banja Luka, (2011), str. 104-117.

istraživača, najznačajniji doprinos razvoju metoda registracije i identifikacije na osnovu crteža papilarnih linija pružio je Englez Viljem Heršel. Heršel bio administrator jednog okruga u današnjem Bangladešu i zbog velikog broja nepismenih žitelja, pri sklapanju ugovornih obaveza sa stanovništvom od 1858. godine počeo je da koristi otiske prstiju umesto dotadašnjih oznaka za nepismene u obliku krstića. To je u praksi dovodilo do mnogobrojnih nesporazuma i sukoba. Ubrzo su se pokazale prednosti ovog načina overe, jer su prevare praktično iskorenjene. Podstaknut (motivisan) ovim uspesima, Heršel je organizovao prikupljanje i proučavanje otisaka prstiju. Na osnovu toga je 1877. godine predložio da se u zatvorima Indije uzimanje otisaka prstiju uvede kao obavezno sredstvo identifikacije, ali taj predlog nije prihvaćen. Kada je oktobra 1880. godine u londonskom časopisu *Priroda* (engl. *The Nature*) pročitao članak škotskog lekara Henrija Fuldsa o identifikaciji lica na osnovu papilarnih linija, Heršel je odmah objavio članak o svojim istraživanjima na tom polju. Smatra se da je Heršel detaljnije izučavao otiske papilarnih linija i to pre Fuldsa.

Ipak, najznačajniji rad iz ove oblasti pripada Frensisu Galtonu, koji je na osnovu radova Heršela preduzeo opsežna naučna istraživanja o prirodi papilarnih linija, kako sa biološkog, tako i sa kriminalističkog stanovišta. Rezultate svojih istraživanja Galton je publikovao 1891. godine u pomenutom časopisu *Priroda,* a 1892. godine objavio je i knjigu pod naslovom *Otisci prstiju* (engl. *Fingerprints*). Bez obzira na činjenicu što nije u potpunosti razradio sistem klasifikacije papilarnih linija, nesporno je da je prvi u svetu naučno obradio papilarne linije i postavio temelj za razradu metode klasifikacije. Na osnovu njegovog naučnog ugleda, otisci papilarnih linija od tada počinju ozbiljnije da se proučavaju.

Do primene otisaka prstiju u engleskoj policiji došlo je tek kada je Edvard Henri, koji je bio prijatelj i saradnik Heršela, 1899. godine razradio, a 1900. godine objavio svoj sistem klasifikacije otisaka prstiju. Henri je 1901. godine postavljen za načelnika odeljenja za identifikaciju u Skotland Jard– u. Pomenuti

sistem klasifikacije je nazvan Galton-Henrijev, a sama metoda je nazvana identifikacija na osnovu otisaka prstiju. Ubrzo je ova metoda prihvaćena i u drugim evropskim zemljama. Tako je u Austro-Ugarskoj uvedena 1903. godine, u Nemačkoj 1907, a u Beogradu 1911. godine. Interesantno je napomenuti da je poslednja u Evropi ovu metodu uvela Francuska, 1914. godine, zbog toga što se poznati francuski kriminalista Alfons Bertijon, tvorac antropometrijske metode, tome protivio do kraja svog života!

Međutim, Engleska nije prva zemlja u kojoj je metoda otisaka prstiju zvanično uvedena u policijsku praksu, već ta čast pripada Argentini i našem Ivanu Vučetiću, koji je sa roditeljima 1884. godine emigrirao iz Dalmacije u sastavu tadašnje Austro-Ugarske u Argentinu, a. Ivan Vučetić je bio zaposlen u upravi policije grada Buenos Ajresa sa zadatkom da organizuje kriminalističku registraciju lica. Na osnovu novinskih informacija o Galtonovim istraživanjima, Vučetić je 1891. godine razvio sopstvenu metodu identifikacije osoba na osnovu otisaka prstiju. Do kraja te godine registrovao je čak 600 lica. Interesantno je da je Vučetić potpuno samostalno došao do osnovne klasifikacije na četiri tipa crteža papilarnih linija lukove, leve petlje, desne petlje i kružne uzorake, kao i Frensis Galton, koji je koristio iskustvo istočnih naroda i rad Purkinjea. Sa porastom zbirke otisaka bio je prinuđen da produbi klasifikaciju. Opredelio se za brojanje papilarnih linija što je još jedna slučajna podudarnost sa metodom usvojenom u Evropi.

Prva identifikacija izvršena na osnovu tragova papilarnih linija, obavljena je već 1892. godine u toku rasvetljavanja dvostrukog ubistva dece u varošici Nekoeho, na obali Atlanskog okeana. Tako je dokazano da je jedna žena ubila svoju vanbračnu decu da bi se udala za čoveka kog je volela. I pored toga, 1893. godine Vučetiću je zabranjen dalji rad na otiscima prstiju, da bi već 1894. godine preimućstva ove metode bila toliko očigledna da je metoda identifikacije tada priznata i u Argentini i uvedena kao zvanična metoda za registraciju i identifikaciju lica. Iste godine Vučetić je objavio rezultate svojih istraživanja u knjizi *Daktiloskopija,* a 1904. godine je izdao knjigu *Uporedna*

daktiloskopija (španski *Dactiloskopia Comparada*) u kojoj je izložio svoja dotadašnja otkrića.

Vučetić je ovu metodu nazvao "inkofalangometrija", verovatno zbog sličnosti sa izrazom antropometrija. 1894. godine jedan novinar, u svome članku, zapitao se zašto se ova metoda ne bi zvala *daktiloskopija* pošto reč daktilos- znači prst, a *skopein* – posmatranje. Od tada se naziv *daktiloskopija* koristi u svim zemljama u kojima je u upotrebi Vučetićev sistem, a to su zemlje Južne Amerike, a u Evropi - Španija, Francuska i ondašnja Kraljevina Jugoslavija. Kasnije je kao univerzalna reč prihvaćena u svim jezicima.

Osnovne karakteristike papilarnih linija su:[137]

a) *Postojanost,* što obezbeđuje trajnost crteža

Papilarne linije su kod ljudi nepromenljive u pogledu oblika i karakteristika. Do promene može doći samo izuzetno i to u slučaju povreda u vidu dubokih opekotina ili posekotina. Posledica tih povreda je promena crteža papilarnih linija, ali samo na napadnutoj površini, dok svi ostali delovi papilarnih linija ostaju nepromenjeni. Same promene papilarnih linija, nastale ovim putem dobijaju trajni karakter, tj. ne menjaju se sve do eventualne nove povrede. Plitka oštećenja epiderma, čak do potpunog uništenja papilarnih linija, kao npr. kod zidarskih radnika, su privremenog karaktera jer se epiderm brzo regeneriše u potpuno istom obliku.

Rast deteta ne utiče na crtež papilarnih linija, on se samo uvećava. Pored toga što su nepromenljivi, crteži papilarnih linija su i trajni. Zanimljivo je da se crtež papilarnih linija formira još dok je beba u utrobi majke, oko šestog meseca trudnoće, i nepromenljiv je od rođenja pa sve do raspadanja tkiva nakon smrti, odnosno, trajnost papilarnih linija je veća od životnog ciklusa čoveka.

[137] Z. S, M. M. *op.cit*

b) *Različitost,* odnosno individualnost crteža papilarnih linija

Površina kože pokrivena papilarnim linijama je relativno mala, ali je bogatstvo crteža i detalja neverovatno veliko. Papilarne linije nisu glatke krive, već obrazuju i mnoge detalje.

Svi detalji mogu se svesti na tri oblika:

- početak ili kraj papilarnih linija,
- račvanje ili spajanje papilarnih linija i
- izuzetni oblici (delte, mostići, ostrvca, manje crte, veće tačkice i sl.).

Kombinacijom ovih dobijaju se mnogi specifični detalji. Ovakvo bogatstvo detalja čini crtež papilarnih linija prosto neponovljivim. Dugogodišnjim pregledanjem mnogo miliona crteža papilarnih linija naučnici i kriminalisti - praktičari su se uverili da na celom svetu (od oko 6 milijardi ljudi) ne postoje dva prsta sa potpuno jednakim crtežom papilarnih linija. Dakle, ne samo što se ne mogu pojaviti dva jednaka crteža papilarnih linija kod različitih lica, već se ne mogu pojaviti ni na dva prsta iste ruke. U tom smislu proučavani su i proveravani crteži papilarnih linija kod jednojajčanih blizanaca, i tada je uočena izvesna sličnost, ali je uvek bilo mnogo razlika u opisanim detaljima da su se veoma lako razlikovali. Što je još važnije, utvrđeno je da se čak deo crteža papilarnih linija sa jednog prsta, veličine 0,5 cm^2, ne može sresti na istom prstu niti pak na bilo kom drugom prstu u svetu. Zato se s pravom kaže da su crteži papilarnih linija jedinstveni i neponovljivi.

c) *Preslikavanje* crteža papilarnih linija

Crteži papilarnih linija se mogu preslikati, odnosno prenositi na predmete koji se prstima dotaknu. Sve ovo zajedno omogućava široku primenu papilarnih linija u kriminalističke svrhe, jer se često na mestu izvršenja krivičnog dela mogu naći preslikani otisci papilarnih linija na dodirnute predmete. Naročito su za oblast kriminalističke tehnike značajni takozvani utisci ili reljefni tragovi papilarnih linija. Oni su trodimenzionalni prikazi (negativi) crteža papilarnih linija na koži.

d) *Grupisanje* crteža papilarnih linija

Nepromenljivost i individualnost crteža papilarnih linija imale bi samo teoretski, a mali praktičan značaj da nije uočena mogućnost njihove klasifikacije po određenim sistemima. Naime, da ne postoji mogućnost grupisanja određenih specifičnih oblika papilarnih linija, ne bi bilo moguće ni formiranje zbirki uzetih otisaka, već bi u najboljem slučaju mogla da se izvrši samo direktna identifikacija. To je za kriminalističke potrebe nedovoljno i apsolutno neprihvatljivo. Uprkos apsolutnoj raznolikosti crteža papilarnih linija kod ljudi, empirijski je utvrđeno da se oni ipak mogu grupisati na svega nekoliko osnovnih grupa po opštoj konfiguraciji crteža, odnosno sličnosti, što omogućava relativno lako formiranje zbirki otisaka po određenom sistemu klasifikacije, slika 15.

a) Detalji otiska prsta

b) Minucije: početak papilarne linije i račvanje

Slika 15 Detalji otiska prsta i minucije

Karakteristike dobijene iz slike otiska prsta mogu se podeliti u dve grupe: globalne karakteristike koje predstavljaju grube uzorke vidljive na prvi pogled i lokalne karakteristike.[138]

Prepoznavanje se vrši svrstavanjem određenog tipa otiska na osnovu uzetog uzorka i potom identifikaciju na osnovu lokalnih karakteristika.[139]

[138] Prepoznavanje otiska prsta, objavljeno http://dosl.zesoi.fer.hr/seminari/1998_1999/visnjic-safarzik/index2.html,pristupljeno 19.04.2013.

Globalne karakteristike nisu dovoljne za identifikaciju, ali su dovoljne za grupisanje otisaka prstiju. Tu spadaju osnovni oblici papilarnih linija (luk, petlja, krug), središnja tačka, delta, karakteristične linije i papilarni broj.[140]

Osnovnih oblika crteža papilarnih linija na čovečijim prstima ima relativno malo. Tri osnovna oblika, prikazana na slici 16, koja preovlađuju po svojoj sličnosti konfiguracije kod svih ljudi na svetu su:[141]

- *Lučni,*
- *Petljani i*
- *Kružni* crteži papilarnih linija.

Lučni crteži papilarnih linija su takvi crteži kod kojih papilarne linije idu u vidu lukova sa većim ili manjim ispupčenjima prema vrhu, od jedne ivice prsta prema drugoj i ne vraćaju se nazad.

Petljani crteži papilarnih linija su takvi crteži kod kojih papilarne linije polaze sa jedne strane prsta, idu ka centru, gde se savijaju i vraćaju na istu stranu, praveći petlju, čiji je otvor na strani odakle polaze papilarne linije, dok se na suprotnoj strani formira crtež u vidu grčkog slova "delta". Prema strani otvora petlje ovakvi crteži papilarnih linija se dele na leve i desne petlje. U zavisnosti od toga na kojoj strani se nalazi otvor razlikuju se dve vrste petlji i to otvor na strani palca, radijalna petlja, i otvor na strani malog prsta, ulnarna petlja.[142]

Kružni crteži papilarnih linija su takvi crteži u čijim centrima papilarne linije formiraju krugove, ovale, elipse, spirale, duple spirale, petlje blizance, kovite, duple petlje i druge slične crteže, a sa svake strane se javlja po jedna delta, ukupno dve delte, a u izuzetnim slučajevima, kod složenih otisaka i više od dve delte.

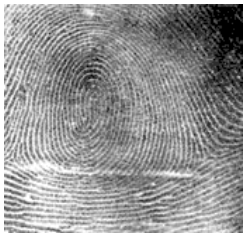
---

[139] *Ibid.*
[140] *Ibid*.
[141] Z. S, M. M. *op.cit*
[142] Otisak prsta, objavljeno
http://arka.foi.hr/~mschatten/radovi/Fingerprint.pdf, pristupljeno 11.03.2013.

Čist luk

Leva petlja

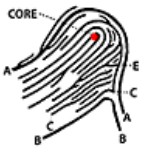
Desna petlja



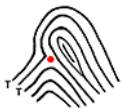
Otisak kružnog uzorka

Slika 16 Osnovni oblici papilarnih linija

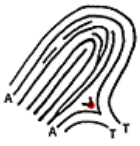
Petljasti oblik je zastupljen u 60%, spiralni u 30%, lučni u 5% i ostali u 5% slučajeva.[143]



Središna tačka (*engl. core pointse)* nalazi negde na sredini otiska i predstavlja referentnu tačku pri obradi otiska.



Karakteristične linije (*engl. type lines)* su dve papilarne linije unutar otiska koje okružuju područje otiska.



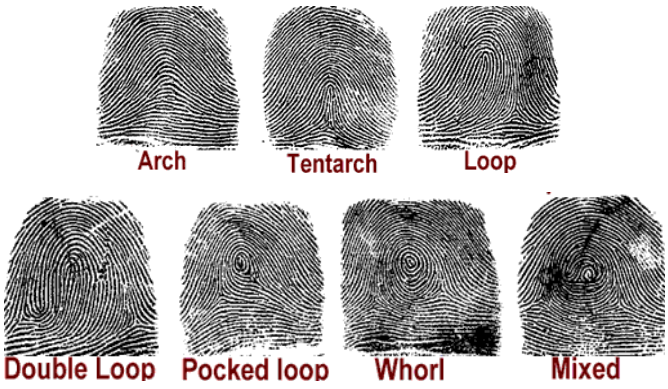
Delta je prva tačka grananja unutar područja uzorka, odnosno bilo koja tačka smeštena direktno ispod centra papilarnih linija.

[143] Prepoznavanje otiska prsta, objavljeno http://dosl.zesoi.fer.hr/seminari/1998_1999/visnjic-safarzik/index2.html, pristupljeno 19.04.2013.

Papilarni broj je broj papilarnih linija u području uzorka (slika 17), a određuje se brojanjem papilarnih linija koje seku zamišljenu dužinu povučenu između delte i središne tačke.

Slika 17 Određivanje papilarnog broja

Prema modifikovanom Vučetićevom sistemu, koji se primenjuje u Srbiji, u monodaktiloskopiji, razlikuje se šest podvrsta lučnih uzoraka, po tri petljana (tri leva, tri desna petlja) i šesnaest podvrsta kružnih uzoraka, što je ukupno 26 različitih podvrsta.[144] U svetu je najzastupljenija podela na sedam podtipova otisaka prsta, slika 18, i to: luk (*arch*), jeloviti luk (*tentarch*), petlja (*loop*), dvostruka petlja (*double loop*), jamičasta petlja (*pocked loop*), spirala (*whorl*) i mešoviti (*mixed*). [145]

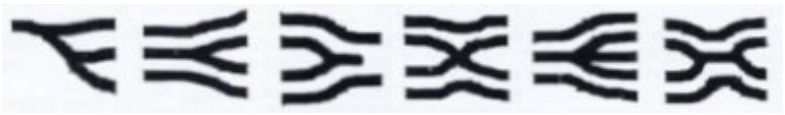


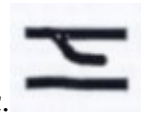
Slika 18 Osnovni podtipovi uzoraka otiska prsta

[144] Z. S, M. M. *op.cit*
[145] M. Tripunović, Z. Anđelković *Otisak prsta-biometrijski podaci*, INFOTEH-JAHORINA, Mart (2007).

Lokalne karakteristike su minucijske tačke ili minucije koje predstavljaju prekid papilarnih linija i upravo one predstavljaju karakteristike na osnovu kojih se vrši identifikacija.[146]

U principu, postoji pet različitih minucijskih karakteristika. Prvo, postoje različite vrste minucija, slika 19. To su, najčešće: [147]

a.  b. 

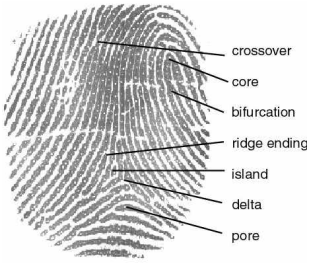
c.  d.  e.  f.  g. 

Slika 19 Minucijske karakteristike

1. Vrste minucije:
    a. papilarni početak ili završetak (nagli prekid papilarnih linija)
    b. papilarno grananje – račvanje (tačka grananja u više novih)
    c. manja račva (razdvajanje papilarnih linija)
    d. papilarna tačka (veća tačka)
    e. papilarni ogib (linija koja se deli u dve i zatim ponovo spaja stvarajući zatvoreno područje bez uzorka)
    f. kratka papilarna linija (manja crta)
    g. mostić (crta koja spaja dve papilarne linije)
2. Orijentacija minucije predstavlja smer minucijske linije
3. Udaljenost papilarnih linija oko minucije
4. Zakrivljenost minucija koje predstavljaju promenu minucijskog smera
5. Minucijske koordinate koje predstavljaju udaljenost minucije od središne tačke i delte.

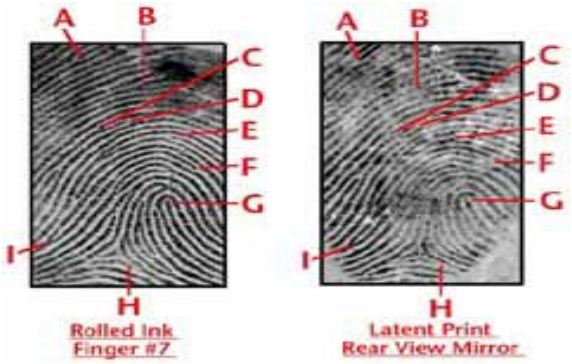
[146] Prepoznavanje otiska prsta, *op.cit.*
[147] *Ibid.*

Korišćenje minucijskih karakteristika je ilustrovano na slici 20.

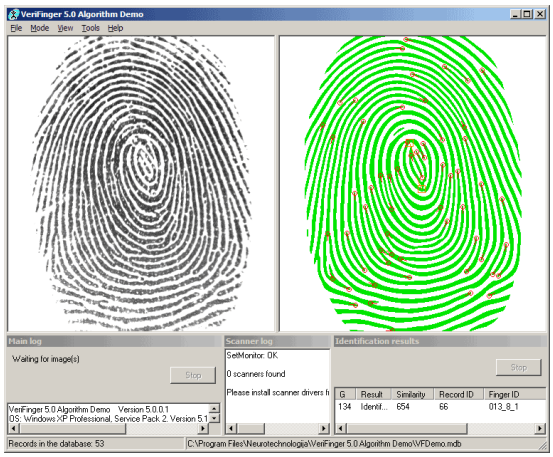


crossover – ukrštanje, *core* – središte, *bifurcation* – račva, *ridge ending* – kraj linije, *island* – ostrvo, *delta* – delta i *pore* – pora.

a) Lokalne karakteristike



b) Obeležavanje minucija na nespornom otisku i spornom tragu ili otisku



c) Obeležavanje minucija (crvena boja) na automatskom sistemu

Slika 20 Minucijske karakteristike i njihovo korišćenje

Ranije se otisak prsta uzimao uz pomoć mastila i papira, odnosno daktiloskopskog fiša, tako što bi prst koji je stavljen u specijalnu daktiloskopsku pastu, valjanjem od jednog kraja ka drugom ostavljao otisak na papiru, koji bi se nakon toga skenirao. Danas je ovakav način prevaziđen. Zahvaljujući razvoju biometrijske tehnologije sada je dovoljno prisloniti prst na skener, a rezultat se dobija za par sekundi.

Biometrija prepoznavanja otiska se u celosti zasniva na papilaroskopiji. Papilaroskopija je širi pojam od daktiloskopije, jer obuhvata ne samo otiske prstiju – daktiloskopiju (grčki: *dactilo* - prst + latinski: *scopein* - gledati), nego i dlanova - heiroskopiju, kao i neke druge pomoćne grane identifikacije (poroskopiju i daktiloskopiju). Daktiloskopija je metoda koja se bavi proučavanjem otisaka papilarnih linija na čovekovim prstima. Kod nas je uvedena po metodi *Ivana Vučetića* koji je osmislio sistem za klasifikaciju papilarnih linija, odnosno otisaka prstiju. Sistem je nazvao ikonofalangometrija.

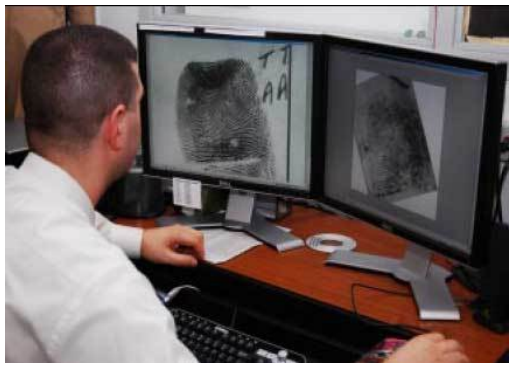
Svaka daktiloskopska baza se klasifikuje, odnosno deli u zbirke. Kako bi olakšao pretragu Vučetić je napravio grubu podelu u četiri osnovne grupe otisaka. Kada su baze postale veće, četiri grupe dobile su podgrupe što je rezultiralo bržom pretragom.

U Republici Srbiji pri Nacionalno kriminalističko-tehničkom centru postoji odsek za daktiloskopiju (sa dve grupe, u Novom Sadu i Nišu) gde stručnjaci mahom rade na identifikaciji otisaka pronađenih na mestima izvršenja krivičnih dela. U zbirci se nalazi oko 200.000 registrovanih lica, osumnjičenih za izvršenje raznih krivičnih dela. Njihovi otisci su zajedno sa fotografijama i osnovnim ličnim podacima ušli u bazu podataka uz odobrenje suda (ili po ranijem zakonu, kada su postojali osnovi sumnje i bez odobrenja suda). Podaci se čuvaju u evidencijama policije trajno, na osnovu Zakona o policiji.

Razvojem tehnologije, danas se klasična daktiloskopija primenjuje u digitalnom okruženju, pa su naredni pasusi posvećeni automatizovanoj identifikaciji otiska prsta.

6.1.2. Sistemi za automatsku identifikaciju sa otiskom prsta

Sistem za automatizovanu identifikaciju otiska prsta (*engl. Automated Fingerprint Identification System, AFIS*) predstavlja moderan računarski sistem za identifikaciju i obradu otisaka papilarnih linija. Posebno je značajan u borbi protiv terorizma i organizovanog kriminala, jer omogućava sigurnu, efikasnu i brzu identifikaciju kriminalaca. Koristi se za kriminalističke (identifikacija kriminalaca) i civilne svrhe (identifikacija građana, identifikacija leševa nepoznatih lica i identifikacionih dokumenta građana). Primena ovog sistema omogućila je izradu kvalitetnih i zaštićenih identifikacionih dokumenata koji su usaglašeni sa evropskim i svetskim standardima, *AFIS* i *FIIS*. Ovaj sistem se koristi u Ministarstvu unutrašnjih poslova Republike Srbije. Na slici 21 prikazano je radno mesto operativca na sistemu *AFIS*.



Slika 21 Radno mesto u sistemu AFIS

Konfiguraciju ovog sistema, projektovanog za potrebe Ministarstva unutrašnjih poslova Republike Srbije, čini Omnitrakov centralni sistem i radne stanice sa odgovarajućom periferijom koje se nalaze na udaljenim lokacijama. *Omnitrak* predstavlja sistem baziran na principima otvorenog sistema koji uključuje opremu specijalno dizajniranu za snimanje, unošenje, procesiranje i ispitivanje otisaka prstiju i tragova, kao i otisaka dlanova i bridova.[148] Radne stanice imaju digitalne komponente, na primer, digitalnu kameru i skener visoke rezolucije, kao i štampače za različite tipove štampe, kao što su

[148] I. Šetrajčić, N. Petrović, *Specijalistički kriminalistički projekat - AFIS I FIIS*.

daktiloskopski kartoni, dokumente u boji i izveštaje. Komponente Omnitrak sistema *AFIS* prikazane su na slici 22.

Radna stanica

Radna stanica Print scan

Radna stanica Multiprint scan

Slika 22 Komponente sistema AFIS

Postoji više baza u kojima su raspoređeni podaci sistema *AFIS*, a to su:[149]

- desetoprstne baze (desetoprstna baza osumnjičenih lica sadrži opisne podatke, fotografije, otiske deset prstiju, dlanova, kontrolnih otisaka, bridova),
- dvoprsne baze sadrže opisne podatke za sva lica sa otiscima dva kažiprsta (valjana i na dodir),
- baza dlanova (opisne podatke osumnjičenih lica sa otiscima njihovih dlanova i bridova),
- baza nerešenih slučajeva otisaka prstiju i otisaka dlanova (sadrži otiske pronađene na mestu izvršenog krivičnog dela).

[149] *Ibid.*

6.1.3. Metodologija rada sa sistemom AFIS

Identifikacija osobe na osnovu otisaka prstiju je jedna od najstarijih, najpoznatijih i najpouzdanijih biometrijskih tehnologija. Pa ipak, ona i dalje predstavlja polje aktivnog istraživanja i razvoja, jer postoji dosta izazova koje je potrebno prevazići. Ovakvi biometrijski sistemi su zasnovani na upoređivanju uzetog uzorka sa uzorkom uskladištenim u bazi podataka. Koji će se pristup pritom koristiti zavisi od namene sistema. Recimo, u bezbednosnom polju primene povoljnije je korišćenje centralne baze podataka, ali sa druge strane takav pristup zahteva značajnija finansijska ulaganja, pa se koristi samo na područjima gde je to nužno, kao što je kriminalistika. Uzorci mogu biti uskladišteni u centralnoj bazi podataka, ili na hard disku računara pa svaki ovlašćeni korisnik može da sa sobom nosi uzorak, na magnetnoj ili čip kartici.

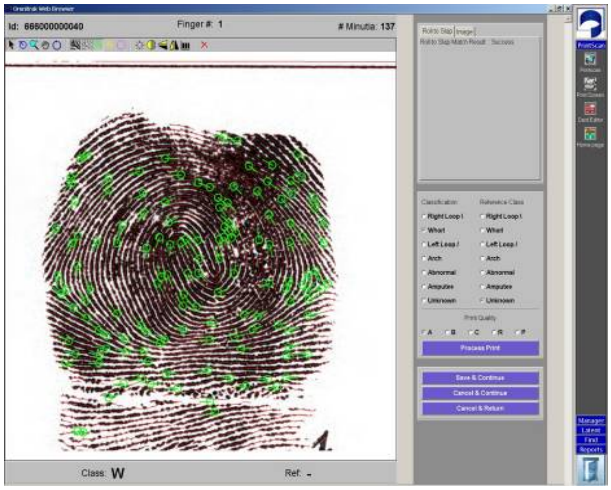
Prepoznavanje ili identifikacija se vrši upoređivanjem skupa karakterističnih detalja uzetog otiska prsta sa skupom karakterističnih detalja uskladištenog u bazi, pri čemu treba imati u vidu da svaki otisak prsta sadrži oko 100 karakterističnih detalja, a deo otiska koji je obuhvaćen skenerom sadrži od 30 do 40 detalja.[150] Broj individualnih karakteristika koje se moraju poklopiti da bi se dokazalo da dva otiska potiču od iste osobe razlikuje se u zavisnosti od države i kreće se u rasponu od devet do petnaest. U Republici Srbiji se traži poklapanje dvanaest karakteristika.

Brojna su pitanja, naročito u sudskim postupcima, zašto se traži toliki broj individualnih anatomskih obeležja pri identifikaciji. Može se slobodno reći da što je broj poklapanja anatomskih karakteristika veći, time je i pouzdaniji metod identifikacije, odnosno manja greška, pa postaje gotovo nemoguće da će se pojaviti još neki crtež papilarnih linija sa istim karakteristikama na istom mestu.

U našoj kriminalističko-tehničkoj i kriminalističkoj literaturi, potvrđena je policijska praksa, zasnovana na naučno - statističkom metodu, da se na osnovu 12 identičnih karakteristika na istoj oblasti papilarnih linija, ne mogu

[150] I. Šetrajčić, N. Petrović, *Specijalistički kriminalistički projekat - AFIS I FIIS.*

pronaći dva ista čoveka na svetu, čime je mogućnost greške isključena i metoda identifikacije veoma pouzdana, slika 23. Prema važećim propisima ekspertiza se radi po pravilima nauke i struke, a pravila struke su izvedena iz, do sada, poznatih naučnih metoda i istraživanja.[151]



Slika 23 Identifikacija osobe na osnovu otiska prsta

U procesu prepoznavanja otiska se koriste dve glavne metode: prepoznavanje ukupnog uzorka (globalne strukture) i prepoznavanje na temelju minucija (lokalne strukture). Osnov prve metode je analiza celokupnog prsta, dok je osnov druge metode analiza račvanja i završetaka linija, kao i drugih ranije opisanih karakteristika.

Posmatrano sa informatičkog stanovišta, drugi pristup zahteva oko 250 bajta memorije, pa je mnogo brži, jer analizira i upoređuje samo nekoliko karakterističnih tačaka, dok prvi pristup traži oko 100 kilobajta memorije i zahteva više računarskog vremena.[152]

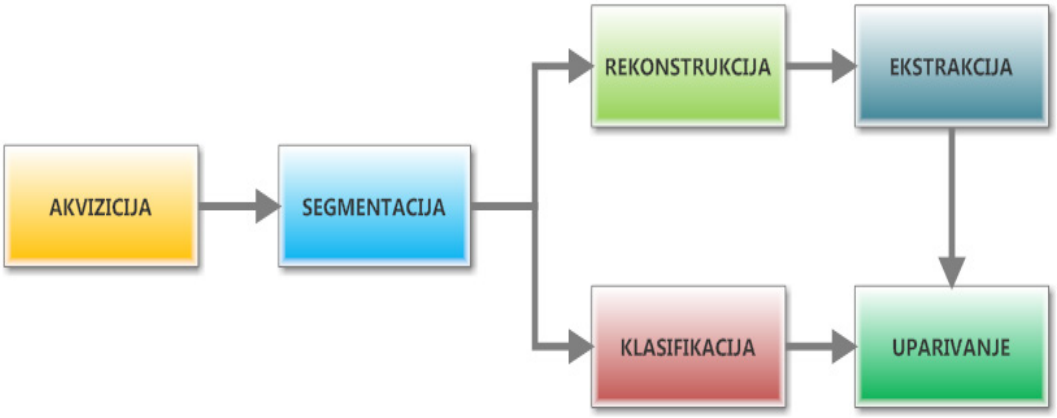
Dakle, prvi korak u procesu identifikacije, bilo da je izvodi čovek ili mašina, je prepoznavanje kojem tipu pripada uzorak (globalna struktura, četiri tipa), nakon čega se nalaze detalji i porede. Otisci u elektronskom obliku, u

[151] Z. S, M. M. *op.cit*
[152] Z. S, M. M. *op.cit*

stvari predstavljaju digitalne slike, a sistem za prepoznavanje otisaka se sastoji od sledećih komponenti: [153]

- *podsistema za predprocesiranje* - komponenta koja ima zadatak da priredi digitalnu sliku prema zadatim normama za proces prepoznavanja otiska, a sastoji se od normalizacije slike po osvetljenju, kontrastu, veličini, rotaciji i neutralizaciji pozadine,
- *podsistema za detekciju* otiska, komponenta koja ima zadatak da pronađe otisak na slici i da utvrdi njegov tačan položaj,
- *podsistema za prepoznavanje,* komponenta u kojoj se suštinski odvija proces utvrđivanje identiteta.

Osnovni koraci u automatizovanom prepoznavanju otisaka, koje susrećemo u sistemu *AFIS*, a prikazanih grafički na blok dijagramu 2, su akvizicija slike, segmentacija slike, rekonstrukcija slike, ekstrakcija karakteristika, poređenje (uparivanje) minucija i klasifikacija otiska.[154]



Blok dijagram 2 Osnovni koraci u automatizovanom prepoznavanju otisaka

Prva faza je *akvizicija* u kojoj sistem elektronskim skenerom beleži otisak prsta, i to tako što se prst *valja* prsta preko skenera ili samo *dodirom* skenera prstom ili dlanom. Ovaj način akvizicije daje sliku otiska mnogo boljeg kvaliteta

[153] Otisak prsta, *op.cit.*
[154] M. Tripunović, Z. Anđelković *Otisak prsta-biometrijski podaci*, INFOTEH-JAHORINA, Mart (2007).

u odnosu na sliku koja bi se dobila tako što bi se prst na koji je naneto mastilo otisnuo na papir, pa onda skenirao (takozvana *off line* akvizicija).

Nakon toga sledi faza *segmentacije*, proces u kojem se otisak izdvaja od pozadine slike, pa se tako izdvojeni podaci dalje obrađuju, odnosno analiziraju radi nalaženja karakteristika otiska. Prsti su podložni spoljnim uticajima, kao što su znoj, prljavština i slično, pa se ovi uticaji pre analize moraju neutralisati, kako bi papilarne linije bile čiste i dobro vidljive. Kao što je već ranije rečeno, neophodno je podešavanje atributa slike (osvetljenje, kontrast i veličinu, rotaciju otiska i neutralizovati pozadinu). Za to *AFIS* koristi filtere kojima se odbacuju sve linije koje nisu u smeru papilarnih.

Faza *rekonstrukcije* slike treba da ostvari dva osnovna cilja, a to su povećanje kontrasta između grebena i dolina, kao i povezivanje prekinutih grebena.

U fazi *ekstrakcije* na osnovu uočenih minucija iz rekonstruisanog otiska formira se uzorak ili šablon. Nakon ove, sledi faza *uparivanja* u kojoj se formirani uzorak otiska prsta upoređuje sa postojećim uzorcima iz baze podataka. To je zapravo ekvivalent ranije opisanog postupka vizuelnog uparivanja minucija. Prilikom upoređivanja mogu da nastanu određeni problemi zbog različite pozicije, usmerenja i pritiska prsta na senzorskoj ploči ili odsustva nekih karakterističnih detalja zbog oštećenja, prljavštine, znojenja ili lošeg prislanjanja na senzorsku površinu, a u slučaju kada se radi o kriminalističkim tragovima sa mesta uviđaja i zbog odsustva pojedinih detalja.

Klasifikacija otiska predstavlja proces svrstavanja otiska u neki od osnovnih tipova. Razvijeni su različiti algoritmi pomoću kojih se vrši klasifikacija.

U praksi, vrlo često se dešava da otisak papilarnih linija pronađen na licu mesta, nema sve potrebne elemente za klasifikaciju (fragment otiska). Bez obzira na to, najbitnije je da otisak sadrži potreban broj lokalnih karakteristika

(minucija), koje će sistem prepoznati, uporediti sa bazom otisaka poznatih izvršioca krivičnih dela i izvršiti identifikaciju.[155]

Sistem automatizovane identifikacije koristi brojne algoritme putem kojih se proveravaju i upoređuju različita usmerenja slike i stepen podudarnosti sa minucijama, a nakon toga određuje stepen preklapanja.

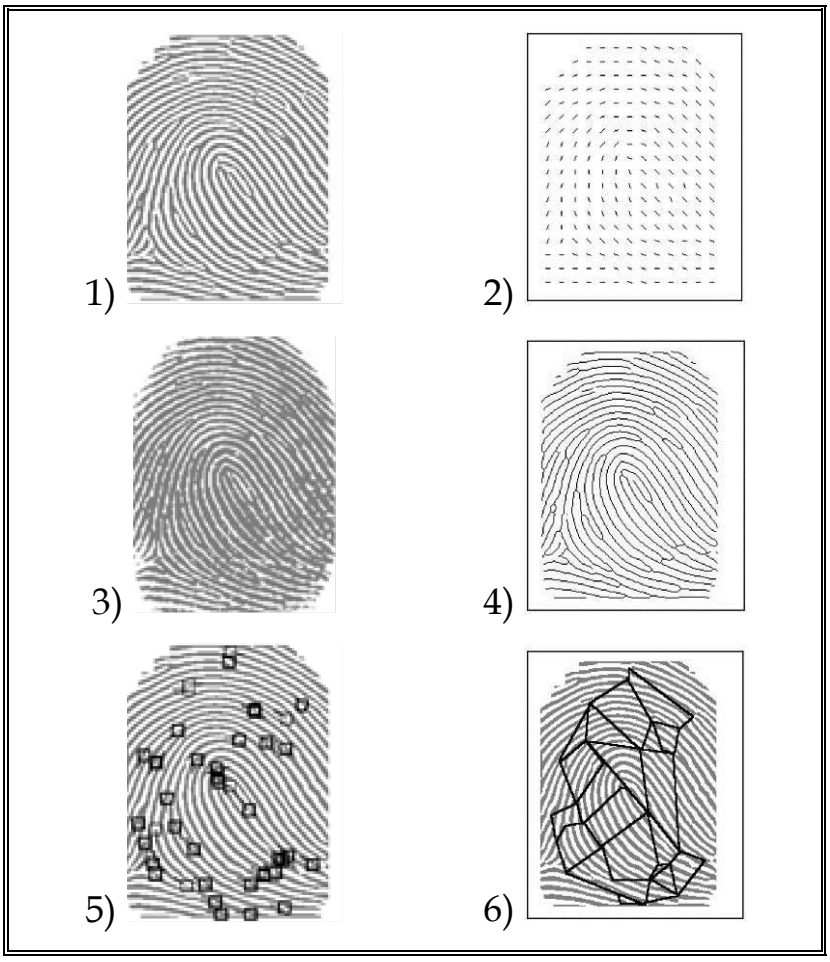
Postoje dva osnovna pristupa u procesu nalaženja minucija, i to:

- *pristup diskriminacije,* koji se temelji na položaju središnje tačke, delte i broja papilarnih linija među njima. Nedostatak ovog pristupa se ogleda u tome što dosta zavisi od kvaliteta uzorka, a često je teško odrediti i položaj središnje tačke. Pored toga, delta često i nije dostupna, jer se nalazi na samoj ivici otiska.[156]
- *strukturni (sintakički) pristup,* koji se bazira na toku papilarnih linija, kao i na karakterističnim oblicima koje na njima nalazimo, kako bi se dalje, po hijerarhijskom pristupu, razvrstali u manje podgrupe.[157]

U praksi najčešće korišćeni pristup određivanja minucija i njihovog međusobnog odnosa, ilustrovan grafički na slici 24, sadrži sledeće korake:

1) Pretvaranje originala otiska u računarski čitljiv oblik (sa papira ili skenera),
2) Određivanje logičke orijentacije otiska,
3) *Binarizacija* originalne slika otiska,
4) Formiranje kontura otiska ili ”linija kostura”,
5) Određivanje minucija (automatski ili ručno), i
6) Određivanje grafa minucija.

[155] Z. S, M. M. *op.cit.*
[156] Prepoznavanje otiska prstiju, *op.cit.*
[157] *Ibid.*



Slika 24 Proces određivanja minucija

Uz pomoć različitih programskih algoritama, vrši se pretraživanje baze uzoraka po sličnosti, po svim izdvojenim osobinama, pojedinačno i zbirno. Nakon izvršenog pretraživanja treba generisati rezultate pretraživanja, tako što će algoritam na osnovu matematičkih proračuna o sličnosti uzorka iz baze uzoraka sa ulaznim uzorkom, uzorku iz baze dodeliti broj koji pokazuje stepen sličnosti. Dakle, uzorak sa dodeljenim najvećim brojem je najsličniji ulaznom uzorku!

Na taj način se u koloni mogu poređati otisci iz baze po stepenu sličnosti sa ulaznim otiskom, a po brojčanim izrazima u kojima može biti od 5 do 20 lokalnih karakteristika (može i manje i više od toga, u zavisnosti kako se podesi sistem), koje potom čovek – operativac ponovo analizira, odnosno verifikuje rezultat. Zato se za *AFIS* kaže da je *automatizovan,* a ne automatski sistem

identifikacije! Računar služi samo da brže pronađe podatak u bazi, tako da ono što se radilo nekada danima, mašina sada uradi u nekoliko sekundi.[158]

Kako bi se prevazišle pogreške, recimo zbog mokrih prstiju ili prstiju čija je površina oštećena (posekotine, modrice i sl.), uvode se nove generacije algoritama koje znaju da se izbore sa ovakvim problemima. Značajno je i korišćenje filtera koji imaju za cilj da sačuvaju pravu strukturu otiska. Biometrijski sistemi koji rade sa otiscima prstiju veoma su pouzdani, pa je zanimljivo istaći da su najveće baze podataka i najbolji algoritmi za pretraživanje razvijeni upravo za potrebe ove metode.[159]

Tačnost biometrijskih sistema se može odrediti preko dva specifična parametra, i to: preko stope prihvatanja pogrešno prepoznatog identiteta, *FAR*, odnosno slučaja pogrešnog prihvatanja identiteta koji nastupa kada se ulazni uzorak neke osobe dovoljno preklapa sa uzorkom iz baze uzoraka neke druge osobe, i preko stope pogrešnog neprihvatanja identiteta, *FRR*, odnosno pogrešnog odbijanja da se prihvati identitet osobe koju treba identifikovati, zato što se njen ulazni uzorak nedovoljno preklapa sa ranije uzetim uzorkom te osobe u bazi uzoraka, pa sistem zaključuje da je reč o osobi za koju nema zabeležene lične podatke. Kod kvalitetnih sistema za rad sa otiscima prstiju vrednosti oba koeficijenta, *FAR* i *FRR*, iznose 0,05 %.[160] U praktičnom radu, ova biometrijska tehnologija se koristi na dva načina, i to:

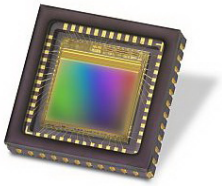
- uz pomoć *slike* prsta, koja se dobija tako što se prst prisloni na određenu površinu i na njoj zadrži neko vreme potrebno da prst snimi specijalnim fotoaparatom. Ova tehnika ima dosta ograničenja, jer se ne snima ceo otisak prsta, ali je dovoljna za kontrolu pristupa preko prepoznatog otiska ili za mobilnu proveru identiteta,

[158] L. O'Gorman, *Fingerprint Verification, available on,* http://scgwww.epfl.ch/courses/notes/2%20Fingerprints.pdf, pristupljeno 11.03.2013.
[159] D. Maltoni, R. Cappelli, *Fingerprint Recognition*, Handbook of Biometric (eds. A.K.Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 23-43.
[160] Ž. Radmilović, Identifikacija temeljem otisaka prstiju**,** *Biometrijska identifikacija,* Stručni članak, (2008).

- uz pomoć *skeniranja,* u postupku valjanja prsta preko površine skenera. Dobijena slika se zapiše u memoriju i potom softverski obradi. Na ovaj način se prikupi više detalja o karakteristikama prsta, na primer i delte. Ova tehnika je bolja od slikanja prsta i koriste je kriminalističke službe.

Da bi identifikacija bila uspešna, ulazni senzor mora biti u mogućnosti da prikupi sve potrebne podatke za identifikaciju i to u različitim uslovima rada. Na tržištu postoje više tehnologija koje se koriste u realizaciji ulaznih senzora za uzimanje otiska prsta. Najpoznatije su optički senzori, kapacitivni senzori, termo-električni senzori, senzori električnog polja, senzori bez dodira i senzori osetljivi na pritisak.[161]

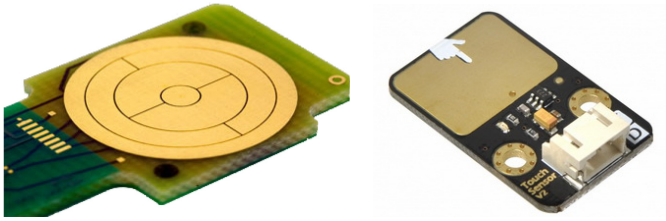
Optička metoda se najčešće koristi u praksi. U svom funkcionisanju koristi digitalne kamere za analizu papilarnih linija. Zasniva se na *CCD* senzoru koji beleži sliku prsta prislonjenog na staklo, a *LED* diode osvetljavaju ispupčenja i udubljenja otiska. Prednosti ove metode su jednostavnost rada i niska cena. Nedostatak su, takozvani, „*latentni otisci*". Naime, na staklu senzora, na koje se prst prislanja celom površinom, ostaje otisak prsta nakon slikanja, kao i na svakoj drugoj staklenoj površini. Ako se taj otisak ne ukloni pre nove upotrebe senzora, to može da ometa sledeće skeniranje. U isto vreme takav otisak predstavlja i sigurnosni rizik za osobu koja ga je dala, jer je taj otisak moguće skinuti. Optički senzor je prikazan na slici 25.



Slika 25 Optički senzor

[161] D. Maltoni, R. Cappelli, *Fingerprint Recognition*, Handbook of Biometric (eds. A.K.Jain, P. Flynn, A. A. Ross), Springer, (2008), str.23-43.

Pored optičke, često se primenjuje i metoda merenja kapacitativnosti[162]. Kapacitativni senzori su veličine pečata, slika 26. Kada se prst prisloni na ovakav senzor niz piksela meri varijacije električnog potencijala, koje su posledice postojanja brazdi na koži prsta i kapacitativnosti između senzora i prsta. Pritiskom prsta na senzor, koji možemo posmatrati kao mrežu veoma malih kondenzatora, ovi kondenzatori se u zavisnosti od udaljenosti kože prsta od podloge različito naelektrišu i tako formiraju električnu sliku prsta sa statičkim elektricitetom. Slabosti ove tehnike su pojava zavisnosti osvetljaja slike prsta u odnosu na vlažnost prsta, mokri prsti daju tamnu, a suvi svetlu sliku.



Slika 26 Kapacitativni senzor

Termoelektrična metoda[163] je prilično retka. Kada je prst prislonjen uz senzor, ovakav senzor meri razliku u temperaturi ispupčenja na otisku i vazduha uhvaćenog u udubljenju. Zahvaljujući tome, dobija se slika visoke rezolucije (oko 500 *dpi*, sa 256 nijansi sive), čak i u slučaju kada je prst prljav ili otisak plitak. Termoelektrični senzor je prikazan na slici 27.

Slika 27 Termoelektrični senzor

[162] D. Maltoni, R. Cappelli, *Fingerprint Recognition,* Handbook of Biometric (eds. A.K.Jain, P. Flynn, A. A. Ross), Springer, (2008), str.23-43.
[163] *Ibid.*

Prilikom skeniranja prsta uz pomoć termoelektričnog senzora neophodno je prevući prst preko senzora, pa se tako rešava i problem čišćenja senzora i latentnih otisaka. Nedostaci ove metode se ogledaju u tome što korisnik mora da zna kako da koristi senzor, kao i u povećanoj potrošnji energije zbog potrebe za zagrevanjem senzora jer treba izbeći poklapanje temperature senzora i prsta. Senzori koji mere temperaturu prsta mogu biti manji i od samog prsta, a podaci o toploti mogu se dobiti prelaskom prsta preko senzora. Oni sadrže niz tačaka kojima se može detektovati razlika temperature kože, bora na koži prsta, i vazduha, odnosno udubljenja na koži prsta.

Senzori sa električnim poljem, engl. *E-Field sensors*, mere električno polje ispod gornjeg sloja kože, odnosno tamo gde otisak počinje.[164] Ova metoda je prilično osetljiva i beleži suve, istrošene i zaprljane otiske. Njeni nedostaci su mala rezolucija snimka i malo polje skeniranja, što povećava procenat greške. Ovi senzori stvaraju električno polje i pomoću niza piksela mere varijacije u polju, slika 28. Varijacije su posledica nabranosti kože prsta.

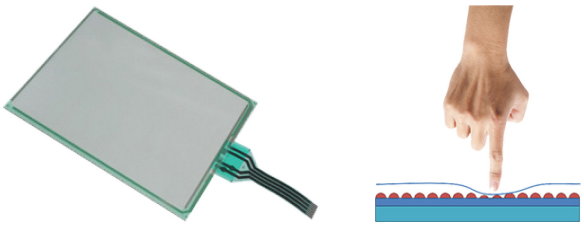
Slika 28 Senzor sa električnim poljem

Senzori bez dodira su u osnovi slični optičkim senzorima.[165] Prst se postavlja na predviđeno mesto radi uzimanja slike, slika 29. Problemi u radu sa ovim senzorima se pojavljuju kao posledica nakupljene prljavštine, a koja može onemogućiti pravilno prepoznavanje otiska. Drugi nedostatak se ogleda u tome što ovi senzori zahtevaju složenije algoritme za prepoznavanje.

[164] *FVC2006 web site, available on,* http://bias.csr.unibo.it/fvc2006, pristupljeno 09.01.2013. godine
[165] *Ibid.*

Slika 29 Senzor bez dodira

Senzori osetljivi na pritisak beleže samo ispupčenja otiska kada prst dođe u kontakt sa senzorom, slika 30. [166] To se dešava zahvaljujući upotrebi piezoelektričnih kristala koji pod pritiskom ili uvijanjem generišu električni potencijal. Nedostatak je očitani podatak koji je jednobitni (crno-bela slika). Međutim, ovi senzori podjednako dobro rade sa suvim i vlažnim prstima, a i površina skeniranja je prilično velika.

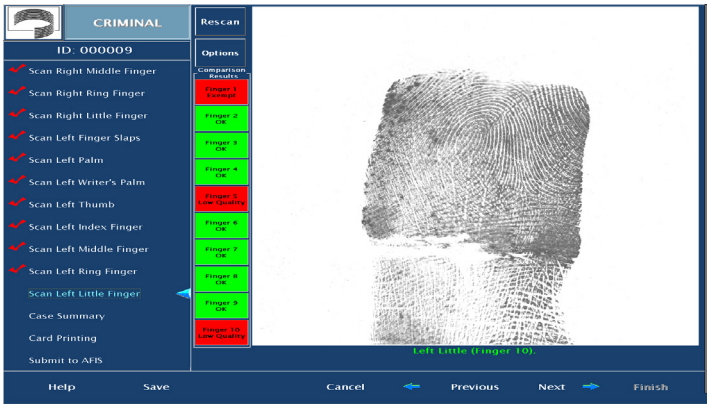


Slika 30 Senzor osetljiv na pritisak

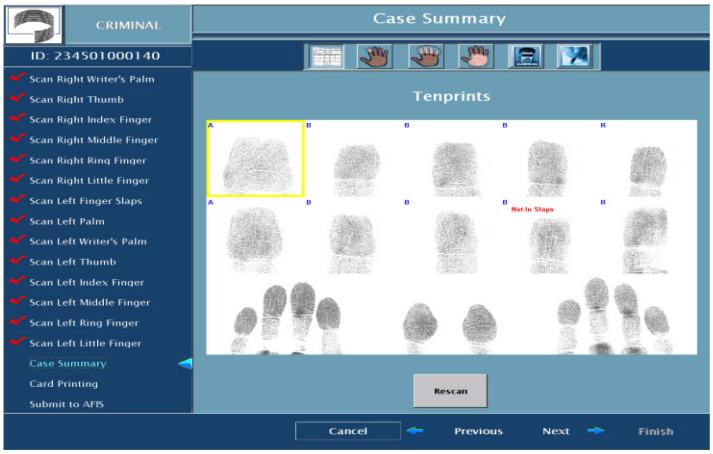
U svetu se stalno se radi na razvoju novih senzora, a posebno na razvoju onih koji bi mogli lako da prepoznaju lažno podmetanje prsta. Za postupak verifikacije i identifikacije postoji više standarda, a najpoznatiji je onaj koji je propisao američki Nacionalni institut za standarde i tehnologiju (*National Institute of Standards and Technology, NIST*).[167] Na slici 31 je prikazan primer izveštaja koje generišu sistemi za identifikaciju na osnovu otisaka prstiju u slučaju skeniranja prsta u živo. Zelenom bojom su prikazani prsti koji su dobro uzeti, crvenom da su loše uzeti ili sa lošom rezolucijom pa se moraju ponoviti. Na slici 32 prikazan je izgled skeniranih otisaka obe ruke uzetih različitim

166 *Ibid.*
167 M.T., Z.A. *op.cit.*

tehnikama, snimanje valjanjem prstiju - gornji deo ekrana, i snimanje dodirom - donji deo ekrana.



Slika 31 Primer izveštaja o kvalitetu rada za proces skeniranja prstiju u živo



Slika 32 Izgled skeniranih otisaka obe ruke uzetih različitim tehnikama

6.1.4. Primena sistema za identifikaciju na osnovu otisaka prstiju

Intenzivan razvoj tehnologije koje se koriste u sistemima za identifikaciju na osnovu otisaka prstiju bitno je uticao na širenje polja primene ove biometrijske metode. Ovakvi sistemi su napravili revoluciju, između ostalog, na polju kontrole pristupa određenim lokacijama i podacima, identifikacije izvršilaca krivičnih dela, kontrole broja sati koje zaposleni provedu na radnom mestu, zdravstvenoj zaštiti, graničnoj kontroli, finansijskim transakcijama, kao i bezbednom pristupu ličnim uređajima.

6.1.4.1. Kontrola pristupa određenim lokacijama i podacima

Jedinstvenost karakteristika, relativno jednostavna i ekonomski povoljna tehnologija akvizicije otiska prsta pružaju ovoj biometrijskoj metodi mogućnost uspešne primene na područjima u kojima se zahteva visok stepen bezbednosti. Tu se pre svega podrazumeva obezbeđenje fizičkog pristupa određenim lokacijama, kao i obezbeđenje pristupa zaštićenim informacijama. Korišćenjem ove biometrijske tehnike u značajnoj meri se eliminiše potreba za korišćenjem nesigurnog mehanizma korisničkog imena i lozinke. Primer uređaja za kontrolu pristupa zaštićenim objektima biometrijskim tehnikama zasnovanom na otisku prsta, a koji se koristi za ove namene, prikazan je na slici 33.

Slika 33 Uređaj za kontrolu pristupa

Kontrola pristupa određenim mestima i objektima široko se primenjuje u državnim ustanovama, radnim organizacijama, industrijskim postrojenjima, fabrikama, vojnim ustanovama, zaštićenim laboratorijama, policiji, objektima za posebne namene... Primenom ove biometrijske metode omogućen je i jednostavniji, ali i bezbedniji, pristup u stanove, kuće, garaže, poslovne objekte. Njenom primenom, sa jedne strane, smanjuje se potreba za osobljem zaposlenim u sektoru obezbeđenja, a sa druge strane smanjuje se mogućnost zloupotrebe.[168] Pod kontrolom pristupa podacima uobičajeno podrazumevamo pristup podacima koji se čuvaju u vladinim računarskim mrežama, pristup podacima kompanija koji predstavljaju poslovnu tajnu ili pristup privatnim podacima koje čuvamo u ličnim uređajima: u *laptop*-u ili *smart* telefonu. U oba

[168] *Physical access control biometric, available on* http://www.findbiometrics.com/physical-access/, pristupljeno 19.12.2012.

slučaja, bilo da je reč o pristupu određenim lokacijama ili je u pitanju pristup određenim podacima, postupak se sastoji u skeniranju otiska prsta koji se nakon toga upoređuje sa uzorkom u bazi. Dakle, da bi neka osoba pristupila zaštićenoj lokaciji ili zaštićenim informacijama, sistem mora da uzet uzorak otiska prsta uporedi sa otiskom prsta ranije ostavljenog u sistemu i da na osnovu rezultata poređenja donese odluku o identitetu osobe. Procenat lažnog prihvatanja ili lažnog odbijanja je, kao što je već naglašeno, veoma mali. Biometrija otiska prsta predstavlja značajnu prepreku za kradljivce identiteta i *hakere,* kojima je cilj da neovlašćeno dođu u posed određenih podataka. Lozinke i brojevi za personalnu identifikaciju, *PIN*, lako mogu biti ukradeni ili otkriveni i nakon toga zloupotrebljeni od strane kriminalaca, što nije slučaj sa fizičkim karakteristikama prsta koje je gotovo nemoguće falsifikovati. Smanjuje se rizik ljudske greške kao i rizik od gubitka podataka.

Može se ograničiti i kontrola pristupa kompjuterskim određenim datotekama i programima. Zbog toga, vojska i vlade zemalja koriste i ovaj vid zaštite kako bi osigurale svoje računarske mreže i sisteme koji zahtevaju visok nivo bezbednosti.[169] Kako bi sačuvali stvari u našim domovima od krađe, stalno smo u potrazi za efikasnim načinom zaštite. Jedan od načina efikasne zaštite predstavlja primena ove tehnologije na brave ulaznih vrata stana. Brava sa biometrijskim ključem zahteva od vlasnika stana da se pre ulaska u stan identifikuje kako bi se vrata otključala, slika 34.

Slika 34 Brava ulaznih vrata stana sa biometrijskim ključem

[169] *Logical access control biometric available on,* http://www.findbiometrics.com/logical-access/, pristupljeno 19.12.2012.

Brava sa biometrijskim ključem, ugrađena na ulazna vrata kuće ili stana, može se priključiti na bezbednosni sistem koji ima zadatak da nadzire ulaz u stan i po potrebi obavesti vlasnika preko mreže mobilne telefonije ako neko pokušava neovlašćeno da uđe ili je već ušao. Takođe, biometrijska brava se može upotrebiti i za otvaranje raznih vrsta ormarića u kome se čuvaju stvari.[170]

6.1.4.2. Kontrola prisutnosti zaposlenih

Evidencija broja sati koje zaposleni provedu na radnom mestu interesuje svakog poslodavca. Uređaji za kontrolu prisutnosti koji rade sa identifikacionim karticama mogu biti obmanuti tako što neko drugi koristi identifikacionu karticu zaposlenog. Navedena kontrola postala je mnogo pouzdanija i lakša od kada je počela da se za te namene koristi biometrijska tehnologija sa otiskom prsta. Primer uređaja koji koristi opisanu tehnologiju kontrole prisutnosti je prikazan na slici 35.

Slika 35 Uređaj za biometrijsku kontrolu prisutnosti zaposlenih

Zaposleni se prilikom dolaska i odlaska sa posla registruju primenom ovog uređaja, tako da poslodavac u svakom trenutku zna broj sati provedenih od strane zaposlenog na radu. Čak i kada postoji prekovremeni rad ili rad kod kuće, poslodavac primenom ove tehnologije zna broj provedenih sati zaposlenog u radu.[171]

[170] *Biometric Fingerprint Lock, available on* http://www.findbiometrics.com/locks/, pristupljeno 19.12.2012.
[171] *Biometric for Time and Attendance, available on* http://www.findbiometrics.com/time-attendance/, pristupljeno 19.12.2012.

Takođe, ukoliko se navedeni uređaji postave na određenim ulazima prostorija, na primer sala za predavanje, može se proveriti ko je u nekom vremenu u njima bio prisutan, recimo imena studenata prisutnih na predavanjima.

6.1.4.3. Biometrija u sistemu zdravstvene zaštite

Primena biometrije u sistemu zdravstvene zaštite uvela je pravu malu revoluciju na polju zdravstvene bezbednosti.[172] Ponekad čujemo o greškama nastalim u sistemu zdravstvene zaštite zbog pomešane zdravstvene dokumentacije, gde pacijentu nije na vreme dijagnostikovana bolest ili je prepisan neodgovarajući lek, ili što je češći slučaj, kada su u pitanju javne ličnosti, da njihovi privatni podaci izađu u javnost.

Primena biometrijske tehnike sa otiskom prsta predstavlja jedan od efikasnih načina za prevazilaženje pomenutih i sličnih problema. Suština primene u ovoj oblasti je što se sa sigurnošću može utvrditi da li neka osoba ima status ovlašćenog lica koje ima dozvolu da dođe u posed nečijih zdravstvenih podataka ili da bude potpisnik nekog dokumenta. Biometrijski sistemi pružaju mogućnost pacijentima da se osećaju sigurnije, u smislu da će njihovi podaci ostati u statusu lekarske tajne, jer će samo ovlašćena osoba moći da dođe u posed istih.

Takođe, biometrijska tehnologija pruža mogućnost da se, kada je to potrebno, podaci o zdravstvenom stanju pacijenta bezbedno prenose iz jedne u drugu zemlju.

Problem greške u dodeli terapije može nastati ukoliko u ruke lekara dođe pogrešan karton pacijenta, što može dovesti do teških posledica. Pomenuti problem je primenom biometrije prevaziđen jer se uz pomoć ove tehnologije prvo utvrđuje identitet pacijenta i tek potom omogućava lekaru pristup podacima upisanim u zdravstveni karton tog pacijenta. Sa druge strane, njenom primenom farmaceuti mogu na vreme, daljinskim pristupom

[172] *Biometric in HealthCare, available on* http://www.findbiometrics.com/health-care/, pristupljeno 19.12.2012.

određenom delu kartona pacijenta, da saznaju da li je kupac leka eventualno alergičan na isti. Uvođenjem i primenom biometrijske tehnologije izmenio se izgled zdravstvene bezbednosti. Ovaj način rada se primenjuje u Sjedinjenim Američkim Državama od 2009. godine, čija se upotreba sve više širi u svetu.

6.1.4.4. Kontrola graničnih prelaza

Biometrijske tehnologije, posebno one koje su primenjene na otiske prstiju, su u upotrebi u bezbednosnim sistemima za kontrolu graničnih prelaza. Naročito su značajne na aerodromima. Primer sistema za kontrolu graničnih prelaza koji koristi biometrijsku tehniku sa otiskom prsta dat na slici 36.

Slika 36 Uređaj za kontrolu graničnog prelaza sa otiskom prsta

Za pristup bazi biometrijskih podataka mogu da se koriste i elektronski čitači pasoša. Neki granični sistemi podržavaju dve faze kontrole. U prvoj kontroli koriste se čitač biometrijskog pasoša, a u drugoj uzimanje otiska prsta. Time se postiže najpreciznija identifikacija.[173]

[173] *Border control, available on* http://www.findbiometrics.com/border-control-airports/, pristupljeno 19.12.2012.

6.1.4.5. Zaštita finansijskih transakcija

Zbog sve češćih zloupotreba identiteta, neophodno je ostvarivanje efektivne i efikasne bezbednosti u svim vidovima poslovnih transakcija, a pogotovu finansijskim. Elektronske transakcije, sa jedne strane, pružaju učesnicima brojne prednosti koje se ogledaju prevashodno u uštođenom vremenu i novcu. Sa druge strane otvaraju mogućnost zloupotreba kao posledicu krađe identiteta. Ne samo što novac može biti ukraden, već mogu biti ukradeni brojevi kreditnih kartica i njihove pristupne lozinke, brojevi računa u banci i slično. Svako od nas je svestan mogućnosti gubitka novčanika sa kreditnim karticama i eventualne zloupotrebe. Zabrinuti smo i kada na bankomatu unosimo kartični identifikacioni broj- *PIN*, kao i pri *online* kupovini na Internetu, gde „*cyber*" kriminalci uvek iznalaze nove načine za prevaru i krađu.

Biometrijska tehnologija sa otiskom prsta uspešno nalazi primenu i u finansijskim transakcijama, jer se tako postiže daleko veća sigurnost u odnosu na bilo koji drugi konvencionalni sistem koji je danas u upotrebi. Njenom primenom, uz kombinaciju sa kartičnim identifikacionim brojem- *PIN*-om, pomenuti problemi mogu biti prevaziđeni i sa znatno većom sigurnošću se može obaviti bilo kakva finansijska transakcija. Banke koriste ovu biometrijsku tehniku, kako bi osigurale rad svojih računarskih centara i kako bi omogućile efikasne i bezbedne novčane transakcije, kako u realnom okruženju, tako i pri *online* elektronskim sistemima plaćanja.

Navedimo primer rada sistema plaćanja poznat pod imenom „*Pay by Touch*".[174] Pre korišćenja ovog sistema korisnik je obavezan da se registruje, kao i prodavnice koje nude ovakav sistem plaćanja robe ili usluga. Prilikom registracije korisnik mora da priloži na uvid svoja lična dokumenta radi povezivanja ličnih podataka sa računom u banci. Nakon toga, korisnik daje prazan ček i uzima mu se otisak prsta. U slučaju *online* plaćanja, korisnik koristi

[174] Tehnologije biometrijskih plaćanja, objavljeno na http://www.e-drustvo.org/proceedings/YuInfo2008/html/pdf/060.pdf, pristupljeno 19.12.2012.

lozinku za logovanje na elektronski novčanik. Korisnik može samo lično da vrši ove finansijske transakcije, odnosno nije u mogućnosti da ovlasti drugu osobu. Navedeni način plaćanja ima svojih prednosti i nedostataka. Prednost je u tome što korisnik prilikom plaćanja ne mora da unosi osetljive podatke, kao što je identifikacioni broj- *PIN* i slično. Nedostatak je u tome što bilo koja promena na prstu, kao što je ogrebotina ili posekotina, rezultira time da sistem ne prepoznaje otisak i korisnik ostaje bez elektronskog novčanika.

Čekovi predstavljaju rasprostranjeni način bezgotovinskog plaćanja. Zbog toga savremena tehnologija ide u pravcu razvijanja elektronskog čeka čiji je cilj da zameni papirni. Suština nove tehnologije je da korisnik na svom računaru instalira odgovarajući softver, a identifikacija se obavlja preko *PIN*-a i *smart* kartice. Negativna strana ovog sistema je odsustvo mobilnosti, jer se softver i kartica moraju reinstalirati prilikom svake promene mesta boravišta korisnika.

Da bi se ovaj problem prevazišao, razvijen je sistem putem koga se pomenuta transakcija odvija na Internetu, gde je samo potrebno ulogovati se u sistem. Kod ovakvog načina plaćanja, kao prvo, potrebno je da korisnik ima otvoren čekovni račun u banci koja ima zaključen ugovor sa provajderom e-čeka. Korisnik se uloguje putem Interneta u sistem, dobija ček i podatke koje treba da popuni (podaci kao na standardnom čeku), a druge potrebne podatke sistem automatski dodaje. Potpisivanje ovakvog čeka vrši se biometrijom sa otiskom prsta.[175]

6.1.4.6. Kontrola pristupa ličnim uređajima

Jedna od najozbiljnijih bezbednosnih pretnji svim ličnim elektronskim uređajima, kao što su *laptop* ili mobilni telefon, predstavlja njegovo neovlašćeno korišćenje. Danas su lični računarski uređaji u širokoj upotrebi, kako u poslovnom svetu, tako i u državnoj upravi. Lični uređaji nam daju mogućnost da sa sobom ponesemo i određene podatke koji su nam potrebni i da tim podacima možemo pristupiti u svakom trenutku.

[175] *Ibid.*

Zahvaljujući pre svega *Wi-Fi-u* (bežičnoj tehnologiji), lični elektronski uređaji se koriste se, između ostalog, i za primanje i slanje elektronske pošte sa različitih lokacija na kojima se možemo nalaziti. *Wi-Fi* je ugrađen i u skoro sve *smart* mobilne telefone.

Kao što je rečeno, većina ličnih uređaja ima zadatak da vlasniku tokom putovanja omogući primanje i slanje poslovne elektronske pošte, pa ako bi neko drugi imao pristup našem uređaju, to bi moglo dovesti do kompromitovanja poslovnih tajni. Znači da posedovanje ličnog uređaja vuče za sobom i određene rizike u pogledu bezbednosti. Treba voditi računa da nam, kako ove uređaje uvek možemo lako nositi sa sobom prilikom putovanja i rada, lako mogu biti ukradeni. Tehnologija zaštite ličnog uređaja sa otiskom prsta nudi dobro rešenje i za ovaj problem. Iako neovlašćeno lice može doći u posed *laptop*-a, neće moći i da pristupi podacima, jer se neće moći prethodno identifikovati.

Dakle, primenom biometrijske tehnike zasnovane na korišćenju otiska prsta može se znatno povećavati bezbednost ličnih elektronskih uređaja. Senzori za uzimanje otiska prsta se ugrađuju na računare, tastaturu ili gornju površinu, a mogu se praviti u vidu *USB* nadogradnje- modula. Primer uređaja za uzimanje otiska prsta, koji se može naći u sastavu ličnog uređaja, je prikazan na slici 37.

Slika 37 Primer uređaja u okviru ličnog uređaja za uzimanje otiska prsta

Vredi pomenuti, da se poslednjih godina i u automobilskoj industriji primenjuje ova biometrijska tehnika za ulazak u automobile bez konvencionalnog ključa, odnosno sa biometrijskim ključem.

6.1.5. Prednosti i nedostaci biometrijskih sistema sa otiskom prstiju

Otisci prstiju se vekovima koriste za utvrđivanje identiteta, tako da ova tehnologija nije nova za ljude i zbog toga je oni lako prihvataju. Najveća prednost primene ovog sistema ogleda se u tome što je postupak veoma brz i jednostavan, tačnost rada veoma velika- sa veoma malom greškom prilikom očitavanja otiska, a uređaji za uzimanje otiska spadaju među najjeftinije. Sistem zasnovan na otiscima prsta je veoma skalabilan i može imati više hiljada korisnika. Još jedna prednost ove tehnologije je u tome što ne zahteva velike investicione troškove. Zbog svih pomenutih prednosti, biometrijski sistemi sa otiskom prstiju zauzimaju oko 40% tržišta.[176]

Izloženost prstiju dejstvu spoljašnje sredine predstavlja jedan od osnovnih problema sa kojima se susreće ova biometrijska tehnika. Bitan nedostatak ove metode je to što se ona ne može koristiti kod osoba kojima nedostaju prsti ili kod osoba koje imaju određene promene u vidu oštećenja na prstima, na primer kod fizičkih radnika.

Drugi veći nedostatak ove biometrijske metode leži u činjenici da otisak prsta nije teško falsifikovati, niti ga skinuti sa neke površine, bez znanja njegovog vlasnika. Zbog prevazilaženja ovog problema vrše se brojna istraživanja, a akcenat je stavljen na istovremenom merenju temperature prsta, pulsa ili krvnom pritisku ispitivane osobe, a sve to u cilju odbacivanja lažnih karakterističnih detalja.

Treba navesti i određeni otpor koji ljudi pokazuju prema ovoj biometrijskoj tehnici, zbog toga što se otisak prsta tradicionalno koristio za identifikaciju osumnjičenih osoba, odnosno onoga što se često vezuje za policijski rad, pa se osećaju neugodno prilikom primene u svakodnevnim životnim aktivnostima.[177]

[176] Otisak prsta, *op.cit.*
[177] *Ibid.*

Takođe, nedostatak je i u tome što do greške u prihvatanju identiteta može doći i zbog različite pozicije prsta na senzorskoj površini ili pak loše prislonjenog prsta na senzorskoj površini.

6.2. Biometrijski sistemi identifikacije sa slikom lica

Lice predstavlja najvažniji deo čovekovog spoljašnjeg izgleda pomoću kojeg se ljudi međusobno prepoznaju, odnosno razlikuju. Iako svaki čovek poseduje mnogo fizičkih karakteristika i specifičnosti u ponašanju, ono što prvo primetimo kod neke osobe jesu njene crte lica. One su jedinstvene, nepromenljive, karakteristične za svakog čoveka i na osnovu njih se svaka osoba može identifikovati, pa čak i nakon plastične operacije.[178]

Pored toga, na osnovu crta lica možemo saznati i informacije o polu i starosti osobe, porodičnoj pripadnosti (na osnovu sličnosti), emotivnom stanju i trenutnom raspoloženju. Danas se prepoznavanje lica koristi kao metoda biometrijske autentifikacije, koja se sastoji u upoređivanju slike određene osobe sa biometrijskim uzorkom uskladištenim u bazi podataka.

Biometrijska metoda identifikacije prepoznavanjem lica predstavlja deo fizičke biometrije, koja se temelji na jedinstvenim karakteristikama svakog čoveka, u konkretnom slučaju, crtama lica. Osnova ove metode zasniva se na činjenici da svako lice sadrži jedinstveni skup fizičkih karakteristika, koje je moguće izmeriti i upoređivati.[179] Ovaj vid identifikacije se primenjivao i u prošlosti, najviše u policiji koja je za identifikaciju osumnjičenog koristila ranije snimljenu fotografiju lica sa kriminalističkim dosijeom i upoređivala je sa licem osumnjičenog. Ovo je i bio način rada u vreme kada nije postojala računarska tehnologija. Sa pojavom računara manuelan način pretraživanja dosijea i upoređivanja fotografija iz dosijea prestupnika zamenjen je automatizovanim računarskim pretraživanjem i upoređivanjem. Za prepoznavanje ljudskog lica koriste se digitalne fotografije i video snimci u kombinaciji sa računarima sa

[178] M. Savvides, J. Heo, S. W. Park, *Face Recognition*, Handbook of Biometrics, (*eds.* A.K.Jain, P.Flynn,A.A.Ross), Springer, (2008), str. 43.
[179] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics,* Springer, (2011).

instaliranim odgovarajućim softverskim paketima, pa je i dolaženje do identifikacije osumnjičenog brže, pogodnije i sigurnije u odnosu na manuelni način identifikacije koji se ranije koristio.

Krajem XIX i početkom XX veka u policijskoj obradi su se koristile dve metode portretne registracije zasnovane na naučnoj obradi francuskog kriminaliste i tvorca antropometrijskog metoda identifikacije, *Alfonsa Bertijona*[180] i to metoda *ličnog opisa* (fr. *portret parlé* , govorni opis) i metoda *foto–registracije i identifikacije* pomoću takozvane „sinjalektičke fotografije" (tropozna fotografija sa prikazom anfasa, desnog profila i levog poluprofila uz slobodnu proceduru parametara pre vršenja fotografisanja).[181]

Još je 1904. godine Zakonom za merenje, opis i identifikovanje krivaca bila predviđena tzv. *Bertijonova metoda.*[182] Prvi slučaj kada je fotografija korišćena kao dokazno sredstvo u sudu odigrao se još 1864. godine, a i danas se koristi kao dokaz u mnogim krivičnim predmetima, posebno za krivična dela krađe, napada i otmice.[183]

Biometrija zasnovana na crtama lica se najčešće koristi u okruženjima gde je potreban pouzdan, ali i nenametljiv sistem za kontrolu pristupa, kao recimo pristup bankama, osiguravajućim kompanijama, upravnim zgradama kompanija, aerodromima i državnoj administraciji. Veoma često se kombinuje sa automatskim vratima i barijerama, obezbeđujući nesmetan protok ljudi, ali efikasan i jednostavan nadzor.

U javnom sektoru značaj primene biometrije lica se ogleda u prevenciji kriminala, jer primena ove tehnologije pruža mogućnost da se teroristi i kriminalci prepoznaju u masi što je posebno dobilo na značaju nakon

---

[180] *Alfons Bertijon,*francuski policajac i naučnik koji se bavio istraživanjima u oblasti biometrije. Osmislio je prve metode registracije kriminalaca zahvaljujući antropometriji. On je 1950.godine objavio knjigu "*Pravna fotografija"* u kojoj je detaljno opisao kako treba slikati kriminalce i mesta izvršenja krivičnih dela.

[181] V. Mitrović, *Kriminalistička tehnika*, VŠUP Zemun, Beograd, (1990), str. 34 – 44.

[182] R. G. Malenčić, *Tehnička policija i njen rad*, Štamparija Jovanović i Bogdanov, Novi Sad, (1933), str.110.

[183] M. Bromby, *Computerised Facial Recognition*, Systems: The Surrounding Legal Problems, *available on* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1551840, pristupljeno 14.12.2012.

terorističkih napada na Sjedinjene Američke Države 11. septembra 2001. godine.[184]

Ovaj način identifikacije i dalje ostavlja dosta izazova, budući da je lice ipak sklono promenama, a koje su uslovljene bilo prirodnim procesima-starenjem, ali i veštačkim zahvatima, na primer, šminkom, nošenjem naočara ili plastičnom operacijom. Ove promene često predstavljaju veću prepreku u procesu prepoznavanja, posebno kada se radi o velikim bazama podataka.[185]

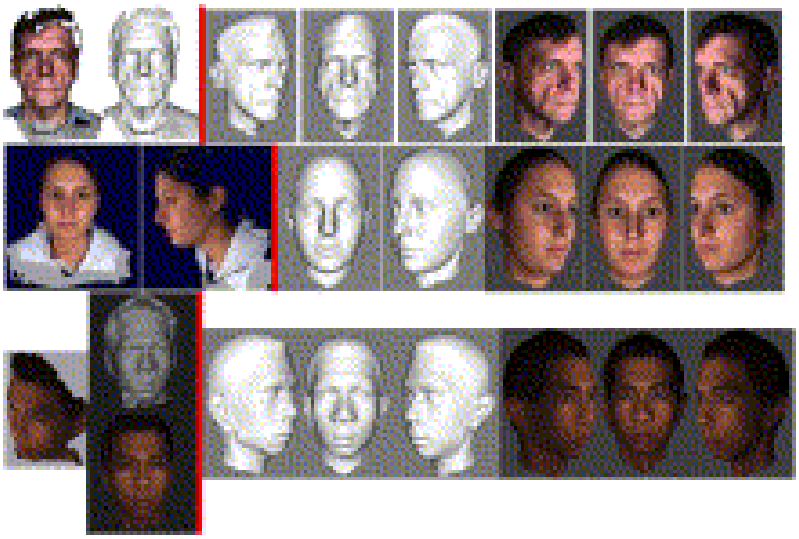
Takođe, veliki problem predstavlja i položaj kamere koja snima lice i osvetljenje scene. Da bi prepoznavanje bilo efikasno kamera prilikom snimanja mora biti na određenoj udaljenosti od glave, glava strogo centrirana prema položaju kamere, kao i da nema varijacija u osvetljenju tokom snimanja lica.[186] Primeri fotografija snimljenih bez pridržavanja pravila o jednolikom osvetljenju lica prikazane su na slici 38, a na slici 39 nalaze se fotografije snimljene bez pridržavanja pravila o jednolikom položaju glave u odnosu na kameru.

Navedeni uslovi sprečavaju široku rasprostranjenost ovih sistema u svakodnevnom životu, budući da se zbog nepridržavanja napred navedenih uslova snimanja češće dolazi do pojave lažnog prihvatanja ili do lažnog odbacivanja identiteta.

Da bi se ovi problemi praktično prevazišli, traže se novi algoritmi koji će otkloniti nepravilnosti u snimanju i tako smanjiti procenat greške. Na primer, neki algoritmi to postižu sa trodimenzionalnom slikom, odnosno sa *3D* tehnologijom, pa se tim putem otklanjaju nedostaci *2D* tehnologije.[187]

[184] *Ibid.*
[185] M. Savvides, J. Heo, S. W. Park, *op.cit*. str. 43.
[186] D. Dessimoz, C. Champod, J. Richiardi, A. Drygajlo, *Multimodal Biometrics for Identity Documents*, *Research Report*, (2005), str. 61.
[187] M. Savvides, J. Heo, S. W. Park, *op.cit*. str. 44.

Slika 38 Fotografije lica pri različitim svetlosnim uslovima



Slika 39 Fotografije lica pri različitim položajima glave

Mehanizam percepcije omogućava ljudima razlikovanje osoba od drugih objekata, a identifikacija razlikovanje od drugih lica. Čovek preko svojih čula vrši uočavanje osoba između drugih objekata na slici, dok računari koriste posebne algoritme za detekciju lica za tu namenu. Proces identifikacije lica se znatno razlikuje kod čoveka i računarskog programa. Stepen tačnosti u prepoznavanju, kada se stavi u odnos ljudsko i računarsko prepoznavanje, može se objasniti uz pomoć primera prikazanog na slici 40, na kojoj se nalaze dve fotografije istog lica, ali sa izmenjenim detaljima slike.

Slika 40 Fotografije lica iste osobe sa izmenjenim detaljima

Na prvi pogled, oko prosečnog čoveka ne bi zapazilo da su u pitanju dve različite osobe. Nasuprot ljudskom načinu prepoznavanja, računarska identifikacija je sasvim drugačija. Ljudski mozak prepoznaje razliku u boji kose, frizuri, nošenju naočara, dok računar, sa druge strane, polazi od matematičkog merenja karakteristika lica, kao što je, recimo, međusobni razmak očiju. Računar vrši proračune koji su precizniji od ljudskog prepoznavanja.[188]

6.2.1. Biometrijske tehnologije za prepoznavanje osoba na osnovu fotografije lica

U ovom delu rada će biće prikazane tehnologije za prepoznavanje lica posmatrane prvenstveno sa aspekta menadžmenta, uz osvrt na ključne detalje same tehnologije. Prikazana je i odgovarajuća arhitektura sistema. Izložene su metode za prepoznavanje lica uz analizu najčešće korišćenih algoritama. Opisano je prepoznavanje lica sa fotografije, video snimka i *3D* snimka.

Primetno je sve veće interesovanje naučne javnosti u pogledu istraživanja crta lica. Ova tehnologija je posebno napredovala u poslednje dve decenije. Začetke njenog razvoja susrećemo još 1960. godine, ali ekspanzija na polju detekcije i prepoznavanja lica se dešava tek u 21. veku.

Prvi sistemi bili su tako dizajnirani da se odredi položaj određenih crta lica na fotografijama, kao što su nos, uši, oči i usta, nakon čega su se vršila potrebna matematička merenja radi upoređivanja. Ovakvi sistemi su se u

[188] *Computerised Facial Recognition, available on* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1551840, pristupljeno 15.12.2012.

velikoj meri oslanjali na ljudski faktor, jer su se merenja vršila ručno, što je predstavljalo najveći nedostatak sistema.[189]

Preokret u razvoju novih biometrijskih tehnologija desio se 1987. godine kada su *Kirby i Sirovich* uveli nov holistički pristup algoritmima za prepoznavanje lica, zasnovanih na uvođenju glavnih komponenti lica, *eigenfaces-a*. Veliki doprinos potom su dali su *Turk i Pentland* 1991. godine, kada su otkrili da upotreba ranije poznate matematičke tehnike vektora sopstvenih vrednosti (engl. *eigenvectors*) može uspešno koristiti za automatsko prepoznavanje lica na slici.[190]

Biometrija lica se može koristiti u procesu verifikacije i identifikacije, s tim što je efikasnija prilikom verifikacije identiteta.

Verifikacija je proces provere nečije tvrdnje o identitetu. Sistem treba da uspostavi određeni stepen sigurnosti da je tvrdnja te osobe tačna kako bi se osobi omogućilo da ostvari određeni cilj, kao što je pristup određenoj lokaciji ili podizanje novca sa bankomata. To je najjednostavniji zadatak koji se postavlja pred ove biometrijske sisteme. Dakle, u ovim slučajevima karakteristike lica se već nalaze u bazi podataka. Kako bi pristup bio odobren, potrebno je da se uzeti biometrijski podatak poklopi sa podatkom uskladištenim u bazi podataka. Sistem kao rezultat procesa prepoznaje, ili ne prepoznaje, korisnika. Prepoznavanje nekog lica je bitno za operativne metode i u borbi protiv terorizma.

Identifikacija predstavlja proces u kome se utvrđuje identitet određene osobe. Ovaj proces je mnogo složeniji u odnosu na proces verifikacije. U ovom procesu sistem upoređuje sliku osobe sa biometrijskim podacima u bazi, kako bi utvrdio njen identitet. Ovde je važno napraviti razliku između *otvorenog* sistema**,** kada ne znamo da li je određeno lice upisano u bazu i *zatvorenog*, kada znamo da je određeno lice sigurno upisano u bazu podataka. U zatvorenim sistemima uzeta slika se upoređuje sa svim slikama u bazi radi dobijanja

[189] *Biometric gov. Face Recognition, available on* http://www.biometrics.gov/Documents/facerec.pdf, pristupljeno 15.12.2012.
[190] *Ibid.*

rezultata. Identifikacija lica preko fotografije u formi dokaza je mnogo složeniji posao, posebno kada se koristi kao dokazno sredstvo u sudskom postupku.[191]

Biometrijska tehnologija prepoznavanja lica je jednostavna ako se pođe od stava da se podaci koji se koriste za identifikaciju mogu lako zahvatiti i potom uporediti sa podacima u bazi podataka.

Međutim, ključna stvar za efikasno funkcionisanje ove tehnologije su dobro odabrani algoritmi. Treba imati u vidu i ranije navedene zahteve u pogledu snimanja, jer efikasnost u prepoznavanju zavisi ne samo od odabranog algoritma, već i od drugih okolnosti, kao recimo od kvaliteta i položaja fotoaparata, varijacija u osvetljenju glave, rotacije glave i slično.

Obično se u literaturi navode tri osnovna načina za zahvatanje ulaznog uzorka lica, pa sledstveno tome i prepoznavanja lica, putem:[192]

- fotografije,
- video snimka,
- 3D tehnologije.

Zbog različitih načina zahvatanja lica, varira i korišćena tehnologija. Dakle, tehnologija sa jedne strane zavisi od toga da li je u pitanju statička ili dinamička slika, a sa druge strane zavisi od aplikacije, odnosno upotrebljenog algoritma.[193]

Algoritmi za prepoznavanje lica mogu se razvrstati prema tri glavna pristupa u predstavljanju lica, kao predmeta rada:[194]

- metod zasnovan na izgledu, odnosno pojavi lica,
- metod zasnovan na prepoznavanju *2D* i *3D* modela lica,
- metod zasnovan na teksturi lica.

[191] *Ibid.*
[192] *Ibid.*
[193] Y.W.Zhao, R.Chellapa, *Image-based Face Recognition, Issues and Methods, available on* http://www.face-rec.org/interesting-papers/General/Chapter_figure.pdf, pristupljeno 14.04.2012.
[194] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Springer, (2011).

6.2.1.1. Metodi zasnovani na izgledu lica

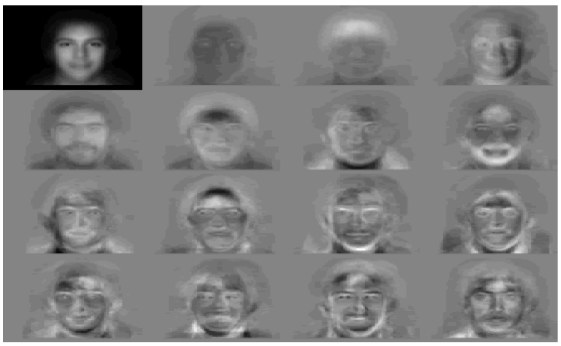
Metodi zasnovani na izgledu su holistički metodi i rade sa prikazom celokupnog izgleda lica.[195] Transformisani celokupan izgled lica dobija se mapiranjem, projektovanjem slike iz visokodimenzionalnog prostora u niskodimenzionalni prostor, predstavljan skupom osnovnih vektora. Mapiranje može biti linearno i nelinearno, a najčešće korišćene šeme su:

- Analiza glavnih komponenti (*engl. Principal Component Analysys, PCA)*,
- Analiza nezavisnih komponenata *(engl. Independent Component Analysys, ICA)*,
- Analiza linearne razlike (*engl. Linear Discriminant Analysys, LDA)*.

Svaki od pomenutih pristupa ima svoj osnovni vektor visokodimenzionalnog prostora vektora lica, koji se zasniva na različitim statističkim pogledima. Kada se vektor lica projektuje na osnovni vektor, dobijeni koeficijent služi za prepoznavanje.

PCA metod koristi koncept glavnih komponenti u postupku prepoznavanja lica. Danas se *PCA* metod najčešće primenjuje, a prvi put su ovaj koncept uveli *Kirby i Sirovich*, a praktično iskoristili *Turk* i *Pentland*. Bazira se na strukturi lica opisanih preko skupa *eigenfaces*-a, karakteristika lica (ili lica duhova!) koje se izdvajaju i služe za upoređivanje.[196] Glavne komponente lica, *eigenfaces*, predstavljene su skupom sopstvenih vektora, *eigenvectors,* koji se koriste za računarsko prepoznavanje ljudskog lica, ilustrovane su na slici 41.

[195] *Ibid.*
[196] *Biometric gov. Face Recognition, op.cit*



Slika 41 Ilustracija primene PCA metode[197]

PCA metod koristi *eigenfaces* algoritme za dimenzionalno smanjivanje, kako bi se izdvojile karakteristike lica potrebne za prepoznavanje. Slike moraju biti iste veličine i normalizovane. Nakon toga se redukuju dimenzije podataka i izdvajaju se one karakteristike koje se mogu uporediti. Svaka slika se može prikazati kao vektor svojstvenih lica u jednodimenzionalnoj mreži. Koristi sopstvene vektore (*eigenvectors*) i sopstvene vrednosti (*eigenvalues*). Umesto baze podataka za smeštaj podataka o licima i slika lica koristi se struktura foldera.[198]

Dakle, potrebno je izdvojiti one karakteristike lica koje se mogu efikasno uporediti. Da bi verovatnoća greške bila 1:1000, potrebno je da na fotografiji prednji, frontalni deo lica bude prikazan u celosti.[199]

Nedostatak opisanog metoda se ogleda u greškama do kojih dolazi zbog varijacija u osvetljenju i promenama izraza lica. Postojeći problemi se mogu prevazići metodom *LDA* o kojoj će dalje biti reči.

ICA metod je sličan *PCA* metodi. Ali, dok *PCA* zahteva ortogonalnu osnovu za nalaženje glavnih komponenti, *ICA* metod nalaženja nezavisnih komponenti se zasniva na neortogonalnoj osnovi, tako da su transformisane karakteristike statistički nezavisne.[200]

---

[197] Turk, M., Pentland, A., *Face recognition using eigenfaces. In: Proceedings of IEEE Computer Vision and Pattern Recognition,* Maui, Hawaii, December (1991), str. 586–590.
[198] Ž. Nikolic, *Prepoznavanje lica primenom analize osnovnih komponenti*, Telekomunikacioni forum TELFOR 2007, Srbija, Beograd, Novembar (2007).
[199] *Biometric gov. Face Recognition, op.cit*
[200] M. Savvides, J. Heo, S. W. Park, *op.cit*. str. 47.

LDA metod koristi statistički pristup za klasifikaciju uzoraka nepoznatih klasa, baziranih na uzorcima poznatih klasa. Cilj primene *LDA* tehnike je da se takvim pristupom poveća razlika među uočenim klasama, a istovremeno smanji razlika unutar instanci klase. Na slici 42, svaki red slika predstavlja klasu u kojoj postoje razlike na licu unutar iste klase. Nedostatak ovakvog pristupa se ogleda u tome što u praksi postoji mali broj probnih uzoraka lica kojima se utvrđuju njegove varijacije.[201]

LDA metod se prilično često koristi za prepoznavanje lica i razvijen je niz modifikacija ovog postupka (*DLDA* varijanta i *Gram-Schmidt LDA (GSLDA)* varijanta. [202]

Slika 42 Prikaz varijacija između šest klasa primenom LDA metoda[203]

Interesantno je napomenuti da nezavisna istraživanja pokazuju da ni jedan od izloženih metoda za prepoznavanje lica (*PCA, ICA i LDA*) nije optimalan u svim uslovima rada, već da izbor najboljeg metoda zavisi od cilja postavljenog sistemu.[204]

6.2.1.2. Metodi zasnovani na modelima lica

Metodi prepoznavanja zasnovani na modelima lica koriste *2D i 3D* modele lica i imaju za cilj da prevaziđu ranije pomenute probleme sa varijacijama izgleda lica. Tri posebno interesantna pristupa, koja koriste *2D i 3D* modele lica,

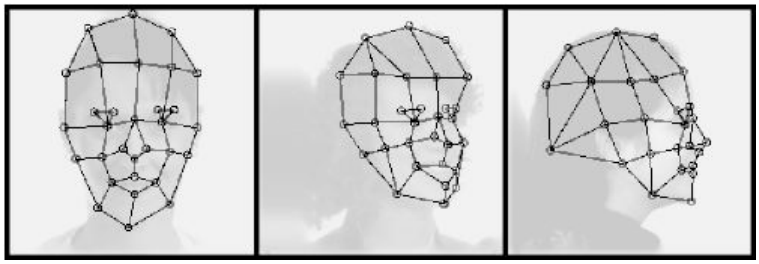
[201] *Biometric gov. Face Recognition, op.cit*
[202] M. Savvides, J. Heo, S. W. Park, *op.cit. str.45*
[203] Juwei Lu, „*Boosting Linear Discriminant Analysis for Facial Recognition*," (2002).
[204] K. Delac, M. Grgic, S. Grgic, *Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set, Int. J. Imaging Systems and Technology 15(5),* (2005), str. 252-260.

su poznata su pod nazivima Upoređivanje grafova elastičnih veza lica (engl. *Elastic Bunch Graph Matching, EBGM*), Model aktivnog izgleda lica (engl. *Active Appearance Model, AMM*) i Podesivi *3D* model lica (engl. *3-D Morphable Model*).[205]

U *EBGM* modelu, lica osoba su, u memoriji računara predstavljena semantičkom mrežom, odnosno odgovarajućim grafovima, slika 43. Čvorovi u takvom grafu reprezentuju karakteristične tačke na licu, kao što su nos oči, usta, a grane grafa služe za predstavljanje elastičnih veza između karakterističnih tačaka lica. Vrednosti atributa grana grafa, posredstvom tehnike talasića (engl. *wavelets*), opisuju međusobne udaljenosti tih karakterističnih tačaka. Da li je upitno lice dovoljno slično nekom licu iz baze podataka, određuje se metodom upoređivanja grafova, odnosno upoređivanjem vrednosti odgovarajućih atributa iz ulaznog grafa i grafa veza karakterističnih tačaka lica iz baze podataka. Značajno je istaći da promena izraza lica, frizure i sl. ne utiču na identifikaciju. Osvetljenje ne predstavlja problem sve dok može da se prepozna lice među objektima na slici.[206]

EBGM model koristi model sa nelinearnim karakteristikama, pa može da odgovori realnim problemima za koji ranije nismo imali dobar odgovor u linearnoj analizi, kao što su varijacije osvetljaja (na primer, mešanje spoljašnje i unutrašnjeg osvetljenja), položaja prilikom slikanja (na primer, uspravan i povinut položaj čoveka) i različiti izrazi lica (osmeh u odnosu na ozbiljnost). *EBGM* metod koristi *Gabor-ov*[207] *filter* za izdvajanje karakteristika i detektovanje oblika. Nedostatak ovog metoda se ogleda u tome što postoje teškoće u postavljanju i lociranju lica, ali se one mogu prevazići primenom *PCA* i *LDA* metode. [208]

[205] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *op.cit.*
[206] *Computerised Facial Recognition, op.cit.*
[207] Mađarski nobelovac Dennis Gabor
[208] *Biometric gov. Face Recognition, op.cit.*



Slika 43 Grafovi pridruženi licu po EBGM metodu[209]

AMM model lica je na osnovu statistike izveden model lica koji objedinjuje model varijacija oblika crta posmatranog lica sa standardizovanim modelom varijacije izgleda lica. [210] Za svako novo lice zadato njegovom slikom treba naći vrednosti parametara standardizovanog modela tako da razlike između slike lica i sintetizovanog modela lica projektovanog na ulaznu sliku lica budu minimalne. Uzorak u bazi podataka sadrži dobijene vrednosti parametara standardizovanog modela varijacije izgleda lica.

Podesivi *3D* model lica umesto dvodimenzionalnog koristi trodimenzionalni prostor za definisanje modela lica. *3D* modeli trebali bi biti mnogo pogodniji od ranije izloženih *2D* modela za realnije predstavljanje situacija koje susrećemo u radu sa ljudskim licem, kao što su crte lica, položaja lica prilikom slikanja (*en face*, poluprofil, profil), osvetljenja. Kao parametri koriste se oblik i tekstura, sa jedne strane, kao i odgovarajući algoritmi sa druge strane.[211]

6.2.1.3. Metodi zasnovani na teksturi lica

Metodi zasnovani na teksturi lica teže da prevaziđu probleme varijacije u osvetljenju, poziciji kamere, odnosno centriranju lica, kao i druge probleme o kojima je u tekstu bilo reci. Primer takvih pristupa su Metod lokalnih binarnih

[209] Laurenz Wiskott, "*Face recognition by Elastic Bunch Graph Matching*, " April (1996).
[210] Xiaoguang.Lu, *Image Analysis for Face Recognition,* Dept. of Computer Science & Engineering, Michigan State University, East Lansing, (2004).
[211] *Ibid*.

obrazaca (engl. *Local Binary Patterns, LBP*) i Metod histograma orijentisanih gradijenata (engl. *Histogram of oriented gradients, HOG*).[212]

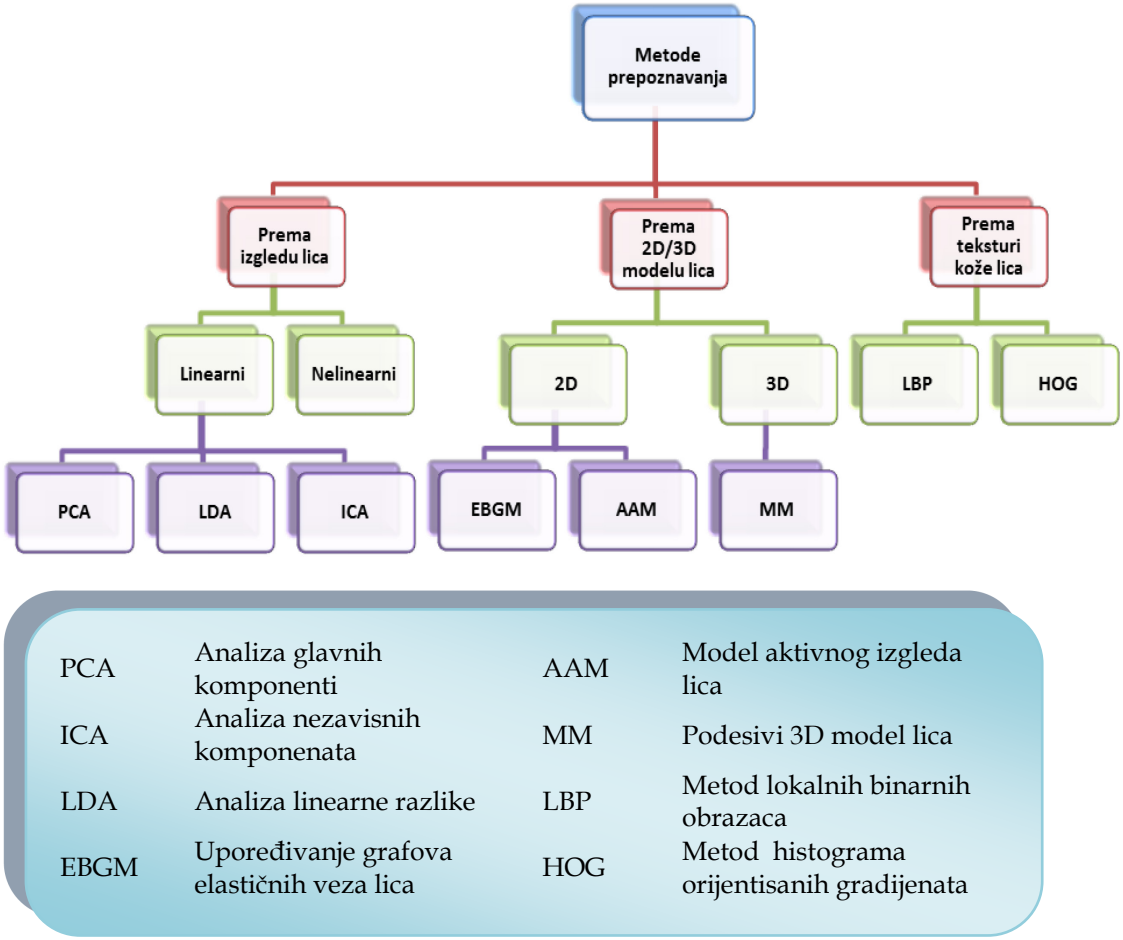
Metod lokalnih binarnih obrazaca, *LBP*, za izvlačenje karakteristika lica u obliku teksture, koristi radije prostor slike, umesto prostora objekta. Tipično je slika lica data u rasterskom formatu, pa se za opis teksture koristi mogućnost nalaženja karakterističnih obrazaca u međusobnom položaju susednih piksela slike. Možemo drugačije reći da se u ovom pristupu vizuelna struktura kože, tekstura, pretvara u brojeve koji se čuvaju u bazi podataka. U postupku identifikacije lica umesto upoređivanja vizuelnih detalja kože lica, upoređuju se brojevi. Treba istaći da su istraživanja pokazala da se preciznost u identifikaciji povećala primenom ovog načina identifikacije.[213] Takođe, treba istaći da kombinovanje *LBP* metode sa histogramom orijentisanih gradijenata u nekim slučajevima značajno unapređuje performanse.[214]

Metod histograma orijentisanih gradijenata, *HOG*, slično svim postupcima koje koriste histogram, formira distribuciju gradijenata intenziteta osvetljaja piksela kako bi opisao pojavu lokalnog obrasca teksture, odnosno oblika. Kako ovaj metod radi u prostor slike, gradijenti intenziteta se izračunavaju imajući u vidu uniformni rasterski format digitalizovane slike lica. Cela slika lica se deli u male povezane regione, i na osnovu vrednosti intenziteta osvetljaja piksela koji pripadaju regionu određuje se histogram, odnosno deskriptor slike lica.

Na slici 44 dat je integralan prikaz svih izloženih postupaka za prepoznavanje lica, odnosno klasifikacija metoda prepoznavanje lica. Ipak, i pored nespornog napretka, prepoznavanje osobe samo na osnovu slike njenog lica i dalje ima ograničenu upotrebu. U svetu se vrše brojna istraživanja sa ciljem da se osmisle i naprave nove generacije algoritama, kojima bi se

[212] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *op.cit.*
[213] M. Pietikäinen, G.Zhao, A. Hadid, *available on* http://www.comp.hkbu.edu.hk/~icpr06/tutorials/Pietikainen.html, pristupljeno 13.03.2013.
[214] Xiaoyu Wang, Tony X. Han, Shuicheng Yan, "*An HOG-LBP Human Detector with Partial Occlusion Handling*", ICCV (2009).

prevazišli postojeći problemi i koji bi bili znatno efikasniji u prepoznavanju lica. Pouzdanost sistema za prepoznavanje lica zavisi ne samo od odabranog metoda rada i kvaliteta slika lica, već i od demografskih karakteristika populacije koja koristi ovakav sistem. Istraživanja su pokazala da je lakše prepoznati muškarce nego žene, kao i da je lakše prepoznati starije nego mlađe ljude. Takođe, zapaženo je pouzdanost prepoznavanja lica opada od trenutka upisivanja slike lica, *faceprint*-a, u bazu podataka, što zajedno sa već navedenim nedostacima, čini raspoloživu tehnologiju prepoznavanja lica manje preciznom u poređenju sa tehnologijom prepoznavanja osobe na osnovu irisa ili izložene tehnologije prepoznavanja osoba na otiska prsta, *fingerprint*-a.



Slika 44 Klasifikacija metoda prepoznavanja lica na osnovu slike lica

6.2.2. Ostale biometrijske tehnologije za prepoznavanje lica

Biometrijske tehnologije za prepoznavanje lica na osnovu video zapisa su u poslednje vreme postale posebno interesantne zbog mogućnosti istovremenog daljinskog uzimanja više biometrijskih karakteristika više ljudi u posmatranom prostoru, a da se pritom ljudi ne ometaju u njihovim aktivnostima.[215]

Prepoznavanje lica snimljenog video-kamerom predstavlja, takođe, jedan od načina da se prevaziđu neki od opisanih problema, kao što je, na primer, varijacija osvetljenja. Ipak, treba reći da su ovi sistemi još u razvoju, mada se vrše se brojna istraživanja.

Na primer, pomenimo da je vlada Sjedinjenih Američkih Država finansirala projekat *Multiple Biometric Grand Challenge (MBGC)*, koji je imao za cilj kombinovanje biometrijskih podataka prikupljenih na daljinu, kao što su podaci potrebni za prepoznavanje osobe na osnovu hoda, sa konvencionalno prikupljenim biometrijskim podacima.[216]

Međutim, kod prepoznavanja na osnovu video zapisa postoje brojna ograničenja, koja smanjuju efektivnost i efikasnost ove klase biometrijskih sistema. Recimo, potrebno je da arhitektura sistema bude takva da omogući lociranje lica na video zapisu u situaciji kada se u kadru nalaze i brojni objekti. Ovi sistemi su limitirani i u pogledu veličine slike, što sužava mogućnosti izbora algoritma za prepoznavanje osobe na osnovu slike lica. Ekstraktovane slike lica su veoma male, tako da često nije ispunjen uslov da slika ima 90 *piksela*, a što nameće standard *ISO/IEC 19794-5*.[217]

Imajući u vidu, napred pomenuta ograničenja, može se zaključiti da je potrebno sprovesti još mnogo istraživačkog napora kako bi se usavršila faza detekcije lica, odnosno normalizacije ekstraktovane slike lica.

---

[215] S. Paunović, L. Nešić, J.Kovačević, *Biometrical identification via facial photography*, Međunarodni naučni skup „Dani Arčibalda Rajsa“, Beograd (2013).
[216] *Facial Recognition Technology, op.cit.*
[217] *Ibid.*

Pored postojećih tehnologija za prepoznavanje lica, u razvoju su i biometrijske tehnologije zasnovane na fotogrametriji i stereofotogrametriji, kao što su *3D* fotogrametrijska antropologija i *3D* facijalna rekonstrukcija.[218]

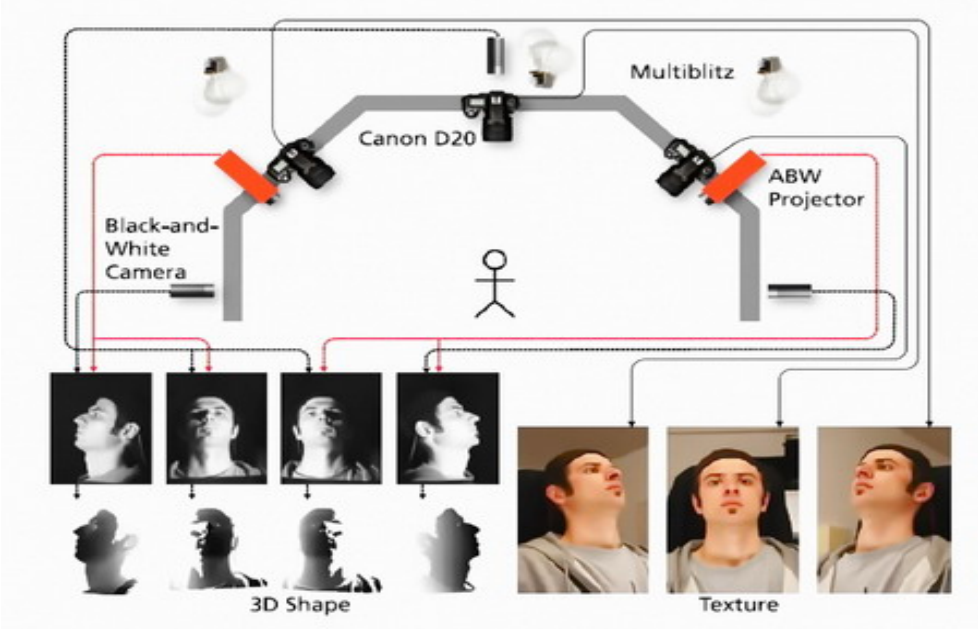
Za kriminalistiku je veoma značajna metoda *3D* fotogrametrijska antropologija, koja se zasniva na prepoznavanju i identifikovanju određenih osoba iz snimaka zabeleženih kamerom, na primer preko sistema video nadzora.[219] Velika vizuelna sličnost digitalne slike lica i glave sa stvarnim izgledom osobe, pa time i licem, može se postići *3D* facijalnom rekonstrukcijom. Međutim, ova metoda nije naročito pouzdana, jer se zasniva na subjektivnoj proceni osobe koja vrši facijalnu rekonstrukciju.

Računarska aplikacija *3D* facijalnu rekonstrukciju lica osobe formira na osnovu izgleda kostura lica i oblika i konture glave.

Prvo se vrši detaljno snimanje lobanje, a nakon toga se vrše merenja određenih tačaka na licu i lobanji. Pod pomenutim merenjima podrazumeva se izračunavanje udaljenosti svake tačke na lobanji i tako se izrađuje digitalni model glave.

Prilikom identifikacije *CT* snimak glave osobe koja se identifikuje stavlja se u superpoziciju, odnosno preklapa se, sa izrađenim digitalnim modelom. Radi simuliranja konačnog izgleda lica dodaje se meko tkivo na lobanju i dobija osnova spoljašnjeg izgleda lica, da bi se zatim na osnovu određenih karakteristika i potrebne procene odredila boja kože, izgled očiju, kose i drugih detalja izgleda.[220] *3D* fotogrametrijski proces rekonstrukcije lica osobe prikazan je na slici 45.

[218] Ž. Radmilović, *Biometrijska identifikacija*, (2008), objavljeno http://www.mup.hr/UserDocsImages/PA/onkd/3_4_2008/radmilovic.pdf, pristupljeno 15.12.2012.
[219] *Ibid.*
[220] *Ibid*.



Slika 45 3D fotogrametrijski proces rekonstrukcije lica[221]

6.2.3. Metodologija rada sa biometrijskim sistemima za identifikaciju osoba na osnovu slike lica

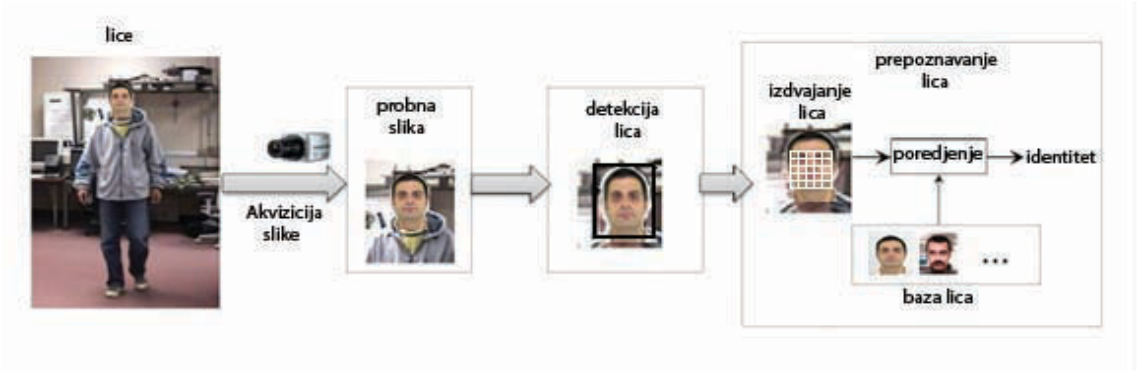
Proces identifikacije osobe na osnovu slike lica započinje uzimanjem odgovarajućeg biometrijskog podatka- fotografisanjem lica. Uzeti biometrijski podatak se potom obrađuje kako bi se priredio za upoređivanje sa ranije uzetim biometrijskim podatkom posmatrane osobe. Uzimanje biometrijskog podataka je proces u kome uređaj za skeniranje prihvata podatke koji se odnose na lice osobe, procesira ih, vrši kompresiju i u skladu sa odbranom strukturom podataka, templejtom, strukturira ih radi pripreme za upis u bazu. Nakon toga vrši upis biometrijskog uzorka, bilo u lokalnu bazu podataka, bilo u centralnu bazu ili na lokalni prenosni uređaj (na primer, *smart* karticu). Kada je u pitanju biometrija crta lica, navedeni proces se ponavlja uzimanjem nekoliko slika posmatrane osobe i dobijeni podaci se unose u bazu kako bi se formirala baza uzoraka lica ili *faceprint*[222]. Preporučuje se da se slike uzimaju sa blago različitim uglovima koji zatvaraju normala na lice i os koja prolazi kroz centar kamere.

[221] Stan Zi Li, Anil K.Jain, *Handbook of Face recognition*, second edition, Springer (2011).
[222] *Faceprint* (niz brojeva koji predstavljaju lice u bazi podataka).

Već je ranije rečeno da se uzimanje slike lica određene osobe može uraditi sa znanjem, ali i bez znanja te osobe, pa se u tome ogleda i atraktivnost ovog sistema u slučajevima nadzora. Uzimanje potrebnog biometrijskog uzorka se može vršiti na osnovu fotografije ili video zapisa. Ovaj postupak je jednostavan, ako ga vrše ljudi, ali ne i za slučaj računarske aplikacije! Rad sa video zapisima, zbog njegove dinamičke prirode, je prilično zahtevan. Aplikacija prvo treba da analizira snimljenu scenu sa ciljem da otkrije lice i njegov položaj na sceni. Programskim putem se pretražuje kadar koji generiše video-kamera, i to tako što se lice najpre traži u niskoj rezoluciji, a nakon toga, ako se pronađe oblik u vidu lica, kamera se prebacuje na režim rada sa visokom rezolucijom. Treba imati u vidu da je mnogo lakše locirati lice na fotografiji iz pasoša nego u nekoj drugoj sredini kada je potrebno osobu izdvojiti od drugih objekata. [223]

Tipičan sistem za prepoznavanje osoba na osnovu lica, prikazan na slici 46, obuhvata tri modula kojima se vrši: [224]

- uzimanje podataka,
- detekcija lica, i
- upoređivanje.



Slika 46 Faze rada biometrijskog sistema identifikacije na osnovu lica

[223] *Facial Recognition Technology, op.cit.*
[224] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Springer, (2011).

Nakon što smo preko akvizicionog uređaja došli do fotografije dela tela osobe sa obuhvaćenim licem, probna slika na slici 46, proces prepoznavanja se nastavlja izvršavanjem nekoliko sukcesivnih faza obrade slike:

- detekcija lica,
- podešavanje ili poravnanje slike,
- izdvajanje tražene karakteristike,
- poređenje izdvojene karakteristike lica sa uskladištenim karakteristikama u bazi karakteristika.

Detekcija i poravnanje su koraci koji prethode fazi prepoznavanja, dok se u fazi prepoznavanja vrši izdvajanja karakteristika i njeno upoređivanja sa uskladištenim karakteristikama lica.[225]

Prvi korak u obradi akviririane slike je detekcija, korak kojim se lice izdvaja iz pozadine fotografije. U slučaju video zapisa detekcija lica će se izvršiti korišćenjem komponente za praćenje lica (*engl. face tracking*).[226]

Nakon toga sledi drugi korak, faza poravnanja ili podešavanja, u kojem se određuju veličina i položaj lica u odnosu na kameru. Potrebno je da lice bude okrenuto ne više od 40 stepeni prema kameri, kako bi sistem uspeo da ga registruje i analizira. Najveći broj sistema za prepoznavanje lica vrši prepoznavanje na osnovu tzv. *mirne slike.* Pod *mirnom slikom* se podrazumeva frontalna fotografija lica, sa uobičajenim izrazom lica. *Mirna slika* u odnosu na korišćenje *žive slike* smanjuje veličinu numeričkog koda kojim se slika lica predstavlja u bazi podataka.[227]

U fazi prepoznavanja sistem treba da izdvoji potrebne karakteristike lica. Locirati lice i izdvojiti tražene karakteristike je ključna stvar za efikasan rad svakog biometrijskog sistema. Proces počinje koracima normalizacije i lokalizacije.

[225] Stan Z. Li Anil K. Jain, *Handbook of Face Recognition*, Springer, (2011).
[226] *Ibid.*
[227] Marios Savvides, Jingu Heo, Sung Won Park, *Face recognition*, Handbook of biometrics, Springer, (2008), str 45.

Normalizacija predstavlja izuzetno važan korak u ovoj fazi. Vrši se standardizacija akviririrane slike u smislu njene veličine, poze i osvetljenja, u odnosu na slike koje se čuvaju u bazi podataka. Cilj normalizacije je da se uzeta slika transformiše u format sa kojima radi baza slika, kako bi se izvršile pripreme za poređenje.[228]

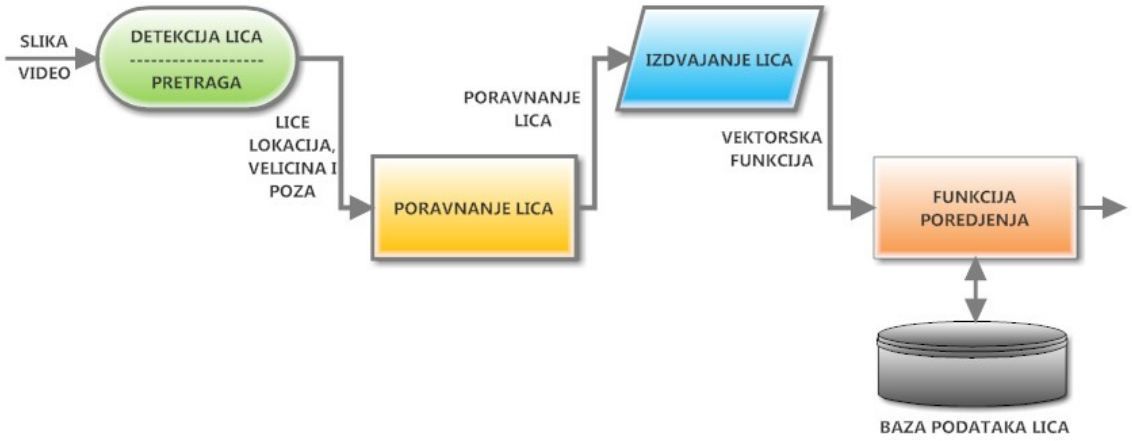
Dakle, u ovoj fazi treba normalizovati frontalnu sliku, da bi se dobila *mirna slika*. To je statistička tehnika korekcije ili umanjivanja razlika u licu istog čoveka na različitim slikama. Ova korekcija se sprovodi sa ciljem smanjivanja razlika između različitih slika lica. Normalizacija slike lica se vrši uz poštovanje fotometrijskih osobina, kao što su osvetljenje i sive boje.[229]

Lokalizacija karakteristika lica, kao sto su oči, nos i usta, vrši se uz pomoć tačaka za lokalizaciju, dok se normalizacija vrši imajući u vidu geometrijske osobine, kao što su veličina i poza. Konačnom rezultatu prethodi *kodiranje,* proces u kojem se *2D* frontalna slika pretvara u digitalni kod pogodan za dalju upotrebu. Dakle, algoritam konvertuje lice osobe u otisak lica, uzorak, i tipično se izdvaja u formi vektora.

Nakon toga se vrši *upoređivanje* tako uzetog uzorka sa uzorkom uskladištenim u bazi podataka. Uzeti podaci se mogu koristiti kao filter, ako smo prethodno sortirali bazu podataka lica po različitim vrednostima mogućih karakteristika lica, pa se u tom slučaju brzo pronalaze uzorci u bazi sa zadatim stepenom podudaranja.

Važno je znati da rezultati prepoznavanja ne zavise samo od izdvojenih karakteristika lica predstavljenih uzorkom, već i od kvaliteta uzimanja uzorka, algoritama za transformaciju slike, načina izdvajanja lica, postupaka klasifikacije i poređenja uzoraka, tako da u svakom konkretnom biometrijskom sistemu za prepoznavanje osoba na osnovu lica postoji veći broj faktora koji utiču na rezultat prepoznavanja (blok dijagram 3).[230]

[228] *Facial Recognition Technology, op.cit.*
[229] Stan Z. Li Anil K. Jain, *op.cit*.
[230] *Ibid.*



Blok dijagram 3 Faktori uticaja na rezultat prepoznavanja

6.2.4. Primena sistema za identifikaciju na osnovu slike lica

U ovom delu će biti reči o primeni biometrije lica i značaju primene, kako u javnom, tako i u privatnom sektoru. Analiza je rađena prema oblastima primene. Obrađene su samo pojedine oblasti, jer zbog širokog polja primene nije bilo moguće analizirati sve.

Biometrija lica se tradicionalno koristi za zvanična dokumenta, kao što su pasoši, vozačke dozvole i lične karte. Prvi korisnici sistema za prepoznavanje lica bili su policija i sudovi. Danas se ova tehnologija primenjuje na različitim poljima društvenog života i to na graničnim prelazima, kod fizičkog pristupa određenim lokacijama i podacima, prilikom novčanih transakcija....

6.2.4.1. Bezbedonosni nadzor u policiji i pravosuđu

Bezbedonosni nadzor za potrebe policije i pravosuđa zasnovan na tehnikama sa biometrijom lica posebno je značajan u borbi protiv terorizma i kriminala, pa se iz tog razloga najviše primenjuje u istrazi, odnosno radi pronalaženja osumnjičenih u masi potencijalnih osumnjičenih. Policija putem ove biometrijske tehnike vrši nadzor nad određenim prostorom tako što proverava identitet određenog lica u masi ljudi, pa je zato veoma značajna u borbi protiv terorizma.

Dosadašnja iskustva svedoče o uspešnom korišćenju ove biometrijske tehnike u istražnim radnjama, kada je reč o potrazi za kriminalcima, osumnjičenim teroristima i nestalom decom. Naime, prepoznavanje osobe na osnovu lica može da se izvrši iz daleka i bez neposrednog kontakta sa osobom, tako da ona nije ni svesna da se prati radi identifikacije.

Takođe, značajno je istaći da primena ove metode omogućava veoma efikasno i brzo prepoznavanje huligana na fudbalskim utakmicama ili prevaranata u kockarnicama.

Posebno je korisna kod zatvorske uprave, kao i kod kontrole baze podataka osuđenika. Ova biometrija se koristi i prilikom sastavljanja profila nepoznatog počinioca, na osnovu kojeg se nakon toga pretražuje baza slika lica.

6.2.4.2. Primena na graničnim prelazima

Ova biometrija tehnika pruža efikasnu bezbednosnu kontrolu na graničnim prelazima. Naime, na graničnim prelazima postoje dva stuba kontrole, i to kontrola čitanjem podataka iz pasoša, na osnovu kojih se utvrđuje elektronski profil uz, recimo, skeniranje irisa ili otiska prsta.

Čitanje biometrijskih podataka iz pasoša obuhvata i optičku biometriju, koja se sastoji u skeniranju pohranjene digitalne slike i potom očitavanja ličnih podataka iz baze podataka. Veoma je značajna na aerodromima, kada se traži visok stepen sigurnosti prilikom provere identiteta, jer je reč o veoma osetljivim bezbedonosnim pitanjima. Važno je napomenuti da primena ove biometrijske tehnologije ne pruža samo visoku sigurnost u vezi provere identiteta putnika, već i visok nivo efikasnosti na graničnim prelazima i aerodromima, jer omogućava brzo utvrđivanje stvarnog identiteta.

U većini zemalja, pogranične službe koriste sistem za prepoznavanje lica koji funkcioniše tako što sistem poredi lice nosioca putne isprave sa slikom pohranjenom u mikročipu njegovog e-pasoša i na osnovu takvog upoređivanja utvrđuje da li je nosilac pasoša pravi vlasnik ili ne.

6.2.4.3. Obezbeđenje fizičkog pristupa određenim lokacijama, objektima, podacima i ličnim uređajima

U cilju obezbeđenja pristupa zaštićenim lokacijama, kao što su vojni i policijski objekti, banke i sefovi, primenjuje se ova biometrijska tehnologija. Primena biometrije lica omogućava efikasniji, sigurniji i ekonomičniji pristup ličnim uređajima, kao što su laptopovi ili mobilni telefoni, budući da je pristup takvim uređajima uslovljen prethodnim podudaranjem u poređenju uzetog biometrijskog uzorka sa uzorkom zapisanim u bazi podataka. Ilustracije radi, uz pomoć ove biometrije, umesto ukucavanja lozinke u laptop-u dovoljno je da nam kamera ugrađena u laptop snimi lice, uporedi ga sa ranije pohranjenim podatkom u laptop-u i u slučaju podudaranja omogući dalji pristup resursima uređaja.

Autentifikacijom korisnika pruža se veća sigurnost i prilikom pristupa određenim informacijama, pa vlade često koriste ovu biometriju kako bi ograničile pristup logičkim resursima sistema samo licima sa potrebnim privilegijama. Posebno je značajna za pristup informacijama u policiji i vojsci, odnosno na poljima gde postoji veća potreba za bezbednošću.

6.2.4.4. Obezbeđenje finansijskih servisa

U savremenoj poslovnoj interakciji, identifikacija preko lica klijenta je veoma značajna za bezbedan rad finansijskih servisa, na primer, pristup bankomatima ili bankarskim trezorima, radi smanjenja mogućnosti zloupotreba od strane kradljivaca identiteta i hakera, koji mogu ukrasti lozinku i identifikacioni lični broj, *PIN*, i potom ih zloupotrebiti.

6.2.4.5. Ostale primene

Ne manje značajna je i primena ove biometrijske metode na izborima. Naime, dešavalo se da se glasači registruju u biračke spiskove pod različitim imenima, kako bi mogli da glasaju više puta. Primenom identifikacione biometrijske metode sa prepoznavanjem lica glasača onemogućen je ovaj vid zloupotrebe. Primera radi, u Meksiku je 2000. godine korišćen *Visionics Facelet* sistem za borbu protiv lažiranja izbora. Ovaj sistem je funkcionisao tako što je

analizirao bazu podataka slika sa registrovanim glasačkim karticama i identifikovao duplikate. [231]

Slična tehnologija se koristi i u Sjedinjenim Američkim Državama radi sprečavanja lica da imaju više identifikacionih kartica, odnosno vozačkih dozvola.

6.2.5. Prednosti i nedostaci biometrijskih sistema sa slikom lica

Kako bi se doneo pravilan zaključak o praktičnom značaju ove biometrijske grane važno je analizirati polja primene, sa jedne strane, a sa druge strane njene prednosti i nedostatke u odnosu na konkurentske metode identifikacije.

Jedna od bitnih prednosti ove biometrijske tehnike u odnosu na ostale ogleda se u tome što se u postupku akvizicije uzorka ne zahteva neposredan kontakt sa osobom, tako da se ne ometa rad i postupanje ispitanika tokom uzimanja uzorka, a u nekim slučajevima pojedinac nije ni svestan da se vrši određivanje njegovog identiteta.[232]

Primena ove biometrijske discipline može uticati preventivno na smanjenje stope kriminala kada ljudi postanu svesni da će kao osumnjičene, službe za nadzor moći da ih prepoznaju i u masi ljudi, budući da pravilno dizajniran sistem može prepoznati pojedinca ne samo na aerodromima, već i na drugim mestima, kao što su stadioni ili pešačke zone na ulicama.

Postoje baze podataka koje mogu da obuhvate veliki procenat stanovništva, kao što je recimo baza podataka za vozačke dozvole u Sjedinjenim Američkim Državama, koja pokriva oko 95% odraslog stanovništva.[233]

Generalno, u poređenju sa ostalim biometrijskim metodama, ljudi imaju manju odbojnost kada je u pitanju ova biometrija zbog jednostavnog načina uzimanja uzorka, pa je i lakše prihvataju, nego biometriju zasnovanu na skeniranju oka.

---

[231] *Stan Z. Li Anil K. Jain, op.cit..*
[232] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Springer, (2011).
[233] *Ibid.*

Drugi razlog, koji joj ide u prilog, je i taj što se identifikacija i ranije primarno vršila uzimanjem fotografija. Ljudi već imaju iskustva sa takvim načinom identifikacije, tako da ne pružaju otpor. Takođe, važno je reći da osobe ne osećaju strah zbog mogućih posledica akvizicije uzoraka na zdravstveno stanje, kao što je slučaj kod skeniranja mrežnjače ili mogućih kožnih bolesti, kao što je slučaj kod biometrije otiska prsta.

Sve je veća zainteresovanost u svetu za primenu ove biometrijske tehnike, posebno na Internetu, konkretno radi pristupa određenim aplikacijama na mreži, kao što je to slučaj, na primer, sa *Facebook*-om.[234]

Ali, pored napred navedenih prednosti, ovaj biometrijski metod pokazuje i više nedostataka, koji ograničavaju njegovu praktičnu upotrebljivost. Pre svega, tehnologija koju koristi ovaj metod je dovoljno precizna za verifikaciju prijavljenog identiteta, odnosno autentifikaciju, ali može biti nedovoljna u postupku identifikacije.

Performanse posmatranog biometrijskog sistema zavise i od konkretnog izgleda lica osobe, na primer, od upotrebe šminke, naočara, drugačije frizure, a poseban problem predstavljaju teškoće u uočavanju razlika kod provere blizanaca.

Takođe, jedan od bitnih nedostataka je to što lice osobina čoveka nije vremenski invarijantna biometrijska osobina, za razliku, na primer, od šarenice oka. Kao posledica promena tokom vremena, lice nije toliko jedinstveno i zbog toga je stepen sigurnosti u procesu prepoznavanja niži. Kako bi se postigao viši stepen sigurnosti, preporučljivo je ovaj metod kombinovati sa drugim biometrijskim tehnologijama.

Prepoznavanje preko fotografije je dosta efikasno i brzo, ali je postupak identifikacije u prekršajnoprocesnom ili krivičnoprocesnom postupku težak i naporan posao, kada je neophodno izvršiti identifikaciju anatomskih obeležja po modifikovanom Bertijonovom sistemu, što ne dovodi uvek do povoljnih

[234] *Ibid.*

rezultata usled primene kamera nedovoljne rezolucije i neprilagođenih uglova snimanja.

Da bi se dobio sistem sa dobrim performansama u procesu identifikacije, ova biometrijska tehnika zahteva, već ranije opisanu, značajnu saradnju osobe sa tehničkim osobljem u procesu akvizicije uzorka, što ne ide u prilog ranije iznete tvrdnje da ova metode ne uznemirava ljude tokom uzimanja uzorka.

U nekim slučajevima čak je onemogućeno uzimanje lica kao biometrijskog podatka! To je slučaj kod određenih grupa ljudi u Indiji koji smatraju da slikanje krade njihovu dušu ili pak u mnogim zemljama u kojima žene zbog verskih zabrana nose veo.

Biometrijski sistem prepoznavanja lica je, kao i ostali sistemi, sklon napadima u cilju kompromitovanja. Najlakši i najjednostavniji napad uljeza na sistem u procesu akvizicije tako što se umesto fotografije čoveka-napadača, u sistem unese fotografije lica koje ima pravo pristupa sistemu. To je i logično jer je fotografija takvog lica uglavnom dostupna javnosti.

Na primer, fotografisanje poznatih ličnosti, ne samo na javnom, već i na privatnom posedu, koje vrše *paparaci*. Ljudi, često, sami svoje fotografije čine javno dostupnim publikovanjem, na primer, na društvenim mrežama.

Sistemi koji koriste video-monitoring su takođe skloni napadu. Posebno iz razloga što emitovanje podmetnutog video zapisa, u elektronskoj komunikaciji koji koristi sistem video nadzora, može biti identično očekivanom snimku uživo- u realnom vremenu određenog korisnika.

Sa druge strane, uvođenjem *3D* sistema smanjuje se rizik od navedenih napada, ali i ovi sistemi imaju nedostatak koji se manifestuje u nedostatku fiziološke informacije.[235]

[235] K. Delac, M. Grgic, S. Grgic, *Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set,* Int. J. Imaging Systems and Technology 15(5), (2005), str. 252-260.

6.3. Biometrijski sistemi identifikacije sa glasovnim zapisom

6.3.1 Osnov rada sistema identifikacije sa glasovnim zapisom

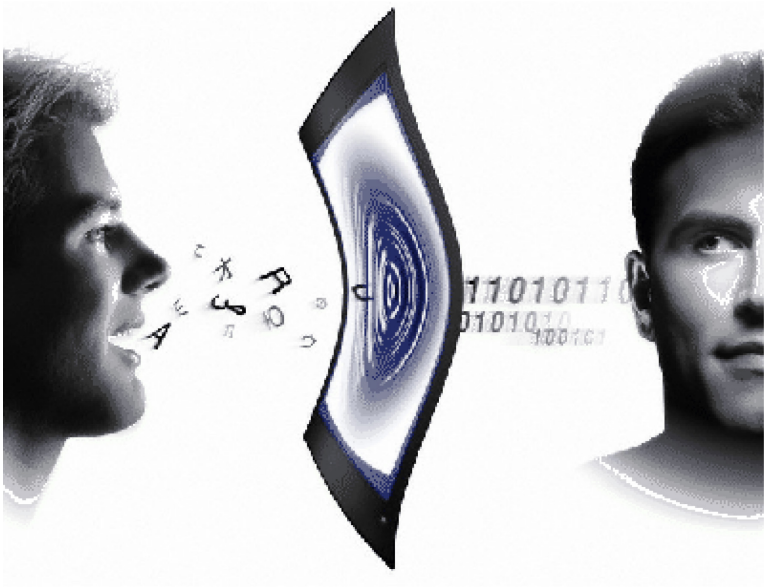
Analiza specifičnih karakteristika govora započeta je još pre ere tranzistora i prvih elektronskih računara. Melvil Bel, otac Aleksandra Bela, još je 1867. godine započeo sa istraživanjem na prevođenju govora u vizuelnu formu. Kao fonetičar, Melvil Bel, bavio se problemom vizuelizacije glasova kako bi pomogao gluvim osobama da nauče da govore i osobama sa smetnjama u govornom aparatu.[236]

Međutim, u tom trenutku raspoloživa tehnologija nije bila dovoljna, pa nije mogla da na adekvatan način podrži ovu ideju. Kasnije se u policiji nastavilo sa razvojem ideje Melvila Bela. Kako se nova tehnologija tranzistora i čipova od pedesetih godina prošlog veka decenijama razvijala i napredovala. Danas imamo kvalitetna softverska rešenja koja omogućavaju vizualizaciju govora.

Biometrija glasa koristi biometrijski model fizičkih karakteristika ljudskog glasa, odnosno numerički model generisanog zvuka i načina izgovora, grafički ilustrovan na slici 47, a koji je karakterističan za svakog pojedinca.[237]

Kada govorimo o identifikaciji putem generisanog zvuka, potrebno je istaći razliku između prepoznavanja govora i prepoznavanja glasa, odnosno govornika. Prepoznavanje govora se svodi na prepoznavanje izgovorenih reči, odnosno transformaciju govornih signala u reči jezika, dok biometrijski metod prepoznavanja na osnovu glasa u stvari predstavlja jedan od načina identifikacije govornika, odnosno prepoznavanje onog ko je izgovorio te reči.[238]

[236] Judith Felson Duchan, *The Phonetic Notation System of Melville Bell and its Role in the History of Phonetics*, Journal of Speech-Language Pathology and Audiology - Vol. 30, No. 1, Spring (2006).
[237] Lisa Myers "*An Exploration of Voice Biometrics*" Information Security Reading room, SANS Institute, (2004).
[238] S. Paunović, L. Nešić, J.Kovačević, *Application of Voice Biometrics in Protection Systems and Crime Fighting,* Journal of Information Technology and Applications (JITA), Banja Luka, BiH, (2012).



Slika 47 Numerički model načina izgovora i generisanog zvuka

Svrha prepoznavanja glasa je autentifikacija određene osobe na osnovu jedinstvenih glasovnih karakteristika, obzirom na to da glas predstavlja unikatan i nepromenljiv identifikator.[239] Jedinstvenost se sa jedne strane, ogleda u tome što se glas kod ljudi razlikuje po visini, jačini i boji, a sa druge strane, razlikuje se način verbalizacije odnosno izražavanja reči zbog različitog načina upotrebe mišića vokalnog trakta, usta, jezika i vilice. Nijedna osoba na svetu ne može da promeni svoj glas do potpune neprepoznatljivosti. Zanimljivo je istaći da čak i kod jednojajčanih blizanaca govor nije identičan zbog automatizovanih govornih navika. U prilog jedinstvenosti ističe se i to da ljudi na različite načine artikulišu glasove, prave pauze u govoru, koriste poštapalice koje umeću umesto pauze, način započinjanja govora, brzina i ritam govora, intonacija, sve su to pojave koje su neretko presudne u identifikaciji govornika.

Biometrija glasa se sve češće primenjuje u javnom i privatnom sektoru, imajući u vidu da je jednostavna za upotrebu, prihvatljiva od strane građana i ekonomski pogodnija, jer ima mogućnost implementacije po znatno nižoj ceni u odnosu na ostale biometrijske tehnologije. Sa druge strane, ova biometrija nije naročito pouzdana, pa se iz tog razloga prvenstveno koristi u verifikacione, a

[239] Carnet Hrvatska akademska i istraživačka mreža, Biometrija CCERT-PUBDOC-2006-09-167.

ne u identifikacione svrhe. Dakle, koristi se i kao dopunska biometrija, odnosno u kombinaciji sa nekom drugom biometrijskom metodom.

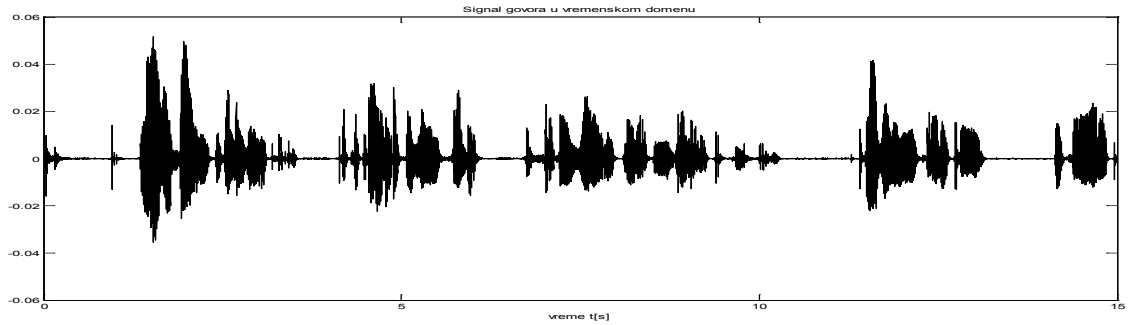
6.3.2. Sistemi identifikacije na osnovu glasovnih zapisa

Tehnologija biometrije glasa najmanje je nametljiva, ali istovremeno i najmanje pouzdana od razmatranih tehnologija. U praksi, prepoznavanje govornika na osnovu karakteristika njegovog glasa često se svodi na postupak u kojem govornik prvo izgovori u mikrofon neku od poznatih rečenica- *fraza*, a nakon toga softver vrši analizu generisanog zvučnog signala- *glasa*, upoređivanjem izgovorene fraze sa postojećim ranije memorisanim uzorkom u bazi.[240]

Dakle, proces identifikacije ima dve jasno definisane faze. Prva faza je upisivanje glasovnog uzorka govornika, a druga je verifikacija, odnosno identifikacija govornika. Zadatak prve faze se sastoji u uzimanju biometrijskog uzorka, "*otiska glasa*". Kao što je rečeno, uzorak glasa može biti izgovor neke fraze, teksta ili niza brojeva, koji se potom zapišu u bazu podataka i koji služe za identifikaciju određenog lica u drugoj fazi rada sistema. Dakle, govornik izgovara određenu frazu u mikrofon. Mikrofon je taj ulazni senzor, koji generisani akustički talas pretvara u električni signal. U mikroelektronskim komponentama koje se nalaze na zvučnim karticama, konkretno uz pomoć *A/D* (*Analogno-Digitalnih*) konvertora, ovaj analogni električni signal se pretvara u vremenski niz binarnih brojeva, kako bi se prilagodio za rad sa centralnim procesorom i mnogostrukim aplikacijama. Obično se pritom zahvaćeni zvuk filtrira u određenom frekvencijskom opsegu, vrši se normalizacija amplitude u interval vrednosti, na primer, od -1 do 1, kvantizuje u odgovarajući broj kvantizacionih nivoa, i tako redom. Konačno, kada je akustični signal reprezentovan vremenskim nizom brojeva, moguće je primeniti veliki broj sofisticiranih postupaka kako bi se signala izvuklo sve ono što je značajno i

[240] V. Vasković, M. Todorović, *Tehnologije biometrijskih plaćanja*, Beogradska Poslovna Škola, Beograd, (2008).

korisno sa stanovišta krajnjeg cilja, a potisnulo sve ono što je nepotrebno i neinformativno, primer sa slike 48.



Slika 48 Snimak govornog signala u trajanju od 15 sek, sa periodom odabiranja 8KHz

Algoritam za analizu posmatranih osobina glasa u uzetom uzorku, kao što su, visina, jačina, ton, trajanje glasa i slično, izdvaja jedinstvene karakteristike glasa, pa nakon određivanja tih vrednosti formira biometrijski uzorak koji skladišti u bazu glasovnih podataka. Postupak traje kratko, obično od 2 do 8 sekundi. Dakle, u ovoj fazi, izgovorena fraza se pretvara iz analognog u digitalni format koji se čuva u bazi i služi za buduća poređenja. Sledeća faza rada sistema se odvija tokom verifikacije, odnosno identifikacije. Potrebno je da ispitivani pojedinac nešto izgovori, a zatim se tako uzeti glasovni uzorak upoređuje sa uzorkom sačuvanim u bazi podataka. U praksi, ispitanik ispred mikrofona čita određeni tekst ili seriju brojeva. Obrada zahvaćenog uzorka je veoma kratka, reda sekunde. Sistemi koji se primenjuju za prepoznavanje glasa i identifikaciju govornika mogu se podeliti na zavisne, nezavisne i integrisane sisteme.

Kod zavisnog sistema, govornik izgovara unapred određeni tekst, koji se nakon toga poredi sa uzorkom iz baze. Dakle, govornik izgovara ili čita specifične reči, odnosno izgovara određenu frazu. Pod frazom se, recimo, podrazumeva izgovor imena, grada rođenja, omiljene boje ili recimo niz određenih brojeva. Veoma je jednostavna za korišćenje, jer je za identifikaciju dovoljno upoređivanje izgovorene fraze, lozinke, sa onom sačuvanoj u bazi.

Za razliku od ovog sistema, nezavisni sistem analizira samo kvalitet glasa, a izgovoreni tekst nema uticaja na proces identifikacije. Dakle, ovde se ne zahteva izgovaranje određene reči, već se prepoznavanje može izvršiti izgovorom bilo kojih reči. Zapravo, ovde se radi o izgovaranju upitnog teksta. Preciznije, autentifikacija pomoću upitnog teksta sastoji se u tome što osoba izgovara specifičan tekst, primera radi, niz brojeva od 0 do 9, pri čemu se upitni tekst posebno generiše, recimo sa: "Molim vas izgovorite 33 56 87". Interesantno je naglasiti da postoji specifičnost u izgovoru broja deset u poređenju sa nizom brojeva od 0 do 9, a što se mora imati u vidu prilikom projektovanja ovih sistema, u cilju sigurnije i brze identifikacije govornika.

Verifikacija govornika u integrisanom sistemu se odvija u dva koraka: sistem za identifikaciju govora prvo prepozna neki tekst (lozinku, lične informacije ili broj) koji je izgovoren, a nakon toga se vrši upoređivanje karakteristika glasa ispitanika u sistemu za identifikaciju govornika. Ovaj sistem se najčešće primenjuje kod bankovnih transakcija.

Uzmimo, kao primer, *ViaVoice* softverski proizvod kompanije *IBM*, koji omogućava verifikaciju korisnika putem telefona, i to kombinovanjem dva izvora informacija – karakteristika glasa korisnika, engl. *voiceprint*, i znanje korisnika (lozinka i lične informacije). U toku konverzacije, *ViaVoice* postavlja korisniku slučajna pitanja. Zatim ide provera tako dobijenih odgovora, kao i njegovog "*voiceprint*"-a. Kada se uzeti uzorak poklopi sa uzorkom u bazi, *ViaVoice* zaključuje da je reč o pravom korisniku. Ono što je važno istaći, a tiče se pre svega korisnika, odnosi se na vremensko trajanje pomenute provere.

Naime, trajanje identifikacije zavisi od tačnosti odgovora i procene "*voiceprint*"-a korisnika. Logično je, kada je u pitanju pravi korisnik, da identifikacija traje veoma kratko, jer se proces sastoji od postavljanja samo jednog pitanja. Novo pitanje sledi u situacijama kada sistem ne može pouzdano da izvede pozitivan zaključak ili ako je u pitanju lažno predstavljanje. U koliko dođe do pokušaja prevare sistema, provera traje znatno duže iz razloga što tada

ViaVoice postavlja više pitanja sve dok prevarant ne da pogrešan odgovor ili *ViaVoice* ne zaključi da su glasovi definitivno različiti.

Poslednjih godina, zahvaljujući tehnološkim inovacijama, biometrija glasa se sve više unapređuje. Naime, ranije je bilo potrebno da se svaka reč izgovara razgovetno i odvojeno, kako bi sistem mogao da izvrši prepoznavanje. Danas to nije neophodno jer novi sistemi omogućavaju prepoznavanje govornika i u slučajevima kada se ne prave pauze između izgovorenih reči, u režimu kontinuiranog ili tečnog govora. Računarska aplikacija pritom može i da prepoznaje izgovorene reči i prikazuje ih na monitoru, odnosno preslikava glas u tekstualni zapis, čak i kada se priča veoma brzo, na primer, i do 160 reči u minuti. Takođe, važno je istaći da neki sistemi uspešno rade i sa neuronskim mrežama, koje "pamte" kako svaka osoba izgovara reči i na taj način se smanjuje mogućnost grešaka u prepoznavanju. Ipak, greške u izvođenju zaključaka su neminovne jer biometrijski postupci koriste do izvesne mere precizan matematički model fizičke osobine.

6.3.3. Primena sistema za identifikaciju sa glasovnim zapisom

Imajući u vidu prethodno opisane karakteristike biometrije sa glasovnim zapisom, nije začuđujuće što je široko polje njene primene. Ova biometrija se koristi za obezbeđenje fizičkog pristupa lokacijama i objektima, za pristup ličnim uređajima, pri obavljanju konvencionalnih ili elektronskih transakcija, u službama bezbednosti, policiji, prilikom sprovođenja sudskih odluka, ali i u mnogim drugim poljima.

6.3.3.1. Fizički pristup određenim lokacijama i objektima

Za fizički pristup određenoj lokaciji, ili za ulazak u određeni objekat, koristi se "uzorak glasa", najčešće u kombinaciji sa drugim modelima identifikacije, kao što su šifre, biometrija otiska prsta ili irisa, čime se postiže maksimalna bezbednost.

Primera radi, često se za ulazak u neki zaštićeni objekat, kao što su objekti službe bezbednosti, banke, poslovni ili stambeni kompleksi, koristi ova

biometrija tehnologija. Lica koja nameravaju da uđu u zaštićeni objekat izgovaraju određenu frazu ili odgovaraju na pitanje, a zatim se uzorak njihovog glasa poredi sa uzorkom u bazi. Samo u koliko se na osnovu glasovnog zapisa u bazi prepozna ulazni uzorak, licu će biti omogućen ulaz.

6.3.3.2. Sigurniji i brži pristup ličnim uređajima

Implementacija ove biometrijske tehnike u mobilne telefone, *laptop*-ove i druge lične uređaje je izuzetno značajna jer pruža visok nivo zaštite pomenutih uređaja od zloupotrebe neovlašćenih lica. Zloupotrebe mogu biti sprečene tako što bi pristup nekom od pomenutih uređaja uslovili izgovorom određene fraze. Kada vlasnik izgovori frazu, sistem će ga prepoznati i on će bez problema moći da koristi neki od pomenutih uređaja. Međutim, ukoliko neko neovlašćeno pokuša da pristupi takvom uređaju, sistem ga neće prepoznati i odbiće mu pristup. Ovakav način je lakši i brži od korišćenja lozinki, prosto iz razloga što nam ukucavanje lozinke oduzima vreme, a možemo je i zaboraviti. Zapisivanje lozinke lako može da kompromituje sistem zaštite!

Savremeni *smart* telefoni imaju mogućnost rada sa govornim komandama i na taj način omogućavaju rad sa telefonom bez kontakta sa tastaturom. Ilustracije radi, kada želimo nekog da pozovemo, umesto ukucavanja broja telefona, dovoljno je da kažemo ime osobe koju želimo da pozovemo. Telefon će prepoznati ime iz memorije i nazvati tu osobu.

6.3.3.3. Novčane transakcije na bankomatima

Biometrija glasa ima praktičnu primenu na bankomatima, jer se može smanjiti broj zloupotreba. Naime, prilikom podizanja gotovine na bankomatu, autentifikujemo se putem ličnog broja, *PIN*-a. Šta se dešava u koliko neko vidi *PIN* koji ukucavamo ili ako je na bankomatu uljez ugradio kameru koja snima tastaturu za vreme ukucavanja? To može biti kamera ugrađena na reklamnu kutiju na bankomatu. Naravno, kartica se može zloupotrebiti. Pomenuti načini zloupotrebe *PIN*-a određene osobe su jednostavni za izvođenje i prilično česti, a njihov broj se može smanjiti tako što bi se prilikom identifikacije korisnika sa *PIN* brojem primenjivao i ovaj biometrijski metod. Dakle, sistem bi prvo morao

da identifikuje osobu koja namerava da podigne novac, bilo izgovorom određene fraze ili odgovorom na određena pitanja, pa bi joj, uz kombinaciju sa ukucavanjem *PIN*-a, bilo omogućeno podizanje novca. Ovakav način podizanja novca ne oduzima mnogo vremena, a istovremeno pruža mnogo veću sigurnost. Veoma važno polje primene ove tehnologije je kod telefonskog bankarstva koje je u poslednje vreme zbog jednostavnosti u razvoju. U savremenom svetu većina banaka ima pozivne centre, kao i sisteme koji se baziraju na automatskom prepoznavanju glasa primenom ove biometrije. Ukratko, telefonsko bankarstvo predstavlja obavljanje platnog prometa (transfer novca, transakcije sa vrednosnim papirima i slične transakcije) na bazi instrukcija klijenta preko transakcionog računa i to tako što klijent ili stupa u kontakt sa službenikom banke i tako inicira operacije na računaru banke ili uspostavlja direktnu vezu sa računarskim centrom banke.[241]

6.3.3.4. Službe bezbednosti

Značajno polje primene ove tehnologije je u službama bezbednosti, bilo javnim, bilo tajnim. Jedna od primena je, svakako, praćenje upotrebe telefonskih linija u cilju nadzora saobraćaja. Ovo je jako značajno jer su danas klasični načini praćenja slabo primenljivi. Da bi se operaterima olakšao posao praćenja, računar simultano prati veći broj telefonskih linija sve do pojave ključnih reči na nekoj od njih. Kada se te reči pojave, snimljeni razgovor se prosleđuje ljudskom operateru kako bi proverio sadržaj razgovora. Značajno je istaći da ukoliko se očekuje razgovor sa određenom osobom, onda se takvi sistemi kombinuju sa automatskim prepoznavanjem govornika i na taj način se povećava sigurnost identifikovanja tražene osobe.[242]

6.3.3.5. Identifikovanje osumnjičenog, istraga i sprovođenje sudskih odluka

Korišćenje ove biometrije veoma je značajno kod sprovođenja istražnih radnji, jer daje mogućnost da se putem snimljenog glasa identifikuje

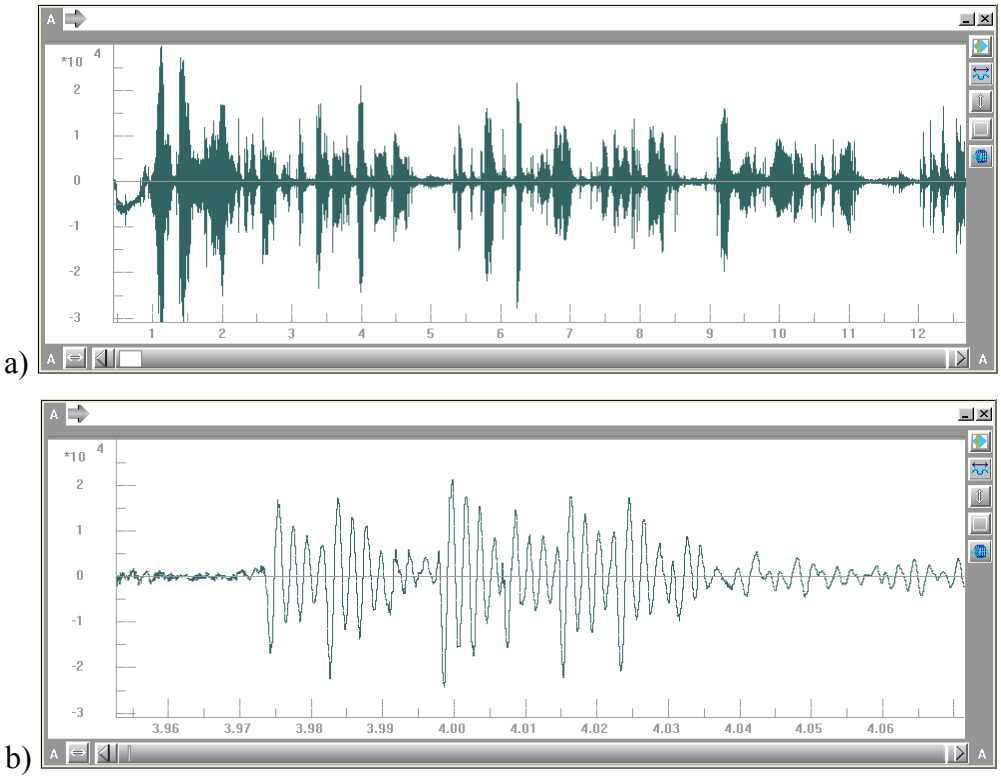
[241] http://www.cbmn.org/slike_i_fajlovi/fajlovi/fajlovi_press_centar/magistarski_gordana_dedeic.pdf, pristupljeno dana 18.010.2013.
[242] Davor Petrinović, *Digitalna obrada govora*, Fakultet elektrotehnike i računarstva, Zagreb, (2002).

osumnjičeni. Kada otmičar, recimo, pozove policiju i zatraži nekakve uslove, snimljeni glas postaje dokaz na osnovu kojeg stručnjak za veštačenje uspeva da otkrije kriminalca. Takođe, njen značaj se posebno izdvaja u slučajevima kidnapovanja, ucena, pretećih poziva, podvala i lažnih dojava telefonskim putem, snimaka na traci, digitalnih zapisa govora i transkripata govora. Ovde se uglavnom koristi zavisni sistem, a važno je razviti i dobre mehanizme za filtriranje informacija zbog postojanja velikog broja podataka.

Forenzika koristi i biometriju identifikacije putem glasa kako bi utvrdila identitet izvršioca krivičnog dela. Treba naglasiti da je ova forenzička disciplina u poređenju sa ostalim, u kojima se koriste druge biometrijske tehnike, najsloženija, jer je, na primer, otisak prsta uvek isti, trajan i nepromenljiv, za razliku od govora na koji se može svesno uticati.

Za razliku od prethodno pomenutih primena identifikacije govornika, gde se identifikacija dopušta i sa određenom verovatnoćom greške u odlučivanju, kod forenzičke identifikacije govornika greške nisu dopustive. Iz tih razloga, postupak glasovne identifikacije nije moguće u potpunosti automatizovati, odnosno prepustiti mašini da donosi odluke. U ovom slučaju, računari su samo pomoćno sredstvo koje čovek koristi da bi došao do zaključka. Da bi se glasovni zapis mogao koristiti u sudskom postupku kao dokaz, neophodno je uočiti i predočiti govorne karakteristike glasa sa spornog snimka, i uporediti ih sa govornim karakteristikama glasa sa nespornog snimka. To se postiže sprovođenjem određenih analiza: auditivno lingvističko-fonetskih i instrumentalnih, odnosno računarskih analiza. Auditivne lingvističko-fonetske analize sprovodi fonetičar i sastoje se iz određivanja govornih karakteristika sa ciljem uočavanja: patoloških pojava, govornih mana, postojanja česte upotrebe poštapalica i uzrečica, pripadnosti određenom govornom području na osnovu izgovora određenih reči, na primer, akcentovanja. Rezultat ove analize se oslanja na znanje i iskustvo stručnjaka i subjektivnog je karaktera. Ilustracija oscilogramskog prikaza signala govora, sa uvećanjem određenog vremenskog fragmenta, data je na slici 49. U zavisnosti

od načina digitalizacije potrebno je oba snimka koja se porede (sporni i nesporni) pravilno podesiti, kako bi bili istih ili sličnih karakteristika.[243]

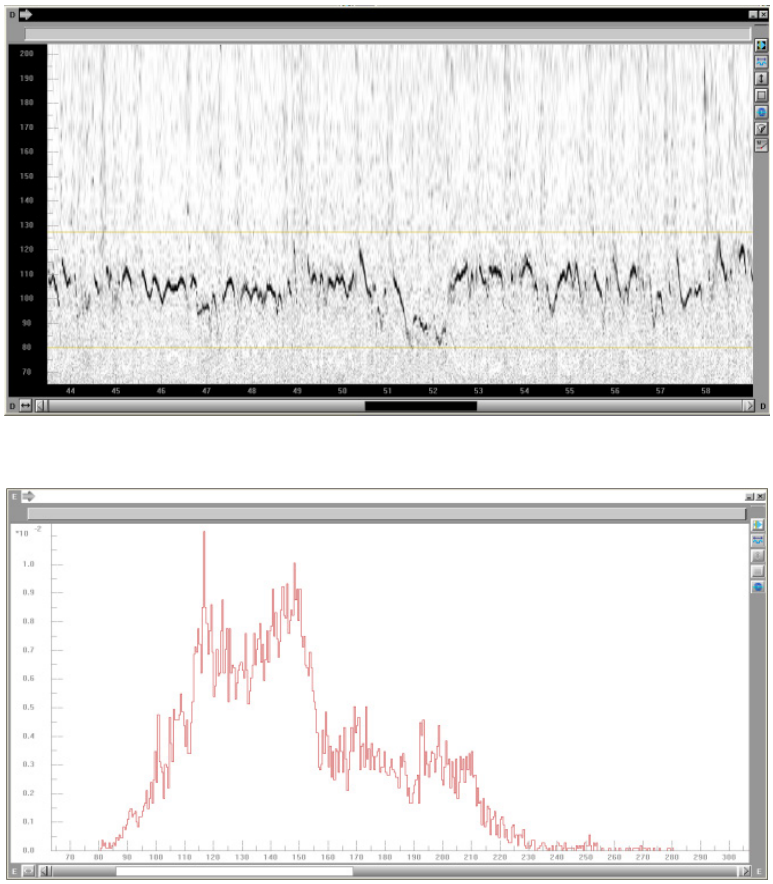


Slika 49 a) Oscilogramski prikaz signala govora u trajanju od 12 sekundi b) Uvećani deo snimka u trajanju od 1 sekunde

Instrumentalne analize sprovodi inženjer, korišćenjem savremene tehnologije, najčešće podržane računarom, odnosno adekvatnim softverom. Zapis glasa koji dolazi na obradu je uglavnom digitalizovan, a ukoliko nije, potrebno ga je prethodno digitalizovati.

Sve operacije koje se sprovode tokom instrumentalne analize, sprovode se korišćenjem posebnog softvera prilagođenog za forenzičku identifikaciju govornika. Nakon prilagođavanja snimaka, vrši se određivanje osnovne učestanosti glasa govornika sa snimaka i međusobno upoređivanje. Primer određivanja osnovne učestanosti glasa govornika je dat na slici 50.

[243] Ovde je reč o karakteristikama snimka – snimljenog signala, a ne o karakteristikama glasa govornika.



Slika 50 Određivanje osnovne učestanosti govornog signala

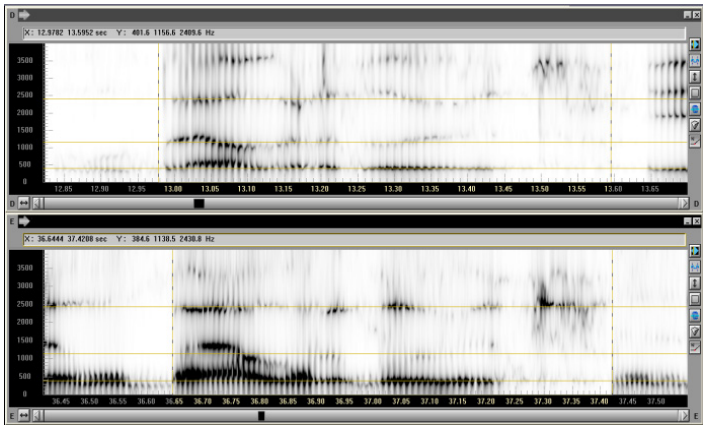
Nakon što smo odredili osnovnu učestanost glasa govornika, korisno je posmatrati spektrogram signala, odnosno tzv. "*digitalni otisak glasa*", kako bi poredili formantne vrednosti i oblike formanata određenih sličnih, ili istih, reči i glasova na spornom i nespornom snimku, slika 51.

Sve instrumentalne analize zasnovane su na primeni Furije-ovih transformacija, koje su osnov za transformaciju signala iz vremenskog u frekventni ili spektralni domen. Sličan postupak analize sprovodi se i kod automatizovanih sistema za prepoznavanje govornika, s tom razlikom što se kod forenzičkog identifikovanja govornika odluka prepušta stručnjaku, a kod automatizovanih sistema odluku samostalno donosi računar.

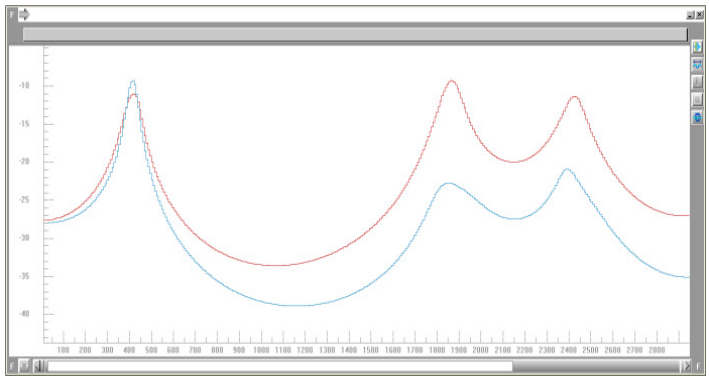
Važno je istaći da je neophodan pristanak osumnjičenog za sprovođenje ove metode, jer je potrebna njegova voljna saradnja. Da bi uzorak glasa koji se

uzima od osumnjičenog bio adekvatan za analizu, potrebno je da uzorak obuhvata sve govorne karakteristike, drugim rečima potrebno je snimiti način izgovora svih glasova, akcenat, opseg govornih sposobnosti, snimiti glas u određenim emotivnim stanjima i drugo. Zato se u postupku uzorkovanja sprovode tri načina snimanja. Prvo se osumnjičenom daje da pročita određeni tekst, potom ponavlja rečenice koje mu se diktiraju, a koje su izdvojene kao podobne za analizu, i na kraju se radi sa spontanim govorom kako bi se dobio uzorak glasa u najprirodnijoj situaciji.

a)



b)



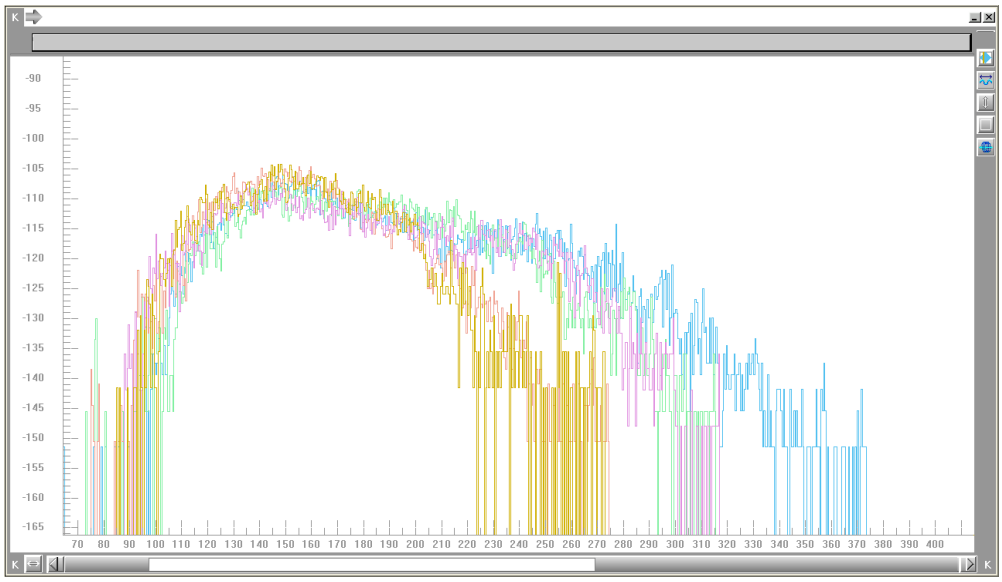
Slika 51 a) Spektrogram jedne izgovorene rečenice spornog i nespornog snimka b) Usrednjeni spektar prva tri formanta glasa I

Prilikom analize koriste se različiti markeri, ali se visina glasa ne može uzeti kao osnov za zaključivanje da su u pitanju iste osobe, jer se visina glasa menja u zavisnosti od situacije. Navedimo realan primer: kamera je u večernjim časovima zabeležila lopova pri izvršenju pljačke. Na snimku je registrovan

visok ton njegovog glasa.[244] Nakon njegovog privođenja u policiju, glas mu je bio nizak jer je bio umoran i uplašen. Dakle, visina glasa nije element putem koga se može sa sigurnošću zaključiti da se radi o istoj osobi. Važno je naglasiti da i u slučajevima kada pronađemo sličnost u visini glasa, ona ne može automatski poslužiti kao dokaz, imajući u vidu da se radi o različitim situacijama. Drugi primer: Visok glas imaju i osumnjičeni i osoba koja je uzbuđena, s tim što u prvom slučaju, razlog toga je prevara koju vrši, a u drugom, razlog je uzbuđenje. Ako posmatramo promenu osnovne učestanosti glasa iste osobe u različitim situacijama, slika 52, možemo reći da postoje određene razlike, ali i velike sličnosti. Zato se osnovna učestanost može koristiti kao parametar za dokazivanje sličnosti, ali ne može biti jedini. Iz tih razloga se sprovodi više analiza i posmatraju različite karakteristike glasa.

Važno utvrditi i sadržaj izgovorenih reči, posebno kada je snimak lošeg kvaliteta ili kada se radi o osobi sa stranim akcentom. Prilikom identifikacije bitno je otkloniti i prisustvo drugih zvukova, kao što su plakanje, lajanje, disanje i ostali šumovi i smetnje. Zanimljivo je istaći da forenzičari prilikom analize upoređuju i opisuju glasove u kontekstu jezičkih jedinica, a naročito samoglasnika i suglasnika. Recimo, forenzički fonetičar može zaključiti da je samoglasnik „I" različit u dva uzorka ili da je u oba uzorka suglasnik „T" proizveden na specifičan način. Uzeti materijal forenzičari analiziraju sa jezičkog stanovišta, ali i sa stanovišta nejezičkih karakteristika, a sve u cilju utvrđivanja kvaliteta glasa, tona, visine, intenziteta, frekvencije, jačine, učestalosti, kao i kvaliteta govora. U kvalitet govora se ubraja izgovor, akcenat, govorni glasovi, kao što su suglasnici i samoglasnici. Takođe, ubrajaju se i suglasnici koji se proizvode zaustavljanjem struje vazduha, kao što su *p, t, k, b, d* i *g,* naglašavanje, intonacija i slično.

[244] Policijska akademija www.kpa.ed.rs, (2012), pregledano 22.01.2013. godine.



Slika 52 Histogrami osnovne učestanosti glasa iste osobe snimljeni u različitim situacijama

Takođe, potrebno je istaći primenu ove biometrijske metode i u oblasti sprovođenja sudskih odluka, na primer, kod uslovno puštenih osuđenika. Uslovno pušteni osuđenici su obavezni da se „*jave*“ telefonom do određenog vremena kako bi potvrdili svoje prisustvo na određenom mestu. U Luizijani, Sjedinjene Američke Države, osobe na uslovnoj slobodi su u obavezi da se u tačno određeno vreme telefonom jave službenom licu i izgovore određenu frazu kako bi potvrdili svoje prisustvo na određenom mestu, a računar utvrđuje identitet pozivaoca.

6.3.3.6. Elektronska kupovina i novčane transakcije

U razvijenim državama se sve više primenjuje sistem plaćanja bez kartice. To omogućava brže obavljanje transakcija i ne zahteva mnogo vremena, ali i stvara veći rizik od zloupotreba. Primenom biometrijske tehnike sa glasovnim zapisom smanjen je procenat zloupotrebe u slučaju *online* kupovine. Naime, u savremenom svetu sve se češće primenjuje ovaj način kupovine budući da ona ne zahteva vreme za odlazak u kupovinu, već se kupovina može vršiti “*iz fotelje*”, i često je povoljnija u odnosu na kupovinu u tradicionalnim trgovinama.

Međutim, ovakav način kupovine nosi sa sobom i rizike, a jedan od njih je mogućnost zloupotrebe kartice, što znači da neko može neovlašćeno da dođe u posed naše, recimo *Visa* kartice i na taj način izvrši *online* kupovinu. Ovaj problem kompanija *Visa* je rešila tako što je uvela primenu biometrije glasa prilikom ovog načina kupovine. Konkretno, vlasnik *Visa* kartice mora da izgovori određenu frazu u mikrofon na svom računaru radi potvrde identiteta. Tek nakon potvrdnog odgovora biće omogućena *online* kupovina. Takođe, *Visa* kompanija je omogućila korisnicima njenih usluga i pogodnosti promene lozinke telefonskim putem što za rezultat ima obostranu uštedu kako vremena tako i novca.

Interesantan je primer i mogućeg unapređenja kupovine preko *E-Bay* aukcijske *web* stranice za *online* kupovinu. Korisnik usluga na ovom sajtu se mora pridržavati jasno određenih pravila ako želi da licitira ili odmah kupi neki predmet, u protivnom će mu biti onemogućeno korišćenje servisa. Međutim, na ovaj način problem nije rešen, jer neko može otvoriti i drugi nalog putem kojeg će ponovo dobiti pristup ovom sajtu. Primenom ove biometrijske tehnike napred opisani problem bi mogao veoma lako biti rešen i tako što bi se od korisnika zahtevalo izgovaranje određene fraze u mikrofon radi registracije. Dakle, korisnik bi pristup određenim Internet servisima imao samo u koliko bi sistem dao pozitivan odgovor, odnosno ukoliko bi prepoznao datog korisnika. Primenom ovakvog načina registracije, broj zloupotreba bi bio znatno smanjen na mnogim Internet servisima slične namene.

6.3.3.7. Primena glasovne biometrije u automobilskoj industriji

Pored već pomenutih *smart* mobilnih telefona, drugi primer masovne primene *smart* tehnologija su savremeni automobili. Dodatna oprema može da obuhvati *FM* radio, *CD*, klima-uređaj, grejanje, ventilaciju, kao i razne elektronske podizače, kao što su prozori, svetla, sedišta. Raspoložive tehnologije danas pružaju mogućnost da se u automobile ugradi i satelitska navigacija koja vozača vodi do traženog mesta, ugradnju telefonske i Internet veze i raznih sistema za zabavu, kao što su *TV*, *DVD*, video igre i drugo.

Međutim, važno je napomenuti da ovakve dodatne uređaje nije preporučljivo manuelno podešavati tokom vožnje, jer oduzimaju pažnju vozaču i mogu prouzrokovati saobraćajne nezgode. Upotreba ovakvih uređaja uz pomoć glasovnih komandi omogućava vozaču da i dalje koristi vid i ruke za pravilno upravljanje automobilom.

Ova biometrijska tehnika se može primeniti umesto kartice prilikom ulaska ili izlaska iz garaže: izgovaranjem određene fraze se postiže mnogo sigurniji i brži način od provlačenja kartice, koja se pri tome još i lako može izgubiti ili oštetiti.

6.3.3.8. Primena glasovne biometrije u obrazovanju

U Sjedinjenim Američkim Državama ova biometrija je počela da se od 2007. primenjuje i u školama, kod distribucije obroka – užina, tako što đaci izgovaraju svoje ime i identifikacioni broj.

6.3.3.9. Primena glasovne biometrije u poslovnom svetu

Primenom glasovne biometrije može da se povećava produktivnost rada zaposlenih u kompanijama, a samim tim i profit kompanija. Kada pišemo određeni izveštaj ili obrađujemo tekst, to činimo kucanjem dirki na tastaturi računara. Tako šaljemo i elektronsku poštu. Takvi poslovi, naravno, zahtevaju određeno vreme. Primenom ove biometrijske tehnologije u navedenim slučajevima postiže se veća efikasnost, jer se štedi vreme potrebno za neku od pomenutih radnji, obzirom da je mnogo brže i lakše diktirati tekst, nego ga kucati. Istraživanja su pokazala da bi se sa korišćenjem ove metode vreme od 18 minuta koje je u proseku potrebno za kucanje 900 reči smanjilo na 6,5 minuta.[245]

Neke kompanije kao što je, recimo *Bell Canada,* zaposlenima omogućavaju pristup određenim podacima proverom identiteta zaposlenog putem telefonskog poziva. Znači, primenom ove biometrije u konkretnom slučaju zaposleni nisu vezani za laptop, preko koga su ranije jedino mogli da

[245] Dragon Naturally Speaking Review, *available on* www.dragonnaturallyspeakingreview.com, pristupljeno 22.01.2013.

pristupe podacima, već podacima mogu pristupiti brže i sigurnije putem telefonskog poziva.

Jedna od navedenih prednosti se može ilustrovati u narednom primeru. Zaposleni u kompanijama često zaboravljaju šifre, a njihova promena zahteva proceduru koja je skupa. Kompanija *PerSay* istakla je da kompanije troše milione dolara na održavanje šifri koje njihovi zaposleni koriste za pristup kompanijskoj mreži. Ova biometrijska tehnologija omogućava zaposlenima da sami menjaju svoje lozinke bez pozivanja tehničke podrške. Promena lozinke se vrši na taj način što sistem postavi pitanje zaposlenom koji namerava da promeni lozinku i nakon dobijenog odgovora sistem vrši autentifikaciju. Znači, ukoliko sistem prepozna glas zaposlenog, istom će biti omogućena promena lozinke. Istraživanja kompanije *Gartner Group*, koja se bavi konsaltingom u oblasti informacionih tehnologija, pokazala su da se čak od 20% do 50% svih poziva upućenih tehničkoj podršci odnosi na zahteve za promenu šifre. Iz ekonomskog ugla to može da se opiše ovako: prosečna cena promene šifre iznosi do 32 $ po pozivu, a primena automatizovane glasovne promene šifre umanjila bi prosečnu cenu na svega 0,50 $ po pozivu.[246]

Primena ove biometrije omogućava i revizorima da dođu do određenih zaštićenih poslovnih podataka tako što će se uzorak glasa revizora upisati u bazu podataka. Svaki put, kada revizor ima potrebu da dođe do nekih od ovih podataka, pošto sistem prepozna njegov glas, dobiće pristup tim podacima.[247]

U oblasti socijalnog osiguranja, konkretno, u Sjedinjenim Američkim Državama, poslodavci prijavljuju doprinose zaposlenih *on-line*, glasovnom prijavom i uz korišćenje *PIN* broja. Ovaj način prijave ima brojne pogodnosti, a i pruža veću sigurnost zaštite ovako prijavljenih podataka.

[246] Joaquin Gonzalez-Rodriguez, Doroteo Torre Toledano, Javier Ortega-Garcia,"*Voice biometrics*", Handbook of Biometrics, Springer, (2008), str. 151-170.

[247]Judith A. Markowitz, *Voicebiometric,* Vol. 43, No. 9, September (2000).

6.3.4. Prednosti i nedostaci biometrijskih sistema sa glasovnim zapisom

Svaka metoda identifikacije, pa tako i sa glasovnim zapisima, ima svoje prednosti i nedostatke. Što se tiče biometrije glasa, istraživanja su pokazala da je glas pouzdaniji od šifri i kodova, jer ga je nemoguće imitirati ili precizno veštački napraviti. Takođe, malo je verovatno da će uzorak glasa „pasti u pogrešne ruke" i dovesti do zloupotrebe.

Dalje, prednost se ogleda i u tome što je ova biometrijska tehnika jednostavna za korišćenje. Takođe, nije ni skupa, jer ne zahteva poseban hardver, već su dovoljni telefon i mikrofon. Ono što je bitno, a slobodno se može reći i da je najvažnije, je to što je prihvaćena u društvu. Naime, za građane je govor sasvim prirodna stvar, pa im je samim tim i ova metoda veoma prihvatljiva. Ona ne zahteva posebne uređaje, kao što recimo zahteva metoda otiska prsta ili snimanje irisa.

Posebno je važno istaći da je ovo jedina biometrijska metoda koja korisnicima daje mogućnost da se autentifikuju na daljinu. Dalje, proces upisivanja u sistem je kratak, a proces autentifikacije je brz. Od izuzetne važnosti je i to što biometrijski uzorak zauzima jako malo memorije, a skladištenje se vrši ne samo u velikim bazama podataka, već i na mobilnim telefonima i smart karticama.

Danas su raspoloživi softverski paketi koji omogućavaju korisnicima da svoj govor putem računara pretvaraju u tekstualni oblik i da ga potom direktno smeštaju u program za obradu teksta ili elektronsku poštu. Takođe, svim funkcijama iz menija računara ili telefona se može pristupiti i glasom, bez upotrebe ruku. Osobama sa invaliditetom, pa nisu u mogućnosti da koriste ruke za kucanje na tastaturi, ili osobe koje imaju problema sa vidom, a ne mogu da koriste Brajevu tastaturu, rado koriste glasovni sistem komunikacije.

Pored gore pomenutih prednosti biometrijske metode imaju i nedostatke, od kojih na prvom mestu treba pomenuti mogućnost da neko snimi izgovor određene osobe i da to kasnije zloupotrebi. Međutim, procenat takvih zloupotreba je veoma mali što pokazuju i istraživanja IBM centra. Iz napred

pomenutog istraživanja proizilazi da kada bi korisnici prilikom registracije na Internetu, preko telefona, koristili ovu biometriju, hakeri bi bili pogrešno prihvaćeni u 0.00001 % slučajeva.[248] Kako bi se sprečila ova vrsta napada, sistem radi provere može pitati korisnika da ponovi slučajni skup reči ili fraza u određenom redosledu.

Drugi važan nedostatak je i u tome što je glas podložan promenama, a što može da dovede do greške. Osnovni faktori koji utiču na promenu glasa su:[249]

- Godište korisnika (glas se menja sa godinama);
- Bolest (glas se menja usled prehlade, upale grla i sl.);
- Akustika (glas određuje i sredina u kojoj se vrši autentifikacija);
- Emotivno stanje osobe (glas se menja, na primer, usled hapšenja ili stresa);
- Pogrešno pročitane i izgovorene unapred definisane reči ili fraze;
- Udaljenost od mikrofona ili korišćenje drugog tipa mikrofona.

[248] Voice Biometrics Conference, *Voice Biometric Authentication Systems, available on* http://www.authentify.com/solutions/voice_biometrics.html, pristupljeno 22.01.2013.
[249] H. Gravnes, *User's trust in biometric Authentication Systems*, Master Thesis, Gjovik University Collage, Norway, (2005).

7. MULTIBIOMETRIJSKI SISTEMI ZA UTVRĐIVANJE IDENTITETA

Danas se biometrijski sistemi primenjuju u svim aspektima društva. Počev od uspešne identifikacije i elektronske komunikacije pa preko finansijskih, medicinskih i bezbednosnih aktivnosti, pa do fizičke zaštite i zaštite poslovanja vladinih agencija. Međutim, imajući u vidu ranije izloženu prirodu biometrijskih karakteristika možemo zaključiti da su biometrijski sistemi, koji koriste samo jednu biometrijsku karakteristiku, limitirani u pogledu preciznosti njihovog zaključivanja. Navedeni problemi se često mogu prevazići upotrebom biometrijskih sistema koji za utvrđivanje identiteta istovremeno koriste više različitih biometrijskih podataka. Istovremeno, ovakvi sistemi za korisnike mogu biti pogodniji i imati veći stepen preciznosti u zaključivanju, što vodi pouzdanijem postupku identifikacije.

Naime, kada se u postupku identifikacije koristi samo jedna biometrijska karakteristika veća je mogućnost da dođe do pogreške u krajnjem rezultatu u odnosu na situaciju kada se za identifikaciju koristi fuzija nezavisnih biometrijskih karakteristika. To se može bliže objasniti sledećim primerom. Biometrijska tehnika zasnovana na prepoznavanju glasa služi za utvrđivanje identiteta govornika, odnosno za prepoznavanje osobe na osnovu karakteristike njenog glasa. Glas je podložan varijacijama, naročito zbog prehlade, starosti ili trenutnog emotivnog stanja, tako da u aplikacijama koje koriste ovu biometrijsku tehniku može doći do pojave greške u radu tipa *FRR*, odnosno do slučaja kada sistem odbija da identifikuje pravog korisnika jer mu se zbog prehlade izmenio glas. Do greške opisanog tipa može doći i u slučaju kada se za identifikaciju koristi biometrija crta lica, na primer, zbog našminkanog lica, ili zbog naočara ili jednostavno zbog uslova snimanja i pojave svetlosnih varijacija u slici.

Takođe, zbog ranije navedenih razloga deo populacije neće moći ni da se upiše u bazu identifikacionih dokumenta, jer ili nema traženu fizičku osobinu

ili je ona toliko izmenjena da je specifični ulazni senzor ne može zapaziti i prevesti u računarski čitljiv oblik. Za ovaj tip greške je rečeno da je poznat pod akronimom *FTE*, odnosno kao *stopa neprihvatanja unosa biometrijskog podatka*.

Veličina šteta do koje može doći zbog ovakvih grešaka zavisi od polja primene, ali ona može biti nenadoknadiva na polju bezbednosti. Prevazilaženje pomenutih problema predstavljao je u proteklom vremenu veliki izazov za primenu biometrijskih sistema. Istraživanja su pokazala da se bolji rezultati u radu biometrijskih sistema mogu postići ukoliko se istovremeno u procesu donošenja odluke kombinuje više nezavisnih biometrijskih osobina, pri čemu se vodi računa da se pronađu efikasne kombinacije za međusobno povezivanje određenih biometrijskih karakteristika.

Jedan mogući pogled na takve sisteme, sa stanovišta vrste uzoraka u bazi biometrijskih podataka, izložen je u poglavlju 5 ovoga rada. Kako je ova oblast poslednjih godina u veoma dinamičnom razvoju, u literaturi se za izloženu kategoriju biometrijskih sistema mogu sresti različite terminološke odrednice. Čest naziv za sisteme koji istovremeno koriste više ulaznih biometrijskih podataka je multibiometrijski ili višebiometrijski sistemi (engl. *Multibiometric System*).

Među prvim multibiometrijskim sistemima su sistemi u kojima su se kombinovale biometrijske karakteristike glasa i crta lica, koristeći zvučni zapis i podatke sa fotografija i video snimaka[250] Posebno se ističe značaj ovih sistema na polju bezbednosti, a pored toga daju rešenja i za menadžment identiteta.

Što se tiče finansijskog aspekata, koji je veoma važan faktor u praktičnoj primeni, posebno u vremenu ekonomske krize, može se uočiti da multibiometrijski sistemi samim tim što zahtevaju snažnije računarske sisteme imaju i nešto veće troškove. Osnovni cilj multibiometrijskih sistema je da se poveća procenat tačnosti zaključivanja prilikom utvrđivanja identiteta. Kao što se vidi sa slike 53, multibiometrijski sistemi su sistemi koji kombinuju više

[250] D. Dessimoz, J. Richiardi, C. Champod, A. Drygajlo, *Multimodal Biometrics for Identity Documents (MBioID)*, Institut de Police Scientifique, June (2006), available on, http://www.europeanbiometrics.info.

biometrijskih podataka o jednoj biometrijskoj osobini dobijenih korišćenjem više senzora, ili korišćenjem više različitih uzoraka dobijenim jednim senzorom, ili na osnovu više karakteristika dobijenih radom više algoritama nad jednim uzorkom, ili pomoću više karakteristika dobijenih nekim algoritmom nad više uzoraka iste vrste, ili kombinacijom opisanih postupaka nad više raznovrsnih biometrijskih osobina. Nezavisnost osobina obezbeđuje značajan napredak u performansama.[251]

U zavisnosti od vrste i broja izvora biometrijskih podataka multibiometrijski sistemi se mogu podeliti i na: multisenzorske, sa više uzoraka jedne biometrijske osobine (na primer, više slika lica), sa više instanci (na primer, sa više otisaka različitih prstiju), sa više algoritama za izvođenje karakteristika, na multimodalne (izvlačenje zaključaka na osnovu više biometrijskih osobina) i hibridne sisteme.[252]

Slika 53 Klasifikacija multibiometrijskih sistema u zavisnosti od vrste i broja izvora

[251] Christopher Middendorff , Kevin W. Bowyer, *Multibiometrics Using Face and Ear*, Handbook of Biometrics, (2008), str. 315-335.
[252] A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*, Springer, New York, USA, 1st edition, (2006).

7.1. Unimodalni biometrijski sistemi za utvrđivanje identiteta

Multibiometrijski sistemi za utvrđivanje identiteta sa jednom biometrijskom osobinom su sistemi koji za identifikaciju koriste jednu biometrijsku osobinu sa više uzoraka u prostoru i vremenu. Do više biometrijskih podataka o jednoj biometrijskoj osobini dolazi se korišćenjem ili više senzora, ili više algoritama, ili više uzoraka u prostoru i/ili vremenu. Ako se termin *mod* u razmatranom kontekstu odnosi samo na broj posmatranih biometrijskih osobina, onda se ovi sistemi mogu nazvati i *unimodalni multibiometrijski sistemi.*[253] Pored toga što se postiže veći stepen preciznosti prilikom identifikacije, fleksibilniji su za korisnike samim tim jer koriste više podataka o nekoj biometrijskoj osobini. U slučaju kada neki korisnik nije u mogućnosti da koristi neki biometrijski podatak, on se može zameniti drugim. Na primer, ako je reč o osobini anatomije kože prsta, onda se u ovoj kategoriji multibiometrijskih sistema umesto otiska jednog prsta uzimaju otisci dva ili više različitih prstiju. Pored svega ovoga, smanjuje se i procenat zloupotrebe jer se sistem ojačava, a napad postaje komplikovaniji.[254]

Danas dominiraju unimodalni biometrijski sistemi, odnosno sistemi identifikacije koji koriste samo jednu biometrijsku osobinu neke osobe opisanu jednim podatkom. Ovakvi sistemi se i danas najčešće implementiraju, kako u civilnim primenama, tako i u okviru državnih institucija i organizacija. Iako su povoljniji sa ekonomskog stanovišta i jednostavniji sa tehničkog stanovišta, ovakvi sistemi imaju određene slabosti i podložni su greškama, kao na primer, zbog lošeg osvetljenja kod biometrije crta lica ili zbog nečistog optičkog skenera kod biometrije otiska prsta. Prvi korak ka unapređenju njihovih performansi može se postići nadgradnjom ovih sistema kako bi stekli osobine unimodalnih multibiometrijskih sistema.

[253] A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 43–47.

[254] A. Ross, *An introduction to multibiometrics*, West Virginia University, Morgantown,WV 26506 USA, (2007).

7.1.1. Osvrt na unimodalne multibiometrijske sisteme za identifikaciju

Multisenzorski sistemi, odnosno višestruki senzori su takvi sistemi koji koriste više senzora prilikom uzimanja biometrijske osobine određenog korisnika. Na primer, kod biometrije zasnovane na prepoznavanju crta lica mogu da se koriste dve ili više *2D* kamera ili kod otiska prsta kapacitivni i optički senzor. Mogu se uzimati *2D i 3D* slike lica istog korisnika i kombinovati ih na nivou podataka, kao i na nivou rezultata upoređivanja. Verifikacioni sistem baziran na šaci kombinuje geometrijske karakteristike šake sa otiskom dlana na nivou karakteristika i na nivou rezultata upoređivanja. Spajanje na nivou rezultata podudaranja može dati bolje rezultate nego spajanje na nivou karakteristika.[255]

Multialgoritamski sistemi su sistemi koji koriste samo jedan senzor za uzimanje biometrijskih podataka, ali koristi više klasifikatora. Sistem koristi višestruke šeme algoritama, čime sistem postaje otporniji na varijacije ulaznih podataka, posebno kada je u pitanju biometrijski sistem zasnovan na crtama lica.[256] Postoje klasifikatori koji analiziraju isti set karakteristika, a postoje i oni koji generišu svoje grupe karakteristika. Za poboljšanje performansi podudaranja mogu se kombinovati rezultati poklapanja upoređivača koji se bazira na detaljima otiska prsta sa upoređivačem koji se bazira na teksturi. Lu i saradnici izdvajaju tri različite vrste seta karakteristika slike lica osobe (pomoću *PCA, LDA i ICA*) i integrišu izlaz odgovarajućeg klasifikatora na nivou rezultata upoređivanja.[257]

Sistemi sa više instanci biometrijskih karakteristika su dizajnirani tako da se sa jednim senzorom uzimaju podaci pomoću kojih se dolazi do više biometrijskih karakteristika jedne osobe, a u cilju preciznije identifikacije.

---

[255] Kumar, A. D. C. M. Wong, H. C. Shen, A. K. Jan, *Personal verification using palmprint and hand geometry biometric,* Guildford, UK: Proc. Of 4th Int I Cinf. On Audio and Video-based Biometric Person Authentication (AVBPA), Jun (2003).

[256] A.Ross, K. Nandakumar, A. K. Jain, "*Introduction to Multibiometrics*", Handbook of Biometric (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 272.

[257]A.Ross, A., A K. Jain, J. Reisman., *A hybrid fingerprint matcher*. T. 36. Pattern Recognition, Jul (2003).

Senzorom se uzima više uzoraka sa istog biometrijskog izvora, ali u različitim vremenskim intervalima ili pri različitim prostornim uslovima akvizicije podataka. Tako se kod sistema za prepoznavanja lica može uzeti frontalna slika, kao i slika levog i desnog profila, čime se prevazilazi problem varijacije poza. Slično je i kod sistema koji koristi otisak prsta kao uzorak. Ovaj sistem treba da bude tako dizajniran da automatski odabira „*optimalan*" podskup koji će na najbolji način predstaviti varijacije ulaznih podataka kod pojedinaca.

Sistem sa više uzoraka koristi višestruke uzorke iste biometrijske osobine jedne osobe uzete sa različitih izvora biometrijskih podataka. Od istog korisnika se uzima više uzoraka iste biometrijske osobine, kako bi se uzeo što bolji uzorak koji se poredi sa uzorkom u bazi podataka. Na primer, od istog korisnika se uzima uzorak levog i desnog kažiprsta ili recimo, levi i desni iris. Ovi sistemi su u upotrebi u SAD na graničnim prelazima. Na primer, to je levi i desni kažiprst ili, levi i desni iris pojedinca.[258] Recimo *US VISIT* biometrijski sistem, na graničnom prelazu za ulazak u zemlji pored provere putnih dokumenata vrši proveru lica koje namerava da uđe u zemlju korišćenjem otisaka prstiju leve i desne ruke. *IAFIS* koristi kombinaciju svih deset prstiju radi provere identiteta u bazi podataka.

7.1.2. Ograničenja unimodalnih multibiometrijskih sistema

Cilj identifikacije je da se pravom korisniku odobri pristup, a da se odbije pristup neovlašćenom korisniku. Međutim, rezultati identifikacije nisu uvek precizni, tako da se dešava da se pravom korisniku ne odobri pristup sistemu, a da se dozvoli pristup neovlašćenom korisniku. Kada se za identifikaciju koristi samo jedna biometrijska karakteristika češće dolazi do greške u odnosu na to kada se za identifikaciju koristi fuzija nezavisnih biometrijskih karakteristika.[259]

[258]Christopher Middendorff , Kevin W. Bowyer, *Multibiometrics Using Face and Ear*, Handbook (2008), str. 315-335.

[259] A.Jain and A.Ross. *Multibiometric systems*. Communication of the ACM. Vol 47, No 1, January (2004).

7.1.2.1. Pogrešno očitani podaci i promena biometrijske karakteristike

Jedan od razloga koji može dovesti do pogreške prilikom identifikacije osobe, što može za posledicu da ima neprepoznavanje osobe ranije unete u bazu podataka, su pogrešno očitani ulazni podaci (tip *FRR*[260] greške). Razlozi koji dovode do ovakvih pogrešaka mogu da potiču od pogrešne interakcije korisnika sa ulaznim senzorom, ali i od promene posmatrane biometrijske karakteristike. Ilustrujmo navedene stavove sledećim primerom. U biometriji prepoznavanja govornika na osnovu glasa vrši se identifikacija govornika, odnosno prepoznavanje onoga ko je izgovorio reči, na osnovu prepoznavanja karakteristika glasa. Međutim, glas je podložan promenama, između ostalog, zbog prehlade, starosti ili trenutnog psihičkog stanja, što može dovesti do greške prilikom identifikacije ili u slučajevima kada se uzorak glasa uzima u bučnom ambijentu, pa biometrijski sistem nije u mogućnosti da pravilno izmeri karakteristike glasa. Kada je u pitanju identifikacija putem biometrije crta lica do greške u identifikaciji može doći ukoliko korisnik nosi naočare, ukoliko je našminkan ili ukoliko se ne uzme dobar uzorak za poređenje zbog svetlosnih varijacija u okruženju. Kod biometrije otiska prsta, zbog lošeg položaja prsta na senzoru takođe može doći do greške. Neke biometrijske karakteristike se vremenom menjaju. Tako recimo, crte lica se menjaju starenjem, a ožiljci menjaju karakteristike otiska prsta, što je čest slučaj kod radnika koji obavljaju teške fizičke poslove.

7.1.2.2. Nemogućnost izdvajanja potrebne biometrijske karakteristike

U ograničenja unimodalnih biometrijskih sistema spada i verovatnoća da *neki korisnici neće moći da daju zahtevane biometrijske podatke*. U praksi to znači da unimodalni biometrijski sistemi ne mogu uvek da izdvoje biometrijsku karakteristiku koja im je potrebna za identifikaciju. Recimo, kod biometrije otiska prsta problem nastaje kod korisnika koji imaju loše otisnute grebene na

[260] FRR *False Rejection Rate* (Procenat pogrešnog odbijanja).

prstu.[261] Istraživanja su pokazala da oko 4% ljudi ima nečitak otisak prsta, bilo zbog ožiljka, starosti ili nečitkih karakteristika, što dovodi do greške tipa *FTE,* odnosno neuspešnog upisa u sistem. Ovaj deo populacije neće moći da se upiše, na primer, u bazu za dobijanje identifikacionih dokumenta, *ID*.[262]

7.1.2.3. Neuniverzalnost

U biometriji se polazi od stava da svaka biometrijska karakteristika treba da bude *jedinstvena* za svakog čoveka. Međutim, to u praksi nije uvek slučaj, posebno kada je u pitanju biometrija crta lica. Naime, biometrijski sistemi zasnovani na crtama lica su dosta ograničeni, budući da među ljudima mogu da se nađu dosta slični, posebno kada su u pitanju identični blizanci. To dovodi do pogrešnog rezultata pri poređenja uskladištenih karakteristika, odnosno do greške tipa FAR u postupku identifikacije.

7.1.2.4. Zloupotreba

Unimodalni sistemi su podložniji zloupotrebi. To se naročito odnosi na sisteme koji za identifikaciju koriste osobine ponašanja, kao recimo glas, jer lako može doći do imitacije glasa. Kada je u pitanju otisak prsta, otisak se lako može skinuti sa neke staklene površine i potom zloupotrebiti. Pored ovih i fizičke karakteristike su takođe osetljive na napad.

Pomenuta ograničenja unimodalnih multibiometrijskih sistema se mogu prevazići primenom multimodalnih multibiometrijskih sistema, odnosno sa istovremenim kombinovanjem više biometrijskih podataka o različitim biometrijskim osobinama. Pored toga što se postiže veći stepen preciznosti prilikom identifikacije, ovakvi sistemi fleksibilniji sa stanovišta korisnika jer koriste više njegovih biometrijskih karakteristika.[263]

---

[261] A.Ross, K. Nandakumar, A. K. Jain, "*Introduction to Multibiometrics*", Handbook of Biometric (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 273.

[262] D. Dessimoz, J. Richiardi, *Multimodal Biometric for Identity Documents*, Research Report (2005).

[263] S. Paunović, D. Starčević, *Multibiometrijski sistemi za utvrđivanje identiteta*, Simpozijum o operacionim istraživanjima, Zbornik radova SYMOPIS 2013, FON, Beograd, Zlatibor, R.Srbija, (2013).

7.2. Multimodalni biometrijski sistemi za utvrđivanje identiteta

Kada se za identifikaciju koristi jedna biometrijska karakteristika, ili kada se radi sa više karakteristika jednog moda, neki delovi postupaka za određivanje identiteta postaju kritični u pogledu tačnosti obradnih podataka, odnosno njihove preciznosti, pa češće dolazi do greške u radu sistema u odnosu na postupke koji za identifikaciju koriste fuziju više nezavisnih biometrijskih osobina – modova. Tada kažemo da je reč o multimodalnoj biometriji, odnosno o multibiometrijskom sistemu za utvrđivanje identiteta sa više biometrijskih osobina.

Da bi multimodalni sistemi bili precizniji od unimodalnih, ali i dovoljno brzi, važno je pronaći efikasne kombinacije za fuziju biometrijskih karakteristika. Kao što je rečeno, među prvim multimodalnim sistemima bili su sistemi nastali kombinovanjem biometrijskih karakteristika glasa i crta lica.[264] Cilj njihove primene bio je prevazilaženje već opisanih ograničenja koja nameću unimodalni sistemi, čime se povećavala ne samo preciznost rada i pouzdanost zaključivanja procesa identifikacije, već i ukupan broj implementiranih biometrijskih sistema, kao i broj različitih primena u društvu.[265] Takvi multimodalni biometrijski sistemi pokazuju posebnu prednost u borbi protiv zloupotrebe biometrijskih tehnologija, jer omogućavaju veći stepen sigurnosti rada ovim sistemima, imajući u vidu da se od korisnika zahteva fizička prisutnost prilikom prikupljanja podataka.

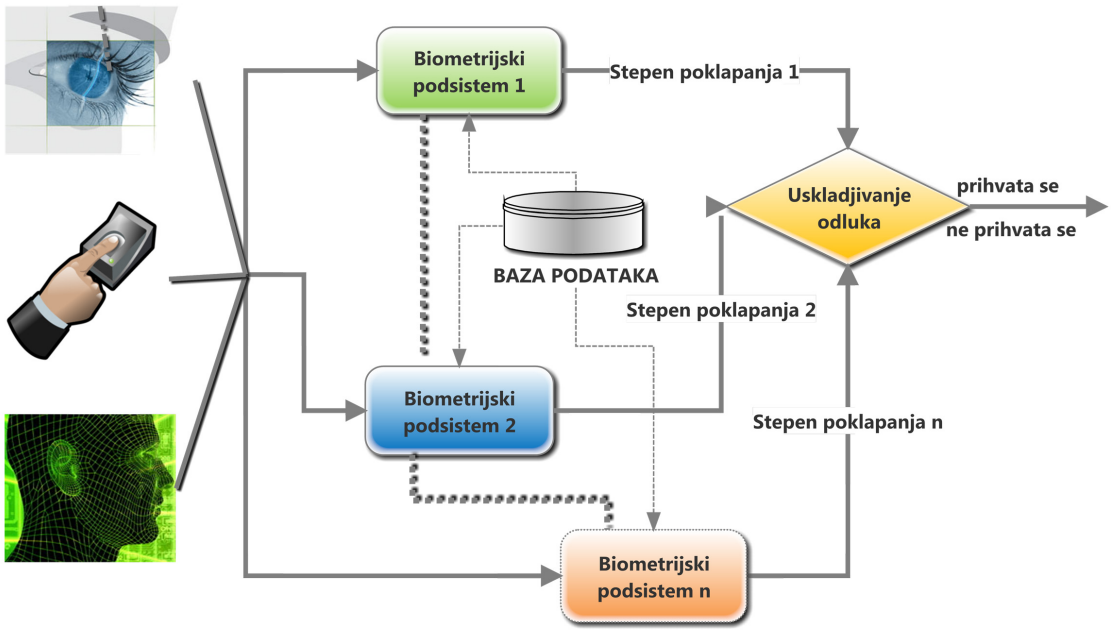
Suština multimodalnih sistema se ogleda u tome što se koristi više međusobno nezavisnih postupaka u procesu izračunava stepena poklapanja unetih biometrijskih podataka sa onima uskladištenim u bazi podataka.[266] Na taj način se eliminiše ili znatno redukuje broj komponenti čiji otkaz, ili nedovoljno siguran rad, može da ugrozi sistem kao celinu. Dobijeni

[264] A.R, K. N A. K. J, *op.cit.* str. 272.
[265] A. Nagar, K. Nandakumar, A. K. Jain, *Tehnical report: Multibiometric Cryptosystems,* Under review for IEEE TIFTS, vol. 7, NO.1, February (2012).
[266] Y.Xu, D.Zhang, J.Yang, *A feature extraction method for use with bimodal biometrics*, Pattern Recognition 43 (2010), str. 1106–1115.

međurezultati nezavisnih komponenti sistema se potom usklađuju radi donošenja konačne odluke. Izloženi princip rada multimodalnog biometrijskog sistema ilustrovan je na blok dijagramu 4.

Naravno, identifikacija postaje sofisticirana i skuplja, jer se kombinuju različite tehnike biometrijske identifikacije, ali se dobija veća preciznost podataka i pouzdanost zaključivanja, a može se uticati i na smanjivanje zahtevanog napora korisnika u procesu identifikacije.

Treba reći da se intenzivnija primena multimodalnih sistema odvija poslednjih godina, pa se u raspoloživoj literaturi uglavnom nalaze postignuti rezultati rada ispitnih sistema u pogledu tačnosti za pojedine multimodalne kombinacije, ali bez podataka koji bi se odnosili na postignute performanse takvih sistema, odnosno što je još važnije, na uticaj broja instanci zapisa u bazi podataka na ponašanje performansi sistema.



Blok dijagram 4 Princip rada multimodalnog biometrijskog sistema

Prema dostupnim izvorima, ne postoji jednostavan način odabiranja biometrijskih metoda koje će se koristiti u multimodalnom sistemu. Ipak, možemo reći da se u većini slučajeva najbolji rezultate dobijaju kombinacijom

biometrijskih metoda koje i u unimodalnim sistemima pružaju veliku tačnost, što je i očekivano, ali zadovoljavajući rezultati se postižu i kombinovanjem tehnika koje same za sebe obezbeđuju srednju tačnost rada sistema. Među najčešće korišćenim tehnikama u multimodalnoj biometriji ubrajaju se tehnike koje rade sa otiscima prstiju, sa slikama lica i snimcima irisa (šarenice oka).

Ukoliko se koristi veći broj prethodno nabrojanih metoda, može se izgraditi jedan sigurniji biometrijski sistem. U praksi je poželjna kombinacija fizičkih i ponašajnih karakteristika, jer se time smanjuje mogućnost prevare biometrijskog sistema u postupku identifikacije ili verifikacije. Već je rečeno da se ovi metodi koriste na graničnim prelazima za kontrolu ulaska ili izlaska putnika, za kontrolu pristupa nekom prostoru, civilnoj identifikaciji, mrežnoj zaštiti.

Multimodalna biometrija se može koristiti i kao podrška standardnim postupcima za proveru identiteta, ukoliko iz izvornih dokumenata i zapisa nije moguće dobiti dovoljan broj podataka kojima bi se opisala neka osoba. Upravo je preporučljiva kombinacija standardnih zaštitnih mehanizama i biometrijskih podataka, jer uvek postoji mogućnost zloupotrebe. Jedan od primera je lažni otisak prsta. Ako se koristi samo jedna biometrijska tehnika, a nepozvana osoba poseduje lažni otisak prsta, s kojim obavlja autentifikaciju u ime neke osobe u konkretnom slučaju može doći do zloupotrebe. Ali, ukoliko se koristi verifikacija na osnovu prepoznavanja lica, ili još bolje na osnovu prepoznavanja šarenice ili na osnovu provere rasporeda vena, tada se s većom sigurnošću može utvrditi da li se radi o toj osobi ili je reč o pokušaju krađe identiteta.

Multimodalni sistemi imaju značajne prednosti nad unimodalnim. U slučaju da je neka biometrijska karakteristika slična za više ljudi, prisutnost druge metode sprečava pojavu pogrešnog prihvatanja. Prevara sistema se drastično otežava postojanjem većeg broja metoda koji se koriste prilikom identifikacije.

7.2.1. Opšta arhitektura multimodalnih biometrijskih sistema za utvrđivanje identiteta

Arhitektura multimodalnog biometrijskog sistema za identifikaciju često zavisi od šireg konteksta u kojima su ovi sistemi implementirani. Tipični multibiometrijski sistemi se pored različitih senzora za uzimanje biometrijskih karakteristika, uglavnom uključuju i sledeće algoritme:

- algoritmi za izvođenje biometrijskih uzoraka ili šablona (obrađuju se ulazni ili *sirovi* biometrijski podaci u cilju formiranja posebnog skupa podataka – *karakteristika*, kojima u računaru reprezentujemo posmatranu osobinu čoveka),
- algoritmi za poređenje, na osnovu kojih se novi biometrijski šabloni upoređuju sa jednim ili više postojećih šablona u bazi podataka,
- algoritmi za odlučivanje, koriste prethodne međurezultate u poređenju šablona kako bi utvrdili, ili potvrdili, identitet osobe.

Prilikom dizajniranja multimodalnog sistema, potrebno je analizirati sledeća pitanja: [267]

- izbor biometrijskih osobina i broja izvedenih karakteristika,
- logički nivo obrade na kome će doći do spajanja (fuzije) biometrijskih podataka,
- način na koji će se biometrijski podaci integrisati,
- finansijske resurse.

Smatra se da su biometrijski sistemi koji integrišu informacije u ranoj fazi obrade u opštem slučaju efikasniji od onih sistema koji obavljaju integraciju u kasnim fazama, imajući u vidu da biometrijski podaci na ulasku imaju bogatije informacije od rezultata podudaranja ili izlazne odluke upoređivača.

Izbor biometrijskih osobina i broja kombinovanih izvedenih karakteristika zavisi od polja primene biometrijskog sistema, odnosno od zahtevanog stepena

[267] U.M.Bubeck. *Multibiometric Authentication*, Term Project CS 574, San Diego State University, (2003).

sigurnosti rada biometrijskog sistema.[268] Tako, na primer, za pristup ličnom uređaju, mobilnom telefonu, najjednostavnije je kombinovati otisak prsta i glas, a kod ATM uređaja, recimo crte lica i glas, dok je kod pristupa nekim obezbeđenim lokacijama potrebna kombinacija uzimanja otiska prsta i slike lica, kao i skeniranje irisa. Izbor kombinacije izvedenih biometrijskih karakteristika je veoma važan jer je uspešnost utvrđivanja identiteta uslovljena odgovarajućom kombinacijom karakteristika. Potrebno je naglasiti da se ne mogu proizvoljno kombinovati biometrijske karakteristike, već one moraju biti kompatibilne.

Najčešće kombinacije biometrijskih osobina prikazane su u Tabeli 1.[269]

Tabela 1 Moguće kombinacije kompatibilnih biometrijskih karakteristika

Kombinacija	Karakteristika	Karakteristika	Karakteristika
1	Glas	Crte lica	
2	Glas	Pomeranje usana	
3	Glas	Crte lica	Pomeranje usana
4	Otisak prsta	Crte lica	
5	Otisak prsta	Crte lica	Glas
6	Otisak prsta	Crte lica	Geometrija dlana
7	Otisak prsta	Glas	Geometrija dlana
8	Otisak prsta	Geometrija dlana	
9	Termogram lica	Crte lica	
10	Dužica oka	Crte lica	
11	Otisak šake	Geometrija dlana	
12	Oblik uha	Glas	

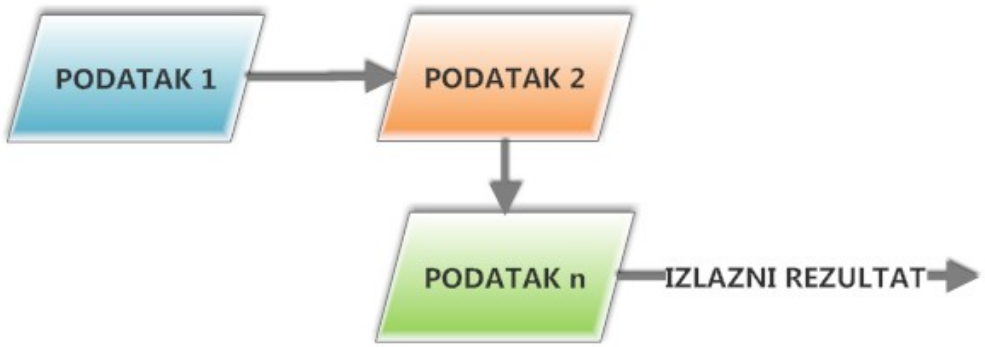
[268] J. Lee, B. Moghaddam, H. Pfister, and R. Machiraju, *Finding Optimal Views for 3D Face Shape Modeling,* In Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG), Seoul, Korea, May (2004), str. 31–36.
[269] L. Hong, A. Jain, S. Pankanti. *Can Multibiometrics Improve Performance?*

7.2.2. *Arhitektura multimodalnog sistema i režimi rada*

Arhitektura multimodalnog biometrijskog sistema može da se projektuje tako da omogući rad sistema u tri različita režima, i to u:[270]

- rednom,
- paralelnom,
- hijerarhijskom.

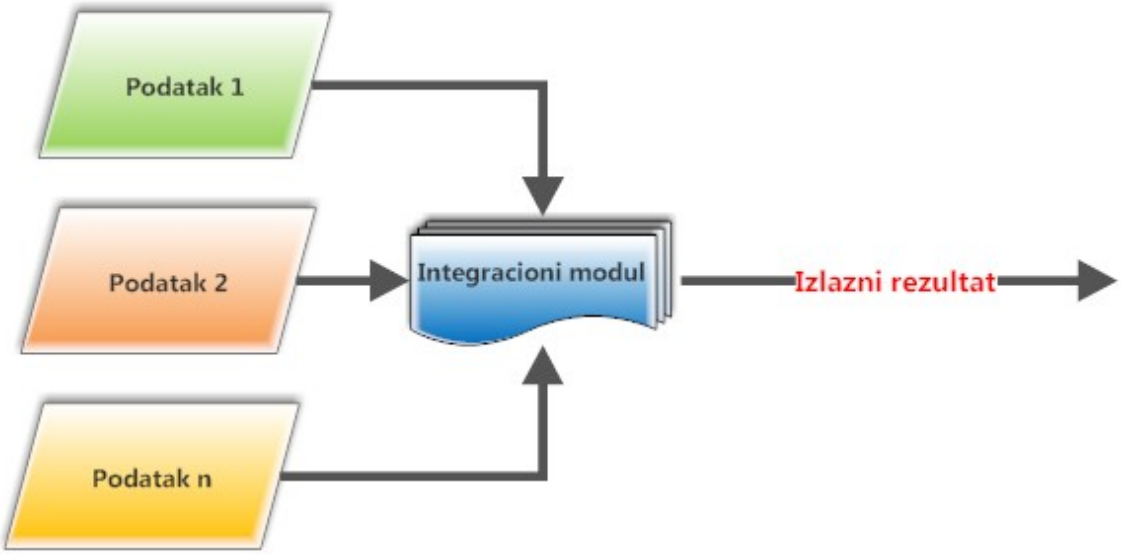
Multimodalni biometrijski sistemi koji se zasnivaju na *rednom* režimu rada obradu ulaznih podataka vrše serijski, korak po korak, blok dijagram 5, tako da rezultat obrade nekog podatka utiče na sledeći po redu rezultat obrade, a koji se vrši sa narednim podatkom. U rednom režimu rada, ukoliko biometrijski sistem u nekom koraku rada može da utvrdi identitet osobe sa projektovanim stepenom sigurnosti, neće zahtevati izvršenje sledećeg koraka sa novim biometrijskim podatkom. Pored toga, korisnik ima mogućnost da odabere redosled unosa biometrijskih podataka. Zbog izloženog načina rada, redni sistemi zahtevaju jake i efikasne algoritme. Prvi redni sistem predstavljen je od strane Honga i Džejn.[271] Taj sistem je koristio dva biometrijska podatka, crte lica i otisak prsta. Funkcionisao je na taj način što se biometrijski identifikator crta lica koristio za dobijanje osnovnog rezultata, a biometrijski identifikator otiska prsta je imao ulogu da potvrdi dobijeni rezultat.



Blok dijagram 5 Ilustracija arhitekture sistema sa rednim sjedinjavanjem podataka

[270] A. Ross and A. K. Jain. Information Fusion in Biometrics, Pattern Recognition Letters, *Special Issue on Multimodal Biometrics,* 24(13), (2003), str. 2115–2125.
[271] L. Hong and A. K. Jain. Integrating Faces and Fingerprints for Personal Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 20(12), December (1998), str. 1295–1307.

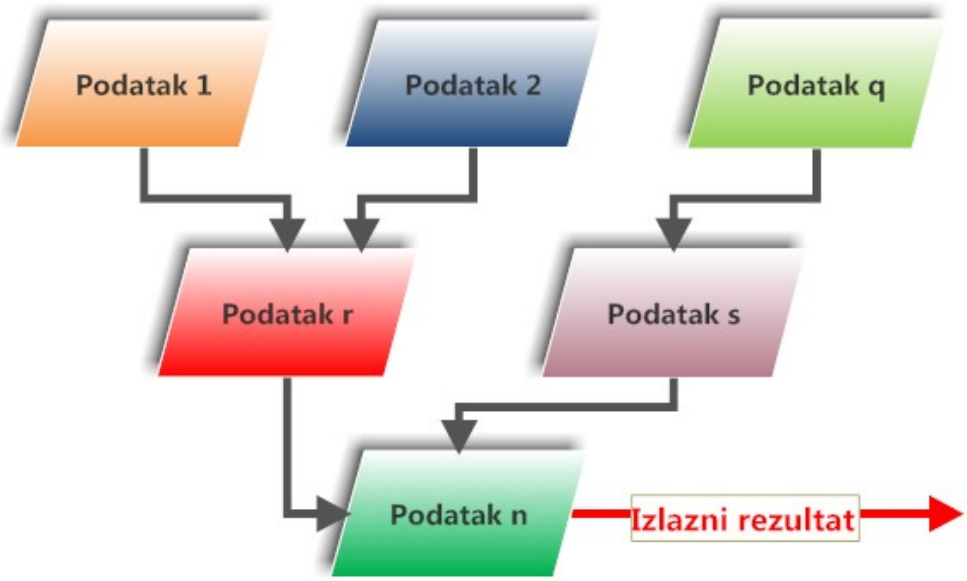
Arhitektura multimodalnog biometrijskog sistema sa *paralelnim* režimom rada sastoji se u tome što se svi biometrijski podaci nezavisno obrađuju putem odgovarajuće programske šeme, blok dijagram 6. Teorijski, sistemi sa paralelnim režimom rada postižu bolju tačnost krajnjeg rezultata jer se u trenutku donošenja odluke koriste *svi* raspoloživi podaci. Većina multimodalnih biometrijskih sistema za utvrđivanje identiteta koristi paralelnu arhitekturu, jer je primarni cilj smanjenje grešaka.[272] Takođe, važno je istaći da arhitektura sa paralelnim režimom rada omogućava jednostavnu paralelizaciju procesa, a koja se izvodi u multiprocesorskom okruženju kakvu danas imaju većina komercijalnih računarskih sistema.



Blok dijagram 6 Ilustracija arhitekture sistema sa paralelnim sjedinjavanjem podataka

Arhitektura multimodalnog biometrijskog sistema sa *hijerarhijskim* režimom rada predstavlja kombinaciju opisane redne i paralelne arhitekture, blok dijagram 7. Kod ove arhitekture multimodalni sistem je tako projektovan da rešava probleme nedostatka ili pojave sitnih šumova odnosno, grešaka pri očitavanju biometrijskih osobina.

[272] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. K. Jain. Large Scale Evaluation of Multimodal Biometric Authentication Using State - of - the - Art Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 27(3), March (2005), str. 450–455.



Blok dijagram 7 Ilustracija arhitektura sistema sa hijerarhijskim sjedinjavanjem podataka

Prilikom izbora arhitekture uvek treba voditi računa o nameni aplikacije. Recimo, za pristup ATM terminalima se pogodna je redna arhitektura, a za pristup strogo zaštićenim lokacijama pogodnija je paralelna arhitektura.

7.2.3. Načini povezivanja biometrijskih podataka u multimodalnim sistemima

Načini povezivanja ili fuzije više biometrijskih podataka u multimodalnim sistemima bitno utiče na efikasnost i preciznost ovih sistema. Sam proces sjedinjavanja biometrijskih podataka može da se odvija na različitim logičkim obradnim nivoima koje smo opisali kod unimodalnih biometrijskog sistema. Kako je prvi zadatak biometrijskog sistema uzimanje biometrijskih uzoraka, završetkom uzimanja biometrijskih podataka određen je i prvi mogući nivo na kom može da se obavi fuzija. Rezultat fuzije na ovom nivou je agregirani uzorak dobijen kombinacijom više uzetih uzoraka. Na primer, agregirani uzorak je kombinacija sirovih podataka dobijenih iz više otisaka prstiju iste osobe.

U drugoj fazi obrade se na osnovu uzetog sirovog biometrijskog uzorka izvode određene karakteristike i smeštaju u šablon, pa se fuzija na ovom nivou

vrši sjedinjavanjem više formiranih šablona u jedan jedinstveni šablon koji se zapisuje u bazu podataka. U sledećoj, trećoj fazi obrade ispituje se podudaranje izvedene karakteristike sa postojećim u bazi podataka, pri čemu se kod multimodalnih sistema upoređuje više izvedenih karakteristika, ili modova, sa relevantnim zapisima u bazi podataka, pa se dobijeni rezultati u pogledu sličnosti fuzijom kombinuju kako bi se dobio jedinstveni rezultat, skalar, kao mera sličnosti. Konačno, u poslednjoj četvrtoj fazi obrade treba doneti odluku da li je sistem utvrdio, ili nije utvrdio, identitet ispitivane osobe. Fuzija podataka se na nivou odluke može vršiti tako, što se prvo se za svaki ispitivani biometrijski mod pojedinačno donosi odluka, pa se tek nakon toga, recimo glasovima većine, dolazi do konačne odluke.[273]

Najvažniji preduslovi za efikasan i precizan rad multimodalnog sistema su vezani za rad ulaznih senzora. Senzori treba da budu tako dizajnirani da mogu da brzo prikupe biometrijske podatke i da ih upišu u sistem bez greške, a sve to pritom uz što nižu cenu. Pored toga, imajući u vidu mogućnosti senzora i odabranu kombinaciju biometrijskih karakteristika, neophodno je sprovesti potrebne analize na više mogućih nivoa fuzije podataka, kako bi se odabrao onaj nivo koji je pri datim uslovima najpreciziji i najefikasniji. Danas je dostupan veliki broj senzora i mogućih skupova akviriranih biometrijskih podataka, pa je za svaku aplikaciju iz tog razloga potrebno naći najbolje rešenje.

Biometrijska fuzija se primenjuje, kako u postupcima identifikacije, tako i u postupcima verifikacije korisnika. Naravno da je zadatak koji se postavlja pred sisteme za identifikaciju mnogo izazovniji u odnosu na zadatak postavljen pred sisteme za verifikaciju. Iskustva u primeni pokazuju da su se u praksi najbolji rezultati pokazali kod biometrijskog modaliteta otiska prsta. Treba posebno istaći multibiometrijske sisteme koji za identifikaciju koriste kombinaciju više otisaka prstiju, kao što je sistem AFIS. Takođe, konstatovano

[273] A. Hicklin, B. Ulery, C. Watson, *A Brief Introduction to Biometric Fusion,* Mitretek Systems, National Institute of Standards and Technology, (2006), str. 3-5.

je da je fuzija na nivou upoređivanja karakteristika do sada dala najbolje rezultate.[274]

Analize koje su sprovedene u više slučajeva su pokazale da dve najveće prednosti koje možemo očekivati, ako primenimo biometrijsku fuziju, su preciznost i efikasnost. Međutim, na osnovu činjenice da se u procesu fuzije vrši obrada nad više skupova podataka, nego što je reč kod unimodalnih sistema, vodi nas ka zahtevu za jačim računarskim sistemima, a što samim tim dovodi do većih troškova. Pored toga, zahteva se i više vremena za obavljanje zadatka obzirom da se sakuplja više biometrijskih podataka. Imajući u vidu izazove koje biometrija postavlja u odnosu na pravo privatnosti, možemo reći da zahtev za prikupljanjem više podataka o nekoj osobi stvara i veću opasnost da se povredi njeno pravo na privatnost.

Umesto izloženog konvencionalnog pristupa mestu mogućeg sjedinjavanja multimodalnih biometrijskih podataka, *Sanderson* i *Paliwal* su nivoe fuzije podelili na dve osnovne grupe, i to:[275]

- fuzije koje se vrše pre upoređivanja,
- fuzije koje se vrše nakon upoređivanja.

Pristupi kasnijim fuzijama se mogu zasnivati i na konceptu rangiranja rezultata, odnosno bodovanja rezultata poređenja. Kada je u pitanju identifikacioni režim rada, izlazni rezultat sistema može da se posmatra kao rang lista identiteta upisanih u bazu podataka. U ovom slučaju izlazni rezultat ukazuje na skup mogućih identiteta sortiranjem dobijenih skorova podudaranja po opadajućem redosledu.

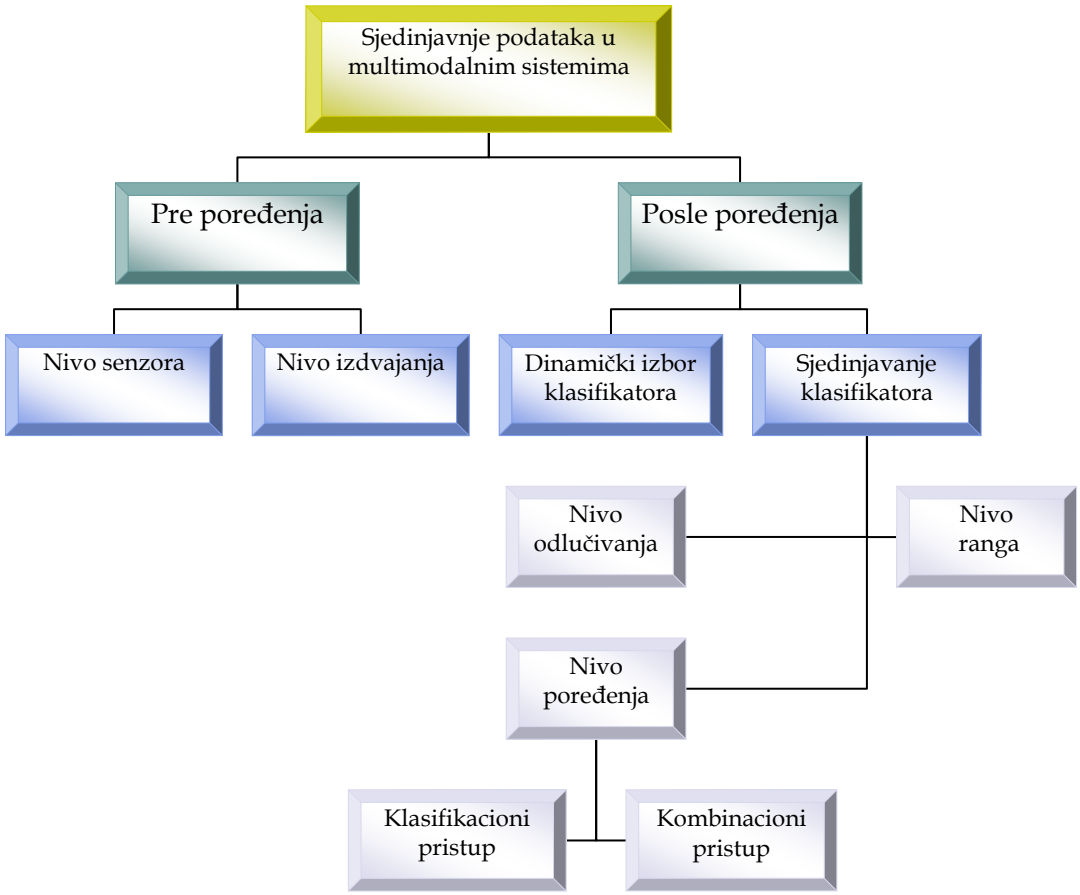
Cilj metode fuzije na ovom nivou je konsolidovanje izlaznih rangova pojedinačnih biometrijskih sistema radi dobijanja zajedničkog ranga za svaki identitet. Rang pruža bolji uvid u proces donošenja odluka, ali oni otkrivaju manje informacije nego rezultat predstavljen bodovanjem, skorom. Za razliku

[274] *Ibid*. str. 4.
[275] A.Ross, K. Nandakumar, A. K. Jain, "*Introduction to Multibiometrics*", Handbook of Biometrics (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 275.

od upoređivanja dobijenih bodova, rangiranje pruža mogućnost upoređivanja rada više biometrijskih sistema. Zbog toga, u ovom slučaju nije potrebna normalizacija dobijenih skorova.[276]

Normalizacija je inače važna faza kod tehnologija fuzije u multimodalnoj biometriji. Cilj normalizacije je podešavanje parametara koji se odnose na lokaciju i skalu distribucije rezultata poređenja, skorova, na izlazu zasebnih modula za poređenje, kako bi se rezulti dobijeni iz više modula doveli na isti nivo radi daljeg upoređivanja.[277]

Na slici 54 je prema *Sanderson-u* i *Paliwal-u* data taksonomija mogućih tehnika sjedinjavanja podataka u multimodalnim sistemima.



Slika 54 Grupni prikaz tehnika sjedinjavanja kod multimodalnog biometrijskog sistema

[276] *Ibid. Str. 283.*
[277] *Ibid. Str. 276.*

U prvu grupu tehnika pre poređenja karakteristika spadaju fuzije na nivou senzora i na nivou sjedinjavanja izvedenih karakteristika (vektor karakteristika), a u drugu grupu spadaju fuzije na nivou rezultata podudaranja i nivou odluke.[278] Analizirajući odnos grupe tehnika koji pripadaju modelu ranije, odnosno kasnije fuzije, može se zaključiti da tehnike koje pripadaju modelu ranije fuzije u opštem slučaju imaju prednost iz razloga što u ranijoj fuziji u algoritam ulaze ne samo uzeti biometrijski podaci, već i njihovi međusobni odnosi čime se smanjuje entropija posmatranog sistema. Kao ilustraciju navedenog stava, možemo reći da biometrijska karakteristika sadrži više informacija o konkretnom biometrijskom modalitetu, nego što imamo na izlazu modula za poređenja, a koji pak sadrži više informacija nego odluka dobijena na izlazu modula za odlučivanje.[279]

7.2.3.1. Fuzije pre upoređivanja

Fuzije na nivou senzora

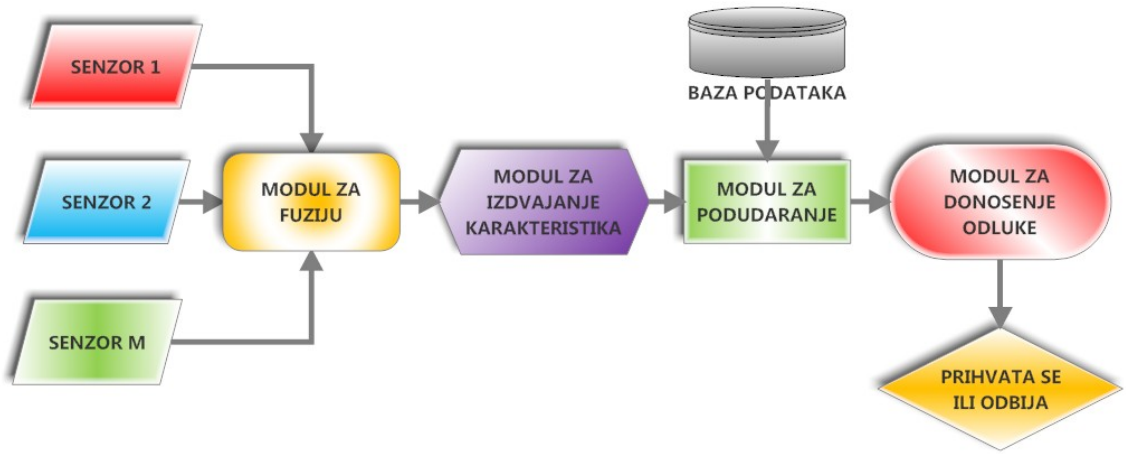
Mogućnosti fuzije biometrijskih podataka na nivou senzora veoma su zavisne od nivoa tehnologije korišćene u realizaciji senzora. Kao dobru ilustraciju navedenog iskaza navešćemo uzimanje biometrijskih podatka o crtama lica ispitivane osobe. Sa ranije dostupnim tehnologijama bilo je nemoguće zamisliti dobijanje 3D slike objekta kojeg snimimo, na primer, frontalni izgled glave ispitivane osobe. Danas, biometrijska fuzija to omogućava kombinacijom senzora koji generiše video zapis *en face* portreta lica osobe i senzora koji daje 3D dubinsku sliku lica. U biometrijskim sistemima biometrijski podaci se mogu prikupljati putem različitih senzora bar na dva načina, i to:[280]

- korišćenjem više različitih, ali kompatibilnih, senzora radi uzimanja podataka o *jednoj* biometrijskoj osobini, ili

[278] A.R, K. N A. K. J*, op.cit.* str. 275.
[279] I.Milenković, D. Starčević, S. Paunović, *Fuzija informacija u multimodalnoj biometriji*, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011).
[280] A.R, K. N A. K. J*, op.cit.* str. 275.

- korišćenjem *jednog* senzora za uzimanje više instanci podataka u vezi neke biometrijske osobine.

Na primer, crte lica ispitanika se mogu uzeti putem različitih kamera, a otisci više prstiju istog ispitanika se mogu uzeti jednim senzorom. Na senzorskom ili prvom nivou rada biometrijskog sistema može doći do fuzije uzetih sirovih uzoraka njihovim kombinovanjem u jedinstven uzorak, blok dijagram 8. Metod fuzije na ovom nivou vrši se na jedan od ranije pomenutih načina. Dakle, do integracije uzoraka u jedinstveni agregirani uzorak dolazi odmah nakon njihovog uzimanja, a svakako pre izvođenja odgovarajućih biometrijskih karakteristika. Da bi se mogla izvršiti fuzija više uzetih uzoraka na ovom nivou obrade sami sirovi uzorci međusobno moraju biti usklađeni. Ukoliko uzeti podaci nisu usklađeni, fuzija postaje veoma složena ili čak nemoguća. Na primer, nije jednostavno sjediniti slike lica dobijene kamerama koje rade sa različitim rezolucijama. Na osnovu već izloženih stavova može se zaključiti da fuzija na senzorskom nivou vodi ka najefikasnijim biometrijskim sistemima, jer se sjedinjavanjem sirovih ulaznih podataka najbolje održavaju zahvaćene biometrijske informacije potrebne u postupku identifikacije. Međutim, ono što u praksi predstavlja značajnu prepreku ovom vidu fuzije je neophodnost da svi zahvaćeni podaci budu međusobno usklađeni, a što nije lako postići, pa se iz tog razloga fuzija na ovom nivou obrade retko koristi.

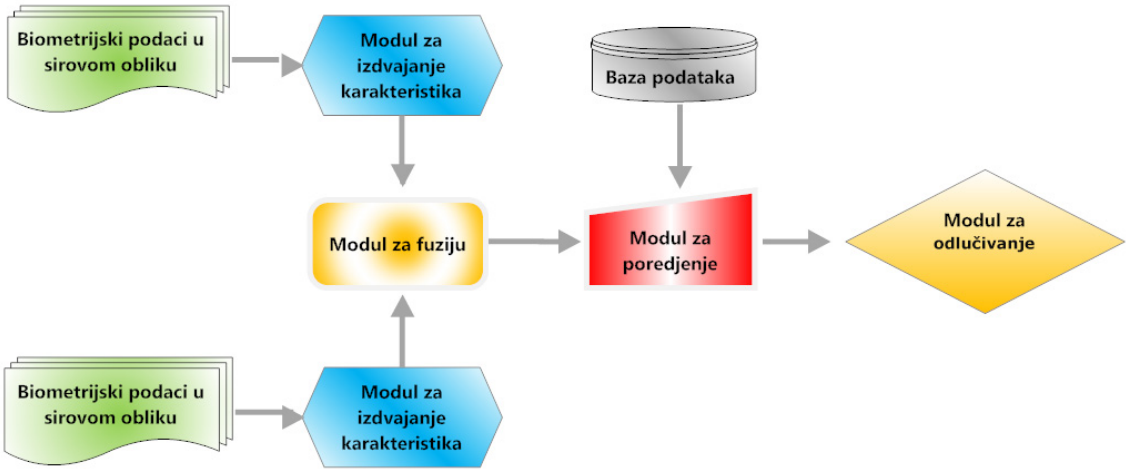


Blok dijagram 8 Fuzija biometrijskih podataka na nivou senzora

Fuzija na nivou izdvajanja karakteristika

U unimodalnim biometrijskim sistemima nakon uzimanja biometrijskog uzorka u formi sirovog ulaznog podatka, potrebno je programski izvesti odgovarajuće karakteristike, kao jednostavnije reprezente posmatrane biometrijske osobine, i konvertovati ih u unapred dogovorenu strukturu podataka, *šablon*, pogodniju za efikasnu računarsku obradu.

Kada su u pitanju multimodalni biometrijski sistemi, nakon izvođenja svih pojedinačnih karakteristika, može da se izvrši objedinjavanje, ili fuzija, svih korišćenih pojedinačnih struktura podataka za smeštaj biometrijskih karakteristika u jedinstvenu strukturu zapisa, ili šablon, u bazi podataka, što je ilustrovano na blok dijagramu 9.



Blok dijagram 9 Fuzija biometrijskih podataka na nivou izvođenja karakteristika

U praksi, u multibiometrijskim sistemima svaki modul za izdvajanje karakteristika daje izlaz u obliku vektora karakteristika, pa da bi se putem fuzije dobio nov biometrijski podatak potrebno je individualne vektore karakteristika povezati u jedinstveni vektor. Dakle, od posebno izvedenih biometrijskih karakteristika formira se u modulu za integraciju zajednički

vektor izdvojenih biometrijskih karakteristika, koji se zatim poredi sa šablonom unetim prilikom prijave korisnika u bazu podataka.[281]

Postupak integracije individualnih vektora karakteristika u jedinstveni vektor karakteristika ne svodi se na puko prepisivanje vrednosti, već mu u opštem slučaju prethode procesi normalizacije, transformacije i redukcije šema.

Cilj procesa normalizacije je modifikacija položaja prethodno izvedenih karakterističnih tačaka i razmere opsega vrednosti biometrijskih karakteristika, kako bi se različite biometrijske karakteristike mapirale u zajednički domen. Na ovaj način se rešava i problem suvišnih podataka o biometrijskim karakteristikama. Redukcija šema se postiže odabirom minimalnog seta karakteristika primenom postupka za smanjenje dimenzionalnosti.[282] Do smanjenja dimenzionalnosti dolazi i kada je neki vektor podvrgnut linearnom i nelinearnom mapiranju, jer ga to projektuje u niži dimenzionalni prostor.

Vektori karakteristika se dele na homogene i nehomogene. Homogeni vektori su vektori istog biometrijskog modaliteta, na primer, otisci više prstiju istog ispitanika u slučaju biometrije sa otiscima prstiju. Nehomogeni vektori su vektori različitih biometrijskih modaliteta, kao na primer biometrijski modalitet geometrije dlana i slike crta lica. Kada su vektori ulaznih podataka homogeni, krajnji vektor može biti izračunat kao prosek korisnikovih pojedinačnih vektora karakteristika, dok kod nehomogenih mogu se ulančavati u oblik jedinstvenog vektora karakteristika. Istraživanja su pokazala da biometrijski podaci moraju biti kompatibilni, odnosno međusobno usklađeni, jer u suprotnom povezivanje podataka nije moguće. Na primer, nije moguće povezati podatke koji se odnose na analizu glavnih komponenti kod biometrijskog modaliteta lica i minucije kod biometrijskog modaliteta otiska prsta, s obzirom da se radi o nekompatibilnim biometrijskim karakteristikama. Istraživači su analizirali različite kombinacije biometrijskih karakteristika nehomogenih vektora (otisak

[281] U.M.Bubeck. *Multibiometric Authentication*,Term Project CS 574, San Diego State University, (2003).
[282] P. J. Huber, *Robust Statistics*, John Wiley & Sons, (1981).

šake i geometrije dlana, kao i crte lica sa geometrijom šake), ali su došli do ograničenih rezultata.[283]

Pristup fuziji u slučaju nehomogenih vektora se u praksi ređe sreće, usled sledećih problema: [284]

- Vektori karakteristika različitih biometrijskih modaliteta mogu biti nekompatibilni (na primer, otisak prsta predstavljen preko minucija i lice predstavljeno preko koeficijenata karakterističnih vektora);
- Veze između vektora različitih biometrijskih modaliteta nisu poznate;
- U nekim slučajevima konkatenacija vektora različitih modaliteta dovodi do problema predimenzioniranosti, odnosno da vreme izračunavanja postaje neprihvatljivo dugo;
- U mnogim komercijalnim biometrijskim sistemima prodavci ne omogućuju pristupe vektorima karakteristika, jer programski sistem predstavlja poslovnu tajnu, usled čega se istraživači više fokusiraju na metode fuzije u kasnijim fazama procesiranja.

Ross i *Govindarajan* primenili su fuziju na nivou izvođenja karakteristika, gde su za biometrijske modalitete uzeli crte lica i geometriju šake. Izvršena je konkatenacija karakteristika geometrije šake i karakteristika lica dobijenih primenom diskriminacione analize na crno-beloj slici lica. Uspešnost ovog istraživanja bila je ograničena.

Prilikom istraživanja nad setom podataka koji je prikupio *Michigan State University*, procenat prepoznavanja svih ispitanika iz skupa sa pravom pristupa sistemu, (engl. *Genuine Acceptance Rate-GAR*), u slučaju fuzije na nivou karakteristika bio je 93% pri vrednosti *FAR* parametra od 1%, dok je prilikom fuzije na nivou poređenja vrednost *GAR* parametra pala na 79% pri zadržanoj vrednosti *FAR* greške od 1%. Međutim, prilikom ispitivanja nad setom podataka koji su istraživači prikupili u okviru svog projekta, fuzija na nivou

[283] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain. Personal Verification Using Palmprint and Hand Geometry Biometric. *In Proceedings of Fourth International Conference on Audio - and Video - Based Biometric Person Authentication (AVBPA),* Guildford, U.K. June (2003), str. 668 – 678.
[284] A.R., K. N., A. K. J, *op.cit.* str. 277.

karakteristika je pokazala nešto slabije performanse od fuzije na nivou poređenja. [285]

X. Zhou i *B. Banu* su analizirali multimodalni biometrijski sistem čiji su modaliteti bili profil lica i hod. U tom radu predstavljen je inovativan pristup koji se sastoji od sledećih koraka: [286]

- Iz video zapisa vrši se izdvajanje profila lica, kao i silueta koje karakterišu različite položaje ljudskog tela u određenim tačkama hoda,
- Na osnovu profila lica izdvojenih iz video zapisa generiše se profil lica visoke rezolucije. Takođe, generiše se kompaktna prostorno-vremenska reprezentacija hoda u video zapisu, kako bi se rešili problemi vezani za ulazak drugih predmeta u kadar i vremensku sinhronizaciju.
- Na vektorima koji reprezentuju profil lica visoke rezolucije i kompaktnu reprezentaciju hoda primenjuje se analiza glavnih komponenti, kako bi se smanjile njihove dimenzije.
- Dobijeni vektori se normalizuju, zatim se vrši njihovo povezivanje. Kako bi se rešio problem predimenzioniranosti dobijenih vektora, posebnim postupkom međusobnog kombinovanja svih karakteristika lica i hoda iz jedne video sekvence izvode se srodne karakteristike. Zatim se na te izvedene karakteristike primenjuje diskriminaciona analiza, kako bi performanse sistema bile što bolje.
- Na kraju, nad karakteristikom koja je dobijena kao rezultat svih ovih transformacija, vrši se identifikacija identiteta na osnovu metode prvog najbližeg suseda[287].

Pokazano je da ovakav multimodalni pristup ima bolje performanse od sistema koji koriste samo jedan od ova dva biometrijska modaliteta, kao i od

[285] A.Ross, R.Govindarajan, *Feature Level Fusion Using Hand and Face Biometrics*, Proc. Of SPIE conference on Biometric Technology for Human Identification II, vol 5779, Mart (2005), str. 196-204.

[286] X.Zhou, B. Banu, *Feature fusion of side face and gait for video-based human identification*, Pattern Recognition 41 (2008), str. 778 – 795.

[287] I. Milenković, D. Starčević, S. Paunović, *Fuzija informacija u multimodalnoj biometriji*, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011).

multimodalnog sistema kod koga se fuzija informacija vrši na nivou poređenja. Konkretno, prilikom primene fuzije na nivou izdvajanja karakteristika, sistem je imao *GAR* od 97,8 %, dok je primenom samo modaliteta lica *GAR* bio 91,1%, a primenom samo modaliteta hoda 93,3%.

Y. Yao, *X. Jing* i *H. Wong* su analizirali multimodalni sistem koji kombinuje modalitete crta lica i otiska šake, sa fuzijom na nivou izvođenja karakteristika. Za izvođenje karakteristika pojedinačnih modaliteta korišćene su tehnike analiza glavnih komponenti i Bajesove transformacije[288].

Prilikom fuzije tako dobijenih karakteristika korišćeni su težinski faktori koji se odnose na stepen nezavisnosti između ove dve biometrijske karakteristike. Testiranje je izvršeno nad bazom od 119 osoba, sa po 20 uzoraka lica i otiska šake svake osobe.

Rezultati su pokazali prednost multimodalnog pristupa poboljšanjem performansi u odnosu na performanse sistema pri korišćenju samo jednog od ova dva biometrijska modaliteta, kao i poboljšanje u odnosu na fuziju prostom konkatenacijom vektora karakteristika. [289]

Y. Xu, D. Zhang i *J. Yang* su u svom radu predstavili jedan mogući pristup fuziji na nivou karakteristika, konstruisan za primenu u bimodalnim biometrijskim sistemima. Pristup je testiran nad tri različite kombinacije biometrijskih modaliteta, i to nad kombinacijom otisaka obe šake, kombinacijom otiska šake i crte lica, kao i kombinacijom modaliteta crta lica i uva. Za metod fuzije karakteristika predložena je jedna varijacija metode analize glavnih komponenti (*Matrix - Based Complex Principal Component Analysis - MCPCA*). Istraživači su pokazali ovakav pristup dovodi do poboljšanja performansi u odnosu na rezultate postignute klasičnom analizom glavnih komponenti.

---

[288] P. Verlinde and G. Cholet. Comparing Decision Fusion Paradigms using k -NN based Classifiers, Decision Trees and Logistic Regression in a Multimodal Identity Verification Application. In *Proceedings of Second International Conference on Audio and Video - Based Biometric Person Authentication (AVBPA),* Washington D.C., U.S.A., March (1999), str. 188 – 193.

[289] Y.Yao, X.Jing, H.Wong, *Face and palmprint feature level fusion for single sample biometrics recognition,* Neurocomputing 70 (2007), str. 1582–1586.

Uočeni nedostatak se ogleda u činjenici da korišćene biometrijske karakteristike moraju biti istih dimenzija. Pri testiranju korišćene su baze sa sledećim elementima: 189 osoba sa po 10 otisaka svake šake - za modalitete obe šake, 120 osoba sa po 10 uzoraka šake i lica – za modalitete šake i lica, 17 osoba – za modalitete lica i uha. [290]

7.2.3.2. Fuzije posle poređenja

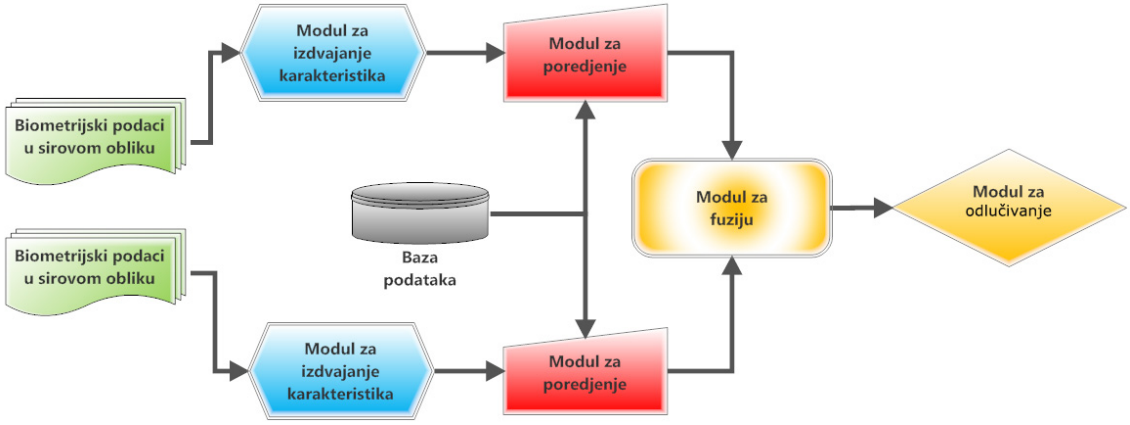
Fuzije na nivou rezultata poređenja

Pored do sada izloženih postupaka multimodalne biometrije korišćenjem fuzije na nivou senzora, odnosno na nivou izvođenja karakteristika, za koje kako smo pokazali da spadaju u postupke rane fuzije, u literaturi se može naći više pristupa fuziji biometrijskih podataka na nivou rezultata poređenja karakteristika, odnosno fuzije na nivou odluke, za koje smo rekli da spadaju u postupke kasne fuzije.

Metod fuzije na nivou rezultata poređenja sastoji se u merenju stepena podudaranja individualnih biometrijskih informacija, a koje se nakon toga koriste u postupku fuzije radi iznalaženja jedinstvene mere podudaranja. Da se podsetimo, posmatrane biometrijske karakteristike se izvode nezavisno za svaki modalitet i potom se svaka od njih posebno poredi sa karakteristikama smeštenim u šablonima u bazi podataka.

Rezultati tog poređenja kombinuju se kako bi se generisao novi, izvedeni rezultat poređenja, koji se potom prosleđuje dalje modulu za odlučivanje, blok dijagram 10.[291]

[290] Y.Xu, D.Zhang, J.Yang, *A feature extraction method for use with bimodal biometrics*, Pattern Recognition 43 (2010), str. 1106–1115.
[291] A.Ross, K. Nandakumar, A. K. Jain, "*Introduction to Multibiometrics*", Handbook of Biometric (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 273.



Blok dijagram 10 Fuzija biometrijskih podataka na nivou rezultata poređenja karakteristika

Samo ćemo navesti da se u literaturi metode fuzije na nivou rezultata poređenja karakteristika prema pristupu integraciji podataka mogu svrstati u kategoriju postupaka sa pristupom na bazi gustine (engl. *density-based schemes*), transformacionim pristupom (engl. *transformation-based scheme*) i sa klasifikacionim pristupom (engl. *classifier-based schemes*). [292]Radovi iz ove oblasti pokazuju i da je kod ovog metoda fuzije potrebno prethodno normalizovati mere podudaranja. [293]

A. Jain, K. Nandakumara i *A. Ross* analizirali su različite metode normalizacije rezultata rada modula za poređenje. Ukazali su da je neophodno sprovesti postupak normalizacije rezultata poređenja ukoliko se vrši direktna fuzija rezultata poređenja, a bez njihove prethodne interpretacije u okviru nekog statističkog okvira. Na taj način vrši se transformacija tih rezultata u zajednički domen, kako bi njihova fuzija mogla da se izvrši na smislen način. Modaliteti nad kojima su autori rada vršili testiranja su lica, otisak prsta i geometrija šake. Eksperimenti su vršeni nad bazom od 100 osoba, sa po 5 uzoraka svakog modaliteta po osobi. Primenom fuzije podataka na nivou poređenja, performanse sistema značajno su unapređene u odnosu na unimodalni pristup.

[292] A.R., K. N., A. K. J., *op.cit.* str. 279.
[293] Y. Wang, T. Tan, and A. K. Jain. *Combining Face and Iris Biometrics for Identity Verification*. In Proceedings of Fourth International Conference on Audio - and Video - Based Biometric Person Authentication (AVBPA), Guildford, U.K.., June (2003), str. 805 – 813.

Na primer, pri vrednosti parametra *FAR* od 0,1%, procenat uspešno prepoznatih ispitanika, *GAR* na osnovu otiska prsta je 83,6%, dok je pri istoj vrednosti za *FAR*, naznačena multimodalna kombinacija daje vrednost za *GAR* sistema 98,6% u slučaju primene z-normalizacije skora sa kasnijom fuzijom metodom zbira normalizovanih skorova.

Prema rezultatima istraživanja najbolje performanse sa multimodalnim sistemima dobijaju se primenom min-max, *tanh* i *z-score* metoda normalizacija i sa fuzijom zasnovanom na zbiru rezultata. Takođe, važno je napomenuti da su *min-max* i *z-score* metode osetljive na prisustvo ekstremnih vrednosti u podacima.[294]

R. Snelick, U. Uludag, A. Mink, M. Indovina i *A. Jain* analizirali su nekoliko metoda normalizacije rezultata, kao i više različitih metoda za fuziju tako dobijenih normalizovanih rezultata pojedinačnih modula za poređenje. Pored revizije rezultata rada metoda koje se uobičajeno koriste u ove svrhe, predložili su adaptivni metod normalizacije, uz pomoć kojeg se postiže veći stepen razdvajanja raspodela legitimnih korisnika sistema i takozvanih "uljeza". Istakli su i dva inovativna metoda fuzije podataka.

U prvom metodu fuzije vrednost koeficijenata dodeljenih izlazima pojedinačnih modula za poređenje određuje se na osnovu vrednosti *EER* (engl. *Equal Error Rate*) odgovarajućih unimodalnih biometrijskih sistema, pri čemu se vrednost *EER* parametra definiše kao radna tačka biometrijskog sistema u kojoj su izjednačene vrednosti *FAR* i *FRR* parametra.

Drugi metod za svakog korisnika dodeljuje specifične vrednosti koeficijentima na izlazima pojedinačnih modula za poređenje. Za testiranje metoda korišćeni su modaliteti lica i otiska prsta. Baza nad kojom su testovi vršeni sadržala je biometrijske podatke 1000 osoba, sa po dva uzorka lica i

[294] A.Jain, K.Nandakumara, A.Ross, *Score normalization in multimodal biometric systems*, Pattern Recognition 38 (2005), str. 2270–2285.

otiska prsta. Upotrebom multimodalnog pristupa ostvareno je značajno poboljšanje performansi. [295]

D. Maurer i *J. P. Baker* predložili su korišćenje Bajesovih mreža verovatnoća za fuziju na nivou poređenja. Prilikom projektovanja mreže, uzeta je u obzir i procena kvaliteta rezultata poređenja. Korišćeni su biometrijski modaliteti glasa i otiska prsta. Kombinovanjem *NIST*[296]-ove baze od 2700 osoba sa dva uzorka otisaka svih deset prstiju i *XM2VTS*[297] baze od 295 osoba sa po četiri snimljene sesije, dobijena je baza za testiranje sastavljena od takozvanih "kimeričkih" osoba. Pod "kimeričkom" osobom podrazumevamo virtuelan identitet dobijen kombinacijom pojedinačnih biometrijskih modaliteta različitih osoba. Performanse ovog sistema prilikom korišćenja Bajesovih mreža verovatnoća pokazale su se bolje nego pri primeni metoda koje se zasnivaju na primeni koeficijenata u formi težinskih faktora.

Mogući nedostatak ovakvog pristupa zasniva se na činjenici da je potrebna veća količina biometrijskih podataka za treniranje sistema nego što je to slučaj sa prethodno opisanim tehnikama.[298]

M. Vatsa, R. Singh i *A. Noore* analizirali su korišćenje jedne varijacije metode maksimalno granične hiperravni uz pomoć specijalizovanog računara za podršku paralelne obrade skupa vektora. Prilikom fuzije uzet je u obzir i kvalitet biometrijskih podataka. Korišćeni biometrijski modaliteti su lice i šarenica oka.

Sistem je testiran nad bazom od 300 osoba, sa po sedam uzoraka lica i šarenice oka. Performanse predloženog metoda fuzije upoređene su sa performansama unimodalnog pristupa, kao i sa tri alternativne metode fuzije podataka na nivou rezultata poređenja, metodom zbira skorova, zbira skorova

[295] R.Snelick, U.Uludag, A.Mink, M.Indovina, A.Jain, *Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems*, IEEE Transactions on Pattern analysis and Machine Intelligence, vol. 27, no. 3, Mart (2005).
[296] *NIST.*
[297] *XM2VTS.*
[298] D.Maurer, J.P. Baker, *Fusing multimodal biometrics with quality estimates via a Bayesian belief network*, Pattern Recognition 41 (2008), str. 821 – 832.

uz primenu težinskih faktora koji odražavaju kvalitet biometrijskih podataka, kao i još jedne varijacije metode maksimalno granične hiperravni (*C-SVM fusion*). Predložena metoda pokazala se bolja od alternativnih, sa ostvarenim vrednošću *EER* parametra od 0,55%.[299]

Analizirani radovi su pokazali da se fuzija na ovom nivou često primenjuje zbog lakoće pristupa i obrade rezultata, tačnosti rezultata, kao i zbog boljih performansi u odnosu na nivo odlučivanja.

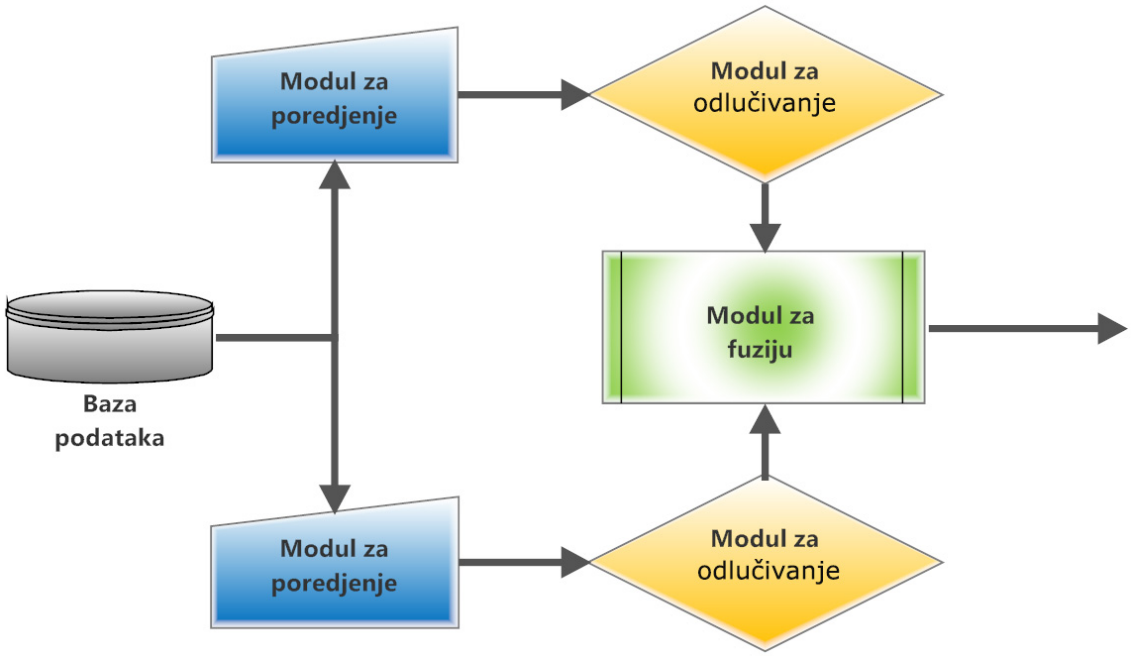
Fuzija na nivou odlučivanja

Fuziju biometrijskih podataka na nivou odlučivanja odlikuje kombinovanje rezultata dobijenih sa izlaza modula odlučivanja za svaki analizirani biometrijski podatak, *blok dijagram 11*.

Metod fuzije na ovom nivou sastoji se u formiranju konačne odluke na osnovu tako dobijenih podataka. Svaki posmatrani podsistem se ponaša kao zaseban unimodalni biometrijski sistem, a nakon toga dolazi do konsolidacije dobijenih rezultata. Fuzija na ovom nivou je dosta popularna u biometrijskim sistemima, jer mnogi komercijalni proizvođači, u okviru svojih proizvoda iz domena unimodalne biometrije, istraživačima ili integratorima sistema čine dostupnom samo finalnu odluku, dok sam način funkcionisanja sistema za krajnjeg korisnika predstavlja "crnu kutiju".

U tom slučaju fuziju podataka moguće je izvršiti samo na nivou odlučivanja. Neke od metoda integracija parcijalnih odluka zasnivaju se na primeni pravila „*AND*" i „*OR*", metoda većinskog glasanja, metoda većinskog glasanja sa primenom težinskih faktora, Bajesovog odlučivanja ili Dempster-Šeferove teorije dokaza.

[299] M.Vatsa, R. Singh. A. Noore, *Integrating image quality in 2ν-SVM biometric match score fusion*, International Journal of Neural Systems, Vol. 17, No. 5 (2007), str. 343–351.



Blok dijagram 11 Fuzija biometrijskih podataka na nivou odlučivanja

K. Kryszczuk, J. Richiardi, P. Prodanov i *A. Drygajlo* analizirali su mogućnosti integracija informacija u multimodalnim biometrijskim sistemima za potrebe verifikacije tvrđenog identiteta na nivou odlučivanja.

Korišćeni su biometrijski modaliteti glasa i lica. Opisan je pristup u kome svaki od unimodalnih biometrijskih sistema prosleđuje modulu za fuziju određene parametre. To su vrednosti CID_F, MR_F, za lice, kao i CID_s, MR_s za glas. *CID* (engl. *Claimed Identity*) predstavlja potvrdu ili odbijanje tvrđenog identiteta koji je predmet procesa verifikacije, sa vrednostima 1 i 0, respektivno.

MR (engl. *Modality Reliability*) označava pouzdanost donete odluke i takođe može uzeti vrednost 1 ili 0. Na primer, vrednost parametra $MR_f = 1$ ima značenje „Odluka koja se odnosi na modalitet lica je pouzdana".

Sam mehanizam sa pravilima odlučivanja na osnovu ovako definisane semantike parametara *CID* i *MR* predstavljen je u Tabeli 2 [300].

[300] K. Kryszczuk, J. Richiardi, P. Prodanov, A. Drygajlo, *Reliability-Based Decision Fusion in Multimodal Biometric Verification Systems*, International Journal of Neural Systems, Vol. 17, No. 5 (2007), str. 343–351.

Tabela 2 Primer pravila fuzije informacija na nivou odlučivanja

Lice	Glas	Konačna odluka
$CID_F = 1$	$CID_{s=1}$	1
$CID_F = 1$	$CID_{s=0}$	1: ako važi $P(MR_f = 1) > P(MR_{s=} 1)$ 0: inače
$CID_F = 0$	$CID_{s=1}$	1: ako važi $P(MR_f = 1) < P(MR_{s=} 1)$ 0: inače
$CID_F = 0$	$CID_{s=0}$	0

Za testiranje korišćena je *BANCA* baza podataka, koja sadrži podatke prikupljene od 52 različite osobe. Upotrebom multimodalnog pristupa ostvareno je poboljšanje performansi sistema.

Analizom radova koji obrađuju problem fuzije na svim pomenutim nivoima pokazuje se da najviše prednosti pruža spajanje na nivou rezultata upoređivanja karakteristika iz razloga što se relativno lako kombinuju prethodni rezultati obrade modaliteta u sistemu. Nedostatak fuzije u ranoj fazi obrade se ogleda u tome što se zahteva kompatibilnost biometrijskih podataka, što nije uvek lako postići. Što se tiče fuzije u kasnijoj fazi, recimo na nivou odluke, istraživanja su ukazala na nedostatak fuzije na ovom nivou jer su mogućnosti integracije dosta krute jer se raspolažu manjim brojem informacija, nego na prethodnim nivoima.[301]

[301] A. Ross, A. K. Jain, *Multimodal biometric: an overview,* Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austrija), Septembar (2004), str. 1221-1224.

8. STUDIJA SLUČAJA: MULTIMODALNI BIOMETRIJSKI SISTEM ZA UTVRĐIVANJE IDENTITETA

8.1. Postavka problema studije

U skladu sa postavljenim Planom istraživanja na doktorskoj disertaciji, studija slučaja ima za cilj da definiše, opiše rad i dobijene rezultate jedne klase multimodalnih biometrijskih sistema, kao okvirnog rešenja za proveru postavljenih hipoteza. U daljem tekstu za takav multimodalni biometrijski sistem koristićemo termin ispitni multimodalni biometrijski sistem za utvrđivanje identiteta. Već je u prethodnom poglavlju rečeno da je prilikom dizajniranja multimodalnog sistema, potrebno analizirati sledeća pitanja koja određuju metodologiju razvoja: [302]

- izbor biometrijskih osobina i broj izvedenih karakteristika,
- logički nivo obrade na kome će doći do spajanja (fuzije) biometrijskih podataka,
- način na koji će se biometrijski podaci integrisati,
- finansijske resurse.

Imajući u vidu izloženi pregled raspoložive literature i uvida u praksu korišćenja biometrijskih sistema u svetu, za potrebe ove doktorske disertacije opredelili smo se da istražujemo problem biometrijske multimodalnosti za utvrđivanje identiteta u slučaju kada se koriste dve biometrijske osobine čoveka, anatomske strukture prstiju i lica, što nas vodi ka dva veoma često korišćena biometrijska moda sa kojima radi računarski sistem, a to su otisak prsta i slike lica. Upravo navedene biometrijske modalitete obuhvataju i identifikacioni dokumenti koji se najčešće koriste u svetu, a u tu svrhu koristi ih i Ministarstvo unutrašnjih poslova Republike Srbije, što je detaljno izloženo u poglavlju 3 i 6.

[302] U.M.Bubeck. *Multibiometric Authentication*, Term Project CS 574, San Diego State University, (2003).

Prvi zadatak koji je proizašao iz postavljenog cilja istraživanja, i odabrane klase multimodalnog biometrijskog sistema za utvrđivanje identiteta, bio je formiranje ispitne biometrijske baze podataka. Postoje dva moguća pristupa njenom formiranju, u prvom se kreiraju sopstvene biometrijske baze podataka sa otiscima prstiju i slikama lica, a u drugom pristupu na osnovu pretraživanja Interneta pronalaze se formirane i dostupne biometrijske baze podataka.

Prednost prvog pristupa se ogleda u činjenici što možemo da nadziremo i upravljamo kompletnim procesom formiranja takve baze podataka, što praktično znači da je podešavamo prema konkretnim zahtevima eksperimenata koje nameravamo da sprovodimo. Nedostaci takvog pristupa su znatno veći troškove formiranja ispitne biometrijske baze, nego kada dovlačimo i koristimo gotovu bazu podataka sa Interneta, jer moramo da raspolažemo odgovarajućom opremom, prostorom i vremenom, kao i ljudima koji vrše uzimanje biometrijskih podataka. Možda je ipak najveće ograničenje prvog pristupa broj ispitanika koji su saglasni da im uzmemo biometrijske podatke za eksperimentalne svrhe, a sa obavezom da štitimo njihovo pravo na privatnost biometrijskih podataka.

Prednost drugog pristupa se ogleda generalno u nižoj ceni formiranja ispitne baze podataka, jer su neke baze koje se mogu naći na Internetu uz određene uslove javno dostupne. Druga prednost drugog pristupa je u tome što neke baze biometrijskih podataka imaju *de facto* status referentnih baza podataka, pa je verodostojnije na njima međusobno upoređivati rezultata rada različitih algoritama iste namene, a koji se koriste u obradi biometrijskih podataka. Osnovni nedostatak drugog pristupa je krutost raspoloživih baza podataka, odnosno činjenica da se njihovi sadržaji ne mogu podešavati prema specifičnim potrebama nameravanog ispitivanja.

Uzimajući u obzir navedene prednosti i ograničenja oba pristupa, za potrebe naše studije odlučili smo da formiramo dve ispitne biometrijske baze podataka. Prva biometrijska baza podataka formirana je neposrednim

uzimanjem potrebnih biometrijskih podataka u okviru Laboratorije za multimedijalne komunikacije koja deluje na Fakultetu organizacionih nauka, a druga baza biometrijskih podataka je izvedena na osnovu dostupnih biometrijskih baza podataka na Internetu. Ova druga baza podataka sadrži više biometrijskih podataka i dozvoljava finije ispitivanje osetljivosti korišćenih algoritama na broj ispitanika u bazi podataka.

Nakon odabiranja ispitne klase multimodalnog biometrijskog sistema i formiranja odgovarajućih ispitnih baza biometrijskih karakteristika, bilo je potrebno odrediti arhitekturu takvog multimodalnog sistema i potom se opredeliti za neki od mogućih režima rada takvog sistema, da bi se istražio rad i ponašanje sistema i potvrde ili opovrgnu postavljene hipoteze. Opredelili smo se za paralelnu arhitekturu biometrijskog obradnog sistema i integraciju biometrijskih podataka na nivou rezultata upoređivanja ispitnog uzorka sa uzorcima uskladištenim u bazi uzoraka. Poslednji korak u dizajnu ispitnog sistema se odnosi na odabiranje nekih od poznatih metoda obrade, odnosno integracije biometrijskih podataka implementiranih u nekom od programskih jezika.

Potrebno je naglasiti upravo radi razjašnjenja poslednjeg metodološkog pitanja, koje se odnosi na zahtevane finansijske resurse, da smo se opredelili za dizajn prevashodno orijentisan na javna i slobodno dostupna programska rešenja sa otvorenim kodom (engl. *open source*). Dakle, naša konstrukcija ispitnog multimodalnog biometrijskog sistema se prvenstveno svodi na integraciju odabranih programskih komponenata, razvijenih širom sveta za potrebe takvih sistema, u jedinstvenu radnu celinu. Na taj način se minimiziraju troškovi razvoja, odnosno potrebe za finansijskim resursima. Osnovne gradivne komponente sistema čine programska rešenja koja podržavaju rad sa odabranim senzorima za uzimanje otisaka prstiju i slike crta lica. Ove komponente u načelu obezbeđuju isporučioci senzora. Na osnovu dobijenih sirovih biometrijskih podataka druge programske komponente treba da izvedu odabrane biometrijske karakteristike. Biometrijske karakteristike upisuju se u

skladu sa postavljenom strukturom zapisa, kao uzorak u bazu podataka. Posebnim programom za vreme rada sistema u režimu utvrđivanja identiteta, uzorci iz baze se čitaju i upoređuju sa ulaznim uzorkom. Namenski napisani programi, koje pišu integratori sistema, imaju zadatak da povežu odabrane programske komponente u celinu, kao i da obezbede komunikaciju korisnika sa sistemom. U okviru ove disertacije samo ćemo naznačiti čiji je softver korišćen za ekstrakciju i poređenje biometrijskih karakteristika.

Formiranjem eksperimentalnog multimodalnog sistema stvaraju se uslovi za sprovođenje odgovarajućih ispitnih testova nad opisanim bazama podataka. Dobijene rezultate potom treba analizirati sa stanovišta performansi u postupku utvrđivanja identiteta i izvesti odgovarajuće zaključke u odnosu na postavljene hipoteze.

Formalna specifikacija postupka utvrđivanje identiteta može da se posmatra na sledeći način:[303]

Neka imamo bazu biometrijskih uzoraka $\{I_1, I_2, ... I_N,\}$. Neka se na ulazu biometrijskog sistema nalazi uzorak nepoznate osobe I_Q. Biometrijski sistem treba da koristeći postupak uparivanja S uporedi ulazni uzorak I_Q sa *svakim* uzorkom u bazi. Ako je postupak S mera sličnosti dva posmatrana uzorka, onda najveća dobijena vrednost funkcije S na izlazu postupka uparivanja S (I_Q, I_K), dobijena za uzorak I_K iz baze uzoraka, određuje uzorak I_K kao *najsličniji* ulaznom uzorku I_Q. Ali, da bismo mogli *tvrditi* da uzorci I_Q i I_K pripadaju istoj osobi, potrebno je da dobijena vrednost sličnosti S (I_Q, I_K) bude veća ili jednaka postavljenom sigurnosnom pragu sličnosti t, ranije definisanom u poglavlju 5. Ako je, naprotiv, S (I_Q,I_K)<t, onda će sistem da zaključi da osoba sa uzorkom I_Q nema pohranjen uzorak u bazi uzoraka.

[303] A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, January (2004).

8.2. Formiranje ispitnih biometrijskih baza podataka

8.2.1. Multimodalna biometrijska baza kreirana na Fakultetu

Multimodalna biometrijska baza formirana je u Laboratoriji za multimedijalne komunikacije na Fakultetu organizacionih nauka, Baza I, i sadrži biometrijske podatke prikupljene od 39 ispitanika. Kreirana biometrijska baza je višenamenska i formirana je u skladu sa širim potrebama Projekta Ministarstva prosvete, nauke i tehnološkog razvoja čiji je nosilac ova Laboratorija.[304] Obuhvata više biometrijskih modova, i to: otiske prstiju, šaka, slike lica iz više položaja kamere u odnosu na glavu ispitanika, video zapis lica, kao i njihove glasovne zapise. Takođe, baza sadrži i posebne video zapise ispitanika kojima se opisuju i istražuju osobine hoda ispitanika koje pripadaju ponašajnim osobinama. Imajući u vidu naš predmet i cilj istraživanja, iz ove baze podataka koristili smo samo biometrijske modalitete otisaka prstiju i slike lica.

Otisci prstiju prikupljeni su uz pomoć dva različita skenera, optičkog i kapacitivnog. Za svakog ispitanika prikupljeno je po 16 uzoraka, i to po 4 uzorka kažiprsta i srednjeg prsta, leve i desne ruke. Uzorci sa optičkog skenera sačuvani su u *.png* formatu rezolucije 500x550 *piksela* i sa dubinom zapisa od 8 *bita* po *pikselu*. Otisci prsta prikupljeni putem kapacitativnog skenera su rezolucije 192x512 *piksela*, sa dubinom zapisa od 8 *bita* po *pikselu*, i sačuvani u *.bmp* formatu.

Akvizicija slika i video zapisa se odvijala u posebno pripremanom ambijentu sačinjenom od stolice, panoa i opreme za slikanje i snimanje. Ispitanik je sedeo na stolici, iza njega je postavljen jednobojni panel, koji obezbeđuje homogenu i jednobojnu pozadinu, a ispred njega foto-aparat i Internet kamera.

[304] Projekat *Primena multimodalne biometrije u menadžmentu identiteta*, finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, pod zavodnim brojem TR-32013.

Lice svakog ispitanika fotografisano je iz 9 različitih uglova. Početna pozicija fotoaparata je 0 stepeni, položaj kojim se dobija *en face* snimak lica. Naredne pozicije su 30, 45, 60 i 90 stepeni, respektivno na levu i desnu stranu od ispitanika. Kompletan proces uzimanja slika lica je sniman i korišćenjem Internet video-kamere, pri čemu se dešava da ispitanik izađe iz vidokruga kamere. Na ovaj način se simulira situacija iz realnog života u kojima sigurnosna kamera snima osobu iz različitih uglova.

Slike lica su kreirane uz pomoć foto aparata sa rezolucijom 10 *Mega piksela*, kako bi se dobio prosečan kvalitet slike sačuvan u .jpg formatu. Video snimci su snimani u .avi formatu rezolucije 320x240 *piksela* i sa 30 okvira u sekundi.

8.2.2. Kimerička multimodalna biometrijska baza

Za ispitivanje ponašanja algoritama implementiranih u programske komponente obradnog sistema u realnim uslovima ponekad je potrebno da odgovarajuća baza biometrijskih podataka sadrži znatno više podataka nego što ih ima u bazi formiranoj u Laboratoriji za multimedijalne komunikacije. U konkretnim slučajevima potrebno je takvu bazu naći na Internetu. Baza bi trebalo da bude multimodalna, sa traženim biometrijskim karakteristikama, što nije uvek moguće. Ako se, pak, mogu naći dve unimodalne baze sa traženim brojem uzoraka, ali dobijene od dve različite grupe ispitanika, moguće je formirati veštačku, ili *kimeričku*, multimodalnu biometrijsku bazu podataka.

Naš zahtev je bio da druga multimodalna baza sadrži biometrijske podatke za bar 500 ispitanika. Sa obzirom da u javnom domenu nije bilo moguće naći multimodalnu bazu ovog obima, izvršeno je spajanje podataka iz dostupnih baza *CASIA–FingerprintV5* i *CASIA-FaceV5*, formiranih od strane Instituta za automatizaciju kineske akademije nauka.[305] U daljem tekstu rada kimeričku bazu skraćeno ćemo nazivati Baza II.

[305] http://www.idealtest.org/index.jsp, pristupljeno 11.10.2012.

Baza *CASIA–FingerprintV5* originalno sadrži 20000 otisaka prstiju prikupljenih od 500 ispitanika. Otisci prstiju uzeti su u okviru jedne sesije. Za akviziciju podataka korišćen je model senzora *URU4000*. Prikupljeni su podaci od osoba oba pola, raspodeljenih po različitim starosnim grupama. Od svakog subjekta prikupljeno je 40 otisaka prsta, po pet od svakog skeniranog prsta. Akvizicija je vršena za palac, kažiprst, srednji prst i domali prst svake ruke. Prilikom uzimanja podataka od ispitanika bilo je zatraženo da rotiraju prste sa različitom jačinom pritiska, kako bi u uzorku bile zabeležene moguće varijacije unutar iste klase. Svi otisci prsta zapamćeni su u rezoluciji 328x356 piksela, sa dubinom od 8 bita po pikselu.

Baza *CASIA-FaceV5* originalno sadrži 2500 slika lica prikupljenih od 500 ispitanika. Slikanje lica svakog ispitanika vršeno je pomoću *Logitech USB* kamere i u okviru jedne sesije. Svaka slika crta lica je memorisana u formatu .bmp datoteke sa rezolucijom 640x480 *piksela*, pri čemu svaki *piksel* ima dubinu od 16 *bita*.

8.3. Ispitni multimodalni biometrijski sistem za utvrđivanje identiteta

8.3.1. Arhitektura ispitnog multimodalnog sistema za utvrđivanje identiteta

Opredelili smo se za arhitekturu ispitnog multimodalnog sistema sa paralelnim režimom rada. Kao što je rečeno u poglavlju 7, arhitektura sistema sa *paralelnim* režimom obrade omogućava da se biometrijski podaci relevantnih modova *simultano* obrađuju na svim logičkim nivoima koji prethode procesu fuzije, odnosno do nivoa integracije podataka, naravno u slučaju kada računarski sistem raspolaže sa više aplikativnih procesora. Savremeni računarski sistemi imaju procesore sa više jezgara, pa se simultana obrada pojedinih biometrijskih modova može jednostavno ostvariti sa povoljnim odnosom cene i postignutih performansi. Pored bržeg rada, sistemi sa paralelnim režimom rada mogu postići veću preciznost i doneti bolje zaključke,

jer se u trenutku donošenja odluke koriste više podataka, nego u rednom ili serijskom režimu rada.

8.3.2. Režim rada ispitnog multimodalnog sistema

Naš multimodalni biometrijski sistem projektovan je da radi u režimu integracije biometrijskih podataka na nivou izlaza skorova iz modula upoređivanja ulazne upitne karakteristike sa uzorcima uskladištenih karakteristika u relevantnoj bazi karakteristika. Dakle, simultano za oba posmatrana moda, otiska prsta i slike crta lica, u prvom koraku može da se uzme odgovarajući biometrijski podatak I_Q od ispitanika Q pomoću senzora. U drugom koraku, na osnovu akviriranog sirovog biometrijskog podatka može da se izvede odgovarajuća karakteristika I_Q, i potom u trećem koraku da se pomoću odabrane funkcije sličnosti S izračuna skor podudaranja karakteristike I_Q sa svakom od uskladištenih karakteristika I_K, S (I_Q, I_K). Naravno potrebno je da se algoritmi na osnovu kojih se implementira funkcija sličnosti S u opštem slučaju razlikuju, kao i da zavise od odabranog biometrijskog moda, načina izvođenja i predstavljanja karakteristike u bazi podataka.

Za potrebe našeg istraživanja u kojem se ispituju performanse multimodalnog biometrijskog sistema sa otiscima prstiju i slikama lica korisnika, korišćena sa dva javno dostupna *open source* programska rešenja. Za rad sa otiscima prsta korišćen je *NIST*-ov programski paket *NBIS* (engl. *NIST Biometric Image Software - NBIS*), razvijen od strane Nacionalnog instituta za standarde i tehnologiju Sjedinjenih Američkih Država (*The National Institute of Standards and Technology - NIST*).[306] Ovo programsko rešenje ima više paketa, a za naše potrebe koristili smo *MINDCT* paket za izdvajanje karakteristika iz akviriranih otisaka prstiju sa *BOZORTH3* modulom za upoređivanje izdvojenih karakteristika. Za rad sa drugim modom, slikama lica ispitanika, napisana je aplikacija uz pomoć biblioteke otvorenog koda za računarsku viziju *OpenCV*

[306] http://www.nist.gov/itl/iad/ig/special_dbases.cfm, pristupljeno 05.10.2012.

(engl. *Open Source Computer Vision Library – OpenCV*).[307] U *OpenCV* biblioteci za identifikaciju osobe na osnovu slika lica koriste se metodi analize glavnih komponenti, *PCA* i metod klasifikacije uzoraka nepoznatih klasa statističkim pristupom, *LDA*, ranije opisan u 6. poglavlju rada.

Nakon izračunavanja skorova poređenja S (I_Q, I_K) za oba posmatrana moda, prsta s_1 i lica s_2, a pre fuzije oba skora u jedinstven skor, potrebno je normalizovati vrednosti oba skora. U našem istraživanju multimodalne biometrije za normalizaciju dobijenih skorova poređenja, za modove otiska prsta i slike crta lica, koristili smo četiri postupka normalizacije izložena u radu Snelicka i koautora, poznate pod nazivima *Min-Max*, *Z-score*, *Tanh i Adaptivna normalizacija (AD).* [308]

8.3.2.1. Normalizacija skorova poređenja

U formulama koje slede, konkretnu vrednost skora poređenja koja ulazi u postupak normalizacije predstavljena je sa s, gde *S* predstavlja slučajnu promenljivu skorova poređenja, a *n* normalizovanu vrednost skora.

Min-Max metoda preslikava sve vrednosti ulaznih skorova poređenja u interval vrednosti [0,1]. Izrazi *min(S)* i *max(S)* označavaju minimalne, odnosno maksimalne vrednosti slučajne promenljive *S*, respektivno.

$$n = \frac{s - \min(S)}{\max(S) - \min(S)} \tag{1}$$

Z-score metoda standardizuje slučajnu promenljivu S na normalnu raspodelu sa aritmetičkom sredinom 0 i standardnom devijacijom 1, odnosno sa N(0,1). Izrazi *mean(S) i std(S)* označavaju aritmetičku sredinu, odnosno standardnu devijaciju slučajne promenljive *S*, respektivno.

[307] http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html?highlight=pca, pristupljeno 15.11.2012.

[308] R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, *Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems,* IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, March (2005), str. 450-455.

$$n = \frac{s - mean(S)}{std(S)} \tag{2}$$

Tanh metod pripada takozvanim robusnim statističkim metodima i ima takođe zadatak da preslika ulazne skorove poređenja u interval [0,1].

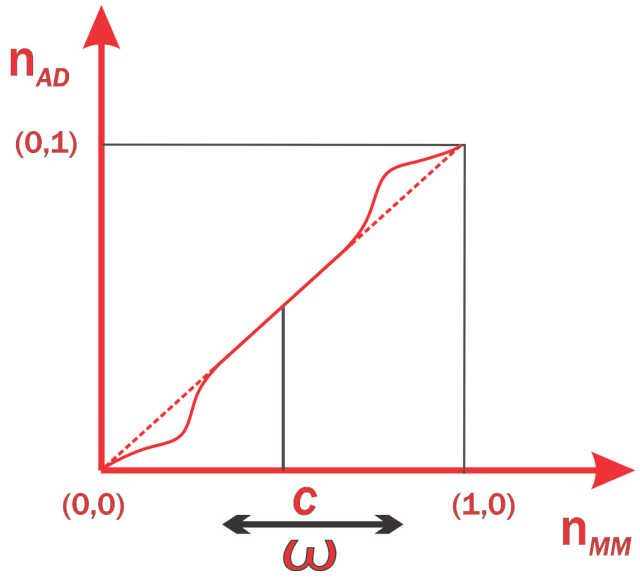
$$n = \frac{1}{2}\left[\tanh\left(0.01\frac{s - mean(S)}{std(S)}\right) + 1\right] \tag{3}$$

Adaptivna kvadratna-linijska-kvadratna normalizacija (QLQ): Snelick i ostali[309] su razvili metod normalizacije u kojem greške individualnih modula za poređenje proističu iz preklapanja raspodela skorova za autorizovane korisnike i uljeze. Oni su opisali ovu oblast preklapanja sa dva parametra, centrom *c* i širinom ω. U svom radu su naveli da je cilj primene adaptivnog postupka normalizacije povećanje razdvajanje raspodela autorizovanih korisnika i uljeza, pri čemu skorovi takođe treba da se preslikaju na opseg vrednosti [0,1].

Adaptivna normalizacija je formulisana izrazom $n_{AD} = f(n_{MM})$, gde $f(n_{MM})$, označava funkciju mapiranja koja se primenjuje na *Min-Max* (MM) normalizovane skorove, n_{MM}. Zona preklapanja, sa centrom *c* i širinom ω, ostaje nepromenjena dok se druga područja mapiraju sa dva segmenta kvadratne funkcije, dijagram 2:[310]

$$n_{AD} = \begin{cases} \frac{1}{(c-\frac{\omega}{2})} n_{MM}^2 \\ \left(c+\frac{\omega}{2}\right)+\sqrt{\left(1-c-\frac{\omega}{2}\right)\left(n_{MM}-c-\frac{\omega}{2}\right)} \end{cases} \begin{matrix} n_{MM} \le (c-\omega/2) \\ (c-\frac{\omega}{2}) < n_{MM} \le (c+\frac{\omega}{2}) \end{matrix} \tag{4}$$

[309] *Ibid.str. 450.*
[310] *Ibid.str. 451.*



Dijagram 2 Adaptivna QLQ normalizacija

8.3.2.2. Fuzija skorova upoređenja

Testiranje hipoteza o prednostima multimodalne biometrije u odnosno na unimodalna rešenja vršeno je u fazi fuzije kombinovanjem normalizovanih izlaznih parcijalnih skorova poređenja u jedinstveni multimodalni skor, kao integralne mere podudaranja ulaznih biometrijskih podataka sa onim uskladištenim u bazi podataka za svakog korisnika. Korišćena su tri načina kombinovanja normalizovanih parcijalnih skorova, i to: metod fuzije prostim sabiranjem normalizovanih skorova, metod fuzije sabiranjem normalizovanih skorova pomnoženih sa težinskim koeficijentima dodeljenih modulima upoređivanja za posmatrani biometrijski mod i metod fuzije sabiranjem normalizovanih skorova pomnoženih sa težinskim koeficijentima dodeljenih modulima upoređivanja, ali koji mogu biti specifični za svakog korisnika pojedinačno.

Posebno treba reći da treći postupak integracije normalizovanih skorova omogućava neku od strategije suprotstavljanja problemu opisanom u 5. poglavlju disertacije terminom *biometrijska menažerija*. Naime, težinski faktori specifični za svakog korisnika mogu se podesiti tako da, u slučaju kada karakteristike korisnika sistema imaju obeležje poznato u biometrijskoj

menažeriji kao tip *jagnjeta*, bolje razdvajaju takvog korisnika od uljeza čije karakteristike pripadaju tipu *vuk* i na taj način umanje vrednost FAR parametra sistema. Dakle, ovakvim pristupom se minimizira jedna od sistemskih slabosti biometrijskih sistema.

U formulama koje slede n_i^m predstavlja normalizovani skor na m-tom modulu za uparivanje karakteristika i-tog korisnika. Integralni skor za i-tog korisnika, kao rezultat postupka fuzije, je označen sa f_i.

Fuzija izvedena postupkom prostog zbira normalizovanih skorova:

$$f_i = \sum_{m=1}^{M} n_i^m, \forall i \tag{5}$$

Fuzija izvedena postupkom zbira normalizovanih skorova pomnoženih sa težinskim koeficijentima dodeljenih modulima upoređivanja:

$$f_i = \sum_{m=1}^{M} \omega^m n_i^m, \forall i \tag{6}$$

gde ω^m predstavlja težinske faktore dodeljen svakom modulu upoređivanja zasnovane na vrednosti skora za koju važi jednakost vrednosti parametara FAR i FRR (EER tačka), a r^m predstavlja EER vrednost m-tog modula upoređivanja, po formuli:

$$\omega^m = \frac{1/\Sigma_{m=\frac{1}{r^m}}^{M}}{r^m} \tag{7}$$

Fuzija izvedena postupkom zbira normalizovanih skorova pomnoženih sa težinskim koeficijentima dodeljenih modulima upoređivanja specifičnih za svakog pojedinačnog korisnika:

$$f_i = \sum_{m=1}^{M} \omega_i^m \, n_i^m, \forall i \tag{8}$$

gde ω_i^m predstavlja težinski koeficijent m-tog modula upoređivanja za i-tog korisnika, a izračunava se na sledeći način:

$$\omega_i^m = \frac{1}{\sum_{m=1}^{M} d_i^m} d_i^m \tag{9}$$

$$d_i^m = \frac{\mu_i^m(autor) - \mu_i^m(uljez)}{\sqrt{(\sigma_i^m(autor))^2 + (\sigma_i^m(uljez))^2}} \tag{10}$$

gde su $\mu_i^m(autor)$ i $\mu_i^m(uljez)$ očekivane vrednosti raspodela skorova autorizovanih korisnika i uljeza, a $(\sigma_i^m(autor))^2$ i $(\sigma_i^m(uljez))^2$ njihove varijanse. Formula (10) omogućava izračunavanje vrednosti d_i^m, kao mere udaljenosti raspodela *i*-tog autorizovanog korisnika i uljeza kada se koristi *m*-ti modul za upoređivanje. Ako je d_i^m malo, onda je i-ti korisnik na m-tom modulu za upoređivanje u statusu jagnjeta, pa treba primeniti posebne težinske koeficijente, date formulom (9), kojima se smanjuje ova slabost.

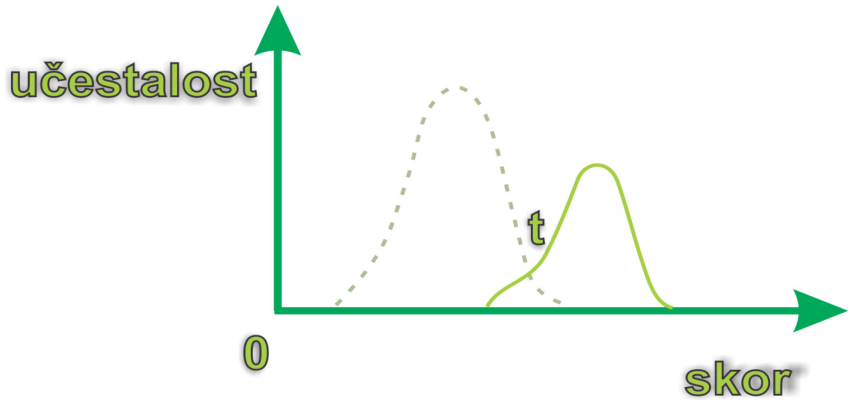
8.3.3. Postupak ispitivanja performansi multimodalnog biometrijskog sistema

U ovom delu rada je izložen postupak ispitivanja performansi eksperimentalnog multimodalnog biometrijskog sistema u slučajevima kada se koriste po jedan ili oba raspoloživa biometrijska modaliteta, otiska prsta i slike lica. U skladu sa postavljenim hipotezama istražuje se odnos performansi biometrijskog sistema, tako što se prvo analizira rad sistema u unimodalnim režimima rada, a zatim i u multimodalnom režimu rada. U istraživanju se koriste četiri prethodno opisana postupka normalizacije podataka, a svaki postupak normalizacije prate odabrana tri načina integracije multimodalnih biometrijskih podataka. Ceo postupak istraživanja se kompletno ponavlja nad dve odvojene, i ranije opisane multimodalne biometrijske baze podataka.

Imajući u vidu da baze podataka sadrže više instanci jednog moda, ispitivanje sistema započinje prvim korakom tako što se jedan od otisaka *nekog* prsta iz baze podataka koristi kao ulazni podatak za upoređivanje sa svim ostalim otiscima *istog* prsta odabrane osobe, kako bi se odredio skor sličnosti. Pritom se izabrani otisak prsta markira u bazi podataka da ne bi bio uzet u postupku upoređivanja. Postupak se ponavlja za sve ostale prste odabrane

osobe. Nakon toga ceo proces se ponavlja za sve ostale osobe u biometrijskoj bazi sa otiscima prstiju. Svi dobijeni skorovi se memorišu i na kraju se generiše histogram skorova pravih korisnika koji se javlja u režimu verifikacije identiteta.

U drugom koraku se instanca otiska *nekog* prsta jedne osobe upoređuje sa *svim* instancama otisaka *istog* prsta *svih drugih* osoba u bazi otisaka prstiju kako bi se dobili odgovarajući skorovi sličnosti. Postupak se ponavlja za instance drugih prstiju *iste* osobe. Nakon toga postupak se ponavlja sa otiscima drugih osoba, naravno vodeći računa da su neki skorovi sličnosti već ranije generisani! Svi dobijeni skorovi se memorišu i na kraju se generiše histogram skorova koji u režimu verifikacije odgovara skorovima uljeza, odnosno osobama koje se lažno predstavljaju. Primer tako generisanih histograma skorova pravih korisnika i uljeza dat je na dijagramu 3.



Dijagram 3 Primer histograma raspodele skorova

Gore navedeni postupak se primenjuje za svaki od modova, a u našem slučaju za uzorke slika lica u bazi lica.

Nakon što se odrede histogrami za oba biometrijska moda variranjem vrednosti sigurnosnog praga, *t*, može se odrediti zavisnost parametara ranije definisanih parametara *FAR* i *FRR*, odnosno *ROC* dijagram radnih karakteristika (engl. *Receiver Operating Characteristic - ROC*).

U cilju provere postavljenih hipoteza ukupno je izvršeno 40 različitih testova rada biometrijskog sistema, a rezultati rada su privremeno zapisani u odgovarajuće datoteke. Potom je u postupku postprocesorske obrade posebnim programima sa mogućnošću grafičkog prikaza izvršeno spajanje pojedinih rezultata obrade, tako da je dobijeno ukupno 8 grafičkih prikaza, po četiri za svaku korišćenu bazu podataka. Svaki grafički prikaz pokazuje performanse sistema u uobičajenom pravouglom koordinatnom sistemu sa stopom pogrešnog prihvatanja identiteta, parametar *FAR* ili češće *FMR* (engl. *False Match Rate, FMR*) na x-osi i stopom prihvatanja autorizovanih korisnika (engl. *Genuine Accept Rate, GAR*) na y-osi.

Svaki grafik sadrži prikaz uticaj odabranog načina normalizacije skorova na performanse sistema koristeći tri načina fuzije odabranih biometrijskih modaliteta, otiska prsta i slike lica. Radi upoređenja i kvantitativne provere polazne hipoteze da multimodalna biometrija pruža bolje performanse u odnosu na unimodalne sisteme, na istom grafiku su date performanse sistema kada radi u oba unimodalna režima rada.

U prikazanim rezultatima zanemaren je procenat ispitanika koji ne može da daju svoje biometrijske uzorke (engl. *Failure to capture rate*, *FTC*), tako da važi jednačina:

$$GAR = 1 - FRR \tag{11}$$

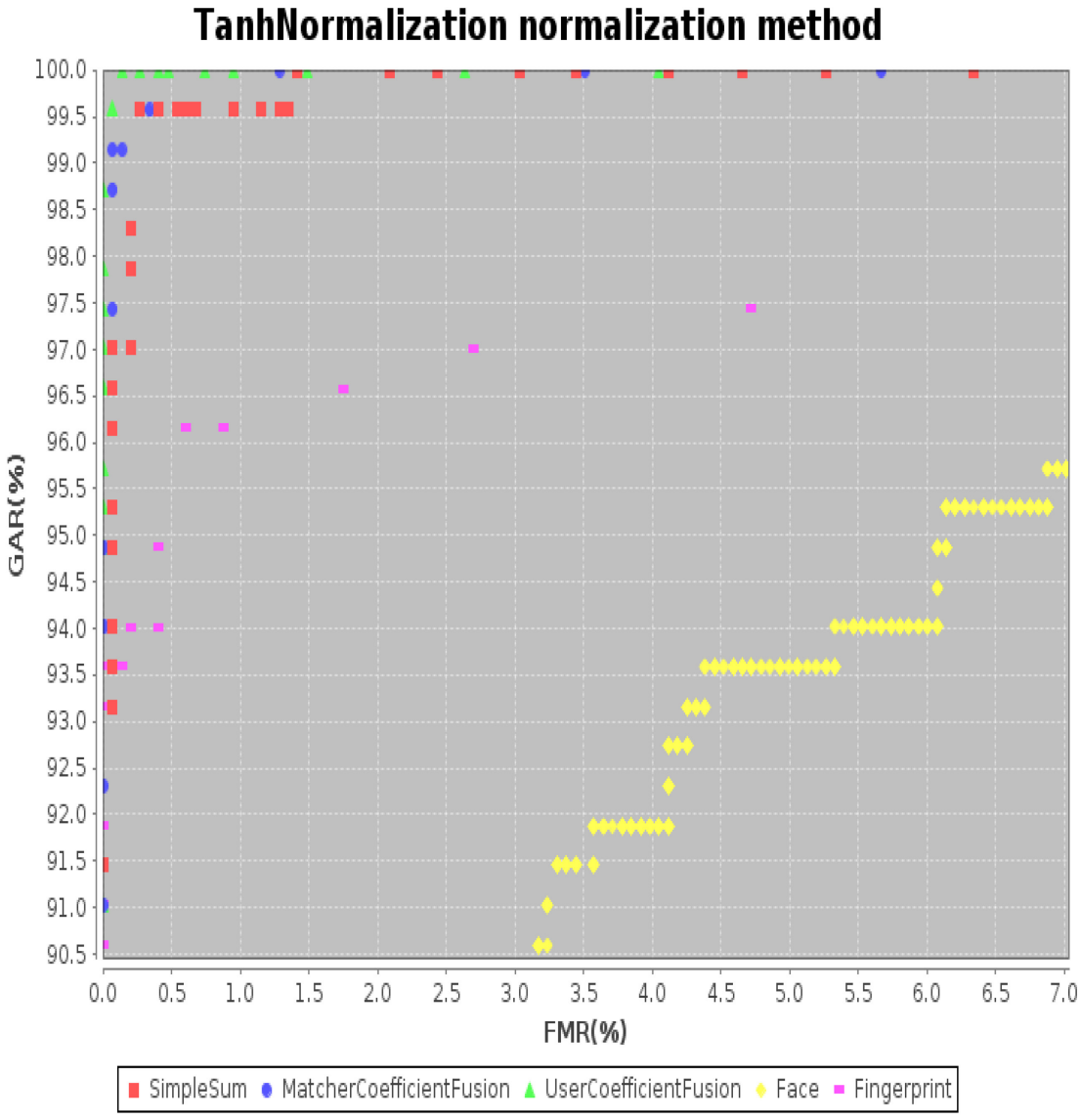
U legendi grafika korišćeni su sledeći engleski izrazi:

SimpleSum	za fuziju skorova tehnikom prostog zbira
MatcherCoefficientFusion	za fuziju skorova tehnikom težinskih koeficijenata dodeljenih modulima za upoređivanje
UserCoefficientFusion	za fuziju skorova tehnikom težinskih koeficijenata dodeljenih modulima za upoređivanje za svakog korisnika
Face	biometrijski mod predstavljen slikom lica osobe
Fingerprint	biometrijski mod predstavljen otiskom prsta osobe.

8.4. Rezultati ispitivanja multimodalnog biometrijskog sistema

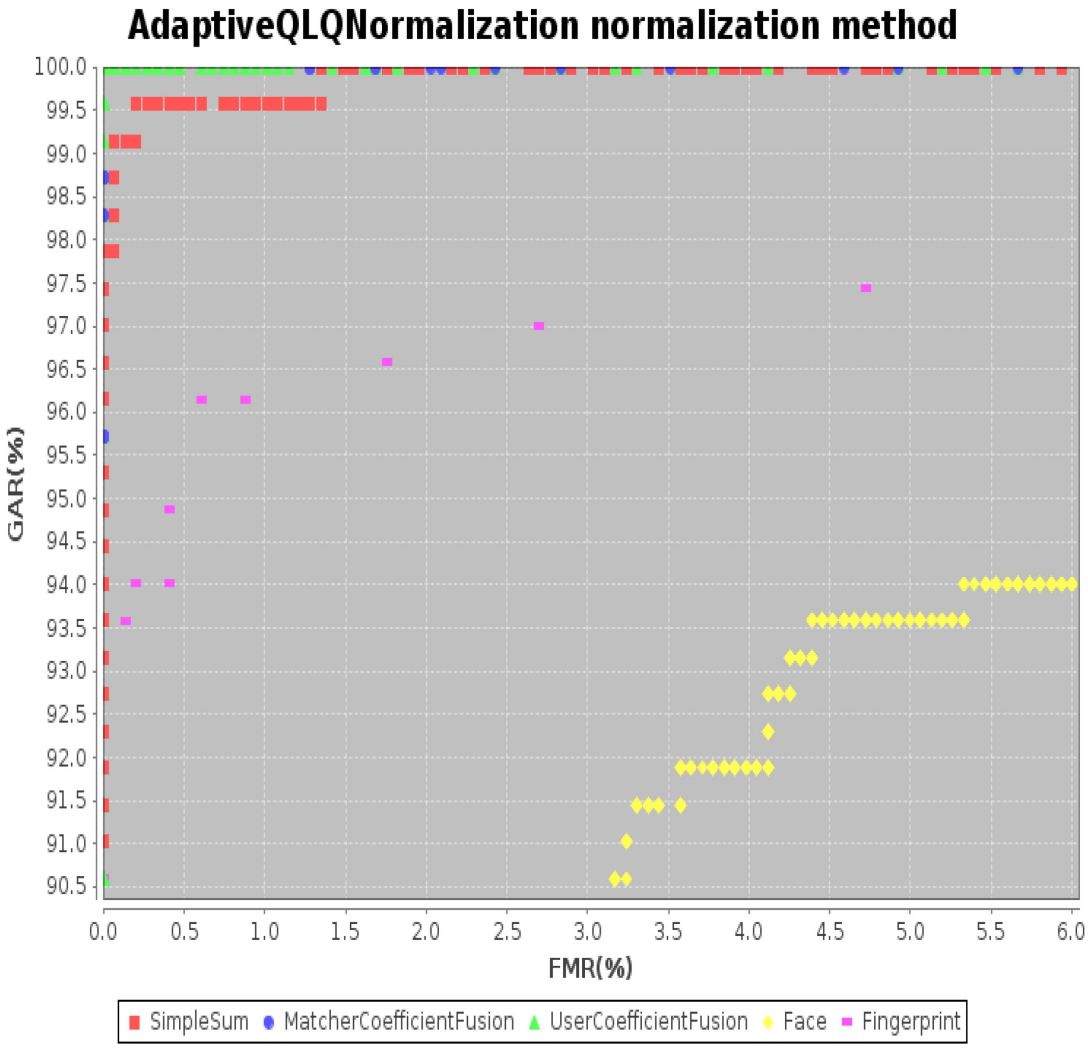
8.4.1. Performanse biometrijskog sistema u radu sa Bazom I

Na dijagramu 4 prikazane su performanse biometrijskog sistema sa *Tanh* metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa Bazom I, formiranom na Fakultetu organizacionih nauka.



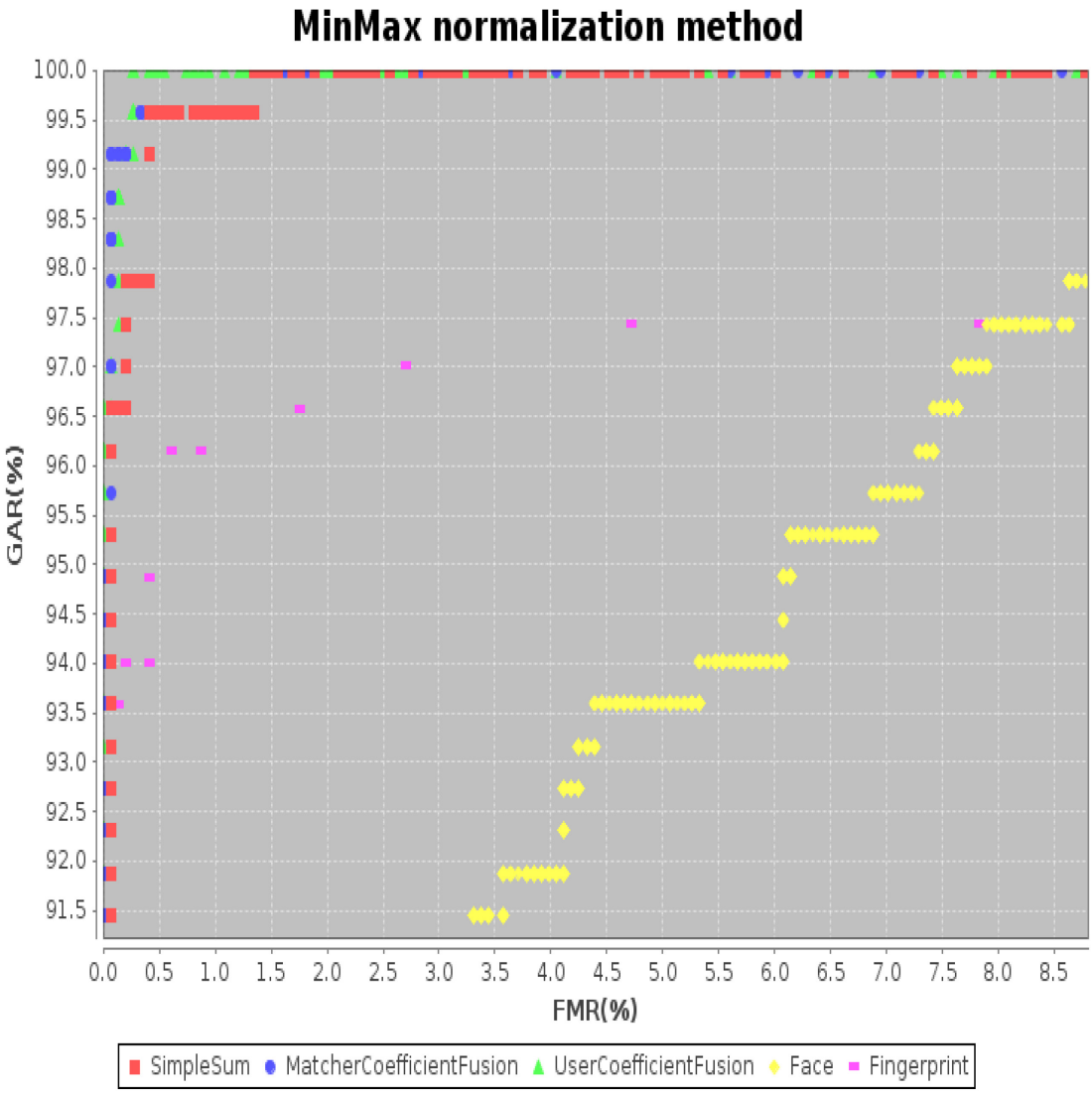
Dijagram 4 Performanse sistema sa Tanh *metodom normalizacije u radu sa Bazom I*

Na dijagramu 5 prikazane su performanse biometrijskog sistema sa QLQ adaptivnom metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa Bazom I, formiranom na Fakultetu organizacionih nauka.



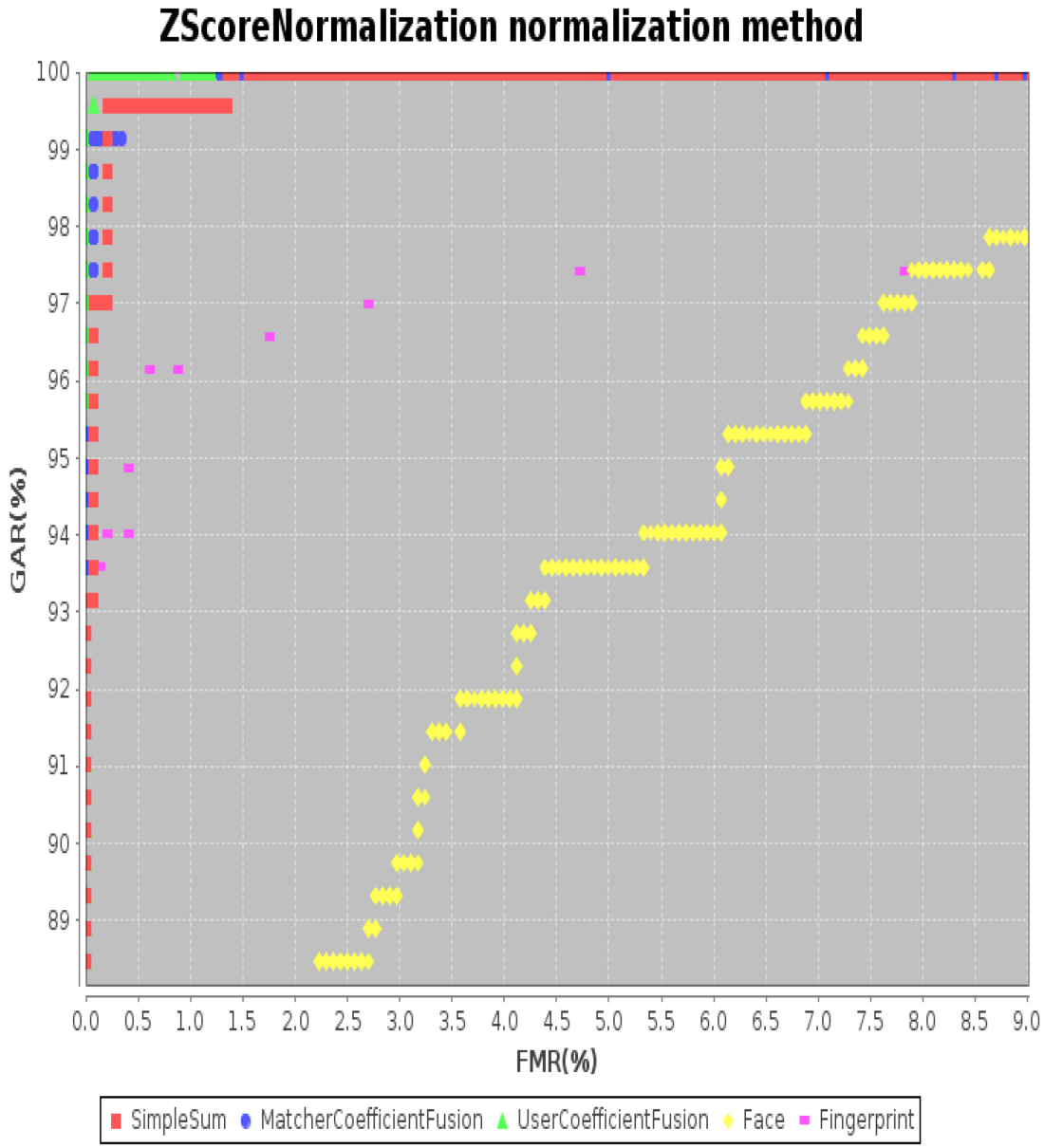
Dijagram 5 Performanse sistema sa QLQ *metodom normalizacije u radu sa Bazom*

Na dijagramu 6 prikazane su performanse biometrijskog sistema sa *MinMax* metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa Bazom I, formiranom na Fakultetu organizacionih nauka.



Dijagram 6 Performanse sistema sa metodom MinMax *normalizacije u radu sa Bazom I*

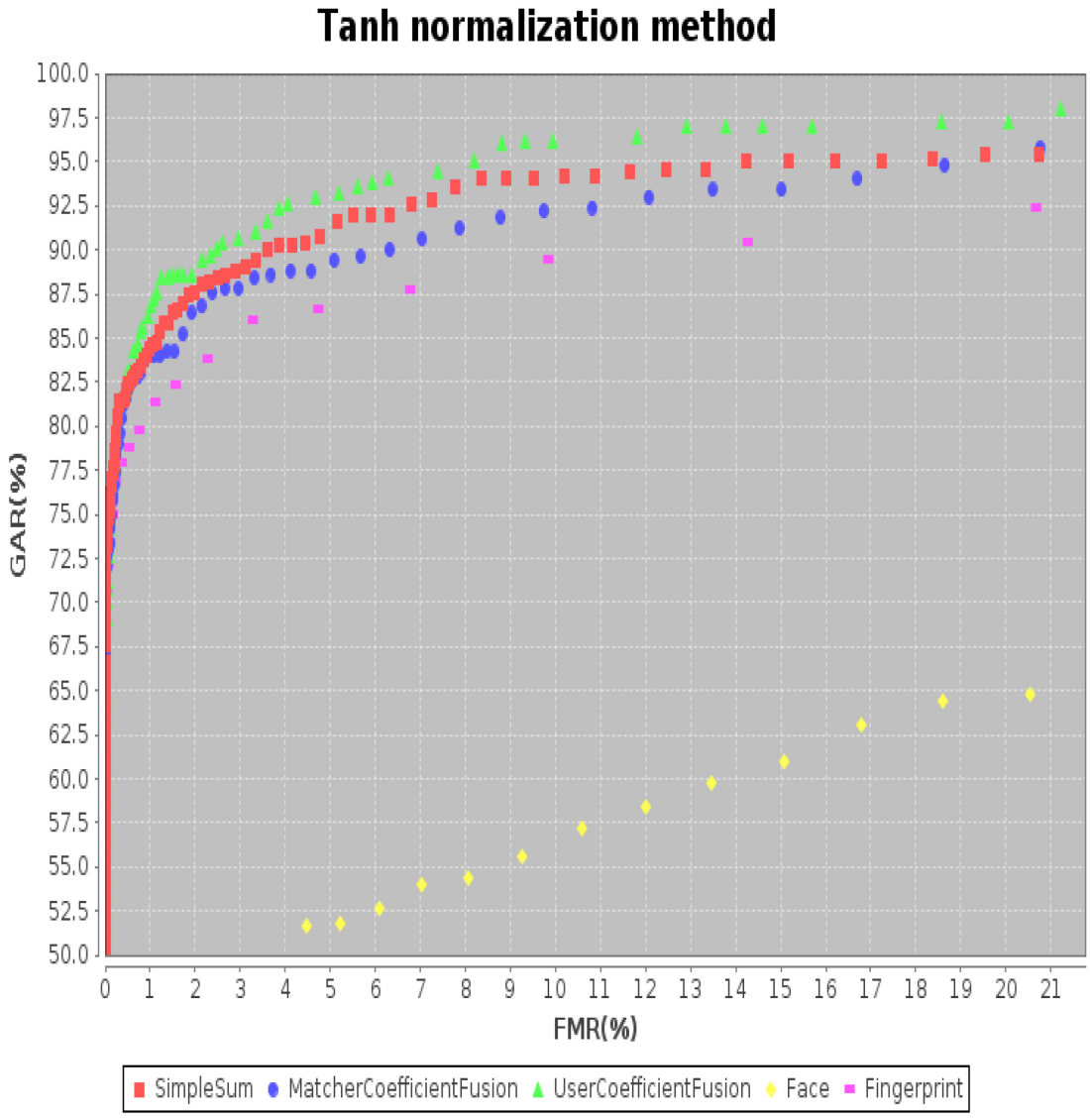
Na dijagramu 7 prikazane su performanse biometrijskog sistema sa *ZScore* metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa Bazom I, formiranom na Fakultetu organizacionih nauka.



Dijagram 7 Performanse sistema sa metodom ZScore *normalizacije u radu sa Bazom I*

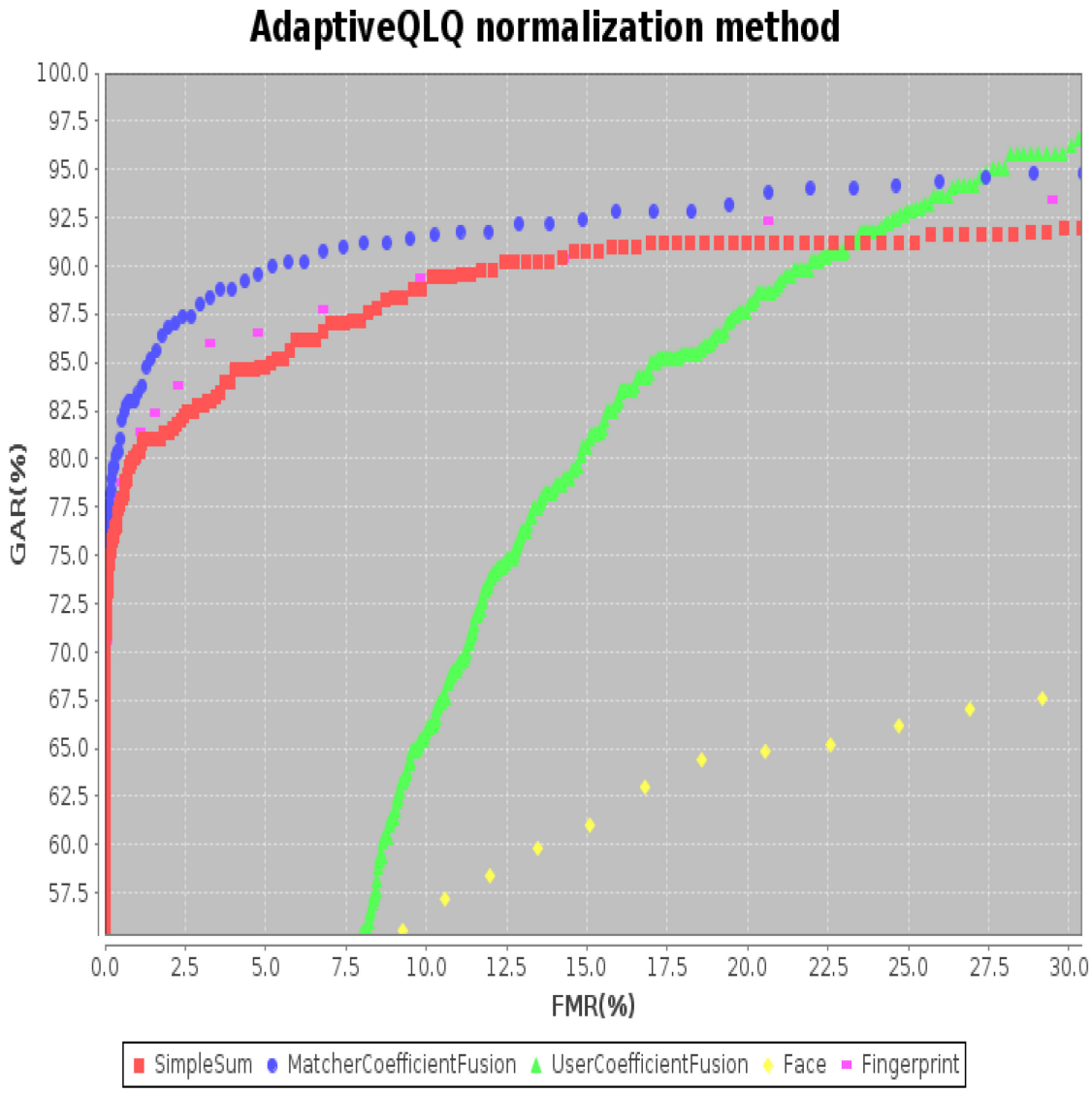
8.4.2. Performanse biometrijskog sistema u radu sa Bazom II

Na dijagramu 8 prikazane su performanse biometrijskog sistema sa *Tanh* metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa kimeričkom bazom biometrijskih podataka, Bazom II.



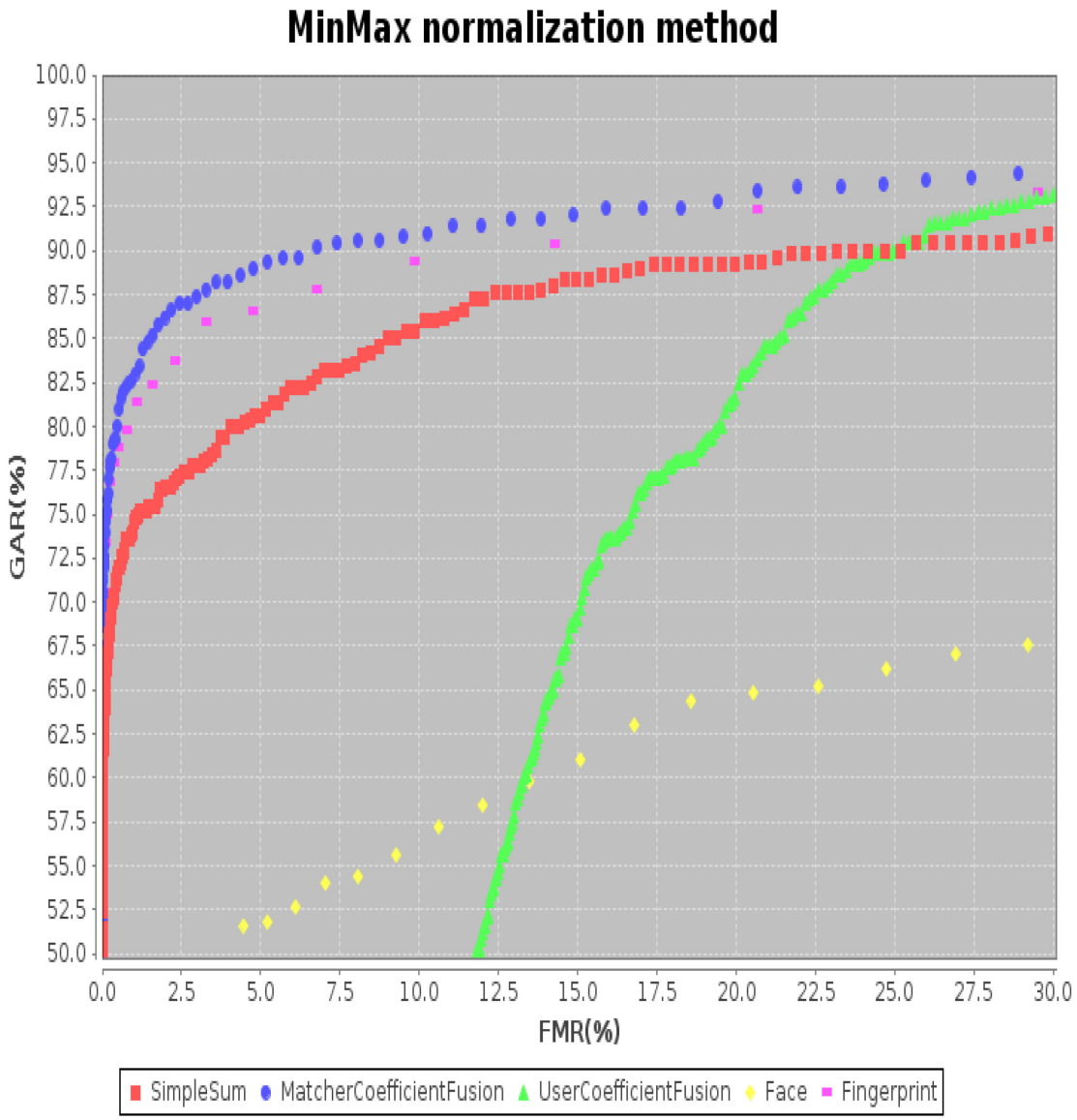
Dijagram 8 Performanse sistema sa Tanh *metodom normalizacije u radu sa Bazom II*

Na dijagramu 9 prikazane su performanse biometrijskog sistema sa *QLQ* adaptivnom metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa kimeričkom bazom biometrijskih podataka, Bazom II.



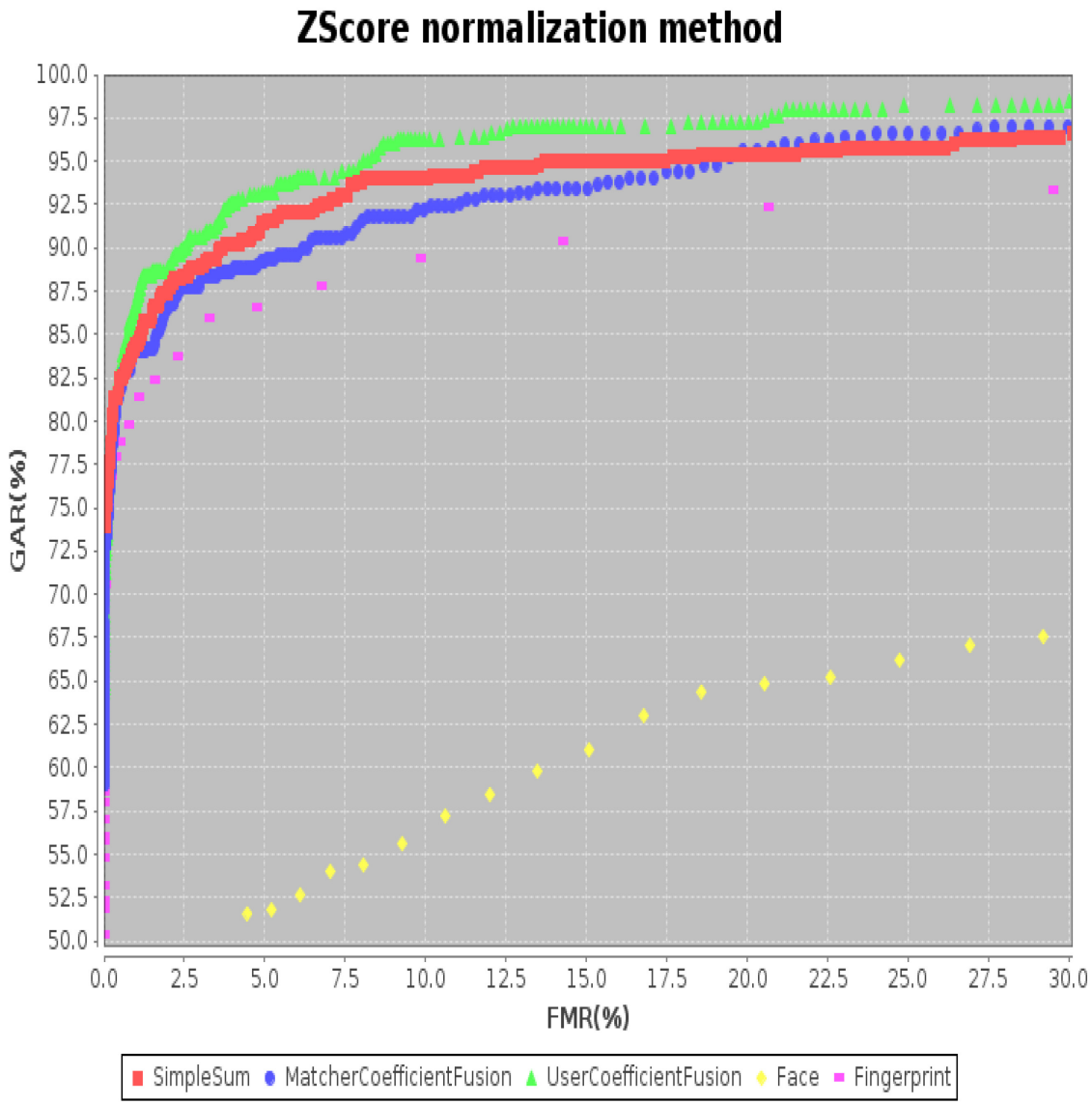
Dijagram 9 Performanse sistema sa QLQ *metodom normalizacije u radu sa Bazom I*

Na dijagramu 10 prikazane su performanse biometrijskog sistema sa *MinMax* metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa kimeričkom bazom biometrijskih podataka, Bazom II.



Dijagram 10 Performanse sist. sa MinMax *metodom normalizacije u radu sa Bazom II*

Na dijagramu 11 prikazane su performanse biometrijskog sistema sa *QLQ* adaptivnom metodom normalizacije skorova u multimodalnom i unimodalnim režimima rada sa kimeričkom bazom biometrijskih podataka, Bazom II.



Dijagram 11 Perform. sistema sa ZScore *metodom normalizacije u radu sa Bazom II*

8.5. Analiza performansi ispitnog multimodalnog sistema

8.5.1. Analiza performansi nad bazom Fakulteta organizacionih nauka

Podaci koje je generisao eksperimentalni biometrijski sistem u radu sa bazom podataka Baza I, odnosno sa bazom formiranom na Fakultetu organizacionih nauka, su obrađeni u skladu sa opisom datim u sekciji 8.3.3. Uvid u grafičke prikaze svodnih rezultata obrade, datih dijagrama 4, 5, 6, i 7, kvalitativno potvrđuje jednu od polaznih hipoteza *da primena multimodalnih biometrijskih metoda u sistemima identifikacije omogućava nalaženje rešenja sa boljim performansama u odnosu na konkurentska unimodalna rešenja*.

Za ocenu performansi biometrijskih sistema korišćeni su uobičajeni *ROC* dijagrami sa *FMR*/*GAR* stopama kao osama koordinatnog sistema. Na ovim graficima su, pored postignutih performansi multimodalnih rešenja, uporedno prikazane i performanse biometrijskog sistema kada sistem radi sa samo jednim od dva biometrijska modaliteta, otiskom prsta i slikom lica. Kao što je već rečeno, u multimodalnom rešenju se povezuju skorovi dobijeni na izlazima oba modula za upoređivanje karakteristika, tako što se skorovi najpre podvrgnu procesu normalizacije jednom od četiri odabrana metoda u jedinstveni skor, a potom se integrišu pomoću jedne od tri razmatrane metode fuzije.

Za sve navedene kombinacije unimodalna rešenja su znatno slabija od multimodalnih rešenja. Korisno je performanse biometrijskog sistema identifikacije posmatrati preko vrednosti *EER* parametra, odnosno preko one vrednosti sigurnosnog praga, *t* koji kao radnu tačka sistema definiše onu tačku u kojoj su izjednačene vrednosti *FMR* i *FRR* merene procentima. U Tabeli 3 prikazane su ocenjene vrednosti *EER* parametara za različite ispitivane kombinacije metoda normalizacije i metoda fuzije multimodalnog sistema u radu nad bazom Fakulteta organizacionih nauka (Baza I). Manje vrednosti *EER* upućuje na bolji biometrijski sistem.

Tabela 3 Vrednosti EER parametara u procentima za različite kombinacije metoda normalizacije i metoda fuzije

Metod normalizacije	*Metod fuzije*		
	Prost zbir normalizovanih skorova	***Zbir sa težinskim koeficijentima modula upoređivanja***	***Zbir sa težinskim koeficijentima modula upoređivanja posebnim za svakog korisnika***
MinMax	0,7	0,4	**0,2**
Tanh	0,5	0,3	**0,1**
ZScore	0,3	0,2	**0,1**
QLQ	0,5	0,3	**<0,1**

Prema rezultatima prikazanim u Tabeli 3 najbolja tačnost u postupku identifikacije, *cca* 0,1%, multimodalnog biometrijskog sistema, u slučaju rada sa bazom podataka kreiranom na Fakultetu organizacionih nauka, dobija se kombinacijom metoda *QLQ* adaptivnog sistema normalizacije skoreva sa izlaska modula za upoređenje i metoda fuzije normalizovanih skoreva prethodno pomnoženih težinskim koeficijentima modula upoređivanja specifičnim za svakog korisnika. Navedeni metod fuzije normalizovanih podataka prema dobijenim podacima se pokazao kao optimalan metod fuzije u bilo kojoj kombinaciji sa metodom normalizacije.

Ipak, interesantno je napomenuti da se u našem istraživanju kao najrobusniji metod normalizacije nametnuo *ZScore* metod, jer statistički posmatrano daje vrlo dobre rezultate u pogledu tačnosti rada multimodalnog sistema bez obzira na korišćeni metod fuzije. U našem slučaju u režimu unimodalnog rada sa otiscima prstiju ocenili smo *EER* vrednost *cca* 3 %, a sa slikom lica *cca* 6 %, što i kvantitativno potvrđuje ispravnost polazne hipoteze o prednosti multimodalnih (*EER* 0,1%) nad pojedinim unimodalnim rešenjima

(*EER* 3%, odnosno *EER* 6%). Istraživanje sprovedeno nad bazom podataka Fakulteta organizacionih nauka pokazuje dobro slaganje sa rezultatima publikovanim od strane *Jaina*, *Nandakumara* i *Rossa*.[311]

Ako se porede dobijeni rezultati za *EER* sa rezultatima *Snelicka* i ostalih, može se primetiti da smo dobili više puta bolje vrednosti, ali odmah treba naglasiti da je i naš broj ispitanika (39) bio više puta manji od baze ispitanika u *Snelickovom* istraživanju (972).[312] Upravo to je bio i jedan od razloga da se istraživanje ponovi sa bazom koja sadrži veći broj korisnika, odnosno koja će za više od reda veličine nadmašiti broj korisnika u opisanom eksperimentu.

8.5.2. Analiza performansi nad kimeričkom bazom

Grafički prikaz svodnih rezultata istraživanja sa eksperimentalnim biometrijskim sistemom nad bazom kimeričkom bazom podataka, Baza II, koja sadrži biometrijske podatke o 500 korisnika, dat je dijagramima 8, 9, 10 i 11. Odmah se može primetiti da postoji uočljiva razlika između ovih dijagrama i dijagrama koji su se odnosili na rad sa Bazom I. Jasno iskazana prednost multimodalnih biometrijskih sistema, izložena u sekciji 8.5.1, nije potvrđena za sve istraživane kombinacije normalizacije skorova i odabrane tehnike fuzionisanja normalizovanih skorova!

U Tabeli 4 prikazane su ocenjene vrednosti EER parametara za različite ispitivane kombinacije metoda normalizacije i metoda fuzije multimodalnog sistema u radu nad kimeričkom bazom, Baza II.

[311] A.Jain, K.Nandakumara, A.Ross, *Score normalization in multimodal biometric systems*, Pattern Recognition 38 (2005), str. 2270–2285.
[312] R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, *Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems,* IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, March 2005.

Tabela 4 Vrednosti EER parametara u procentima za različite kombinacije metoda normalizacije i metoda fuzije

Metod normalizacije	*Metod fuzije*		
	Prost zbir normalizovanih skorova	***Zbir sa težinskim koeficijentima modula upoređivanja***	***Zbir sa težinskim koeficijentima modula upoređivanja posebnim za svakog korisnika***
MinMax	12,5	**8,5**	18
Tanh	7,2	8,1	**6,5**
ZScore	7,4	8,2	**6,2**
QLQ	10	**8**	16

Prema rezultatima prikazanim u *Tabeli 4* najbolja tačnost u postupku identifikacije, *cca* 6,2%, multimodalnog biometrijskog sistema, u slučaju rada sa kimeričkom bazom podataka, dobija se kombinacijom metoda *ZScore* normalizacije skoreva sa izlaska modula za upoređenje i metoda fuzije normalizovanih skoreva prethodno pomnoženih težinskim koeficijentima modula za upoređivanje specifičnim za svakog korisnika. Zadovoljavajuće rezultate (*EER cca* 6,5%) dobili smo i u slučaju kombinacije *Tanh* metoda normalizacije sa istim metodom fuzije. Još treba pomenuti kombinaciju *QLQ* metoda normalizacije i metod fuzije sa zbirom normalizovanih skoreva prethodno pomnoženih težinskim koeficijentima modula upoređivanja (*EER cca* 8%) i *MinMax* tehniku normalizacije u kombinaciji sa istim metodom fuzije (*EER cca* 8,5).

U ovom delu istraživanja *ZScore* metodu, kao robusnom metodu normalizacije, pridružio se i *Tanh* metod normalizacije, jer daju slične rezultate u pogledu tačnosti sistema, bez obzira na korišćeni metod fuzije. Upravo, primena ove dve tehnike normalizacije i u drugom nizu eksperimenata potvrđuje polaznu hipotezu da *primena multimodalnih biometrijskih metoda u*

sistemima identifikacije omogućava nalaženje rešenja sa boljim performansama u odnosu na konkurentska unimodalna rešenja.

Međutim, metod fuzije sa težinskim koeficijentima modula za upoređivanja specifičnim za svakog korisnika pokazao je neprihvatljivo velike varijacije za vrednost *EER* parametara (*EER* od 6,2 do 18 procenata!). Znatno stabilnije ponašanje ima metod fuzije sa težinskim koeficijentima samo za module upoređivanja. Metod fuzije zasnovan na prostom zbiru normalizovanih skorova daje nešto lošije rezultate od ovog metoda fuzije, ali bolje od metoda fuzije sa koeficijentima modula za upoređivanje specifičnim za svakog korisnika.

Ako se opet porede naši rezultati sa rezultatima koje je dobio *Snelick*, oni su sada lošiji više puta nego njegovi. Postoji veći broj mogućih razloga za to, od kojih je verovatno najvažniji kvalitet ulaznih biometrijskih podataka. Verovatno je *FERET* baza, koju je koristio *Snelick*, kvalitetnije priređena od baze *CASIA-FaceV5*, a poznato je da kvalitet slike bitno utiče na proces prepoznavanja. Što se tiče baza otisaka, *Snelick* je raspolagao vlastitom bazom otisaka prstiju, verovatno profesionalno uređenom za potrebe državnih organa, jer nije mogao da o njoj da više podataka.[313]

8.5.3. Zaključna diskusija dobijenih rezultata

Rezultati istraživanja, prikazani u prethodne dve sekcije rada, potvrdili su polaznu hipotezu da multimodalna biometrija ima prednost u oceni najvažnije mere performansi biometrijskog sistema u postupku utvrđivanja identiteta, a to je tačnost rada.

Sprovedena istraživanja i dobijeni rezultati sa Bazom I (*EER* <0.1%) su pokazala da bar u slučajevima zatvorenih sistema sa manjim brojem korisnika, multimodalni biometrijski sistemi mogu postići tačnost bolju od *state-of-the-art* unimodalnih sistema. Navedeni zaključak vredi i u slučajevima kada se raspolaže ograničenim finansijskim sredstvima, pa se za implementaciju koristi

[313] *Ibid.*

neprofesionalna oprema i *open source* programska rešenja, a dobijeni rezultati porede sa profesionalnim vlasničkim rešenjima.[314] Na taj način je potvrđena i posebna hipoteza da se u slučaju postojanja polaznih projektnih ograničenja u pogledu tačnosti rada biometrijskog sistema kod multimodalnih sistema može uticati na povoljniji odnos cene i performansi, nego što je to slučaj za unimodalne sisteme.

Zbog činjenice da u svom radu kombinuju dva ili više biometrijskih modaliteta, multimodalni biometrijski sistemi obezbeđuju minimiziranje značaja mogućih grešaka pri zahvatanju, *FTC* i unosu biometrijskih podataka u sistem, *FTE* (engl. *Failure to Capture, FTC* i *Failure to Enroll*, *FTE*), jer u slučaju nemogućnosti zahvatanja ili unosa jednog od dva biometrijska podatka korisnika, mogu da nastave rad u unimodalnom režimu rada. Dakle, multimodalni biometrijski sistemi poseduju redudantnost koja im omogućava da izbegnu fatalne nedostatke unimodalnih sistema. Na ovaj način potvrđena je i posebna hipoteza o mogućem minimiziranju značaja greške u slučaju multimodalnih sistema, a ne o kardinalnom nedostatku zbog kojeg unimodalni biometrijski sistem ne može da radi.

Korišćenje postojećih *de iure* ili *de facto* međunarodnih standarda u oblasti koja reguliše smeštaj i korišćenje *sirovih* biometrijskih podataka, odnosno izvedenih biometrijskih *karakteristika*, stvara u skladu sa odgovarajućim zakonskim rešenjima realne tehničko-tehnološke uslove za efikasnu razmenu i korišćenje biometrijskih podataka o licima sa kriminalističkim dosijeom, kao i međusobno povezivanje odgovarajućih bezbednosnih mehanizama država u borbi protiv terorizma i organizovanog kriminala.

Istovremeno, kao što je to pokazano u radu, široka primena biometrije u sistemima bezbednosti ugrožava normalan rad sistema za zaštitu svedoka, pa je potvrđena posebna hipoteza da nalaženje rešenja opisanog problema treba tražiti u širem prostoru nego što je to samo prostor biometrije.

---

[314] A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.

Posebno treba istaći da je sprovedeno istraživanje pokazalo da rezultate publikovane u dostupnoj literaturi treba prihvatiti sa oprezom, i pažljivo interpretirati, imajući u vidu mnoge faktore, kao što su, na primer, prikupljanje i izgradnje baze biometrijskih podataka (obim i kvalitet), razvoj biometrijskog sistema (razvoj sopstvenog sistema na bazi *open source* rešenja, kombinacija sopstvenog razvoja sa integracijom komercijalno dostupnih *off-the shelf* komponenata (*COTS*) ili nabavka zatvorenog vlasničkog sistema), kvalitet obuke ljudi koji održavaju i omogućavaju eksploataciju biometrijskog sistema kao i načina, kvalitet opreme koja se koristi, namena biometrijskog sistema (zatvoren ili otvoren biometrijski sistem).

Važno je zapaziti da postojanje značajne razlike u izmerenim performansama eksperimentalnog biometrijskog sistema, u istoj konfiguraciji hardvera, sistemskog i aplikativnog softvera, a u radu sa dve baze podataka različitog obima i kvaliteta biometrijskih podataka, upućuje na značajnu zavisnost efikasnosti odabranih postupaka za upoređivanje karakteristika, normalizaciju i agregiranje skorova, od kvaliteta i broja ulaznih podataka. Zbog toga treba voditi računa o ograničenim mogućnostima manjih, *pilot*, projekata koji obično prethode realizaciji složenijih projekata.

I ova istraživanja su pokazala da biometrijski sistemi identifikacije zbog prirode rada, a to je rad sistema statističkim podacima, uvek unose dozu neizvesnosti u tačnost rezultata, što treba imati u vidu prilikom određivanja domena korišćenja. Neizvesnost zaključaka se može minimizirati, ili ukloniti u nekim slučajevima, kombinovanjem automatskog rada sa dodatnim automatizovanim procedurama u kojima učestvuje i čovek.

9. ZAKLJUČAK

U svetu čije su odrednice globalna ekonomija, Internet, česta i snažna migracija ljudi, regionalna politička nestabilnost i ukorenjen organizovan kriminal, pitanje svakodnevnog utvrđivanja identiteta ljudi u navedenim kontekstima je od ključnog značaja za bezbednost i efikasno funkcionisanje svakog društva. U ovom radu smo prikazali rezultate istraživanja koja su obuhvatila primenu biometrije u realizaciji sistema menadžmenta identitetom, kao opšteg okvira za rešavanje navedenog problema. Danas za te namene još uvek se dominantno koriste unimodalni biometrijski sistemi, odnosno sistemi identifikacije koje koriste samo jedan vid ili modalitet identifikacije ljudi. Međutim, poznato je da biometrijski sistemi identifikacije zbog prirode rada, a to je rad sistema sa izvedenim statističkim podacima o anatomskim i fiziološkim obeležjima ljudi, uvek unose dozu neizvesnosti u tačnost rezultata. U nekim važnim društvenim aktivnostima, na primer na polju bezbednosti, zdravstva ili finansija, tačnost zaključaka nekih unimodalnih biometrijskih sistema postaje upitna, jer pojedinačni propusti mogu da izazovu nesagledivu štetu pojedincu ili zajednici. Rešenja se poslednjih nekoliko godina traže u istovremenom kombinovanju više biometrijskih modaliteta, odnosno u multimodalnoj biometriji. Identifikacija postaje sofisticirana, jer se kombinuje više tehnika biometrijske identifikacije. Integrisanjem različitih biometrijskih postupaka teži se dobijanju veće tačnosti u procesu identifikacije, uz istovremeno smanjivanje angažmana korisnika, kako u procesu pripreme podataka za sistem identifikacije, tako i u samom procesu identifikacije. Naša istraživanja su potvrdila hipotezu da se neizvesnost zaključaka koju daju biometrijski sistemi identifikacije može minimizirati, a u nekim slučajevima i ukloniti, kombinovanjem automatskog rada sistema sa dodatnim automatizovanim procedurama u kojima učestvuje i čovek. U dostupnoj i analiziranoj literaturi ima podataka o tome kako određena kombinacija biometrijskih modaliteta i obradnih postupaka utiče na performanse sistema u

procesu identifikacije, ali ne može se reći da postoje i decidirani stavovi, a pogotovo ne na području tehnoekonomske analize. Naša istraživanja su imala za cilj da doprinesu boljem sagledavanju mogućnosti i ograničenja primene multimodalnih biometrijskih sistema u postupcima identifikacije lica, kao neophodnog preduslova za uspostavljanje sistema menadžmenta identitetom. Sproveli smo analitičko i eksperimentalno istraživanje u naučnom, tehničkom, tehnološkom, pravnom, finansijskom i organizacionom domenu, kako bismo izveli odgovarajuća zapažanja, preporuke i konkretne zaključke potrebne za procenu mogućnosti primene multimodalnih biometrijskih sistema u sistemima identifikacije.

Primena biometrije sa jedne strane znatno unapređuje bezbednosne uslove i poslovno-finansijsko okruženje, ali otvara i brojne kontroverze, jer ulazeći u sve pore društvenog života može da ugrozi osnovno ljudsko pravo na privatnost. U ovom radu su navedene i analizirane društvene i pravne konotacije primene biometrije sa stanovišta društvene opravdanosti sa prikazom pravnih aspekata biometrije i pravnog regulisanja zaštite biometrijskih podataka. Posebno mesto je posvećeno problemu menadžmenta identiteta, sa tehničko-tehnološkim pogledima na proces implementacije takvih sistema. Izložena su osnovna obeležja identiteta, kao i specifičnosti elektronskih dokumenata u slučaju kada se koristi biometrijski identitet. Odgovarajuća pažnja je data *smart* tehnologiji, kao dominantnoj informacionoj tehnologiji u okviru koje se implementiraju biometrijska elektronska dokumenta. Uočeno je da snažna sprega procesa globalizacija i pitanja bezbednosti, stvara potrebu za međunarodnim povezivanjem nacionalnih bezbednosnih sistema mehanizmom zasnovanim na primeni biometrije. Navedeni su odgovarajući međunarodni standardi u domenu biometrijskih elektronskih dokumenata, kao i pregled stanja u Srbiji u ovoj oblasti.

Jedan od najvažnijih doprinosa u sprovedenom istraživanju odnosi se na bitan, ali do sada u naučnoj literaturi nedovoljno prepoznat problem uticaja biometrijskih sistema identifikacije na program zaštite svedoka. Nakon

globalne primene biometrijskih sistema identifikacije, pojavio se značajan problem u važnom odbrambenom segmentu društva – programu zaštite svedoka, kao mehanizmu zaštite od organizovanog kriminala i međunarodnog terorizma. Naime, uočeno je da jačanje društvene bezbednosti uz pomoć biometrijskih tehnika, istovremeno ugrožava normalan rad učesnika u programu zaštite svedoka. U radu je predložen sklop mera u okviru mogućeg pristupa unapređenju programa zaštite svedoka u slučaju široke primene biometrijskih sistema za utvrđivanje identiteta. Na osnovu kritičkog osvrta na dostupne izvore, u radu je dat celovit prikaz prednosti i nedostataka biometrijskih sistema za utvrđivanje identiteta, sa akcentom na moguće pristupe implementaciji. Sa više tehničkih detalja je elaborirano pitanje privatnosti u kontekstu biometrijskih sistema menadžmenta identitetom, a izložen je i predlog jedne moguće klasifikacije takvih sistema.

Nakon, razmatranja pre svega pravnih, organizacionih i tehnoloških aspekata primene biometrije u utvrđivanju identiteta, u radu je nastavljena dubinska tehničko-tehnološka analiza, na primeru multibiometrijskih sistema za utvrđivanje identiteta korišćenjem samo jedne biometrijske osobine čoveka. Imajući u vidu dominantnu upotrebu otisaka prstiju i slike lica u međunarodnim elektronskim identifikacionim dokumentima, kao i činjenicu da i nacionalna elektronska identifikaciona dokumenta koriste ove biometrijske modalitete, posebna pažnja je data biometrijskim sistemima identifikacije koji rade sa otiskom prsta, odnosno sa slikom lica. Uzimajući u obzir sve šire korišćenje glasovnih zapisa ljudi u postupcima identifikacije prilikom elektronskog poslovanja i pristupa obezbeđenim objektima ili uređajima, u ovom delu rada su detaljnije prikazani i biometrijski sistemi sa glasovnim zapisom. Dat je skraćeni prikaz najvažnijih dostupnih naučnih radova za sva tri biometrijska modaliteta, koji predstavljaju osnov za rad odgovarajućih algoritama i tehnika u oblasti biometrije. Za sva tri opisana biometrijska sistema identifikacije navedeni su primeri iz prakse, kao i pregled njihovih prednosti i nedostataka. Posebno su analizirani jednostavniji multibiometrijski sistemi koji

rade sa više instanci jednog biometrijskog modaliteta, sa osvrtom na njihova ograničenja u praktičnom radu, ali i potrebom korisnika da ta ograničenja budu prevaziđena. Više prostora je dato prikazu multibiometrijskih sistema za utvrđivanje identiteta kada se koristi više biometrijskih modaliteta. Izložena je opšta arhitektura takvih sistema i opisani mogući režimi njihovog rada. Posebna pažnja je data načinima povezivanja biometrijskih podataka u multimodalnim sistema, jer od načina njihovog povezivanja zavise i performanse sistema u realnim uslovima korišćenja.

Studija slučaja je korišćena kao najprikladniji metodološki okvir za proveru postavljenih hipoteza u oblasti primene multimodalne biometrije u procesu utvrđivanja identiteta. Na osnovu ranije u radu izloženog teorijskog osnova, u studiji slučaja su istraživane mogućnosti i ograničenja rada biometrijskog sistema sa dva često korišćena biometrijska modaliteta, otiskom prsta i slikom lica. Nakon tako postavljenog problema, u radu je izložena i potom praktično primenjena metodologija za rešavanja problema koji se javljaju u sistemima multimodalne biometrije. Izložene su specifičnosti dve korišćene biometrijske baze podataka. Opisan je i eksperimentalan, ispitni multimodalni sistem za utvrđivanje identiteta preko njegove arhitekture, odabranih režima rada, kao i navođenjem postupka ispitivanja performansi ovog sistema. Posebno treba istaći deo rada u kojem su prezentovani rezultati ispitivanja. Završni deo rada je posvećen analizi i interpretaciji dobijenih rezultata radi određivanja, kako performansi rada multimodalnog biometrijskog sistema, tako i oceni ispunjenja polaznih hipoteza.

Rezultati istraživanja potvrdili su polaznu hipotezu da multimodalna biometrija ima prednost u ostvarenju tačnosti rada, kao najvažnije mere performansi biometrijskog sistema u postupku utvrđivanja identiteta. Dobijeni rezultati su pokazali da bar u slučajevima zatvorenih sistema sa manjim brojem korisnika, multimodalni biometrijski sistemi mogu postići tačnost bolju od *state-of-the-art* unimodalnih sistema. Navedeni zaključak vredi i u slučajevima kada se raspolaže ograničenim finansijskim sredstvima, odnosno kada se za

implementaciju koristi manje kvalitetna oprema i *open source* programska rešenja. Na taj način je potvrđena i posebna hipoteza da se, ako postoje polazna projektna ograničenja u pogledu tačnosti rada biometrijskog sistema, kod multimodalnih sistema može uticati na povoljniji odnos cene i performansi, nego što je to slučaj kod unimodalnih sistema.

Zbog činjenice da u svom radu kombinuju dva ili više biometrijskih modaliteta, multimodalni biometrijski sistemi u nekom trenutku mogu ispoljiti svojstvo redundantnosti, što im obezbeđuje minimiziranje značaja mogućih grešaka pri zahvatanju i unosu biometrijskih podataka u sistem. U našem slučaju, u nemogućnosti da zahvate ili unesu jedan od dva zahtevana biometrijska podatka, sistem može da po potrebi nastavi rad sa smanjenom tačnošću, odnosno sa degradiranim performansama u unimodalnom režimu rada. Na ovaj način potvrđena je i posebna hipoteza o mogućem minimiziranju grešaka u slučaju multimodalnog sistema, a ne o fatalnom nedostatku unimodalnog biometrijskog sistema.

Korišćenje postojećih *de iure* ili *de facto* međunarodnih standarda u oblasti koja reguliše smeštaj i korišćenje *sirovih* biometrijskih podataka, odnosno izvedenih biometrijskih *karakteristika*, stvara u skladu sa odgovarajućim zakonskim rešenjima realne tehničko-tehnološke uslove za efikasnu razmenu i korišćenje biometrijskih podataka o licima sa kriminalističkim dosijeom, kao i međusobno povezivanje odgovarajućih bezbednosnih mehanizama država u borbi protiv terorizma i organizovanog kriminala.

Posebno treba istaći nalaz da primena biometrije u nekim segmentima sistema bezbednosti dovodi do kontraproduktivnih efekata u drugim segmentima ovog sistema! Naime, širenje primene biometrije ugrožava normalan rad sistema za zaštitu svedoka, pa je potvrđena posebna hipoteza da rešenja za ovaj problem treba tražiti u širem prostoru nego što je to samo prostor biometrije. U radu je predložen mogući sklop mera kao prostor rešenja.

I ova istraživanja su pokazala da biometrijski sistemi identifikacije zbog prirode rada, a to je rad sistema statističkim podacima, uvek unose dozu

neizvesnosti u tačnost rezultata, što treba imati u vidu prilikom određivanja domena korišćenja. Neizvesnost zaključaka se može minimizirati, ili ukloniti u nekim slučajevima, kombinovanjem automatskog rada sa dodatnim automatizovanim procedurama u kojima učestvuje i čovek.

Što se tiče mogućih tema za dalja istraživanja, treba istaći da se pokazalo da rezultate publikovane u dostupnoj literaturi u oblasti multimodalnih biometrijskih sistema treba prihvatiti sa oprezom imajući u vidu mnoge faktore koje utiču na realizovane performanse sistema. Važno je zapaziti da postojanje značajne razlike u izmerenim performansama eksperimentalnog biometrijskog sistema, u istoj konfiguraciji hardvera, sistemskog i aplikativnog softvera, u radu sa dve baze podataka različitog obima i kvaliteta biometrijskih podataka, upućuje na značajnu zavisnost efikasnosti odabranih postupaka za upoređivanje karakteristika, normalizaciju i agregiranje skorova, od kvaliteta i broja ulaznih podataka. Zbog toga prilikom budućih projekata treba voditi računa o ograničenim mogućnostima manjih, *pilot*, projekata koji obično prethode realizaciji složenijih projekata. Poželjno bi bilo istražiti zavisnost najpoznatijih metoda izvlačenja karakteristika, normalizacije skorova i postupaka agregacije u odnosu na veličinu baza biometrijskih podataka.

LITERATURA

1. A Smart Card Alliance White Paper "*Secure Personal Identification Systems: Policy, process and Technology Choices for a Privacy-Sensitive Solution*", February (2002).
2. A. Hicklin, B. Ulery, C. Watson, *A Brief Introduction to Biometric Fusion,* Mitretek Systems, National Institute of Standards and Technology, (2006), str. 3-5.
3. A. K. Jain, A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, January (2004).
4. A. K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167 (2007), str. 43–47.
5. A. K. Jain, Patrick Flynn, A. A. Ross, Eds., *Handbook of Biometrics*, Springer, (2008).
6. A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain. Personal Verification Using Palmprint and Hand Geometry Biometric. *In Proceedings of Fourth International Conference on Audio - and Video - Based Biometric Person Authentication (AVBPA),* Guildford, U.K., June (2003), str. 668 – 678.
7. A. Nagar, K. Nandakumar, A. K. Jain, *Technical report: Multibiometric Cryptosystems,* under review for IEEE TIFTS, vol. 7, NO.1, February (2012).
8. A. Ross and A. K. Jain. Information Fusion in Biometrics, Pattern Recognition Letters, *Special Issue on Multimodal Biometrics,* 24(13), (2003), str. 2115–2125.
9. A. Ross, A. K. Jain, *Multimodal biometric: an overview,* Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna), Septembar (2004), str. 1221-1224.

10. A. Ross, *An introduction to multibiometrics*, West Virginia University, Morgantown, WV 26506 USA, (2007).
11. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*, Springer, New York, USA, 1st edition, (2006).
12. A. Adler, *Biometric System Security,* Handbook, Springer (2008), str. 382-383.
13. A. Jain, K. Nandakumara, A. Ross, *Score normalization in multimodal biometric systems*, Pattern Recognition 38 (2005), str. 2270–2285.
14. A.K. Jain, A. Ross, S. Pankanti, Biometric Identification, CACM (2008).
15. A.K. Jain, A. Ross, *Introduction to Biometric,* Handbook of Biometrics, Springer, (2008), str. 6-12.
16. A. Ross, A., A K. Jain, J. Reisman., *A hybrid fingerprint matcher*. T. 36. Pattern Recognition, Jul (2003).
17. A. Ross, K. Nandakumar, A. K. Jain, "*Introduction to Multibiometrics*", Handbook of Biometric (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 272-275.
18. A. Ross, R. Govindarajan, *Feature Level Fusion Using Hand and Face Biometrics*, Proc. Of SPIE conference on Biometric Technology for Human Identification II, vol 5779, Mart (2005), str. 196-204.
19. *A. Smart Card Alliance, „Smart Card and Biometrics in Privacy –Sensitive Secure Personal Identification Systems", (2002).*
20. Anil K. Jain and Arun Ross, *Introduction to Biometrics*, Handbook of Biometrics, (2008), str. 1-23.
21. Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Handbook of Biometrics, Springer, (2011).
22. Anil K. Jain, Flynn, A. A. Ross, Eds., *Handbook of Biometrics*, (*The Law and the Use of Biometrics*), Springer, (2008), str 358-359.
23. Carnet Hrvatska akademska i istraživačka mreža, Biometrija CCERT-PUBDOC-2006-09-167.

24. Christopher Middendorff, Kevin W. Bowyer, *Multibiometrics Using Face and Ear*, Handbook of Biometrics, (2008), str. 315-335.
25. D. Dessimoz, C. Champod, J. Richiardi, A. Drygajlo, *Multimodal Biometrics for Identity Documents*, Research Report, (2005), str. 61.
26. D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, *Multimodal biometrics for identity documents*, Forensic Science International 167, (2007), str. 154–159.
27. D. Maltoni, R. Cappelli, *Fingerprint Recognition*, Handbook of Biometric (eds. A.K. Jain, P. Flynn, A. A. Ross), Springer, (2008), str. 23-43.
28. D. Maurer, J.P. Baker, *Fusing multimodal biometrics with quality estimates via a Bayesian belief network*, Pattern Recognition 41 (2008), str. 821 – 832.
29. Davor Petrinović, *Digitalna obrada govora*, Fakultet elektrotehnike i računarstva, Zagreb (2002).
30. Douglas A. Kash, *Witness Protection Program is critical weapon in the war of crime*, The FBI Law Enforcement Bulletin, USA, No.5, Vol 74, May (2004).
31. Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda, Rim, 4. novembar 1950. godine.
32. M.Paunović i S. Carić, *Evropski sud za ljudska prava nadležnost i postupak*, Centar za publikacije Pravnog fakulteta univerziteta u Beogradu, (2007).
33. H. Chan, R. Lee, Th. Dillon, E. Chang, *E-commerce: Fundamentals and Applications*, John Wiley & Sons, (2001).
34. H. Gravnes, *User's trust in biometric Authentication Systems*, Master Thesis, Gjovik University Collage, Norway, (2005).
35. J. Lee, B. Moghaddam, H. Pfister, and R. Machiraju, *Finding Optimal Views for 3D Face Shape Modeling*. In Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG Seoul, Korea), May (2004), str. 31–36.
36. Joaquin Gonzalez-Rodriguez, Doroteo Torre Toledano, Javier Ortega-Garcia, "*Voice biometrics*", Handbook of Biometrics, Springer, (2008), str. 151-170.
37. Judith A. Markowitz, *Voicebiometric,* Vol. 43, No. 9., September (2000).

38. Judith Felson Duchan, *The Phonetic Notation System of Melville Bell and its Role in the History of Phonetics*, Journal of Speech-Language Pathology and Audiology - Vol. 30, No. 1, (2006).
39. Juwei Lu, „*Boosting Linear Discriminant Analysis for Facial Recognition*," (2002).
40. K. Delac, M. Grgic, S. Grgic, *Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set, Int. J. Imaging Systems and Technology* 15(5), (2005), str. 252-260.
41. K. Kryszczuk, J. Richiardi, P. Prodanov, A. Drygajlo, *Reliability-Based Decision Fusion in Multimodal Biometric Verification Systems*, International Journal of Neural Systems, Vol. 17, No. 5 (2007), str. 343–351.
42. G. Ilić, M. Majić, B. Ilić, *Komentar Zakona o Programu zaštite učesnika u krivičnom postupku*, Beograd, (2006).
43. Konvencija UN protiv transnacionalnog organizovanog kriminala (UNCATOC), sa dopunskim protokolima, koja je stupila na snagu 29. 09.2003. godine.
44. Krivičnopravna Konvencija o korupciji, od 27.01. 1999. godine.
45. Kumar, A. D. C. M. Wong, H. C. Shen, A. K. Jan, *Personal verification using palmprint and hand geometry biometric,* Guildford, UK: Proc. Of 4th Int I Cinf. On Audio and Video-based Biometric Person Authentication (AVBPA), Jun (2003).
46. L. Hong and A. K. Jain. Integrating Faces and Fingerprints for Personal Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 20(12), December (1998), str. 1295–1307.
47. L. Hong, A. Jain, S. Pankanti. *Can Multibiometrics Improve Performance?*
48. Laurenz Wiskott, "*Face recognition by Elastic Bunch Graph Matching*, " April (1996).
49. Lisa Myers "*An Exploration of Voice Biometrics*" Information Security Reading room, SANS Institute, (2004).

50. M. Savvides, J. Heo, S. W. Park, *Face Recognition*, Handbook of Biometrics, (*eds.* A.K.Jain, P.Flynn, A.A. Ross), Springer, (2008), str. 43.
51. M. Tripunović, Z. Anđelković *Otisak prsta-biometrijski podaci*, INFOTEH-JAHORINA, Mart (2007).
52. M.Vatsa, R. Singh. A. Noore, *Integrating image quality in 2ν-SVM biometric match score fusion*, International Journal of Neural Systems, Vol. 17, No. 5 (2007), str. 343–351.
53. Marek Rejman-Greene, *Privacy Issues in the Application of Biometrics: a European Perspective*, Biometric Systems, (2005) str. 335-359.
54. Međunarodni krivični sud za bivšu Jugoslaviju (*ICTY*) koji je uspostavljen na osnovu rezolucije saveta bezbednosti UN br. 827 od 25. maja 1993. godine.
55. I. Milenković, D. Starčević, S. Paunović, *Fuzija informacija u multimodalnoj biometriji*, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011).
56. Miletić E., Lilić S,. Vitkauskas D., *Podrška instituciji poverinika za informacije od javnog značaja i Zaštitu podataka o ličnosti*, „IBF International Consulting, (2010).
57. N. Yager, T. Dunstone, *The Biometric Menagerie*, IEEE, (vol. 32 no. 2), February (2010), str. 220-230.
58. Nalini K. Ratha, Venu Govindaraju, *Advances in Biometrics: Sensors, Algorithms and Systems*, Springer, London, (2008), str. 423-425.
59. Nataša Pirc Musar, *Vodič kroz Zakon o zaštiti podataka o ličnosti,* Beograd (2009).
60. Oliver Subotić, *Biometrijski sistemi identifikacije: (kritička studija),* Beograd, (2007).
61. P. J. Huber. *Robust Statistics*. John Wiley & Sons, (1981).
62. P. Verlinde and G. Cholet. Comparing Decision Fusion Paradigms using k -NN based Classifiers, Decision Trees and Logistic Regression in a Multimodal Identity Verification Application. In *Proceedings of Second International Conference on Audio and Video - Based Biometric Person*

Authentication (AVBPA), Washington D.C., U.S.A., March (1999), str. 188 – 193.

63. Perry R. Cook, *Human Computer Interface Technology*, Biometrics Introduction and Issues Princeton University, Princeton, New Jersey, USA., October 21, (2002).
64. Pravilnik o ličnoj karti (Službeni glasnik RS br.11/2007 I 9/2007).
65. Pravilnik o putnim ispravama, (Službeni glasnik RS br**.** 54/2008 i 34/2010).
66. Preporuka sa oznakom N° R (97) 13 o zastrašivanju svedoka i prava odbrane, doneta na 600. zasedanju zamenika ministara 10. juna 1997. godine.
67. Preporuka o kaznenoj politici u Evropi za vreme promena, N° R (96) 8.
68. Preporuka o nasilju u porodici, N° R(84) 4.
69. Preporuka o zaštiti i pružanju pomoći žrtvama , N° R (87) 21.
70. Preporuka Rec. (2005) 9 o zaštiti svedoka i svedoka saradnika, usvojena od strane Komiteta ministara 20 aprila 2005.godine.
71. Preporuka u vezi seksualnog iskorišćavanja i izlaganja dece i omladine pornografiji, prostituciji i krijumčarenju, N° R (91) 11.
72. Projekat „*Primena multimodalne biometrije u menadžmentu identiteta*“, finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije, pod zavodnim brojem TR-32013.
73. R. G. Malenčić, *Tehnička policija i njen rad*, Štamparija Jovanović i Bogdanov, Novi Sad, (1933), str.110.
74. R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, *Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems,* IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, March (2005).
75. Radna grupa, "*Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata*", MUP (2002-2004).

76. Radna grupa, *„Projekat integrisanog rešenja obezbeđenja i kontrole prelaska državne granice“*, (2003).
77. Radna grupa, *„Osnovni koncepti novih elektronskih identifikacionih dokumenata “* MUP, (2004).
78. *Report of the Defense Science Board Task Force on Defense Biometrics, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington,* March (2007).
79. S. Hoffman, Biometrics, *Retinal Scanning, and the Right to Privacy in the 21st Century*, Syracuse Science & Technology Law Reporter, Vo. 22, Article 2, (2010), str. 38.
80. S. Paunović, D. Starčević, *Multimodalna biometrija i menadžment identiteta*, Zbornik konferencije ITEO 2010, Banja Luka, Republika Srpska, BiH (2010).
81. S. Brajušković, *Biometrijska identifikacija i pravo na privatnost*, jun (2011).
82. S. Paunović, D.Starčević, I. Milenković, *Menadžment identiteta i pitanja privatnosti*, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011).
83. Saša Paunović, *Menadžment identiteta i elektronska dokumenta zasnovana na biometrijskom identitetu,* Simpozijum o operacionim istraživanjima, Zbornik radova SYMOPIS 2011, Ekonomski fakultet, Beograd, (2011).
84. Saša Paunović, *Primena specijalizovanih biometrijskih sistema za identifikaciju*, Magistarska teza, Fakultet organizacionih nauka, Univerzitet u Beogradu, Beograd (2009).
85. S. Paunović, D. Starčević, *Mulibiometrijski sistemi za utvrđivanje identiteta*, Simpozijum o operacionim istraživanjima, Zbornik radova SYMOPIS 2013, FON, Beograd, Zlatibor, R.Srbija, (2013).
86. S. Paunović, D. Starčević, L. Nešić, *Identity Management and Witness Protection System,* Management, Beograd, (2013).
87. S. Paunović, L. Nešić, J.Kovačević, *Application of Voice Biometrics in Protection Systems and Crime Fighting,* Journal of Information Technology and Applications (JITA), Banja Luka, BiH, (2012).

88. S. Paunović, L. Nešić, J.Kovačević, *Biometrical identification via facial photography,* Međunarodni naučni skup „Dani Arčibalda Rajsa“, Beograd (2013).
89. Sedma međunarodna konferencija o elektronskoj trgovini i elektronskom poslovanju, Zbornik radova, Palić, (2007).
90. Stan Zi Li, Anil K.Jain, *Handbook of Face recognition*, second edition, Springer, (2011).
91. Statut međunarodnog krivičnog suda (*ICC*) koji je stupio na snagu 1. jula 2002. godine.
92. Strategija zaštite podataka o ličnosti "Službeni glasnik RS", br. 58/2010 od 20. 08. 2010. godine.
93. Terrance E. Boult and Robert Woodworth, *Privacy and Security Enhancements in Biometrics,* Advances in Biometrics, Springer-Verlag London Limited (2008).
94. *The e Europe SMART Card Charter, ELETRONIC IDENTITY WHITE PAPER, (2003).*
95. Turk, M., Pentland, A., *Face recognition using eigenfaces. In: Proceedings of IEEE Computer Vision and Pattern Recognition,* Maui, Hawaii, December (1991). str. 586–590.
96. U.M.Bubeck. *Multibiometric Authentication*, Term Project CS 574, San Diego State University, (2003).
97. United Kingdom Parlament, *House of Commons Hansard Debates*, November (2003).
98. United Nations Office on Drugs and Crime, *Good practices for the protection of witnesses in criminal proceedings involving organized crime,* N.York, (2008).
99. V. Mitrović, *Kriminalistička tehnika*, VŠUP Zemun, Beograd, (1990), str. 34 – 44.
100. Vojkan Vasković, Miomir Todorović, *Tehnologije biometrijskih plaćanja*, Beogradska Poslovna Škola, Beograd (2008).

101. X.Zhou, B. Banu, *Feature fusion of side face and gait for video-based human identification*, Pattern Recognition 41 (2008), str. 778 – 795.
102. Xiaoguang.Lu, *Image Analysis for Face Recognition,* Dept. of Computer Science & Engineering, Michigan State University, East Lansing, (2004).
103. Xiaoyu Wang, Tony X. Han, Shuicheng Yan, "*An HOG-LBP Human Detector with Partial Occlusion Handling*", ICCV (2009).
104. Y. Wang, T. Tan, and A. K. Jain. *Combining Face and Iris Biometrics for Identity Verification*. In Proceedings of Fourth International Conference on Audio - and Video - Based Biometric Person Authentication (AVBPA), Guildford, U.K., June (2003), str. 805 – 813.
105. Y.Xu, D.Zhang, J.Yang, *A feature extraction method for use with bimodal biometrics*, Pattern Recognition 43 (2010), str. 1106–1115.
106. Y.Yao, X.Jing, H.Wong, *Face and palmprint feature level fusion for single sample biometrics recognition,* Neurocomputing 70 (2007), str. 1582–1586.
107. Yvon Dandurand, Kristin Farr, *A Review of Selected Witness Protection Programs*, Her Majesty the Queen in Right of Canada, Report No. 001, Canada, (2010).
108. Z. Skakavac, M. Milivojević, *Neki teorijsko-istorijski i empirijski aspekti tragova papilarnih linija*, Zbornik radova „Kriminalističko forenzička istraživanja“, Internacionalna Asocijacija Kriminalista, Banja Luka, (2011), str. 104-117.
109. Zakon o ličnoj karti, (Službeni glasnik RS br. 62/2006 i 36/2011).
110. Zakon o programu zaštite učesnika u krivičnom postupku, (Službeni glasnik R. Srbije br. 85/2005).
111. Zakon o putnoj ispravi, (Službeni glasnik br. br. 90/2007, 116/2008, 104/2009 и 76/2010).
112. Zakon o zaštiti podataka o ličnosti, (Službeni glasnik RS", br. 97/2008, 104/2009).
113. Ž. Nikolic, *Prepoznavanje lica primenom analize osnovnih komponenti*, Telekomunikacioni forum TELFOR 2007, Srbija, Beograd, (2007).

114. Ž. Radmilović, Identifikacija temeljem otisaka prstiju, *Biometrijska identifikacija,* Stručni članak, (2008).
115. *Biometric Fingerprint Lock, available on, www.findbiometrics.com/locks/,* pristupljeno 19.12.2012.
116. *Biometric for Time and Attendance, available on, http://www.findbiometrics.com/time-attendance/,* pristupljeno 19.12.2012.
117. *Biometric Gov. Face Recognition, available on, www.biometrics.gov/Documents/facerec.pdf,* pristupljeno 15.12.2012.
118. *Biometric in HealthCare, available on, http://www.findbiometrics.com/health-care/,* pristupljeno 19.12.2012.
119. Biometrija i menadžment identiteta, objavljeno *www.Biometrics_and_identity_management_schematic* pristupljeno 13.04.2012.
120. *Border control, available on http://www.findbiometrics.com/border-control-airports/,* pristupljeno 19.12.2012.
121. *Computerised Facial Recognition, available on papers.ssrn.com/sol3/papers.cfm?abstract_id=1551840,* pristupljeno 15.12.2012.
122. D. Dessimoz, J. Richiardi, C. Champod, A. Drygajlo, *Multimodal Biometrics for Identity Documents (MBioID)*, Institut de Police Scientifique, June (2006), *available on, www.europeanbiometrics.info.*
123. *Dragon Naturally Speaking Review, available on www.dragonnaturallyspeakingreview.com/,* pristupljeno 22.01.2013.
124. *Fingerprint Recognition, available on, www.biometrics.gov/Documents/FingerprintRec.pdf#page=1,* pristupljeno 19.04.2012.
125. *FVC2006 web site, available on http://bias.csr.unibo.it/fvc2006,* pristupljeno 09.01.2013.
126. *collopy.case.edu/mbac423f05/projects/biometrics.pdf,* pristupljeno_13.03.2013.
127. *docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html?highlight=pca,* pristupljeno 15.11.2012.

128. *en.wikipedia.org/wiki/File:Map_of_countries_with_biometric_passports.svg*, pristupljeno dana 14.03.2013. godine.
129. *ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf*, pristupljeno, jun 2013.
130. *www.cbmn.org/slike_i_fajlovi/fajlovi/fajlovi_press_centar/magistarski_gordana_dedeic.pdf*, pristupljeno 18.10.2013.
131. *www.e-drustvo.org/proceedings/YuInfo2008/html/pdf/060.pdf*, pristupljeno 19.12.2012.
132. *http://www.idealtest.org/index.jsp*, pristupljeno 11.10.2012.
133. *www.mhrr.gov.ba/PDF/MedunarodniPakt%20B.pdf,* pristupljeno 11.03.2013.
134. *www.nist.gov/itl/iad/ig/special_dbases.cfm*, pristupljeno 05.10.2012.
135. *www.nist.gov/itl/idms/*, pristupljeno 14.10.2012.
136. *www.privatnost-srbija.com/skup2011/Resanovic.pdf,* pristupljeno 17.12.2012.
137. *www.sostelefon.org.rs/zakoni/12.%20Univerzalna%20deklaracija%20o%20ljudskim%20pravima.pdf*, pristupljeno 11.03.2013.
138. *www.sostelefon.org.rs/zakoni/12.%20Univerzalna%20deklaracija%20o%20ljudskim%20pravima.pdf*, pristupljeno 13.04.2013.
139. *www.usmarshals.gov/duties/factsheets/witsec-2011.html*, pristupljeno 13.04.2012.
140. L. O'Gorman, *Fingerprint Verification, available on, scgwww.epfl.ch/courses/notes/2%20Fingerprints.pdf*, 11.03.2013.
141. *Logical access control biometric, available on www.findbiometrics.com/logical-access/*, pristupljeno 19.12.2012.
142. M. Bromby, *Computerised Facial Recognition, Systems: The Surrounding Legal Problems, available on, papers.ssrn.com/sol3/papers.cfm?abstract_id=1551840*, pristupljeno 14.12.2012.
143. M. Pietikäinen, G.Zhao, A. Hadid, *available on www.comp.hkbu.edu.hk/~icpr06/tutorials/Pietikainen.html*, pristupljeno 13.03.2013.

144. Otisak prsta, objavljeno *arka.foi.hr/~mschatten/radovi/Fingerprint.pdf*, pristupljeno 11.03.2013.
145. *Physical access control biometric, available on www.findbiometrics.com/physical-access/*, pristupljeno 19.12.2012.
146. Policijska akademija www.kpa.ed.rs, (2012), pregledano 22.01.2013.
147. Prepoznavanje otiska prsta, objavljeno dosl.zesoi.fer.hr/seminari/1998_1999/visnjicsafarzik/index2.html , pristupljeno 19.04.2013.
148. *Principles of protection Tool 5.17 Witness protection, available on www.unodc.org/documents/humantrafficking/Toolkitfiles/0858296_tool_5-17.pdf*, pristupljeno 15.01.2013.
149. US Marshal Service, *available on www.usmarshals.gov/witsec/index.html*, pristupljeno 13.04.2012.
150. Voice Biometrics Conference, *Voice Biometric Authentication Systems, available on www.authentify.com/solutions/voice_biometrics.html*, pristupljeno 22.01.2013.
151. *www.poverenik.org.rs/index.php/sr/javna-rasprava.html*, pristupljeno 19.12.2012.
152. Y.W.Zhao, R.Chellapa, *Image-based Face Recognition*, Issues and Methods, *www.face-rec.org/interestingpapers/General/Chapter_figure.pdf*, pristupljeno 14.04.2012.
153. Ž. Radmilović, *Biometrijska identifikacija*, 2008. godina, objavljeno www.mup.hr/UserDocsImages/PA/onkd/3_4_2008/radmilovic.pdf, pristupljeno 15.12.2012.

Prilog 1.

IZJAVA O AUTORSTVU

Potpisani SAŠA PAUNOVIĆ
broj indeksa 114/96

Izjavljujem
da je doktorska disertacija pod naslovom:
„Primena multimodalne biometrije u sistemima za utrđivanje identiteta“

rezultat sopstvenog istraživačkog rada,
da predložena disertacija u celini ni u delovima nije bila predložena za dobijanje bilo koje diplome prema studijskim programima drugih visokoškolskih ustanova,
da su rezultati korektno navedeni i
da nisam kršio/la autorska prava i koristio intelektualnu svojinu drugih lica.

Potpis doktoranda

U Beogradu, _____

_____

Prilog 2.

IZJAVA O ISTOVETNOSTI ŠTAMPANE I ELEKTRONSKE VERZIJE DOKTORSKOG RADA

Ime i prezime autora: Saša Paunović
Broj indeksa: 114/96
Studijski program: Odnosi sa javnošću i multimedijalne komunikacije
Naslov rada: Primena multimodalne biometrije u sistemima za utvrđivanje identiteta
Mentor: dr Dušan Starčević

Potpisani/a: _____

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao/la za objavljivanje na portalu Digitalnog repozitorijuma Univerziteta u Beogradu.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis doktoranda

U Beogradu, _____ _____

Prilog 3.

IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom: Primena multimodalne biometrije u sistemima za utrđivanje identiteta, koja je moje autorsko delo.

Disertaciju sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalni repozitorijum Univerziteta u Beogradu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo
2. Autorstvo – nekomercijalno
3. Autorstvo – nekomercijalno – bez prerade
4. Autorstvo – nekomercijalno – deliti pod istim uslovima
5. Autorstvo – bez prerade
6. Autorstvo – deliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponuđenih licenci, kratak opis licenci dat je na poleđini lista).

Potpis doktoranda

U Beogradu, _____

_____

1. Autorstvo – Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo – nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo – nekomercijalno – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo – nekomercijalno – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.