UNIVERZITET U BEOGRADU

FAKULTET ORGANIZACIONIH NAUKA

Ivan Č. Milenković

OKVIR ZA EVALUACIJU MULTIMODALNIH BIOMETRIJSKIH SISTEMA

DOKTORSKA DISERTACIJA

Beograd, 2021

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Ivan Č. Milenković

FRAMEWORK FOR EVALUATION OF MULTIMODAL BIOMETRIC SYSTEMS

DISSERTATION PROPOSAL

Belgrade, 2021

Mentor:

_____

Dr Dejan Simić, redovni profesor

Fakultet organizacionih nauka, Univerzitet u Beogradu

Članovi komisije:

_____

Dr Dušan Starčević, profesor emeritus

Fakultet organizacionih nauka, Univerzitet u Beogradu

_____

Dr Boško Nikolić, redovni profesor

Elektrotehnički fakultet, Univerzitet u Beogradu

Datum odbrane: _____

Okvir za evaluaciju multimodalnih biometrijskih sistema

Apstrakt:

Primena biometrijskih tehnologija danas u ljudskom društvu postaje sve češća, gotovo da možemo konstatovati da je ona deo naše svakodnevnice. Prilikom implementacije biometrijske autentikacije, svaki sistem ima svoje zahteve i ograničenja, u zavisnosti od konkretnog scenarija u kojem se sistem koristi. Za odabir odgovarajućeg biometrijskog modaliteta, kao i algoritama za rad sa biometrijskim modalitetom, neophodno je sprovesti odgovarajuću evaluaciju performansi rada biometrijskog sistema. Ipak, ovu evaluaciju nije uvek lako sprovesti, kako za unimodalne, tako i za multimodalne biometrijske sisteme. Čak i kada su dostupne javne baze biometrijskih podataka za evaluaciju algoritama određenog biometrijskog modaliteta, potrebno je prilagoditi rad sistema protokolu testiranja koji konkretna baza definiše. U slučaju multimodalnog pristupa, evaluacija se dodatno komplikuje usled upotrebe različitih algoritama za fuziju informacija. Kako u dostupnoj relevantnoj literaturi nije pronađen detaljan prikaz modela evaluacije multimodalnih biometrijskih sistema, a radi prevazilaženja ovih teškoća, u okviru ovog doktorata definisan je objedinjeni model evaluacije multimodalnih biometrijskih sistema. Za definisanje ovog modela primenjena je MDA (*Model Driven Architecture*) paradigma. U okviru objedinjenog modela dat je metamodel evaluacije multimodalnih biometrijskih sistema, koji predstavlja svojevrsnu ontologiju pojmova značajnih za ovu oblast. Primenom ovog metamodela, moguće je kreirati modele evaluacije različitih biometrijskih sistema. Na osnovu modela evaluacije multimodalnih biometrijskih sistema kreiran je prototip okvira za evaluaciju multimodalnih biometrijskih sistema. Pomoću predloženog okvira moguća je evaluacija performansi multimodalnog biometrijskog sistema u različitim slučajevima korišćenja. Eksperimentalni rezultati evaluacije nad konkretnom bazom i algoritmima pokazuju da primena okvira skraćuje za četiri puta vreme potrebno za evaluaciju. Razvijena je i nova metoda za analitičko određivanje praga osetljivosti u skladu sa postavljenim parametrima željenog ponašanja sistema. Na kraju, na primeru alata koji je koristio neke od funkcionalnosti okvira, prikazano je kako primena okvira može učiniti efikasnijim proces obrazovanja inženjera u oblasti biometrije.

Ključne reči: biometrija, multimodalna biometrija, evaluacija performansi, gejmifikacija

Naučna oblast: Organizacione nauke

Uža naučna oblast: Informacione tehnologije

UDK:

Framework for evaluation of multimodal biometric systems

Abstract:

Application of biometric technologies in our contemporary human society is getting more frequent, so we can almost state that biometric technologies are part of our everyday life. When implementing biometric authentication, each system has specific requirements and constraints, which depend on the actual scenario in which the system is being used. In order to choose the adequate biometric modality, and also a fitting algorithm for the chosen modality, it is necessary to perform an evaluation of the biometric system performance. However, this evaluation is not always easy to conduct. This fact is true for both the unimodal and multimodal biometric systems. Even when open biometrics databases are available for evaluation, it is necessary to adapt system to work with testing protocol of the chosen open database. Moreover, if the biometric system uses multiple biometric modalities, evaluation gets even more complicated because of different available fusion algorithms. In order to overcome these difficulties, as there is not a detailed model of multimodal biometric systems available in relevant literature, this thesis presents a unified multimodal biometric systems evaluation model. Presented model is based on MDA (Model Driven Architecture) paradigm. A part of the unified multimodal biometric systems evaluation model is the metamodel of multimodal biometric system evaluation, which represents an ontology of terms used in this domain. Based on unified multimodal biometric systems evaluation model, a prototype framework for multimodal biometrics systems evaluation has been created. By using proposed framework it is possible to evaluate performance of multimodal biometric system in different use cases. Experimental evaluation results based on used database and algorithms show that the use of framework shortens time necessary for evaluation to a quarter of previously required time. Also, a new analytical method for biometric system threshold optimization, based on the predefined desired system behavior was developed. As final, a learning tool based on some of the framework functionalities is used to show how the use of framework can make the process of educating engineers in the field of biometrics more efficient.

Keywords: biometrics, multimodal biometrics, performance evaluation, gamification

Scientific area: Organizational sciences

Specific scientific area: Information technologies

UDC:

SADRŽAJ

Slike

Tabele

1 UVOD

1.1 Problem i predmet istraživanja

Biometrijsko prepoznavanje osobe možemo definisati kao prepoznavanje osobe na osnovu njenih fizioloških ili bihejviorističkih karakteristika [1]. Može se koristiti kao alternativa standardnim metodama autentikacije koje se zasnivaju na nečemu što osoba zna ili poseduje. Ukoliko biometrijska autentikacija podrazumeva korišćenje više različitih biometrijskih modaliteta, takav pristup naziva se multimodalna biometrija. Multimodalna biometrija koristi se kako bi se unapredila preciznost i bezbednost biometrijskog sistema.

Problem koji se razmatra u okviru istraživanja nastao je kao posledica sve češće upotrebe biometrijskih metoda u praksi. Danas je dostupan značajan broj komercijalnih rešenja i rešenja otvorenog koda, koja omogućavaju rad sa različitim biometrijskim modalitetima. Međutim, u ovoj oblasti i dalje postoje određeni izazovi. Prilikom poređenja i evaluacije performansi različitih algoritama, kako za multimodalnu, tako i za unimodalnu biometriju, javljaju se određene nedorečenosti. Uporednu analizu dva rešenja koja rade sa istim modalitetom nije uvek jednostavno izvršiti. Čak i kada su dostupne javne baze sa biometrijskim podacima određenog modaliteta, potrebno je izvršiti prilogođavanje sistema protokolu za testiranje konkretne baze.

Pored ovih inicijalnih teškoća i tumačenje različitih parametara, koji služe kao pokazatelji preciznosti i performansi biometrijskog sistema, može biti kompleksan zadatak. Ukoliko se uzmu u obzir samo neki od parametara, na primer ukupan FMR (eng. *False Match Rate*) i FNMR (eng. *False Non Match Rate*), moguće je lako previdеti određene konkretne scenarije u kojima biometrijski sistem ima značajno lošije rezultate od proseka [2]. Zato je često od koristi imati u vidu i druge pokazatelje, kao što je na primer biometrijska menažerija [3], koji mogu ukazati na neke suštinske nedostatke samog sistema u određenim situacijama.

Podešavanje praga osetljivosti sistema je jedan od zadataka koji se nalazi pred projektantom biometrijskog sistema. Prilikom njegovog određivanja, projektant se suočava sa dva suprotstavljena cilja, potrebom da sistem bude što bezbedniji i potrebom da sistem bude što upotrebljiviji za krajnjeg korisnika. Favorizovanje jedne ili druge potrebe ima uticaj na FMR i FNMR parametre sistema. Najčešće se u praksi prag osetljivosti određuje iskustveno [1], ili na osnovu određenog kontrolnog seta podataka. Ovde se postavlja pitanje da li je moguće ovaj problem rešiti na analitički način.

Sve navedene teškoće se multiplikuju prilikom primene multimodalnog pristupa. Projektant biometrijskog sistema nalazi se pred izborom različitih metoda fuzije informacija, koje imaju svoje prednosti i mane. Takođe, javlja se dilema izbora pogodnih modaliteta, kao i podešavanja praga osetljivosti sistema, posebno kod primene serijskog pristupa fuziji informacija.

Na osnovu svega navedenog, možemo uočiti potrebu za metodološkim pristupom razvoju edukativnog evaluacionog multimodalnog biometrijskog sistema. Korišćenjem navedene metodologije realizovaće se okvir (engl. *framework*) koji bi omogućio lakšu

analizu performansi multimodalnih biometrijskih sistema. Takav pristup bi mogao imati višestruku primenu i značaj. Multimodalni biometrijski sistemi mogu se uspešno integrisati sa sistemima za menadžment identiteta [4]. Najširu primenu predmetni okvir mogao bi imati prilikom edukacije novih kadrova u okviru ove oblasti. Sa druge strane, iskusni inženjeri biometrijskih sistema bi ga mogli koristiti kao sredstvo za efikasniju analizu problema podešavanja parametara sistema, ali i kao sredstvo za podršku prilikom donošenja odluka.

Predmet istraživanja je upravo razvoj odgovarajućeg metodološkog pristupa za evaluaciju performansi multimodalnih biometrijskih sistema. Razvoj multimodalnih biometrijskih sistema moguć je ne samo pomoću kompletne implementacije svih delova od početka, već i uz primenu okvira i rešenja otvorenog koda [5]. Kako se pokazalo da primena tehnika gejmifikacije u edukaciji ima pozitivan rezultat [6], poseban predmet istraživanja jesu mogućnosti upotrebe tehnika gejmifikacije kako bi se unapredio proces edukacije budućih biometrijskih inženjera.

Dalje, potrebno je postići metodološki korektnu evaluaciju performansi multimodalnih biometrijskih sistema u različitim scenarijima korišćenja. Neophodno je omogućiti kombinovanje različitih biometrijskih modaliteta, algoritama za rad sa biometrijskim modalitetima, metoda za fuziju informacija, kao i testiranje nad bazama biometrijskih podataka. Takođe, istražene su mogućnosti i načini za jednostavno uključivanje novih modaliteta i algoritama, kako bi se postigla modularna struktura okvira.

1.2 Cilj istraživanja i polazne hipoteze

Cilj istraživanja je podizanje kvaliteta i efikasnosti procesa obrazovanja biometrijskih inženjera uvođenjem okvira za evaluaciju multimomodalnih biometrijskih sistema u nastavni proces. U okviru osnovnog cilja istraživanja potrebno je pronaći način za prikaz i evaluaciju uticaja različitih ulaza u multimodalni biometrijski sistem i izbora algoritama fuzije na njegovu preciznost i performanse. Poseban cilj je razvoj okvira za evaluaciju multimodalnih biometrijskih sistema.

Opšta hipoteza: Moguće je razviti okvir za evaluaciju performansi multimodalnih biometrijskih sistema koji bi omogućio ispitivanje performansi različitih kombinacija biometrijskih modaliteteta, algoritama za rad sa biometrijskim modalitetima i metoda za fuziju informacija.

Pomoćne hipoteze:

H1 - Razvoj okvira za evaluaciju multimodalnih biometrijskih sistema bi omogućio evaluaciju performansi sistema u različitim scenarijima korišćenja.

H2 - Moguće je razviti novu metodu za optimizaciju određivanja praga osetljivosti multimodalnog biometrijskog sistema u skladu sa predefinisanim parametrima.

H3 - Okvir za evaluaciju multimodalnih biometrijskih sistema može proces obrazovanja inženjera u oblasti biometrije učiniti efikasnijim.

H4 – Proširenje standardne metodologije razvoja informacionog sistema zasnovane na UML jeziku uvođenjem novih koncepata specifičnih za biometrijske sisteme, evaluaciju biometrijskih sistema i njihovu primenu u obrazovanju olakšava i podiže kvalitet realizacije okvira za evaluaciju multimodalnih biometrijskih sistema.

1.3 Struktura rada

Disertacija je podeljena na 14 poglavlja. U prvom poglavlju izneti su problem i predmet istraživanja, opisani ciljevi istraživanja i postavljene hipoteze. Nakon toga, u nastavku poglavlja je izneta struktura disertacije.

Drugo poglavlje bavi se temom menadžmenta identiteta. Razmotren je problem identiteta i opisane su aktivnosti sistema za menadžment identiteta. Izvršeno je poređenje metoda autentikacije koje se mogu primeniti u sistemu za menadžment identiteta. Dat je pregled različitih arhitektura koje se mogu primeniti u sistemima za menadžment identiteta, kao i opis različitih elemenata koje ove arhitekture uključuju. U posebnom potpoglavlju 2.1 dat je pregled upotrebe *blockchain* i DLT (eng. *Distributed ledger technology*) tehnologija u sistemima za menadžment identiteta. U okviru ovog potpoglavlja, posebna podsekcija 2.1.1 je posvećena kombinaciji biometrijskog prepoznavanja sa ovim tehnologijama.

Treće poglavlje posvećeno je biometriji. Objašnjen je pojam biometrije i iznet kratak prikaz razvoja tehnika biometrijskog prepoznavanja kroz istoriju. Zatim je izvršena klasifikacija i dat sažet prikaz svakog od biometrijskih modaliteta, uz opis pratećih algoritama kao i problema koji su vezani za konkretne modalitete. U potpoglavlju 3.1 izvršen je osvrt na fiziološke biometrijske modalitete, konkretno otisak prsta, lice i iris. Zatim su u potpoglavlju 3.2 prikazani i različiti bihejvioristički biometrijski modaliteti, kao što su rad sa tastaturom, mišem, upotreba mobilnog telefona i ljudski hod. Od kombinovanih biometrijskih modaliteta, u potpoglavlju 3.3 analizirana je upotreba glasa za prepoznavanje osoba. Naredna sekcija 3.4 odnosi se na opšte karakteristike rada jednog biometrijskog sistema.

Četvrto poglavlje odnosi se na multimodalnu biometriju. U poglavlju 4.1 opisani su potencijalni nedostaci unimodalnog pristupa, kao i data klasifikacija multibiometrijskih sistema. Poglavlje 4.2 posvećeno je fuziji informacija u mutimodalnoj biometriji. Izvršen je uporedan prikaz različitih nivoa fuzije informacija, u zavisnosti od toga u kom trenutku procesiranja biometrijskih podataka se vrši fuzija. U poslednjem potpoglavlju ove glave, prikazane su različite primene multimodalne biometrije, bilo u akademskim radovima ili u komercijalnoj praksi.

Peto poglavlje razmatra teme bitne za evaluaciju biometrijskih sistema. Različiti parametri koji se koriste za evaluaciju biometrijskih sistema opisani su u prvom potpoglavlju. Naredna celina, 5.2 razmatra fenomen biometrijske menažerije, koji pruža dodatni uvid u evaluaciju performansi biometrijskog sistema. Na kraju, u potpoglavlju 5.3 opisane su neke od otvorenih baza biometrijskih podataka koje se koriste za evaluaciju.

Šesto poglavlje bavi se optimizacijom praga osetljivosti u multimodalnom biometrijskom sistemu. Dat je predlog nove metode za određivanje i optimizaciju praga osetljivosti u sekvencijalnom multimodalnom biometrijskom sistemu. Potpoglavlje 6.1 opisuje evaluaciju predložene metode nad NIST-BSSR bazom skorova poređenja. Sledeće potpoglavlje 6.2 evaluira predloženu metodu nad generisanom bazom skorova poređenja.

U sedmom poglavlju dat je predlog objedinjenog modela za evaluaciju multimodalnih biometrijskih sistema. Predložen pristup zasnovan je na MDA (eng. *Model Driven Architecture*) paradigmi i preslikavanje okvira za evaluaciju multimodalnih sistema na ovaj pristup opisano je u prvom potpoglavlju. U ostatku poglavlja, fokus je bio na metamodelima koji mogu poslužiti za kreiranje modela evaluacije odgovarajućeg biometrijskog sistema. U skladu sa tim, sledeće potpoglavlje, 7.2 opisuje metamodel digitalnog reprezenta osobe. U potpoglavlju 7.3 prikazan je metamodel upotrebljivosti biometrijskog modaliteta. Metamodel načina evaluacije biometrijskog sistema dat je u potpoglavlju 7.4. Transformacija biometrijskih podataka predstavljena je u metamodelu u okviru potpoglavlja 7.5. Metamodel akvizicije opisan je u potpoglavlju 7.6, dok je metamodel uslova okruženja predstavljen u potpoglavlju 7.7.

Modelovanje evaluacije multimodalnih biometrijskih sistema prikazano je u poglavlju 8. Najznačajniji koncepti evaluacije prošireni su pomoću profila zasnovanih na konceptima definisanim u objedinjenom modelu evaluacije opisanom u sedmom poglavlju. Za svaki od profila definisani su određeni stereotipovi klasa, kao i prikazane odgovarajuće vrednosti pridodate stereotipima. U potpoglavlju 8.1 opisano je modelovanje evaluacije biometrijske akvizicije. Potpoglavlje 8.2 opisuje modelovanje poređenja biometrijskih podataka. Modelovanje fuzije informacija opisano je u potpoglavlju 8.3. Naredno potpoglavlje 8.4 opisuje modelovanje prikaza evaluacije biometrijskog sistema. Nakon toga, u poslednjem potpoglavlju ove celine opisano je modelovanje osoba u bazi biometrijskog sistema.

U devetom poglavlju iznet je predlog procesa razvoja i evaluacije multimodalnih biometrijskih sistema. Za potrebe ovog procesa odabran je *Unified* proces [7], metodologija zasnovana na iterativno inkrementalnom pristupu razvoja softvera. Faze razvoja (discipline) definisane ovom metodologijom dopunjene su aktivnostima od značaja za evaluaciju i razvoj multimodalnih biometrijskih sistema. Svaka od aktivnosti je opisana i prikazana u okviru odgovarajuće faze razvoja.

Deseto poglavlje sadrži opis okvira za evaluaciju performansi biometrijskih sistema. Potpoglavlje 10.1 prikazuje pregled postojećih rešenja u ovoj oblasti. Zatim, u potpoglavlju 10.2 opisan je MMBio, okvir za razvoj multimodalnih biometrijskih sistema. Ovaj okvir upotrebljen je kao osnova za izradu okvira za evaluaciju performansi biometrijskih sistema. U potpoglavlju 10.3 opisani su korisnički zahtevi za evaluaciju performansi multimodalnog biometrijskog sistema. Potpoglavlje 10.4 prikazuje arhitekturu okvira za evaluaciju performansi multimodalnog biometrijskog sistema, kao i odnos između okvira za evaluaciju i okvira za razvoj multimodalnih biometrijskih sistema. Potpoglavlje 10.5 opisuje evaluaciju performansi konkretnog multimodalnog biometrijskog sistema. U okviru ovog potpoglavlja opisane su registracija dostupnih algoritama i baza podataka, odabir parametara evaluacije i na kraju prikaz rezultata evaluacije.

Tema jedanaestog poglavlja jeste upotreba edukativnih biometrijskih alata u procesu obrazovanja. U potpoglavlju 11.1 definisan je pojam gejmifikacije i opisani su mehanizmi koji se koriste u ovoj oblasti. Pregled primena koncepta gejmifikacije u edukaciji dat je u sledećem potpoglavlju. Zatim, u potpoglavlju 11.3 opisani su korisnički zahtevi za biometrijski alat u procesu obrazovanja. Na kraju, u potpoglavlju 11.4 izneta je studija slučaja gde je predstavljena primena edukativnog biometrijskog sistema u procesu obrazovanja. Sistem je razvijen upotrebom okvira za evaluaciju multimodalnih

biometrijskih sistema, a evaluacija je izvršena na kursu “Biometrijskih tehnologija”, u okviru master akademskih studija na Fakultetu organizacionih nauka. Opis eksperimenta je iznet u potpogavlju 11.4.1, a uticaj primene alata na ishod kursa i motivaciju studenata prikazan u potpoglavljima 11.4.2 i 11.4.3.

Zaključci vezani za okvir za evaluaciju multimodalnih biometrijskih sistema, kao i smernice za dalji rad prikazane su u poglavlju 12. Zatim, u poglavlju 13 prikazane su definicije termina i skraćenica koje su bile često korišćene u tekstu disertacije. Na kraju rada, u poglavlju 14 data je lista referenci upotrebljenih u radu. Reference su formatirane po IEEE standardu.

2 MENADŽMENT IDENTITETA

Za puno razumevanje važnosti problema biometrijske autentikacije, potrebno je razmotriti problem menadžmenta identiteta. Kao jedan od načina autentikacije korisnika, upravo u ovoj oblasti biometrijske tehnologije imaju svoju primenu. Pregledom razvoja kao i aktuelnih problema ove oblasti, stiče se bolji uvid u važnost problema adekvatne evaluacije performansi biometrijskih sistema.

Kako bismo mogli da govorimo o menadžmentu identiteta, potrebno je da se osvrnemo i na sam pojam identiteta. Ukoliko ga posmatramo iz ugla različitih naučnih i stručnih oblasti, ovaj pojam može da ima drugačija značenja. Pojam identiteta iz ugla pravnih nauka razlikuje se od viđenja iz ugla psihologije ili filozofije. Ipak u kontekstu menadžmenta identiteta, definicija data od strane Slouna [8] primarno ističe tehnološki aspekt ovog problema, a na koji se prevashodno misli kada je reč o sistemima za menadžment ideniteta. Sloun smatra da identitet treba posmatrati kao koncept koji nam omogućava da na jedinstven način identifikujemo entitet (osobu, organizaciju, računar) u okviru datog konteksta.

Da bismo tačno utvrdili određeni identitet, potrebno je to da uradimo na osnovu dostupnih informacija. Po Vajndliju [9] razlika između *online* i tradicionalnog poslovanja upravo se ogleda u činjenici da znaci poverenja na koje se ljudi uobičajeno oslanjaju u direktnom kontaktu nisu primenljivi u *online* okruženju, ili su pak veoma laki za falsifikovanje. Ova činjenica ukazuje na uvećani rizik od napada kao što su krađa identiteta ili pak neželjeno curenje poverljivih podataka. Kako bi se mogućnost pojavljivanja ovih neželjenih događaja svela na najmanju moguću meru, neophodna je upotreba pažljivo projektovanih sistema za menadžment identiteta koji u fokusu imaju bezbednost korisnika [10].

Sistem za menadžment identiteta je odgovoran za sledeće aktivnosti: identifikaciju, autentikaciju, autorizaciju, upravljanje korisničkim nalozima i praćenje aktivnosti korisnika (eng. *audit*) [10]. Identifikacija predstavlja proces zahtevanja određenog identiteta, dok se proces verifikacije zahtevanog identiteta naziva autentikacija. Neki od autora posmatraju identifikaciju kao deo procesa autentikacije [11], ali ipak se često i ovi pojmovi pominju odvojeno.

Metode autentikacije korisnika mogu se podeliti u tri kategorije [10]. To su autentikacija pomoću šifara, autentikacija na osnovu tokena i autentikacija zasnovana na biometrijskom prepoznavanju. Autentikacija pomoću šifara je najzastupljeniji [12] i najduže prisutan model. Iako lak za implementaciju, ovaj pristup ima potencijalnih problema. Kao prvo, korisnik je potrebno da pamti šifru za svaku aplikaciju. S obzirom da se danas se sve više aktivnosti (kao što su e-trgovina, upotreba društvenih mreža, bankarstvo...) obavlja preko interneta, broj šifara koje čak i prosečna osoba mora da zapamti je sve veći. Ovo često ima za rezultat ponavljanje šifara, kao i činjenicu da neki od korisnika mogu odabrati šifre koje nisu dovoljno bezbedne [13]. Takođe, u slučaju kada korisnik zaboravi šifru, potrebno mu je omogućiti kanal pomoću koga može dobiti novu. Kod nekih aplikacija koje se smatraju manje senzitivnim, to je moguće uraditi automatski, na primer putem *mail*-a, ali postoje i slučajevi kada to nije moguće uradiiti bez direktnog angažovanja korisničke podrške. Ovo može biti značajan trošak za kompaniju koja ovu podršku obezbeđuje.

Drugi pristup autentikaciji bazira se na konceptu tokena, odnosno nečega što korisnik poseduje [10]. Prednost u odnosu na upotrebu šifri jeste izbegavanje rizika postavljanja slabe šifre od strane korisnika. Ipak, bilo da je u pitanju fizički ili digitalni token, potencijalni problem ovog pristupa jeste krađa tokena. Ukoliko napadač poseduje odgovarajući token, može da pristupi servisu koji je njime zaštićen.

Ovaj problem moguće je rešiti primenom biometrijske autentikacije. Biometrijska autentikacija se zasniva na nečemu što osoba jeste [14]. Time se rešavaju problemi slabih lozinki, njihovog zaboravljanja, kao i gubitka tokena. Ipak, ni ovaj način autentikacije nije idealan. Za razliku od lozinki i tokena, u slučaju čijeg kompromitovanja moguće je izdati novu lozinku ili token korisniku, to nije slučaj sa biometrijskim podacima [15]. Usled ovoga, bezbedno skladištenje biometrijskih podataka predstavlja veoma veliki bezbednosni izazov, kao i potencijalni rizik. Jedan od pristupa rešavanju ovog problema je upotreba nekog od pristupa koji ima za cilj generisanje tokena na osnovu biometrijskih podataka osobe. Mana ovakvog pristupa rešavanju problema jeste smanjena preciznost biometrijskog prepoznavanja [15]. U tabeli 1, možemo videti uporedan prikaz karakteristika različitih metoda autentikacije.

Tabela 1 – Poređenje različitih metoda autentikacije [10]

Metod autentikacije	Troškovi implementacije	Prihvatljivost	Mogućnost zamene	Nivo bezbednosti
Šifre	Niski	Visoka	Da	Nizak
Tokeni	Srednji	Srednja	Da	Srednji
Biometrija	Potencijalno visoki	Potencijalno niska	Ne	Visok

Ovde možemo primetiti da iako druge metode autentikacije imaju određene prednosti u odnosu na biometriju, ona nudi dodatan nivo bezbednosti koji nije moguće postići isključivom upotrebom šifara ili tokena. Sistemi za menadžment identiteta imaju danas sve bitniju ulogu, pa samim tim je i njihova bezbednost sve značajnija. Stoga, upotreba biometrije kao autentikacione metode je sve učestalija.

Odabir odgovarajuće biometrijske metode za potrebe određenog sistema za menadžment identiteta nije uvek lak zadatak. Pre odabira, potrebno je izvršiti evaluaciju različitih mogućih modaliteta i rešenja, kako bi odabir optimalnog rešenja za određeni slučaj korišćenja bio moguć.

Po završetku procesa identifikacije i autentikacije, korisnik uglavnom želi da pristupi određenim servisima ili resursima za koji su izvršene ove aktivnosti. Proces utvrđivanja prava korisnika da pristupi određenim resursima ili servisima naziva se autorizacija. Upravljanje korisničkim nalozima direktno je povezano sa autorizacijom, jer se na taj način ostvaruje konzistentnost prava korisnika sa njihovim statusom u okviru organizacije [10] [16].

Svaki put kada korisnik sistema treba da se autentikuje na servis koji koristi, proces identifikacije i autentikacije zahteva određeno vreme [16]. Iako možda na prvi pogled količina utrošenog vremena može delovati zanemarljivo, u slučaju svakodnevne upotrebe većeg broja servisa, ukupno vreme može se značajno uvećati [16]. Takođe, sa povećanim brojem logovanja, raste i broj neuspešnih autentikacija, naročito u slučaju upotrebe šifara (usled grešaka korisnika prilikom unosa kredencijala) [16]. Sve ovo utiče na zadovoljstvo korisnika, gde treba imati na umu da ono direktno utiče na odluku da li će korisnik nastaviti sa upotrebom određenih servisa u budućnosti.

Pojam bitan za rešavanje upravo ovih problema jeste SSO (eng. *Single Sign-On*). SSO je povezan sa svim aktivnostima sistema za menadžment identiteta, ali pre svega sa autorizacijom i upravljanjem korisničkim nalozima [16]. Osnovna ideja SSO funkcionalnosti jeste da korisnik jedanput prođe kroz proces identifikacije i autentikacije, a da onda može dalje da koristi različite servise bez potrebe za ponavljanjem ovih procesa.

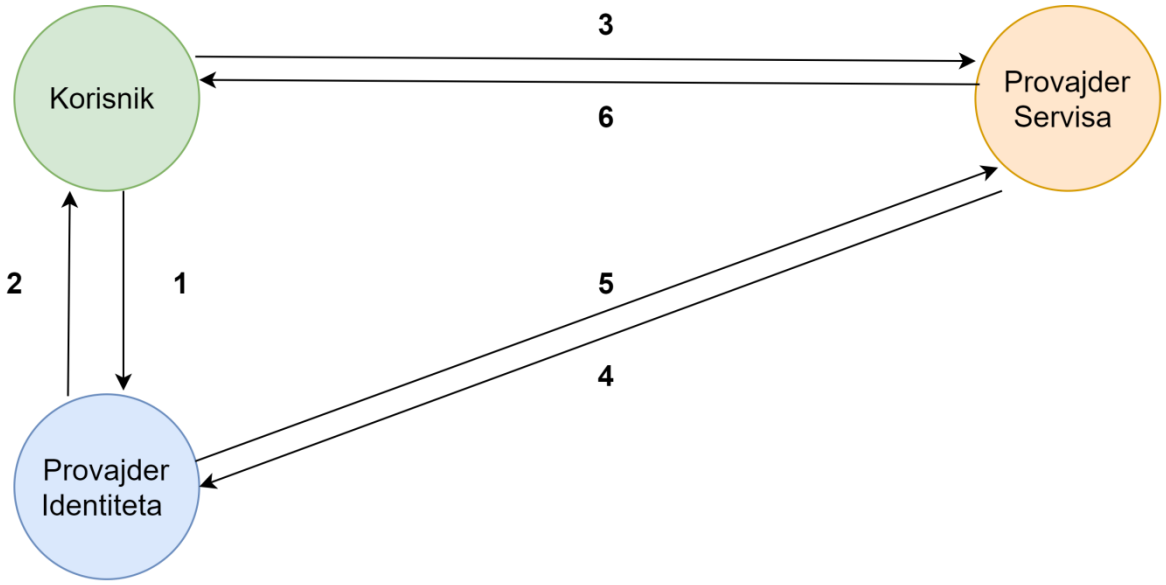
Prilikom implementacije SSO funkcionalnosti, neophodno je obratiti dodatnu pažnju na bezbednost autentikacije [16]. Ovo se odnosi kako na sam način autentikacije, gde na primer možemo primeniti višefaktorsku autentikaciju, tako i na skladištenje kredencijala za autentikaciju. Upotreba biometrije kao dodatnog načina autentikacije može značajno unaprediti bezbednost sistema. Pored ovoga, potrebno je obezbediti i obostranu autentikaciju, kako bi se sprečili napadi lažnog predstavljanja (eng. *spoofing*) [17]. Nažalost, ukoliko u bilo kom od ovih segmenata dođe do bezbednosnih propusta i neko zlonameran te propuste iskoristi, napadač potencijalno dobija pristup ne samo jednom, već čitavom nizu različitih servisa.

Već sam opis *Single Sign-On* funkcionalnosti ukazuje na činjenicu da je realizaciju sistema za menadžment identiteta moguće uraditi putem različitih pristupa. Različiti pristupi imaće različite arhitekture. Kako bi mogli da izvršimo pregled različitih logičkih pristupa razvoju arhitektura, potrebno je da definišemo osnovne pojmove koji se u njima javljaju. To su pre svega korisnik sistema, provajder identiteta i provajder servisa [10].

Korisnik sistema upotrebljava servise koje pruža provajder servisa. Korisnik mora imati makar jedan digitalni identitet kako bi mogao da upotrebljava servise dostupne u okviru konteksta definisanog digitalnim identitetom. Kako bi potvrdio zahtevani digitalni identitet, korisnik servisa komunicira sa provajderom identiteta. Provajder identiteta je zadužen za prihvatanje ili odbijanje zahtevanog identiteta korisnika, ali je takođe povezan i sa pružaocem servisa. Provajder identiteta garantuje identitet korisnika pružaocu servisa. U zavisnosti od informacija dobijenih od provajdera identiteta, pružalac usluga dozvoljava ili odbija korišćenje zahtevanih servisa [18].

Na slici 1 možemo videti primer tradicionalne centralizovane arhitekture sistema za menadžment identiteta sa numerisanim redosledom koraka u hipotetičkom scenariju korišćenja [10]. U okviru koraka 1 korisnik sistema se identifikuje provajderu identiteta. Po uspešnoj identifikaciji korisnika sistema, potrebno je izvršiti autentikaciju korisnika. Po završetku autentikacije, korisnik dobija token od provajdera identiteta (korak 2), koji se zatim prosleđuje provajderu servisa u koraku 3. Pomoću tokena, provajder servisa vrši verifikaciju kredencijala korisnika i zahteva za uslugama. Ovo se radi u oviru koraka 4 i 5, gde provajder identiteta i servisa komuniciraju kako bi potvrdili

podatke koji se nalaze unutar tokena. Po uspešnoj validaciji, korisnik sistema može pristupiti korišćenju željenih usluga (korak 6).



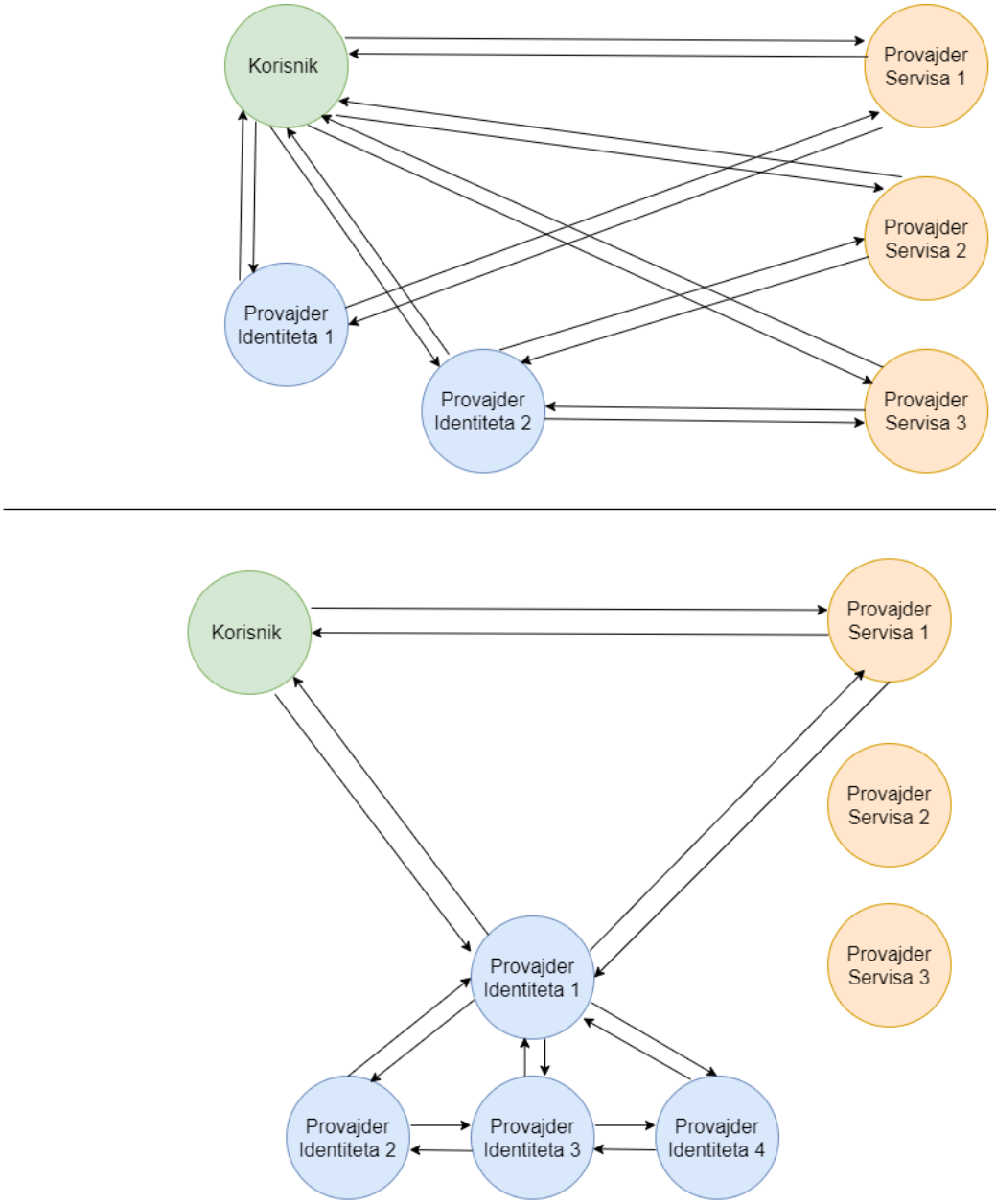
Slika 1 – Tradicionalna centralizovana arhitektura [10]

Pregledom implementacija sistema za menadžment identiteta koje su u upotrebi, možemo primetiti određene šablone vezane za njihovu strukturu. U skladu sa prethodno definisanim pojmovima, logičke arhitekture možemo klasifikovati na sledeći način: [10]

- Tradicionalna centralizovana arhitektura
- Arhitektura heterogene mreže
- Arhitektura zasnovana na konceptu federacije

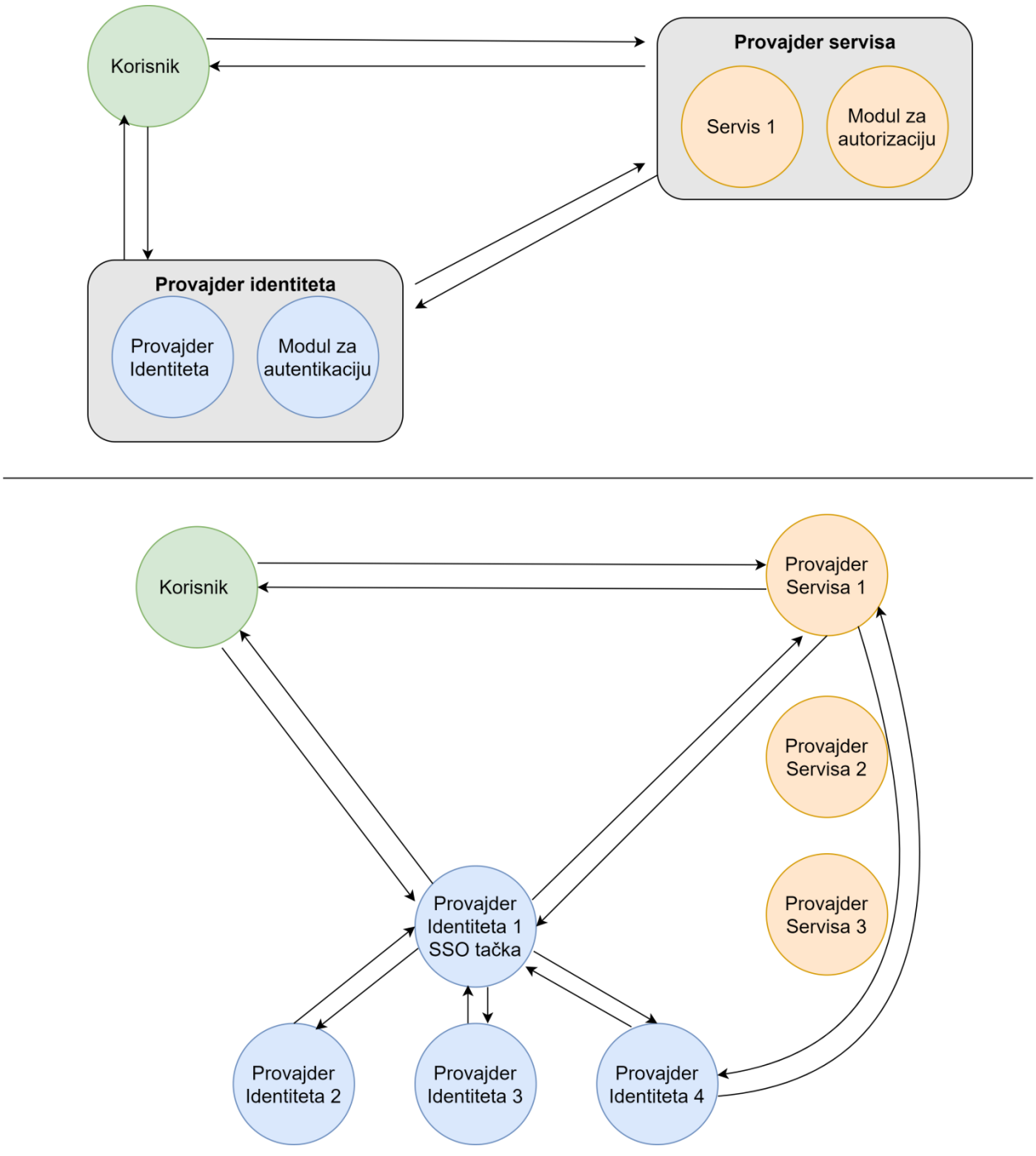
Arhitektura heterogene mreže nastaje u situacijama kada nije moguće primeniti tehnički bolja rešenja usled organizacionih ograničenja. Korisnik može koristiti servise različitih provajdera, a svaki servis može imati posebnog provajdera identiteta. Razlozi nastajanja ovakvih arhitektura mogu biti različiti, od odbijanja delova organizacije da integrišu svoj sistem sa ostatkom organizacije do postojanja "legacy" sistema, ili pak prethodnih delimično uspešnih pokušaja uspostavljanja sistema za menadžment identiteta.

Ukoliko imamo situaciju da više provajdera identiteta imaju saradnju, odnosno da dele podatke za koje su nadležni, tada možemo reći da je u pitanju arhitektura zasnovana na konceptu federacije. Na taj način se postiže da korisnik može biti identifikovan od strane svakog učesnika federacije. Glavna prednost ovog pristupa je mogućnost korišćenja usluga čak i kada se provajderi servisa i identiteta ne nalaze u okviru iste organizacije. Na slici 2 možemo videti prikaze arhitektura heterogene mreže i federacije.



Slika 2 – Arhitekture heterogene mreže i federacije [10]

Dodatno, moguće su izvesne varijacije kod svih nabrojanih tipova arhitektura [10]. Grafički prikaz varijacija dat je na slici 3. U okviru aktivnosti identifikacije, autentikacije i autorizacije moguće su različite podele odgovornosti. Za svaku od ovih aktivnosti može biti zadužen poseban modul. Takođe, *Single Sign-On* funkcionalnost može se kombinovati sa prethodnim logičkim arhitekturama. Tako da možemo imati situaciju gde je provajder servisa odgovoran za autentikaciju, ili pak tradicionalnu centralizovanu arhitekturu sa primenom SSO koncepta.



Slika 3 – Varijacije u arhitekturama [10]

Bitna stavka koja se javlja kako kod različitih sistema za menadžment identiteta, tako i u okviru stručnih i naučnih radova vezanih za ovu oblast, jeste značaj bezbedne autentikacije za ovaj tip sistema. Ovo nas upućuje na važnost adekvatne implementacije biometrijske autentikacije, kao jednog od glavnih načina autentikacije korisnika.

2.1 DLT i *Blockchain* tehnologija

Prilikom razmatranja oblasti menadžementa ideniteta, svakako moramo razmotriti uticaj i primenu DLT i *blockchain* tehnologija u okviru sistema za menadžment identiteta. *Blockchain* tehnologija se može posmatrati kao javna glavna knjiga transakcija određenog sistema, u okviru koje su transakcije pohranjene u lancu blokova [19]. Široj javnosti najpoznatiji scenario korišćenja ove tehnologije je njena upotreba kod kriptovaluta. Na primer, kod *Bitcoin*-a primenom asimetrične kriptografije vrši se potvrda transakcija, dok se istovremeno primenom heš funkcija održava integritet transakcija kroz celokupan sistem [20].

Koncept javnog *blockchain*-a kakav se nalazi u osnovi *Bitcoin*-a zapravo je samo jedan primer implementacije sistema zasnovanih na konceptu distribuirane javne knjige. Termin *blockchain*-a se često vezuje i za zapravo širi pojam distribuirane glavne knjige (eng. *Distributed ledger technology - DLT*). DLT predstavlja distribuiranu bazu podataka koja postoji kod više različitih učesnika. Karakteriše je odsustvo centralnog procesora koji se bavi skladištenjem i obradom transakcija. Ova odgovornost je kod DLT tehnologije podeljena na ravnopravne učesnike. Za implementaciju ovog koncepta nisu neophodni *proof of work* ili *proof of stake* pristupi koji mogu biti hardverski zahtevni, već su mogući i algoritmi bazirani na koncenzusu, kao što je slučaj na primer kod *Hyperledger Fabric*-a [21].

Popularizacija *blockhain* tehnologije i sistema zasnovanih na konceptu distribuirane glavne knjige imala je značajan uticaj i na oblast menadžmenta identiteta. Primena ovih koncepata u okviru sistema za menadžment identiteta nudi rešenje za određene izazove koji se javljaju prilikom dizajna i implementacije sistema, a na koje nije uvek lako ili jednostavno odgovoriti tradicionalnim pristupom. Pa autorima rada [22] primena koncepta distribuirane glavne knjige u okviru sistema za menadžment identiteta donosi sledeće benefite:

- Decentralizaciju – primenom *ledger*-a nemamo samo jedan entitet koji ima kontrolu nad identitetima
- Otpornost na neovlašćene izmene podataka
- Inkluzivnost – smanjuju se institucionalne barijere za potencijalno marginalizovane grupe ljudi
- Smanjenje troškova
- Bolju kontrola identiteta od strane korisnika

U ovom radu data je i jedna podela trenutno dostupnih rešenja za menadžment identiteta uz primenu *blockchain* tehnologije. Ona se mogu podeliti na sledeće dve kategorije sistema [22]:

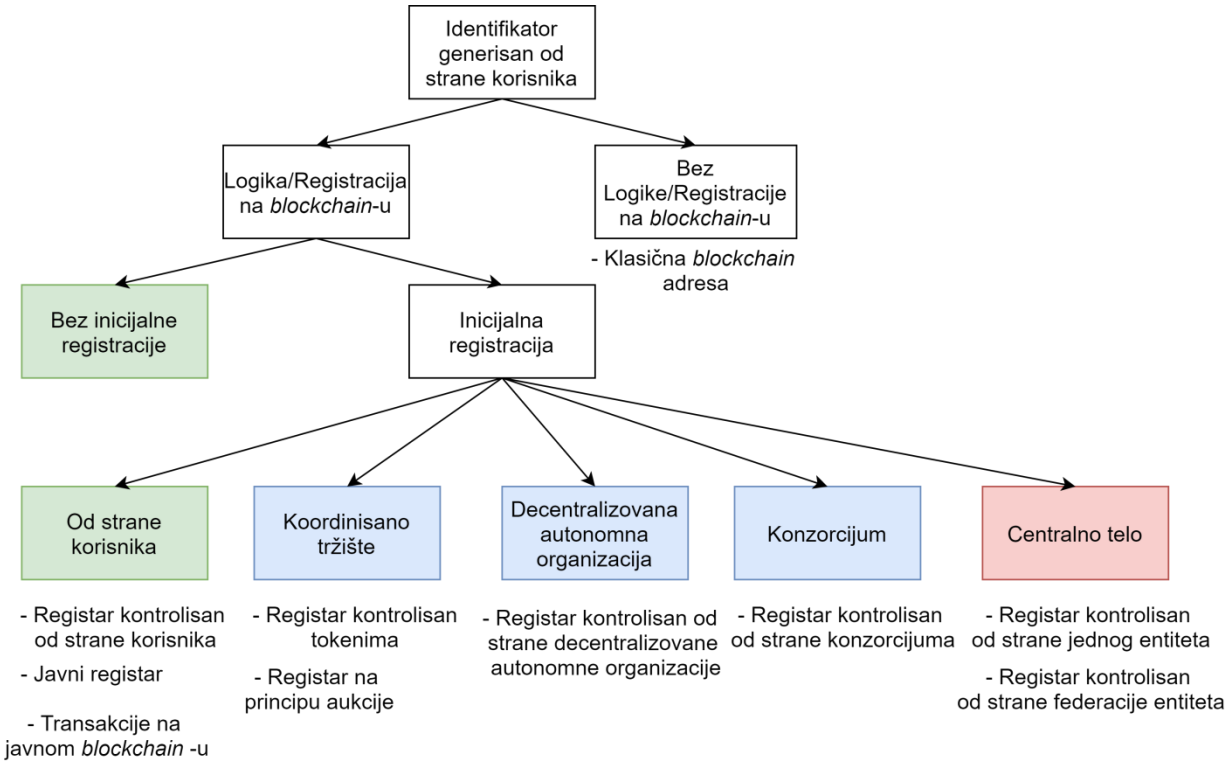
- Suvereni identitet (eng. *Self-sovereign identity*)
- Model sa proverom identiteta

Kod prve kategorije sistema korisnik sam kontroliše svoj identitet i on ne može biti oduzet od strane treće strane. Primer ovakvog sistema bio bi *Sovrin* [23]. Ovaj sistem se zasniva na konceptu javne distribuirane glavne knjige (DLT), ali koja se izvršava samo na autorizovanim sistemima. Na taj način se izbegava potreba za *proof of work* konceptom. *Sovrin* omogućava korisniku da kreira veći broj digitalnih identifikatora

pomoću kojih može imati odvojene identitete za različite potrebe komunikacije. Pomoću koncepta sidara poverenja (eng. *trust anchors*), omogućava se bolje upravljanje poverenjem u okviru mreže.

Sa druge strane kod sistema sa proverom identiteta vrši se početna provera identiteta na osnovu nekih od postojećih kredencijala, kao što su na primer lični dokumenti. Primer ovakvog sistema bio bi *IDChainZ* [24], rešenje koje funkcioniše po ovom principu. Po validaciji identiteta, korisnik može preko sistema da podesi koje podatke želi da pruži na uvid određenom trećem licu.

U izveštaju objavljenom od strane NIST-a (eng. *National Institute of Standards and Technology*) uz pomoć taksonomskog pristupa dat je uvid u problematiku sistema za menadžment identiteta baziranim na *blockchain* tehnologiji [25]. Naglašava se da primena *blockchain*-a može rešiti različite probleme koji se javljaju kod tradicionalnog pristupa ili federacije. Zapravo, primena blockhain tehnologije omogućava realizaciju pristupa menadžmenta identiteta fokusiranog na korisnika (eng. *user centric*), gde korisnik ima kontrolu nad pristupom sopstvenim podacima. Dat je pogled na modele autoriteta, šeme organizacije identifikatora, metode za upravljanje identifikatorima i kredencijalima, arhitekture sistema i upotrebu javnih registara podataka. Pogled autora na problem nastanka digitalnih identifikatora dat je na slici 4.



Slika 4 – Podela načina nastanka digitalnih identifikatora u sistemima za menadžment identiteta baziranim na *blockchain*-u [25]

Početni korak u svakoj od šema jeste generisanje *blockchain* adresa pomoću odgovarajućih privatnih ključeva. Međutim, ovaj korak nije dovoljan za potrebe sistema za menadžment identiteta, neophodna je i dodatna logika i registar identifikatora.

Crvenom bojom obeležene su šeme koje se baziraju na pristupu "od vrha ka dnu" (eng. *top down approach*), zelenom one koje pripadaju *bottom-up* pristupu, dok su plavom označena međurešenja, koja imaju elemente oba pristupa.

Na osnovu ove šeme, kao i ostale analizirane literature, možemo zaključiti da su DLT i *blockchain* doneli dodatne mogućnosti za oblast menadžmenta identiteta. Kako proces autentikacije svakako i dalje ostaje zastupljen u sistemima ove kategorije, ostaje samo da vidimo kako se biometrijska autentikacija uklapa sa primenom *blockchain* tehnologije.

2.1.1 Biometrijska autentikacija i *blockchain*

Upotreba biometrijske autentikacije u kombinaciji sa *blockchain* i DLT tehnologijama donosi određene izazove. Iako neke od kompanija koje se bave rešenjima za menadžment digitalnih identiteta baziranih na ovim tehnologijama potencijalno nude i biometrijsku autentikaciju, detalji implementacije takvih rešenja uglavnom nisu javno dostupni. Takođe i naučni radovi koji analiziraju ovu problematiku nisu preterano brojni. Ipak, sa obzirom na aktuelnost tehnologija, očekuje se rast broja kako rešenja, tako i publikacija u ovoj oblasti. Pregled trenutno dostupnih informacija dat je u okviru ovog poglavlja.

Autori [26] primećuju da prilikom pokušaja kombinovanja biometrijske autentikacije i *blockchain* tehnologije, dolazi do određenih problema. Ovi problemi posebno su izraženi kod javnih *blockchain* sistema, pre nego kod onih gde postoji poverenje između učesnika. To su pre svega troškovi čuvanja biometrijskih podataka ili obavljanja transakcija na *blockchain*-u, privatnost, skalabilnost, ograničen kapacitet za procesiranje transakcija i bezbednost. Kao najbolji odnos između potencijalnih troškova implementacije i benefita, autori predlažu skladištenje biometrijskih šablona na *blockchain*-u, dok se sam proces ekstrakcije karakteristika i poređenja odvija van *blockchain* sistema. Na taj način se sistem štiti od napada kao što su izmena biometrijskih šablona ili presretanje podataka u komunikaciji između baze podataka i modula za poređenje, a opet se ne menja preterano način funkcionisanja biometrijskog sistema.

U radu [27] predstavljen je nešto rigorozniji pogled na pitanje skladištenja biometrijskih šablona na javni *blockchain*, čak i kada su zaštićeni nekom od šema za enkripciju. Autor zauzima stav da za takav postupak ne postoji opravdanje u bilo kojoj situaciji. Racionalizacija je da su ovi podaci previše osetljivi da bi bili izloženi riziku, bilo usled nekog previda prilikom dizajna šeme za enkripciju ili dostignuća u okviru novih tehnologija kao što je kvantno računarstvo. Kao alternativa, predložen je sistem privatnih ključeva koji predstavljaju dokaz vlasništva nad tipom identifikatora poznatijim pod nazivom distribuirani identifikator. Upotreba ovih identifikatora regulisana je sistemom koji koristi DLT tehnologiju, a ključevi se štite biometrijskom autentikacijom u okviru samog biometrijskog senzora. Na taj način ne postoji centralna baza biometrijskih podataka, a opet se koriste benefiti biometrijske autentikacije.

Primena kombinacije tehnologija biometrijske autentikacije i *blokchain*-a uglavnom se može videti kod startapa koji koriste privatnu *blockchain* arhitekturu. Kompanija *INTELid* koja nudi rešenja za menadžment identiteta na bazi *blockchain* tehnologije je sklopila partnerstvo sa *ValidSoft*-om. Rezultat partnerstva je rad na integraciji

biometrijske glasovne autentikacije u sistem za menadžment identiteta [28]. Kompanija Blinking nudi autentikaciju pomoću lica i otiska prsta u kombinaciji sa sistemom za menadžment identiteta. Ovaj sistem zasnovan je na privatnoj *blockchain* arhitekturi, konkretno *Hyperledger Fabric* platformi [29]. Pored ovih, još jedan startap po imenu Zamna, fokusiran pre svega na potrebe aeroindustrije, koristi kombinaciju ovih tehnologija [30].

Dodatni primer kombinacije ovih tehnologija može se videti i u saradnji kompanija *OnFido* i *Agora* [31]. Prva od ove dve kompanije integriše svoje rešenje za biometrijsku autentikaciju pomoću oficijelnih dokumenata u sistem za onlajn glasanje razvijen od strane druge kompanije. Usled osetljivosti ovog procesa, biometrijska autentikacija omogućava potvrdu identiteta na samom uređaju, primenom odgovarajućih tehnika za utvrđivanje *liveness*-a korisnika, kao i ispravnosti identifikacionog dokumenta. Ukoliko analiza podataka pokaže da su i lični dokument i glasač pravi, kao i da se slika sa dokumenta poklapa sa slikom glasača prikupljenom pomoću kamere uređaja za glasanje, glasaču se dozvoljava dalji pristup sistemu.

Precizan način integracije biometrijske autentikacije i *blockchain* tehnologije, odnosno načina skladištenja biometrijskih šablona nije moguće utvrditi kod komercijalnih rešenja. Ipak, kompanije svakako koriste ove tehnologije u svojim rešenjima usled prednosti koje svaka od njih pruža. U nekim slučajevima moguće je da je naglašavanje kombinacije upotrebe ovih tehnologija pre svega promotivnog karaktera, drugi pak verovatno koriste biometrijsko prepoznavanje na mobilnom uređaju za potrebe *digital onboarding*-a, ali bez pamćenja šablona na *blockchain*-u. Moguće da su se određene kompanije odlučile i za skladištenje samih šablona na *blockchain*-u, u slučaju privatne *blockchain* arhitekture, što možemo pretpostaviti na primer iz objave [28]. Svakako, ovde je potrebno naglasiti rizike takvog pristupa, čak i kada posmatrana *blockchain* arhitektura nije javnog karaktera. Ipak, sa druge strane moguće je da postoje organizacije koje žele baš ovakvu implementaciju biometrijske autentikacije u konkretnom sistemu za menadžment identiteta.

3 BIOMETRIJA

Definicija biometrijskog prepoznavanja govori o uspostavljanju identiteta individue na osnovu njenih fizioloških ili bihejviorističkih karakteristika [32]. Fiziološke karakteristike su one koje su urođene, dok su bihejviorističke rezultat nečijih stečenih navika. Konkretne biometrijske karakteristike se nazivaju biometrijski modaliteti. Primeri biometrijskih modaliteta su lice, glas, otisak prsta, hod i iris.

Jedna od prednosti biometrije u odnosu na ostale metode autentikacije jeste da biometrija pored rešavanja određenih problema kao što su zaboravljanje šifara i gubitak tokena nudi i određene mogućnosti koje su nedostupne prilikom primene standardnih metoda autentikacije. To su nemogućnost poricanja, kao i takozvana negativna identifikacija. Negativna identifikacija se odnosi na mogućnost rada sa nekooperativnim subjektima, odnosno utvrđivanje da li se nečiji biometrijski podaci nalaze u bazi čak i u situacijama kada ta osoba ne želi da učestvuje u procesu autentikacije.

Kada danas govorimo o pojmu biometrije, većini ljudi će prva asocijacija biti na nešto savremeno, nastalo kao rezultat sve bržeg razvoja tehnologije. Činjenica je da su se prvi automatizovani sistemi za biometrijsko prepoznavanje pojavili tek sa adekvatnim stepenom razvoja računara, otprilike sedamdesetih godina dvadesetog veka, a da je šira komercijalna primena kasnila još nekoliko decenija usled značajnih hardverskih zahteva ovakvih sistema. Ipak, koncepti biometrijskog prepoznavanja daleko su duže prisutni u određenim oblicima.

Kao prvo, ljudi uglavnom veoma dobro prepoznaju druge ljude na osnovu lica. Sistemi za prepoznavanje lica tek su relativno skoro postali bolji u ovom zadatku, pre svega usled primene neuronskih mreža [33]. Glas i hod takođe su karakteristike na osnovu kojih razlikujemo osobe u okviru naših svakodnevnih interakcija.

Pored ovih instiktivnih sposobnosti prepoznavanja, postoje indicije da su ljudi već i u antičkom dobu znali da su otisci prsta karakteristični za svakog pojedinca. Jedan od primera jeste kineski pečat iz antičkog perioda koji sadrži prikaz otiska prsta [34]. Ipak, dokaze ovog tipa ne možemo smatrati pouzdanim, tako da se tek krajem osamnaestog veka u radu Mejera pojavila konstatacija da raspored grebena otiska prsta nikada nije isti kod dve različite osobe [35]. Tokom 19. veka, javlja se prva upotreba biometrijskog prepoznavanja u forenzičke svrhe. Pored otisaka prstiju, jedno vreme je u upotrebi bio i takozvani Bertilionov sistem, koji se zasnivao na merenju delova tela individue, odnosno na konceptu koji je danas poznat kao *soft biometrics* [35]. Ovaj sistem se ipak pokazao nedovoljno preciznim, tako da je posle određenog vremena povučen iz upotrebe.

Sir Edvard Henri je zajedno sa svojim saradnicima, kao generalni policijski inspektor u Bengalu, koloniji tadašnje Britanske imperije, uspostavio sistem pretrage otisaka prstiju. Ovaj sistem, poznat kao Henrijev sistem, je poslužio kao osnova za dalju implementaciju prepoznavanja otisaka u forenzičkoj praksi. U Sjedinjenim Američkim Državama, FBI (eng. *Federal Bureau of Investigation*) je 1924. godine formirao posebno odeljenje za identifikaciju otisaka prstiju, a broj prikupljenih kartona sa otiscima prstiju različitih osoba već tada je iznosio 810,000 [35].

Sa prikupljanjem sve većeg broja otisaka prstiju, proces ručnog poređenja velikog broja kartona sa nečijim otiscima prstiju postao je sve obimniji i zahtevniji. Primena Henrijevog sistema jednostavno više nije bila praktična. Ovaj proces započet je tokom 1960-tih godina, ali tek je tokom sedamdesetih godina prethodnog veka došlo do značajnih proboja u ovoj oblasti. Kako bi rešio probleme vezane za ovaj proces, FBI je uspostavio saradnju sa NIST-om (eng. *National Institute of Standards and Technology*). Jedan od rezultata ove saradnje jeste M40 algoritam, prvi operativni algoritam za poređenje otisaka prstiju, koji je korišćen za smanjenje potrebnog obima ručnih poređenja [36]. Primenom ovog algoritma, forenzičkim ekspertima je omogućen uvid u listu identiteta osoba sa sličnim otiscima prstiju, čime se značajno smanjilo vreme potrebno za pretragu baze.

Na osnovu ugovora sa FBI-jem, *Rockwell International* je izradio studiju sa kojom je zaključio da bi automatizacija ovog procesa omogućila smanjenje trajanja upita sa nedelja na sate i donela uštede od 14 miliona dolara godišnje [37]. Zaključak ove studije je da ovaj proces treba uraditi inkrementalno, usled velikog obima i kompleksnosti zadatka. Dalji rad na AIDS (eng. *Automated Identification Division System*) nastavljen je tokom sedamdesetih godina, sa više faza razvoja sistema, a sve sa krajnjim ciljem pretraživanja baze podataka identiteta pomoću otisaka prstiju, kao i njene potpune digitalizacije [37].

Sledeći biometrijski modalitet koji je našao svoju primenu jeste geometrija šake. David Sidlauskas je 1985 godine podneo zahtev za patent jednog ovakvog sistema, koji je odobren 1988 godine [38], a na osnovu koga su se pojavili prvi komercijalni sistemi ovog tipa. Tokom devedesetih godina, upotreba geometrije šake bila je prisutna u različitim organizacijama u Sjedinjenim Američkim Državama. INPASS sistem sa biometrijskom autentikacijom pomoću otiska šake korišćen je u SAD za kontrolu granica na aerodromima [39]. Volt Dizni je za ulaz u svoj tematski park takođe implementirao biometrijsku autentikaciju pomoću geometrije šake [40]. Ovi sistemi su bili među prvim implementiranim komercijalnim biometrijskim sistemima za kontrolu pristupa koji su radili sa značajnijim brojem ljudi.

Sa širom primenom biometrijskog prepoznavanja, pitanja vezana za pravne aspekte ove tehnologije postala su sve bitnija. Na primer, program nadzora uz primenu lica kao biometrijskog modaliteta u gradu Tampi, Sjedinjenim Američkim Državama pokazao se kao promašaj [41]. Ovaj sistem je prvi put testiran prilikom održavanja *Super Bowl*-a, a zatim i primenom samog video nadzora širom grada. Međutim, pored pokretanja brojnih javnih rasprava, sam sistem nije bio uspešan u prepoznavanju traženih kriminalaca, a percipiran je kao značajno narušavanje privatnosti velikog broja pojedinaca.

Ipak, sa napretkom tehnologije, upotreba biometrijskog prepoznavanja postala je sve češća u svetu. Danas biometrijska autentikacija predstavlja sastavni deo različitih sistema, od pametnih telefona, preko društvenih mreža do kontrole granica. U zavisnosti od potreba sistema, različiti tipovi biometrijskih modaliteta se primenjuju. Više detalja o različitim biometrijskim modalitetetima izneto je u nastavku ovog poglavlja.

3.1 Fiziološki biometrijski modaliteti

Fiziološki biometrijski modaliteti predstavljaju urođene fizičke karakteristike pojedinca. Primeri fizioloških biometrijskih modaliteta su lice, otisak prsta, geometrija šake, uho i iris. Generalno, češće se primenjuju u praksi od bihejviorističkih biometrijskih modaliteta usled veće preciznosti prepoznavanja i lakše akvizicije adekvatnog uzorka. Detalji o nekim od fizioloških biometrijskih modaliteta dati su u nastavku teksta.

3.1.1 Otisak prsta

Otisak prsta danas je jedan od češće upotrebljavanih biometrijskih modaliteta u praksi. Duga praksa upotrebe ovog modaliteta za forenzičke svrhe, kao i dobre performanse doprinele su širokoj rasprostranjenosti primene ovog modaliteta.

Metode za poređenje otisaka prstiju se mogu podeliti u tri kategorije [35]:

- Poređenje bazirano na korelaciji otisaka
- Poređenje bazirano na minucijama
- Poređenje bazirano na karakteristikama koje nisu minucije

Metode koje se zasnivaju na poređenju minucija najzastupljenije su u literaturi i praksi [35]. Ovi algoritmi se zasnivaju na sličnom principu koji koriste i forenzički eksperti kada vrše poređenje otisaka. Minucija predstavlja različite tipova prekida u grebenima otiska prsta (eng. *ridges*). Uglavnom se predstavljaju pomoću koordinata lokacija, ugla i tipa minucije (da li je u pitanju bifurkacija, kraj grebena ili neki drugi tip minucije).

NIST je sproveo istraživanje kako bi ispitao preciznost algoritama za prepoznavanje otiska prsta nad velikim bazama biometrijskih podataka, koje sadrže podatke nekoliko miliona otisaka prstiju [42]. Prilikom identifikacije, najprecizniji algoritmi su u slučaju rada sa jednim otiskom kažiprsta ostvarili rezultat od 1.9% FNIR (eng. *False Negative Identification Rate*). U slučaju kombinacije podataka dva otiska kažiprsta, ovaj rezultat je značajno bolji i FNIR metrika iznosi oko 0.27%. Najbolja preciznost očekivano je postignuta za otiske svih 10 prstiju, gde je vrednost FNIR parametra iznosila 0.09%.

Za potrebe akvizicije otiska prsta većinom se koriste za tu namenu specijalizovani senzori. Postoje različiti tipovi senzora, kao što su optički, kapacitivni ili senzori bazirani na ultrazvučnoj tehnologiji. Novija istraživanja u ovoj oblasti bave se beskontaktnom akvizicijom otisaka prstiju. Ovde su mogući različiti pristupi, od upotrebe specijalizovanih senzora, preko korišćenja hardvera opšte namene kao što su kamere na pametnim telefonima.

U radu [43] opisan je biometrijski sistem za poređenje otisaka prstiju koji akviziciju vrši pomoću pametnih telefona. Opisani su algoritmi za segmentaciju otiska sa slike, pretprocesiranje, skaliranje, ekstrakciju minucija i poređenje. Nad bazom od 1800 otisaka prikupljenim od 25 osoba, EER (eng. *Equal Error Rate*) ovog pristupa iznosio je 3,74%. Sličan pristup koristi i kompanija Veridium koja nudi komercijalno rešenje *4F:Touchless ID*. Ovo rešenje za autentikaciju korisnika skenira otiske 4 prsta pomoću kamere pametnog telefona [44].

Istraživanje u oblasti parcijalnih otisaka prstiju jedan je od pravaca koji je aktivan poslednjih godina. Upotreba beskontaktnog skeniranja otisaka prstiju često dovodi do

pojave parcijalnih otisaka prstiju. U radu [45] prikazan je novi pristup za rad sa trodimenzionalnim otiscima prstiju, uz primenu konvolucionih neuronskih mreža nad različitim reprezentacijama samog otiska. Na taj način se pokušava rešiti problem većeg broja pozicija u kojima se otisak prsta može naći usled odsustva kontaktne površine senzora. Rezultati istraživanja ukazuju na unapređenje performansi u odnosu na postojeće metode.

Problem parcijalnih otisaka se javlja i kod kontaktnih senzora koji imaju malu površinu, što je čest slučaj na uređajima gde postoji ograničena količina prostora za senzor (kao što su mobilni telefoni). Klasični algoritmi bazirani na minucijama u slučaju parcijalnih otisaka često nemaju dovoljno informacija na osnovu kojih bi mogli da donesu odluku. U radu [46] opisan je multibiometrijski pristup koji koristi dva algoritma za ekstrakciju karakteristika, kao i njihovo kasnije poređenje. Pored minucija, u upotrebi je i specifičan oblik grebena otiska prsta – RSF (eng. *Ridge Shape Features*). Fuzija se vrši na nivou skorova poređenja. Primena ovog pristupa kod senzora sa malom površinom donela je poboljšanja kod akvizicije podataka u odnosu na isključivu upotrebu minucija za dalje potrebe poređenja.

Uz otiske koji su voljno ostavljeni od strane korisnika nekog sistema za autentikaciju, istraživanje vezano za još jednu kategoriju parcijalnih otisaka prstiju je danas aktuelno, a to su latentni otisci prstiju. Ova kategorija otisaka se koristi u forenzici, a označava otiske koji su ostavljeni na predmetima. Ovakvi otisci imaju slabije izražene grebene i lošijeg su kvaliteta. U radu [47] predstavljen je algoritam za rad sa latentnim otiscima prstiju baziran na neuronskoj konvolucionoj mreži. Algoritam se pokazao među najboljim u javno dostupnim rezultatima, sa stopom identifikacije od 75.3% za WVU bazu [48]. Takođe, autori navode da se fuzijom sa skorovima dobijenim od strane drugih komercijalnih rešenja može dodatno unaprediti preciznost prepoznavanja.

3.1.2 Lice

Kada govorimo o fiziološkim modalitetima, pored otiska prsta, lice danas predstavlja jedan od najznačajnijih biometrijskih modaliteta. Pogodno je za korišćenje bilo u scenarijima kontrole pristupa, odnosno biometrijske verifikacije, kao i u scenarijima kod kojih nije obezbeđena kooperativnost korisnika biometrijskog sistema. Ljudi u svome svakodnevnom životu pomoću lica prepoznaju druge osobe, tako da imaju manje primedbi kada je potrebno da negde ostave ovaj biometrijski podatak, u odnosu na otisak prsta ili iris.

Algoritme koji se koriste za prepoznavanje lica možemo podeliti u nekoliko kategorija. Prva kategorija jesu algoritmi koji se zasnivaju na nekoj od standardnih statističkih metoda. U ovu kategoriju spadaju radovi [49]. Algoritmi iz ove kategorije su jedno vreme bili češće upotrebljavani u praksi. Razlog tome jeste što nisu preterano hardverski zahtevni, a i za njihovu upotrebu nije potrebno imati prethodno prikupljene velike baze podataka za treniranje algoritma. Drugi tip pristupa jeste primena neuronskih mreža. Iako teorijska osnova ovog pristupa nije skorijeg datuma [50] [51], tek poslednjih godina njihova primena ima smisla u praksi [52] [53]. Razlog za ovu činjenicu jeste zahtevnost treniranja, kako u smislu potrebnog hardvera, tako i potrebne velike količine podataka.

Performanse najboljih komercijalnih algoritama za prepoznavanje lica možemo pratiti u okviru NIST-ove FRVT (eng. *Face Recognition Vendor Test*) evaluacije [54]. Testiranje je izvršeno nad nekoliko setova podataka – set prikupljen od policijskih istraga, aplikacije za vize, aplikacije za imigracione papire, fotografije prikupljene prilikom prelaska granice, policijiski setovi podataka, kao i podaci sa kamera za video nadzor. Na primer, prilikom ispitivanja na setu aplikacija za vizu, najbolji algoritam prilikom FMR-a od 0.000001% daje vrednost FNMR metrike od 0.0027%, dok u slučaju podataka sa kamera za video nadzor i iste vrednosti FMR-a, vrednost FNMR metrike tog algoritma iznosi 0.0301%.

Za akviziciju lica, pored primene standardnih kamera, koriste se i specijalizovani senzori kao što su termalne kamere. U radu autora Krišta i Ivasić-Kos [55] navodi se da termalne kamere imaju prednost u tome što nisu osetljive na osvetljenje, ali da imaju i manu da im preciznost opada sa udaljavanjem od senzora akvizicije. Autori predlažu kombinaciju vidljivog i infracrvenog spektra, kao i upotrebu konvolucionih neuronskih mreža za prevazilaženje ovih problema.

3.1.3 Iris

Iris je mišić oka koji kontroliše veličinu zenice, kako bi na taj način regulisao količinu svetlosti koja ulazi u oko [56]. Kao biometrijski modalitet odlikuje se veoma visokom preciznošću. Glavni razlog preciznosti prepoznavanja je izuzetna složenost i individualnost ovog biometrijskog modaliteta. Takođe, pošto je iris zapravo unutrašnji organ, zaštićeniji je od promena usled uticaja spoljne sredine.

Ipak, složenost irisa je prilikom početnih istraživanja zadavala probleme naučnicima. Prvi uspešan algoritam koji je razvio Džon Dugman objavljen je 1993. godine u IEEE časopisu [57], a zatim i patentiran [58]. Ključ ovog algoritma je test statističke nezavisnosti, koji usled visokih stepeni slobode garantuje prolaz testa u slučaju irisa različitih očiju, ali i pad kada se porede karakteristike irisa dobijene od istog oka. Prihvaćen od strane brojnih kompanija, ovaj algoritam se i danas nalazi u gotovo svim komercijalnim rešenjima ovog tipa, naravno uz odgovarajuća kontinualna poboljšanja sa prolaskom vremena.

NIST je sproveo IREX IX evaluaciju [59] kako bi utvrdio preciznost komercijalnih algoritama za prepoznavanje irisa. Trenutno prilikom poređenja irisa oba oka, kod verifikacije najbolji rezultati daju FNMR-a od 0.0057% pri vrednosti FMR metrike od 10^{-5}. Rezultati još 4 proizvođača su po navodima NIST-a približne preciznosti, gde razlika u odnosu na najbolji rezultat nije statistički značajna.

Novija istraživanja vezana za iris kao biometrijski modalitet pre svega se fokusiraju na aspekte kao što su upotrebljivost i bezbednost. U radu [60] dat je pregled pristupa za zaštitu od lažiranja irisa prilikom akvizicije. Izvršena je podela pristupa detekcije napada na osnovu tri kriterijuma. Prvi kriterijum je da li se oko posmatra kao statički ili dinamički entitet. Drugi kriterijum je definisan na osnovu činjenice da li stimulacija irisa od strane senzora dovodi do promena na irisu ili ne. Poslednji kriterijum se odnosi na lakoću primenljivosti pristupa u komercijalnim sistemima za prepoznavanje irisa. Razmotrene su i različite metodologije napada kao što su štampani napad (eng. *print attack*), kontaktna sočiva sa teksturom, napadi sa upotrebom displeja, kao i pokušaji sabotiranja akvizicije radnjama korisnika.

Autori [60] zaključuju da je istraživanje u ovoj oblasti još uvek aktuelan i otvoren problem. Takođe, konstatuju da je evaluacija rezultata u ovoj oblasti posebno izazovna. Razlozi su različiti, od činjenice da standardne mere i pristupi koji se koriste kod određivanja preciznosti biometrijskih sistema mogu dati lažnu sliku o uspešnosti evaluirane metode, do specifičnosti implementacije sistema kao i uticaja akcija korisnika na uspešnost lažiranja biometrijskih podataka. Na kraju rada date su sugestije za unapređenje stanja u ovoj oblasti, kao što su kreiranje lako dostupnih platformi za testiranje algoritama, obezbeđivanje javno dostupnih baza podataka za testiranje i razvoja dostupnih algoritama otvorenog koda.

Tradicionalni senzori za akviziciju irisa baziraju se na NIR (eng. *near infrared*) tehnologiji. Mana ovog pristupa jeste da zahteva da korisnik bude u relativnoj blizini senzora, sa orijentacionim rastojanjem od jednog metra. Pored zahteva koji se odnose na rastojanje, potrebno je da korisnik bude u razumnoj meri kooperativan kako bi proces akvizicije mogao nesmetano da se odvija. Kako bi se poboljšala upotrebljivost sistema za prepoznavanje irisa, kao i omogućila njegova upotreba u različitim uslovima korišćenja, potrebno je unaprediti ovu tehnologiju tako da akvizicija bude moguća sa veće razdaljine i u manje otežanim uslovima. U radu [61] dat je pregled dostignuća u oblasti prepoznavanja irisa na daljinu. Prikazana su trenutna dostignuća u ovoj oblasti i dat njihov uporedni prikaz. Zaključak je da je u ovoj oblasti došlo do značajnog napretka, kako u rastojanju sa koga je moguća akvizicija tako i u smanjenju invazivnosti akvizicije i unapređenju preciznosti prepoznavanja. Ipak, postoji još uvek prostor za unapređenje prepoznavanja irisa na daljinu, kako u oblasti senzora tako i u delu vezanom za procesiranje slike, ekstrakciju karakteristika i poređenje.

3.2 Bihejvioristički biometrijski modaliteti

Od ponašajnih biometrijskih modaliteta, rađene su studije sa različitim biometrijskim modalitetima kao što su hod, rad sa tastaturom, rad sa mišem i potpis. Iako sama preciznost ovih metoda najčešće nije na nivou popularnih fizioloških modaliteta, njihova upotreba može biti pogodna u određenim situacijama. Neki od ovih modaliteta nisu invanzivni, dok se drugi mogu lako integrisati u postojeće sisteme za nadzor. Ovi modaliteti uvek mogu poslužiti i kao dodatni izvor informacija za multimodalni biometrijski sistem.

Istraživanje [62] bavilo se biometrijskim prepoznavanjem uz upotrebu informacija vezanih za rad sa tastaturom, mišem, upotrebu aplikacija i opterećenost sistema. Tokom perioda od 10 nedelja prikupljeni su podaci od 99 korisnika. Kako rezultati vezani za ove modalitete mogu da imaju značajne varijacije u kraćem vremenskom periodu, ideja je bila proveriti da li se modaliteti mogu koristiti za autentikaciju korisnika na osnovu njihovih akcija u dužem vremenskom periodu. Rezultati pokazuju da se kombinacija upotrebljenih modaliteta na uzorku ove veličine može pouzdano koristiti za kontinualnu autentikaciju korisnika.

Široka rasprostranjenost pametnih mobilnih telefona i činjenica da ih ljudi konstantno koriste takođe otvara nove mogućnosti za upotrebu ove kategorije metoda. U doktorskoj disertaciji [63] opisano je nekoliko multimodalnih biometrijskih sistema za autentikaciju korisnika pametnih telefona koji koristi bihejviorističke biometrijske modalitete. Prikazane su različite kombinacije modaliteta koji se mogu koristiti, od načina kucanja PIN koda, do držanja telefona, načina potpisivanja na ekranu osetljivom

na dodir, načina otključavanja telefona i upotrebe glasa kao dodatnog biometrijskog modaliteta. Autor [63] zaključuje da prednost primene kombinacije ovih modaliteta jeste lakoća upotrebljivosti, gde korisnik gotovo da nema potrebe za dodatnim akcijama radi autentikacije, kao i široka dostupnost hardvera neophodnog za akviziciju na današnjim pametnim telefonima.

Kao ekstenzija prethodno opisane teze, u radu [64] predstavljen je bimodalni sistem koji koristi način na koji korisnik otključava telefon, kao i način na koji ga prinosi uhu prilikom javljanja za potrebe verifikacije korisnika. Za akviziciju ovih podataka koriste se senzori dostupni na pametnim telefonima, a to su akcelerometar, žiroskop, senzor za gravitaciju i magnetometar. Testiranje je izvršeno nad 10,200 uzoraka prikupljenih od 85 osoba. U najboljoj kombinaciji algoritama, sa primenom RF (eng. *Random Forest*) algoritma, sistem je ispravno prihvatio 99,35% korisnika.

Prepoznavanje potpisa korisnika je takođe značajan modalitet u ovoj kategoriji. Potpis je jedan od prihvaćenih modaliteta potvrđivanja nečijeg identiteta koji ima dugu tradiciju upotrebe. Kako bi i u digitalnom svetu mogao da se koristi za potrebe autentikacije, pored samog oblika potpisa prate se i drugi parametri, kao što su kretanje olovke tokom vremena i nivo pritiska u samoj olovci u određenom trenutku. U radu [65] prikazana je primena rekurentnih neuronskih mreža sa sijamskom arhitekturom (eng. *Recurrent Neural Networks with a Siamese architecture*) koje se koriste za izračunavanje metrika distance između dva različita potpisa. Za evaluaciju upotrebljena je *BiosecureID* [66] baza podataka koja sadrži 11,200 potpisa prikupljenih od 400 korisnika tokom četiri akvizicione sesije. U slučaju namernih falsifikata potpisa najbolja vrednost EER parametra bila je 5,5%, dok je u slučaju upotrebe drugih potpisa pravih (eng. *genuine*) korisnika ta vrednost iznosila 3%. Ovi parametri pokazali su unapređenje u odnosu na dosadašnja istraživanja u ovoj oblasti.

Još jedan od bihejviorističkih biometrijskih modaliteta jeste hod. Prednost ovog modaliteta jeste relativno laka akvizicija podataka na daljinu, čak i bez znanja subjekta, što može biti posebno zgodno za upotrebu u sistemima za nadzor. U ovoj oblasti objavljen je značajan broj radova, sa različitim pristupima rešavanju ovog problema. Pristupi koji se koriste se razlikuju, jedna kategorija radova zasniva se na predefinisanim modelima, koji koriste predznanja o ljudskoj figuri i načinu hoda, dok druga pak ne polazi od ovakvih pretpostavki [67].

Značajan broj radova u ovoj oblasti koncetrisao se na podizanje preciznosti sistema, primenom različitih algoritama mašinskog učenja. Posebna pažnja se daje poboljšanju performansi u situacijama gde okluzija, odeća, ugao posmatranja ili drugi razlozi dodatno otežavaju prepoznavanje osobe. Drugi dominantan pravac je upotreba inovativnog, a opet široko dostupnog hardvera radi akvizicije podataka za potrebe prepoznavanja hoda.

Širaga i ostali [68] predlažu korišćenje konvolutivnih neuronskih mreža za robustno prepoznavanje hoda. Kao ulaz u neuronsku mrežu predlažu energetsku sliku hoda (eng. *Gait Energy Image*). Ova slika se dobija kao kombinacija sekvence silueta hoda u toku jednog ciklusa hoda. Predstavlja kombinaciju statičkih i dinamičkih aspekata hoda. Evaluacija je vršena nad dva seta podataka, od kojih je jedan prikupljen od strane kooperativnih, a drugi od strane nekooperativnih subjekata. Rezultati su pokazali poboljšanja u odnosu na druge metode, a posebno u slučaju verifikacije gde se EER

kretao između 1% i 2.7% za kooperativne korisnike (u zavisnosti od ugla posmatranja), dok je kod nekooperativnih korisnika najbolji EER bio 1.6%.

Akvizicija podataka za prepoznavanje hoda pomoću Kinect senzora veoma je popularan pristup u objavljenim naučnim radovima. U radu [69] predlaže se upotreba *deep learning* pristupa za rad sa podacima prikupljenim Kinect senzorom. Milovanović i ostali [70] predlažu upotrebu CBIR (eng. *Content-Based Image Retrieval*) metoda za poređenje prikupljenih podataka. U radu Sun i ostalih [71] predlaže se kombinacija 2D silueta prikupljenih od Kinect kamere kao i trodimenzionalnih podataka od strane odgovarajućeg senzora.

Rad [72] zasniva se na pristupu koji koristi mobilni telefon kao sredstvo za akviziciju podataka. Baza podataka sadrži podatake 30 osoba, od kojih je svaka obavljala različite fizičke aktivnosti kao što su hodanje, penjanje uz i niz stepenice, dok je nosila pametni telefon. Za akviziciju podataka su korišćeni akcelorometar i žiroskop. Korišćen je koncept *i-vector* karakteristika kako bi se poboljšala preciznost. Po izvođenju ovih *i-vector* karakteristika, vrši se linearna diskriminaciona analiza ili probabilistička linearna diskriminaciona analiza, kako bi se maksimizovale razlike između korisnika, a minimizovale razlike između istih uzoraka dva korisnika. EER u najboljoj kombinaciji algoritama iznosio je oko 6.1%.

Wang i ostali [73] predložili su novi eksperimentalni pristup prepoznavanju hoda koji za akviziciju koristi komercijalne WiFi uređaje. Na osnovu informacija o stanju kanala (eng. *Channel State Information*) na prijemniku, prikupljaju se podaci kao što su brzina hoda, vreme ciklusa hoda, veličina koraka i brzina kretanja ruku i nogu. Rezultati istraživanja pokazuju izvodljivost biometrijskog prepoznavanja hoda ovim pristupom uz određena ograničenja. Potrebno je da korisnik hoda u određenom predefinisanom pravcu u dužini oko 5,5 metara. Takođe, promena pozicije senzora zahteva ponovno treniranje sistema, tako da je ovaj pristup pogodan samo za prostore u kojima korisnik nema previše izbora oko pravca i smera kretanja. U slučaju upotrebe jednog prijemnika, teško je razdvojiti signale koji pripadaju različitim osobama koje se nalaze jedna blizu druge. Ovaj poslednji problem autori predlažu da reše uvođenjem većeg broja prijemnika kao i primenom novih algoritama.

Na osnovu pregleda radova, možemo zaključiti da postoje različiti biometrijski modaliteti u ovoj kategoriji koji se mogu koristiti za prepoznavanje osoba. Preciznost ovih metoda je uglavnom na nižem nivou nego kod fizioloških biometrijskih modaliteta. Pošto često nedostaju i obimnije javno dostupne baze biometrijskih podataka za određene modalitete, ovu preciznost nije uvek moguće sa pouzdanošću utvrditi. Ipak, bihejvioristički biometrijski modaliteti imaju neke druge prednosti u odnosu na fiziološke modalitete kao što su manja invanzivnost i teže lažiranje biometrijskih podataka. Takođe, mogu se koristiti u kombinaciji sa nekim od fizioloških modaliteta kako bi se multimodalnim pristupom dodatno poboljšala preciznost sistema.

3.3 Kombinovani biometrijski modaliteti

Nema prepreka da biometrijski modalitet predstavlja kombinaciju dve prethodno navedene kategorije biometrijskih modaliteta, a primer takvog biometrijskog modaliteta jeste glas. On je pogodan je za različite tipove primena. Ljudi su navikli da komuniciraju pomoću glasa i njegova upotreba kao biometrijskog modaliteta im dolazi

lakše nego drugi, intruzivniji biometrijski modaliteti kao što je na primer iris. Očekivanja su da će upravljanje pametnim telefonima i računarima pomoću glasa biti sve češće korišćena funkcionalnost, te je dodavanje glasovne autentikacije logičan korak.

Kao što je već naglašeno, glas odnosno govor korisnika ima dva aspekta, fiziološki i ponašajni. Fiziološki parametri nastali su usled specifičnosti vokalnog trakta svake individue, dok akcenat, izbor reči i intonaciju možemo okarakterisati kao ponašajne karakteristike [74]. Na osnovu kombinacije ovih parametara koja je specifična za svakog pojedinca, algoritmi za prepoznavanje glasa pokušavaju da razlikuju osobe.

Kod prepoznavanja govornika imamo dva potencijalna pristupa. Prvi pristup zahteva od korisnika izgovaranje određene zadate fraze (eng. *text dependent speaker recognition*). Prednost ovog pristupa je u tome što zahteva algoritme manje hardverski zahtevne za treniranje. Mana ovog pristupa je što se može koristiti samo u situacijama kada korisnik želi da sarađuje. Za potrebe nadzora, na primer na nekom međunarodnom aerodromu, od značaja bi bilo prepoznavanje korisnika na osnovu karakteristika samog glasa, bez obzira na izgovoren sadržaj (eng. *text independent speaker recognition*). Ovakav scenario prepoznavanja je dodatno kompleksan, jer uglavnom uključuje i pozadinsku buku, kao i veći broj ljudi koji razgovaraju na određenom prostoru.

Klasični sistemi za tekstualno zavisno prepoznavanje korisnika koriste algoritme kao što su MFCC (eng. *Mel Frequency Cepstral*) ili LPCC (eng. *Linear Predictive Cepstral Coefficients*) za ekstrakciju karakterisitka i HMM (eng. *Hidden Markov Model*) za poređenje karakteristika. Ovi algoritmi se generalno javljaju kod prepoznavanja govora, ali se modeli mogu prilagoditi i za prepoznavanje specifičnog korisnika.

Jedna od standardnih metoda koja se koristi u ovom domenu jeste GMM (eng. *Gaussian Mixture Model*) uz eventualnu primenu SVM (eng. *Support Vector Machines*), kao što je urađeno u radu [75]. Radovi novijeg datuma generalno se više bave problemom tekstualno nezavisnog prepoznavanja korisnika. Ovde je upotreba *deep learning* tehnika i razvoj hardvera otvorila nove mogućnosti za prepoznavanje glasa, pogotovu u otežanim uslovima.

Bitno je napomenuti da granice između oblasti tekstualno zavisnog i tekstualno nezavisnog prepoznavanja nisu toliko oštre. U radu [76] predložena je primena metode GMM-UBM (eng. *Gaussian Mixture Model – Universal Background Model*) koja je dotle korišćena pre svega za tekstualno nezavisno prepoznavanje u kontekstu tekstualno zavisnog. Primena ovog algoritma dodala je nove opcije balansa između preciznosti i kompleksnosti i veličine modela.

Primena *i-vector* pristupa, pristupa popularnog za rešavanje različitih problema vezanih za glas je takođe zasnovana na ovim algoritmima (GMM/UBM). Primenom linearne diskriminacione analize može se vršiti poređenje da li dobijeni supervektori pripadaju istim osobama [77]. Moguće su i kombinacije upotrebe *i-vector*-a sa upotrebom neuronskih mreža [78]. Jedan od novijih pristupa bazira se na primeni neuronskih mreža za ekstrakciju karakteristika, takozvanih *x-vector*-a. Dok upotreba *i-vector* pristupa u kombinaciji sa DNN mrežom za klasterizaciju zahteva upotrebu transkribovanih glasovnih podataka prilikom treninga, za primenu *x-vector*-a dovoljne su samo labele govornika [79]. Ovaj pristup je stoga posebno pogodan kada imamo na

raspolaganju veoma obimne setove podataka i možemo ga smatrati kandidatom za novi standard u oblast prepoznavanja govornika.

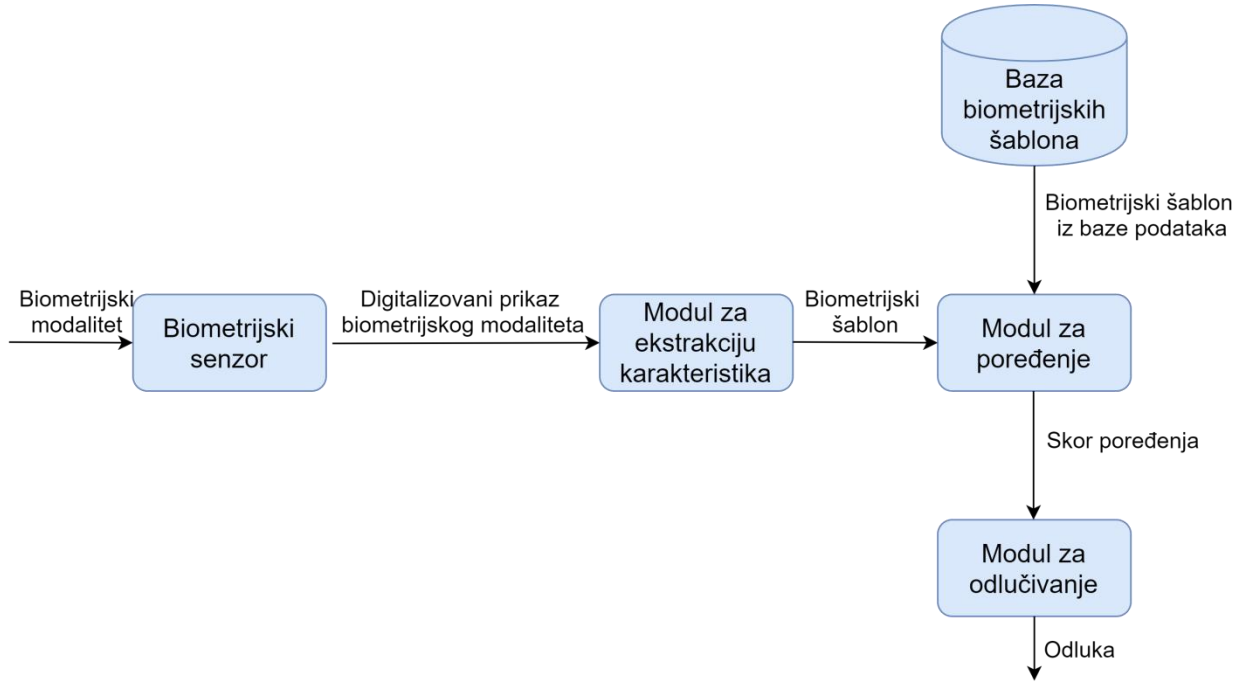
Trenutno je u toku *NIST 2020 CTS Speaker Recognition Challenge* [80]. Ova evaluacija ima za cilj proveru preciznosti algoritama za identifikaciju govornika preko telefonske linije. Za trening algoritma dozvoljeno je korišćenje različitih javnih ili privatnih baza govornika. Od trenutno objavljenih rezultata, najbolji algoritmi imaju EER od otprilike 3% na ovoj evaluaciji.

3.4 Biometrijski sistem

U opštem slučaju, biometrijski sistem se sastoji od sledećih modula [1]:

- Biometrijskog senzora
- Modula za ekstrakciju karakteristika
- Modula za poređenje
- Biometrijske baze podataka
- Modula za odlučivanje

Šematski prikaz modula i njihovih međusobnih zavisnosti dat je na slici 5. Biometrijski senzor zadužen je za digitalizaciju podataka kako bi mogla da se izvrši njihova dalja obrada. Neki od biometrijskih senzora su specijalizovani, kao na primer senzor za rad sa irisom oka, dok u drugim situacijama je moguća i upotreba hardvera koji ima opštu namenu. Primeri za ovaj drugi slučaj bili bi upotreba kamere ili mikrofona ugrađenog u laptop računar za potrebe biometrijske autentikacije.



Slika 5 – Šematski prikaz biometrijskog sistema [1]

Modul za ekstrakciju podataka na osnovu podataka dobijenih od biometrijskog senzora generiše biometrijski šablon za osobu čiji su biometrijski podaci prikupljeni pomoću senzora. Biometrijski šablon je zapravo vektor koji predstavlja reprezentaciju

određenog biometrijskog modaliteta. Ekstrakcija karakteristika u teoriji ima sličnosti sa ponašanjem heš funkcija u kriptografiji [14]. Slično kao kod idealne heš funkcije, dva različita ulaza u heš funkciju nikada ne bi trebali da daju isti izlaz. Međutim, pošto su u pitanju digitalizovani podaci, kao i usled različitih kvaliteta samih algoritama za ekstrakciju, verovatnoća kolizije prilikom ekstrakcije karakteristika zavisi od biometrijskog modaliteta, kao i korišćenog senzora i algoritma za ekstrakciju podataka.

Takođe, pod kolizijom možemo smatrati i situaciju kada su biometrijski šabloni različitih osoba dovoljno slični, da modul za poređenje ne može na jasan način da izvrši njihovu separaciju. Zadatak ovog modula je da vrši poređenje biometrijskih šablona i da kao rezultat vrati njihovu meru sličnosti, ili u slučaju metrike rastojanja, njihovu distancu. Ova mera sličnosti ili distance naziva se skor poređenja.

Distance dobijene iz modula poređenja koriste se za donošenje konačne odluke biometrijskog sistema. Biometrijski sistem može raditi u dva režima [1] [14]. To su režim verifikacije i režim identifikacije [1]. U slučaju režima verifikacije, logika je slična kao kod klasičnih metoda autentikacije. Korisnik se identifikuje pomoću svojih kredencijala, a biometrijski podaci prikupljeni putem akvizicije pomoću biometrijskog senzora se porede sa biometrijskim šablonom koji se nalazi u bazi podataka u okviru profila tog korisnika. Ukoliko je sličnost između šablona dovoljno velika, korisniku se odobrava pristup sistemu. Ukoliko nije, pristup sistemu mu je zabranjen.

Kod režima identifikacije ne koriste se kredencijali za identifikaciju. Biometrijski podaci osobe čiji identitet je potrebno utvrditi porede se sa šablonima u biometrijskoj bazi podataka. U zavisnosti od podešavanja sistema, moguće je poređenje sa šablonima svih osoba u bazi, ali pak samo do trenutka kada je sličnost između šablona veća od neke predefinisane granice.

Pojam granice, odnosno praga osetljivosti (eng. *threshold*) biometrijskog sistema bitan je za svaki biometrijski sistem. U zavisnosti od toga gde se postavi granica, biometrijski sistem će imati odgovarajuće performanse. Ukoliko je prag osetljivosti rigorozniji, manje su šanse da će sistem pogrešno prihvatiti ili identifikovati osobu. Međutim, veće su šanse da dođe i do takozvanog lažnog odbijanja identiteta, usled manje tolerancije na razlike između biometrijskih šablona. U slučaju kada je prag osetljivosti manje rigorozno definisan, tada je situacija obrnuta. Veće su šanse da sistem pogrešno prihvati ili identifikuje osobu, ali manje su i šanse da dođe do lažnog odbijanja identiteta.

4 MULTIMODALNA BIOMETRIJA

4.1 Prednosti i mane multibiometrijskog i multimodalnog pristupa

Iako biometrijski sistemi koji se oslanjaju na isključivo jedan modalitet imaju uspešnu primenu u praksi, unapređenje preciznosti i bezbednosti biometrijskog sistema, kao i smanjenje troškova implementacije sistema su ciljevi koji uvek predstavljaju izazov sa kojim se suočava projektant biometrijskog sistema.

Kao što je već pomenuto, biometrijski sistem je zapravo sistem za prepoznavanje šablona, koji donosi odluke koje su zasnovane na verovatnoćama [81]. Neki od standardnih izazova koji se javljaju kod biometrijskog prepoznavanja dati su u radu [82]:

- Šum u ulaznim podacima
- Varijacije unutar klase
- Jedinstvenost biometrijske karakteristike
- Problemi sa univerzalnošću biometrijske karakteristike
- Mogućnost prevare lažiranjem biometrijskih podataka
- Problemi vezani za interoperabilnost
- Ostali izazovi

Šum u ulaznim podacima može imati različite uzroke. U nekim situacijama, može biti posledica nepravilnog održavanja površina biometrijskih senzora, kao što je na primer akumulacija prašine i nečistoće na optičkom senzoru za akviziciju otiska prsta [83]. Drugi uzrok mogu biti izmene u biometrijskom modalitetu. U slučaju glasa kao biometrijskog modaliteta, uzrok bi mogla biti prehlada, dok bi kod hoda to mogla biti povreda noge. Pored ovih, do šuma u ulaznim podacima može doći i usled loših uslova u okruženju prilikom akvizicije.

Varijacije unutar klase se odnose na promene bilo samog biometrijskog modaliteta usled protoka vremena, ili na razlike u korišćenju samog biometrijskog senzora tokom različitih akvizicionih sesija od strane iste osobe. Poznato je da starenje utiče na preciznost prepoznavanja kod lica kao biometrijskog modaliteta [84].

Jedinstvenost biometrijske karakteristike može biti potencijalan problem ukoliko algoritam za ekstrakciju karakteristika nema dovoljnu diskriminativnu vrednost, ili pak ukoliko prilikom procesa digitalizacije na senzoru dolazi do gubitka informacija. Tada, usled ograničenja hardvera ili algoritama dolazi se do konačnog broja različitih hipotetičkih šablona, odnosno povećava se verovatnoća da dve različite osobe budu reprezentovane istom biometrijskom karakteristikom.

Problemi sa univerzalnošću biometrijske karakteristike vezani su za činjenicu da određene grupe osoba mogu iz različitih razloga imati lošiji kvalitet biometrijskih podataka kod određenog modaliteta, ili čak u ekstremnoj situaciji biti u nemogućnosti da zadovolje minimalan potreban kvalitet biometrijskih podataka neophodan za adekvatan rad sistema. Kod starijih osoba, česta je situacija da je kvalitet otiska prsta slabiji nego kod mlađe populacije [85].

Što se potencijalnih prevara vezanih za problem lažiranja biometrijskih podataka tiče, one predstavljaju veliki rizik za različite tipove biometrijskih sistema. Napadi variraju u karakteru od jednostavnijih koji zahtevaju minimalno tehničko znanje, do kompleksnijih koji zahtevaju specifičan hardver ili softver. Primer jednostavnog napada bi bio prikaz slike ili videa druge osobe kod lica kao biometrijskog modaliteta. Korišćenje specifičnog softvera za imitiranje glasa druge osobe [86], ili kreiranje lažnih otisaka prstiju [87], primeri su kompleksnijih napada. Veoma je značajno da biometrijski sistem bude zaštićen od napada lažiranjem biometrijskih podataka i za rešavanje ovog problema postoje različiti pristupi [88] [89].

Kada govorimo o interoperabilnosti u oblasti biometrije, fokus je na mogućnostima kooperacije biometrijskih sistema različitih proizvođača. U ovoj oblasti postoje određeni standardi, ali oni se često odnose na određeni aspekt biometrijskih sistema, a i njihova prihvaćenost u praksi je diskutabilna [5].

Jedan pravac rešavanja navedenih problema jeste dalje usavršavanje konkretnih unimodalnih biometrijskih sistema. Međutim, postoji i alternativni pravac kojim se značajan deo navedenih problema može rešiti, a to je primena multibiometrijskog pristupa i multimodalne biometrije.

Multibiometrijski pristup podrazumeva upotrebu više različitih izvora biometrijskih podataka. Po autorima rada [82], multibiometrijski sistemi se mogu klasifikovati na sledeće podtipove:

- Sistemi koji koriste više biometrijskih senzora
- Sistemi koji koriste više algoritama
- Sistemi koji koriste više različitih instanci jednog biometrijskog modaliteta
- Sistemi koji uzimaju više uzoraka jednog biometrijskog modaliteta
- Multimodalni sistemi
- Hibridni sistemi

Prva kategorija multibiometrijskih sistema se odnosi na upotrebu više različitih tipova biometrijskih senzora u okviru jednog sistema. Upotreba dodatnih senzora pruža dodatne podatke za dalju obradu, sa idejom da različiti senzori imaju komplementarnu ulogu. *Face ID* razvijen za upotrebu na pametnim telefonima kompanije Apple zasniva se na kombinaciji infracrvene fotografije lica i projektora tačaka koji očitava mapu emitovanih infracrvenih tačaka, na osnovu koje se formira trodimenzionalni prikaz lica [90]. Kombinacija ova dva tipa sirovih biometrijskih podataka predstavlja ulaz u dalju ekstrakciju karakteristika.

Sistemi koji koriste više algoritama upotrebljavaju više različitih biometrijskih algoritama za ekstrakciju karakteristika i poređenje. Na taj način, ukoliko se zna da algoritam ima slabosti u određenom slučaju korišćenja, taj nedostatak se može nadomestiti primenom drugog algoritma koji je u tom slučaju korišćenja bolji.

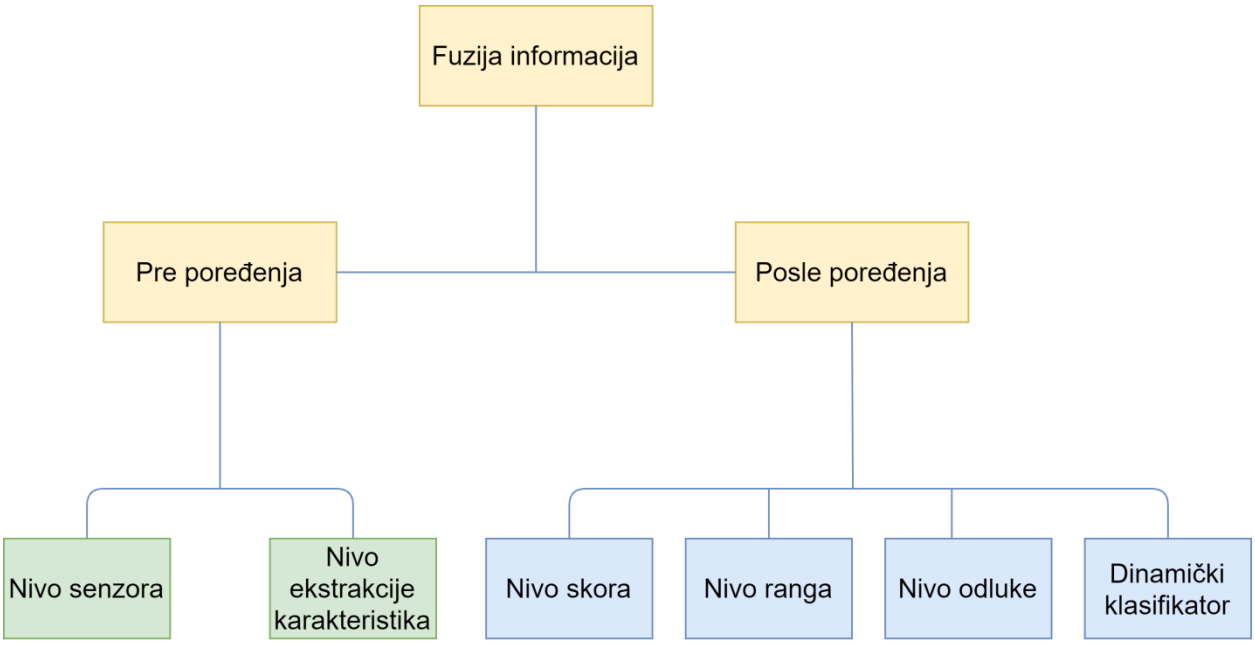
Sistemi koji koriste više instanci jednog biometrijskog modaliteta mogu se upotrebljavati u situacijama kada je biometrijski modalitet redundantan, kao što je slučaj kod otiska prsta, ili kod irisa. Jedan ovakav sistem bi mogao zahtevati upotrebu otiska kažiprsta obe ruke, ili irisa oba oka.

Multimodalni biometrijski sistemi uzimaju podatke od više različitih biometrijskih modaliteta. Moguće su različite kombinacije modaliteta, kao što su lice i glas, otisak prsta i otisak šake ili bilo koja druga kombinacija. Ideja je da se uvođenjem dodatnih modaliteta reše neki od navedenih potencijalnih problema biometrijskih sistema.

Poslednja kategorija data u podeli su takozvani hibridni sistemi. Ova kategorija sistema podrazumeva kombinovanje više prethodno navedenih pristupa. Na taj način se različiti benefiti koji svaki od pristupa pruža mogu iskoristiti prilikom projektovanja biometrijskog sistema.

4.2 Fuzija informacija u multimodalnoj biometriji

Za sve kategorije multibiometrijskih sistema, kako bi se mogli iskoristiti različiti izvori informacija, potrebno je definisati način na koji će se vršiti fuzija informacija. Izbor nivoa i konkretnog algoritma fuzije može imati značajan uticaj na performanse sistema [91]. Na slici 6 možemo videti šematski prikaz različitih nivoa na kojima se može vršiti fuzija informacija.



Slika 6 – Šematski prikaz različitih nivoa fuzije informacija [82]

U slučaju fuzije informacija na nivou senzora, podaci dobijeni na svakom od senzora formiraju celinu koja se dalje obrađuje od strane biometrijskog sistema. Fuziju na ovom nivou je smisleno moguće uraditi samo u okviru jednog biometrijskog modaliteta, tako da ovaj nivo fuzije suštinski spada u kategoriju multibiometrijskih sistema. Ipak, bitno ga je imati u vidu, pošto potencijalno može da poboljša preciznost sistema.

Drugi tip fuzije informacija koji je moguće izvršiti pre poređenja jeste fuzija na nivou ekstrakcije karakteristika. Ovde su mogući različiti pristupi za formiranje izvedene biometrijske karakteristike, od proste konkatenacije dobijenih vektora pojedinačnih modaliteta, preko kompleksnijih metoda fuzije informacija. Saini i Sinha u radu opisuju multimodalni biometrijski sistem baziran na GWT (eng. *Gabor-Wigner Transformation*) tranformaciji za ekstrakciju karakteristika i PSO (*eng. Particle Swarm Optimization*)

metodi za redukciju veličine vektora [92]. Korišćeni biometrijski modaliteti su lice i otisak šake, a baza za testiranje imala je 150 osoba. Autori u okviru rada porede uticaj različitih nivoa fuzije informacija na performanse sistema, a najbolji rezultat je dala hibridna šema, koja kombinuju skorove dobijene fuzijom na nivou ekstrakcije karakteristika sa skorovima unimodalnih sistema.

Kada je reč o fuziju na nivou skorova, različite biometrijske karakteristike se kreiraju za svaki od biometrijskih modaliteta. Svaka od karakteristika se poredi sa odgovarajućim šablonom u bazi biometrijskih podataka. Rezultat poređenja ovih karakteristika je skor poređenja. U slučaju skorova sličnosti, što je veći skor, to je veća verovatnoća da biometrijski podaci pripadaju istoj osobi. Generisani skorovi podataka se prilikom fuzije na ovom nivou koriste za kreiranje novog, izvedenog skora poređenja, ili u nekim situacijama za direktno donošenje odluke. Većina objavljenih radova vezanih za fuziju informacija vezana je za ovaj nivo fuzije.

Jedna od prvih evaluacija multimodalnih biometrijskih sistema na većem broju osoba sa upotrebom komercijalnih biometrijskih rešenja prikazana je u radu [93]. Prethodne dostupne evaluacije zasnivale su se na algoritmima razvijenim od strane istraživača, kao i na manjim bazama podataka. Testiranje je izvršeno nad bazom od 972 osobe. Otisak prsta i lice su korišćeni kao biometrijski modaliteti. Fuzija je izvršena na nivou poređenja skorova. Različite kombinacije tehnika normalizacije skorova i njihove fuzije prikazane su u radu. Najbolji rezultat je dala kombinacija težinskih skorova personalizovanih za pojedinačnog korisnika i adaptivne tehnike normalizacije sa EER vrednošću od 0.63%.

Sim, Asmuni, Hasan i Otman su razvili multimodalni sistem koji koristi iris i lice kao biometrijske modalitete [94]. Fokus ovog rada je bio na slikama koje nisu idealnog kvaliteta. Uzrok mogu biti ekstremni uglovi iz kojih je snimano lice, refleksija, promene izraza lica ili mutne slike. Fuzija informacija je izvršena na nivou skorova, i težinski faktori su prilagođeni za svakog korisnika sistema. Za testiranje sistema, autori su razvili sopstvenu UTMIFM (*University of Tecnology Malaysia Iris and Face Multimodal Datasets*) bazu. Za poređenje, takođe su koristili ORL bazu [95], kao i UBIRIS v2 bazu irisa [96]. Rezultati multimodalnog pristupa pokazuju GAR od 95% kada je vrednost FAR 0.01%, dok je kod irisa i lica za istu vrednost FAR metrike vrednost GAR-a oko 94% i 83% redom.

Tabela 2 – Uporedni prikaz preciznosti različitih multimodalnih biometrijskih sistema (EER kao parametar) [91]

Rad	Godina	Biometrijski modaliteti	Nivo fuzije	Broj identiteta u bazi	EER unimodalnog	EER multimodalnog
Snelick, Uludag, Mink, Indovina i Jain [93]	2005.	Otisak prsta i lice	Skorovi	972	2.16% 3.96%	0.63%
Sim, Asmun, Hassan i Othman [94]	2014.	Iris i lice	Skorovi	300	~7%, ~3%	~2%
Saini i Sinha [92]	2014.	Lice i otisak šake	Ekstrakcija karakteristika / skorovi	150	4,88%, 8,85%	1,65%
Monwar i Gavrilova [97]	2009.	Lice, uvo, potpis	Rangiranje	30	~5.6%, ~7.5% ~5%	1.12%

Ukoliko biometrijski sistem funkcioniše u identifikacionom modu, moguće je koristiti fuziju metodom rangiranja. Takav sistem za svaki modalitet formira listu najsličnijih identiteta kao izlaz. Prvi kandidat na listi je onaj koji je najsličniji, a ostali elementi liste sortirani su u opadajućem redosledu po njihovim skorovima sličnosti. Ovaj metod fuzije informacija primenjen je u radu [97].

Neki komercijalni unimodalni biometrijski sistemi rade kao "crne kutije", a njihov jedini izlaz je konačna odluka. Integracija takvih unimodalnih biometrijskih sistema u multimodalni biometrijski sistem zahteva upotrebu fuzije na nivou donošenja odluka. Fuzija na nivou donošenja odluka koristi različite algoritme za glasanje kako bi se donela konačna odluka. U radu [98] opisan je sistem koji koristi ovaj nivo fuzije informacija. Primenjeni algoritmi su AND i OR pravila, većinsko glasanje, većinsko glasanje sa težinskim faktorima i BKS (eng. *Behaviour-Knowledge Space*) metoda.

Pored unapređenja preciznosti, mehanizam fuzije informacija se može koristiti i za druge svrhe kao što je zaštita biometrijskih šablona [99]. Primenom IFO (eng. *indexing first one*) heš metode, pokušava se zaštititi biometrijska karakteristika. Cilj je da se omogući njeno eventualno povlačenje, spreči poređenje sa biometrijskim zapisima u drugoj bazi, kao i onemogući rekonstrukcija sirovog biometrijskog podataka na osnovu izvedene karakteristike. Fuzijom podataka na nivou ekstrakcije uz primenu specifične tehnike mapiranja vrednosti celih brojeva i upotrebu logičkog operatora ILI, dodaje se još jedan nivo zaštite biometrijskih karakteristika. Iako je preciznost sistema u ovom

slučaju niža nego kod klasične upotrebe irisa kao biometrijskog modaliteta, podignut je nivo zaštite biometrijskih šablona.

Tabela 3 – Uporedni prikaz preciznosti biometrijskih sistema (rangiranje kao parametar)

Rad	Godina	Biometrijski modaliteti	Nivo fuzije	Broj identiteta u bazi	Rang 1. preciznost
G. Goswami, P. Mittal, A. Majumdar, M. Vatsa and R. Singh [100]	2016.	Otisak prsta lice i iris	Nivo karakteristika	18000 (parcijalni podaci)	99,1%
M. Sultana, P. P. Paul and M. L. Gavrilova [101]	2017.	Lice, uho i ponašanje na društvenim mrežama	Nivo skorova	241	99,2%

U radu [100] prikazan je pristup koji koji pokušava da eliminiše potrebu za odvojenom fuzijom informacija na nivou karakteristika, a da pri tome iskoristi prednosti obavljanja tog zadatka na ovom nivou pre nego na nivou skorova, gde je sačuvana manja količina informacija o biometrijskim modalitetima. Za te potrebe razvijen je GSRC (eng. *Group Sparse Representation based Classifier*) algoritam, koji uklanja potrebu za posebnim algoritmima za ekstrakciju karakteristika i poređenje, a istovremeno i omogućava fuziju informacija i poređenje ne samo na osnovu više biometrijskih modaliteta, već i više različitih reprezentacija svakog od modaliteta. Izvršena je evaluacija nad dve biometrijske baze, od kojih jedna sadrži podatke 18000 osoba. Korišćeni modaliteti su otisak prsta, lice i iris. Pristup se pokazao nad ovim podacima bolji u odnosu na algoritme sa kojima je upoređivan, sa preciznoću identifikacije od 99,1% pri upotrebi sva tri biometrijska modaliteta na WVU bazi [48] i 62.3% na privatnoj bazi dobijenoj od bezbednosnih agencija. Takođe, čak i u slučaju kada podaci za neki od biometrijskih modaliteta nisu dostupni, bilo je moguće izvršiti identifikaciju u 61.8% slučajeva.

Istraživanje opisano u radu [101] je pored fizioloških biometrijskih modaliteta kao što su lice i uho, uključilo i podatke vezane za ponašanje na društvenim mrežama. Za prikupljanje informacija o društvenom ponašanju korišćena je mreža Tviter. Za evaluaciju podataka korišćeno je nekoliko javnih setova podataka. Fuzija informacija je izvšrena na nivou skorova. Kombinacija lica, uha i podataka prikupljenih sa društvenih mreža imala je preciznost identifikacije od 99,2% na kimeričkoj bazi dobijenoj pomoću kombinacije razlilčitih setova podataka. Rezultati istraživanja pokazuju da interakcije na društvenim mrežama mogu da pruže dovoljno informacija za unapređenje preciznosti identifikacije individue.

4.3 Primene multimodalne biometrije

Potencijal multimodalne biometrije privukao je pažnju kako istraživačke zajednice, tako i kompanija koja nude rešenja iz ove oblasti i različitih organizacija koja ova rešenja primenjuju za rešavanje sopstvenih problema. Konkretni modeli primene se razlikuju,

od opštijih kao što su kontrola pristupa određenoj lokaciji ili autentikacije za potrebe *web* aplikacija, do onih koji imaju užu primenu u konkretnoj oblasti. Primeri specijalizovanih slučajeva primene uključuju kontrolu pristupa automobilu, zaštitu sistema e-trgovine kao i zaštitu mobilnih uređaja [91]. Ostatak ovog poglavlja opisuje primene prikazane u radu [91], kao i dodatne identifikovane scenarije primene multimodalne biometrije.

Lupu je u radu [102] predložio kontrolu pristupa automobilu uz pomoć multimodalne biometrije. Sistem koristi tri biometrijska modaliteta, a to su otisak prsta, glas i iris. U slučaju validacije identiteta, korisniku se odobrava pristup upravljanju kolima. U suprotnom, ako uljez pokuša da preuzme identitet vlasnika automobila, ne bi mu bilo moguće da ih pokrene. Takođe, sistem bi obavestio policiju ili odgovarajuću bezbednosnu agenciju o lokaciji na kojoj je pokušana provala.

U radu Betija i ostalih [103] prikazana je upotreba sekvencijalne fuzije informacija u multimodalnom biometrijskom sistemu, bazirana na konceptu staze. Svrha testiranog sistema je bila kontrola pristupa određenoj lokaciji. Ovaj pristup specifično je dizajniran za zgrade koje imaju nekoliko kontrolnih tačaka na kojima se vrši provera identiteta. Kretanje korisnika kroz zgradu se prati i odluka sistema na svakoj od kontrolnih tačaka zavisi od rezultata prethodno izvršenih provera.

Dehnavi i Fard [104] predložili su upotrebu multimodalnog pristupa za praćenje studenata tokom nastave na daljinu. Predloženi model kombinuje dve bihejviorističke karakteristike (pokreti miša i dinamika kucanja na tastaturi), kao i jedan fiziološki (dvodimenzionalno lice). Ovakva kombinacija biometrijskih modaliteta omogućava kontinualno praćenje prisustva studenta. Za realizaciju ovog zadatka osmišljen je specijalizovan ACT (eng. *Attendance Control Tracker*) algoritam. Biometrijski podaci studenta se za potrebe ovog sistema konstantno prikupljaju i šalju na server. Prikazana je i detaljna arhitektura sistema. Testiranje je izvršeno na Claroline LMS (eng. *Learning Management System*) otvorenog koda [105], a autori naglašavaju da je ovaj pristup moguće koristiti i na bilo kom drugom sistemu za učenje na daljinu.

Trevin i ostali su testirali upotrebljivost (eng. *usability*) glasa, lica i prepoznavanja pokreta prilikom kontrole pristupa mobilnim uređajima. Za poređenje sa drugim metodama autentikacije, korišćeni su osmocifreni PIN kodovi u pisanom i glasovnom obliku. Kako autentikacija pravi prekid u toku razmišljanja korisnika, primarni fokus ove studije bio je uticaj autentikacije na radnu memoriju korisnika. Rezultati istraživanja su pokazali da svaki od modaliteta ima svoje prednosti i nedostatke. Glas se u ovom istraživanju pokazao manje upotrebljivim od preostalih testiranih modaliteta usled problema sa akvizicijom. U slučaju glasovne autentikacije, učesnici studije prijavili su određeno ometanje u procesu rada i pamćenja. Kombinacija lica i glasa takođe je rezultovala u većoj vrednosti FTA (eng. *Failure To Acquire*) greške, pošto proces akvizicije zahteva veću koordinaciju od strane korisnika.

Kompanija Aware nudi Knomi, okvir za autentikaciju na mobilnim uređajima [106]. Ovaj okvir se može koristiti za *onboarding* u različitim situacijama, uz integraciju sa sistemima za menadžment identiteta. Od modaliteta za biometrijsku autentikaciju u upotrebi su lice i glas. Prilikom registracije korisnika na sistem, vrši se poređenje slike lica prikupljene pomoću "selfija" sa slikom koja se nalazi na nekom od dokumenata kao što su lična karta ili pasoš. Uz pomoć primene specijalno treniranih algoritama, vrši se

provera da li prikupljena fotografija dolazi od stvarnog korisnika. Knomi je trenutno u upotrebi u nekoliko mobilnih aplikacija banaka iz Latinske Amerike [107].

Kompanija InCadence je u okviru saradnje sa američkim ministarstvom inostranih poslova (eng. *USA State Department*) razvila THOR (eng. *Tactical High-Threat Operational Response*) sistem [108]. Njegova namena je kontrola pristupa objektima ministarstva. Ovaj multimodalni biometrijski sistem omogućava akviziciju podataka lica, irisa i otiska prsta, kao i naknadnu identifikaciju lica na osnovu ovih biometrijskih modaliteta. Na osnovu prikupljenih biometrijskih podataka, moguće je poređenje sa vladinim bazama biometrijskih podataka, te provera tačnosti podataka i eventualne kriminalne pozadine osoba procesuiranih u okviru ovog sistema.

Još jedno rešenje za rad sa digitalnim identitetima koje koristi multimodalni biometrijski pristup jeste IdentityX razvijeno od strane kompanije DAON. U zavisnosti od odabranog režima rada (obrada biometrijskih podataka na serveru, uređaju ili u okviru same aplikacije na uređaju), dostupni su različiti biometrijski modaliteti. U studijama slučajeva koje su iznete za ovo rešenje najčešće korišćeni modaliteti su lice i glas. Neke od ogranizacija koje koriste ovo rešenje su USAA (eng. *United Services Automobile Association*) – organizacija koja se bavi osiguranjem, bankarstvom i finansijskim uslugama članovima američke vojske i njihovim članovima porodica, kao i Mox, virtuelna banka iz Hongkonga [109] [110]. Konretno, za USAA broj korisnika koji koristi funckionalnosti biometrijskog prepoznavanja iznosi preko jednog miliona [109].

Upotreba multimodalne biometrije za potrebe autentikacije glasača na izborima je još jedna primena ovog pristupa. Konkretno, u Keniji je korišćeno rešenje kompanije Idemia/Safran za autentikaciju glasača na šest značajnih izbora, između ostalog i na predsedničkim [111]. Od modaliteta korišćeni su otisak prsta i lice. Realizacija izbora izvršena je uz pomoć preko 45 000 tableta pripremljenih specijalno za ovu svrhu. Pored njihove upotrebe kao uređaja za akviziciju biometrijskih podataka, ovi uređaji zajedno sa pratećim softverom omogućavaju bezbedan prenos glasova, kao i praćenje izlaznosti na izborima. Ovaj projekat pratile su određene kontroverze, tačnije opozicioni kandidati su izneli tvrdnje da je sistem za glasanje bio neadekvatno obezbeđen, a izbori su poništeni od strane vrhovnog suda [112]. Ipak, možemo pretpostaviti da ove činjenice pre ukazuju na kompleksnost sprovođenja aktivnosti ovog tipa u nestabilnom okruženju, kao i važnost obuke operatera koji koriste tehnologiju, nego na same manjkavosti biometrijskog prepoznavanja prilikom rešavanja problema ovog tipa.

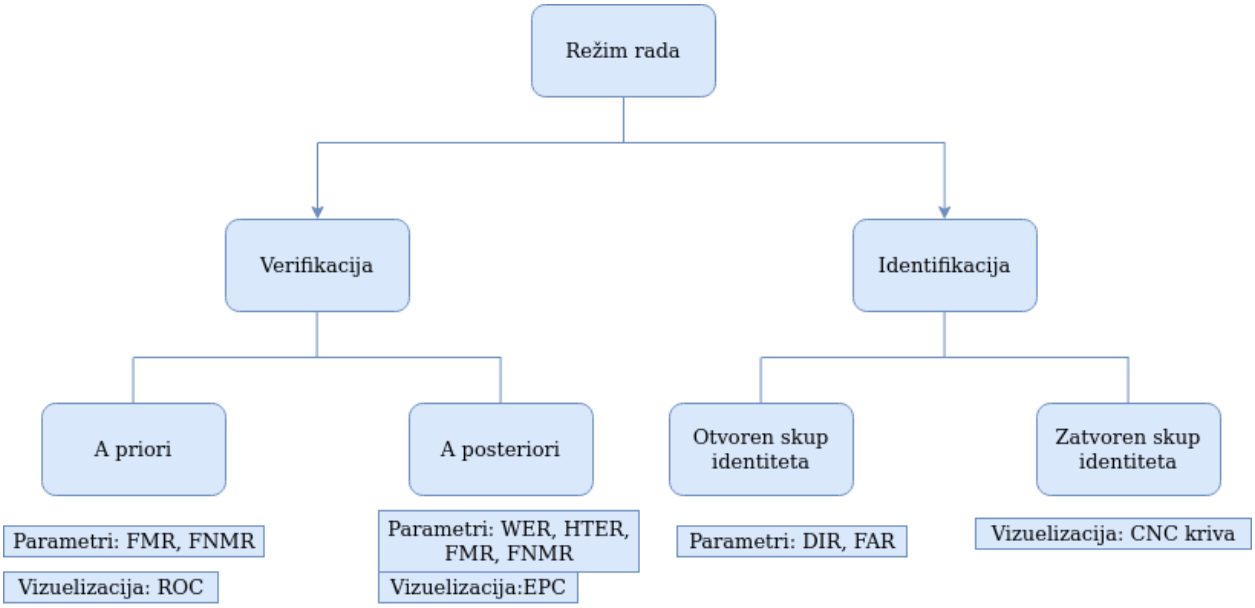
Na osnovu analize dostupne literature možemo zaključiti da iako su multimodalni sistemi ređe u upotrebi od svojih unimodalnih parnjaka, njihove mogućnosti primene su bile razmatrane kako od strane akademske zajednice, tako i implementirane u praksi od strane komercijalnih kompanija. Možemo primetiti trend upotrebe multimodalne biometrije u situacijama kada je potreban dodatni nivo bezbednosti i otpornosti na lažiranje biometrijskih podataka. Još jedan scenario gde je više modaliteta prisutno u upotrebi jeste u situacijama kada to doprinosi upotrebljivosti, pre nego preciznosti samog sistema. U ovim slučajevima, postoji ili izbor između biometrijskog modaliteta pomoću koga će biti izvršena autentikacija, ili sistem funkcioniše sekvencijalno, pa samo u određenim situacijama je potrebna upotreba više modaliteta.

5 EVALUACIJA BIOMETRIJSKIH SISTEMA

5.1 Parametri evaluacije biometrijskog sistema

Kada evaluiramo određeni biometrijski sistem, neophodno je da na određeni način kvantifikujemo rezultate izvršene evaluacije. S obzirom na činjenicu da je iz velike količine podataka u određenim situacijama lakše izvući zaključke ukoliko je dat grafički prikaz podataka, često je potrebno da dobijene rezultate evaluacije predstavimo i vizuelno.

Za potrebe evaluacije različitih aspekata biometrijskih sistema koriste se odgovarajuće metrike. Za različite režime rada biometrijskog sistema, moguće je koristiti parametre i vizuelizacije specifične za odgovarajući režim. U radu [113], data je klasifikacija metrika upravo po ovom kriterijumu (slika 7). Dalje, kada biometrijski sistem radi u režimu verifikacije, metrike i načine vizuelizacije moguće je klasifikovati na *a priori* i *a posteriori* pristupe. U slučaju pak rada sistema u režimu identifikacije, bitna karakteristika za dublju klasifikaciju metrika jeste činjenica da li sistem radi sa otvorenim ili zatvorenim skupom identiteta.



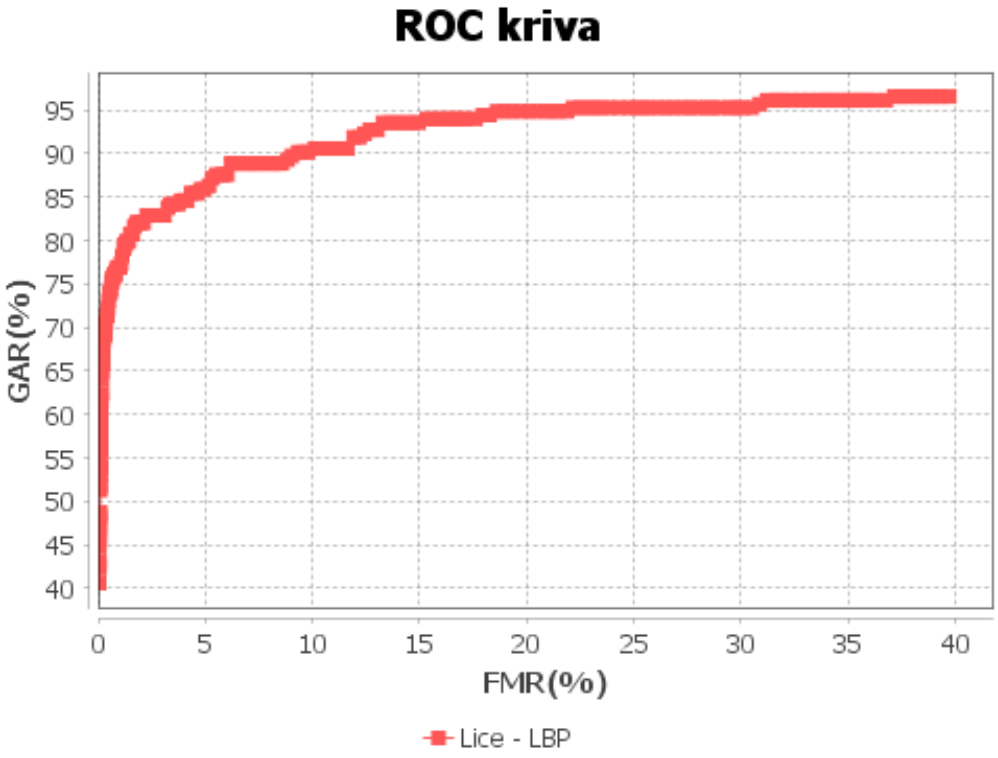
Slika 7 – Klasifikacija parametara evaluacije biometrijskih sistema po percepciji autora [113]

Fokus ove klasifikacije kao i većine istraživačkih radova u dostupnoj literaturi vezanoj za biometrijsko prepoznavanje jeste na određivanju preciznosti sistema. Ipak, pogotovu za potrebe konkretnih implementacija, mogu biti značajni i drugi parametri kao što su upotrebljivost ili brzina rada biometrijskog algoritma. U tehničkom izveštaju [114] možemo videti da je kao jedan od parametara sistema razmatran maksimalan moguć broj poređenja biometrijskih šablona u minuti, na određenoj hardverskoj konfiguraciji.

5.1.1 Parametri evaluacije biometrijskog sistema u verifikacionom modu

Jedan od prvih radova koji je pokušao da na jednom mestu sistematizuje parametre evaluacije koji su se koristili u praksi jeste rad Vajmana [115]. Vajman naglašava da se u okviru evaluacije biometrijskih sistema tradicionalno koriste pojmovi FAR (eng. *False Accept Rate*) i FRR (eng. *False Reject Rate*). FAR se odnosi na procenat transakcija sistema gde je greškom sistema prihvaćen uljez, odnosno pogrešan korisnik. FRR definiše procenat transakcija u kojima je pravi, legitimni korisnik odbijen, odnosno neprepoznat od strane biometrijskog sistema. U poređenju sa matematičkim pojmovima, FRR i FAR odgovaraju greškama prve i druge vrste prilikom evaluacije hipoteza.

U radu Vajmana [115] takođe su date matematičke definicije ROC (eng. *Receiver Operating Characteristic*) krive i parametara koji su na njoj prikazani. Bez ulaženja u detalje, ovde će biti iznet kratak opis suštine ove vizuelizacije. Prilikom opisa opštih karakteristika biometrijskog sistema, spomenuli smo pojam praga osetljivosti (eng. *threshold*). ROC kriva na svojim osama ima definisane iznose GAR (eng. *Genuine Acceptance Rate*) i FMR metrika. GAR metrika se dobija kao razlika jedinice i FRR metrike [1], a to je zapravo procenat prihvaćenih transakcija pravih korisnika. Svaka tačka na ROC dijagramu definiše odnos između FRR i GAR metrika za jednu konkretnu vrednost praga osetljivosti. Uvidom u ROC krivu možemo zaključiti kako određena vrednost praga osetljivosti ima uticaj na preciznost biometrijskog prepoznavanja posmatranog sistema. Primer ROC krive kreirane na osnovu rezultata iz kasnijeg istraživanja dat je na slici 8.



Slika 8 – ROC kriva koja prikazuje odnos GAR i FMR metrika

Vizuelizacija koja ima određene sličnosti sa ROC krivom jeste takozvana DET (eng. *Detection Rate Tradeoff*) kriva [113] [115] [116]. Razlika u odnosu na ROC krivu jeste što umesto GAR parametra, na njoj se direktno prikazuje FRR. Često se radi detaljnijeg uvida u odnos grešaka koristi logaritamska skala za predstavljanje rezultata na DET krivi.

Dok se ROC i DET krive klasifikuju u kategoriju *a priori* pristupa, EPC (eng. *Expected Performance Curve*) kriva [117] spada u *a posteriori* pristupe. Autori [117] predlažu ovaj tip vizuelizacije kao objektivniji od ROC i DET krivi. Za njegovu realizaciju neophodna je upotreba dva seta podataka, jednog za trening sistema, odnosno definisanje praga osetljivosti, a drugog za evaluaciju. Na EPC grafiku se prikazuju HTER (eng. *Half Total Error Rate*), kao i alfa vrednost. Ova alfa vrednost zapravo predstavlja parametar za minimalnu vrednost greške u zavisnosti od parametra alfa koji prioritizuje određen tip greške – FAR ili FRR.

Pored grafičkih vizuelizacija, koje pokušavaju da predstave više različitih kombinacija performansi na jednoj slici, u upotrebi su i čisto numerički parametri evaluacije, kao što je HTER pomenut u prethodnom pasusu. HTER vrednost se izračunava za konkretnu vrednost praga osetljivosti, a njena vrednost dobija se kao aritmetička sredina vrednosti FAR i FRR grešaka. Pored ovog parametra, u upotrebi je često i EER (eng. *Equal Error Rate*) metrika, koja označava vrednost na DET/ROC krivi gde su vrednosti ove dve greške jednake.

5.1.2 Parametri evaluacije biometrijskog sistema u identifikacionom modu

Kada razmatramo problem evaluacije biometrijskog sistema koji funkcioniše u režimu identifikacije, autori [113] razmatraju dva potencijalna scenarija. U prvom scenariju se identifikacija vrši u okviru zatvorenog skupa identiteta. Ovde se najčešće preciznost sistema prikazuje pomoću CMC kriva (eng. *Cumulative Match Characteristic*). Ova kriva pokazuje stopu identifikacije na određenom rangu prepoznavanja. U fiktivnom slučaju idealnog biometrijskog sistema, preciznost bi trebala da bude stopostotna na prvom rangu. Kako to uglavnom nije slučaj, uvidom u ovu krivu možemo zaključiti koliko sistem često greši u identifikaciji, odnosno pogrešno da prioritet lažnom identitetu prilikom identifikacije. Ovde je bitno primetiti da i broj subjekata u bazi utiče na preciznost na određenom rangu.

Kada je reč o sistemu sa otvorenim skupom identiteta, problem koji se zapravo rešava jeste utvđivanje sledeće činjenice - da li se osoba čiji se biometrijski podaci ispituju zapravo nalazi u određenoj bazi. Dve metrike koje se ovde koriste jesu DIR (eng. *Detection and Identification Rate*) i FAR (eng. *False Alarm Rate*).

DIR opisuje šansu da sistem prepozna osobu sa liste traženih osoba definisane pomoću biometrijskih podataka koji se nalaze u bazi. Sa druge strane, ukoliko sistem nije dovoljno precizan, ili je podešen da bude osetljiv, postoji mogućnost da osoba može greškom biti uparena sa nekim od identiteta iz baze. FAR (eng. *False Alarm Rate*) parametar opisuje verovatnoću nastanka greške ovog tipa. Kako ovaj tip greške može u praksi imati različite negativne posledice, poželjno je da vrednost FAR metrike bude što manja. Slično kao i kod FAR (eng. *False Accept Rate*) i FRR (eng. *False Reject Rate*) metrika, metrike DIR (eng. *Detection and Identification Rate*) i FAR (eng. *False Alarm*

Rate) su u međusobnoj zavisnosti. Davanje prioriteta jednoj od metrika može uticati na vrednost druge.

Pored ovih parametara, u radovima [113] [115] [116] pominju se i PR (eng. *Penetration rate*) i BER (eng. *Binning Error Rate*). Ovi parametri vezani su za eventualnu mogućnost particionisanja biometrijske baze za potrebe bržeg pretraživanja. PR se odnosi na prosečan procenat šablona u bazi podataka sa kojima je potrebno izvršiti poređenje prilikom identifikacije. Manja vrednost ovog parametra implicira da sistem efikasnije radi usled podele na veći broj particija, te da je pretraživanje efikasnije. Ipak, treba imati u vidu i BER parametar, koji označava mogućnost pretraživanja u pogrešnoj particiji. Visoka vrednost ovog parametra potencijalno ukazuje na činjenicu da broj particija prevazilazi sposobnost algoritma da efektivno obavlja particionisanje.

5.2 Biometrijska menažerija

U biometrijskim sistemima prilikom poređenja performansi sistema pri radu sa konkretnim osobama, često je moguće uočiti da performanse sistema zavise od konkretne osobe [118]. To znači da sistem pri radu sa određenim osobama može imati bolje performanse nego pri radu sa nekim drugim korisnicima sistema, kod kojih češće nastaju greške. U slučaju da je ova pojava prisutna, tačno utvrđivanje grupe osoba kod kojih se ova pojava manifestuje može biti veoma značajna. U literaturi koja se bavi ovom problematikom opisano je nekoliko opštih tipova korisnika, gde svaki tip karakteriše određeno specifično ponašanje.

Dodington je prvi u radu [3] svaki od ovih tipova korisnika označio pomoću konkretne životinjske vrste koja slikovito opisuje karakteristike grupe. Na taj način definisani su osnovni članovi biometrijske menažerije: ovce, koze, jagnjad i vukovi [3]. Eksperiment je sproveden nad podacima govornika iz *NIST Speaker Recognition Evaluation*-a [119] održanog 1998. godine. Za testiranje su korišćeni biometrijski podaci 500 osoba, sa podjednakom zastupljenošću osoba različitog pola. Svaka osoba imala je uzorke prikupljene u tri različita tipa okruženja, sa tri različite dužine uzorka, sa ukupno po 5000 uzoraka u svakom od tipova okruženja. Početna hipoteza bila je da ne postoje razlike između raspodela skorova poređenja pojedinaca. Kako bi ova hipoteza bila proverena, primenjeni su različiti standardni statistički testovi. Testovi su odbacili hipotezu da ne postoje razlike između pojedinačnih korisnika. Međutim, autori naglašavaju da postoji mogućnost da ovo nije činjenica specifičnosti biometrijskih karakteristika korisnika, već potencijalno drugih skrivenih uzroka, kao što su tip i karakteristike uređaja pomoću koga je vršena akvizicija podataka [3]. Takođe, ovaj rad se uglavnom bavi dokazivanjem postojanja biometrijske menažerije, a samo minimalno njenim uticajem na performanse sistema.

Po Dodingtonu, ovce predstavljaju dominantnu grupu korisnika biometrijskog sistema [3]. U proseku daju dobre rezultate prilikom poređenja sa sopstvenim biometrijskim podacima, a loše prilikom poređenja sa tuđima. Koze su osobe koje iz nekog razloga daju loše rezultate prilikom poređenja sa sopstvenim biometrijskim podacima. U slučaju primene neke metrike sličnosti, skorovi poređenja sa sopstvenim biometrijskim podacima za ovu grupu korisnika imaju nisku vrednost. Koze znatno i to neproporcionalno svojoj brojnosti doprinose FNMR metrici biometrijskog sistema.

Terminom jagnjad Dodington je označio osobe koje je lako oponašati [3]. Prilikom poređenja drugih osoba sa njihovim biometrijskim podacima, dobijaju se dobri rezultati, koji mogu dovesti do prihvatanja korisnika koji su se lažno predstavili sistemu. Jagnjad prouzrokuju znatan deo FMR greške biometrijskog sistema. Vukovi predstavljaju osobe koje su izuzetno uspešne u oponašanju drugih korisnika biometrijskog sistema. U slučaju lažnog predstavljanja imaju visoke skorove poređenja (ako je reč o metrici sličnosti). Takođe, nesrazmerno svojoj brojnosti doprinose FMR grešci celog sistema.

Nil Jeger (eng. *Neil Yager*) i Ted Dunston (eng. *Ted Dunstone*) predložili su proširenje koncepta biometrijske menažerije uvođenjem 4 nova tipa životinja [2]. Oni ukazuju na činjenicu da se članovi Dodingtonove menažerije definišu samo na osnovu skorova poređenja pravih (eng. *genuine*) korisnika ili pak uljeza (eng. *imposter*). Nedostatak ovakvog pristupa jeste previđanje međusobnog odnosa ova dva tipa skorova poređenja. Novi članovi biometrijske menažerije dodati u okviru ovog rada jesu crvi, kameleoni, fantomi i golubice.

Pripadnost jednoj od novih kategorija se definiše na osnovu raspodela skorova poređenja pravih korisnika i uljeza. Golubice karakterišu dobri rezultati poređenja sa sopstvenim biometrijskim karakteristikama, a slabi rezultati u slučaju poređenja sa tuđim. Kameleoni pak se definišu kao osobe koje daju dobra poređenja sa sopstvenim biometrijskim karakteristikama, ali i lako oponašaju tuđe. Fantomi imaju loše rezultate poređenja i sa sopstvenim i sa tuđim biometrijskim karakteristikama, dok crvi imaju loša poređenja sa sopstvenim biometrijskim karakteristikama, ali i mogućnost lakšeg oponašanja tuđih identiteta.

Istraživanje [120] koje su sproveli Teli i saradnici razmatra biometrijsku menažeriju i njenu zavisnost od algoritma prepoznavanja i uzorka podataka (u ovom slučaju slika lica) nad kojim se prepoznavanje vrši. Oslanja se na Dodingtonovu kategorizaciju biometrijske menažerije [3], kao i kategorizaciju koju su definisali Jeger i Danston [2]. Eksperiment je sproveden nad oba tipa menažerije. Autori eksperimenta između ostalog razmatraju tvrdnju da svrstavanje pojedinaca u okviru menažerije ne zavisi samo od karakteristika pojedinca već i od osvetljenja, podešavanja i drugih spoljnih faktora. Osnovna hipoteza je da postoje nivoi menažerije i ta tvrdnja se sprovodi nad oba tipa menažerija. Početni-nulti stepen menažerije po njihovoj definiciji uvek postoji. Ukoliko se prilikom eksperimenta nad dva različita seta podataka (dobijena korišćenjem istog biometrijskog sistema) iste osobe jave kao određene životinje iz menažerije, prisutna je menažerija prvog stepena.

Postojanje drugog stepena biometrijske menažerije takođe podrazumeva korišćenje dva seta podataka. Međutim, ovde je dodatni uslov da između setova postoji razlika u načinu pomoću koga je izvršena akvizicija podataka (npr. kod lica osvetljenje, ugao posmatranja). Ukoliko se „etikete“ životinja menažerije poklapaju i prilikom korišćenja različitih biometrijskih algoritama (nad istim setom podataka) tada je reč o biometrijskoj menažeriji trećeg stepena. Prilikom ispitivanja nad Dodingtonovom menažerijom, vukovi i jaganjci su posmatrani kao jedna kategorija zbog simetrije u ponašanju (jedni imitiraju, drugi su imitirani). Korišćeno je po 16 frontalnih slika lica prikupljenih pod različitim uslovima osvetljenja od strane 257 korisnika. Za rad sa slikama lica upotrebljena su dva algoritma koja su učestvovala u FRVT (eng. *Face vendor recognition test*) [121] evaluaciji.

Nakon sprovedene statističke evaluacije skorova poređenja, utvrđeno je postojanje Dodingtonove menažerije na nultom i prvom stepenu. U slučaju proširenja Dodingtonove menažerije od Jegera i Dunstona, nakon ispitivanja sprovedenog nad 257 pojedinaca i po 16 slika od svakog pojedinca nasumično podeljenih u dve particije, utvrđeno je postojanje novih kategorija životinja, ali samo na početnom, nultom stepenu.

Arun Ros sa saradnicima je sproveo istraživanje pod nazivom „Korišćenje fenomena Dodingtonove menažerije u biometrijskoj fuziji“ [122]. Cilj je bio dizajniranje multimodalnog biometrijskog sistema, koji bi koristio više biometrijskih modaliteta samo kod onih korisnika koji spadaju u neki tip životinja menažerije kod kojih su greške verovatne (koze, vukovi, jagnjad). Istraživanje se oslanja na Dodingtonovu kategorizaciju korisnika sistema i usvaja označavanje korisnika po njegovim principima, kao i na Pohove i Kitlerove *F-Ratio* proračune i klasterovanje korisnika u višestruke grupe na osnovu ovog kriterijuma (eng. *F-Ratio based approach*) [123]. Rezultati pokazuju unapređenje preciznosti poređenja u odnosu na podatke dobijene isključivo od jednog biometrijskog modaliteta. Prednost u odnosu na klasičan multibiometrijski pristup je ušteda vremena potrebnog za procesiranje biometrijskih podataka više modaliteta, kao i bolje korisničko iskustvo prilikom upotrebe sistema.

5.3 Otvorene baze biometrijskih podataka

5.3.1 Lice

Popularni set podataka za rad sa licem jeste *Extended Yale Face Database B* [124]. Ova baza sadrži 16128 slika prikupljenih od 28 različitih osoba. Svaka osoba slikana je u 9 različitih poza i pod 64 različita uslova osvetljenja.

Sledeća takođe veoma često korišćena baza jeste LFW – *Labeled Faces in the Wild* [125]. LFW kolekcija je objavljena kako bi se podstaklo istraživanje u ovoj oblasti. Nastala je kao ekstenzija seta fotografija prikupljenog na Berkliju imenovanog *Faces in the Wild* [126]. Ovaj set sadrži fotografije iz novinskih članaka, na kojima se nalaze lica u različitim pozama, sa raznovrsnim izrazima lica i uslovima osvetljenja pri slikanju. Iako popularna za eksperimente, *Faces in the Wild* baza nije bila pogodna za prepoznavanja lica jer je oko 10% slika u okviru baze bilo pogrešno označeno, a postojao je i određen broj duplikata slika. Usled zahteva akademske zajednice, ovaj set je ručno prečišćen i formulisani su evaluacioni protokoli za rad sa novonastalom kolekcijom podataka.

Slika 9 – Primer fotografija iz LFW baze [125]

U osnovnoj verziji ova baza je sadržala dva protokola za evaluaciju, protokol sa predefinisanim slikama i protokol za slobodnu evaluaciju. Protokol za slobodnu evaluaciju dozvoljava pravljenje novih parova slika iz baze radi kreiranja skorova poređenja. Kako su mnogi istraživači počeli da dodaju podatke van osnovnog LFW seta prilikom treniranja algoritama, došlo je do proširenja scenarija za evaluaciju. Protokoli koji su dodati u novom tehničkom rešenju LFW baze [125]:

- Slobodna evaluacija
- Evaluacija sa ograničenim slikama bez podataka van LFW baze
- Slobodna evaluacija unutar LFW baze
- Ograničena evaluacija sa upotrebom neoznačenih slika van LFW baze
- Neograničena evaluacija unutar baze sa upotrebom neoznačenih slika van LFW baze
- Neograničena evaluacija sa označenim slikama van LFW baze

Kao što se može videti sa slike 9, ova baza sadrži fotografije lica čije poze i uslovi u kojima su slikane značajno variraju. Od objavljivanja, veliki broj različitih radova citirao je ovu bazu kao reper za testiranje. Set sadrži više od 13000 slika lica prikupljenih na internetu. Svako lice je označeno sa imenom osobe kojoj pripada. Jedino ograničenje za ove slike jeste da su detektovane pomoću *Viola-Jones* algoritma [127].

Još jedna značajna baza jeste *CASIA WebFace* [128]. Iako je LFW baza dug period vremena predstavljala standard na osnovu koga su istraživači uspešno evaluirali preciznost svojih algoritama za prepoznavanje lica, javili su se određeni problemi. Sa primenom savršenijih algoritama, njihova preciznost je značajno porasla i dostigla nivo preciznosti između devedeset pet i devedeset devet procenata preciznosti. Pristupi koji su istraživači koristili bili su pre svega dubinsko modelovanje i modelovanje u širinu. Neke od varijacija LBP algoritma bile bi dobar primer modelovanja u širinu, dok duboke neuronske mreže, naprimer CNN (eng. *convolutional neural network*) spadaju u pristupe dubinskog modelovanja. Sa rastom snage računara, treniranje konvolutivnih neuronskih mreža više ne predstavlja teškoću, tako da je ovaj pristup dao najbolje rezultate pri rešavanju problema prepoznavanja lica. Upravo pri testiranju nad LFW bazom, najprecizniji su bili pristupi koji su koristili dodatne podatke pored onih koji su dostupni za trening u okviru LFW baze.

Kako bi nadomestili opisani problem, autori [128] su rešili da formiraju novu, veću bazu koja bi omogućila precizniju i dublju evaluaciju algoritama za prepoznavanje, pomoću

još većeg skupa podataka. Baza je formirana poluautomatski, a sadrži slike dostupne na internetu. Glavna teškoća prilikom prikupljanja slika sa interneta jeste činjenica da nije uvek lako utvrditi identitet osobe kojoj slika pripada. Autori su ovaj problem premostili posebnim pristupom klasterovanju podataka. Zapravo, pored formiranja baze, kao dodatni rezultati eksperimenta nastali su algoritam za prikupljanje i identifikovanje javno dostupnih slika lica na internetu, kao i neuronska mreža koja je upotrebljena za prepoznavanje lica, pošto je zbog obima seta podataka bilo neophodno automatizovati prepoznavanje. Kao izvor podataka korišćen je sajt IMDB, na kome se nalazi veliki broj fotografija poznatih osoba, sa pratećim metapodacima. Baza sadrži slike 10575 osoba koje imaju ukupno 494,414 slika. Metoda klasterovanja slika može se opisati pomoću sledećih koraka:

- Ekstrakcija karakteristika svakog lica pomoću odgovarajućeg algoritma
- U slučaju da se na slici nalazi veći broj poznatih ličnosti, vrši se nalaženje već postojeće pojedinačne fotografije svake od osoba koje se nalaze na slici
- Po prepoznavanju, obavlja se isecanje pojedinačnih lica sa slike i njihovo dodavanje bazi postojećih pojedinačnih lica
- Za preostale slike koje su prikupljene, potrebno je naći poklapanja između slika lica i identiteta poznatih ličnosti na osnovu skorova poređenja i tagovanih imena na IMDB stranici
- Isecanje lica i pamćenje u poseban folder za svaku osobu. Zatim se vrši ručna provera seta podataka i brišu pogrešno klasterovane slike

Majkrosoftova baza *MS-Celeb-1M* sadrži biometrijske podatke 100.000 poznatih ličnosti. Ukupno ima 10 miliona slika. Ovo je trenutno najveći javno dostupan set podataka. Međutim, nije filtriran, tako da sadrži i pogrešne labele, što može predstavljati problem prilikom treninga algoritma na ovoj bazi [129].

Autori navode tri glavna doprinosa svoga rada. Prvi je povezivanje slika sa entitetom u bazi znanja, pre nego izolovanim nizom karaktera koji sadrži samo ime i prezime. Na taj način se izbegavaju mogući nesporazumi prilikom prepoznavanja. Pošto je svakom entitetu u bazi pridružen bogat skup različitih informacija, ovaj pristup prepoznavanju bliži je onome koji koriste ljudi, a i lakše upotrebljiv u različitim vrstama realne primene.

Drugi doprinos je kreiranje evaluacionog scenarija velikog obima, kao i konstruisanje skupa parametara koji se koriste za evaluaciju. Za razliku od većine drugih evaluacionih scenarija za testiranje preciznosti prepoznavanja lica, slike osoba koje se koriste za ocenu preciznosti algoritma nisu javno objavljene. To znači da mogu biti bilo koje od 1 miliona osoba obuhvaćenih eksperimentom, čime se postiže manje varijacija između klasa. Postoje ljudi koji izgledaju veoma slično, ili su pak jednojajčani blizanci. Sa druge strane, isti ljudi mogu drugačije izgledati na različitim fotografijama, što sa rastom uzorka povećava varijaciju unutar klase.

Treći doprinos je veliki set podataka za trening algoritama. Ovaj set podataka se sastoji od slika prvih 100000 javnih ličnosti iz baze, na osnovu frekvencije učestanosti njihovog pojavljivanja. Iako postoji određen broj pogrešno označenih fotografija u ovom setu, sam obim seta značajno otežava njihovo ručno uklanjanje.

5.3.2 Glas

Kada je reč o glasu, dostupan je određeni broj setova podataka za javnu evaluaciju. Posebno je problem prepoznavanja govornika u realnim uslovima, bez ograničenja izgovorenog sadržaja, sa prisutnim šumom kao i sa različitim kvalitetom samog snimka izazov koji je aktuelan u istraživačkoj zajednici.

MIT je objavio bazu korišćenu za prepoznavanje govornika u realnim uslovima sa prisutnim šumom, prikupljenu sa mobilnih uređaja [130]. Ova baza je pre svega fokusirana na tekstualno zavisno prepoznavanje govornika. U okviru svake sesije, za svakog korisnika podaci su prikupljeni na tri različite lokacije, od kojih je svaka imala različit nivo pozadinske buke. Prednost ovakvog pristupa jeste u adaptaciji govornika na uslove okruženja, gde ukoliko je prisutna pozadinska buka, govornici prilagođavaju artikulaciju govora novonastaloj situaciji. Prethodno objavljeni setovi podataka uglavnom su problem pozadinskog šuma rešavali simulacijom šuma, što je za posledicu imalo previđanje ove uzročno posledične veze.

Jedna od javno dostupnih baza za evaluaciju jeste SITW (eng. *Speakers in the Wild*) set podataka [131]. Ovo je jedna od prvih otvorenih baza koja je dizajnirana za prepoznavanje govornika u realnim uslovima. Baza sadrži snimke prikupljene od 299 različitih osoba, sa prosekom od oko 8 različitih sesija po osobi. Neki od snimaka sadrže samo govor jedne osobe, dok je na nekima snimljeno više osoba. Razlikuju se i dužine snimaka, kao i karakter glasovnog zapisa koji je zabeležen (intervju, razgovor više osoba, monolog). Određene sesije snimljene su opremom specijalizovanom za ovaj zadatak, dok su u slučaju drugih za to korišćeni manje kvalitetitni uređaji kao što su mikrofoni na mobilnim telefonima. Autori navode da je i pored velikog broja baza koje su dotle bile navođene u okviru naučnih radova, ovo prvi set podataka koji sadrži podatke realnog karaktera sa odgovarajuće obeleženim snimcima.

Verovatno trenutno najobimnija javna baza govornika jeste *VoxCeleb* [132], otvorena baza podataka govornika, prikupljena sa javnih snimaka dostupnih na *YouTube* servisu. Baza sadrži podatke prikupljene od preko 6000 različitih osoba, sa više od milion glasovnih uzoraka ukupno. U radu [132] pored same baze, opisani su i različiti pristupi gde je ova baza korišćena za trening i evaluaciju različitih algoritama, kao i pokazano da upotreba ovakvo konstruisanog seta podataka pored mogućnosti evaluacije dodatno doprinosi samoj preciznosti algoritama za prepoznavanje govornika.

5.3.3 Otisak prsta

NIST (eng. *National Institute for Standardisation and Technology*) ima nekoliko dostupnih baza sa otiscima prstiju. Jedna od njih je *i NIST Special Database 302*, nastala kao rezultat *Nail to Nail fingerprint Capture Challenge* evaluacije [133]. Specifičnost ovog pristupa se ogleda u činjenici da otisci prstiju obuhvataju podatke prikupljene od jedne strane nokta do druge, te da je na taj način prikupljeno značajno više podataka za dalju obradu nego prostim pritiskom frontalnog dela jagodice prsta. Baza sadrži biometrijske podatke 331 osobe. Pored ovih specijalno prikupljenih otisaka, baza sadrži i otiske prikupljene pomoću klasičnih senzora, kao i poseban podskup latentnih otisaka prstiju.

Još jedna od javno dostupnih baza podataka otisaka prstiju jeste *Sokoto Coventry Fingerprint Dataset* [134]. Ova baza sadrži oko 6000 otisaka prstiju prikupljenih od strane preko 600 različitih osoba. Prvenstvena namena ove baze bila je za detekciju izmenjenih otisaka prstiju, gde su autori koristili kombinaciju originalnih i softverski izmenjenih otisaka prstiju. Za identifikaciju izmena u otiscima korišćena je konvolutivna neuronska mreža. Uspešnost modela objavljenog u radu [134] bila je 99,8% nad ovom bazom i podacima generisanim na osnovu nje.

5.3.4 Iris

CASIA baza je jedna od dostupnih baza za evaluaciju algoritama za prepoznavanje irisa. Postoji više verzija ove baze biometrijskih podataka, poslednja objavljena je *Casia-IrisV4* [135]. Ukupno u ovoj bazi se nalazi 54,607 slika irisa prikupljenih od strane 1800 pravih i 1000 virtuelnih osoba. Ova baza predstavlja ekstenziju podataka prikupljenih u prethodnim verzijama, a sadrži šest različitih podskupova podataka. Prvi podskup prikupljen je specijalno razvijenim senzorom za slikanje irisa iz blizine, i ovi podaci pogodni su za proučavanje detaljne teksture samog irisa. Drugi podskup odnosi se na podatke prikupljene pomoću ručnog senzora, gde su podaci prikupljani u dva režima, sa i bez veštačkog osvetljenja sa senzora. Treći podskup ima podatke irisa prikupljenih od blizanaca. Četvrti sadrži 20,000 slika irisa prikupljenih od 1000 ljudi pomoću senzora za akviziciju sa vizuelnim povratnim informacijama i to je bio prvi set ovog obima koji je bio javno dostupan. U okviru poslednjeg seta podataka nalaze se generisane slike irisa, koje čine podatke od takozvanih "virtuelnih" osoba koje smo pomenuli ranije u opisu baze.

Još jedan popularan set podataka je UBIRIS [96]. On sadrži slike irisa koje nisu idealnog kvaliteta i sadrže određenu količinu šuma. Ovako formiran set podataka služi za evaluaciju onih scenarija gde korisnik ne stavlja glavu na tačno određeno mesto i gleda u senzor, već se akvizicija podataka vrši tokom kretanja korisnika. Prednosti ovakvog pristupa jesu manja invanzivnost kao i izbegavanje dužeg zadržavanja korisnika za potrebe biometrijske autentikacije. Kvalitet slika irisa posebno utiče na performanse segmentacije ovog biometrijskog modaliteta. Baza sadrži 1877 slika irisa prikupljenih od 241 osobe, u okviru dve različite akvizicione sesije.

5.3.5 Multimodalne baze

Multimodalne baze biometrijskih podataka sadrže podatke o više modaliteta prikupljenih od jedne osobe. Jedna takva baza prikupljena je na Fakultetu organizacionih nauka [136]. Biometrijski podaci prikupljeni su od strane 39 osoba. Od biometrijskih modaliteta u bazi se nalaze lice, otisak prsta, uho, šaka i glas. Podaci su prikupljeni u dva kruga akvizicije.

Lice svake osobe u bazi je snimljeno iz 9 različitih pozicija, od frontalnog snimka do profila. Fotografije su snimane fotoaparatom od deset megapiksela, dok su video snimci lica zapamćeni u rezoluciji od 320X240 piskela sa 30 frejmova u sekundi. Otisak prsta je prikupljen pomoću dva senzora, optičkog i kapacitivnog. Uzimani su otisci kažiprsta i srednjeg prsta, na obe ruke, po četiri instance za svaki prst.

Prilikom akvizicije glasa, korisnici su imali tri sesije. U okviru prve sesije, čitali su nizove cifara. U drugoj sesiji čitali su tri slučajno izabrana PIN koda dužine od 4 cifre. U trećoj,

poslednjoj sesiji akvizicija je vršena čitanjem kraćeg, unapred zadatog teksta. Frekvencija uzorkovanja glasa iznosila je 44kHz i vršena je u stereo modu. Za akviziciju šake, korišćen je običan skener za dokumenta, kao i komad crne tkanine za prekrivanje šake i skenera prilikom skeniranja.

Na osnovu analize dostupne literature možemo zaključiti da su javno otvorene multimodalne baze biometrijskih podataka relativno malobrojne, kao i da sadrže ograničenu količinu podataka. Istraživači koji se bave problemima multimodalne biometrije stoga često pribegavaju formiranju takozvanih "kimeričkih" baza podataka. Ove baze se formiraju od više različitih unimodalnih biometrijskih modaliteta, gde postoji pretpostavka međusobne nezavisnosti podataka vezanih za pojedinačne modalitete.

NIST je publikovao multimodalnu bazu podataka prikupljenu na uzorku od pedeset i jedne osobe [137]. Prilikom procesa akvizicije simuliran je proces biometrijske autentikacije za pristup međunarodnom aerodromu. Od modaliteta korišćeni su otisak prsta, lice, iris. Za akviziciju otiska prsta korišćeno je 14 različitih skenera – optičkih, kapacitivnih i beskontaktnih. Za akviziciju lica korišćene su standardne optičke kao i termalne kamere. Za otiske prsta, u okviru pratećeg uputstva koje odgovara ovoj bazi, date su ocene kvaliteta otisaka prstiju.

6 OPTIMIZACIJA PRAGA OSETLJIVOSTI U MULTIMODALNOM BIOMETRIJSKOM SISTEMU

U slučaju procesa biometrijske verifikacije, algoritam za poređenje biometrijskih karakteristika donosi odluku na osnovu praga osetljivosti. Prag osetljivosti određuje koliko biometrijska karakteristika prikupljena akvizicijom sme da se razlikuje od biometrijske karakteristike koja je uskladištena u bazi podataka. Ukoliko se spusti prag osetljivosti, biće manje pogrešnih odbijanja, ali i više lažnih prihvatanja korisnika. Sa druge strane, ako povisimo prag osetljivosti, smanjićemo iznos FAR metrike, ali i pritom povećati FRR. Cilj projektanta sistema je da odredi prag osetljivosti sistema koji predstavlja dobar kompromis između sukobljenih ciljeva minimizacije obe pomenute metrike.

Ovde je bitno primetiti da multimodalni biometrijski sistemi mogu funkcionisati u paralelnom i serijskom (sekvencijalnom) režimu rada. Serijski režim rada predstavlja dobar kompromis između multimodalnih sistema u paralelnom režimu rada i klasičnih unimodalnih sistema [82].

Istraživanje Žanga [138] je kao rezultat imalo predlog novog okvira za serijske multimodalne biometrijske sisteme koji se zasniva na tehnikama delimično nadgledanog učenja. Autori su stavili akcenat na upotrebu manje preciznih ali prihvatljivijih biometrijskih modaliteta u odnosu na preciznije, ali manje prihvatljive za korisnike sistema. Ovaj pristup predstavlja alternativu prethodnim radovima koji su se fokusirali pre svega na performanse, redosled modaliteta i optimizaciju parametara algoritama, bez osvrta na uobičajene zahteve u primeni biometrije.

Marcijalis je sa kolegama [139] predložio teoretski okvir za ocenu performansi fuzije u serijskim multimodalnim biometrijskim sistemima, gde je razmotrio benefite u vidu performansi i ocenio greške u izračunavanju parametara modela. Model je analiziran sa strana njegovih prednosti i mana, i sprovedeni su preliminarni eksperimenti na osnovu otvorene baze biometrijskih skorova.

U radu [140] predložen je novi pristup određivanju gornjeg i donjeg praga osetlivosti u serijskom (sekvencijalnom) multimodalnom biometrijskom sistemu, na taj način da su očekivane mere FAR i FRR za ceo sistem minimizovane. U okviru ovog poglavlja biće izneti detalji pristupa opisanog u radu [140].

Posmatrani problem može se definisati na sledeći način. Pretpostavimo da multimodalni biometrijski sistem vrši seriju od N poređenja biometrijskih karakteristika prilikom verifikacije identiteta individue. Svako poređenje odnosi se na različit biometrijski modalitet.

Prilikom svakog od prvih $N-1$ poređenja, jedna od tri sledeće odluke biće doneta - prihvatanje identiteta kao pravog, odbijanje identiteta kao uljeza ili zahtev za još jednim poređenjem, upotrebom sledećeg biometrijskog modaliteta [140]. Ukoliko sistem za svako od prvih $N-1$ poređenja zahteva da dođe do još jednog poređenja, za poslednje N-to poređenje moguće su samo dve odluke biometrijskog sistema - prihvatanje ili odbijanje traženog identiteta.

Dalje, za svaki od modaliteta, prilikom testiranja sistema biometrijski podaci prikupljeni su od *n* osoba. Svaka osoba dala je *m* biometrijskih uzoraka. Na taj način dobijena je matrica *M* dimenzija *m* x *n*. Komponente matrice *M* su vektori biometrijskih karakteristika.

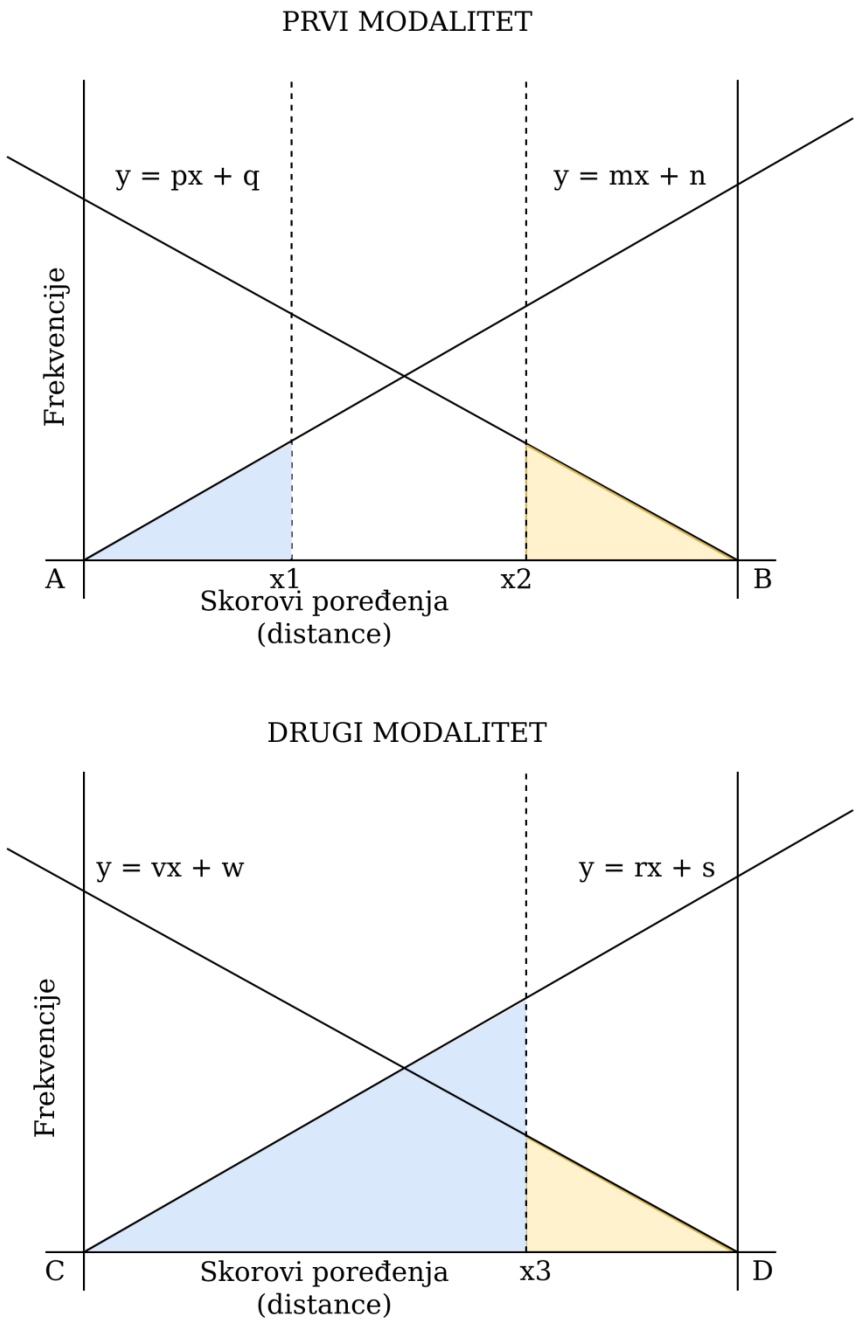
Za početak ograničićemo našu pažnju na prvih *N - 1* poređenja biometrijskih karakteristika. Upotrebom matrice *M* možemo izračunati distance između svaka dva prikupljena uzorka i odrediti raspodele skorova pravih identiteta i uljeza. Raspodela skorova pravih identiteta se dobija računanjem rastojanja između svaka dva elementa koja pripadaju istoj koloni matrice *M*. Raspodela skorova uljeza koristi rastojanja između svake komponente matrice *M* i ostalih elemenata matrice *M* koji ne pripadaju koloni u kojoj se nalazi element sa kojim vršimo poređenje.

Dva uzorka dobijena od iste osobe očekuju se da imaju manje rastojanje između njih u odnosu na rastojanje dobijeno poređenjem uzoraka različitih osoba [140]. Kao rezultat, raspodela skorova pravih korisnika imaće generalno niže vrednosti rastojanja (ili više vrednosti ako su u pitanju metrike sličnosti) u odnosu na raspodelu uljeza. Pošto je broj rastojanja izračunatih za formiranje raspodele pravih korisnika značajno manji od broja skorova dobijenih za raspodelu uljeza, oblik raspodele uljeza češće liči na normalnu raspodelu u odnosu na raspodelu skorova poređenja dobijenih od pravih korisnika.

Neka su sada *A* i *B* respektivno minimalno rastojanje u raspodeli uljeza i maksimalno rastojanje u raspodeli pravih skorova. Kada jedno od prvih *N - 1* poređenja u serijskom biometrijskom sistemu treba da donese odluku, to se vrši na osnovu dve granice $x1,x2 \in [A, B]$ na sledeći način: ukoliko je rastojanje između posmatranog biometrijskog uzorka i onog u bazi manje od *x1*, tada identitet osobe možemo prihvatiti kao pravi. Ukoliko je rastojanje između posmatranog uzorka i onog u bazi veće od *x2* tada odbijamo identitet kao uljeza. Međutim, ako se skor poređenja nalazi u nesigurnom intervalu [*x1*, *x2*], proces verifikacije zahteva poređenje biometrijskih podataka još jednog modaliteta.

Za poslednje poređenje u sekvenci, raspodele skorova pravih korisnika i uljeza formiraju se na isti način - dve vrednosti *C* i *D* se određuju, sa istom svrhom kao i *A* i *B* iz prvog poređenja. Razlika je u tome što se odluka donosi na osnovu treće granice *x3*, koja se nalazi između *C* i *D*. Ukoliko je skor poređenja manji od *x3* tada je identitet osobe nad kojim se vrši verifikacija potvrđen, u suprotnom ga odbacujemo kao uljeza.

Prilikom optimizacije praga osetljivosti multimodalnog biometrijskog sistema, glavni problem je kako odrediti odgovarajuće vrednosti za granice koje su date u sekvenci poređenja. Cilj je da se izvrši optimizacija vrednosti ove dve granice, kako bi se minimizovale vrednosti FRR i FAR.



Slika 10 – Uticaj granica *x1*, *x2* i *x3* na površine koje se koriste za izračunavanje vrednosti parametara FAR i FRR [140]

Rešavanje ovog problema najjednostavnije je predstaviti na primeru bimodalnog biometrijskog sistema. Prvi korak jeste evaluacija FAR i FRR u zavisnosti od vrednosti granica *x1*, *x2* i *x3*. Označimo sa *a(x1)* površinu ispod raspodele uljeza ograničenu sa desne strane vertikalnom linijom koja prolazi kroz *x1*, a sa *b(x2)* površinu ispod raspodele skorova pravih korisnika ograničenom sa leve strane vertikalnom linijom koja prolazi kroz *x2*. Slično, kod drugog biometrijskog modaliteta, *c(x3)* predstavlja površinu ispod raspodele uljeza ograničenom sa desne strane vertikalnom linijom koja prolazi kroz *x3*, a *d(x3)* označava oblast ispod raspodele pravih korisnika ograničenu sa leve strane vertikalnom linijom koja prolazi kroz *x3*.

Verovatnoća za grešku pogrešnog prepoznavanja (eng. *false match*) kod prvog biometrijskog modaliteta odgovara *a(x1)*, a kod drugog modaliteta *c(x3)*. Slično, verovatnoća pogrešnog odbijanja (eng. *false non-match*) je za prvi modalitet *b(x2)*, a za drugi modalitet je *d(x3)*. Na osnovu ovoga možemo zaključiti da su verovatnoće greške pogrešnog prepoznavanja i pogrešnog odbijanja kod kombinacije oba modaliteta redom [140] :

$$a(x1) + [a(x2) - a(x1)] \times c(x3)$$

$$b(x2) + [b(x1) - b(x2)] \times d(x3)$$

Kako bi se odredile odgovarajuće granice nesigurnog intervala u procesu verifikacije, potrebno je izvršiti minimizaciju verovatnoće nastanka greške. Pošto nizak FAR označava visok FRR i obrnuto, potrebno je naći dobar kompromis između ova dva tipa greške. Ovaj kompromis se postiže rešavanjem sledećeg problema višeciljnog programiranja [140]:

$$\min \quad a(x1) + [a(x2) - a(x1)] \times c(x3)$$

$$\min \quad b(x2) + [b(x1) - b(x2)] \times d(x3)$$

$$s.t. A \leq x1 \leq x2 \leq B, C \leq x3 \leq D$$

Radi izračunavanja verovatnoća predstavljenih u formulama, potrebno je aproksimirati raspodele skorova pravih korisnika i uljeza. Ovaj zadak je moguće rešiti primenom metode najmanjih kvadrata [140], ili pak upotrebom metode aproksimacije raspodele u odnosu na poznate raspodele [141]. Za drugi pristup je potrebno upotrebiti neki od statističkih testova kako bi se proverilo uklapanje prikupljenih podataka sa različitim modelima raspodela. U daljim eksperimentima u okviru ove disertacije korišćena je metoda najmanjih kvadrata.

Gornji deo slike 10 predstavlja površine koje smo koristili za izračunavanje FAR (plavo) i FRR (oker) na prvih *N - 1* poređenja. Donji deo slike 10 takođe predstavlja te površine, ali na poslednjem korišćenom modalitetu. Na ovoj slici možemo videti i grafički prikaz granica.

Kod prvog modaliteta, kao šta je prikazano na slici 10, sa *f1(x)* i *g1(x)* predstavićemo linearne izraze *mx + n* i *px +q*. Za drugi modalitet sa *f2(x)* i *g2(x)* označićemo izraze, *rx+s* and *vx + w*. Presekom pravih *f1(x)*, *g1(x)*, *f2(x)* i *g2(x)* sa horizontalnom osom dobijaju se tačke $A = -n/m$, $B = -q/p$, $C = -s/r$, i $D = -w/v$ [140]. Pomoću ovih vrednosti možemo aproksimirati FAR i FRR za svaki modalitet kao [140]:

$$a(x1) = (m \times x1 + n)^2/2m$$

$$b(x2) = -(p \times x2 + q)^2/2p$$

$$c(x3) = (r \times x3 + s)^2/2r$$

$$d(x3) = -(v \times x3 + w)^2/2v$$

Ovo su kvadratne jednačine koje zavise od vrednosti granica *x1*, *x2* i *x3*,. Njihovom kombinacijom dobijamo polinom četvrtog stepena za prikazane funkcije. Za multimodalni sistem, ovi izrazi postaju polinomi stepena *2N*.

Pomoću ovih transformacija, generalni problem optimizacije postaje konkretan problem sa dva cilja, lak za rešavanje primenom standardnih paketa za nelinearno programiranje. Jedan od načina za rešavanje dvokriterijumskog cilja jeste agregacija dve funkcije cilja i optimizacija dobijene funkcije [140]. Za agregaciju ciljeva možemo koristiti težinske faktore. Ukoliko su inicijalne vrednosti težinskih faktora (1,1) tada se ne vrši favorizovanje ni jednog od tipova greški.

6.1 Određivanje praga osetljivosti nad NIST-BSSR1 bazom skorova poređenja

Kako bi se evaluirale performanse predložene metode određivanja praga osetljivosti multimodalnog biometrijskog sistema, upotrebljena je NIST BSSR1 multimodalna baza [142]. Ova baza sadrži tri seta podataka. U okviru ostatka ovog potpoglavlja biće opisani eksperimenti predstavljeni u radu [140] koji su vršeni nad prva dva seta.

NIST BSSR1 (Set 1) baza sadrži skorove generisane poređenjem biometrijskih podataka 517 korisnika. Za svakog korisnika, baza sadrži po jedan set skorova poređenja dva otiska desnog kažiprsta, jedan skor poređenja dva otiska levog kažiprsta i dva seta skorova poređenja dve frontalne slike lica dobijena primenom dva različita rešenja za prepoznavanje osobe na osnovu lica. Setovi skorova lica označeni su labelama “C” i “G”. Skorovi poređenja levog i desnog kažiprsta označeni su sa “Li” i “Ri”. Svaki set poređenja sadrži 517 skorova poređenja podataka koje pripadaju istoj osobi (eng. *genuine*) i 266,772 (516x517) skorova “uljeza” (eng. *imposter*). Za potrebe evaluacije pristupa skorovi sličnosti iz ove baze pretvoreni su u distance.

Kao deo eksperimenta izračunate su optimizovane granice za bimodalni sistem razvijen nad modalitetima BSSR1 biometrijske baze, gde je razmotreno svih 12 mogućih kombinacija različitih rešenja i instanci ova dva modaliteta. U tabeli 4 prikazani su FAR, GAR i TER (eng. *Total error rate*) kod optimizovanih granica sistema.

NIST BSSR1 (Set 2) baza sadrži skorove poređenja dobijene od 6000 korisnika. Za svakog korisnika, baza sadrži jedan set skorova dobijen poređenjem dva desna kažiprsta i jedan set skorova poređenja dva leva kažiprsta. Setovi skorova dobijenih od levog i desnog kažiprsta označeni su sa “Li” i “Ri”. Svaki set poređenja sadrži 6000 skorova poređenja podataka koje pripadaju istoj osobi (eng. *genuine*) i 35,994,000 (5999 × 6000) skorova uljeza (eng. *imposter*). Kao i za NIST BSSR1 (Set 1) bazu, skorovi sličnosti su konvertovani u distance, optimalne granice sistema su određene i ispitane moguće kombinacije modaliteta, instanci modaliteta i rešenja. U tabeli 5 prikazane su FAR, GAR i TER vrednosti za optimizovane granice sistema.

Tabela 4 – FAR, GAR i TER vrednosti za biomodalni sistem pri evaluaciji nad NIST-BSSR1 (Set 1) [140]

1. modalitet	2. modalitet	FAR	GAR	TER
C	G	1.89%	91.88%	10%
G	C	0.21%	85.48%	14.7%
Li	Ri	0.15%	94.59%	5.57%
Ri	Li	0.11%	93.82%	6.3%
Li	C	0.20%	97.3%	2.90%
C	Ri	0.5%	97.68%	2.82%
Ri	C	0.14%	97.88%	2.28%
G	Li	0.42%	98.07%	2.4%
Li	G	0.5%	98.26%	2.24%
G	Ri	0.27%	96.65%	1.62%
Ri	G	0.26%	98.65%	1.61%

Tabela 5 – FAR, GAR i TER vrednosti za biomodalni sistem pri evaluaciji nad NIST-BSSR1 (Set 2) [140]

1. modalitet	2. modalitet	FAR	GAR	TER
Li	Ri	0.96%	95.87%	5.09%
Ri	Li	1.55%	96.12%	5.4%

Brojni radovi referencirali su ovaj set skorova [143] [144] [145] [146]. Prilikom poređenja rezultata, javila su se dva glavna izazova. Prvi je da ne postoji konzistentan način rada nad ovom bazom. Na primer, neki od istraživača na slučajan način formiraju setove za trening i evaluaciju. U tom slučaju nije moguće ponoviti njihove eksperimente. Neki istraživači odbacuju određene skorove usled potencijalnih grešaka prilikom akvizicije, ali ne naglašavaju koje skorove iz baze su odbacili [145]. Drugi problem se odnosi na činjenicu da nije moguće direktno uporediti set granica određen optimizacijom i ROC krive koje predstavljaju standardan način za prikazivanje rezultata istraživanja biometrijskih algoritama.

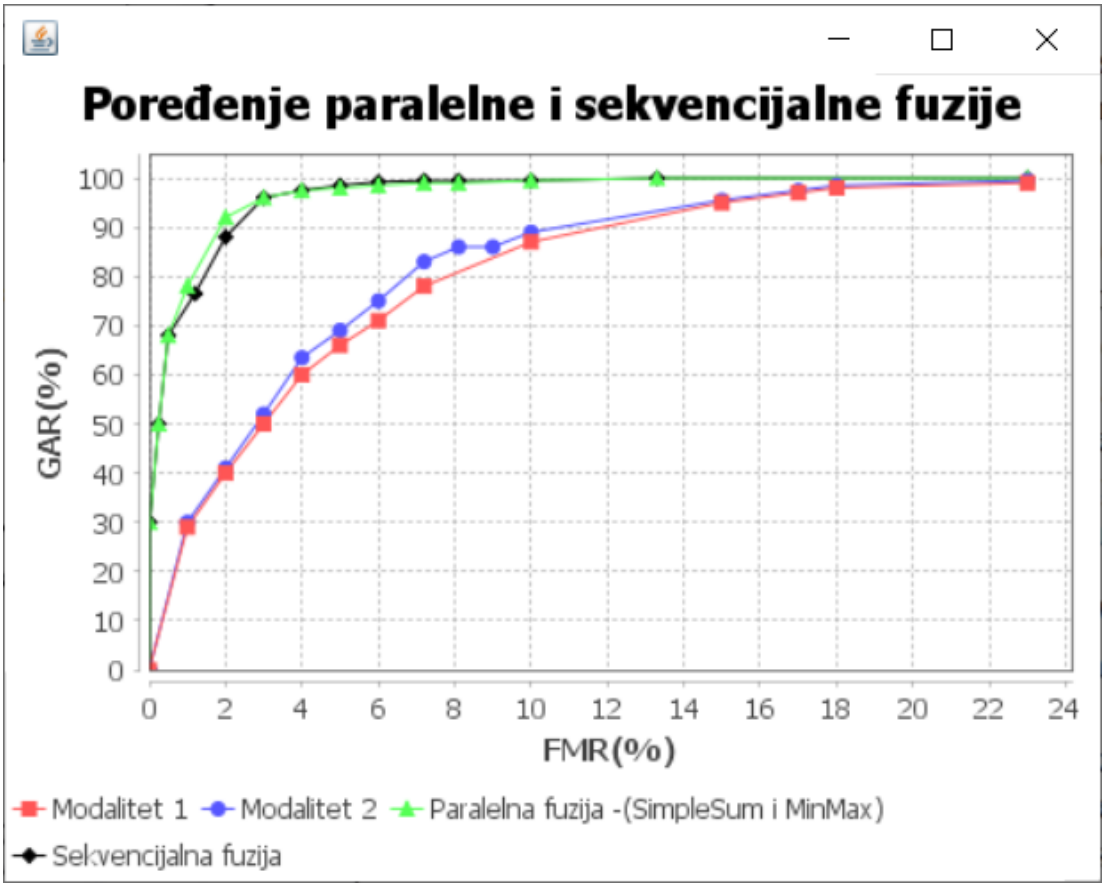
6.2 Određivanje praga osetljivosti nad generisanom bazom skorova poređenja

Kao što je opisano u radu [140], ovaj eksperiment je organizovan na sledeći način. Kao prvo, ulazni podaci neophodni za dobijanje raspodela skorova generisani su na slučajan način u skladu sa pravilima koja ih modeluju na osnovu realnih biometrijskih podataka. Generisani vektori simuliraju ključne informacije koje bi u realnom scenariju bile prikupljene od osobe tokom faze akvizicije biometrijskih podataka.

Prvi uzorak od svakog korisnika generisan je kao vektor slučajnih brojeva sa uniformnom raspodelom [140]. Srednja vrednost i standardna devijacija menjani su kroz instance. Svaki sledeći uzorak koji je generisan za tog korisnika kreiran je kao vektor slučajnih brojeva sa normalnom raspodelom, uz zadržavanje iste srednje vrednosti i varijanse kao odgovarajući prvi uzorak. Na taj način obezbeđeno je da su uzorci dobijeni od iste osobe sličniji jedan drugom prilikom poređenja u odnosu na ostale uzorke.

Nakon toga, urađeno je poređenje euklidskih rastojanja svaka dva generisana vektora. Skorovi poređenja podeljeni su u dve kategorije radi formiranja raspodela skorova pravih korisnika i uljeza. Izvršena je linearizacija izraza kako bi se evaluirale greške pogrešnog prihvatanja i pogrešnog odbijanja, a zatim i napravili višekriterijumski optimizacioni modeli. Svaki triplet (*x1, x2, x3*) optimizovanih granica definiše bimodalni biometrijski sistem, čije će performanse biti evaluirane [140].

Kako bi se odredile FAR i FRR vrednosti svakog sistema upotrebom istih podataka kao za formiranje raspodela skorova pravih korisnika i uljeza, redom prikupljamo odgovore sistema, dobijene kada svaka osoba sa identitetom $i = 1, \ldots, n$ pokuša da se verifikuje kao osoba $k = 1, \ldots, n$, a sve to pomoću biometrijskih uzoraka $j = 1, \ldots, m$ osobe sa oznakom k i optimizovanim granicama sistema. Svaki put kada sistem prihvati osobu i kao osobu k, brojilac za izračunavanje FAR se povećava za jedan. Tako da svaki put kada sistem odbije osobu koja se prijavila sa svojim identitetom, brojilac za FRR se povećava za jedan. Imenilac za FAR je $n(n-1)m^2$, dok za FRR imenilac razlomka ima vrednost $m(m-1)n/2$ [140].



Slika 11 – Poređenje preciznosti sistema baziranog na optimizaciji u odnosu na standardni paralelni pristup [140]

Rezultati nekoliko instanci eksperimenta prikazani su u tabeli 6. Za sve eksperimente par (FAR, GAR) dobijen metodom optimizacije granica daje bolje rezultate u odnosu na bar jedan par (FAR, GAR) iz seta finalnih rezultata dobijenih standardnim metodama fuzije. Ova činjenica ukazuje na uporedivost performansi sekvencijalnih multimodalnih sistema sa optimizacijom granica u poređenju sa standardnim paralelnim pristupom multimodalnoj fuziji. Paralelni prikaz preciznosti za jednu od instanci prikazan je na slici 11.

Tabela 6 – FAR, GAR i TER vrednosti za biomodalni sistem pri evaluaciji nad generisanim podacima [140]

Karakteristike instance	FAR	GAR	TER
n = 100, m = 5, l = 3	9.4%	99.6%	9.8%
n = 100, m = 5, l = 5	2.2%	100%	2.2%
n = 100, m = 5, l = 10	0.05%	99.2%	0.85%
n = 200, m = 5, l = 10	0.001%	99.5%	0.501%

7 OBJEDINJENI MODEL ZA EVALUACIJU MULTIMODALNIH BIOMETRIJSKIH SISTEMA

7.1 Evaluacija multimodalnih biometrijskih sistema i MDA pristup

Kako bi se evaluacija mulitimodalnog biometrijskog sistema izvršila na adekvatan način, potrebno je na odgovarajući način definisati koncepte koje neko ko modeluje sistem može upotrebiti za izradu modela. Poželjno je da ovi koncepti budu definisani odvojeno od tehnologije implementacije, kako bi rešenje problema bilo pre svega u okviru njegovog domena. Pristup evaluacije multimodalnog biometrijskog sistema koji je ovde primenjen zasnovan je na MDA (eng. *Model Driven Architecture*) paradigmi. Glavna prednost ovog pristupa jeste sposobnost da primenom hijerarhijski organizovanih modela smanji kompleksnost modelovanja velikih sistema, kao i olakša interakciju i kolaboraciju između organizacija, ljudi, hardvera i softvera [147]. Način na koji to ova paradigma radi jeste definisanjem strukture, semantike i notacija modela primenom industrijskih standarda.

Ideja iza arhitekture vođene modelom jeste da razvoj rešenja počinje definicijom platformski nezavisnih modela zasnovanih na zahtevima i specifičnosti domena za koje se rešenje razvija [148]. Ovi modeli se opisuju pomoću jezika za modelovanje zasnovanog na MOF (*Meta Object Facility*) standardu/jeziku [149]. Jezik ovog tipa upravo jeste UML (*Unified Modelling Language*).

UML modeli se kasnije odgovarajućim transformacijama mogu pretvoriti u platformski specifične modele, koji pak se mogu transformisati u odgovarajuće implementacije. Ideja jeste da se olakša proces razvoja softvera definisanjem stabilnog modela koji neće biti podložan čestim promenama, dok se implementacijom odgovarajućih transformacija može prebaciti u konkretnu platformski zavisnu implementaciju.

Generalno, pre nego što se UML (*Unified Modelling Language*) jezik pojavio, među grafičkim jezicima za modelovanje situacija je bila prilično neuređena. Različiti eksperti iz oblasti forsirali su raznovrsne, često međusobno nekompatibilne notacije. Alati na raspolaganju bili su ograničenih mogućnosti, pogotovu za proveru konzistentnosti modela ili transformaciju grafičke reprezentacije u programski kod [150].

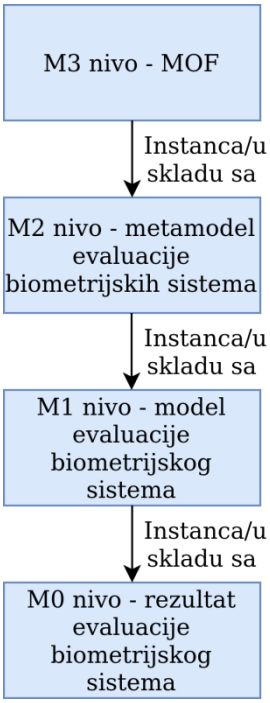
Situacija u ovoj oblasti značajno se poboljšala definisanjem UML standarda, usvojenim od strane OMG grupe (*Object Management Group*). UML je jezik za modelovanje opšte namene u oblasti softverskog inženjerstva, čija je svrha da pruži standardizovan način prikaza dizajna softverskog sistema [151]. Ipak primene UML jezika nisu isključivo moguće samo u ovoj oblasti.

MDA pristup opisuje sledeće nivoe u hijerarhiji modela [152]. Redom, to su M3 nivo odnosno nivo metametamodela, M2 nivo – nivo metamodela, M1 nivo – nivo modela i M0 nivo, nivo instance sistema. Svaki od nivoa predstavlja instancu nivoa koji se nalazi iznad njega. Stoga, svaki od nivoa mora biti u skladu sa pravilima i logikom definisanim u nivou roditelja.

M3 nivo predstavlja nivo metametamodela. Ovaj nivo se nalazi u osnovi hijerarhije. Njegova glavna svrha jeste da definiše jezik za definiciju metamodela. Primer metametamodela jeste MOF (*Meta Object Facility*) jezik. MOF specifikacija predstavlja osnovu za definiciju metamodela u OMG familiji jezika za modelovanje i bazirana je na pojednostavljenoj varijaciji verzije 2 UML jezika za rad sa klasama [152]. Pored definisanja osnova metamodela, dodaje i mogućnosti za modelovanje primenom identifikatora, tagova i refleksivnih operacija koje su generičke i mogu biti primenjene nezavisno od metamodela.

M2 nivo metamodela služi za definisanje jezika za specifikaciju modela. Metamodel se bazira na metapodacima. Metapodaci su zapravo podaci o podacima. Jedan primer metapodataka jeste šema relacione baze podataka. Ona sadrži podatke o tabelama i atributima koji čine bazu podataka. Kada ovo primenimo na metamodele, možemo reći da ovaj nivo služi kao model za konkretne modele koji se razvijaju za različite aplikacije.

M1 nivo predstavlja nivo modela, odnosno koncepte specifične za određenu aplikaciju. M0 nivo predstavlja konkretnu instancu koncepta opisanog na M1 nivou.



Slika 12 – Preslikavanje okvira za evaluaciju multimodalnih biometrijskih sistema na OMG MDA pristup sa 4 nivoa [153]

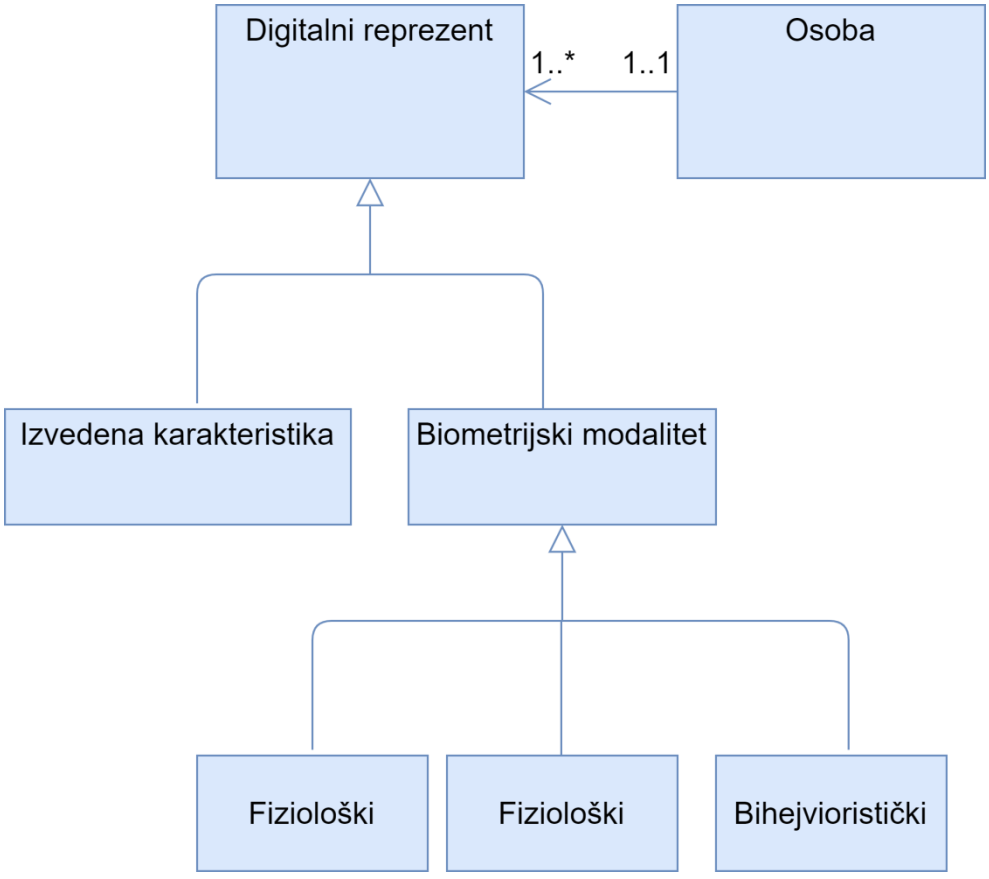
Primena modelom vođenog pristupa na evaluaciju multimodalnih biometrijskih sistema prikazana je na slici 12. Na M3 nivou koristi se MOF standard, pomoću koga je opisan apstraktni jezik za definiciju metamodela. Za grafičku reprezentaciju prikazanih modela koristi se UML. Na taj način je upotrebom ovog standardnog jezika koji je svakako definisan pomoću MOF-a i sadrži njegove funkcionalnosti olakšano predstavljanje definisanih modela. Na M2 nivou definisan je metamodel evaluacije biometrijskih sistema, koji predstavlja svojevrsnu ontologiju pojmova značajnih za ovu oblast. Primenom ovog metamodela, moguće je kreirati modele evaluacije različitih biometrijskih sistema. To odgovara nivou M1 definisanom u modelu vođenim pristupom. Konkretne evaluacije ovih biometrijskih sistema nalaze se na nivou M0.

Sličan pristup prilikom razvoja okvira primenjivan je i u drugim domenima, na primer u oblasti edukativnih igara [154].

7.2 Metamodel digitalnog reprezenta osobe

Prilikom predstavljanja karakteristika osobe u digitalnom domenu, biometrijski podaci mogu se posmatrati kao podaci multimedijalnog karaktera. Jedna osoba, može imati više digitalnih reprezenata. Digitalni reprezenti mogu biti konkretne biometrijske karakteristike, odnosno biometrijski modaliteti ili pak karakteristike izvedene na osnovu odgovarajućih multimedijalnih podataka, kao što je standardna praksa kod multimedijalnih baza podataka [155]. Primer izvedene karakteristike može biti pripadnost određenoj kategoriji "životinja" definisanih u okviru Dodingtonove biometrijske menažerije [3].

Sam biometrijski modalitet možemo definisati kao neku fiziološku ili bihejviorističu karakteristiku osobe na osnovu koje možemo izvršiti njenu jedinstvenu identifikaciju. Samim tim, možemo izvršiti podelu biometrijskih modaliteta na dve kategorije - fiziološke biometrijske modalitete i bihejviorističke biometrijske modalitete [156].



Slika 13 – Metamodel digitalnog reprezenta osobe

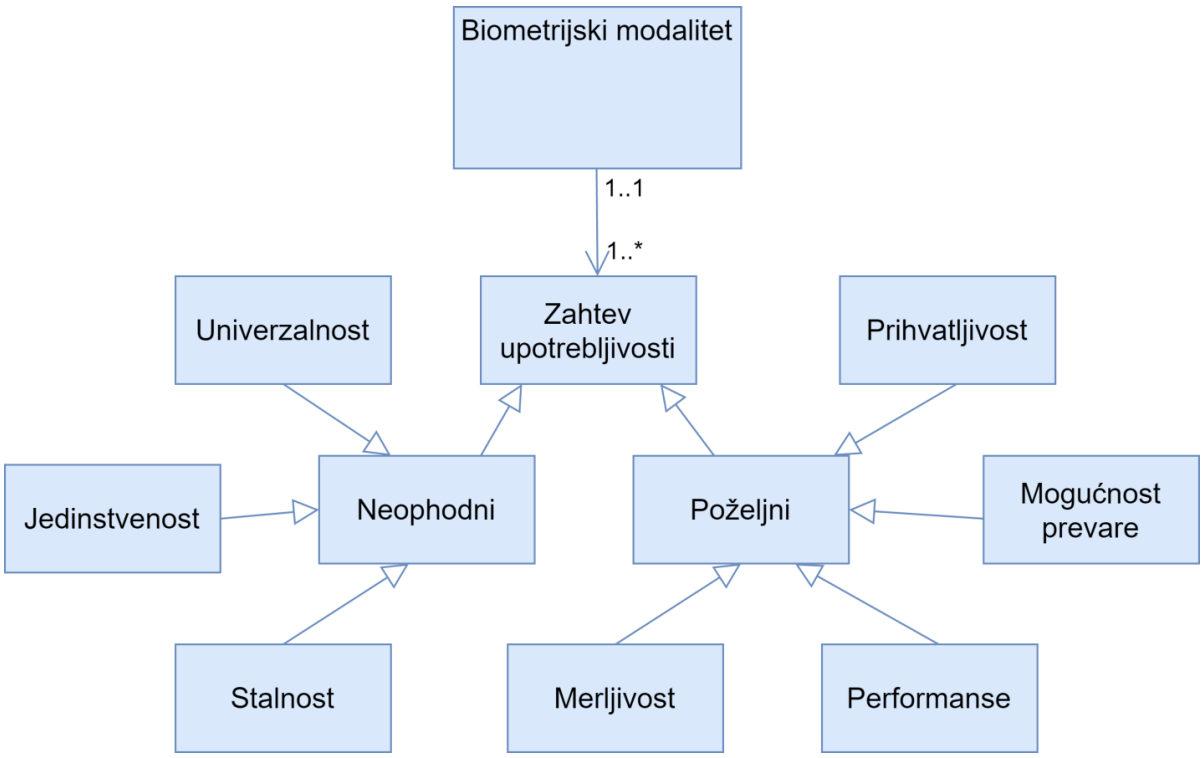
Pod fiziološkim biometrijskim modalitetom osobe smatra se deo ljudskog tela pomoću koga je moguće jedinstveno identifikovati osobu. Primeri ovakvih modaliteta su lice, otisak prsta, iris, retina, otisak šake. Ovi modaliteti su većinom sporije podložni promenama, međutim uglavnom zahtevaju određeni stepen saradnje korisnika prilikom korišćenja biometrijskog sistema.

Bihejvioristički modaliteti baziraju sa na ponašanju i radnjama određene individue. Različiti ljudi rade određene stvari na karakteristične načine. Jedan primer za ovaj biometrijski modalitet je hod. Različite osobe imaju različite načine hoda [67]. Drugi primeri bihejviorističkih modaliteta su način kucanja na tastaturi i potpis.

Pored isključivo bihejviorističkih, ili isključivo fizioloških biometrijskih modaliteta, potrebno je da razmotrimo i treću kategoriju biometrijskih modaliteta. To su kombinovani biometrijski modaliteti. Oni imaju i aspekte fizioloških karakteristika, ali takođe zavise od ponašanja i nesvesnih navika određene individue. U kategoriju ovakvih biometrijskih modaliteta možemo svrstati glas. Boja i karakteristike glasa predstavljaju fiziološke karakteristike, međutim prilikom analize glasa značajnu ulogu imaju i ponašajne navike koje je osoba razvila vezana za svoj govor, kao i uticaj raspoloženja na karakteristike glasa [157].

7.3 Metamodel upotrebljivosti biometrijskog modaliteta

Po autorima [1] biometrijski modalitet je potrebno da zadovoljava određen set karakteristika. One su prikazane na metamodelu Biometrijski modalitet. To su Univerzalnost, Jedinstvenost, Stalnost, Merljivost, Performanse, Prihvatljivost i Mogućnost prevare. U okviru ovog metamodela, biometrijski modaliteti klasifikovani su na osnovu ovih zahteva. Na taj način se prilikom evaluacije biometrijskog sistema, može lakše izvršiti poređenje različitih biometrijskih modaliteta, kao i njihovih prednosti i mana.



Slika 14 – Metamodel upotrebljivosti biometrijskog modaliteta

Univerzalnost govori o tome da bi svaka osoba trebala da poseduje biometrijski modalitet na osnovu koga je moguće izvršiti akviziciju podataka. Na primer, ukoliko neko ne poseduje govorne mogućnosti, ne može koristiti glas kao biometrijski

modalitet. Pored očiglednih nemogućnosti, postoje i drugi slučajevi nemogućnosti upotrebe, što možemo videti ukoliko uzmemo u analizu otisak prsta kao biometrijski modalitet. Iako bi u teoriji svako trebalo da poseduje otisak prsta, postoji određeni procenat osoba koje nemaju otisak usled nedostatka jagodica, ili su im pak otisci veoma slabog kvaliteta usled prirode posla koji obavljaju [35]. Slab kvalitet otisaka za posledicu ima znatno češće pojavljivanje grešaka prilikom rada sistema u odnosu na očekivane performanse.

Jedinstvenost se odnosi na potrebu da instance određenog biometrijskog modaliteta kod različitih osoba budu dovoljno drugačije, kako bi se prilikom ekstrakcije karakteristika iz sirovih biometrijskih podataka dobile dovoljno različite biometrijske karakteristike.

Stalnost ukazuje na potrebu da se biometrijska karakteristika ne menja značajno sa vremenom. Biometrijski modaliteti trpe određene promene sa starenjem, koje mogu uticati na preciznost biometrijskog sistema [158] [159]. Sa druge strane, **merljivost** ukazuje na neophodnost mogućnosti kvantifikacije biometrijske karakteristike, kako bi se dobio odgovarajući ulaz za algoritme za ekstrakciju karakteristika i poređenje biometrijskih modaliteta.

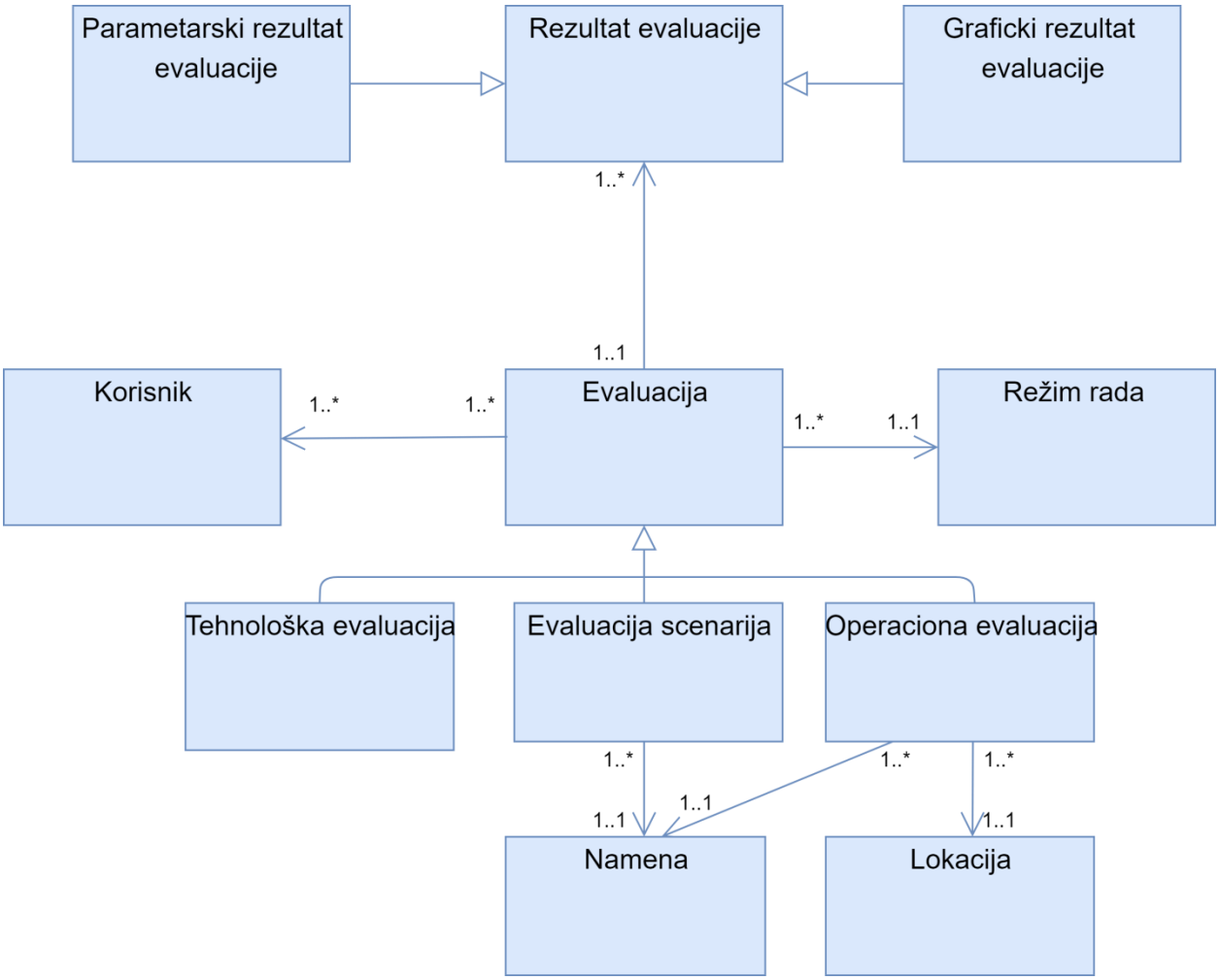
Pored ovih zahteva, koji se klasifikuju kao neophodni zahtevi prihvatljivosti za određeni biometrijski modalitet, radi upotrebe u praksi definišemo i dodatni skup poželjnih zahteva. **Performanse** se odnose kako na preciznost, tako i na vreme potrebno za ekstrakciju podataka. Na primer, iako DNA (eng. *deoxyribonucleic acid*) ima izuzetnu preciznost, potrebno vreme za procesiranje nije praktično za svakodnevnu upotrebu [160]. Takođe, njena upotreba kao biometrijskog modaliteta dolazi u sukob sa sledećim zahtevom, **prihvatljivošću**. Većina ljudi ne bi želela da koristi takav biometrijski sistem, zbog potencijalnih informacija koje bi bile na raspolaganju organizaciji koja je vlasnik sistema. Na kraju, dolazimo i do poslednjeg zahteva, a to je **mogućnost prevare.** Na primer, pomoću lažnog silikonskog modela prsta napravljenog na osnovu nečijeg otiska, potencijalno možemo ostvariti neautorizovan pristup sistemu, ukoliko biometrijski sistem nema odgovarajuće mehanizme zaštite. Neki modaliteti su više izloženi ovom riziku, mada dosta toga zavisi i od tipa senzora koji se koristi za akviziciju. Na primer, kod lica kao biometrijskog modaliteta, teže je izvršiti prevaru ako se koristi infracrveni senzor nego standardna 2D kamera [161].

7.4 Metamodel načina evaluacije biometrijskog sistema

Po autorima [162], postoje tri različita pristupa evaluaciji biometrijskih sistema: tehnološka evaluacija, evaluacija scenarija i operaciona evaluacija. Tehnološka evaluacija se koristi kako bi se utvrdila preciznost samih biometrijskih algoritama [162]. Ideja je da se rezultati dobijeni ovim tipom eksperimenta mogu ponoviti, te je poželjan način testiranja upotreba javnih biometrijskih baza podataka, kao što je na primer FRPC (*Face Recognition Prize Challenge*) [163].

Evaluacija scenarija bavi se utvrđivanjem performansi sistema u specifičnom domenu [162]. Na primer, možemo pokušati da ispitamo da li sistem za prepoznavanje lica može da se primeni za kontrolu pristupa na aerodromu. Uslovi upotrebe sistema su takođe bitni. Spoljni faktori kao što su osvetljenje ili buka moraju biti uzeti u obzir. Rezultati dobijeni ovom evaluacijom bi trebalo da budu ponovljivi.

Operaciona evaluacija se odnosi na primenu scenarija za konkretan slučaj korišćenja [162]. U odnosu na prethodni tip, razlika je sledeća - testiramo sistem za prepoznavanje lica, ali na konkretnom aerodromu, na primer "Nikola Tesla" u Beogradu. Rezultati dobijeni na ovaj način su jedinstveni i nije ih moguće u potpunosti reprodukovati u istom obliku.



Slika 15 – Metamodel evaluacije biometrijskog sistema

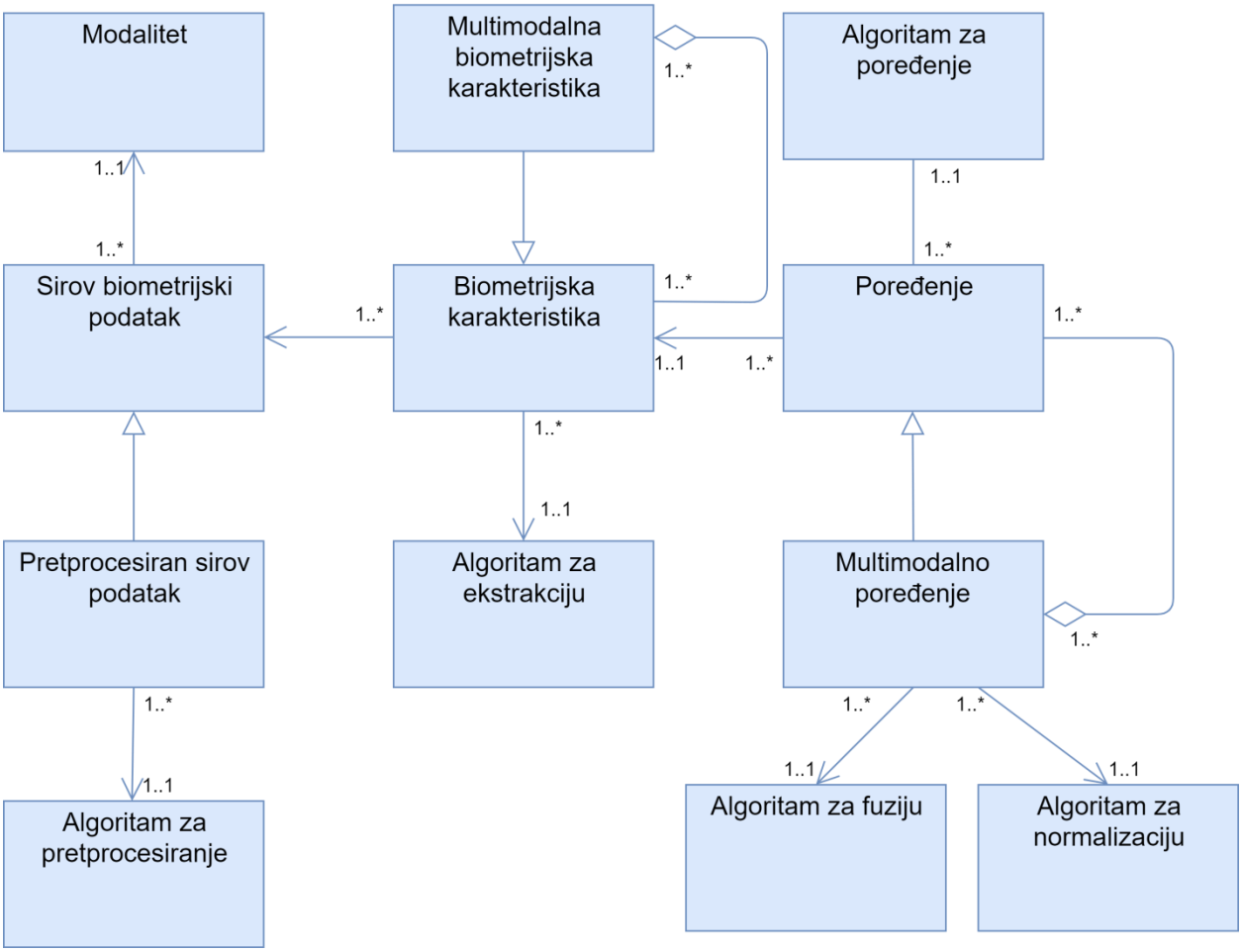
Evaluacija biometrijskog sistema vrši se nad određenim brojem korisnika. Jedna evaluacija može imati jedan ili više rezultata. Rezultati mogu biti grafičkog ili pak parametarskog karaktera. Sa druge strane, biometrijski sistem može funkcionisati u više režima rada [1]. U zavisnosti od režima rada biometrijskog sistema, razlikuju se i načini izračunavanja parametara biometrijskog sistema, kao i potencijalni načini vizuelizacije sprovedene evaluacije. Na primer, u slučaju rada u identifikacionom režimu, preciznost identifikacije se može prikazati CMC (eng. *Cumulative Match Curve*) krivom [70].

7.5 Metamodel transformacije biometrijskih podataka

Korisnik biometrijskog sistema može pomoću procesa akvizicije podataka zapamtiti više sirovih biometrijskih uzoraka u biometrijskom sistemu. Svaki sirovi biometrijski uzorak se odnosi na određeni biometrijski modalitet. Sirovi biometrijski uzorci mogu biti podvrgnuti procesu pretprocesiranja. Cilj ovog procesa jeste povećanje preciznosti

biometrijskog sistema u kasnijim fazama. Primenom različitih algoritama za pretprocesiranje, iz jednog sirovog biometrijskog podatka može se izvesti veći broj pretprocesiranih biometrijskih podataka.

Biometrijska karakteristika nastaje ekstrakcijom specifičnosti karakterističnih za biometrijski modalitet određene osobe. Primenom različitih algoritama za ekstrakciju biometrijskih karakteristika na osnovu jednog sirovog biometrijskog podatka može se dobiti više sirovih biometrijskih karakteristika. Takođe, u slučaju multimodalnog biometrijskog sistema, biometrijska karakteristika može biti takozvana multimodalna biometrijska karakteristika. Ona nastaje spajanjem više biometrijskih karakteristika u jednu pomoću određenog algoritma za fuziju biometrijskih karakteristika.



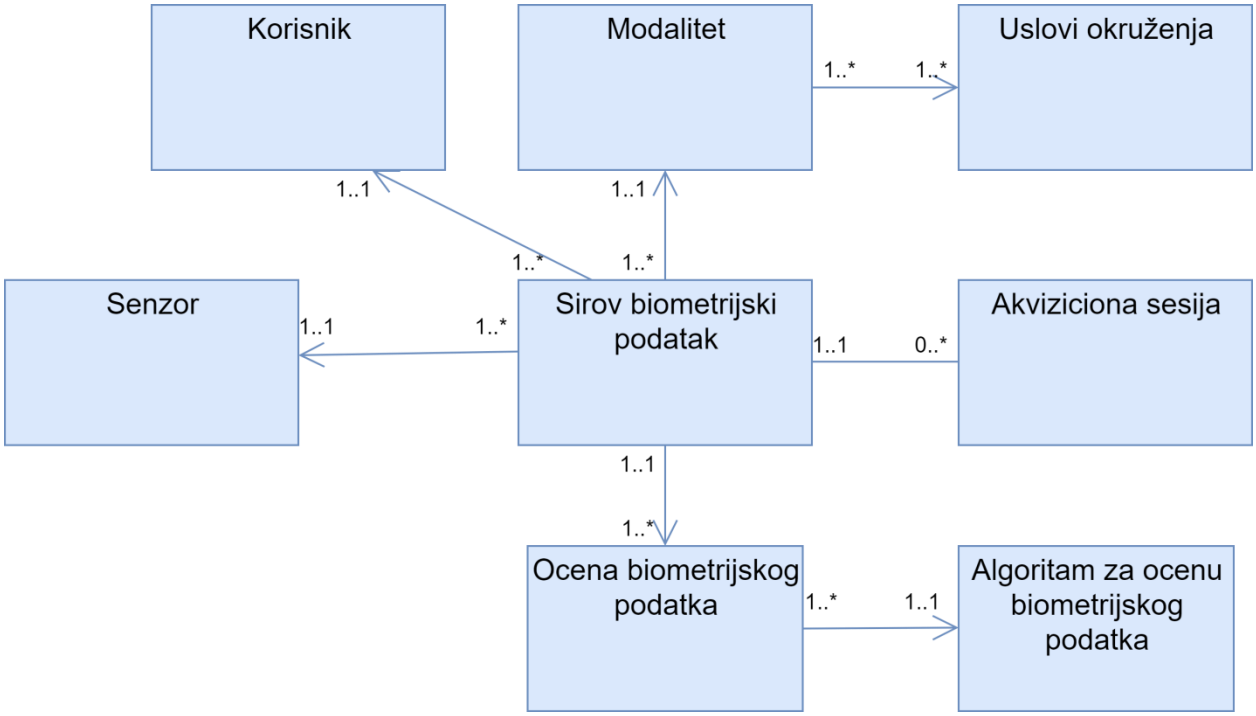
Slika 16 – Metamodel transformacije biometrijskih podataka

Kako bi se dobio odgovarajući skor poređenja na osnovu koga je moguće doneti odluku u okviru biometrijskog sistema, potrebno je uporediti dve biometrijske karakteristike pomoću algoritma za poređenje. U okviru multimodalnih biometrijskih sistema, poređenjem karakteristika dobijenim akvizicijom u odnosu na one koje se nalaze u biometrijskoj bazi podataka, možemo izračunati više biometrijskih poređenja. Postavlja se pitanje kako doneti odluku u biometrijskom sistemu, na osnovu više dobijenih poređenja. Za tu svrhu koristimo algoritme za fuziju informacija. U određenim slučajevima, pre fuzije informacija, potrebno je izvršiti normalizaciju dobijenih skorova

poređenja. Tada se koriste odgovarajući algoritmi za normalizaciju skorova poređenja. Primenom ovih algoritama, vrednosti skorova se normalizuju na zajednički okvir.

7.6 Metamodel akvizicije biometrijskih podataka

U okviru jedne akvizicione sesije može biti prikupljeno više sirovih biometrijskih podataka. Jedan korisnik sistema može dati jedan ili više uzoraka sirovih biometrijskih podataka. Svaki sirovi biometrijski podatak odnosi se na određeni modalitet. Prilikom akvizicije sirovog biometrijskog podatka, korišćen je određeni hardverski uređaj, odnosno senzor. Izbor senzora može uticati na kasnije performanse i preciznost biometrijskog sistema [164].



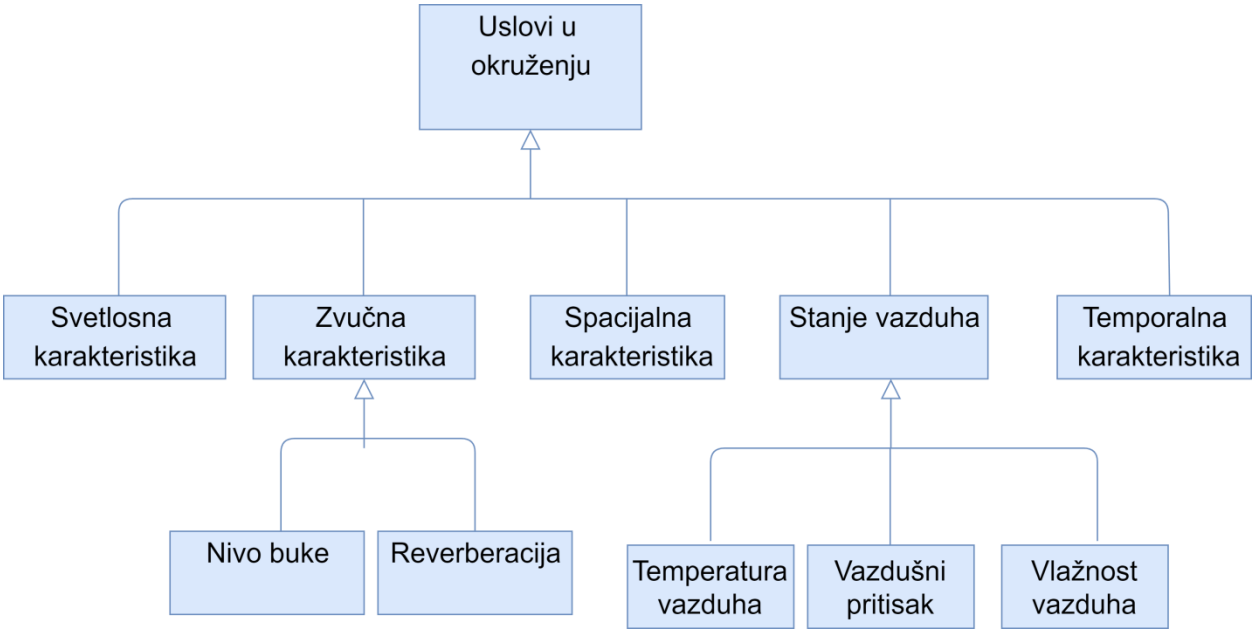
Slika 17 – Metamodel akvizicije biometrijskih podataka

Takođe, bitna stavka koja utiče na kvalitet podataka prikupljenih akvizicijom jesu spoljni uslovi okruženja. Pod spoljnim uslovima smatramo različite uticaje, a u zavisnosti od biometrijskog modaliteta i senzora razlikuju se oni koji imaju najznačajniji efekat na rad biometrijskog sistema. Na primer, kod otiska prsta, vlažnost, temperatura i zaprljanost senzora za akviziciju imaju značajan uticaj na performanse biometrijskog sistema [165]. Prilikom upotrebe klasičnih 2D kamera za akviziciju lica, osvetljenje ima uticaj na preciznost biometrijskog sistema [166]. Ovi uslovi okruženja vezani su pre svega za konkretan biometrijski modalitet.

Jedan od načina procene uticaja uslova akvizicije na sirovi biometrijski podatak jeste primena algoritama za ocenu kvaliteta biometrijskih podataka. Na osnovu izvedenih podataka prilikom ekstrakcije karakteristika kao što je slučaj kod NFIQ algoritma [167], ili poređenjem rezultata sa rezultatima dobijenim od strane nekog etalonskog algoritma, možemo odrediti nivo kvaliteta biometrijskog uzorka.

7.7 Metamodel uslova okruženja

Same uslove okruženja možemo preciznije prikazati i razložiti u okviru posebnog metamodela. Kao osnova za ovaj zadatak poslužio nam je metamodel za opis uslova u određenom prostoru u okruženju opisan u okviru doktorske disertacije Željka Obrenovića [168]. Po ovom metamodelu, možemo identifikovati tri grupe uslova okruženja: svetlosne karakteristike, zvučne karakteristike i stanje vazduha. Zvučne karakteristike dodatno možemo posmatrati kao nivo buke i reverberacione karakteristike, dok stanje vazduha takođe ima različite aspekte, a to su pre svega temperatura vazduha, vazdušni pritisak i vlažnost vazduha.



Slika 18 – Metamodel uslova okruženja

Kako bismo dodatno opisali uslove okruženja relevantne za evaluaciju biometrijskog sistema, ovaj model je proširen sa dve potkategorije: spacijalna karakteristika i temporalna karakteristika (slika 18). Spacijalna karakteristika se odnosi na položaj korisnika sistema u odnosu na senzor sistema. Ako posmatramo dvodimenzionalnu sliku lica kao biometrijski modalitet, ugao lica u odnosu na kameru utiče na preciznost biometrijskog prepoznavanja [169]. Što se temporalnih karakteristika tiče, one se odnose na potrebno vreme interakcije biometrijskog modaliteta korisnika sa senzorom. Unapređenjem senzora za akviziciju može se uticati na smanjenje vrednosti ovog parametra [170].

8 MODELOVANJE EVALUACIJE MULTIMODALNIH BIOMETRIJSKIH SISTEMA

U sastavu ovog poglavlja dat je pregled primene objedinjenog modela evaluacije multimodalnih biometrijskih sistema za proširenje jezika za modelovanje. Kako je danas uobičajen pristup modelovanju zasnovan na objektno orijentisanom pristupu, nastavak rada zasnovan je upravo na ovoj paradigmi.

Standardan način modelovanja objektno orijentisanih sistema jeste pomoću UML jezika [171]. Jedan veoma važan aspekt koji UML poseduje jeste njegova proširivost. To su pre svega mehanizmi koji se odnose na stereotipe, tagove i profile. Ovi apstrakti omogućavaju prilagođavanje UML-a različitim tipovima problema [8]. Veliki broj UML profila predložen je od strane istraživača, stručnjaka iz prakse i organizacija za standardizaciju kako bi se bolje modelovali problemi iz različitih specifičnih domena.

Mehanizmi za proširenje dozvoljavaju precizno definisanje semantike modela, isključivo proširivanjem postojećih koncepata, čime se sprečavaju konflikti sa standardnim pojmovima. Profili se definišu upotrebom stereotipa, tagovanih vrednosti i ograničenja koja su primenjena na specifične elemente modela, kao što su klase, atributi, operacije i aktivnosti [172]. Profil je upravo kolekcija ovakvih ekstenzija koje prilagođavaju standardne koncepte UML jezika specifičnim elementima, kao što su klase, atributi, operacije i aktivnosti [9]. One sve zajedno prilagođavaju UML potrebama određenog domena (zdravstvo, obrazovanje...) ili pak određene razvojne platforme.

Za proširenja definisanjem odgovarajućih profila pomoću koncepata iz objedinjenog modela evaluacije odabrani su sledeći aspekti evaluacije multimodalnih biometrijskih sistema:

- Evaluacija biometrijske akvizicije
- Poređenje biometrijskih podataka
- Fuzija informacija
- Prikaz evaluacije biometrijskog sistema
- Biometrijska menažerija

Naravno, dalji prikaz modela pomoću odgovarajućih profila nije sveobuhvatan i predstavlja samo jedan pogled na problematiku modelovanja evaluacije multimodalnih biometrijskih sistema. Primenjeni koncepti dozvoljavaju i drugačija proširenja, u skladu sa eventualnim izmenjenim zahtevima.

8.1 Modelovanje evaluacije biometrijske akvizicije

U okviru profila evaluacije biometrijske akvizicije definisani su sledeći stereotipi klasa:

- Biometrijski modalitet – detaljniji opis biometrijskog modaliteta
- Biometrijski podatak – biometrijski podatak dobijen akvizicijom

- Izvedena karakteristika – karakteristika korisnika dobijena obradom biometrijskih podataka
- Ocena biometrijskog podatka – opisuje bliže kvalitet biometrijskog podatka dobijenog akvizicijom
- Algoritam za ocenu – opisuje algoritam za ocenu kvaliteta biometrijskog podatka
- Uslovi okruženja – opisuje uslove prilikom akvizicije podataka određenog biometrijskog modaliteta

Pridodate vrednosti stereotipu <<Biometrijski modalitet>> prikazane su u sledećoj tabeli. Vrednosti za svaku pridodatu vrednost definisani su u okviru odgovarajuće enumeracije StepenIspunjenostiZahteva - Niska, Srednja, Visoka.

Tabela 7 – Vrednosti pridodate stereotipu << Biometrijski modalitet >>

Pridodata vrednost:	Tip:	Primer upotrebe
Univerzalnost	StepenIspunjenostiZahteva	Srednja
Jedinstvenost	StepenIspunjenostiZahteva	Visoka
Stalnost	StepenIspunjenostiZahteva	Visoka
Merljivost	StepenIspunjenostiZahteva	Niska
Prihvatljivost	StepenIspunjenostiZahteva	Niska
Performanse	StepenIspunjenostiZahteva	Srednja
MogućnostPrevare	StepenIspunjenostiZahteva	Visoka

Stereotip <<Ocena biometrijskog podatka>> ima pridodatu vrednost *Kvalitet*.

Tabela 8 – Vrednosti pridodate stereotipu << Ocena biometrijskog podatka >>

Pridodata vrednost:	Tip:	Primer upotrebe
Kvalitet	Double	4.0

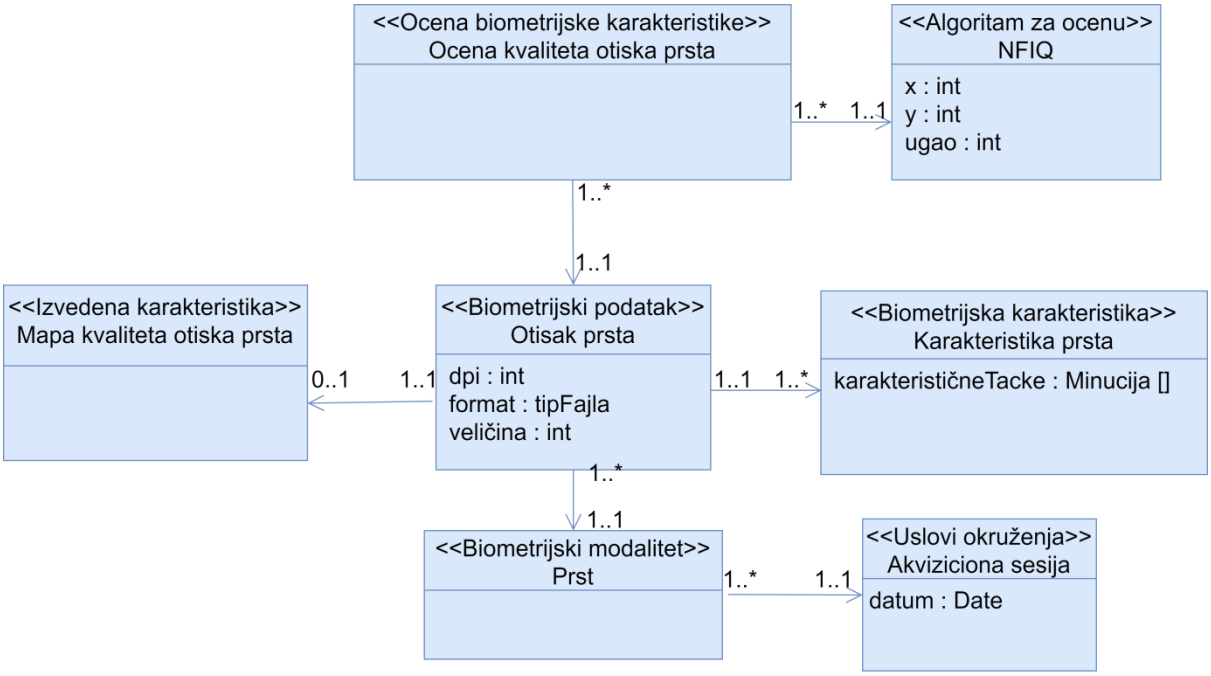
Pomoću stereotipa <<Uslovi okruženja>> i njemu pridodatih vrednosti prikazanih u tabeli 9 detaljnije opisujemo uslove okruženja koji se odnose na neki konkretan biometrijski modalitet u procesu akvizicije. Prikaz spacijalnih karakteristika biometrijskog modaliteta u odnosu na senzor kao koordinatni početak opisan je pomoću atributa sfernog koordinatnog sistema, a to su Radijalno odstojanje, Polarni ugao i Azimutski ugao. Temperatura okruženja prilikom akvizicije data je u celzijusima, dok je

vlažnost prikazana u procentima. Nivo buke je dat je u decibelima, a vazdušni pritisak u milibarima. Vreme interakcije sa senzorom prikazano je u sekundama.

Tabela 9 – Vrednosti pridodate stereotipu << Uslovi okruženja >>

Pridodata vrednost:	Tip:	Primer upotrebe
Radijalno odstojanje	double	5,49
Polarni ugao	double	1.33
Azimutski ugao	double	0.8
Temperatura okruženja	double	23.5
Vlažnost okruženja	double	70
Nivo buke	double	40.6
Vazdušni pritisak	double	1200
Vreme interakcije	double	1.1

Na slici 19 je model akvizicije otiska prsta dodatno opisan primenom odgovarajućeg profila i pomoću definisanih stereotipa. Prilikom akvizicije biometrijskog modaliteta prsta, potrebne su nam informacije o akvizicionoj sesiji, koju dodatno opisujemo stereotipom <<Uslovi okruženja>>. Na osnovu jedne akvizicione sesije, možemo imati više sirovih biometrijskih podataka – otisaka prstiju. Za svaki od otisaka možemo daljim procesiranjem da dobijemo izvedenu karakteristiku, a to je u ovom slučaju Mapa kvaliteta otiska prsta. Svaki otisak prsta možemo oceniti pomoću NFIQ algoritma [167] za ocenu kvaliteta prikupljenog otiska prsta.



Slika 19 – Model evaluacije biometrijske akvizicije

8.2 Modelovanje poređenja biometrijskih podataka

U okviru profila poređenja biometrijskih podataka definisani su sledeći stereotipovi klasa:

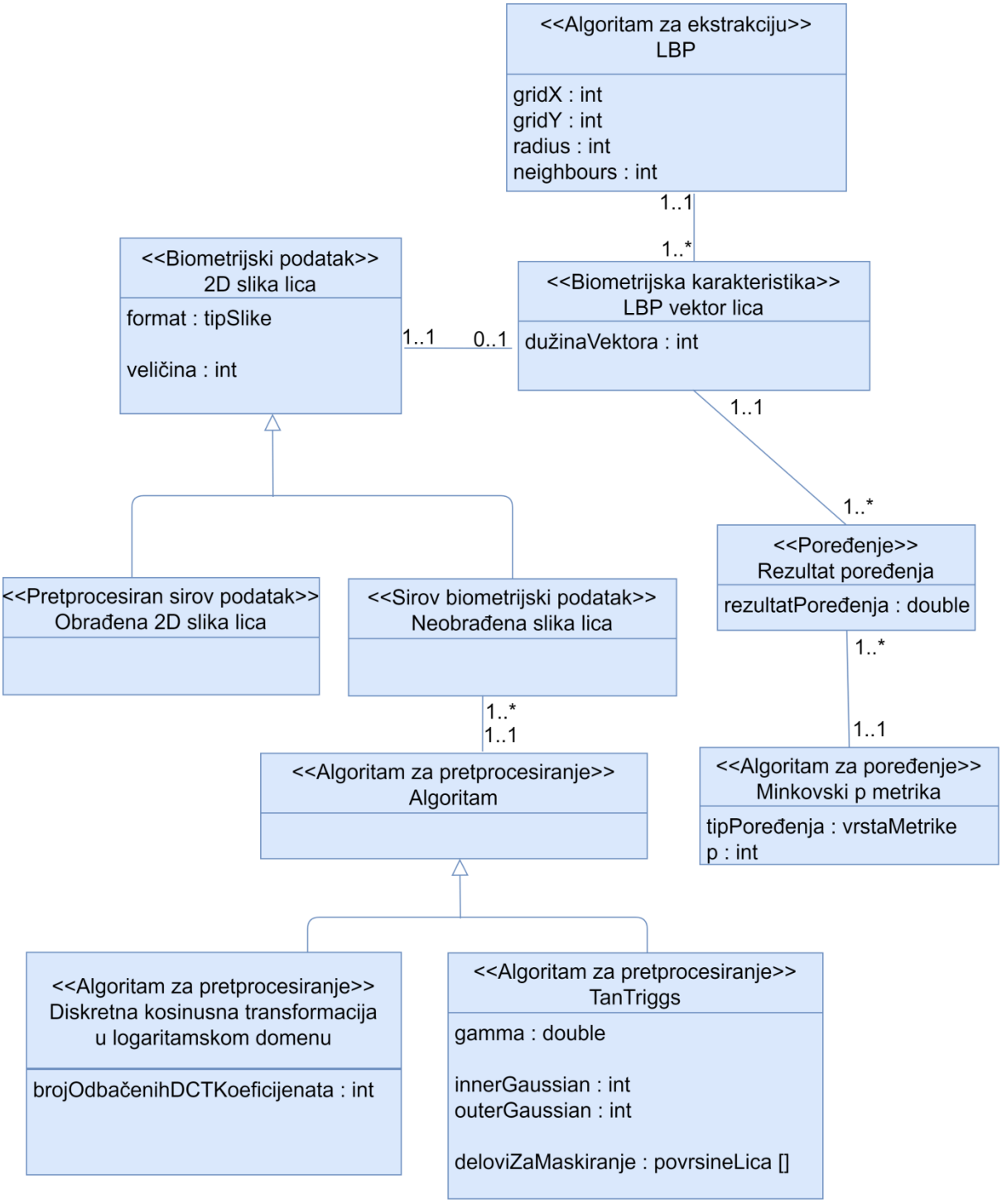
- Sirov biometrijski podatak – biometrijski podatak koji nije dodatno obrađen posle akvizicije
- Pretprocesiran biometrijski podatak – biometrijski podatak koji je nastao kao rezultat pretprocesiranja
- Algoritam za pretprocesiranje – opisuje algoritam za obradu biometrijskih podataka
- Biometrijska karakteristika – digitalizovan opis biometrijskog podatka
- Algoritam za poređenje – opisuje algoritam kojim se vrši poređenje biometrijskih karakteristika
- Poređenje – opisuje rezultate poređenja biometrijskih karakteristika

Takođe, za opis parametara konfiguracije algoritama, opisan je i stereotip atributa - <<Parametar algortima>>. Dodate vrednosti za stereotip <<Poređenje>> prikazane su u tabeli 10. Metrika poređenja je opisana pomoću posebne enumeracije TipoviMetrika čije su vrednosti Metrika sličnosti i Metrika udaljenosti.

Tabela 10 – Vrednosti pridodate stereotipu << Poređenje >>

Pridodata vrednost:	Tip:	Primer upotrebe
Rezultat	Double	67
MetrikaPoređenja	Tipovi metrika	Metrika sličnosti

Na slici 20 dat je primer modela poređenja biometrijskih podataka u unimodalnom sistemu za prepoznavanje lica. Pored profila Poređenja biometrijskih podataka, korišćeni su i koncepti iz profila Modelovanje evaluacije biometrijske akvizicije. Sistem koristi dvodimenzionalne slike lica kao biometrijske podatke. U određenim situacijama moguća je upotreba sirovih biometrijskih podataka, odnosno neobrađene slike lica, dok se u drugim situacijama koriste obrađene slike lica. Za obradu slike lica koristi se neki od raspoloživih algoritama za pretprocesiranje, u ovom slučaju diskretna kosinusna transformacija u logaritamskom domenu [173] i TanTriggs normalizacija [174]. LBP (eng. *Local Binary Pattern*) vektor lica dobijen je ekstrakcijom podataka primenom LBP algoritma [49]. Poređenjem više LBP vektora lica pomoću Minkovski p metrike [175] dobijamo odgovarajući rezultat poređenja.



Slika 20 – Model poređenja biometrijskih podataka

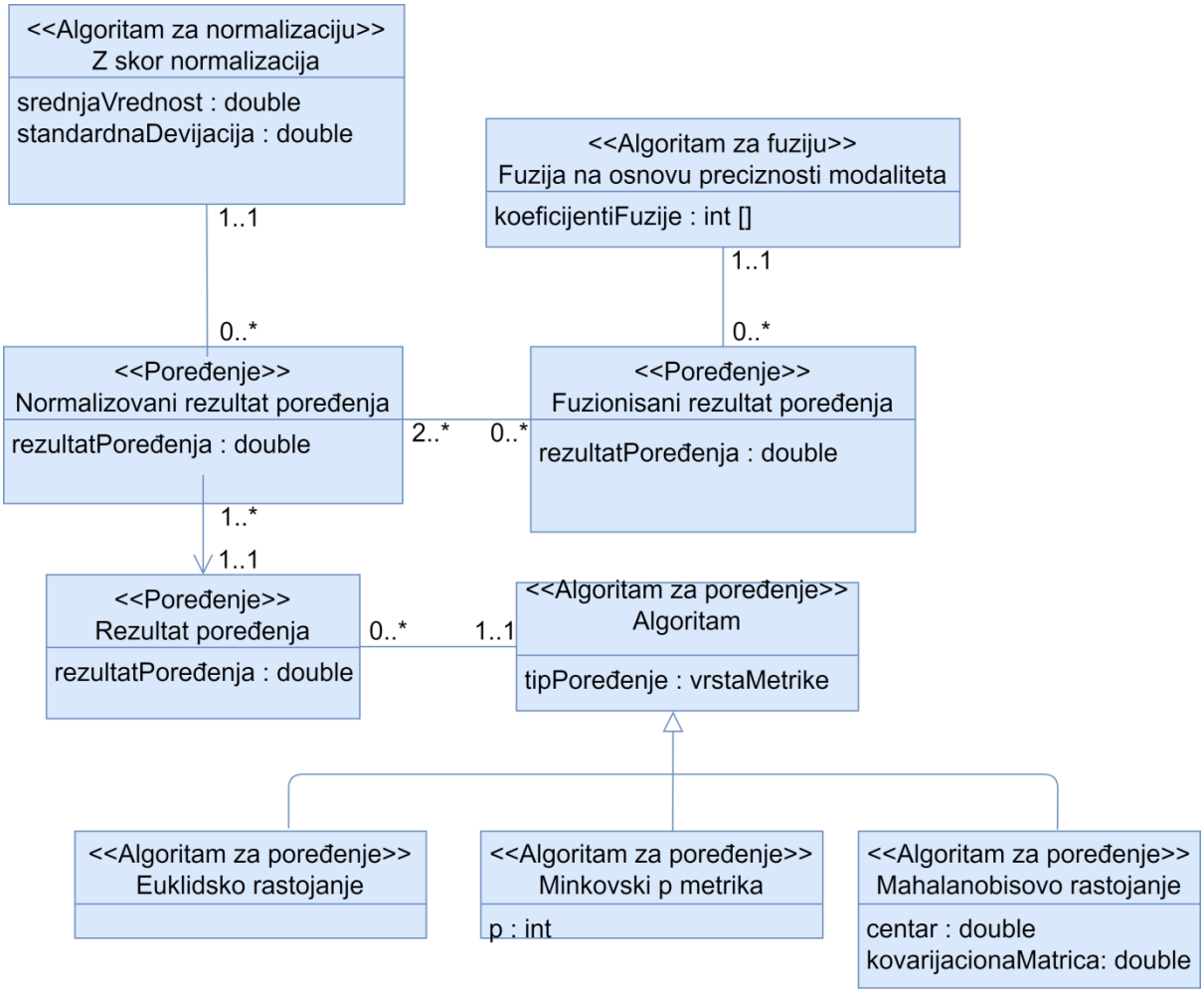
8.3 Modelovanje fuzije informacija

U okviru profila fuzije informacija definisani su sledeći stereotipi klasa:

- algoritam za fuziju – opisuje algoritme za fuziju informacija u multimodalnim biometrijskim sistemima

- algoritam za normalizaciju – opisuje algoritme za normalizaciju podataka radi kasnije fuzije infromacija

Na slici 21 prikazana je fuzija informacija na nivou poređenja u multimodalnom biometrijskom sistemu. Poređenja biometrijskih karakteristika se mogu vršiti pomoću različitih algoritama kao što su Euklidsko rastojanje, Minkovski p metrika ili Mahalanobisovo rastojanje [175]. Tako dobijeni rezultati poređenja se normalizuju pomoću Z skor normalizacije, a onda se normalizovani skorovi upotrebljavaju od strane algoritma za fuziju informaciju, koji je baziran na informacijama o preciznosti modaliteta [176].



Slika 21 – Model fuzije informacija u jednom multimodalnom biometrijskom sistemu

8.4 Modelovanje prikaza evaluacije biometrijskog sistema

U okviru profila prikaza evaluacije definisani su sledeći stereotipi klasa:

- Evaluacija algoritma – opisuje evaluaciju konkretnih algoritama
- Evaluacije scenarija – opisuje evaluaciju primene sistema za određenu namenu
- Operaciona evaluacija – opisuje evaluaciju primene sistema za određenu namenu na određenoj lokaciji
- Parametarski rezultat evaluacije – tekstualni prikaz rezultata evaluacije
- Grafički rezultat evaluacije – grafički prikaz rezultata evaluacije

Stereotip <<Evaluacija Scenarija>> ima pridodatu vrednost *Namena*.

Tabela 11 – Vrednosti pridodate stereotipu << Evaluacija Scenarija >>

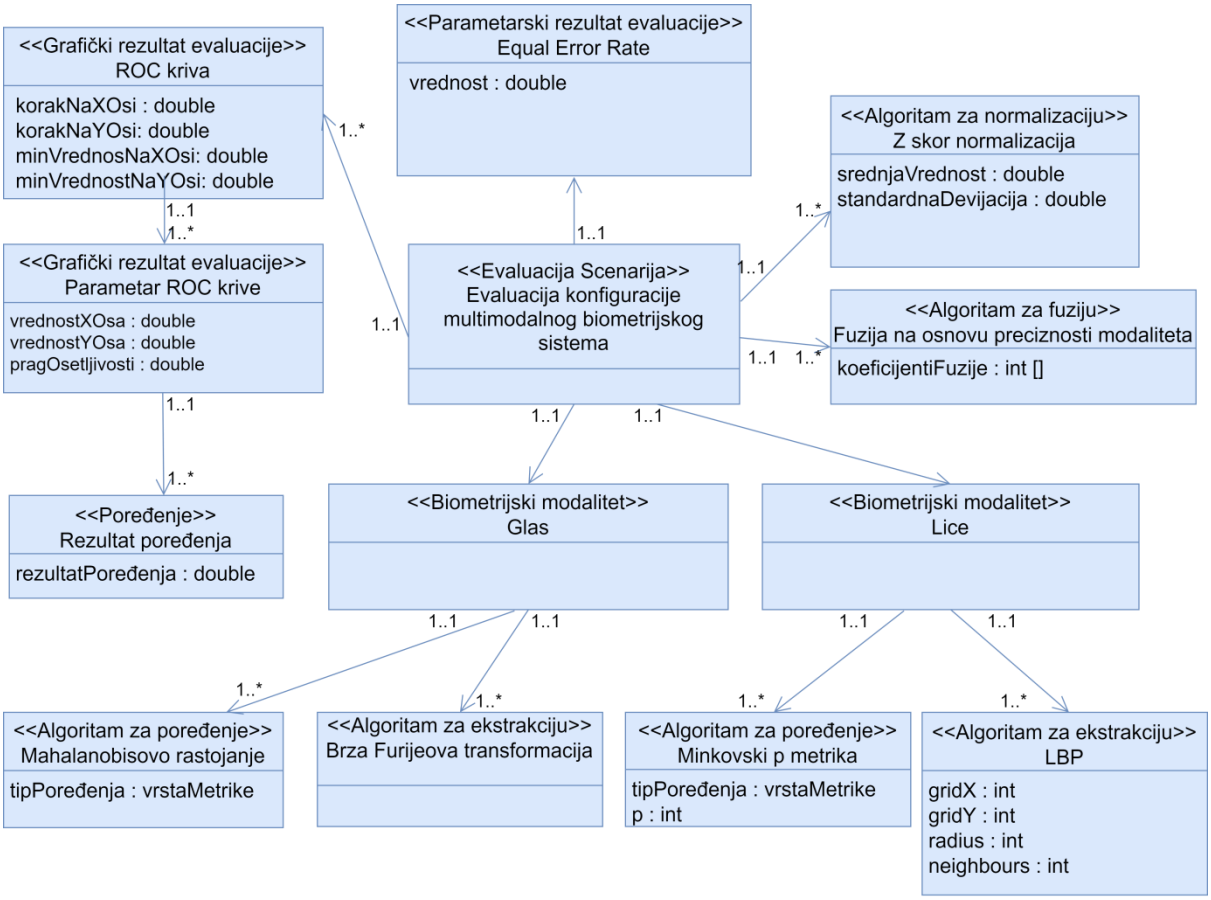
Pridodata vrednost:	Tip:	Primer upotrebe
Namena	String	Autentikacija prisustva studenata na predavanjima

Stereotip <<Operaciona Evaluacija>> ima pridodate vrednosti *Namena i Lokacija.*

Tabela 12 – Vrednosti pridodate stereotipu << Operaciona Evaluacija >>

Pridodata vrednost:	Tip:	Primer upotrebe
Namena	String	Autentikacija prisustva studenata na predavanjima
Lokacija	String	Fakultet Organizacionih nauka

Na slici 22 možemo videti prikaz evaluacije scenarija jednog multimodalnog biometrijskog sistema koji koristi biometrijske modalitete glasa i lica. Za ekstrakciju karakteristika glasa koristi Furijeove transformacije, dok za poređenje karakteristika glasa upotrebljava Mahalanobisovo rastojanje. Što se lica tiče, u upotrebi je LBP algoritam za ekstrakciju karakteristika i Minkovski p distanca za poređenje karakteristika. Fuzija se vrši na osnovu preciznosti pojedinačnih biometrijskih modaliteta. Evaluacija dobijenih poređenja se vrši parametarski, preko EER metrike, i grafički preko ROC krive. Svaka prikazana tačka - parametar ROC krive opisuje ponašanje sistema pri određenom pragu osetljivosti.



Slika 22 – Model evaluacije multimodalnog biometrijskog sistema

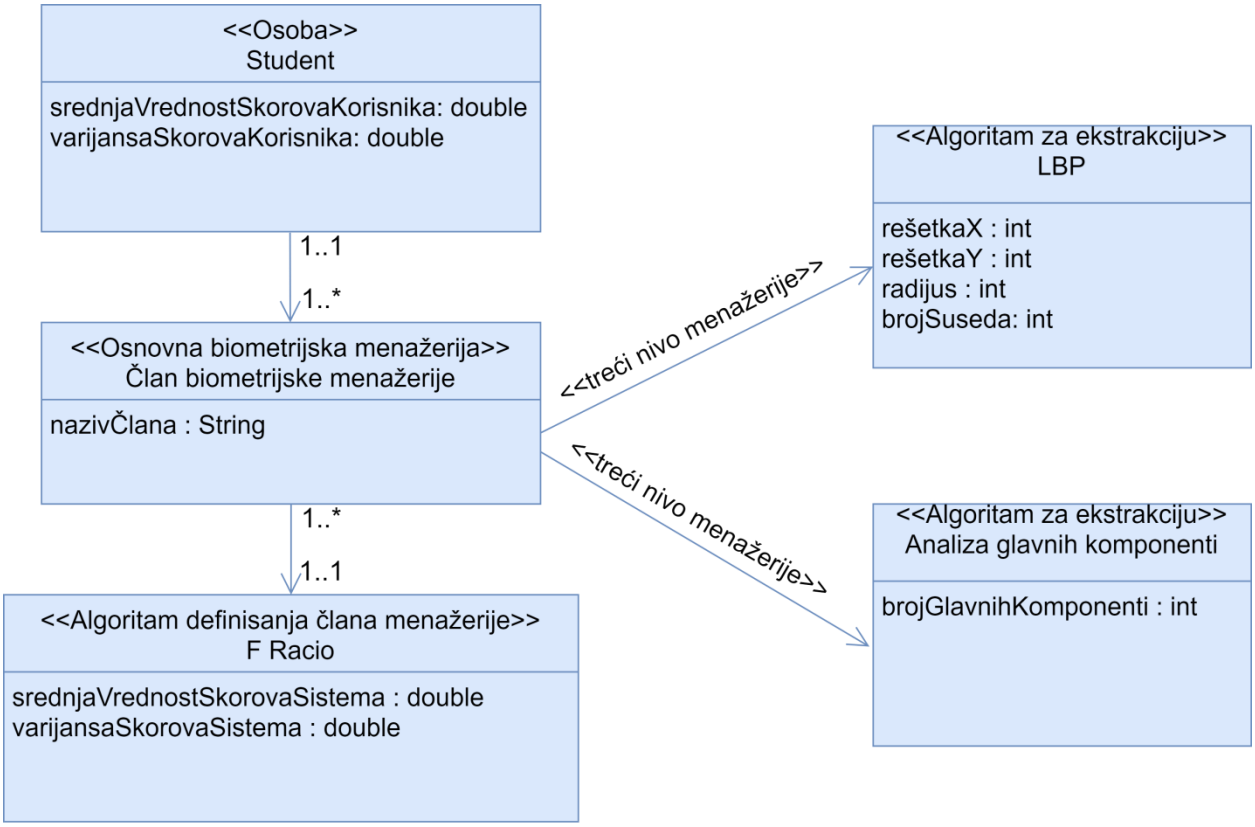
8.5 Modelovanje osoba u bazi biometrijskog sistema

U okviru profila osoba u bazi biometrijskog sistema definisani su sledeći stereotipi klasa:

- Osoba – opisuje karakteristike osobe koje su relevantne za funkcionisanje biometrijskog sistema
- Biometrijska menažerija – opisuje pripadnost osobe određenoj kategoriji biometrijske menažerije
- Algoritam definisanja člana menažerije – opisuje način na koji je izvršena klasifikacija osoba po kategorijama biometrijske menažerije

Takođe, opisani su i stereotipi veza, u skladu sa radom [120], koji definišu nivoe biometrijske menažerije:

- prvi nivo menažerije - označava setove podataka kod kojih ista osoba ima iste "etikete" članova menažerije
- drugi nivo menažerije opisuje uslove okruženja u odnosu na koje je pojavljivanje članova biometrijske menažerije invarijantno
- treći nivo menažerije opisuje biometrijske algoritme kod kojih se isti članovi biometrijske menažerije javljaju kod istih osoba



Slika 23 – Model osobe u bazi biometrijskog sistema

U okviru dijagrama prikazanog na slici 23 možemo videti model osobe u jednoj biometrijskoj bazi koja sadrži podatke studenata koji koriste sistem za biometrijsko prepoznavanje pomoću lica kao biometrijskog modaliteta. Za svakog studenta pamtimo prosečne vrednosti i varijansu skorova poređenja. Na osnovu vrednosti ova dva parametra na celom sistemu, možemo pomoću F-racio algoritma [123] odrediti da li osoba pripada određenoj kategoriji biometrijske menažerije. Ukoliko je prisutna menažerija višeg stepena, na primer javljanje istog člana menažerije kod različitih biometrijskih algoritama, to možemo opisati pomoću odgovarajućeg stereotipa veze kao što je prikazano na slici.

Pridodate vrednosti stereotipu <<Osoba> možemo videti u tabeli 13. Za opis eventualnog hendikepa korisnika prilikom upotrebe određenog biometrijskog modaliteta koristimo nabrajanje Hendikep, koje može imati vrednosti između 0 i 100, Pomoću vrednosti 0 predstavljeno je odsustvo hendikepa, dok vrednost 100 predstavlja potpuni hendikep. Eventualno postojanje hendikepa je potrebno da evidentiramo za otiske prstiju, vid, glas i hod. Pored ovoga, interesuje nas i starost osobe, pošto i ona može imati uticaj na preciznost biometrijskog sistema [85], kao i činjenica da li se osoba bavi manuelnim ili kancelarijskim tipom posla.

Tabela 13 – Vrednosti pridodate stereotipu << Osoba >>

Pridodata vrednost:	Tip:	Primer upotrebe
Starost	Int	32
TipPosla	String	Kancelarijski
Otisci prstiju	MeraHendikepa	0
Vid	Hendikep	0
Hod	Hendikep	100
Glas	Hendikep	0

9 PREDLOG PROCESA RAZVOJA I EVALUACIJE MULTIMODALNIH BIOMETRIJSKIH SISTEMA

U početku, razvoj softvera zasnivao se na filozofiji koju možemo najbolje opisati sintagmom "kodiraj prvo, popravljaj posle". Ovaj pristup podrazumevao je odsustvo ustaljenih procesa kao i precizno definisanih aktivnosti. Međutim, sa rastom kompleksnosti softverskih sistema, prilikom razvoja počeli su da se javljaju različiti problemi, koji su stvarali značajne dodatne troškove, ili čak dovodili do propasti softverskih projekata.

Primeri potencijalnih problema mogu biti: loše preneti korisnički zahtevi, određivanje vremenskih rokova pre razumevanja zahteva i sagledavanja rizika, razvoj softvera koji je težak za izmene, softver koji nije testiran na način na koji će krajnji korisnik da ga upotrebljava [177]. Kao pokušaj rešavanja problema, počele su da se javljaju metodologije za razvoj softvera. Metodologiju za razvoj softvera možemo definisati kao uređen proces koji ima cilj da razvoj softvera učini predvidljivijim i efikasnijim [178].

Za potrebe definisanje procesa razvoja i evaluacije multimodalnih biometrijskih sistema odabran je *Unified* proces [7]. Ova metodologija je zasnovana na iterativno inkrementalnom pristupu, arhitekturalno je orijentisana i fokusirana je na smanjenje rizika prilikom razvoja softvera. Takođe, UML jezik je sastavni deo ove metodologije. Postoje različite varijacije ove metodologije, kao što su RUP (Rational Unified Process) [179] , OUP (*Open Unified Process*) [180] i AUP (*Agile Unified Process*) [181]. Ipak, za potrebe procesa razvoja i evaluacije multimodalnih biometrijskih sistema, fokusiraćemo se na proširenje osnovne metodologije opisane u [7].

Unified proces ima dve dimenzije:

- statičku strikturu
- dinamičku strukturu

Dinamička struktura se odnosi na vremensku dimenziju softverskog projekta. Kako je *Unified* proces iterativnog karaktera, definisane su četiri faze od kojih svaka u sebi uključuje jednu ili više iteracija. Ove četiri faze su [7]:

- Inicijalizacija
- Elaboracija
- Konstrukcija
- Tranzicija

Svaka od faza ima završno dostignuće, kao i tačno definisan skup postavljenih ciljeva. Po minimalnom zadovoljenju ciljeva za određenu fazu prelazi se na sledeću. Iako različite faze imaju fokuse na drugačijim aktivnostima, odnosno disciplinama, prilikom svake iteracije vrše se zadaci iz svih disciplina u određenoj meri.

Statička struktura određuje kako se elementi procesa razvoja softvera, u ovom slučaju aktivnosti, uloge, artefakti i uloge grupišu u okviru odgovarajućih disciplina. Faze razvoja (discipline) koje su od značaja za naš problem su [7]:

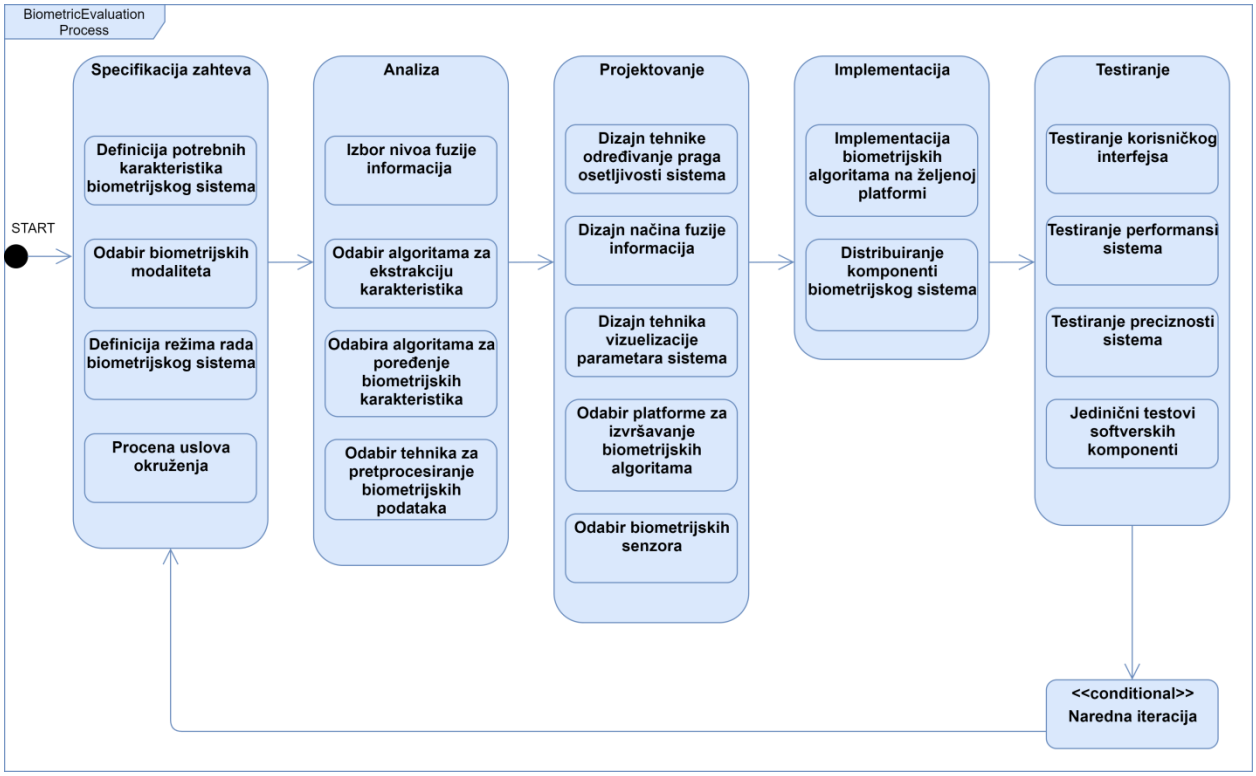
- Definisanje zahteva
- Analiza
- Projektovanje
- Implementacija
- Testiranje

Sve faze dopunjene su aktivnostima koje su od značaja za evaluaciju i razvoj multimodalnih biometrijskih sistema. Primenom profila definisanih u prethodnim poglavljima mogu se preciznije opisati aktivnosti u pojedinačnim fazama. Pregled proširenja po fazama dat je na slici 24.

U okviru faze definisanja zahteva, potrebno je odrediti funkcionalne i nefunkcionalne zahteve koje sistem treba da ispuni. Robert Grejdi je definisao FURPS (*Functionality, Usability, Reliability, Performance, Supportability*) model [182], gde zahteve delimo okvirno na ovih 5 kategorija. Prva kategorija zahteva su funkcionalni, dok upotrebljivost, pouzdanost, performanse i podršku svrstavamo u nefunkcionalne zahteve. Za definisanje zahteva, *Unified* proces koristi UML dijagrame slučajeva korišćenja.

Prilikom određivanja funkcionalnih zahteva neophodno je da definišemo karakteristike biometrijskog sistema koje je potrebno da sistem zadovolji, kao i da se odlučimo za defiiniciju tipa rada biometrijskog sistema. Takođe, prilikom određivanja zahteva, potrebno je opisati okruženje sistema. Za ove potrebe možemo koristiti definisane profile korisnika i evaluacije biometrijske akvizicije. Pomoću stereotipa <<Korisnik>> možemo bliže opisati korisnike biometrijskog sistema. Takođe, možemo koristiti stereotip <<Uslovi okruženja>> iz profila evaluacija biometrijske akvizicije i pomoću asocijacije detaljnije opisati uslove okruženja određenog slučaja korišćenja. Preciznijim određivanjem uslova okruženja lakše možemo da definišemo nefunkcionalne zahteve biometrijskog sistema.

Faza analize zajedno sa fazom projektovanja predstavlja sponu između korisničkih zahteva i implementacije sistema. Dok se u fazi definisanja zahteva koristi jezik koji je razumljiv i drugim zainteresovanim stranama u razvoju, u fazi analize se prelazi na jezik i koncepte koji su prilagođeni potrebama projektanata sistema. Konceptualni model sistema koji je rezultat faze analize je platformski nezavisan i opisuje funkcionalnosti sistema. U ovoj fazi potrebno je izvršiti izbor algoritama za ekstrakciju biometrijskih karakteristika, kao i algoritama za poređenje biometrijskih karakteristika. Pored toga, potrebno je proceniti da li je neophodno pretprocesiranje biometrijskih podataka dobijenih prilikom akvizicije i ako jeste odabrati algoritme pogodne za tu namenu. Ovi zadaci mogu se bolje opisati upotrebom profila poređenja biometrijskih podataka i profila evaluacije biometrijske akvizicije.



Slika 24 – Proširenje standardne *Unified* metode konceptima specifičnim za razvoj i evaluaciju multimodalnih biometrijskih sistema

Faza projektovanja dalje razrađuje koncepte opisane u fazi analize. Konceptualni model prilagođava se zahtevu konkretnih platformi na kojima će se sistem izvršavati. Detaljno se razrađuju i različiti nefunkcionalni zahtevi. Odabir programskih jezika, platformi, operativnog sistema, hardverskih komponenti sistema neke su od odluka koje je potrebno realizovati u ovoj fazi. Kao rezultat se dobijaju projektni modeli koji su detaljniji od konceptualnih, ali i manje generički.

U kontekstu evaluacije i razvoja multimodalnih biometrijskih sistema, u fazi projektovanja potrebno je odabrati platformu za izvršavanje biometrijskih algoritama. U zavisnosti od platforme kao i uslova korišćenja, potrebno je dizajnirati načine fuzije informacija dobijenih od algoritama, kao i tehnike određivanja praga osetljivosti sistema. Ove zadatke možemo realizovati pomoću profila fuzije informacija. Pored toga, u ovoj fazi se vrši i dizajn tehnika vizuelizacije parametara sistema, za šta možemo koristiti profil prikaza evaluacije biometrijskog sistema.

Projektni modeli predstavljaju osnovu za realizaciju naredne faze u metodologiji, faze implementacije. Na osnovu definisanih projektnih modela realizuju se implementacione komponente. Komponente mogu biti u obliku izvornog koda ili izvršnih datoteka. Biometrijski algoritmi se implementiraju kao komponente softverskog sistema. Dakle, neophodno je implementirati biometrijske algoritme za odabrane platforme, uz poštovanje ograničenja svake od platformi. Taj zadatak se može rešiti ili manuelno ili eventualno definisanjem automatskog preslikavanja projektnih modela u implementacione komponente. Takođe, vrši se distribucija implementacionih komponenti biometrijskog sistema, kako bi se obezbedila skalabilnost.

Prilikom testiranja, ispitujemo da li sistem ispunjava postavljene funkcionalne i nefunkcionalne zahteve. U kontekstu razvoja i evaluacije biometrijskih sistema, potrebno je pored jediničnih testova za proveru funkcionalnosti, izvršiti i testiranje preciznosti sistema, performansi kao i testiranje korisničkog interfejsa biometrijskog sistema. U okviru faze testiranja mogu se koristiti koncepti definisani u okviru profila prikaza evaluacije biometrijskog sistema.

10 OKVIR ZA EVALUACIJU PERFORMANSI BIOMETRIJSKIH SISTEMA

10.1 Pregled postojećih rešenja

Jedan pristup evaluaciji jeste izračunavanje odgovarajućih parametara i kreiranje vizuelizacija za svaku konkretnu kombinaciju biometrijskih baza, unimodalnih algoritama za rad sa biometrijskim podacima, kao i multimodalnih algoritama za fuziju informacija [94] [92] [97]. U slučaju primene ovakvog načina evaluacije multimodalnih biometrijskih sistema, za uvođenje novih paramatera, vizuelizacija ili setova biometrijskih podataka potrebno je značajno ulaganje vremena.

Drugi pristup evaluaciji koji je prisutan jeste pomoću razvoja odgovarajućih alata i platformi. U okviru disertacije [183] dat je prikaz MUBI (eng. *MultiBiometric*) alata. Alat je razvijen u programskom jeziku JAVA i bavi se analizom uticaja različitih algoritama za normalizaciju i fuziju. Otvorenog je koda i ima modularnu arhitekturu. Alat isključivo podržava rad sa fuzijom na nivou skorova. Za dodavanje modaliteta potrebno je izračunati skorove pravih korisnika (eng. *genuine*) i uljeza (eng. *imposter*) i u okviru tekstualnih fajlova ih ubaciti u MUBI alat. Učitavanje biometrijskih podataka iz baze, pretprocesiranje, generisanje karakteristika i odgovarajućih skorova poređenja potrebno je uraditi odvojeno, van okvira ovog alata. Moguća je i analiza raspodela skorova poređenja. Alat je dizajniran za evaluaciju multimodalnih biometrijskih sistema u režimu verifikacije.

Autori rada [184] razvili su BEAT platformu za evaluaciju algoritama mašinskog učenja i prepoznavanja paterna. Platforma ima veb interfejs i otvorenog je koda. Rezultate eksperimenata sa platforme moguće je eksportovati preko REST API-ja, a funkcionalnosti je moguće koristiti i iz veb pretraživača. Eksperimenti u okviru platforme se konfigurišu kao niz grafičkih blokova sa određenim funkcionalnostima (eng. *toolchain).* Algoritmi i baze podataka predstavljene su kao blokovi sa odgovarajućim nazivima, ulazima i izlazima. Eksperimente je moguće beležiti i kasnije pretraživati po određenim parametrima. Moguće je dodavanje novih algoritama na platformu, ali samo ukoliko su pisani u programskom jeziku C i mogu se kompajlirati u kombinaciji sa komponentama platforme. Za potrebe rada sa biometrijskim podacima, od vizuelizacija evaluacije dostupni su histogrami skorova poređenja i ROC krive, tako da je primaran fokus razvoja ove platforme bila evaluacija biometrijskih sistema u verifikacionom režimu rada.

Ukoliko je potrebno izvršiti evaluaciju sistema za koji nije poznat korišćeni algoritam, već samo biometrijski sistem koji funkcioniše po principu crne kutije, klasičnu tehnološku evaluaciju nad nekom od otvorenih baza biometrijskih podataka nije moguće izvršiti. U radu [185] dat je predlog protokola za evaluaciju preciznosti ovog tipa sistema. Evaluacija protokola je izvršena kako nad unimodalnim, tako i nad multimodalnim biometrijskim sistemom koji je od modaliteta koristio glas i otisak prsta. Za konkretan scenario korišćenja, primenom protokola određeni su FAR i FRR parametri sistema.

U literaturi se pod terminom okvira (eng. *framework*) za multimodalnu biometriju ponekad predstavljaju predlozi arhitekture konkretnog multimodalnog biometrijskog

sistema. Ovakvi predlozi često su vezani i za konkretne kombinacije biometrijskih modaliteta [186] [187] [188]. U radu [186] predstavljen je predlog fuzije modaliteta lica i otiska prsta na nivou ekstrakcije karakteristika. Dat je predlog arhitekture sistema, a prilikom evaluacije nad kimeričkim setom podataka prikazani su FAR, FRR i EER parametri, kao i date ROC krive. Kombinacija fuzije biometrijskih modaliteta glasa, lica i potpisa opisana je u radu [187]. Fuzija je izvršena na nivou skorova, a kao parametar evaluacije korišćene su vrednosti EER metrike. U slučaju rada [188] predložena je šema za adaptivnu fuziju na nivou skorova, gde je moguće izvršiti optimizaciju težinskih faktora i algoritama za fuziju na osnovu željenog ponašanja sistema. Metoda je evaluirana nad nekoliko kombinacija biometrijskih modaliteta i to nad irisom i otiskom šake, licem i govorom kao i otiskom prsta i šake.

U određenim situacija termin okvir (eng. *framework*) se koristi i prilikom opisa arhitekture biometrijskog rešenja specijalno dizajnirane za primenu u konkretnom poslovnom domenu. Na primer, u radu [189] predstavljena je arhitektura multimodalnog biometrijskog rešenja namenjenom onlajn bankarstvu i ATM uređajima. Predloženi pristup kombinuje „meke“ (eng. *soft*) biometrijske modalitete sa tradicionalnim kao što su lice i otisak prsta.

Na osnovu pregleda literature možemo zaključiti da postoji prostor za unapređenja u odnosu na rešenja opisana u dostupnoj literaturi. Pod terminom okvir često se predstavljaju rešenja koja imaju fokus na određeni domen ili konkretne kombinacije biometrijskih modaliteta. Sa druge strane, postojeći alati za evaluaciju multimodalnih biometrijskih sistema fokusiraju se pre svega na evaluaciju performansi biometrijskog sistema koji radi u režimu verifikacije [183] [184]. Pored ovoga, javljaju se i ograničenja alata na rad sa algoritmima pisanim samo u određenom programskom jeziku [184], ili zavisnost od drugih rešenja za generisanje skorova potrebnih za evaluaciju [183]. U nastavku ovog poglavlja biće opisan predlog rešenja koje ima za cilj prevazilaženje opisanih problema.

10.2 MMBio – Okvir za razvoj multimodalnih biometrijskih sistema

Za realizaciju jednog multimodalnog biometrijskog sistema, potrebne su različite komponente. Rešenja za rad sa unimodalnim biometrijskim modalitetima, moduli za fuziju informacija, biometrijski senzori i prateći softver, baze biometrijskih podataka neophodni su delovi svakog multimodalnog biometrijskog sistema.

Jedan od pristupa razvoju multimodalnog biometrijskog sistema jeste razvoj svih komponenti sistema od nule, bez korišćenja tuđeg koda i rešenja. Ovakav pristup eventualno može biti izvodljiv za veće kompanije koje razvijaju komercijalna rešenja, ili pak državne institucije sa značajnijim budžetima. Prva značajna mana *in-house* razvoja na način koji je opisan jeste visoka cena takvog rešenja. Pored toga, postoji i drugi potencijalni problem, a to je manjak interoperabilnosti takvog sistema.

Ovde se postavlja pitanje šta se zapravo podrazumeva pod terminom interoperabilnost. Termin interoperabilnosti javlja se u različitim kontekstima. IEEE rečnik opisuje interoperabilnost kao sposobnost dva ili više sistema ili komponenti da razmenjuju informacije, kao i da koriste informacije koje su razmenili [190]. U radu [191] identifikovani su različiti mogući nivoi interoperabilnosti poslovnih sistema. To su

interoperabilnost na nivou podataka, resursa i poslovnih procesa. Kao rezultat, u zavisnosti od nivoa interoperabilnosti, mogući oblici integracije između sistema variraju od koordinacije između različitih organizacija, do direktne fizičke integracije sistema.

U užem kontekstu softverskih sistema, jedna od prvih opšte prihvaćenih definicija intereoperabilnosti data je od strane Petera Vegnera [192], koji je opisuje kao sposobnost dve ili više softverskih komponenti da sarađuju bez obzira na razlike u programskom jeziku, interfejsu i platformi za izvršavanje. Kako su biometrijski sistemi potkategorija softverskih sistema, kontekst interoperabilnosti u oblasti biometrije potpada pod ovu definiciju, uz naravno određena proširenje pre svega kada su u pitanju specifičnosti vezane za obradu biometrijskih podataka.

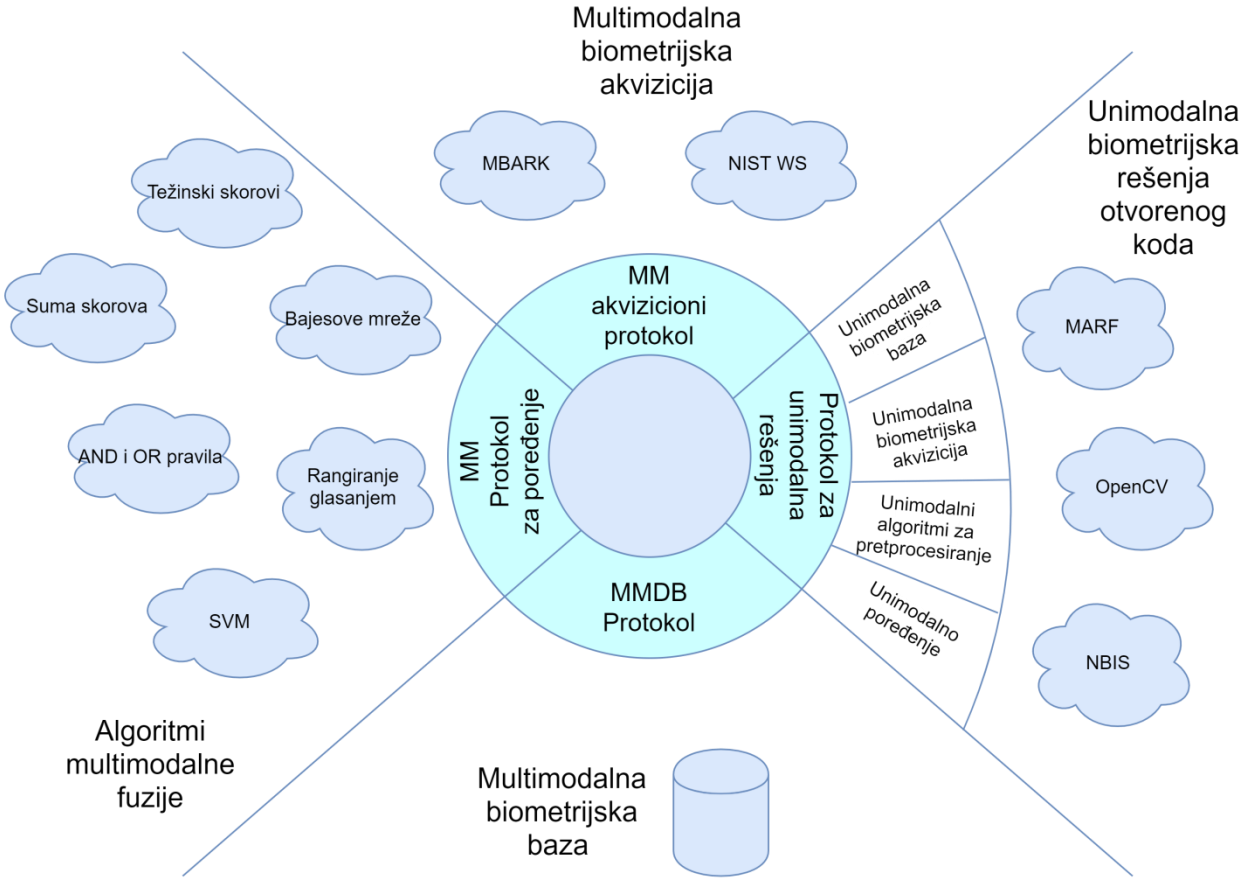
Pokušaja rešavanja problema interoperabilnosti u biometriji pomoću definisanja standarda ili razvojnih okvira bilo je nekoliko. Najznačajnija rešenja su:

- CBEFF (*Common Biometric Exchange File Format*) [193]
- MBARK (*Multimodal Biometric Application Resource Kit*) [194]
- BioAPI (*Biometric Application Programming Interface*) [195]
- WS-BD (*Web Services for Biometric Devices*) [196]
- OASIS BIAS (*OASIS Biometric Identity Assurance Services*) [197]

NIST i BioAPI konzorcijum sa BioAPI standardom pokušali su da definišu arhitekturu i interfejse potrebne za rad biometrijskih uređaja i sistema. Ovaj standard u osnovi ima dva problema – zasnovan je na upotrebi programskog jezika C i ne uključuje razmatranje problema iz ugla servisno orijentisanih arhitektura. Organizacije koje su učestvovale u formiranju i usvajanju ovog standarda, takođe su bile uključene u radu na CBEFF standardu. Ovaj standard se bavi pre svega razmenom biometrijskih podataka između različitih sistema. Njegov fokus je na višem nivou apstrakcije, odnosno na standardizaciji načina čuvanja biometrijskih podataka, pre nego na konkretnom formatu za skladištenje biometrijskih karakteristika.

NIST je takođe bio pokretač još jedne inicijative za standardizaciju u ovoj oblasti a to je WS-BD. Ovaj standard se fokusirao pre svega na biometrijske senzore i akviziciju biometrijskih podataka. Standardni internet protokoli (HTTP, Oauth, OpenID) upotrebljeni su prilikom definisanja ovog standarda. Još jedan projekat bitan za standardizaciju procesa akvizicije u biometrijskim sistemima razvijen je u okviru NIST-a, a to je MBARK. Glavni doprinos ovog projekta jeste definisanje domenski specifičnog progamskog jezika za opis procesa akvizicije.

Kod nabrojanih pristupa možemo uočiti dva nedostatka. Prvi jeste da se većina standarda i okvira fokusira na određeni deo procesa biometrijskog prepoznavanja. Na primer, MBARK se bavi isključivo procesom akvizicije biometrijskih podataka. Drugi nedostatak jeste slaba prihvaćenost ponuđenih standarda. Ovo je posebno česta situacija kod rešenja baziranih na tehnologiji otvorenog koda. Kako autori najčešće razvijaju rešenja u svoje slobodno vreme, ili pak uz relativno skromna raspoloživa sredstva, njihov fokus su uglavnom funkcionalne karakteristike rešenja, pre nego zadovoljenje postojećih standarda.

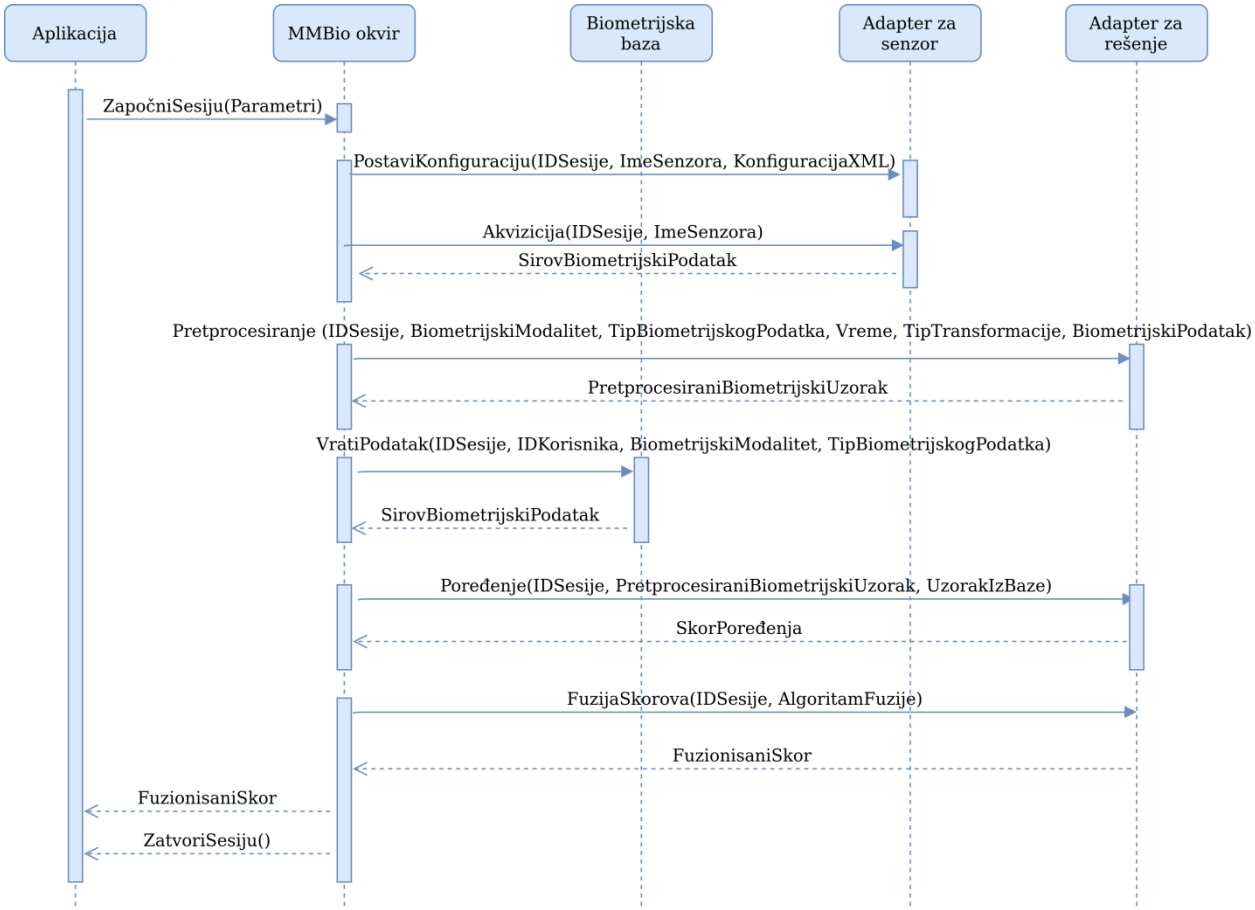


Slika 25 – Šematski prikaz okvira za razvoj multimodalnih biometrijskih sistema [5]

Kako bi se rešio problem interoperabilnosti između rešenja otvorenog koda, na Fakultetu organizacionih nauka, u Laboratoriji za multimedijalne komunikacije, kreiran je MMBio okvir za razvoj multimodalnih biometrijskih sistema[1] [5]. Šematski prikaz okvira dat je na slici 25.

MMBio okvir obezbeđuje međusobnu komunikaciju između senzora za akviziciju, unimodalnih biometrijskih rešenja, baza biometrijskih podataka i modula za poređenje i fuziju informacija. Komunikacija se vrši uz pomoć predefinisanih komunikacionih protokola. Ovaj pristup omogućava platformsku nezavisnost, za razliku od pristupa koji se zasnivaju na serijalizaciji objekata. Protokol je moguće implementirati za različite platforme kao i rešenja. U sličaju da rešenja ne podržavaju direktan rad sa protokolom, translacija komandi protokola u komande koje rešenje razume vrši se uz pomoć specijalno razvijenog komunikacionog adaptera [198].

[1] MMBio okvir je jedan od rezultata projekta Ministarstva prosvete, nauke i tehnološkog razvoja TR32013 - Primena multimodalne biometrije u menadžmentu identiteta,



Slika 26 – Prikaz scenarija verifikacije biometrijskih podataka pomoću MMBio okvira [198]

Na slici 26 prikazan je jedan moguć scenario upotrebe MMBio okvira. Aplikacija započinje verifikacionu sesiju prosleđivanjem željenih parametara konfiguracije okviru. Okvir vrši konfiguraciju senzora. Po uspešnoj konfiguraciji biometrijskog senzora, vrši se akvizicija, i adapter za senzor vraća okviru sirovi biometrijski podatak. Ukoliko je potrebno, u okviru scenarija vrši se pretprocesiranje. Adapteru za unimodalno biometrijsko rešenje prosleđuju se sirovi biometrijski podaci, tip transformacije, vreme zahteva, podaci o tipu biometrijskog podatka i biometrijskog modaliteta, kao i identifikator sesije. Adapter za rešenje po dobijanju zahteva izvršava zadati zadatak i prosleđuje okviru nazad pretprocesirani biometrijski podatak. Po pretprocesiranju, vrši se poređenje biometrijskih podataka dobijenih akvizicijom sa onima koji se nalaze u bazi podataka. Potom se od koraka konfiguracije senzora do koraka poređenja postupak ponavlja za sve biometrijske modalitete u upotrebi. Po dobijanju poređenja za pojedinačne modalitete, vrši se fuzija podataka, dobija fuzionisani skor i završava sesija.

Primenjen je sinhroni model komunikacije, rešenju se šalje zahtev i čeka odgovarajući odgovor, kao u uobičajenoj klijent-server paradigmi [199]. Implementaciju komunikacionog protokola moguće je izvršiti na različite načine [199]. Moguće je koristiti sokete, veb servise ili pak neko rešenje poput RPC (*eng. Remote Procedure Call*). Protokol je trenutno implementiran pomoću REST (*eng. Representational State Transfer*) servisa [199]. Primer protokolne poruke i odgovora dat je u tabelama 14 i 15.

Tabela 14 – Polja zaglavlja u *Verify* zahtevu [198]

Polje	Tip polja	Obavezno	Objašnjenje
IDKorisnika	Integer	DA	ID korisnika čiji je biometrijski uzorak potrebno verifikovati.
BiometrijskiTip	String	DA	Biometrijski modalitet(otisak prsta, lice, ...).
BiometrijskiPodtip	String	NE	Dodatni opis biometrijskog modaliteta u okviru definisanog tipa.
NačinProcesiranja	{sirov, procesiran, ...}	DA	Nivo procesiranja koji je primenjen na biometrijski uzorak.
VremeKreiranja	Date/Time	DA	Vreme kada je biometrijski uzorak prikupljen.

Tabela 15 – Polja zaglavlja u *Verify* odgovoru [198]

Polje	Tip polja	Obavezno	Objašnjenje
StatusniKod	Integer	DA	Statusni kod koji označava rezultat izvršenog zahteva.
StatusnaPoruka	String	NE	Propratna poruka koja zavisi od vrednosti polja StatusniKod.
RezultatVerifikacije	Double	DA	Poruka koja označava rezultat verifikacije.

10.3 Korisnički zahtevi za evaluaciju performansi multimodalnog biometrijskog sistema

U okviru sistema za evaluaciju performansi multimodalnog biometrijskog sistema možemo primetiti dve uloge - korisnika sistema i biometrijskog inženjera. Iako ove dve uloge nisu nužno nespojive, kako bismo postigli preciznu definiciju zahteva jednog ovakvog sistema, neophodno je da ih razdvojimo. Korisnik sistema ima dva glavna scenarija korišćenja - evaluaciju poređenja i evaluaciju akvizicije.

Prilikom evaluacije poređenja, korisnik sistema može isprobati različite kombinacije algoritama, primeniti tehnike za pretprocesiranje, evaluirati samo određeni deo baze podataka, birati različite kombinacije biometrijskih modaliteta. Sve ove akcije dovode do različitih ponašanja biometrijskog sistema, što je moguće videti preko različitih vizuelizacija koje postoje.

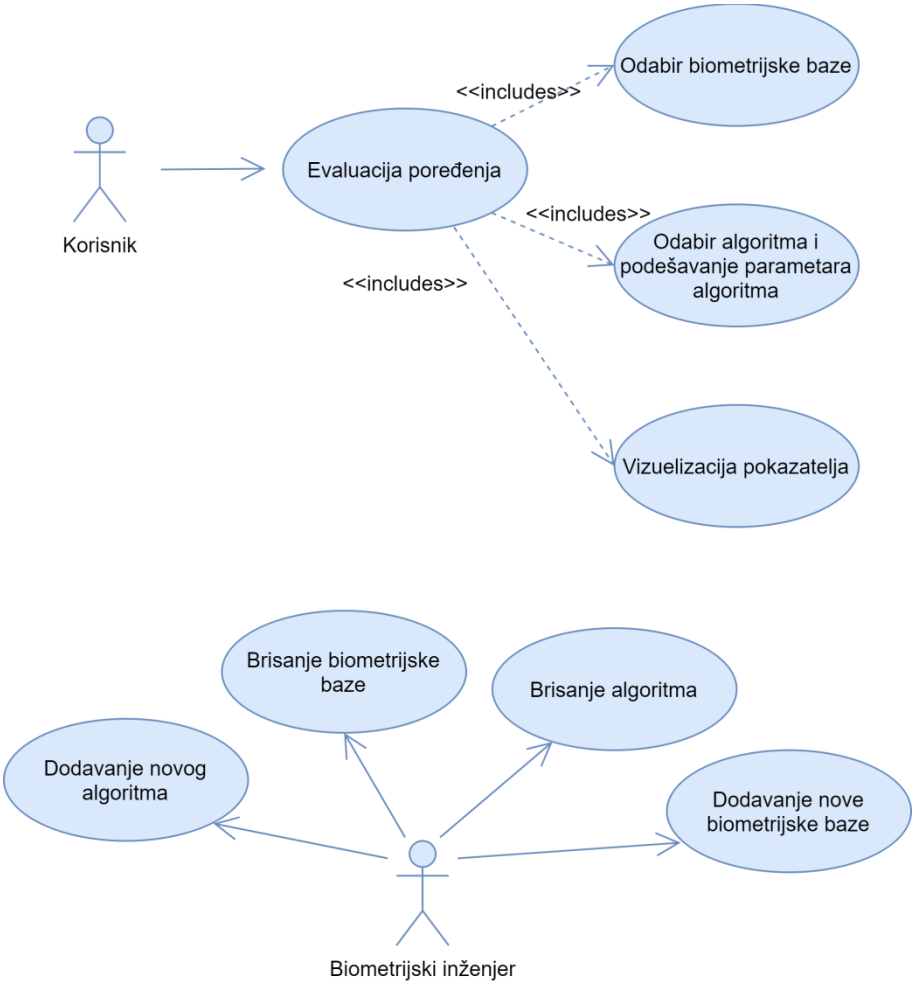
Biometrijski inženjer može dodati nov algoritam za poređenje ili ekstrakciju u bazu postojećih algoritama. U slučaju kada nova biometrijska baza podataka postane dostupna za evaluaciju, potrebno je povezati bazu sa sistemom za evaluaciju performansi. Kada za tom akcijom postoji potreba, može izvršiti i brisanje algoritma ili biometrijske baze sa sistema.

Scenario korišćenja Odabir biometrijske baze

1. Sistem prikazuje dostupne biometrijske baze podataka
2. Korisnik od ponuđenih bira željenu bazu za evaluaciju
3. Opciono: Korisnik bira određeni podskup podataka
4. Sistem prikazuje modalitete dostupne za odabranu bazu podataka
5. Korisnik bira željene biometrijske modalitete za evaluaciju

Scenario korišćenja Odabir algoritma i podešavanje parametara algoritma:

1. Korisnik bira tip algoritma (algoritam za pretprocesiranje, ekstrakciju karakteristika, poređenje, normalizaciju ili fuziju)
2. Sistem prikazuje raspoložive algoritme za određeni zadatak
3. Korisnik bira algoritam za željeni zadatak iz liste ponuđenih algoritama
4. Opciono: Korisnik unosi parametre za rad algoritma



Slika 27 – Dijagram slučajeva korišćenja evaluacije performansi multimodalnog biometrijskog sistema

Scenario korišćenja Vizuelizacija pokazatelja:

1. Sistem prikazuje raspoložive načine vizuelizacije podataka
2. Korisnik bira jedan od ponuđenih načina vizuelizacije rezultata
3. Opciono: Ukoliko su dostupni, korisnik podešava parametre vizuelizacije

Scenario korišćenja Evaluacija poređenja:

1. Korisnik vrši odabir jednog ili više biometrijskih modaliteta (**include** Odabir modaliteta)
2. Opciono: Ukoliko su dostupni za određeni modalitet, korisnik vrši odabir algoritama za pretprocesiranje biometrijskih podataka za odabrane modalitete i podešava njihove parametre (**include** Odabir algoritma i podešavanje parametara algoritma)
3. Korisnik vrši odabir i podešavanje parametara algoritama za ekstrakciju biometrijskih podataka za odabrane modalitete (**include** Odabir algoritma i podešavanje parametara algoritma)
4. Korisnik vrši odabir i podešavanje parametara algoritama za poređenje biometrijskih karakteristika za odabrane modalitete (**include** Odabir algoritma i podešavanje parametara algoritma)
5. Korisnik vrši odabir algoritma za normalizaciju (**include** Odabir algoritma i podešavanje parametara algoritma)
6. Korisnik vrši odabir algoritma za fuziju informacija (**include** Odabir algoritma i podešavanje parametara algoritma)
7. Korisnik definiše željene načine prikaza izračunatih pokazatelja (**include** Vizuelizacija pokazatelja)
8. Sistem vrši izračunavanje pokazatelja primenom zadatih algoritama i modaliteta
9. Sistem prikazuje izračunate parametre i prezentuje ih pomoću izabranih načina prikaza

Scenario korišćenja Dodavanje nove biometrijske baze

1. Biometrijski inženjer odabira modalitet nove biometrijske baze iz ponuđene liste
2. Biometrijski inženjer unosi podatke o bazi podataka (broj osoba u bazi, biometrijski modaliteti, instance modaliteta, broj uzoraka za modalitet, format uzoraka)
3. Sistem proverava da li se format baze poklapa sa zahtevima i datim podacima
4. Sistem pokazuje potvrdu o uspešnom dodavanju nove baze podataka

Alternativni scenario:

4a. Sistem prikazuje grešku ukoliko neka od provera nije uspešno završena

Scenario korišćenja Dodavanje novog biometrijskog algoritma

1. Biometrijski inženjer odabira modalitet novog biometrijskog algoritma iz ponuđene liste
2. Biometrijski inženjer unosi metapodatke o algoritmu
3. Sistem proverava da li se interfejs algoritma poklapa sa sistemom i unetim metapodacima
4. Sistem pokazuje potvrdu o uspešnom dodavanju novog algoritma

Alternativni scenario:

4a. Sistem prikazuje grešku ukoliko interfejs algoritma nije odgovarajući

Scenario korišćenja Brisanje algoritma

1. Biometrijski inženjer iz liste ponuđenih algoritama bira algoritam za brisanje
2. Sistem obaveštava predavača da je potrebno da potvrdi brisanje
3. Biometrijski inženjer daje potvrdu za brisanje algoritma
4. Sistem briše algoritam iz baze

Alternativni scenario:

3.a Biometrijski inženjer odustaje od brisanja algoritma

Scenario korišćenja Brisanje biometrijske baze

1. Biometrijski inženjer iz liste ponuđenih biometrijskih baza bira bazu za brisanje
2. Sistem obaveštava predavača da je potrebno da potvrdi brisanje
3. Biometrijski inženjer daje potvrdu za brisanjem biometrijske baze
4. Sistem uklanja biometrijsku bazu i briše podatke

Alternativni scenario:

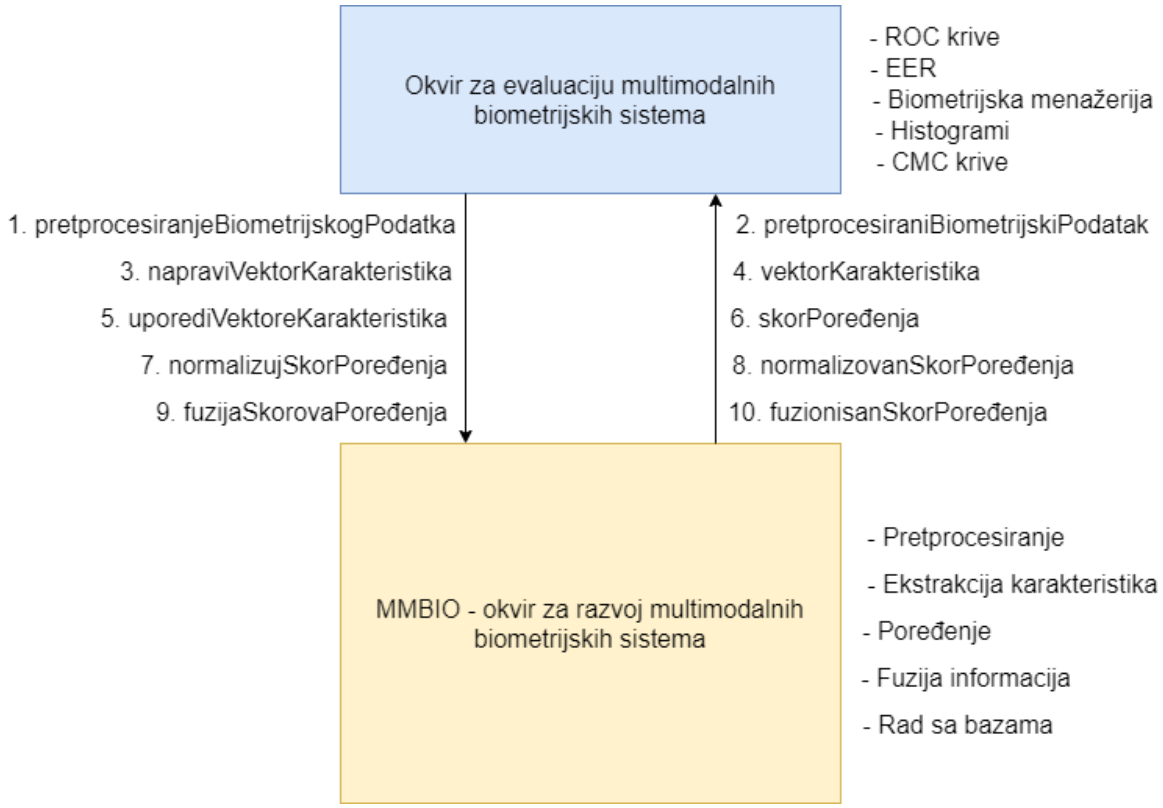
3.a Biometrijski inženjer odustaje od brisanja biometrijske baze

10.4 Arhitektura okvira za evaluaciju performansi multimodalnog biometrijskog sistema

Na osnovu definicije korisničkih zahteva za evaluaciju performansi multiomodalnih biometrijskih sistema, možemo zaključiti da je potrebno razviti generički način za

prikaz, vizuelizaciju parametara i određivanje praga osetljivosti multimodalnog biometrijskog sistema. Implementacija ovih funkcionalnosti za svaki pojedinačni biometrijski sistem koji se evaluira bila bi redundantna aktivnost.

Kako bi se uopšte moglo doći do neophodnih podataka za vizuelizaciju i određivanje parametara, potrebno je izvršiti značajan broj operacija pretprocesiranja, ekstrakcije karakteristika, poređenja i fuzionisanja dobijenih rezultata. Takođe, čak i kod unimodalnog sistema, mogući su izbori različitih kombinacija parametara za pretprocesiranje, ekstrakciju karakteristika i poređenje. Pored toga, moguća su i testiranja sistema nad različitim biometrijskim bazama podataka.



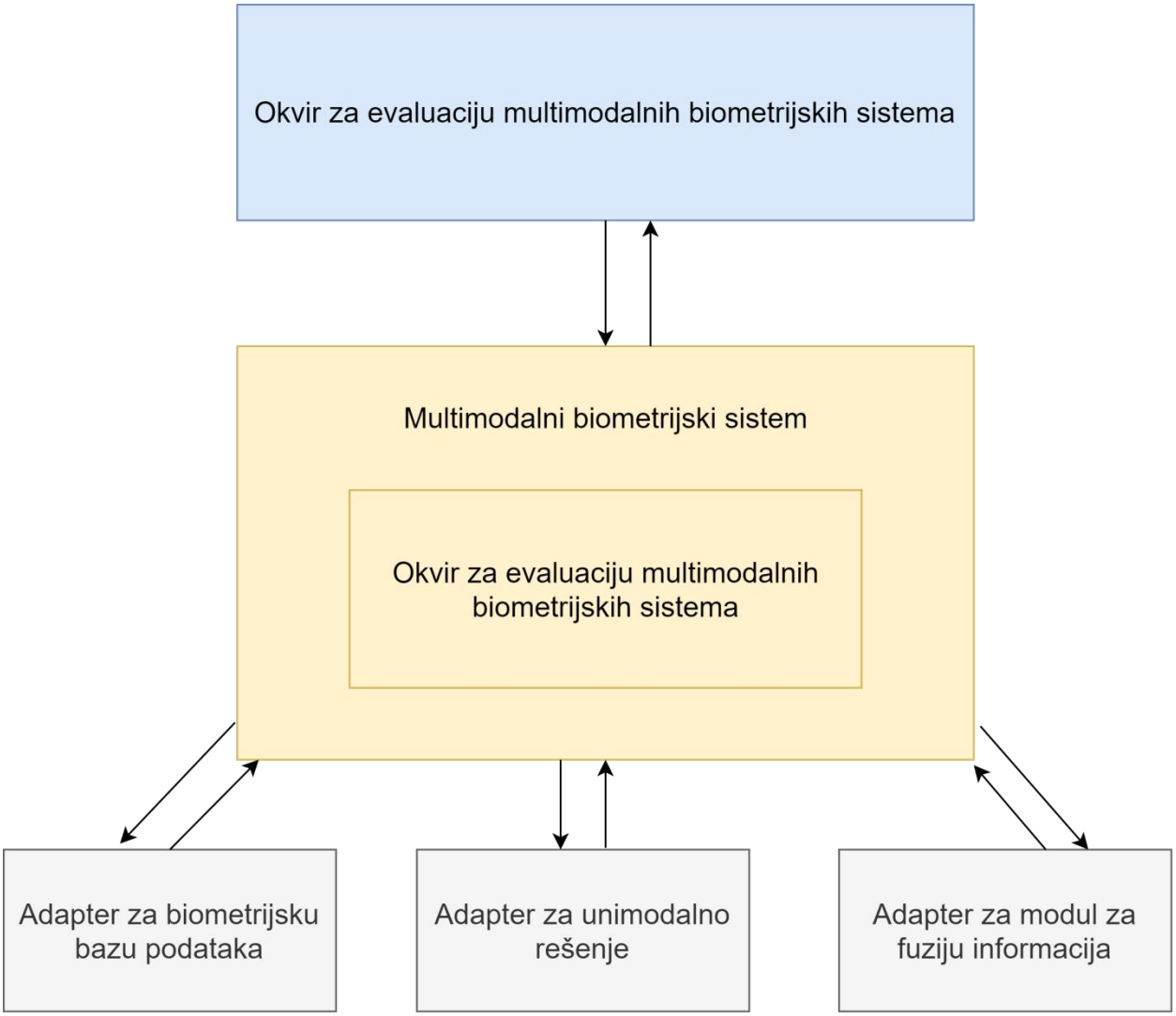
Slika 28 – Odnos između okvira za evaluaciju i okvira za razvoj multimodalnih biometrijskih sistema

U slučaju multimodalnog biometrijskog sistema, evaluacija se dodatno komplikuje izborom modaliteta, kao i načina fuzije informacija dobijenih od pojedinačnih biometrijskih modaliteta. Broj mogućih kombinacija različitih podešavanja sistema se dodatno povećava, i pronalaženje željenih podešavanja za određeni slučaj korišćenja postaje sve zahtevniji zadatak.

Kako bi se razrešile ove poteškoće, zadaci vezani za evaluaciju se mogu uopštiti pomoću okvira za evaluaciju multimodalnih biometrijskih sistema. Razvojem ovakvog okvira, jednom razvijene funkcionalnosti vezane za evaluaciju biometrijskih sistema mogu se ponovo iskoristiti na drugim konkretnim primerima. Osnovu za razvoj okvira predstavljao je objedinjeni model evaluacije multimodalnih biometrijskih sistema, a rad okvira prati predloženi proces razvoja i evaluacije multimodalnih biometrijskih sistema. Implementacija okvira za evaluaciju multimodalnih biometrijskih sistema izvršena je u programskom jeziku JAVA.

Za potrebe direktnih manipulacija biometrijskim podacima, upotrebljen je MMBio – okvir za razvoj multimodalnih biometrijskih sistema. Na taj način se deo zadataka vezan za pretprocesiranje, ekstrakciju karakteristika, poređenje, fuziju informacija i rad sa bazama rešava primenom MMBio okvira. Okvir za evaluaciju multimodalnih biometrijskih sistema ima fokus na različite načine vizuelizacije i izračunavanja izvedenih parametara dobijenih na osnovu poređenja primenom MMBio okvira. Odnos između ova dva okvira prikazan je na slici 28, na kojoj je i dat prikaz funkcija koje okvir za evaluaciju multimodalnih sistema poziva. Rednim brojevima je označen okviran redosled poziva funkcija i pratećih odgovora MMBio okvira.

Primenom MMBio okvira možemo evaluirati jedan multimodalni biometrijski sistem, koji sa jedne strane ima interfejs prema okviru za evaluaciju multimodalnih biometrijskih sistema, dok sa druge strane komunicira sa odgovarajućim adapterima izrađenim za unimodalna rešenja i baze biometrijskih podataka. Prikaz odnosa opisanih komponenti možemo videti na slici 29.



Slika 29 – Odnos između okvira za evaluaciju, unimodalnih rešenja i baze podataka

10.5 Studija slučaja – evaluacija performansi multimodalnog biometrijskog sistema

Za evaluaciju multimodalnog biometrijskog sistema upotrebljena je multimodalna baza biometrijskih podataka prikupljena na Fakultetu organizacionih nauka [136]. Od biometrijskih modaliteta ispitane su performanse lica i otiska prsta, pojedinačno, kao i u kombinaciji. Fuzija informacija izvršena je na nivou skorova, gde je modul za fuziju informacija sadržao algoritme opisane u radu [176], konkretno *MinMax* i *Tanh* algoritme normalizacije, kao i *SimpleSum* i *UserCoefficient* algoritme fuzije. Navedeni rad je jedan od najcitiranijih na ovu temu, a usled jednostavnosti implementacije, nabrojani algoritmi se često koriste prilikom evaluacije performansi multimodalnih biometrijskih sistema, kao na primer u radu [200]. Prilikom određivanja članova biometrijske menažerije, upotrebljen je pristup iz rada [122].

Za rad sa otiskom prsta odabrano je rešenje otvorenog koda *SourceAFIS* [201]. Ono omogućava ekstrakciju minucija sa otiska prsta, kao i poređenje otisaka prstiju na osnovu pronađenih minucija. Poređenje se vrši tako što rešenje formira tabelu parova minucija – tabelu ivica. Ivicu čine dve minucije, njihovo odstojanje, kao i uglovi u odnosu na pravu koja ih spaja. Prednost ovakvog pristupa jeste invarijantnost na rotaciju i pomeraje slike otiska prsta [202]. Rešenje omogućava rad sa programskim jezicima JAVA i C#. Algoritam za ekstrakciju minucija je dizajniran tako da promoviše transparentnost, jer omogućava serijalizaciju i uvid u međustanja tokom izvršavanja koraka algoritma. Sam interfejs biblioteke je dobro dokumentovan i jednostavan za korišćenje.

Prilikom ekstrakcije podataka i poređenja slika lica upotrebljeno je unimodalno rešenje razvijeno uz pomoć *OpenCV* frejmvorka [203]. Ovaj okvir pruža gradivne elemente za razvoj različitih sistema računarske vizije, koji se mogu primeniti prilikom razvoja biometrijskih sistema. Za detekciju pozicije lica na slici koristi se HAAR klasifikator [204]. Po detekciji lica, određuju se koordinate očiju primenom LBF metode za detekciju ključnih tačaka lica [205] i na osnovu njih se vrši standardizacija sadržaja i rotacija isečka koji se koristi za ekstrakciju karakteristika. Za ekstrakciju se koristi LBP algoritam [49], uz upotrebu hi kvadrat distance [175] za poređenje vektora.

10.5.1 Registracija dostupnih algoritama i baza podataka

Kako bi bilo moguće izračunati skorove poređenja radi kreiranja odgovarajućih tekstualnih i vizuelnih evaluacija, potrebno je imati odgovarajuću strukturu biometrijske baze podataka. U slučaju kada baza biometrijskih podataka nije realizovana kao nezavisan modul, potrebno je dati i putanje do odgovarajućih biometrijskih podataka u bazi. Ovo se radi pomoću odgovarajućeg XML fajla, kao što je prikazano na slici 30. Okvir za evaluaciju multimodalnih biometrijskih sistema učitava opis baze i na osnovu njega vrši dalju evaluaciju.

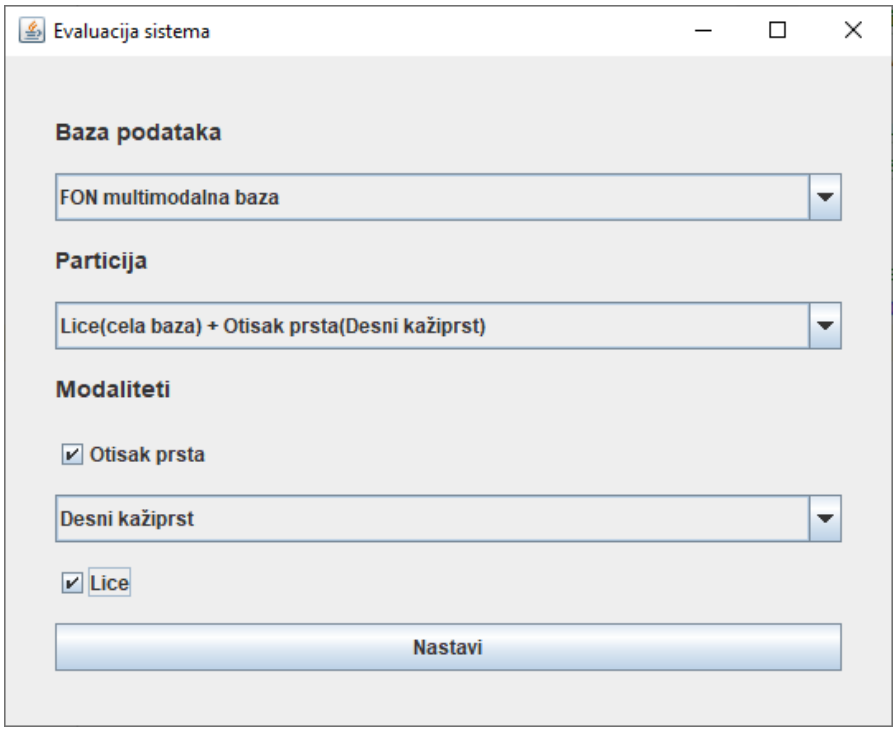
Slika 30 – Struktura baze podataka opisana pomoću XML dokumenta

Takođe, kako bi se prosledili odgovarajući parametri MMBio okviru za komunikaciju sa unimodalnim rešenjima i generisao interfejs za odabir opcija evaluacije, potrebno je opisati algoritme koji mogu biti korišćeni u evaluaciji, njihove modalitete, tip algoritma, eventualne opcije pretprocesiranja, kao i tipove ulaznih i izlaznih podataka. Deo XML fajla koji sadrži tražene informacije prikazan je na slici 31.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<algorithms>
    <algorithm id="1"...>
    <algorithm id="2">
        <name>SourceAfis</name>
        <modality>Otisak prsta</modality>
        <type>Poređenje karakteristika</type>
        <location>127.0.0.1</location>
        <input>Minucije</input>
        <output>Skor sličnosti</output>
    </algorithm>
    <algorithm id="3">
        <name>Sečenje slike - HAAR i LBF</name>
        <modality>Lice</modality>
        <type>Pretprocesiranje</type>
        <location>127.0.0.1</location>
        <input>Slika</input>
        <output>Slika</output>
        <parametar name="sečenje">0.27</parametar>
        <parametar name="rezolucija">130 px</parametar>
    </algorithm>
    <algorithm id="4"...>
```

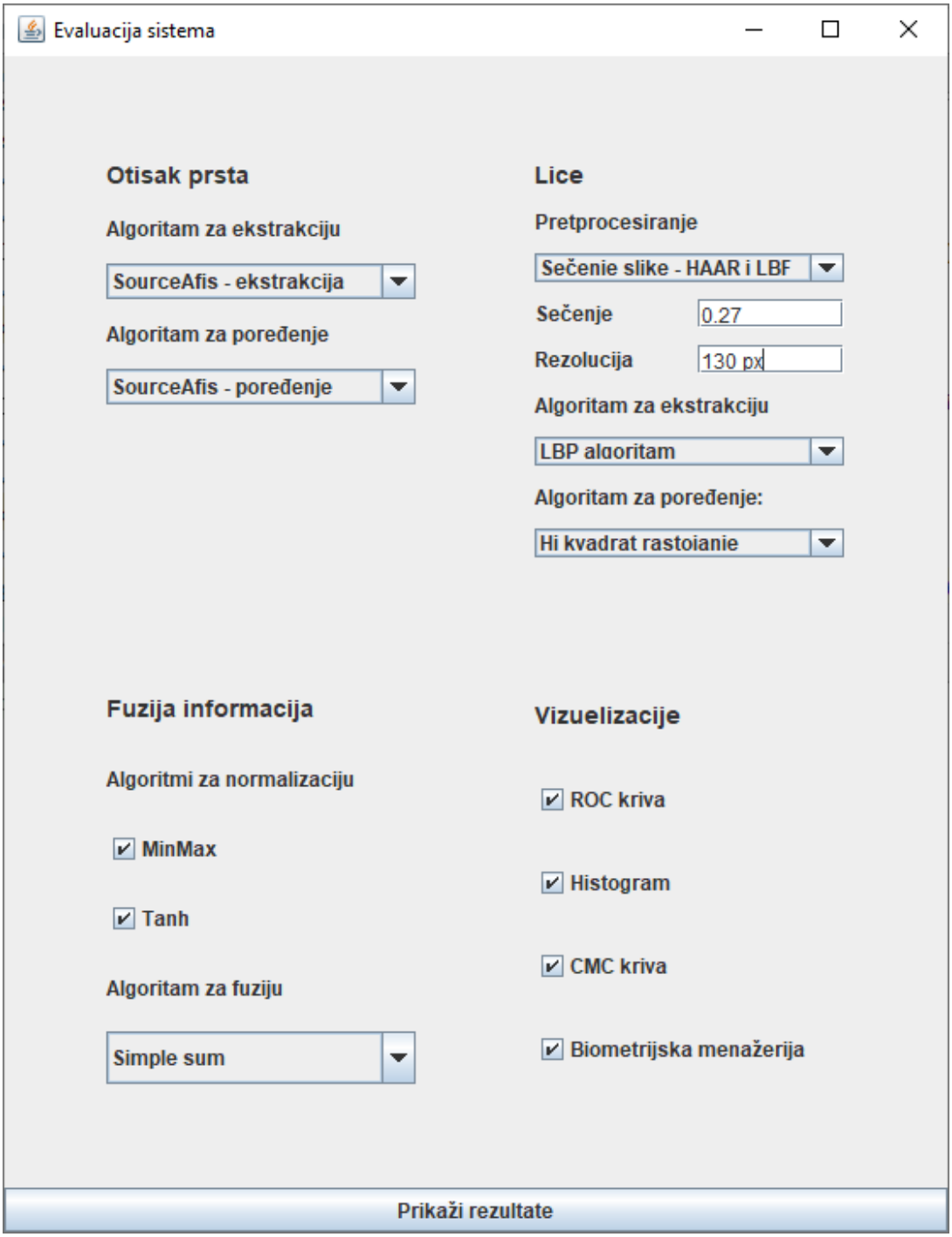
Slika 31 – XML fajl sa opisom algoritama za pretprocesiranje, ekstrakciju i poređenje biometrijskih karakteristika

10.5.2 Odabir parametara evaluacije i prikaz rezultata



Slika 32 – Interfejs za odabir baze i modaliteta

Za početak je potrebno odabrati biometrijsku bazu nad kojom će se vršiti evaluacija sistema (slika 32). U skladu sa odabranom biometrijskom bazom podataka, na grafičkom korisničkom interfejsu se prikazuju modaliteti dostupni u okviru odabrane baze. Ukoliko je za određeni modalitet dostupno više različitih particija baze, moguće je izabrati rad sa konkretnom particijom baze. Po odabiru opcija možemo nastaviti dalje na odabir i podešavanje algoritama i vizuelizacija. Forma za ovaj odabir prikazana je na slici 33.

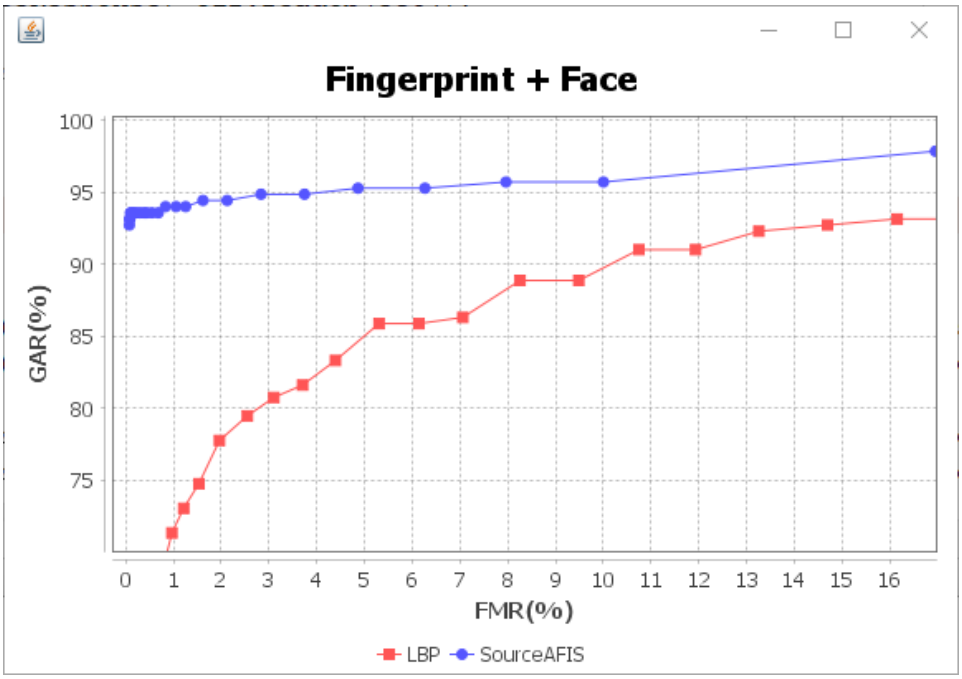


Slika 33 – Interfejs za odabir opcija evaluacije

Ovde se vrši odabir algoritama za ekstrakciju i poređenje za svaki od biometrijskih modaliteta, kao i algoritama za fuziju informacija. Ukoliko algoritam ima dodatne opcije, moguće je podesiti odgovarajuće parametre. Kao rezultat, za potrebe evaluacije sistema dobijamo ROC krive, CMC krive, histograme raspodela skorova poređenja, kao i podatke o broju članova određene kategorije biometrijske menažerije. Parametarski i grafički rezultati evaluacije prikazani su u naredna dva potpoglavlja, u okviru kojih je takođe dat osvrt na dobijene rezultate.

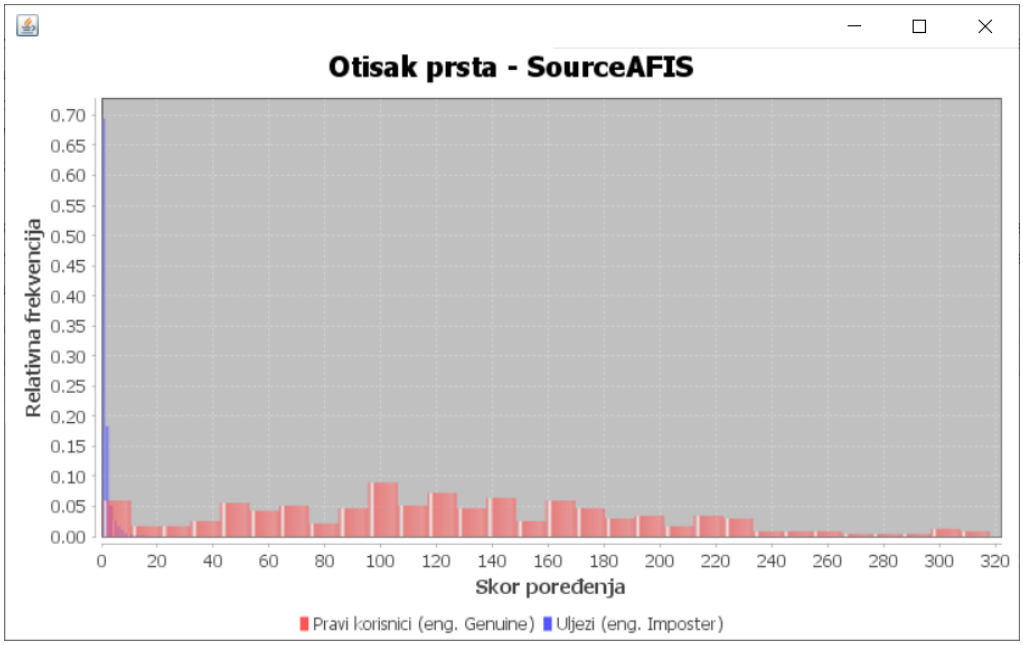
10.5.3 Performanse rada sistema u verifikacionom režimu rada

Pre evaluacije rada sistema u multimodalnom režimu rada potrebno je da razmotrimo performanse pojedinačnih modaliteta. Za početak, uvidom u ROC krive prikazane na slici 34 možemo izvršiti analizu preciznosti rada unimodalnih sistema. U skladu sa očekivanjima, otisak prsta ima bolje performanse od lica, a značajna razlika između modaliteta u ovom slučaju se može pripisati upotrebljenim algoritmima. Za ekstrakciju karakteristika lica koristimo LBP algoritam, koga karakterišu jednostavnost implementacije i visoka brzina izvršavanja, ali i niža preciznost prepoznavanja.



Slika 34 – ROC kriva koja prikazuje performanse pojedinačnih biometrijskih modaliteta

Međutim, iako je preciznost algoritma za prepoznavanje otiska prsta na višem nivou u odnosu na algoritam za prepoznavanje lica, na slici 34 možemo primetiti da je rast GAR metrike u odnosu na FMR spor, odnosno da tek značajno snižavanje praga osetljivosti dovodi do većeg smanjenja procenta odbijenih legitimnih korisnika sistema. Kako bismo bolje razumeli ponašanje *SourceAFIS* algoritma za poređenje otisaka prstiju na ovoj bazi podataka, možemo analizirati histograme raspodela skorova poređenja.



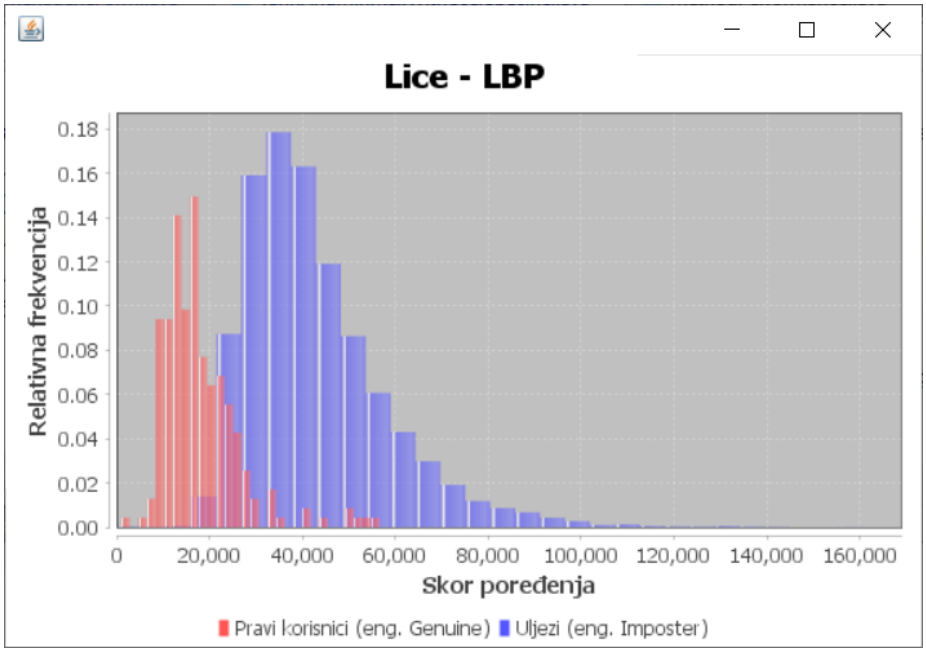
Slika 35 – Histogram raspodele skorova poređenja za biometrijski modalitet otisak prsta

SourceAFIS koristi skorove sličnosti, a njihovi histogrami su prikazani na slici 35. Skorovi poređenja uljeza (eng. *imposter*) su izrazito grupisani sa leve strane, gde su vrednosti skorova poređenja male. Ipak možemo primetiti i da određen procenat skorova poređenja dobijenih na osnovu biometrijskih podataka legitimnih korisnika takođe grupisan sa leve strane dijagrama (eng. *genuine*), što se i poklapa sa zaključcima koje možemo izvući sa ROC krive prikazane na slici 34. Dodatan uvid u ponašanje otiska prsta kao biometrijskog modaliteta možemo videti na slici 36, gde je data forma sa prikazom članova biometrijske menažerije.

Slika 36 – Forma sa prikazom biometrijske menažerije za otisak prsta, lice i različite kombinacije tehnika normalizacije i fuzije

Pojavu koza (eng. *goats*) kod otiska prsta možemo opravdati kombinacijom efekata loše akvizicije otiska prsta i potencijalne mogućnosti da osoba u bazi ima slabije izražene grebene otiska prsta, na primer usled posledica procesa starenja. Međutim, pojavu znatno većeg broja "jagnjadi" za otisak prsta u odnosu na lice potrebno je dodatno objasniti, pogotovu u situaciji kada na ROC krivi (slika 34) vidimo da je preciznost algoritma za poređenje otisaka prstiju na visokom nivou. Možemo primetiti takođe i visok broj jagnjadi kada posmatramo skorove dobijene fuzijom. Kako bismo bolje analizirali ove anomalije, potrebno je da se osvrnemo na metodologiju za izračunavanje članova biometrijske menažerije. U radu [122], kao način određivanja da li je neka osoba iz baze "jagnje" koriste se isključivo skorovi uljeza. Ukoliko je prosek najvećih skorova poređenja sa svakom od ostalih osoba iz baze veći od 90-tog percentila svih skorova iz raspodele uljeza (eng. *imposter*), osoba se smatra potencijalnim jagnjetom. Analizom histograma raspodele skorova otiska prsta prikazanog na slici 34, možemo videti relativno malu varijansu skorova uljeza. Kombinacija ove činjenice sa zapažanjem da je broj uzoraka iz baze relativno mali, objašnjava lakoću sa kojom se korisnici sistema označavaju kao "jagnjad". Sam algoritam u praksi dobro razdvaja raspodele skorova pravih i lažnih korisnika, što možemo lako uočiti sa histograma na slici 35.

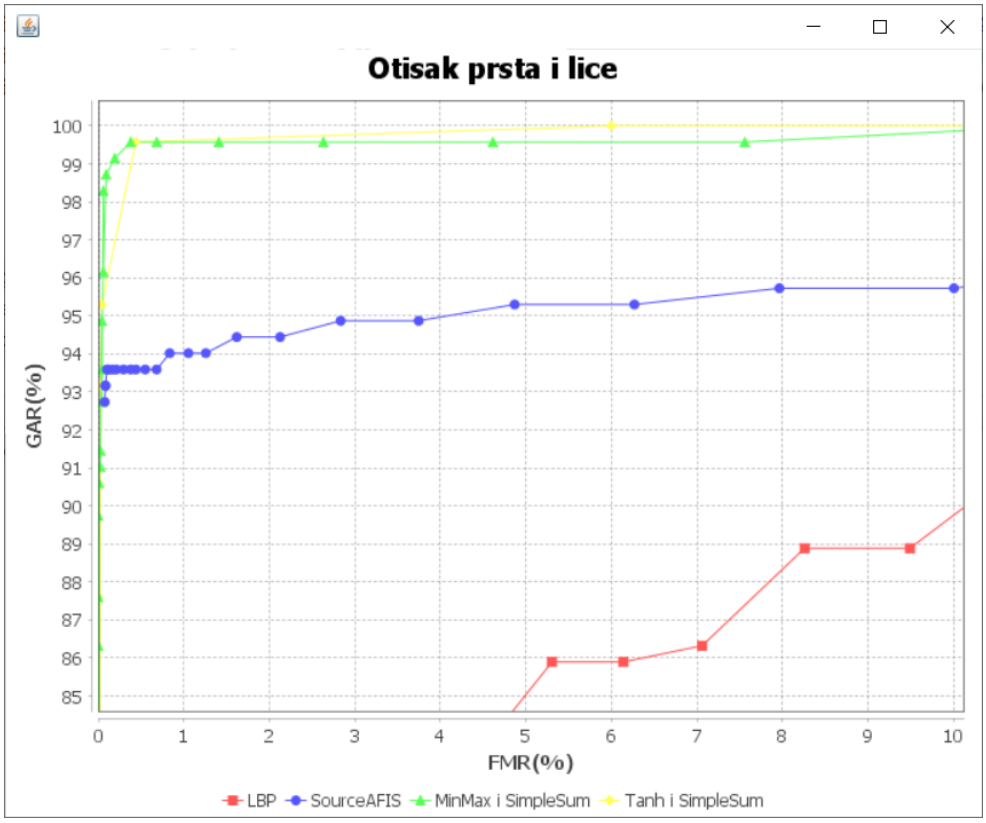
Histogram raspodele skorova za rešenje razvijeno uz pomoć *OpenCV* frejmvorka prikazan je na slici 37. Možemo primetiti značajno preklapanje raspodela skorova uljeza i legitimnih skorova. Ovo preklapanje raspodela u skladu je sa preciznošću ovog modaliteta prikazanom na ROC krivi na slici 34.



Slika 37 – Histogram raspodele skorova poređenja za biometrijski modalitet lice

Nakon sagledavanja svih dostupnih informacija o radu unimodalnih rešenja možemo zaključiti da je za verifikaciju osoba u ovom slučaju bolji izbor upotreba modaliteta otiska prsta uz primenu *SourceAFIS* rešenja u odnosu na upotrebu lica. Ipak, pošto je algoritam otvorenog koda u pitanju, preciznost rada algoritma za prepoznavanje otiska prsta u ovom slučaju nije idealna. Stoga, potrebno je razmotriti kakve performanse može imati sistem koji kombinuje podatke dobijene iz oba pomenuta biometrijska modaliteta.

Na slici 38 prikazana je ROC kriva koja prikazuje performanse *MinMax* i *Tanh* algoritama normalizacije uparenih sa *SimpleSum* algoritmom za fuziju informacija. Ovde možemo videti da oba odabrana algoritma za normalizaciju imaju približne performanse, kao i da se u oba slučaja dobijaju značajna poboljšanja preciznosti sistema. Upotrebom multimodalnog pristupa moguće je smanjiti mogućnost nastanka greške u značajnoj meri.



Slika 38 – ROC kriva koja prikazuje performanse *MinMax* i *Tanh* algoritama normalizacije skorova uparenih sa *SimpleSum* algoritmom za fuziju informacija

Na slici 39 možemo videti ROC krivu koja prikazuje performanse *MinMax* i *Tanh* algoritama normalizacije skorova uparenih sa *UserCoefficient* algoritmom za fuziju informacija. Ovde je preciznost *Tanh* normalizacije na sličnom nivou kao i u prethodno razmotrenom scenariju. Međutim *MinMax* normalizacija daje značajno lošije rezultate, koji su približno na nivou preciznosti upotrebe isključivo LBP algoritma za rad sa licem.

Pad performansi za drugu kombinaciju algoritama može delovati neočekivano, ali dubljom analizom oba upotrebljena algoritma, možemo utvrditi uzroke za takvo ponašanje. *MinMax* normalizacija osetljivija je na pojavu ekstremnih vrednosti skorova poređenja, dok *Tanh* normalizacija spada u takozvane robustne metode. Sa druge strane, prilikom kreiranja težinskih skorova za svakog korisnika, kod odabranog pristupa iz rada [176], koeficijenti ω_i^m (i-ti korisnik u bazi, m-ti biometrijski modalitet) se računaju na sledeći način:

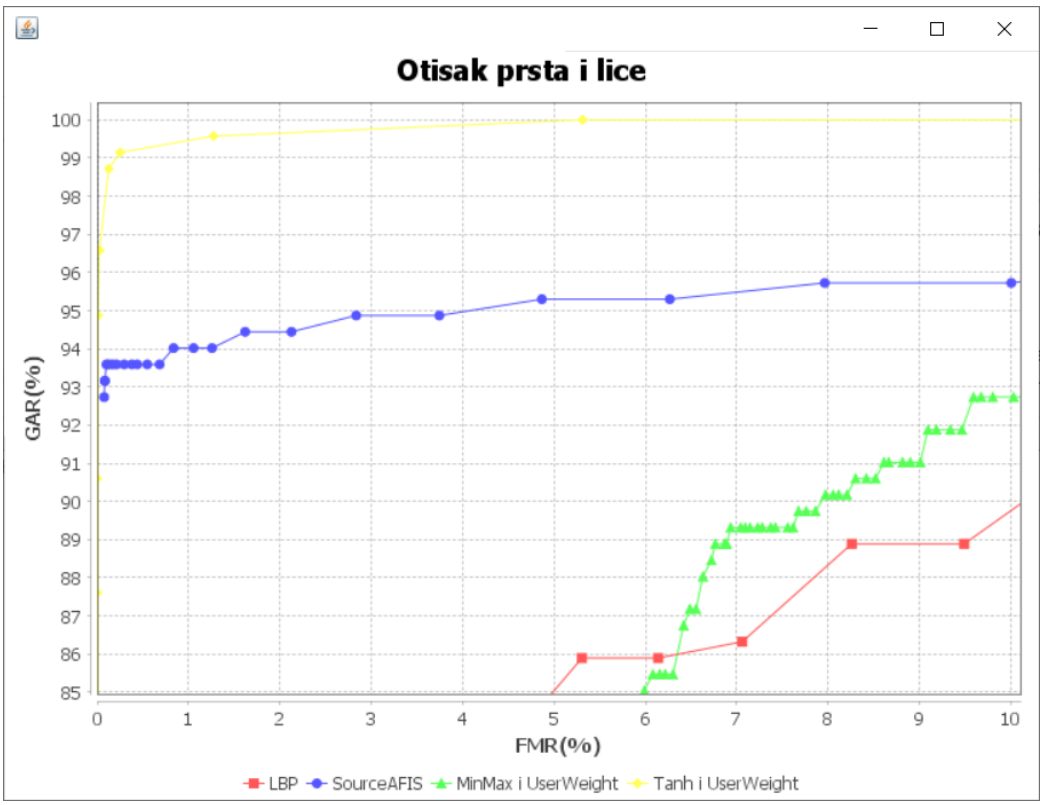
$$\omega_i^m = \frac{1}{\sum_{m=1}^{M} d_i^m} \times d_i^m$$

Vrednosti d_i^m se izračunavaju kao [176]:

$$d_i^m = \frac{\mu_i^m(gen) - \mu_i^m(imp)}{\sqrt{((\sigma_i^m(gen)^2 + \sigma_i^m(imp))^2}}$$

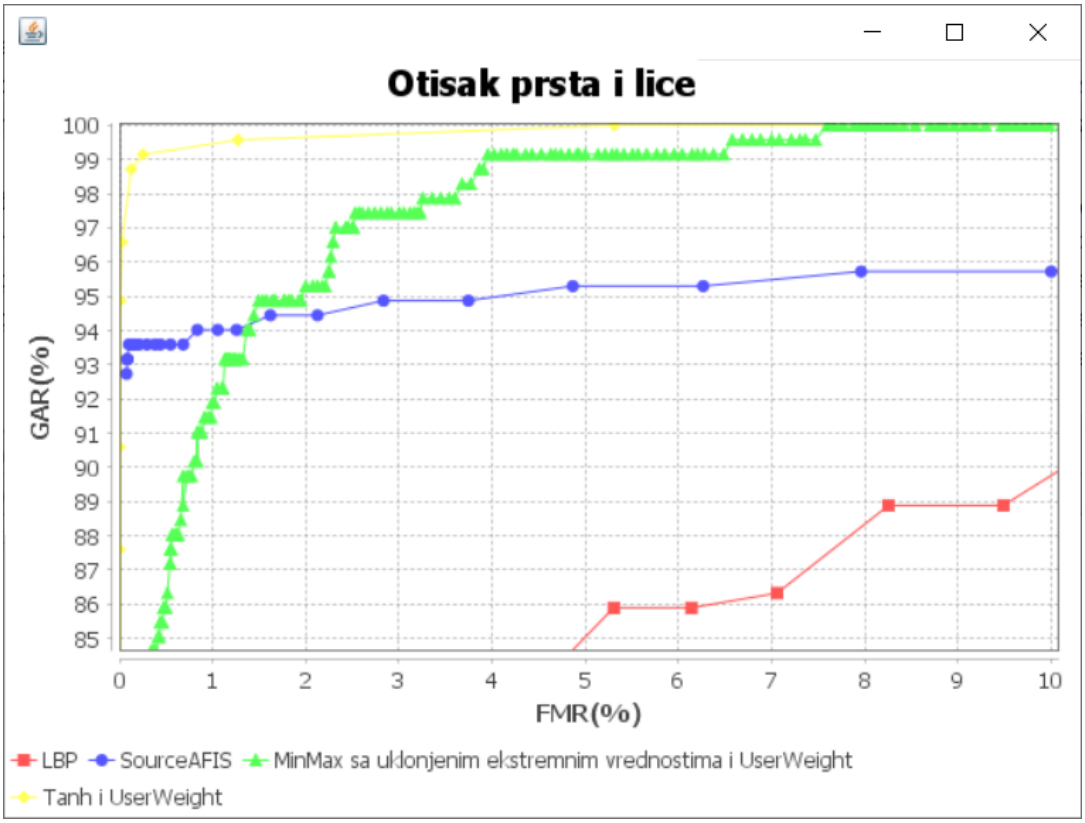
Gde su μ_i^m srednje vrednosti raspodela pravih korisnika i uljeza za i-tog korisnika u bazi, m-ti biometrijski modalitet, a σ_i^m odgovarajuće varijanse. Usled malog broja

biometrijskih šablona za svakog korisnika u bazi i osetljivosti algoritma za normalizaciju skorova, algoritam za fuziju daje često veće težine skorovima lica, usled čega nastaje uočeni pad performansi.



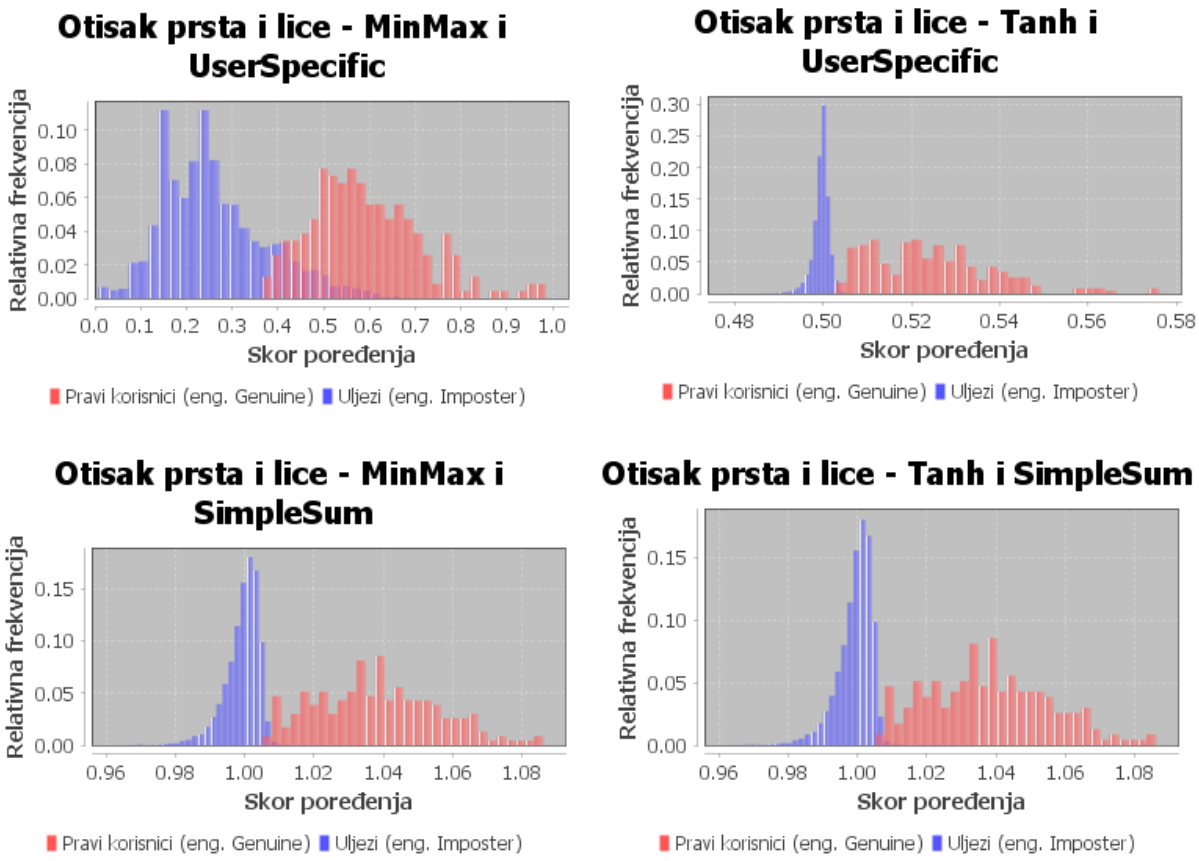
Slika 39 – ROC kriva koja prikazuje performanse *MinMax* i *Tanh* algoritama normalizacije skorova uparenih sa *UserCoefficient* algoritmom za fuziju informacija

Radi provere, ukoliko prilikom normalizacije isključimo gornjih i donjih 5 percentila prilikom normalizacije, preciznost kombinacije ova dva algoritma biće poboljšana. ROC krivu sa ovim rezultatatima možemo videti na slici 39.



Slika 40 – ROC kriva koja prikazuje performanse *MinMax* normalizacije sa uklonjenim ekstremnim vrednostima i *Tanh* normalizacije uparenih sa *UserCoefficient* algoritmom za fuziju informacija

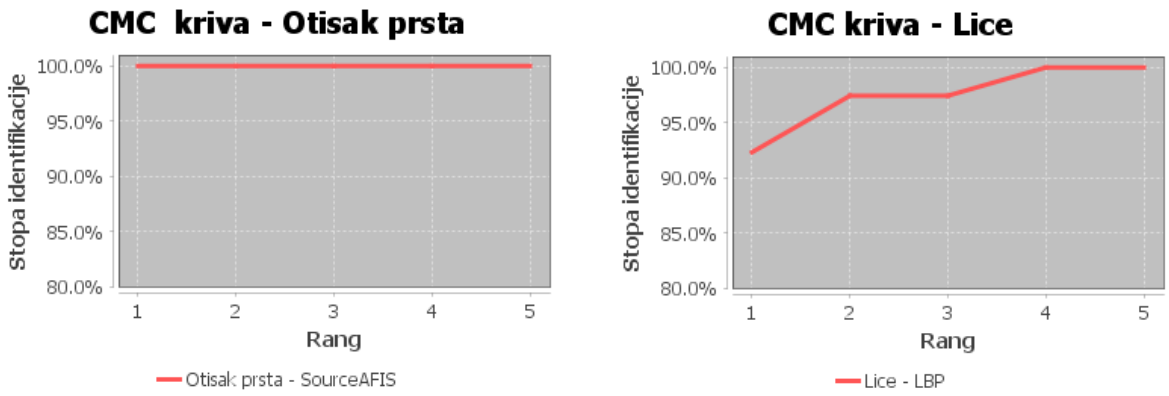
Na kraju, možemo zaključiti da primena fuzije prilagođene korisniku na ovom skupu podataka daje slične rezultate (*UserCoefficient*) kao i primena generičke metode fuzije (*SimpleSum*). Kako prvi algoritam zahteva određeno predznanje o svakom korisniku, možemo zaključiti da aplikacije koje upotrebljava manji broj korisnika je moguće na zadovoljavajući način realizavati primenom multimodalne biometrije sa *SimpleSum* fuzijom i nekim od navedenih algoritama za normalizaciju. Na ovaj način ostvaruje se znatno veća preciznost biometrijskog sistema u odnosu na upotrebu samo jednog biometrijskog modaliteta. Histograme skorova dobijenih fuzijom za sve kombinacije metoda normalizacije i fuzije možemo videti na slici 40.



Slika 41 – Histogram raspodela skorova poređenja po izvršenoj fuziji (*MinMax* i *Tanh* normalizacije u kombinaciji sa *SimpleSum* i *UserSpecific* metodama fuzije)

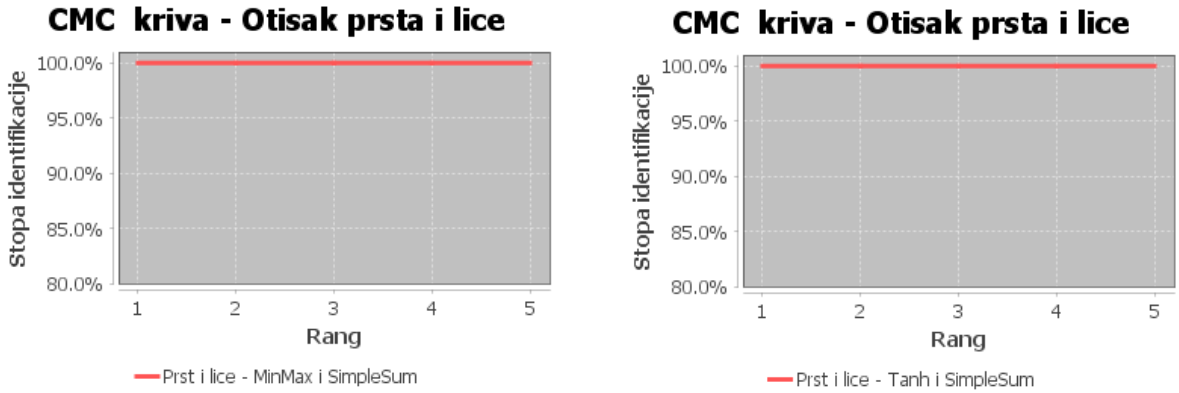
10.5.4 Performanse rada sistema u identifikacionom režimu rada

Preciznost sistema u identifikacionom režimu rada evaluiraćemo pomoću uvida u odgovarajuće CMC krive. Sa njih možemo očitati kumulativnu stopu identifikacije. Ovu stopu izračunavamo na osnovu ranga za svaku osobu iz baze. Rastojanje između dve osobe *d(i,j)* izračunavamo kao prosečnu vrednost skorova poređenja svih uzoraka jedne osobe sa svim uzorcima druge osobe u bazi. Za svaku osobu sortiramo dobijena odstojanja poređenja sa drugim osobama iz baze, a zatim na osnovu kumulativnih stopa identifikacije crtamo CMC krivu.



Slika 42 – CMC krive sa stopama identifikacije za biometrijske modalitete lice i otisak prsta

Na slici 42 možemo videti CMC krive sa stopama identifikacije za pojedinačne biometrijske modalitete. Upotrebom otiska prsta moguća je pouzdana identifikacija osoba u bazi, uz ogradu da postoji problem sa lažnim odbijanjima pravih korisnika, što možemo zaključiti iz prethodnog poglavlja gde je razmatran problem verifikacije. Stoga, predlaže se upotreba multimodalnog biometrijskog pristupa. CMC krive za *MinMax* i *Tanh* normalizaciju u kombinaciji sa *SimpleSum* algoritmom za fuziju prikazane su na slici 43.



Slika 43 – CMC krive sa stopama identifikacije za multimodalni pristup

Nakon evaluacije posmatranog multimodalnog biometrijskog sistema u identifikacionom i verifikacionom režimu rada možemo zaključiti da je primenom okvira moguće uspešno sprovesti evaluaciju performansi multimodalnog biometrijskog sistema. Značajna prednost upotrebe okvira prilikom evaluacije sistema predstavlja činjenica da se na taj način postiže ušteda vremena potrebnog za sprovođenje evaluacije. Na osnovu procene prilikom praktičnog rada na konkretnoj kombinaciji biometrijske baze i algoritama, za evaluaciju sistema primenom okvira bilo je potrebno oko četiri puta manje vremena nego u slučaju rada bez upotrebe okvira.

11 EDUKATIVNI BIOMETRIJSKI ALATI U PROCESU OBRAZOVANJA

Za adekvatnu primenu biometrijskih tehnologija u različite svrhe pre svega neophodni su odgovarajući ljudski resursi [14]. Jedna od ključnih uloga prilikom razvoja i implementacije biometrijskog sistema jeste uloga biometrijskog inženjera. Različiti univerziteti prepoznali su ovu činjenicu i ponudili studentima odgovarajuće studijske programe. Većina ovih programa odnosi se na postdiplomske studije. Univerzitet u Kentu ima program master studija – "Informaciona bezbednost i biometrija" [206], dok Univerzitet u Hertfordširu nudi master i doktorske studije sa nazivom "Procesiranje digitalnih medija i biometrijske tehnologije" [207]. Ipak, postoje i osnovne studije sa fokusom na ovoj tematici. Univerzitet Zapadne Virdžinije ima program osnovnih studija koji se bavi biometrijskim tehnologijama [208]. U okviru ovog poglavlja disertacije biće prikazani izazovi vezani za primenu edukativnih biometrijskih alata u procesu obrazovanja izloženi u radu [14].

Integracija biometrijskih tehnologija u kurikulum studijskog programa može biti veliki izazov. Tokom rada na razvoju kursa "Biometrijskih tehnologija" na master studijama Fakulteta organizacionih nauka, Univerziteta u Beogradu, uočeni su određeni potencijalni problemi [14]. S obzirom da primena biometrijskih tehnologija uključuje upotrebu novih dostignuća iz različitih stručnih i naučnih oblasti, kao što su mašinsko učenje, softversko inženjerstvo, interakcija čovek-računar i administracija računarskih sistema, studenti kojima nedostaje predznanje iz jedne ili više od ovih oblasti mogu imati probleme prilikom savladavanja gradiva.

Prilikom razmatranja izazova koji se javljaju tokom prenošenja znanja iz ove oblasti, možemo uočiti nekoliko njih [14]. Prvi izazov je nedovoljna uključenost studenata u toku izvođenja nastave. Tradicionalni pristup predavanjima može imati teškoća da održi pažnju studenata. Dalje, uočen je manjak timskog rada prilikom izrade projekata. Iako su studenti imali otvorenu mogućnost kolaboracije, nisu je uvek koristili, a zajednički projekti su često pre bili skup nezavisnih celina nego jedna komplementarna jedinica.

Primećen je i nedostatak konstruktivne konkurencije [14]. Studenti su uglavnom obavljali postavljene zadatke u skladu sa traženim zahtevima i završavali svoje obaveze, ali nisu imali mogućnost da budu motivisani dostignućima svojih kolega. U skladu sa ovim zapažanjem, i međusobna komunikacija studenata bila je više usmerena ka zadovoljavanju zadatih ciljeva, pre nego dubljem razumevanju proučavanih koncepata.

Poslednji potencijalni problem koji je primećen jeste uključivanje konkretnih izazova iz prakse u materijale za učenje [14]. Studenti su često imali poteškoća da povežu teorijsko znanje sa praktičnom primenom istog. Pored toga, studentski projekti koji su imali fokus na rešavanju praktičnih problema bili su skloni preteranom fokusu na određeni aspekt problema koji su rešavali, dok su druge bitne aspekte zanemarivali.

Neki od navedenih problema mogu se rešiti primenom specijalizovanih interaktivnih sistema za proces obrazovanja u oblasti biometrije, kao što je rešenje prikazano u radu [209]. Takođe, pored ovog pristupa, proces edukacije biometrijskih inženjera ima mogućnosti za unapređenje i primenom tehnika gejmifikacije. S obzirom da se studenti

mogu naći u različitim ulogama prilikom razvoja i testiranja biometrijskog sistema, ova oblast pogodna je za primenu tehnika gejmifikacije.

Detaljan pregled pojma gejmifikacije, kao i uspešni scenariji primene dati su u nastavku ovog poglavlja. Po definisanju odgovarajućih osnovnih pojmova i mehanizama, izvršen je pregled primena gejmifikacije u oblasti obrazovanja.

11.1 Pojam gejmifikacije i mehanizmi

Osnovna definicija gejmifikacije jeste primena elemenata iz dizajna igara u kontekstu nevezanom za same igre [210]. U poslednje vreme, gejmifikacija je najviše pažnje dobila u okviru oblasti elektronske trgovine, marketinga, inovacija, ljudskih resursa, ali i u okviru oblasti edukacije [6] [211]. U okviru ovog potpoglavlja dat je pregled različitih definicija pojma gejmifikacije, kao i mehanizama gejmifikacije prikazanih u radovima [6] [14] [212].

Prema mišljenju autora [213], primena tehnika gejmifikacije može rezultovati u unapređenju motivacije korisnika, njegovoj boljoj koncentraciji, unapređenim veštinama socijalizacije i građenja zajednice kao i povećanjem zadovoljstva korisnika. Pokretačke snage pozajmljene iz igara stimulišu potencijalne učenike na aktivnu participaciju u procesu učenja. Ove pokretačke snage mogu biti izazovi, takmičenja, saradnja, nagrade ili drugi tipovi mehanika koji su uobičajeni u igrama. Impementacija ovih pokretačkih snaga vrši se pomoću često prisutnih koncepata u igrama kao što su nagradni poeni, lestvice napretka i grupni izazovi. Istraživanja izvršena u radu [214] pokazuju da gejmifikacija može imati značajan emocionalni i socijalni uticaj na studente, s obzirom da sistem nagrada i takmičenja potencijalno ima motivacione efekte.

Sam pojam gejmifikacije je relativno nov. Želja za igrom je nešto što je čoveku svojstveno od pradavnih vremena. Osnovna svrha igara bila je zabava i razonoda [215]. Danas, igre se koriste za reklamiranje, za obuku zaposlenih, za unapređenje međuljudskih odnosa, za sticanje iskustva, za obrazovanje. Kako bi bolje razumeli sam pojam gejmifikacije, potrebno je da prvo definišemo pojam igara, pa tek onda da pređemo na problematiku gejmifikacije, kako bismo mogli da pravilno identifikujemo razlike između ova dva koncepta.

Kombinacijom elemenata osam različitih definicija, Salen et al. [216] dali su sledeći predlog definicije igre: “Igra je sistem u kome se igrači nalaze u veštačkom konfliktu, koji je definisan pravilima i koji ima za rezultat merljiv ishod.” Na sličan način, Adams zaključuje da je “igra tip zabavne aktivnosti, koji se dešava u kontekstu zamišljene realnosti, u kojoj učesnici pokušavaju da ostvare makar jedan tačno definisan netrivijalni cilj ponašajući se u skladu sa pravilima” [217]. Šel [218] definiše igru na jednostavan način kao “aktivnost rešavanja problema kojoj se pristupa za razigranim stavom”.

Sa druge strane, Bartl je definisao gejmifikaciju kao “pozajmljivanje tehnika igara za njihovu upotrebu van konteksta igre” [213]. Po definiciji Verbaha i Huntera “gejmifikacija predstavlja upotrebu elemenata igre i tehnika dizajniranja igara u neigračkom kontekstu” [219]. Ziherman i Kaningem gejmifikaciju predstavljaju kao “proces igračkog razmisljanja i mehanika igre koji angažuje igrača za rešavanje problema” [220]. Sve ove definicije gejmifikacije ukazuju na to da rezultat njene

primene ne mora nužno biti igra. Naprotiv, rezultat primene je pre svega proces koji uključuje elemente igre [219]. Bartl naglašava da gejmifikacija mora uključiti elemente igre, ali ne i samu aktivnost igranja [213]. Ako gejmifikacija uključuje i aktivnost igranja, onda to možemo pre definisati kao ozbiljnu igru (eng. *serious game*).

Igre se uobičajeno sastoje od serije koraka, koji mogu biti nivoi, činovi, runde i slični koncepti [217] [219] [221]. Nivoi označavaju napredak igrača. Oni su pre svega korisni za održavanje dugoročne motivacije igrača. Igrači nastavljaju sa igranjem kako bi dostigli više nivoe. Najbolji način za dizajn nivoa jeste napraviti ih da budu logični, proširivi i fleksibilni [220].

Jedan od načina navođenja igrača na željeni obrazac ponašanja je kroz dva tipa ciklusa aktivnosti: petlji angažovanja i stepenovanog napredovanja [222]. Petlje angažovanja imaju efekte na aktivnosti na mikro nivou, dok stepenovano napredovanje daje igraču pregled njegovog statusa na makro nivou.

U kontekstu igara, nagrade predstavljaju benefite koji se dobijaju za određene akcije ili dostignuća [222]. Nagrade mogu biti intrističke ili ekstrističke [220], a cilj gejmfikovanog sistema je da nudi nagrade koje odgovaraju pre svega unutrašnjim željama igrača, dok se ekstristički motivatori i pritisci koriste samo kada je to neophodno. Neki od primera nagrada [220] mogu biti: status, pristup dodatnom sadržaju, moć u igri i predmeti za upotrebu u okviru igre.

Kako bi se pokrenuli unutrašnji motivacioni mehanizmi igrača, neophodno je pred njih postaviti odgovarajuće izazove [223]. Izazovi daju igraču usmeravanje u okviru gejmifikovanog iskustva, kao i osećaj dubljeg značaja i smislenosti [220]. Izazovi predstavljaju jedan od glavnih izvora zadovoljstva igrača [218]. Kada uvek imaju nešto novo i zanimljivo da postignu, igrači su motivisani. Prilikom dizajna izazova, potrebno je imati na umu koliko izazova igrač želi da postigne, kao i to da izazovi budu ostvarivi prosečnom igraču.

Najjednostavniji način za gejmifikaciju nečega je primena poena, znački i lestvica napredovanja [210] [219]. Ali, za efektivnu primenu tehnika gejmifikacije nije dovoljno zadržati se isključivo na PBL (eng. *points, badges and leaderboards*) konceptima. PBL pristup može biti samo početna strategija. Obimnija lista elemenata predložena je od strane Ziherman i Lindera [223]: poeni, značke (dostignuća), nivoi, lestvice napredovanja i nagrade. Nešto kompleksniji pristup Zihermana i Kaningema [220] jeste MDA okvir: mehanika, dinamika i estetika (eng. *mechanics, dynamics, and aesthetics*). Mehaniku čine funkcionalni elementi igre. Dinamika predstavlja interakciju igrača sa mehanikom igre. Estetika sistema je osećaj koji igrači imaju prilikom međusobne interakcije.

Poeni predstavljaju osnovu svakog sistema za igru [220]. Ovaj često korišćen mehanizam može se koristiti za evaluaciju ponašanja, praćenje rezultata igre i pružanje povratnih informacija igračima. Takođe, koriste za utvrđivanje pobednika, određivanje napretka igrača i obezbeđivanje podataka za dizajnera igre. Prilikom kreiranja sadržaja za igrača, moguće je koristiti pet različitih tipova poena [220] [223]: iskustvene poene, poene za kasnije korišćenje (eng. *redeemable points*), poene reputacije, poene veština i karmičke poene (poeni dobijeni za pomaganje drugima). Najvažniji od ovih tipova

poena jeste koncept iskustvenih poena. Ove poene korisnik može osvojiti pomoću interakcije sa sistemom.

Značke predstavljaju priznanje za dostignuće određenog cilja. U literaturi se značke i dostignuća često koriste kao sinonimi (eng. *badges and achievements*). Pet glavnih razloga za korišćenje znački su [224]:

- Značke predstavljaju mehanizam za postavljanje ciljeva korisniku sistema
- Značke se mogu koristi kao instrukcije o mogućnostima sistema
- Značke pružaju mogućnost evaluacije reputacije korisnika
- Značke predstavljaju statusni simbol i omogućavaju ličnu afirmaciju
- Značke doprinose osećaju pripadnosti grupi

Značke su popularne pre svega jer pružaju priliku igračima da prikažu svoja dostignuća. Prednost znački se ogleda u činjenici da svojim vlasnicima nude mogućnost diskretnog prikazivanja ostvarenih dostignuća, bez negativnih efekata hvalisanja [223].

Lestvica napredovanja prikazuje rang igrača. Rang se računa na osnovu neke vrste skora, uobičajeno izvedene od poena dobijenih za različite aktivnosti igrača. Ovaj mehanizam može biti izuzetno snažan ako se koristi na pravi način, ali može imati i demotivišuće efekte. Igrači vole da porede svoja dostignuća. Žele da znaju gde se nalaze u odnosu na druge igrače. Ukoliko se nalaze previše daleko od onih koji su na vrhu lestvice, može se desiti da prestanu sa trudom.

Ipak, želja igrača za poređenjem skorova je mehanizam koji ima značajne potencijale. Kako bi se iskoristili na pravi način, potrebno je odabrati odgovarajući tip lestvice napredovanja. Postoje dve vrste lestvica napredovanja [225]: direktno kompetitivne i indirektno kompetitivne. Indirektno kompetitivne lestvice napredovanja stavljaju fokus na napredovanje igrača kroz igru, dok direktno kompetitivne promovišu nadmetanje između igrača. Prilikom odabira odgovarajućeg tipa lestvice potrebno je biti oprezan, kako ne bi došlo do neželjenih rezultata. Ipak, usled jednostavnosti implementiranja i značajnog potencijala, lestvice napredovanja predstavljaju jedan od najčešće korišćenih mehanizama gejmifikacije.

Za uspešnu primenu gejmifikacije, elementi igre su samo deo rešenja. Kao što je Adams [217] ukazao, ciljevi su od kritičnog značaja za igru. Cilj je nešto što igrač stremi da ostvari, nešto što ga motiviše i služi kao izvor razonode. Cilj uspešnog gejmifikovanog iskustva nije gubljenje igrača u virtuelnoj realnosti, već njegovo angažovanje na određenim aktivnostima u realnom svetu [219]. Za ovo je bitna motivacija i razumevenja pobuda igrača. Brojne taksonomije napravljene su kako bi se ovaj fenomen što bolje razumeo. Jedna od najcitiranijih jeste Bartlova taksonomija. Bartl je identifikovao četri tipa igrača [213]: igrači motivisani dostignućima, istraživači, društveno orijentisani igrači i takmičari.

Za igrače motivisane dostignućima, glavni izvor zadovoljstva u okviru igre jeste izazov [218]. Ipak, igranje uglavnom nije usamljenička aktivnost i uobičajeno se opisuje kao suštinski društvena [221]. Iako je igrač često fizički sam sa računarom, njegovo iskustvo nije izolovano i može ga razmenjivati sa drugima ili učiti od njih. Ovo je bitan aspekt za razmatranje prilikom dizajna sistema, jer društveno orijentisani igrači često čine jednu

od najbrojnijih grupacija. Ipak, bitno je prilagoditi sistem i ostalim tipovima igrača, kako bi se postigao maksimalan efekat gejmifikacije.

11.2 Primena gejmifikacije u edukaciji

U okviru ovog potpoglavlja dat je pregled mogućih primena tehnika gejmifikacije u edukaciji izloženih u radovima [6] [14] [212]. Sa prolaskom vremena, od pojave inicijalnog interesovanja navedenog u radu [211], sve više radova fokusiralo se na primenu u ovoj oblasti. Brojni istraživači ispitivali su efekte gejmifikacije u različitim domenima obrazovanja. Pa autorima rada [226], primena tehnika gejmifikacije može rezultovati u povećanoj motivaciji studenata, pojačati njihovu koncentraciju prilikom praćenja nastave, dovesti do bolje socijalizacije studenata i povećati njihovo zadovoljstvo procesom učenja.

Hamari i ostali [227] izvršili su ekstenzivnu studiju radova objavljenih na temu gejmifikacije. Oni su analizirali različite konstrukte koji su korišćeni za motivaciju korisnika sistema u objavljenoj literaturi, kao i bihejviorističke i psihološke rezultate eksperimenata koje su autori radova objavili. Najčešće korišćeni konstrukti su lestvice napredovanja, poeni i značke. Najveći broj studija se fokusirao na bihejviorističkim rezultatima. Zaključak autora je da većina studija obuhvaćenih ovim istraživajem ukazuje na to da primena gejmifikacije u globalu ima pozitivne efekte. Iako su uglavnom sva istraživanja saopštila pozitivne efekte, postoje i određeni rizici koje primena gejmifikacije nosi. To su pre svega povećana konkurencija među korisnicima sistema, teškoće u evaluaciji zadataka i otežan dizajn funkcionalnosti sistema. Autori ovog preglednog rada kao česte propuste u metodologiji istraživanja navode mali broj ispitanika u studijama, upotrebu nevalidiranih psihometrijskih mera, nedostatak kontrolnih grupa, kratak vremenski okvir u kome su vršena istraživanja, kao i nedovoljno jasnu prezentaciju rezultata dobijenih studijama.

U radu [228], autori su primenili tehnike gejmfikacije za učenje 3D umetnosti u visokoj edukaciji. Razvili su sistem pod nazivom GLABS koji proširuje standardne LMS (eng. *Learning Management System*) funkcionalnosti, sa mehanikama igre. Različite metodologije kao što su učenje bazirano na rešavanju problema (eng. *Problem-Based Learning*) i učenje zasnovano na rešavanju zadataka (eng. *Quest-Based Learning*) implementirane su u sistemu. Studentima je omogućeno da svoje trodimenzionalne modele pomoću WebGL-a [229] okače na veb platformu. Kako bi i drugi korisnici mogli da uživaju u ovom sadržaju, napravljena je virtuelna realnost upotrebom *Unity engine*-a [230] i *Occulus Rift*-a [231]. Rezultati eksperimenta evaluirani su kvantitativnom analizom. Zaključak autora je da je upotrebljeni pristup imao uspeha ne samo kod poboljšanja motivacije i aktivnosti studenata, već i da je olakšao proces evaluacije studentskih radova.

U radu autora Cheong et al. [232] evaluiran je gejmifikovan kviz sa više ponuđenih odgovora, implementiran u obliku softverskog alata. Studija je sprovedena pomoću upitnika. Rezultati pokazuju određene pozitivne efekte, ali problem predstavlja nedostatak kontrolne grupe nad kojom bi moglo da se izvrši poređenje. Takođe, rezultati su dobijeni na osnovu lične percepcije učesnika ankete, a i period trajanja istraživanja je bio relativno kratak.

Evaluacija efekata gejmifikacije na duže staze je zadatak od velike važnosti, s obzirom da ne postoji veliki broj studija koje se bave ovom temom. Takav eksperiment bi pomogao preciznijem određivanju dugoročnih efekata gejmifikacije i omogućio identifikovanje bihejviorističkih šablona i efekata na performanse učenja učesnika eksperimenta. Jedna takva studije u trajanju od tri godine opisana je u radu [233]. Tehnike gejmifikacije primenjene su na jednosemestralni kurs multimedijalne produkcije, koji se održava na Univerzitetu u Lisabonu. Istraživači su identifikovali nekoliko različitih grupacija učesnika, svaku sa drugačijim ponašanjem i karakterističnim nivoom uspeha na kursu. Kako je kurs menjao oblik tokom godina, promene u ponašanju studenata i njihovim dostignućima pažljivo su praćene. Zaključak autora je da je veoma značajno dozvoliti studentima da uče na svojim greškama i omogućiti im da sami biraju put učenja.

Neki od istraživača su saopštili mešovite rezultate prilikom primene gejmifikacije u okviru univerzitetskog kursa. U istraživačkoj studiji [234], studenti koji su završili gejmifikovanu verziju kursa imali su više ocene u proseku, ali su slabije učestvovali u aktivnostima na času i imali lošije rezultate na aktivnostima koje su zahtevale veštine pisanja. Zaključak autora je da gejmifikacija ima potencijal da poveća motivaciju studenata, ali da je potrebno uložiti značajan napor u dizajn i implementaciju aktivnosti kako bi bila realizovana na odgovarajući način. Pored toga, kvantitativna analiza ukazuje da je efekat na kognitivne sposobnosti studenata donekle ograničen, jer iako su postojale određene statistički značajne razlike u uspehu studenata na kursu, one nisu bile velike.

Studije sa većim brojem ispitanika sprovedena je kako bi se analizirao uticaj znački na poboljšanje učešća i aktivnosti korisnika sistema. U ovoj studiji učestvovalo je preko 1000 participanata [235]. Eksperiment je izvršen na kursu osnovnih diplomskih studija na Ouklandskom univerzitetu. Kurs je imao za temu uvod studenata u okvire i alate koji se koriste za određivanje uticaja zaraznih bolesti u populaciji. Značke su bile ugrađene u alat za elektronsko učenje koji je bio upotrebljavan na kursu. Tokom istraživanja nije bio primećen negativan uticaj upotrebe znački, a bilo je značajnih poboljšanja nekih od parametara aktivnosti studenata koje je studija pratila, kao što su broj odgovora na pitanja i broj dana koje su studenti proveli aktivno koristeći alat. Autori studije zaključuju da efikasnost znački zavisi od velikog broja različitih faktora, kao što su demografske karakteristike korisnika, svrha upotrebe alata i relevantnost odabranih znački za podsticanje studenata na određen tip ponašanja.

Još jedna studija koja je ispitala značaj znački jeste [236]. TRAKLA2 [237], okruženje za *online* obrazovanje, namenjeno pre svega za vežbe simulacije algoritama, upotrebljeno je za testiranje performansi znački. Studenti su dobijali značke za završavanje vežbi sa samo jednim pokušajem, za predavanje domaćih zadataka pre isteka roka ili osvajanje maksimalnog broja poena na nekom od zadataka. Značke nisu imale direktan uticaj na finalne ocene studenata. Rezultati pokazuju da neki od tipova znački su imali statistički značajan uticaj na ponašanje studenata, mada su grupacije na kojima je to primećeno imale mali broj članova. Takođe, autori su istakli potencijalne negativne efekte znački, kao što su smanjena pažnja studenata usled planiranja vremena na način koji je favorizovao takmičarski aspekt eksperimenta.

Gejmifikovan pristup učenju programskog jezika C u okviru univezitetskog kursa opisan je u radu [238]. Za analizu podataka u ovom eksperimentu, upotrebljena je

sekvencijalno pokazna metoda dizajna. Ovaj pristup kombinuje kvalitativni i kvantitativni pristup istraživanju [239]. Autori zaključuju da je upotreba gejmifikacije imala pozitivne rezultate, sa određenim ograničenjima. Gejmifikovani pristup predstavljao je novinu za studente, a okruženje za učenje dizajnirano je sa ciljem da na što bolji način iskoristi vreme dostupno tokom trajanja kursa. Rezultati evaluacije pokazuju da iako je okruženje podstaklo studente na dodatan rad, nije sa sigurnošću utvrđeno da li je to rezultat unutrašnje motivacije, gejmifikacije ili preklapanja većeg broja različitih izvora motivacije.

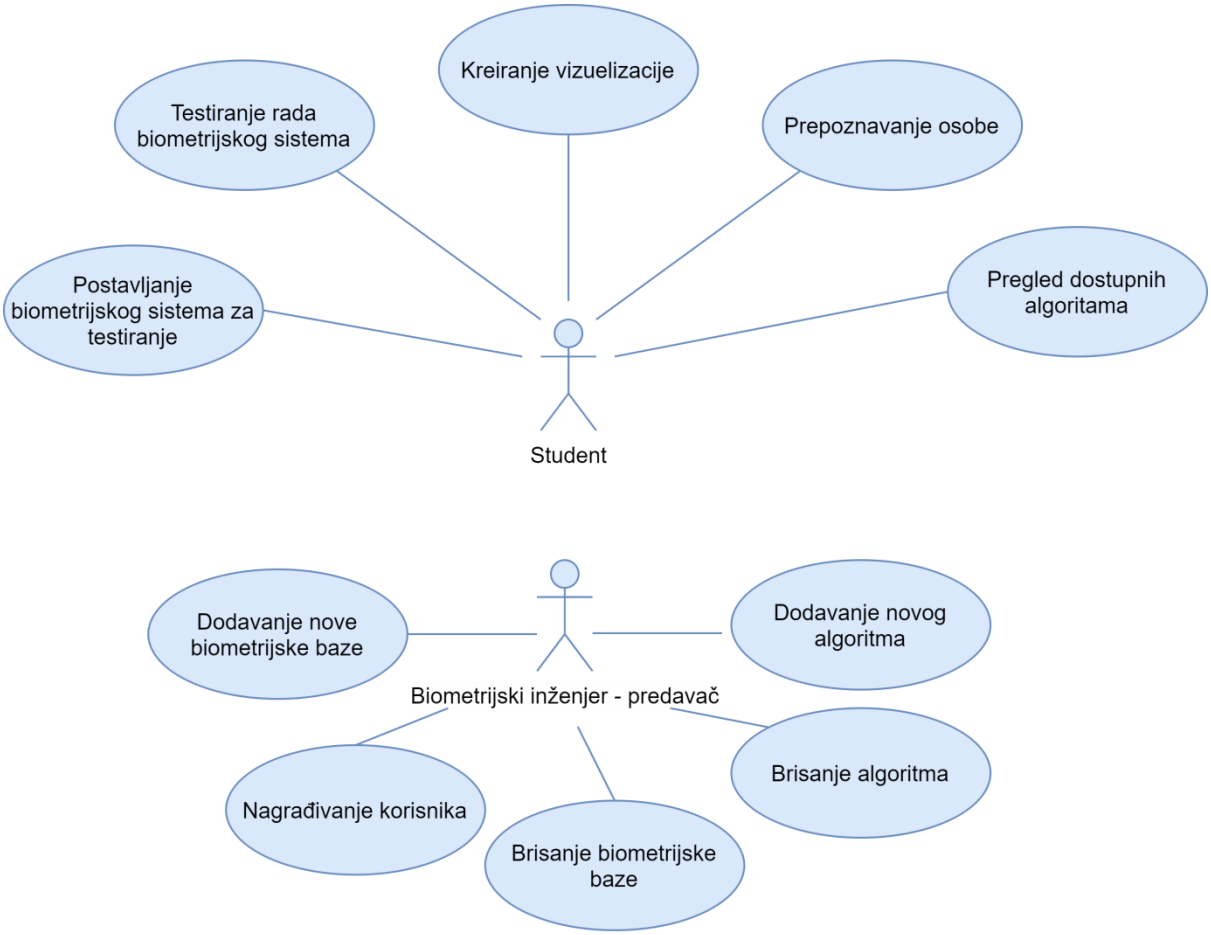
Agilar, Holman i Fišman [240] analizirali su efekte dva gejmifikovana univerzitetska kursa, Uvoda u političku teoriju i Uvoda u informacione studije. Gejmifikovani pristup primenjen je u okviru oba kursa sa željom podsticanja unutrašnjih motivacionih faktora kod studenata. Kursevi su od tehnika gejmifikacije koristili fleksibilne zadatke, odabir težinskih faktora kod ocenjivanja aktivnosti, lestvice napredovanja i poene kuća. Autori navode da je primena mehanizama gejmifikacije uticala na to da studenti imaju pozitivnu percepciju o kursevima, što je pak rezultiralo u poboljšanim nekognitivnim motivacionim ishodima. Upotreba lestvica napredovanja se pokazala kao uspešna, iako su autori inicijalno imali drugačija očekivanja. Ipak, dobijene rezultate treba uzeti sa rezervom, jer postoji mogućnost da su studenti koji nisu bili takmičarski nastrojeni odabrali da ne učestvuju u gejmifikovanoj verziji kursa. Krajnji zaključak autora je da kursevi sa elementima gejmifikacije treba da ostave svojim korisnicima određenu količinu slobode, kako bi se prilagodili različitim tipovima studenata i njihovim načinima razmišljanja.

Štavljanin, Milenković i Šošević [6] koristili su gejmifikaciju kao pristup optimizaciji konverzije vebsajta za *online* učenje. Upotrebljeni gejmifikacioni elementi bili su lestvice napredovanja, poeni, značke i zadaci. Primenjene tehnike imale su za rezultat unapređenja u stepenu konverzije studenata. Ukupan broj pregleda stranice kursa povećao se za 32.98%. Broj preuzetih sadržaja materijala kursa je značajno skočio. Prosečan broj preuzimanja materijala popeo se sa 270.6 na 320.8 preuzimanja. Participanti ovog gejmifikovanog kursa takođe su imali poboljšanu motivaciju i bolje rezultate na testu. Ipak, kako je učešće u okviru ovog eksperimenta bilo na dobrovoljnoj bazi, autori navode da postoji mogućnost da je eksperiment privukao kvalitetnije i bolje motivisane studente u odnosu na kontrolnu grupu.

Na osnovu analize radova koji su pokušali da primene tehnike gejmifikacije u oblasti obrazovanja, može se zaključiti da upotreba ovog pristupa ima potencijalne benefite po motivaciju studenata i njihovo bolje i lakše usvajanje zadatog gradiva. U skladu sa ovim zaključkom, biće formirani korisnički zahtevi za biometrijski alat u procesu obrazovanja, kao i implementirane odgovarajuće funkcionalnosti u nastavku rada.

11.3 Korisnički zahtevi za biometrijski alat u procesu obrazovanja

Kada posmatramo biometrijski alat u procesu obrazovanja, možemo uočiti dve dominatne uloge – studenta i biometrijskog inženjera, odnosno predavača. Student može vršiti pregled dostupnih algoritama, pokušati prepoznavanje osobe sa nekim od ponuđenih algoritama, napraviti vizuelizaciju performansi određenog algoritma, postaviti biometrijski sistem na platformu za testiranje i testirati druge biometrijske sisteme sa odabranim podacima.



Slika 44 – Dijagram slučajeva korišćenja za biometrijski alat u procesu obrazovanja

Predavač, odnosno biometrijski inženjer može da doda novi algoritam među algoritme raspoložive za probu, uključi novu biometrijsku bazu podataka u sistem, kao i da vrši nagrađivanje studenata za uspešno obavljene zadatke. U slučaju potrebe, može i da obriše biometrijsku bazu ili algoritam sa sistema. Dijagram slučajeva korišćenja za opisane scenarije prikazan je na slici 44. U nastavku teksta dati su koraci koje možemo uočiti u okviru pojedinačnih slučajeva korišćenja.

Scenario korišćenja Pregled dostupnih algoritama:

1. Student iz liste modaliteta ponuđenih od strane sistema selektuje željeni modalitet
2. Na osnovu odabranog modaliteta sistem prikazuje algoritme dostupne za rad sa tim modalitetom
3. Student iz liste ponuđenih algoritama bira željeni algoritam
4. Sistem prikazuje detaljne informacije o odabranom algoritmu (opis koraka algoritma, tipove ulaznih i izlaznih podataka)

Scenario korišćenja Prepoznavanje osobe:

1. Student bira način rada biometrijskog sistema (identifikacioni ili verifikacioni režim)
2. (Opciono) U slučaju verifikacije, student odabira zahtevani identitet iz liste ponuđenih
3. Student iz liste modaliteta ponuđenih od strane sistema selektuje željeni modalitet
4. Student odabira biometrijske podatke za proces prepoznavanja
5. Sistem donosi odluku i prikazuje dobijeni rezultat

Scenario korišćenja Kreiranje vizuelizacije:

1. Student iz liste modaliteta ponuđenih od strane sistema selektuje željeni modalitet
2. Na osnovu odabranog modaliteta sistem prikazuje algoritme dostupne za rad sa tim modalitetom
3. Student iz liste ponuđenih algoritama bira željeni algoritam
4. Sistem prikazuje listu baza podataka dostupnih za evaluaciju
5. Student bira bazu podataka za koju želi da izvrši evaluaciju pokazatelja
6. Sistem prikazuje listu dostupnih načina vizuelizacije
7. Student bira željeni način vizuelizacije
8. Sistem prikazuje rezultate evaluacije za odabranu vizuelizaciju

Scenario korišćenja Postavljanje biometrijskog sistema za testiranje:

1. Student unosi podatke o svom biometrijskom sistemu (naziv biometrijskog sistema, format ulaznih podataka, kao i tip izlaza iz sistema)
2. Student odabira fajlove sa biometrijskim algoritmima
3. Sistem proverava da li fajlovi zadovoljavaju tražene uslove i podatke date u specifikaciji
4. Sistem prikazuje potvrdu o uspešnom postavljanju biometrijskog sistema

Alternativni scenario:

4.a Sistem prikazuje grešku ukoliko neka od provera nije uspešna

Scenario korišćenja Testiranje rada biometrijskog sistema:

1. Student odabira biometrijski sistem koji će biti testiran
2. Student odabira biometrijske podatke za testiranje (na primer, sliku lica)

3. (Opciono) Student vrši dodatno pretprocesiranje podataka za testiranje (na primer, izmena uslova osvetljenja na slici)
4. Student bira način rada biometrijskog sistema
5. Student započinje proces prepoznavanja
6. Sistem donosi odluku i prikazuje dobijeni rezultat

Scenario korišćenja Nagrađivanje korisnika

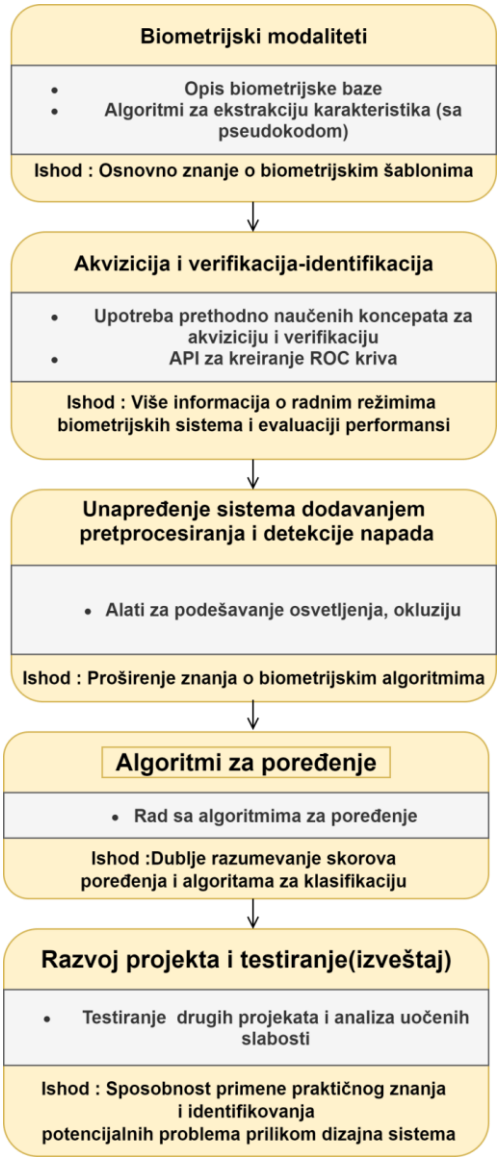
1. Predavač odabira studenta iz liste studenata
2. Predavač odabira tip nagrade
3. Sistem prikazuje obaveštenje o uspešno dodeljenoj znački ili poenima, i upisuje ih u bazu podataka

Scenariji korišćenja Dodavanje nove biometrijske baze, Dodavanje novog algoritma, Brisanje biometrijske baze i Brisanje algoritma ekvivalentni su scenarijima korišćenja definisanim u okviru specifikacije korisničkih zahteva za potrebe evaluacije performansi multimodalnog biometrijskog sistema.

11.4 Studija slučaja – Edukativni biometrijski sistem u procesu obrazovanja

U okviru ovog potpoglavlja dat je prikaz studije slučaja opisane u radu [14]. Na osnovu alata koji je koristio neke od funkcionalnosti okvira, razvijena je *online* platforma za učenje – prototip edukativnog biometrijskog sistema. Prilikom implementacije funkcionalnosti platforme, korišćen je okvir za evaluaciju multimodalnih biometrijskih sistema. Pomoću okvira, realizovani su pregledi dostupnih algoritama, implementirano prepoznavanje osoba, kao i omogućeno kreiranje vizuelizacija.

Za evaluaciju primene prototipa edukativnog biometrijskog sistema u procesu obrazovanja iskorišćen je kurs „Biometrijske tehnologije“, u okviru master akademskih studija na Fakultetu organizacionih nauka. Radi unapređenja angažovanja studenata, primenjeni su elementi gejmifikacije. Implementirane su značke, lestvice napredovanja, zadaci i kolektivni izazovi. Svi ovi elementi uključeni su u *online* platformu za učenje. Platforma za učenje pratila je kurikulum kursa. Prvi deo kursa odnosio se na četiri glavne teme vezane za biometrijske tehnologije. Nastavak, odnosno drugi deo kursa odnosio se na studentske projekte i testiranje sistema [14].



Slika 45 – Tok kursa i ishodi učenja [14]

Kurs počinje sa upoznavanjem studenata sa osnovama funkcionisanja biometrijskih sistema, biometrijskih modaliteta, ekstrakcijom karakteristika i biometrijskim bazama podataka. Sledeća celina se odnosi na upis biometrijskih podataka u bazu podataka, verifikaciju, identifikaciju, kao i ROC (eng. *Recieving Operating Characteristics*) krive, koje su bitne za evaluaciju performansi biometrijskog sistema. U ovom trenutku, studenti bi trebalo da poseduju znanje vezano za proces biometrijskog prepoznavanja integrisano u jednu celinu [14]. Nakon toga, sledeća tema opisuje kako performanse i bezbednost biometrijskog sistema mogu biti unapređeni primenom pretprocesiranja i prepoznavanjem lažiranih biometrijskih podataka. Naredna celina odnosi se na algoritme za poređenje i daje detaljniji uvid u biometrijske skorove i algoritme za klasifikaciju. Grafički prikaz toka kursa kao i ishoda učenja prikazan je na slici 45.

Tradicionalne lekcije sastoje se od predavanja za određenu tematsku celinu, praćenih odgovarajućom prezentacijom. Posle predavanja, studenti dobijaju domaće zadatke koji se odnose na primenu teorijskih znanja u rešavanju praktičnih problema. Platforma za učenje unapređuje ovaj deo procesa učenja davanjem pristupa dodatnim resursima

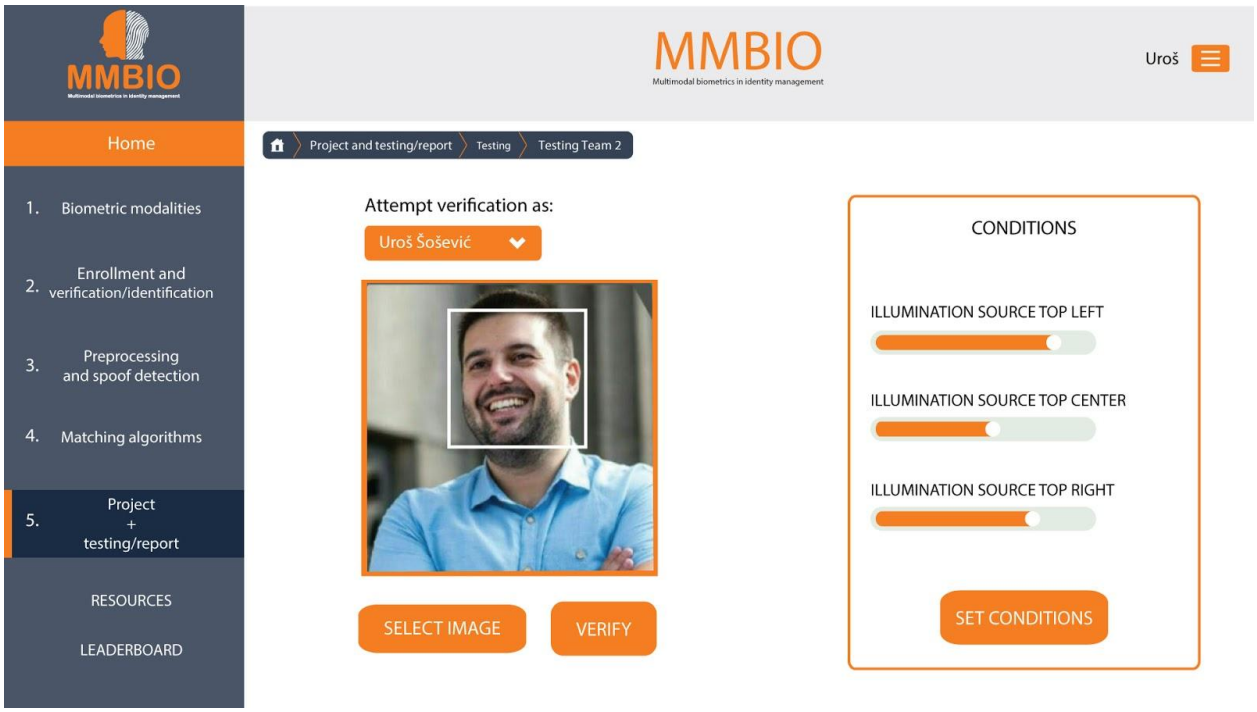
studentima, kao i definisanjem zadataka – izazova [14]. Potrebno je da studenti reše ove izazove u timu. Na taj način imaju priliku da primene stečena teorijska znanja u praksi. Na primer, mogu isprobati različite algoritme za ekstrakciju karakteristika ili za prepoznavanje lica, kao i uporediti rezultate izvršavanja algoritama.

Slika 46 – Studentski profil [14]

Dok izučavaju teme dostupne na platformi, studenti rešavaju zadatke iz svake teme i dobijaju poene kao nagradu za uspešno izvršavanje zadataka [14]. Ovi poeni se obračunavaju za tim kome student pripada i imaju uticaj na poziciju tima na lestvici napredovanja. Posle završetka svih zadataka koji se nalaze u okviru jedne teme, svi članovi tima se nagrađuju sa značkom. Svaka tema ima posebnu značku, a dodatna značka se može osvojiti po završetku sve četiri celine. Kao dodatak, dostignuća je moguće ostvariti i pomoću željene interakcije sa sistemom, na primer testiranjem različitih algoritama za ekstrakciju karakteristika na više slika. Slika 46 prikazuje studentski profil. Ovaj profil sadrži osnovne podatke o studentu, poslednjoj aktivnosti na platformi, kao i značkama dostignuća koje poseduje.

Pored pomenutih primena, najuticajniji element gejmifikacije na platformi – konkurencija, integrisana je u drugom delu kursa, u celini koja se odnosi na studentske projekte. U ovoj fazi, studenti se mogu naći u dve uloge [14]. Prva uloga jeste uloga projektanta biometrijskog sistema. Druga uloga je oponašanje zlonamernog napadača. Kada se nalazi u ulozi projektanta sistema, student ima zadatak da razvije kompletan biometrijski sistem za prepoznavanje lica. Glavni cilj prilikom razvoja sistema jeste konfigurisanje ponašanja sistema u skladu sa datim zahtevima i postavljenim ciljevima. Projektanti biometrijskog sistema mogu odabrati različite metode za normalizaciju podataka, ekstrakciju karakteristika, poređenje dobijenih karakteristika i podešavanje praga osetljivosti sistema. Prilikom postavljanja sistema, studenti pomoću XML dokumenta definišu parametre svog sistema, kako bi dalja integracija bila moguća. Sistem na izlazu daje odgovarajuće skorove i prosleđuje ih MMBio ROC servisu. Ovaj

servis koristi okvir za evaluaciju multimodalnih biometrijskih sistema, i pomoću njega vrši evaluaciju postavljenog sistema. Ukoliko projektanti sistema uspešno zadovolje postavljene ciljeve, njihov tim se nagrađuje poenima [14].



Slika 47 – Ekranska forma za testiranje projekata [14]

Uloga napadača u platformi za učenje je implementirana kao mogućnost da se isproba sistem za biometrijsku verifikaciju nastao kao rezultat timskog projekta. Interfejs ovog dela platforme prikazan je na slici 47. Student može odabrati identitet korisnika sistema koji želi da verifikuje. Slika za verifikaciju može da se odabere i pošalje na platformu sa lokalnog fajl sistema [14]. Postoje opcije podešavanja osvetljenja za sliku koja se koristi za testiranje, kako bi se što bolje isprobale mogućnosti prevare sistema. Klikom na dugme za verifikaciju, proces verifikacije izvršava se u biometrijskom sistemu i kao rezultat se dobija skor za verifikaciju. Ekran takođe sadrži i polje za unos izveštaja o napadu kao i parametre koji su doveli do rezultata. Na ovaj način, studenti mogu da testiraju projekat nastao kao rezultat rada nekog od timova svojih kolega i analiziraju ga kako bi bolje razumeli funkcionisanje sistema za biometrijsko prepoznavanje [14].

11.4.1 Opis eksperimenta

U okviru kursa biometrijskih tehnologija bilo je uključeno 40 studenata. Učesnici kursa bili su podeljeni po slučajnom izboru u dve jednake grupe. Jedna grupa je radila po tradicionalnom pristupu predavanja gradiva, dok je druga u radu koristila i našu platformu.

Kako bi se proverila hipoteza H3 – da okvir za evaluaciju multimodalnih biometrijskih sistema može proces obrazovanja inženjera u oblasti biometrije učiniti efikasnijim, pomoću analize relevantne literature definisane su dve pomoćne hipoteze koje će biti proverene odgovarajućim statističkim metodama. Prva hipoteza je da upotreba gejmifikacije vodi poboljšanju ishoda učenja studenata koji su pohađali kurs iz

biometrijskih tehnologija. Druga hipoteza je da će primena elemenata gejmifikacije imati za rezultat unapređenje u motivaciji studenata, u poređenju sa tradicionalnim pristupom predavanja gradiva.

11.4.2 Uticaj primene alata na ishod kursa

Pre kursa, radi provere da li učesnici obe grupe imaju ekvivalentan nivo predznanja, izvršeno je pismeno testiranje. Test je imao 12 pitanja o osnovnim pojmovima iz oblasti biometrijskih tehnologija. Rezultati testa su prikazani u tabeli 16.

Tabela 16 – Rezultati ulaznog testa [14]

Tip kursa	N	Aritmetička sredina	Standardna devijacija	Standardna greška – srednja vrendost
Tradicionalni	20	57.3500	17.53275	3.92044
Gejmifikovan	20	55.0500	16.92857	3.78534

Rezultati Šapiro Vilk testa [241] pokazuju da rezultati ulaznog testa imaju normalnu raspodelu. Usled toga, može se primeniti t-test nezavisnih uzoraka, kako bi se proverilo da li postoji statistički značajna razlika između dve grupe. Kod Levenovog testa jednakosti varijanse [242] značaj je bio veći od 0.05, te se može pretpostaviti da su varijanse oba skupa podataka jednake.

Tabela 17 – T-test nezavisnih uzoraka za analizu rezultata ulaznog testa [14]

Levenov test jednakosti varijanse	F		.015
	p-vrednost.		.902
t-test za jednakost srednjih vrednosti	t		.422
	Stepeni slobode		38
	p-vrednost dvostranog testa		.675
	Razlika srednjih vrednosti		2.30000
	Standardna devijacija razlike između uzoračkih sredina		5.44965
	95% Interval poverenja razlike	Donja	-8.73224
		Gornja	13.33224

S obzirom da je značaj t-testa veći od 0.05, može se zaključiti da su srednje vrednosti populacija jednake. Ne postoji statistički značajna razlika u rezultatima testa obe grupe studenata. Rezultati testa upućuju na činjenicu da kandidati poseduju određena osnovna znanja o biometrijskim tehnologijama. Pošto je učešće na kursu bilo na dobrovoljnoj osnovi, ovo je donekle i očekivan rezultat [14].

Za evaluaciju ishoda kursa, sprovedeno je testiranje znanja po završetku kursa, kako za gejmifikovanu, tako i za tradicionalnu grupu. Prosečna ocena na evaluaciji za tradicionalnu grupu bila je 73.65 sa standardnom devijacijom od 10.674, dok je prosečna ocena za gejmifikovanu grupu bila 81.2 sa standardnom devijacijom 10.042. Šapiro-Vilk [241] test potvrđuje da podaci odgovaraju normalnoj raspodeli, tako da se može nastaviti sa t-testom nezavisnih uzoraka. S obzirom da je značajnost manja od 0.05, može se zaključiti da postoji statistički značajna razlika između dve grupe [14]. Time je potvrđena prva pomoćna hipoteza - da upotreba gejmifikacije vodi poboljšanju ishoda učenja studenata koji su pohađali kurs iz biometrijskih tehnologija [14].

Tabela 18 – T-test nezavisnih uzoraka za ishode učenja kursa [14]

Levenov test jednakosti varijanse	F		.055
	p-vrednost		.815
t-test za jednakost srednjih vrednosti	t		-2.264
	Stepeni slobode		38
	p-vrednost dvostranog testa		.029
	Razlika srednjih vrednosti		-7.55000
	Standardna devijacija razlike između uzoračkih sredina		3.33551
	95% Interval poverenja razlike	Donja	-14.30240
		Gornja	-.79760

11.4.3 Uticaj primene alata na motivaciju studenata

Za evaluaciju motivacionih aspekata, na kraju kursa participanti dobijaju upitnik sa 12 pitanja na koja je potrebno da odgovore [14]. Cilj je bio da se obuhvate kako unutrašnji (razvojni) tako i spoljašni (represivni) faktori motivacije. Upitnik koji je upotrebljen sadrži kombinaciju pitanja u vezi sa sadržajem kursa i procesa učenja. Pitanja upitnika formulisana su na osnovu sličnog primera iz relevantne literature [243]. Likertova skala [244] sa sedam nivoa slaganja je upotrebljena prilikom izrade upitnika. Pitanja koja su se odnosila na kontekst i sadržaj bila su: „Tema kursa je prijatna i zabavna“, „Znanje koje sam dobio je vredno“, „Postoji veza između teorije i prakse“, „Moguće je uživati u temi kursa“. Takođe, izazovi koji su bili prisutni u procesu učenja obuhvaćeni su pitanjem: „Smatram da su moji kapaciteti u potpunosti iskorišćeni prilikom učenja na ovaj način“. Pouzdanje i mogućnost kontrole procesa učenja pokriveni su pitanjima– „Smatram da se mogu u potpunosti izraziti pri ovom metodu učenja“, “Smatram da proces učenja je prilagođen načinu na koji provodim svoje slobodno vreme”, “Mogu se aktivno uključiti u proces učenja”. Uticaj saradnje sa drugima – “Mogao sam da komuniciram sa svojim kolegama tokom procesa učenja”, dok se stepen relevantnosti gradiva ocenjivao sa “Osećam da ostvarujem bitna dostignuća u toku procesa učenja” i “Mogu da koristim znanja iz različitih oblasti”. Na kraju, u upitnik je bilo uključeno i davanje adekvatnih povratnih informacija sa pitanjem – “Osećam da mogu odmah da vidim rezultate svog učenja”. Kronbahova alfa [245] je primenjena na odgovore prikupljene pomoću upitnika i izračunata alfa vrednost je bila 0.8723. Pošto se ova vrednost tumači kao visoka pouzdanost, može se zaključiti da pitanja iz upitnika mere jedinstveni konstrukt, što je neophodno za nastavak ispitivanja druge pomoćne hipoteze.

Tabela 19 – T-test nezavisnih uzoraka za analizu rezultata motivacionog upitnika [14]

Levenov test jednakosti varijanse	F		2.080
	Sig.		.157
t-test za jednakost srednjih vrednosti	t		-3.186
	Stepeni slobode		38
	p-vrednost dvostranog testa		.003
	Razlika srednjih vrednosti		-.67365
	Standardna devijacija razlike između uzoračkih sredina		.21147
	95% Interval poverenja razlike	Donja	-1.10174
		Gornja	-.24556

Srednja vrednost odgovora sa motivacionog upitnika za grupu koja je učestvovala u gejmifikovanom kursu bila je 5.5917. Srednja vrednost odgovora na upitniku za grupu koja je radila primenom tradicionalnog pristupa bila je 4.918. Kako bi se proverilo da li je primećena razlika statistički značajna, primenjen je t-test, pošto je Šapiro-Vilk test pokazao da podaci imaju normalnu raspodelu. Dobijeni nivo značajnosti je manji od 0.05. Razlika između motivacije tradicionalne i gejmifikovane grupe ima statističku značajnost, te se stoga druga pomoćna hipoteza ne može odbaciti [14].

Kako je statistička analiza pokazala da postoji značajna razlika u motivaciji između dve grupe, bitno je bilo otkriti što više detalja o efektima gejmifikacije na motivaciju studenata. Radi ostvarenja tog cilja, organizovana je fokus grupa koja se sastojala od učesnika gejmifikovanog kursa. U ovoj diskusiji, fokus je bio na načinu na koji su učesnici posmatrali novi pristup učenju, kao i kakav su uticaj različiti elemenati gejmifikacije imali na njihov rad i proces učenja. Takođe, provereno je i da li su studenti smatrali da je prevazilaženje postavljenih izazova interesantno i zabavno.

Na osnovu diskusije, može se zaključiti da su studenti dobro prihvatili gejmifikovani pristup [14]. Izjavili su da je mogućnost testiranja biometrijskog sistema razvijenog od drugih učesnika kursa posebno interesantna. Mogućnost sagledavanja slabosti konkretnog algoritma za biometrijsko prepoznavanje pomogla im je da ostvare bolje razumevanje problema, kao i motivisala ih da ulože dodatni napor u razvoj sopstvenih sistema. Izazovi postavljeni od strane kursa bili su viđeni kao smernice i pokretačka snaga za nova dostignuća.

Najveći deo učesnika kursa bio je pozitivno motivisan takmičenjem sa drugim učesnicima. Ipak, neki od učesnika izjavili su da su bili više zainteresovani za sadržaj kursa nego za takmičenje sa drugim studentima. Takođe, neki od učesnika su konstatovali da se osećaju ograničeno korišćenim okruženjem za učenje, kao i da je fokus bio stavljen isključivo na određene koncepte iz oblasti biometrije [14].

12 ZAKLJUČAK

Primena biometrijske autentikacije danas je u ekspanziji. U upotrebi su različiti biometrijski modaliteti, kao i algoritmi za rad sa biometrijskim modalitetima. Odabir odgovarajućeg biometrijskog modaliteta, odabir algoritama za rad sa biometrijskim modalitetom, definisanje procedura za pretprocesiranje biometrijskih podataka i određivanje praga osetljivosti samo su neki od izazova koji se postavljaju pred biometrijske inženjere. U slučaju primene multimodalnog pristupa, ovi izazovi se multiplikuju usled većeg broja biometrijskih modaliteta koji se koriste u biometrijskom sistemu. Fokus ove disertacije bio je na unapređenju evaluacije multimodalnih biometrijskih sistema, kako bi se kreiranjem okvira za evaluaciju multimodalnih biometrijskih sistema teškoće vezane za proces evaluacije makar delimično otklonile. U okviru nastavka ovog poglavlja, prikazani su doprinosi disertacije, iznete mogućnosti primene ostvarenih dostignuća i dati predlozi za dalji rad.

12.1 Ostvareni doprinosi

Prilikom izrade doktorske disertacije ostvareni su različiti stručni i naučni doprinosi. Izvršen je kritički pregled i sistematizacija pojmova i metoda koje se koriste u oblastima menadžmenta identiteta, biometrije i multimodalne biometrije. Na osnovu izvršenog pregleda literature, uočene su mogućnosti za unapređenja procesa evaluacije multimodalnih biometrijsksih sistema. To su pre svega nepostojanje objedinjenog modela evaluacije multimodalnih biometrijskih sistema u relevantnoj literaturi, zatim mogućnost analitičkog određivanja praga osetljivosti u multimodalnom biometrijskom sistemu, kao i smanjenje vremena potrebnog za evaluaciju konkretnog multimodalnog biometrijskog sistema.

Za potrebe određivanja praga osetljivosti multimodalnog biometrijskog sistema, predložena je nova metoda. Ona omogućava analitičko određivanja praga osetljivosti u serijskim multimodalnim biometrijskim sistemima na osnovu prethodno zadatih parametara, a od kojih zavisi da li će sistem bude popustljiviji ili pak restriktivno podešen. Prilikom evaluacije utvrđeno je da je preciznost novog pristupa u rangu sa metodama za paralelnu fuziju. Primenom ove metode je moguće učiniti korišćenje sistema lagodnijim za korisnika upotrebom dodatnih biometrijskih modaliteta samo u situacijama kada je to neophodno, a uz očuvanje preciznosti rada sistema.

Na osnovu koncepata uočenih u relevantnim naučnim radovima i tehničkim rešenjima, definisan je objedinjeni model za evaluaciju multimodalnih biometrijskih sistema. Pristup korišćen prilikom njegovog definisanja zasnovan je na MDA (*Model Driven Architecture*) paradigmi i UML (*Unified Modelling Language*) jeziku. Kao deo objedinjenog modela evaluacije definisan je metamodel evaluacije multimodalnih biometrijskih sistema, koji predstavlja ontologiju pojmova bitnih u oblasti evaluacije multimodalnih biometrijskih sistema. Pomoću objedinjenog modela evaluacije multimodalnih biometrijskih sistema, za potrebe modelovanja definisana su odgovarajuća proširenja koncepata UML jezika – profili. Prikazana je primena definisanih profila prilikom modelovanja evaluacije multimodalnih biometrijskih sistema.

U programskom jeziku JAVA razvijen je prototip okvira za evaluaciju multimodalnih biometrijskih sistema. Ovaj okvir omogućava ponovnu primenu funkcionalnosti implementiranih za potrebe evaluacije biometrijskih sistema. Kod direktnog rada sa biometrijskim podacima ovaj okvir koristi funkcije MMBio okvira za razvoj multimodalnih biometrijskih sistema [5]. Primenom MMBio okvira dobija se mogućnost evaluacije algoritama pisanih u različitim programskim jezicima. Takođe, okvir za evaluaciju multimodalnih biometrijskih sistema omogućava evaluaciju biometrijskog sistema i u verifikacionom i u identifikacionom režimu rada, sa mogućnošću prikaza vizuelizacija specifičnih za svaki od režima rada.

Primenom prototipa okvira izvršena je evaluacija konkretnog multimodalnog biometrijskog sistema. Za potrebe ove evaluacije upotrebljena je multimodalna baza biometrijskih podataka prikupljena na Fakultetu organizacionih nauka [136], a za rad sa pojedinačnim biometrijskim modalitetima upotrebljeni su SourceAFIS [201] i OpenCV [203], rešenja otvorenog koda. Fuzija informacija izvršena je na nivou skorova. Od vizuelizacija i parametara evaluacije prikazene su ROC i CMC krive, histogrami i članovi biometrijske menažerije. U ovom konkretnom slučaju korišćenja, primena okvira skraćuje za četiri puta vreme potrebno za evaluaciju multimodalnog biometrijskog sistema u odnosu na vreme potrebno za evaluaciju bez primene okvira.

Takođe, ideja je bila proveriti koliko su znanja stečena prilikom razvoja okvira korisna prilikom edukacije studenata u oblasti biometrije. Stoga, izvršena je analiza edukativnih biometrijskih alata, i dat pregled oblasti gejmifikacije, kao i primene gejmifikacije u obrazovanju. Na osnovu analize relevantne literature, definisani su korisnički zahtevi za edukativni biometrijski alat u procesu obrazovanja. Ovaj alat realizovan je upotrebom nekih od funkcionalnosti okvira za evaluaciju multimodalnih biometrijskih sistema. Pokazano je da primena alata rezultuje u poboljšanju motivacije i ishoda učenja studenata u poređenju sa tradicionalnim pristupom učenja. Društveni doprinos ovog alata ogleda se u unapređenju kvaliteta obrazovanja inženjera u oblasti biometrije.

12.2 Mogućnosti primene

Doprinosi ostvareni u okviru ove doktorske disertacije se mogu primeniti u različitim domenima. Definisani objedinjeni model evaluacije multimodalnih biometrijskih sistema mogu upotrebiti biometrijski inženjeri za potrebe modelovanja evaluacije multimodalnih biometrijskih sistema. Predloženi model za analitičko određivanja praga osetljivosti u serijskim multimodalnim biometrijskim sistemima mogao bi biti upotrebljen od strane projektanata multimodalnih biometrijskih sistema, kako bi na odgovarajući način mogli da izvrše podešavanja sistema u skladu sa zahtevima konkretnog scenarija primene. U zavisnosti od tipa aplikacije, moguće je prilagođavanje tako da sistem bude popustljiviji u situacijama kada iskustvo korisnika ima primat, dok bi na primer u slučaju sistema koji štiti osetljive resurse, kao što su finansijske aplikacije ili kontrola pristupa zaštićenoj lokaciji, sistem bio restriktivnije podešen.

Prototip okvira za evaluaciju multimodalnih biometrijskih sistema se može koristiti za potrebe odabira odgovarajućih biometrijskih modaliteta za određen biometrijski sistem. Okvir za evaluaciju omogućava biometrijskim inženjerima lakše poređenje performansi modaliteta, kao i algoritama za odgovarajući modalitet. Pregledom odgovarajućih vizuelizacija i parametara evaluacije moguće je odabrati najbolji modalitet i algoritam za konkretnu situaciju. Moguća je i provera međusobnog uticaja

različitih komponenti sistema, kao što je rad određenog algoritma za pretprocesiranje sa konkretnim algoritmom za ekstrakciju karakteristika. Sve ove mogućnosti mogu biti od pomoći bilo kompanijama koje razvijaju biometrijske sisteme, bilo organizacijama koje bi želele da implementiraju biometrijski sistem radi lakšeg poređenja alternativa.

Moguća je i upotreba okvira za istraživačke svrhe, prilikom poređenja performansi različitih biometrijskih algoritama. Vreme potrebno za poređenje različitih algoritama na različitim setovima podataka se štedi, a takođe je potrebno i manje napora za kreiranje vizuelizacija i parametara evaluacije. Na taj način bi autori radova iz ove oblasti mogli lakše izvršiti poređenje svojih pristupa sa radovima drugih autora, ili pak jednostavnije testirali svoje algoritme u različitim uslovima, kao i sa raznovrsnim setovima podataka.

Razvijen edukativni biometrijski alat se može primeniti za potrebe edukacije biometrijskih inženjera. Njegova primena je moguća kako u formalnom sistemu obrazovanja, tako i od strane kompanija za potrebe obuke zaposlenih na odgovarajućim kursevima.

12.3 Dalji pravci istraživanja

Za poboljšanje optimizacije praga osetljivosti u multimodalnom biometrijskom sistemu potrebno je istražiti dodatne pristupe za modelovanje raspodela skorova. Na taj način bi se eventualno mogle preciznije odrediti granice za definisanje pragova osetljivosti, a samim tim doprinelo i boljem modelovanju ponašanja sistema.

Dalje, jedan od pravaca istraživanja u okviru ove teme jeste unapređenje okvira za evaluaciju multimodalnih biometrijskih sistema. Prilikom evaluacije trenutno su podržani isključivo *a priori* parametri i načini vizuelizacije kao što su ROC krive. Unapređenje sistema moglo bi da se ostvari implementacijom dodatnih parametara i vizuelizacija. Implementacija interfejsa za dodatne baze biometrijskih podataka takođe bi unapredila kvalitet evaluacije algoritama.

Trenutni fokus okvira bio je pre svega na određivanju preciznosti multimodalnih biometrijskih sistema. Pored preciznosti, dodavanje mogućnosti evaluacije drugih parametara, kao što je na primer brzina izvršavanja algoritama za ekstrakciju biometrijskih karakteristika, omogućilo bi sveobuhvatniju evaluaciju biometrijskih sistema.

13 REČNIK TERMINA I SKRAĆENICA ČESTO KORIŠĆENIH U DISERTACIJI

Biometrijska autentikacija – Prepoznavanje osobe na osnovu njenih fizioloških ili bihejviorističkih karakteristika.

Biometrijski šablon – Digitalna reprezentacija određenog biometrijskog modaliteta konkretne osobe, najčešće predstavljena pomoću vektora. Pominje se i pod terminom biometrijska karakteristika. Algoritmi za ekstrakciju karakteristika transformišu sirove podatke prikupljene od strane biometrijskog senzora u biometrijski šablon, odnosno karakteristiku.

Skor poređenja – Vrednost koja određuje sličnost (ili pak različitost) dve biometrijske karakteristike. U slučaju kada koristimo metrike sličnosti, što je veća vrednost skora poređenja, veća je verovatnoća da dva posmatrana biometrijska šablona pripadaju istom korisniku.

Prag osetljivosti (eng. *threshold*) – Numerička vrednost na osnovu koje biometrijski sistem donosi odluku da li dva biometrijska šablona pripadaju istoj osobi. U slučaju upotrebe metrike sličnosti, ukoliko je vrednost skora poređenja veća od praga osetljivosti, tada biometrijski sistem smatra da oba biometrijska šablona pripadaju istoj osobi. Ukoliko je manja, tada je odluka sistema da biometrijski šabloni pripadaju različitim osobama.

Biometrijska verifikacija – U slučaju rada biometrijskog sistema u verifikacionom režimu, sistem odgovara na pitanje da li biometrijski podaci koji se proveravaju odgovaraju biometrijskim podacima osobe čiji identitet želimo verifikovati.

Biometrijska identifikacija – U slučaju rada biometrijskog sistema u režimu identifikacije, sistem odgovara na pitanje kojoj od osoba iz baze odgovaraju biometrijski podaci koji su predmet provere.

Pravi (eng. *genuine*) korisnik – U kontekstu biometrijskog sistema koji radi u verifikacionom režimu, pravi (eng. *genuine*) korisnik je onaj koji prilikom verifikacije verifikuje sopstveni identitet. U kontekstu skorova poređenja, pravi (eng. *genuine*) skor poređenja je skor dobijen poređenjem biometrijskih karakteristika iste osobe.

Uljez (eng. *imposter*) – U kontekstu biometrijskog sistema koji radi u identifikacionom režimu rada, uljez (eng. *imposter*) je onaj korisnik koji prilikom verifikacije pokušava da prevari sistem, odnosno verifikuje tuđ identitet sa svojim biometrijskim podacima. U kontekstu skorova poređenja, skor poređenja uljeza predstavlja skor dobijen poređenjem biometrijskih karakteristika različitih osoba.

FAR (eng. *False Accept Rate*), FMR (eng. *False Match Rate*) – procenat transakcija, odnosno poređenja šablona u sistemu gde je greškom prihvaćen uljez.

FRR (eng. *False Reject Rate*), FNMR (eng. *False Non Match Rate*) – procenat transakcija, odnosno poređenja šablona u sistemu gde je greškom odbačen legitimni korisnik .

GAR (eng. *Genuine Acceptance Rate*) – izračunava se kao razlika jedinice i FNMR metrike, procenat ispravno prihvaćenih transakcija pravih korisnika.

ROC (eng. *Receiver Operating Characteristic*) kriva – Na osama sadrži iznose FMR i GAR metrika. Svaka tačka ove krive prikazuje vrednosti ove dve metrike za jednu konkretnu vrednost praga osetljivosti biometrijskog sistema.

EER (eng. *Equal Error Rate*) – vrednost FMR i FNMR metrika u tački na ROC krivi gde su njihove vrednosti jednake.

TER (eng. *Total Error Rate*) – Zbir vrednosti FMR i FNMR metrika u određenoj tački ROC krive.

CMC kriva (eng. *Cumulative Match Characteristic*) – vizuelizacija evaluacije koja pokazuje stopu identifikacije na određenom rangu prepoznavanja. U slučaju idealnog biometrijskog sistema, preciznost bi bila potpuna već na prvom rangu.

Biometrijska menažerija – Termin koji se koristi da označi grupe korisnika koji nesrazmerno svojoj brojnosti doprinose FRR ili FMR metrici celog biometrijskog sistema . Članovi osnovnog skupa Dodingtonove biometrijske menažerije su ovce, koze, jagnjad i vukovi [3]. Koze su osobe koje imaju problema prilikom poređenja sa sopstvenim biometrijskim šablonima, odnosno nesrazmerno svojoj brojnosti doprinose FRR metrici celog sistema. Termin jagnjad označava osobe koje je lako oponašati, dok se pod vukovima podrazumevaju osobe koje lako oponašaju druge korisnike biometrijskog sistema. Jagnjad i vukovi nesrazmerno svojoj brojnosti doprinose FMR metrici biometrijskog sistema.

14 REFERENCE

[1] K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology, vol. 14, pp. 4-20, 2004.

[2] N. Yager and T. Dunstone, "The biometric menagerie," IEEE transactions on pattern analysis and machine intelligence, vol. 32, pp. 220-230, 2008.

[3] G. Doddington, W. Liggett, A. Martin, M. Przybocki and D. Reynolds, "Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation," in 5th International Conference on Spoken Language Processing, Sydney, Australia, 1998.

[4] B. Jovanović, I. Milenković, M. Bogićević-Sretenović and D. Simić, "Extending identity management system with multimodal biometric authentication," Computer Science and Information Systems, vol. 13, pp. 313-334, 2016.

[5] M. Milovanović, M. Minović and S. Dušan, "Interoperability Framework for Multimodal Biometry: Open Source in Action," Journal of Universal Computer Science, vol. 18, pp. 1558-1575, 2012.

[6] V. Stavljanin, I. Milenkovic and U. Šošević, "Educational website conversion improvement using gamification," The International journal of engineering education, vol. 32, pp. 563-573, 2016.

[7] Jacobson, G. Booch, J. Rumbaugh, J. Rumbaugh and G. Booch, The unified software development process, vol. 1, Addison-Wesley Reading, 1999.

[8] S. Slone, "Identity management," A white paper: The open group identity management work area, 2004.

[9] P. J. Windley, Digital Identity: Unmasking identity management architecture (IMA), O'Reilly Media, Inc., 2005.

[10] I. Milenković, U. Šošević and D. Simić, "Architectures of comprehensive identity and access management," in Proceedings in EIIC-1st Electronic International Interdisciplinary Conference, 2012.

[11] G. Prasad and U. Rajbhandari, Identity management on a shoestring, InfoQ, 2012. Available: https://www.infoq.com/minibooks/Identity-Management-Shoestring/

[12] J. Hermans and P. Valkenburg, "European Identity and Access Management Survey," KPMG and Everett, 2009.

[13] K. Helkala and T. H. Bakås, "National Password Security Survey: Results.," in EISMC, p. 23-33, 2013.

[14] I. Milenković, U. Šošević, D. Simić, M. Minović and M. Milovanović, "Improving student engagement in a biometric classroom: the contribution of gamification," Universal Access in the Information Society, vol. 18, pp. 523-532, 2019.

[15] K. Jain, K. Nandakumar and A. Nagar, "Biometric template security," EURASIP Journal on advances in signal processing, vol. 2008, p. 1–17, 2008. doi: https://doi.org/10.1155/2008/579416

[16] I. Milenković, O. Latinović and D. Simić, "Using Kerberos protocol for single sign-on in identity management systems," JITA-JOURNAL OF INFORMATION TECHNOLOGY AND APLICATIONS, vol. 5, pp. 27-33, 2013. doi: 10.7251/JIT1301027M

[17] R. Dhamija and L. Dusseault, "The seven flaws of identity management: Usability and security challenges," IEEE Security & Privacy, vol. 6, pp. 24-29, 2008. doi: 10.1109/MSP.2008.49
[18] M. Bogićević, I. Milenković and D. Simić, "Identity Management—A Survey," in Innovative Management and Firm Performance, Springer, 2014, pp. 370-384.
[19] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, pp. 352-375, 2018.
[20] R. Grinberg, "Bitcoin: An innovative alternative digital currency," Hastings Sci. & Tech. LJ, vol. 4, p. 159, 2012.
[21] R. Thoomu, "Hyperledger Fabric documentation - Why Hyperledger Fabric," 2017. [Online]. Available: https://fabrictestdocs.readthedocs.io/en/latest/whyfabric.html. [Accessed 14 April 2020].
[22] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," IEEE Security & Privacy, vol. 16, pp. 20-29, 2018. doi: 10.1109/MSP.2018.3111247
[23] Reed, J. Law and D. Hardman, "The technical foundations of Sovrin," 2016. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf. [Accessed 10 October 2020]
[24] ChainZy, "Personal Identity - IDChainZ: KYC and AML Solutions," [Online]. Available: https://www.chainzy.com/media/documents/IDchainZFlyer.pdf. [Accessed 16 May 2020].
[25] L. Lesavre, P. Varin, P. Mell, M. Davidson and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," 2020. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf
[26] O. Delgado-Mohatar, J. Fierrez, R. Tolosana and R. Vera-Rodriguez, "Blockchain and biometrics: A first look into opportunities and challenges," in International Congress on Blockchain and Applications, pp. 169-177, 2019. doi: 10.1007/978-3-030-23813-1_21
[27] P. Garcia, "Biometrics on the blockchain," Biometric Technology Today, vol. 2018, pp. 5-7, 2018. doi: 10.1016/S0969-4765(18)30067-5
[28] INTELid, "INTELid partners with ValidSoft to bring Voice Biometric technology to Blockchain," 5 6 2019. [Online]. Available: https://www.intelid.com/post/intelid-partners-with-validsoft-to-bring-voice-biometric-technology-to-blockchain. [Accessed 16 May 2020].
[29] Blinking, "Multi-Factor Biometric Authentication," [Online]. Available: https://blinking.id/multi-factor-biometric-authentication.html. [Accessed 16 May 2020].
[30] Zamna, "Biometrics," [Online]. Available: https://zamna.com/biometrics/. [Accessed 16 May 2020].
[31] P. Jarratt, "Agora partners with Onfido to enable the future of frictionless e-voting," 24 9 2019. [Online]. Available: https://onfido.com/resources/blog/agora-partners-with-onfido-to-enable-the-future-of-frictionless-e-voting. [Accessed 16 May 2020].
[32] K. Jain, P. Flynn and A. A. Ross, Handbook of biometrics, Springer Science & Business Media, 2007. doi: 10.1007/978-0-387-71041-9
[33] Amos, B. Ludwiczuk and M. Satyanarayanan, "OpenFace - Models and Accuracies," [Online]. Available:

https://cmusatyalab.github.io/openface/models-and-accuracies/. [Accessed 12 May 2020].
[34] H. C. Lee and R. E. Gaensslen, Advances in fingerprint technology, Elsevier, New York, 2001.
[35] Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of fingerprint recognition, Springer Science & Business Media, 2009. doi: 10.1007/978-1-84882-254-2
[36] Federal Bureau of Investigation. National Science and Technology Council, "Fingerprint recognition," [Online]. Available: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf. [Accessed 10 May 2020].
[37] United States Congress, Senate Committee on the Judicary, FBI Statutory Charter: Hearings Before the Committee on the Judiciary, United States Senate, Ninety-fifth Congress, Second Session ... April 20 and 25, 1978, U.S. Government Printing Office, 1979.
[38] P. Sidlauskas, 3D hand profile identification apparatus, Google Patents, 1988.
[39] R. J. Hays, "INS Passenger Accelerated Service System (INSPASS)," 4 1 1996. [Online]. Available: https://web.archive.org/web/20070203233102/http://www.biometrics.org/REPORTS/INSPASS.html. [Accessed 10 May 2020].
[40] N. Duta, "A survey of biometric technology based on hand shape," Pattern Recognition, vol. 42, pp. 2797-2806, 2009. doi: 10.1016/j.patcog.2009.02.007
[41] J. S. Dempsey and L. S. Forst, An introduction to policing, Cengage Learning, 2013.
[42] C. I. Watson, G. P. Fiumara, E. Tabassi, S. L. Cheng, P. A. Flanagan and W. J. Salamon, "Fingerprint vendor technology evaluation," 2015. doi: 10.6028/NIST.IR.8034
[43] R. Raghavendra, C. Busch and B. Yang, "Scaling-robust fingerprint verification with smartphone camera in real-life scenarios," in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013. doi: 10.1109/BTAS.2013.6712736
[44] Veridium, "4F: TouchlessID funkcionalnost," [Online]. Available: https://veridiumid.com/4f-touchless/. [Accessed 27 April 2020].
[45] C. Lin and A. Kumar, "Contactless and partial 3D fingerprint recognition using multi-view deep representation," Pattern Recognition, vol. 83, pp. 314-327, 2018. doi: 10.1016/j.patcog.2018.05.004
[46] W. Lee, S. Cho, H. Choi and J. Kim, "Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners," Expert Systems with Applications, vol. 87, pp. 183-198, 2017. doi: 10.1016/j.eswa.2017.06.019
[47] K. Cao and A. K. Jain, "Automated latent fingerprint recognition," IEEE transactions on pattern analysis and machine intelligence, vol. 41, pp. 788-800, 2018. doi: 10.1109/TPAMI.2018.2818162
[48] S. Crihalmeanu, A. Ross, S. Schuckers and L. Hornak, "A protocol for multibiometric data acquisition, storage and dissemination," in Technical Report, WVU, Lane Department of Computer Science and Electrical Engineering, 2007.
[49] T. Ahonen, A. Hadid and M. Pietikäinen, "Face recognition with local binary patterns," in European conference on computer vision, pp 469-481, 2004. doi: 10.1007/978-3-540-24670-1_36
[50] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of cognitive neuroscience, vol. 3, pp. 71-86, 1991.

[51] S. Lawrence, C. L. Giles, A. C. Tsoi and A. D. Back, "Face recognition: A convolutional neural-network approach," IEEE transactions on neural networks, vol. 8, pp. 98-113, 1997. doi: 10.1109/72.554195
[52] O. M. Parkhi, A. Vedaldi and A. Zisserman, "Deep face recognition," British Machine Vision Association, pp. 1-12, 2015.
[53] Y. Sun, Y. Chen, X. Wang and X. Tang, "Deep learning face representation by joint identification-verification," in Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2, pp 1988-1996, 2014.
[54] M. Ngan, P. Grother and K. Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT)," 2021. Available: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing. [Accessed 16 April 2021]
[55] M. Krišto and M. Ivasic-Kos, "An overview of thermal face recognition methods," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018. doi: 10.23919/MIPRO.2018.8400200
[56] Federal Bureau of Investigation. National Science and Technology Council, "Iris recognition," [Online]. Available: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-iris-recognition.pdf. [Accessed 30 April 2020].
[57] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE transactions on pattern analysis and machine intelligence, vol. 15, pp. 1148-1161, 1993. doi: 10.1109/34.244676
[58] J. G. Daugman, Biometric personal identification system based on iris analysis, Google Patents, 1994.
[59] W. Quinn, G. W. Quinn, P. Grother and J. Matey, IREX IX part one: Performance of Iris recognition algorithms, US Department of Commerce, National Institute of Standards and Technology, 2018.
[60] Czajka and K. W. Bowyer, "Presentation attack detection for iris recognition: An assessment of the state-of-the-art," ACM Computing Surveys (CSUR), vol. 51, pp. 1-35, 2018. doi: 10.1145/3232849
[61] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan and A. Ross, "Long range iris recognition: A survey," Pattern Recognition, vol. 72, pp. 123-143, 2017. doi: 10.1016/j.patcog.2017.05.021
[62] Deutschmann, P. Nordström and L. Nilsson, "Continuous authentication using behavioral biometrics," IT Professional, vol. 15, pp. 12-15, 2013. doi: 10.1109/MITP.2013.50
[63] Buriro, "Behavioral biometrics for smartphone user authentication," Ph.D. dissertation, University of Trento, 2017. Available: http://eprints-phd.biblio.unitn.it/1935/
[64] Buriro, B. Crispo and M. Conti, "AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones," Journal of information security and applications, vol. 44, pp. 89-103, 2019. doi: 10.1016/j.jisa.2018.11.008
[65] R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," Ieee Access, vol. 6, pp. 5128-5138, 2018. doi: 10.1109/ACCESS.2018.2793966
[66] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas and

others, "BiosecurID: a multimodal biometric database," Pattern Analysis and Applications, vol. 13, pp. 235-246, 2010. doi: 10.1007/s10044-009-0151-4

[67] M. Milovanović, "Primena CBIR tehnika u biometrijskoj identifikaciji osoba na osnovu hoda," Doktorska disertacija, Univerzitet u Beogradu, Fakultet organizacionih nauka, 2013.

[68] K. Shiraga, Y. Makihara, D. Muramatsu, T. Echigo and Y. Yagi, "Geinet: View-invariant gait recognition using a convolutional neural network," in 2016 international conference on biometrics (ICB), 2016. doi: 10.1109/ICB.2016.7550060

[69] S. M. H. Bari and M. L. Gavrilova, "Artificial Neural Network Based Gait Recognition Using Kinect Sensor," IEEE Access, vol. 7, pp. 162708-162722, 2019. doi: 10.1109/ACCESS.2019.2952065

[70] M. Milovanovic, M. Minovic and D. Starcevic, "Walking in colors: human gait recognition using Kinect and CBIR," IEEE MultiMedia, vol. 20, pp. 28-36, 2013. doi: 10.1109/MMUL.2013.16

[71] J. Sun, Y. Wang, J. Li, W. Wan, D. Cheng and H. Zhang, "View-invariant gait recognition based on kinect skeleton feature," Multimedia Tools and Applications, vol. 77, pp. 24909-24935, 2018. doi: 10.1007/s11042-018-5722-1

[72] R. San-Segundo, J. D. Echeverry-Correa, C. Salamea-Palacios, S. L. Lutfi and J. M. Pardo, "I-vector analysis for gait-based person identification using smartphone inertial signals," Pervasive and Mobile Computing, vol. 38, pp. 140-153, 2017. doi: 10.1016/j.pmcj.2016.09.007

[73] W. Wang, A. X. Liu and M. Shahzad, "Gait recognition using wifi signals," in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 363-373, 2016. doi: 10.1145/2971648.2971670

[74] T. Kinnunen and H. Li, "An overview of text-independent speaker recognition: From features to supervectors," Speech communication, vol. 52, pp. 12-40, 2010. doi: 10.1016/j.specom.2009.08.009

[75] W. M. Campbell, D. E. Sturim and D. A. Reynolds, "Support vector machines using GMM supervectors for speaker verification," IEEE signal processing letters, vol. 13, pp. 308-311, 2006. doi: 10.1109/LSP.2006.870086

[76] W. Chen, Q. Hong and X. Li, "GMM-UBM for text-dependent speaker recognition," in 2012 International Conference on Audio, Language and Image Processing, 2012. doi: 10.1109/ICALIP.2012.6376656

[77] N. Dehak, P. J. Kenny, R. Dehak, P. Dumouchel and P. Ouellet, "Front-end factor analysis for speaker verification," IEEE Transactions on Audio, Speech, and Language Processing, vol. 19, pp. 788-798, 2010. doi: 10.1109/TASL.2010.2064307

[78] D. Snyder, D. Garcia-Romero, D. Povey and S. Khudanpur, "Deep Neural Network Embeddings for Text-Independent Speaker Verification.," in Interspeech, pp. 999-1003, 2017.

[79] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey and S. Khudanpur, "X-vectors: Robust dnn embeddings for speaker recognition," in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018. doi: 10.1109/ICASSP.2018.8461375

[80] S. O. Sadjadi, C. S. Greenberg, E. Singer, D. A. Reynolds and L. Mason, "NIST 2020 CTS Speaker Recognition Challenge Evaluation Plan," 2020. Available: https://www.nist.gov/system/files/documents/2020/08/06/2020_NIST_CTS_Challenge_Evaluation_Plan_v3_3.pdf [Accessed 29 April 2020]

[81] National Research Council (US) Whither Biometrics Comittee; Pato JN, Millett LI, editors, "Biometric Recognition: Challenges and Opportunities," National Academies Press, Washington (DC), 2010.
[82] A. Ross, K. Nandakumar and A. K. Jain, Handbook of multibiometrics, vol. 6, Springer Science & Business Media, 2006. doi: 10.1007/0-387-33123-9
[83] W. Y. Yau, T. P. Chen and P. Morguet, "Benchmarking of fingerprint sensors," in International Workshop on Biometric Authentication, pp. 89-99, 2004. doi: 10.1007/978-3-540-25976-3_9
[84] Lanitis, "A survey of the effects of aging on biometric identity verification," International Journal of Biometrics, vol. 2, p. 34, 2010. doi: 10.1504/IJBM.2010.030415
[85] S. K. Modi, S. J. Elliott, J. Whetsone and H. Kim, "Impact of age groups on fingerprint recognition performance," in 2007 IEEE Workshop on Automatic Identification Advanced Technologies, 2007. doi: 10.1109/AUTOID.2007.380586
[86] S. Ö. Arik, M. Chrzanowski, A. Coates, G. Diamos, A. Gibiansky, Y. Kang, X. Li, J. Miller, A. Ng, J. Raiman and others, "Deep voice: Real-time neural text-to-speech," in Proceedings of the 34th International Conference on Machine Learning-Volume 70, pp. 195-204, 2017.
[87] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial" gummy" fingers on fingerprint systems," in Optical Security and Counterfeit Deterrence Techniques IV, 2002. doi: https://doi.org/10.1117/12.462719
[88] M. Choudhary, V. Tiwari and U. Venkanna, "Biometric spoofing: Iris presentation attack detection and contact lens discrimination through score-level fusion," Applied Soft Computing, p. 106-206, 2020. doi: 10.1016/j.asoc.2020.106206
[89] S. Marcel, M. S. Nixon and S. Z. Li, Handbook of biometric anti-spoofing, vol. 1, Springer, 2014. doi: 10.1007/978-3-319-92627-8
[90] Apple, "About Face ID advanced technology," 26 2 2020. [Online]. Available: https://support.apple.com/en-us/HT208108. [Accessed 21 June 2020].
[91] I. Milenković, K. Živković and D. Simić, "Application of multimodal biometrics in access control systems," in Symposium proceedings-XV International symposium Symorg 2016: Reshaping the Future Through Sustainable Business Development and Entepreneurship, pp. 762-771, 2016.
[92] N. Saini and A. Sinha, "Face and palmprint multimodal biometric systems using Gabor--Wigner transform as feature extraction," Pattern Analysis and Applications, vol. 18, pp. 921-932, 2015. doi: 10.1007/s10044-014-0414-6
[93] R. Snelick, U. Uludag, A. Mink, M. Indovina and 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, pp. 450-455, 2005. doi: 10.1109/TPAMI.2005.57
[94] M. Sim, H. Asmuni, R. Hassan and R. M. Othman, "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images," Expert Systems with Applications, vol. 41, pp. 5390-5404, 2014. doi: 10.1016/j.eswa.2014.02.051
[95] AT&T Laboratories Cambridge, "The Database of Faces," 2001. [Online]. Available: http://cam-orl.co.uk/facedatabase.html. [Accessed 21 June 2020].
[96] Proença and L. A. Alexandre, "UBIRIS: A noisy iris image database," in International Conference on Image Analysis and Processing, pp. 970-977, 2005. doi: 10.1007/11553595_119

[97] M. M. Monwar and M. L. Gavrilova, "Multimodal biometric system using rank-level fusion approach," IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 39, pp. 867-878, 2009. doi: 10.1109/TSMCB.2008.2009071

[98] M. M. Monwar and M. Gavrilova, "A robust authentication system using multiple biometrics," in Computer and Information Science, Springer, 2008, pp. 189-201. doi: https://doi.org/10.1007/978-3-540-79187-4_17

[99] Y.-H. Khoo, B.-M. Goi, T.-Y. Chai, Y.-L. Lai and Z. Jin, "Multimodal biometrics system using feature-level fusion of iris and fingerprint," in Proceedings of the 2nd International Conference on Advances in Image Processing, pp. 6-10, 2018. doi: 10.1145/3239576.3239599

[100] G. Goswami, P. Mittal, A. Majumdar, M. Vatsa and R. Singh, "Group sparse representation based classification for multi-feature multimodal biometrics," Information Fusion, vol. 32, pp. 3-12, 2016. doi: 10.1016/j.inffus.2015.06.007

[101] M. Sultana, P. P. Paul and M. L. Gavrilova, "Social behavioral information fusion in multimodal biometrics," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, pp. 2176-2187, 2017.

[102] Lupu and V. Lupu, "Multimodal biometrics for access control in an intelligent car," in 2007 International Symposium on Computational Intelligence and Intelligent Informatics, pp. 261-267, 2007. doi: 10.1109/ISCIII.2007.367399

[103] M. Beattie, B. V. K. V. Kumar, S. Lucey and O. Tonguz, "Building access control using coordinated biometric verification," in Workshop Proceedings - Biometrics: Challenges arising from theory to practice, Satellite Workshop to IEEE-ICPR 2004, pp. 9-12, 2004.

[104] M. K. Dehnavi and N. P. Fard, "Presenting a multimodal biometric model for tracking the students in virtual classes," Procedia-Social and Behavioral Sciences, vol. 15, pp. 3456-3462, 2011. doi: 10.1016/j.sbspro.2011.04.318

[105] Claroline Connect LMS, "Oficijelna github stranica," [Online]. Available: https://github.com/claroline/Distribution. [Accessed 23 May 2020].

[106] Aware, "Knomi - oficijelna stranica," [Online]. Available: https://www.aware.com/knomi-mobile-biometric-authentication/. [Accessed 23 May 2020].

[107] Aware, "White paper - Mobile Biometrics and Liveness Detection," 1 2020. [Online]. Available: https://www.aware.com/wp-content/uploads/2020/01/CS_Liveness-LatAM_email.pdf. [Accessed 23 May 2020].

[108] InCadence, "INCADENCE AWARDED $12.6M CONTRACT TO SUPPORT DEPARTMENT OF STATE," 16 8 2016. [Online]. Available: https://www.incadencecorp.com/2016/08/16/incadence-awarded-12-6m-contract-to-support-department-of-state/. [Accessed 24 May 2020].

[109] Daon, "Case study : USAA," [Online]. Available: https://www.daon.com/resources/case-studies/usaa. [Accessed 24 May 2020].

[110] Daon, "Case study : Mox," [Online]. Available: https://www.daon.com/resources/case-studies/mox-bank. [Accessed 24 May 2020].

[111] Idemia, "Kenya selects Safran Identity & Security to accompany its 2017 elections," 27 4 2017. [Online]. Available: https://www.idemia.com/press-release/kenya-selects-safran-identity-security-accompany-its-2017-elections-2017-04-27. [Accessed 25 May 2020].

[112] L. Said-Moorhouse and F. Karimi, "CNN - How Kenya's presidential election unraveled," 25 10 2017. [Online]. Available: https://edition.cnn.com/2017/10/25/africa/kenya-election/index.html. [Accessed 25 May 2020].
[113] N. Poh, C. H. Chan, J. Kittler, J. Fierrez and J. Galbally, "Description of metrics for the evaluation of biometric performance," Biometrics Evaluation and Testing, 2012. Available: https://www.beat-eu.org/project/deliverables-public/d3.3-description-of-metrics-for-the-evaluation-of-biometric-performance
[114] T. Mansfield, G. Kelly, D. Chandler and J. Kane, "Biometric product testing final report," Contract, vol. 92, p. 309, 2001.
[115] L. Wayman, "Technical testing and evaluation of biometric identification devices," in Biometrics, Springer, 1996, pp. 345-368.
[116] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana and F. Scotti, "Accuracy and performance of biometric systems," in Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference (IEEE Cat. No. 04CH37510), pp. 510-515, 2004. doi: 10.1109/IMTC.2004.1351099
[117] S. Bengio and J. Mariéthoz, "The expected performance curve: a new assessment measure for person authentication," 2003. Available: http://publications.idiap.ch/downloads/reports/2003/rr03-84.pdf
[118] Milenković, U. Šošević and M. Minović, "Razvojni okvir za poređenje biometrijskih algoritama," in Zbornik radova Symopis 2014, 2014.
[119] G. R. Doddington, M. A. Przybocki, A. F. Martin and D. A. Reynolds, "The NIST speaker recognition evaluation–overview, methodology, systems, results, perspective," Speech communication, vol. 31, p. 225–254, 2000. doi: 10.1016/S0167-6393(99)00080-1
[120] M. N. Teli, J. R. Beveridge, P. J. Phillips, G. H. Givens, D. S. Bolme and B. A. Draper, "Biometric zoos: Theory and experimental evidence," in 2011 International Joint Conference on Biometrics (IJCB), pp. 1-8, 2011. doi: 10.1109/IJCB.2011.6117479
[121] P. J. Phillips, K. W. Boyer, P. J. Flynn, A. J. O'Toole, P. J. Phillips, C. L. Schott, W. T. Scruggs and M. Sharpe, "FRVT 2006 and ICE 2006 large-scale results," 2007. Available: https://face-rec.org/vendors/FRVT2006andICE2006LargeScaleReport.pdf
[122] Ross, A. Rattani and M. Tistarelli, "Exploiting the “doddington zoo” effect in biometric fusion" in 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, pp. 1-7, 2009. doi: 10.1109/BTAS.2009.5339011
[123] N. Poh and J. Kittler, "Incorporating model-specific score distribution in speaker verification systems," IEEE transactions on audio, speech, and language processing, vol. 16, pp. 594-606, 2008.
[124] K.-C. Lee, J. Ho and D. J. Kriegman, "Acquiring linear subspaces for face recognition under variable lighting," IEEE Transactions on pattern analysis and machine intelligence, vol. 27, pp. 684-698, 2005.
[125] G. B. Huang and E. Learned-Miller, "Labeled faces in the wild: Updates and new reporting procedures," Dept. Comput. Sci., Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep, p. 14–003, 2014.
[126] T. L. Berg, A. C. Berg, J. Edwards and D. A. Forsyth, "Who's in the picture," in Advances in neural information processing systems, pp. 137-144, 2005.
[127] M. Jones and P. Viola, "Fast multi-view face detection," Mitsubishi Electric Research Lab TR-20003-96, vol. 3, p. 2, 2003.

[128] Yi, Z. Lei, S. Liao and S. Z. Li, "Learning face representation from scratch," arXiv preprint arXiv:1411.7923, 2014.
[129] Y. Guo, L. Zhang, Y. Hu, X. He and J. Gao, "Ms-celeb-1m: A dataset and benchmark for large-scale face recognition," in European conference on computer vision, 2016. doi: 10.1007/978-3-319-46487-9_6
[130] R. H. Woo, A. Park and T. J. Hazen, "The MIT mobile device speaker verification corpus: data collection and preliminary experiments," in 2006 IEEE Odyssey-The Speaker and Language Recognition Workshop, pp. 1-6, 2006. doi: 10.1109/ODYSSEY.2006.248083
[131] M. McLaren, L. Ferrer, D. Castan and A. Lawson, "The Speakers in the Wild (SITW) speaker recognition database," in Interspeech, pp. 818-822, 2016. doi: 10.21437/Interspeech.2016-1129
[132] Nagrani, J. S. Chung, W. Xie and A. Zisserman, "Voxceleb: Large-scale speaker verification in the wild," Computer Speech & Language, vol. 60, 2020. doi: 10.1016/j.csl.2019.101027
[133] National Institute for Standardisation and Technology, "NIST Technical Note 2007 - NIST Special Database 302," 12 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2007.pdf. [Accessed 31 May 2020].
[134] Y. I. Shehu, A. Ruiz-Garcia, V. Palade and A. James, "Detection of fingerprint alterations using deep convolutional neural networks," in International Conference on Artificial Neural Networks, pp. 51-60, 2018. doi: 10.1007/978-3-030-01418-6_6
[135] Institute of Automation Chinese Academy of Sciences, "Note on CASIA-IrisV4," [Online]. Available: http://www.cbsr.ia.ac.cn/china/Iris%20Databases%20CH.asp. [Accessed 31 May 2020].
[136] Starčević, M. Minović, M. Milovanović, D. Simić, M. Bogićević and B. Jovanović, "Tehničko rešenje - Multimodalna baza multimedijalnih biometrijskih podataka," Fakultet organizacionih nauka, Beograd, 2011.
[137] National Institute of Standards and Technology, "NIST Technical Note 2002 - NIST Special Database 301," July 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2002.pdf. [Accessed 30 May 2020].
[138] Q. Zhang, Y. Yin, D.-C. Zhan and J. Peng, "A novel serial multimodal biometrics framework based on semisupervised learning techniques," IEEE transactions on information forensics and security, vol. 9, pp. 1681-1694, 2014. doi: 10.1109/TIFS.2014.2346703
[139] G. L. Marcialis, P. Mastinu and F. Roli, "Serial fusion of multi-modal biometric systems," in 2010 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, pp. 1-7, 2010. doi: doi: 10.1109/BIOMS.2010.5610438.
[140] M. Stanojević, I. Milenković, D. Starčević and B. Stanojević, "Optimization of thresholds in serial multimodal biometric systems," in 2016 6th International Conference on Computers Communications and Control (ICCCC), pp. 140-146, 2016. doi: 10.1109/ICCCC.2016.7496752.
[141] M. Stanojević, I. Milenković, D. Starčević and B. Stanojević, "Continuous Distribution Approximation and Thresholds Optimization in Serial Multi-Modal

Biometric Systems," International Journal of Computers Communications & Control, vol. 11, pp. 720-733, 2016. doi: 10.15837/ijccc.2016.5.2683
[142] NIST, "NIST Biometric Scores Set (BSSR1) database," [Online]. Available: https://www.nist.gov/itl/iad/image-group/nist-biometric-scores-set-bssr1. [Accessed 20 May 2020].
[143] Kumar and A. Kumar, "Adaptive management of multimodal biometrics fusion using ant colony optimization," Information Fusion, vol. 32, pp. 49-63, 2016. doi: 10.1016/j.inffus.2015.09.002
[144] H. Mehrotra, R. Singh, M. Vatsa and B. Majhi, "Incremental granular relevance vector machine: A case study in multimodal biometrics," Pattern Recognition, vol. 56, pp. 63-76, 2016. doi: 10.1016/j.patcog.2015.11.013
[145] S. Tulyakov, J. Li and V. Govindaraju, "Enrolled template specific decisions and combinations in verification systems" in 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, pp. 1-7, 2008. doi: 10.1109/BTAS.2008.4699320.
[146] M. Villegas and R. Paredes, "Score fusion by maximizing the area under the roc curve," in Iberian Conference on Pattern Recognition and Image Analysis, pp. 473-480, 2009. doi: 10.1007/978-3-642-02172-5_61
[147] Object Management Group, "MDA Guide rev. 2.0," 1 June 2014. [Online]. Available: https://www.omg.org/cgi-bin/doc?ormsc/14-06-01.pdf. [Accessed 13 12 2020].
[148] Object Management Group, "MDA Specifications," [Online]. Available: https://www.omg.org/mda/specs.htm. [Accessed 29 February 2020].
[149] OMG, " Meta Object Facility (MOF) Core Specification," October 2019. [Online]. Available: https://www.omg.org/spec/MOF/2.5.1. [Accessed 6 March 2020].
[150] Watson, "Visual Modelling: past, present and future," UML White paper, vol. 28, 2008. Available: https://www.uml.org/Visual_Modeling.pdf. [Accessed 18 March 2020].
[151] G. Booch, The unified modeling language user guide, Pearson Education India, 2005.
[152] OCUP 2 Examination Team, "Meta-Modeling and the OMG Meta Object Facility (MOF)," March 2017. [Online]. Available: https://www.omg.org/ocup-2/documents/Meta-ModelingAndtheMOF.pdf.
[153] Millenković, M. Minović and D. Simić, "Metamodel za razvoj i evaluaciju multimodalnih biometrijskih sistema," in Proceedings of INFOTECH ICT Conference & Exhibition, Arandjelovac, 2019.
[154] M. Minović, "Razvoj edukativnih igara zasnovan na MDA pristupu," Doktorska disertacija, Fakultet organizacionih nauka, Univerzitet u Beogradu, 2010.
[155] W. I. Grosky, "Managing multimedia information in database systems," Communications of the ACM, vol. 40, pp. 72-80, 1997. doi: 10.1145/265563.265574
[156] L. Wayman, A. K. Jain, D. Maltoni and D. Maio, Biometric systems: Technology, design and performance evaluation, Springer Science & Business Media, 2005. doi: 10.1007/b138151
[157] E. Rosenberg, F. Bimbot and S. Parthasarathy, "Overview of speaker recognition," in Springer Handbook of Speech Processing, Springer, pp. 725-742, 2008
[158] Harvey, J. Campbell and A. Adler, "Characterization of biometric template aging in a multiyear, multivendor longitudinal fingerprint matching study," IEEE

Transactions on Instrumentation and Measurement, vol. 68, pp. 1071-1079, 2018. doi: 10.1109/TIM.2018.2861998
[159] S. P. Fenker and K. W. Bowyer, "Experimental evidence of a template aging effect in iris biometrics," in 2011 IEEE Workshop on Applications of Computer Vision (WACV), pp. 232-239, 2011. doi: 10.1109/WACV.2011.5711508.
[160] C. Le and R. Jain, "A survey of biometrics security systems," EEUU. Washington University in St. Louis, 2009.
[161] Chingovska, N. Erdogmus, A. Anjos and S. Marcel, "Face recognition systems under spoofing attacks," in Face Recognition Across the Imaging Spectrum, Springer, 2016, pp. 165-194. doi: 10.1007/978-3-319-28501-6_8
[162] P. J. Phillips, A. Martin, C. L. Wilson and M. Przybocki, "An introduction evaluating biometric systems," Computer, vol. 33, pp. 56-63, 2000. doi: 10.1109/2.820040
[163] P. Grother, P. Grother, M. Ngan, K. Hanaoka, C. Boehnen and L. Ericson, The 2017 IARPA Face Recognition Prize Challenge (FRPC), US Department of Commerce, National Institute of Standards and Technology, 2017.
[164] Alonso-Fernandez, F. Roli, G. L. Marcialis, J. Fierrez and J. Ortega-Garcia, "Comparison of fingerprint quality measures using an optical and a capacitive sensor," in 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, pp. 1-6, 2007. doi: 10.1109/BTAS.2007.4401956
[165] A. Olsen, M. Dusio and C. Busch, "Fingerprint skin moisture impact on biometric performance," in 3rd International Workshop on Biometrics and Forensics (IWBF 2015), pp. 1-6, 2015.
[166] J. M. Dawson, S. C. Leffel, C. Whitelam and T. Bourlai, "Collection of multispectral biometric data for cross-spectral identification applications," in Face Recognition Across the Imaging Spectrum, Springer, pp. 21-46, 2016.
[167] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet and K. Ko, "User's guide to NIST biometric image software (NBIS)," 2007. doi: 10.6028/NIST.IR.7392
[168] Ž. Obrenović, "User Interfaces Development based on the Unified Model of Human Computer Interaction," PhD Theses, Faculty of Electrical Engineering, University of Belgrade, 2004.
[169] Z. Bikicki, I. Milenković and D. Starčević, "Using 3D Models for Improving Face Recognition," JITA-JOURNAL OF INFORMATION TECHNOLOGY AND APLICATIONS, vol. 8, pp. 55-61, 2014. doi: 10.7251/JIT1402055B
[170] Genovese, V. Piuri and F. Scotti, Touchless palmprint recognition systems, vol. 60, Springer, 2014. doi: https://doi.org/10.1007/978-3-319-10365-5
[171] Fowler and U. M. L. Distilled, A brief guide to the Standard Object Modeling Language, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 2003.
[172] Y. Verginadis, N. Papageorgiou, D. Apostolou and G. Mentzas, "A review of patterns in collaborative work," in Proceedings of the 16th ACM international conference on Supporting Group Work, 2010.
[173] W. Chen, M. J. Er and S. Wu, "Illumination compensation and normalization for robust face recognition using discrete cosine transform in logarithm domain," IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 36, pp. 458-466, 2006. doi: 10.1109/TSMCB.2005.857353.
[174] X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," IEEE transactions on image processing, vol. 19, pp. 1635-1650, 2010. doi: 10.1109/TIP.2010.2042645

[175] S. D. Bharkad and M. Kokare, "Performance evaluation of distance metrics: application to fingerprint recognition," International Journal of Pattern Recognition and Artificial Intelligence, vol. 25, pp. 777-806, 2011. doi: 10.1142/S0218001411009007
[176] Indovina, U. Uludag, R. Snelick, A. Mink and A. Jain, "Multimodal biometric authentication methods: a COTS approach," in Proc. of Workshop on Multimodal User Authentication, 2003.
[177] L. Lindstrom and R. Jeffries, "Extreme programming and agile software development methodologies," Information systems management, vol. 21, pp. 41-52, 2004. doi: 10.1201/1078/44432.21.3.20040601/82476.7
[178] M. A. Awad, "A comparison between agile and traditional software development methodologies," University of Western Australia, vol. 30, 2005.
[179] Kruchten, The rational unified process: an introduction, Addison-Wesley Professional, 2004.
[180] R. Balduino, "Introduction to OpenUP (Open unified process)," Eclipse site, 2007. Available: https://www.eclipse.org/epf/general/OpenUP.pdf. [Accessed 27 March 2020]
[181] S. Ambler and others, "The agile unified process (aup)," Toronto, Canada. Available: http://www. ambysoft. com/unifiedprocess/agileUP. html, 2005. [Accessed 27 March 2020]
[182] R. B. Grady, Practical Software Metrics for Project Management and Process Improvement, USA: Prentice-Hall, Inc., 1992.
[183] N. Samoska, "Evaluation and performance prediction of multimodal biometric systems," MSc thesis, West Virginia University, 2006.
[184] Anjos, L. El-Shafey and S. Marcel, "BEAT: An open-source web-based open-science platform," arXiv preprint arXiv:1704.02319, 2017.
[185] Cabana, C. Charrier and A. Louis, "Mono and multi-modal biometric systems assessment by a common black box testing framework," Future Generation Computer Systems, vol. 101, pp. 293-303, 2019. doi: 10.1016/j.future.2019.04.053
[186] E. Morwaagole, "A framework for improving accuracy of multimodal biometrics security based on bayesian network," MSc thesis, Staffordshire University, 2018. Available: https://repository.biust.ac.bw/bitstream/handle/123456789/76/MORWAAGOLE%20Emmanuel.pdf?sequence=1&isAllowed=y
[187] Beritelli and G. L. Sciuto, "Performance evaluation of multimodal biometric systems based on mathematical models and probabilistic neural networks," in The International Symposium for Young Scientists in Technology, Engineering and Mathematics, Catania, Italy, 2016.
[188] Kumar, V. Kanhangad and D. Zhang, "A new framework for adaptive multimodal biometrics management," IEEE transactions on Information Forensics and Security, vol. 5, pp. 92-102, 2010.
[189] Pandey, "Multimodal Biometrics Authentication Framework for Banking Systems," International Symposium for Young Scientists in Technology, Engineering and Mathematics, Catania, Italy, pp. 40-46, 2016
[190] Geraci, F. Katki, L. McMonegal, B. Meyer, J. Lane, P. Wilson, J. Radatz, M. Yee, H. Porteous and F. Springsteel, IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries, IEEE Press, 1991.

[191] D. Chen and G. Doumeingts, "European initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap," Annual reviews in control, vol. 27, pp. 153-162, 2003. doi: 10.1016/j.arcontrol.2003.09.001
[192] Wegner, "Interoperability," ACM Computing Surveys (CSUR), vol. 28, pp. 285-287, 1996.
[193] F. L. Podio, J. S. Dunn, L. Reinert, C. J. Tilton and L. O'Gorman, "CBEFF Common Biometric Exchange File Format," 2001. Available: https://apps.dtic.mil/sti/pdfs/ADA408418.pdf. [Accessed 5 March 2020].
[194] National institute of standards and technology, "Multimodal Biometric Application Resource Kit (MBARK) offical web page," [Online]. Available: https://www.nist.gov/services-resources/software/multimodal-biometric-application-resource-kit-mbark. [Accessed 3 March 2020].
[195] ISO/IEC JTC 1/SC 37 Biometrics, ISO/IEC 19784-1:2018 Information technology — Biometric application programming interface — Part 1: BioAPI specification, 2018.
[196] J. Micheals, K. Mangold, M. Aronoff, K. Kwong and K. Marshall, "Specification for WS-Biometric Devices (WS-BD)," NIST Special Publication, vol. 500, p. 288, 2012. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=910334 [Accessed 4 March 2020].
[197] OASIS, "BIAS Messaging Protocol, Standard 1.0,," November 2011. [Online]. Available: http://docs.oasis-open.org/bias/soapprofile/v1.0/errata01/os/biasprofile-v1.0-errata01-os-complete.pdf. [Accessed 5 March 2020].
[198] I. Milenković, Master rad - Razvoj komunikacionog adaptera za multimodalni biometrijski sistem, Beograd: Univerzitet u Beogradu, Fakultet organizacionih nauka, 2013.
[199] I. Milenkovic, O. Latinovic, D. Simic and D. Starcevic, "Razvoj komunikacionog adaptera za multimodalni biometrijski sistem," ITEO 2013 zbornik radova, Banjaluka.
[200] S. Paunović, "Applying multimodal biometrics in identity determining systems," University of Belgrade, Faculty of organizational sciences, 2013.
[201] R. Vazan, "SourceAFIS - fingeprint matcher," [Online]. Available: https://sourceafis.machinezoo.com/algorithm. [Accessed 12 April 2020].
[202] R. Vazan, "SourceAFIS - algorithm description," [Online]. Available: https://sourceafis.machinezoo.com/algorithm. [Accessed 12 April 2020].
[203] Kaehler and G. Bradski, Learning OpenCV 3: computer vision in C++ with the OpenCV library, " O'Reilly Media, Inc.", 2016.
[204] P. I. Wilson and J. Fernandez, "Facial feature detection using Haar classifiers," Journal of Computing Sciences in Colleges, vol. 21, pp. 127-133, 2006.
[205] Ren, X. Cao, Y. Wei and J. Sun, "Face alignment at 3000 fps via regressing local binary features," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1685-1692, 2014.
[206] University of Kent, "Postgraduate biometrics course structure," [Online]. Available: https://www.kent.ac.uk/courses/postgraduate/256/information-security-biometrics#structure. [Accessed 3 March 2020].
[207] University of Hertfordshire, "Masters by research in digital media processing and biometrics programme," [Online]. Available:

https://www.herts.ac.uk/courses/masters-by-research-digital-media-processing-and-biometrics. [Accessed 3 March 2020].
[208] West Virgina University, "Biometrics Systems Major Map," [Online]. Available: https://www.wvu.edu/academics/major-maps/biometric-systems-bsbs. [Accessed 3 March 2020].
[209] U. Šošević, I. Milenković, M. Milovanović and M. Minović, "Support platform for learning about multimodal biometrics," Journal of Universal Computer Science, vol. 19, pp. 1684-1700, 2013.
[210] M. Hugos, Enterprise games: using game mechanics to build a better business, " O'Reilly Media, Inc.", 2012.
[211] McGonigal, Reality is broken: Why games make us better and how they can change the world, Penguin, 2011.
[212] V. Štavljanin, U. Šošević and I. Milenković, "Gamified educational website conversion optimization," in Proceedings of the Second International Conference on Technological Ecosystems for Enhancing Multiculturality, 2014.
[213] R. Bartle, "Hearts, clubs, diamonds, spades: Players who suit MUDs," Journal of MUD research, vol. 1, p. 19, 1996.
[214] F. J. García-Peñalvo, M. Johnson, G. R. Alves, M. Minović and M. Á. Conde-González, "Informal learning recognition through a cloud ecosystem," Future Generation Computer Systems, vol. 32, pp. 282-294, 2014. doi: 10.1016/j.future.2013.08.004
[215] M. Minovic, V. Stavljanin, M. Milovanovic and D. Starcevic, "User-centered design of m-learning system: moodle on the go," Journal of Computing Science and Engineering, vol. 4, pp. 80-95, 2010.
[216] Salen, K. S. Tekinbaş and E. Zimmerman, Rules of play: Game design fundamentals, MIT press, 2004.
[217] E. Adams, Fundamentals of game design, Pearson Education, 2014.
[218] Schell, The Art of Game Design: A book of lenses, AK Peters/CRC Press, 2019.
[219] Werbach and D. Hunter, For the win: How game thinking can revolutionize your business, Wharton Digital Press, 2012.
[220] G. Zichermann and C. Cunningham, Gamification by design: Implementing game mechanics in web and mobile apps, " O'Reilly Media, Inc.", 2011.
[221] J. Newman, Videogames, Routledge, 2012.
[222] Webster university, "Online education offers a flexible experience," 2013. [Online]. Available: http://www.webster.edu/news/2013/news/05082013-online-education.html. [Accessed 2 March 2020].
[223] G. Zichermann and J. Linder, Game-based marketing: inspire customer loyalty through rewards, challenges, and contests, John Wiley & Sons, 2010.
[224] J. Antin and E. F. Churchill, "Badges in social media: A social psychological perspective," in CHI 2011 Gamification Workshop Proceedings, 2011.
[225] J. Radoff, Game on: Energize your business with social media games, John Wiley & Sons, 2011.
[226] E. D. San Millán and R. G. Priego, "Learning by Playing: Is Gamification a Keyword in the New Education Paradigm?," in Gamification: Concepts, Methodologies, Tools, and Applications, IGI Global, 2015, pp. 2063-2112. doi: 10.4018/978-1-4666-8200-9.ch105
[227] J. Hamari, J. Koivisto and H. Sarsa, "Does gamification work?--a literature review of empirical studies on gamification," in 2014 47th Hawaii international conference on system sciences, pp. 3025-3034, 2014. doi: 10.1109/HICSS.2014.377.

[228] Vicent, S. Villagrasa, D. Fonseca and E. Redondo, "Virtual learning scenarios for qualitative assessment in higher education 3D arts," Journal of universal computer science, vol. 21, pp. 1086-1105, 2015.
[229] T. Parisi, WebGL: up and running, " O'Reilly Media, Inc.", 2012.
[230] Unity 3D engine, "Oficijelna veb stranica," [Online]. Available: https://unity.com/. [Accessed 13 2 2020].
[231] Occulus Rif, "Oficijelna veb stranica," [Online]. Available: https://www.oculus.com/rift/. [Accessed 13 2 2021].
[232] Cheong, F. Cheong and J. Filippou, "Quick Quiz: A Gamified Approach for Enhancing Learning.," in PACIS, 2013. Available: https://aisel.aisnet.org/pacis2013/206
[233] G. Barata, S. Gama, J. Jorge and D. Gonçalves, "Studying student differentiation in gamified education: A long-term study," Computers in Human Behavior, vol. 71, pp. 550-585, 2017. doi: 10.1016/j.chb.2016.08.049
[234] Domínguez, J. Saenz-De-Navarrete, L. De-Marcos, L. Fernández-Sanz, C. Pagés and J.-J. Martínez-Herráiz, "Gamifying learning experiences: Practical implications and outcomes," Computers & education, vol. 63, pp. 380-392, 2013.
[235] P. Denny, "The effect of virtual achievements on student engagement," in Proceedings of the SIGCHI conference on human factors in computing systems, pp. 763–772, 2013. doi: https://doi.org/10.1145/2470654.2470763
[236] L. Hakulinen, T. Auvinen and A. Korhonen, "Empirical study on the effect of achievement badges in TRAKLA2 online learning environment," in 2013 Learning and teaching in computing and engineering, pp. 47-54, 2013. doi: 10.1109/LaTiCE.2013.34.
[237] L. Malmi, V. Karavirta, A. Korhonen, J. Nikander, O. Seppälä and P. Silvasti, "Visual algorithm simulation exercise system with automatic assessment: TRAKLA2," Informatics in education, vol. 3, pp. 267-288, 2004.
[238] M.-B. Ibanez, A. Di-Serio and C. Delgado-Kloos, "Gamification for engaging computer science students in learning activities: A case study," IEEE Transactions on learning technologies, vol. 7, pp. 291-301, 2014. doi: 10.1109/TLT.2014.2329293.
[239] M. Olds, B. M. Moskal and R. L. Miller, "Assessment in engineering education: Evolution, approaches and future collaborations," Journal of Engineering Education, vol. 94, pp. 13-25, 2005. doi: 10.1002/j.2168-9830.2005.tb00826.x
[240] S. Aguilar, C. Holman and B. Fishman, "Multiple paths, same goal: Exploring the motivational pathways of two distinct game-inspired university course designs," Games+ Learning+ Society, Madison, WI, 2014.
[241] S. S. Shapiro and M. B. Wilk, "An analysis of variance test for normality (complete samples)," Biometrika, vol. 52, pp. 591-611, 1965.
[242] H. Levene, "Robust tests for equality of variances," Contributions to probability and statistics. Essays in honor of Harold Hotelling, pp. 279-292, 1961.
[243] Kovačević, M. Minović, M. Milovanović, P. O. De Pablos and D. Starčević, "Motivational aspects of different learning contexts:“My mom won’t let me play this game…”," Computers in Human Behavior, vol. 29, pp. 354-363, 2013. doi: 10.1016/j.chb.2012.01.023
[244] R. Likert, "A technique for the measurement of attitudes.," Archives of psychology, 1932.
[245] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," Psychometrika, vol. 16, pp. 297-334, 1951.

Biografija autora

Ivan Milenković rođen je 14.6.1988 u Beogradu. Završio je Matematičku gimnaziju u Beogradu 2007 godine. Iste godine upisuje Fakultet organizacionih nauka Univerziteta u Beogradu - smer Informacioni sistemi i tehnologije, koji završava 2011. godine sa prosečnom ocenom 9.95. Master studije upisuje 2011. godine na Fakultetu organizacionih nauka, smer Informacioni sistemi i tehnologije i završava ih 2013. godine sa prosečnom ocenom 10, odbranivši master rad „Razvoj komunikacionog adaptera za multimodalni biometrijski sistem“. Doktorske studije na Fakultetu organizacionih nauka, smer Informacioni sistemi i kvantitativni menadžment upisao je 2013. godine.

Nosilac je više nagrada i priznanja za uspehe postignute tokom studiranja. Proglašen od strane Univerziteta u Beogradu za najboljeg studenta generacije 2007/2008 Fakulteta organizacionih nauka. Tokom studiranja bio je stipendista Republičkog fonda za razvoj naučnog i umetničkog podmlatka, kao i stipendista Fonda za mlade talente.

Tokom studiranja od oktobra 2010. godine kao saradnik Laboratorije za multimedijalne komunikacije izvodio je vežbe iz predmeta Računarske mreže i telekomunikacije i učestvovao u naučno istraživačkim projektima laboratorije. Od februara 2012. godine zaposlen je na Fakultetu organizacionih nauka kao saradnik u nastavi na Katedri za informacione tehnologije. Od februara 2014. godine zaposlen je na Fakultetu organizacionih nauka kao asistent na Katedri za informacione tehnologije.

Objavio je više radova iz oblasti informacionih tehnologija u zemlji i inostranstvu. Učestvovao u izvođenju projekta „Primena multimodalne biometrije u menadžmentu identiteta“, Ministarstva prosvete, nauke i tehnološkog razvoja, ugovor broj TR-32013 2011 – 2016. Takođe, bio je učesnik međunarodnog projekta ISSES (Information Security Services Education in Serbia). Pored nastavnih i istraživačkih aktivnosti, kandidat ima iskustva u radu na brojnim stručnim projektima, kao i komercijalnim kursevima.

Prilog 1.

Izjava o autorstvu

Ime i prezime autora Ivan Milenković

Broj indeksa 5001/2013

Izjavljujem

da je doktorska disertacija pod naslovom

Okvir za evaluaciju multimodalnih biometrijskih sistema

- rezultat sopstvenog istraživačkog rada;
- da disertacija u celini ni u delovima nije bila predložena za sticanje druge diplome prema studijskim programima drugih visokoškolskih ustanova;
- da su rezultati korektno navedeni i
- da nisam kršio/la autorska prava i koristio/la intelektualnu svojinu drugih lica.

Potpis autora

U Beogradu, 17.5.2021.

_____

Prilog 2.

Izjava o istovetnosti štampane i elektronske verzije doktorskog rada

Ime i prezime autora Ivan Milenković

Broj indeksa 5001/2013

Studijski program Informacioni sistemi i kvantitativni menadžment

Naslov rada Okvir za evaluaciju multimodalnih biometrijskih sistema

Mentor Prof. Dr Dejan Simić, redovni profesor FON-a

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao/la radi pohranjena u **Digitalnom repozitorijumu Univerziteta u Beogradu**.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog naziva 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 autora

U Beogradu, 17.5.2021.

_____

Prilog 3.

Izjava o korišćenju

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom:

Okvir za evaluaciju multimodalnih biometrijskih sistema

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalnom repozitorijumu Univerziteta u Beogradu i dostupnu u otvorenom pristupu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo (CC BY)

2. Autorstvo – nekomercijalno (CC BY-NC)

3. Autorstvo – nekomercijalno – bez prerada (CC BY-NC-ND)

4. Autorstvo – nekomercijalno – deliti pod istim uslovima (CC BY-NC-SA)

5. Autorstvo – bez prerada (CC BY-ND)

6. Autorstvo – deliti pod istim uslovima (CC BY-SA)

(Molimo da zaokružite samo jednu od šest ponuđenih licenci.
Kratak opis licenci je sastavni deo ove izjave).

Potpis autora

U Beogradu, 17.5.2021.

_____

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 prerada**. 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 prerada**. 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.