UNIVERZITET SINGIDUNUM

BEOGRAD

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKA DISERTACIJA

JEDNA KLASA SISTEMA ZA GENERISANJE I DISTRIBUCIJU KRIPTOLOŠKIH KLJUČEVA ZASNOVANA NA VIŠE BIOMETRIJSKIH MODALITETA

Mentor:

Prof. dr Saša Adamović

Student: Jelena M. Gavrilović

Broj indeksa: 460029/2011

Beograd, oktobra 2022. godine

Sažetak

U doktorskoj disertaciji predložena je jedna klasa sistema za generisanje i distribuciju kriptoloških ključeva na osnovu više biometrijskih modaliteta. Teorijskim okvirom obuhvaćena su dva biometrijska modaliteta, otisak prsta i iris.

U radnim režimima sistem koristi heš vrednosti koje su dobijene u početnoj fazi, tj. fazi upisa. Osim ovih vrednosti, u upotrebi su pomoćni podaci koji čine da biometrijski podaci budu poništivi i na ovaj način štite privatnost biometrijskih podataka. Takođe, pružaju zaštitu kriptološkim parametrima. Biometrija irisa, kao izvor najbogatiji sa bioinformacijom, upotrebljena je u svrhu ekstrakcije tajnog ključa, dok se za servis autentifikacije koristi otisak prsta.

Eksperimentalna analiza koja je obuhvatila kompletan istraživački deo rada u tezi, zasniva se na uzorcima dobijenim iz CASIA biometrijske baze podataka, a postignuti eksperimentalni rezultati ukazuju na značajne doprinose koji u velikoj meri podižu performanse ove klase sistema.

Ključne reči: *višemodalna biometrija, poništiva biometrija, biometrijski sistemi, generisanje kriptoloških ključeva, performanse sistema.*

Apstrakt

This dissertation proposes a class of systems for generating and distributing cryptological keys based on multiple biometric modalities. The theoretical framework encompasses two biometric modalities, the fingerprint, and the iris.

In the working modes, the system uses the hash values obtained in the initial phase, i.e., the enrollment phase. In addition to these values, auxiliary data are used to make biometric data revocable and, in this way, protect the privacy of biometric data. In addition, they provide protection for cryptological parameters.

Iris biometrics, as the source that contains the largest number of bio-information, was used to extract the secret key, while the fingerprint is used for authentication purposes. The

experimental analysis, which encompassed the entire research aspect of the thesis, is based on the samples obtained from the CASIA biometric database, and the achieved experimental results indicate significant contributions that greatly improve the performance of this class of systems.

Keywords: *Multimodal Biometrics, Cancelable biometrics, Biometric Systems, Cryptographic Key Generation, System Performance.*

Projekat Decide

Zahvalnost na podršci Fondu za nauku obzirom da je disertacija jedan od rezultata projekta.

Hommage

U disertaciji su, pred svako novo poglavlje, citirane po meni najlepše rečenice Kloda Šenona, kao naučnika čija su istraživanja obeležila svaku etapu mog školovanja.

Zahvalnost

Zahvaljujem se svima koji su verovali u mene i uticali da se ova disertacija privede kraju u pravo vreme!

Hvala vam svima, ne bojim se i radujem se!

Posebnu zahvalnost dugujem mentoru dr Saši Ž. Adamoviću, redovnom profesoru.

SADRŽAJ

Spisak slika

Spisak tabela

„ We know the past but cannot control it.

We control the future but cannot know it. “

Claude Shennon

---

1. Uvod

U uvodnom delu navedeni su osnovni motivi i opšta razmatranja za razvoj nove klase sistema koja će značajno unaprediti performanse postojećih sistema za jednim biometrijskim modalitetom. Detaljno će biti obrazložen predmet istraživanja, očekivani doprinosi i struktura disertacije.

1.1. Značaj teme

Tradicionalni biometrijski sistemi podrazumevaju upotrebu samo jednog biometrijskog modaliteta: dužice oka (engl. *iris*), lica, glasa, elektrokardiograma (EKG), otiska prsta, dlana i drugih modaliteta, za proveru identiteta korisnika (autentifikaciju), kao i generisanje kriptoloških ključeva, dok višemodalni biometrijski sistemi kombinuju dobijenu informaciju iz dva ili više biometrijskih modaliteta.

Na ovaj način višemodalni biometrijski sistemi povećavaju količinu informacije koja se može koristiti u servisima provere identiteta i kriptografskim servisima za generisanje i distribuciju kriptoloških ključeva dovoljnih dužina za standardne kriptografske mehanizme 21. veka uz pomoć dodatnih podataka koji se u literaturi mogu naći pod imenom pomoćni podaci (engl. *helper data*).

Osnovni problem unimodalnih sistema je nedostatak dovoljne količine prikupljene biometrijske informacije, neuniverzalnost uzorka i različiti metodi napada lažiranjem uzorka, kao i drugih vrsta napada. Većina navedenih izazova se rešava upotrebom višemodalnih biometrijskih sistema. Osim navedenog, postoje i druge prednosti koje višemodalne biometrijske sisteme čine pouzdanijim u radu za navedene svrhe.

U disertaciji je predložen jedan sistem za generisanje kriptoloških ključeva na osnovu biometrijskih uzoraka, pri čemu se sigurnost generisanih ključeva postiže upotrebom pomoćnih podataka i upotrebom drugog modaliteta. Empirijskim istraživanjem potvrđeno je da višemodalni

sistem za generisanje ključeva grešku lažnog prihvatanja (engl. *False Acceptance Rate*, FAR) korisnika svodi na 0 i uvećava sigurnost autentifikacionog sistema u celini.

1.2. Cilj istraživanja

Doktorska disertacija ima za cilj definisanje, implementaciju uz analizu radnog okvira jedne klase višemodalnog biometrijskog sistema za generisanje i distribuciju kriptoloških ključeva. Radni okvir je zasnovan na upotrebi više modaliteta. Ciljevi predloženog okvira sistema su robusnost, koja se odnosi na nemogućnost protivnika da na osnovu jednog modaliteta definiše adekvatan kriptološki ključ, kao i privatnost biometrijskih šablona korisnika (engl. *template*).

Naučni cilj istraživanja ogleda se u doprinosu naučnoj zajednici kroz definisanje jednog vida rešenja višemodalnog biometrijskog sistema. Ovakav vid rešenja će zahvaljujući ovoj disertaciji kao i naučnim radovima objavljenim u toku njene izrade, biti dostupan naučnoj zajednici.

Društveni cilj istraživanja je mogućnost implementacije ovakvog predloga rešenja u različite već postojeće sisteme koji se koriste u procesu generisanja i distribucije kriptoloških ključeva a sve u cilju zaštite podataka i privatnosti stanovništva.

1.3. Predmet istraživanja

Disertacija u svom drugom poglavlju sadrži pregled i analizu različitih naučnih istraživanja u oblasti generisanja kriptoloških ključeva, biometrije i biometrijskih sistema. Dobijeni rezultati su se zatim koristili kao smernica za istraživanje koje je izvršeno a potom i predstavljeno kroz naredna poglavlja disertacije. Autor se nada da će analizirani rezultati različitih postojećih istraživanja zajedno sa njenim istraživanjem u okviru ove disertacije, poslužiti svima koji bi dalje istraživali i razvijali obrađenu temu.

Tema ove doktorske disertacije je aktuelna o čemu svedoče brojni relevantni naučni radovi objavljeni u eminentnim naučnim časopisima i zbornicima konferencija međunarodnog značaja. Naučni doprinos ove disertacije i istraživanja obrađenog u njenim okvirima ogleda se u novoj

metodi primene postojećih modaliteta, čime je autor dao doprinos u procesu razvoja kriptološke bezbednosti i biometrijske kriptografije.

U petom poglavlju disertacije, a na osnovu postojećih naučnih saznanja objavljenih u prestižnim naučnim časopisima dat je predlog radnog okvira zasnovanog na novoj metodi primene više biometrijskih modaliteta. Cilj predloženog sistema je generisanje i distribucija kvalitetnih kriptoloških ključeva dovoljnih dužina za primenu u standardizovanim mehanizmima 21. veka na osnovu više biometrijskih modaliteta.

Osnova ovog istraživanja potiče iz rada „ *An Approach to Robust Biometric Key Generation System Design"* [1].

1.4. Hipoteze

U okviru disertacije postavljene su: Opšta hipoteza, Posebna hipoteza kao i pojedinačne hipoteze.

1.4.1. Opšta hipoteza

Opšta hipoteza, od koje je i sam proces istraživanja u disertaciji počeo je: „Biometrijski izvori informacija su dovoljno kvalitetni za sintezu sistema iz domena biometrijske kriptografije a u svrhu generisanja i distribucije kriptoloških ključeva".

1.4.2. Posebna hipoteza

Posebna hipoteza , proistekla iz opšte je sledeća: „Kombinovanjem više biometrijskih modaliteta moguće je poboljšati performanse navedenog sistema i učiniti njegov rad pouzdanijim i bezbednijim".

1.4.3. Pojedinačne hipoteze

Pojedinačne hipoteze koje su korišćene i testirane u samoj disertaciji su:

- kvalitet kriptoloških ključeva je značajno bolji u informaciono-teorijskom smislu (Šenonova entropija, skup NIST statističkih testova za kontrolu slučajnosti generisanih nizova, na osnovu pseudoslučajnih generatora);
- moguće je razviti sistem visokih performansi izborom dobre strategije fuzije;
- upotrebom predloženog rešenje mogu se sprečiti već poznate, odnosno postojeće metode napada na biometrijske sisteme. Ukoliko se napad ne može sprečiti, predloženo rešenje treba da smanji mogućnosti izvođenja, odnosno da umanji efekte samih napada;
- koriste se poznate procene ostvarenog nivoa sigurnosti;
- broj korisnika koji će koristiti sistem ne utiče na robusnost sistema;
- vrste biometrijskih osobina koje je potrebno steći su već poznate i teorijski dokazive da predstavljaju reprezentativni biometrijski uzorak;
- upotreba poznatih i naučno dokazanih metoda u procesu integracije i obrade korišćenih informacija i
- dato rešenje predstavlja kompromis između troškova razvoja i performansi sistema.

1.5. Metode istraživanja i načini za prikupljanje i analizu podataka

Istraživanje je sprovedeno upotrebom dostupnih saznanja iz ove oblasti, prikupljanje informacija za istraživanje izvršeno je na osnovu literature dostupne putem štampanih i relevantnih online izvora, poput radova objavljenih u časopisima i zbornicima relevantnih naučnih konferencija. Analiza postojećeg stanja u ovoj oblasti imala je za cilj da se postave smernice za dalji razvoj u domenu biometrije, kriptografije i kripto biometrijskih sistema .

Od naučnih metoda koristila se:

- analitičko-deduktivna metoda,

- hipotetičko-deduktivna,
- uporedna i komparativna metoda i
- eksperimentalna metoda ispitivanja.

Prikupljanje i analiza podataka izvršena je:

- postavljanjem kriterijuma za poređenje i klasifikaciju,
- poređenjem prikupljenih podataka,
- utvrđivanjem relevantnih činjenica i veza među podacima,
- preispitivanjem hipoteza,
- testiranjem i proverom zaključaka do kojih smo došli i
- postavljanjem budućih ciljeva.

„Use the word 'cybernetics', Norbert, because nobody knows what it means.

This will always put you at an advantage in arguments. “

Claude Shannon

---

2. Pregled u oblasti istraživanja

Kroz drugo poglavlje disertacije autor je razmatrao opšte stanje u oblasti istraživanja, na osnovu najnovijih naučnih saznanja vezanih za ove dve klase biometrijskih sistema. Predočene su prednosti kao i nedostaci postojećih višemodalnih biometrijskih sistema u cilju što preciznijeg isticanja doprinosa ove doktorske disertacije.

Da bi se održala tajnost informacija tokom komunikacije, kriptografija se smatra impresivnim rešenjem i kriptografski ključevi igraju važnu ulogu u obezbeđivanju sigurnosti. Međutim, ove nasumično izvedene ključeve (od 256 bitova) je teško zapamtiti. Takođe, postoji opasnost od narušavanja privatnosti, jer skladištenje, zaštita i prenos ključa preko komunikacione veze mogu dovesti do curenja informacija. Stoga istraživači predlažu upotrebu biometrije korisnika za generisanje kriptografskog ključa u komunikacijskom okruženju zasnovanom na sesiji. Ovo izbegava skladištenje kriptografskih ključeva bez pregovora o tajnosti. Generisanje ključa zasnovano na biometriji obuhvata zabrinutost u vezi sa zaštitom biometrijskog šablona, biometrijskom razmenom podataka između korisnika i opozivom generisanjem ključeva iz biometrije. Autori *Dwivedi, Dey, Sharma* i *Goel* su u radu objavljenom 2019. godine pod nazivom *A fingerprint based crypto-biometric system for secure communication* predložili okvir za sigurnu komunikaciju između dva korisnika pomoću kripto-biometrijskog sistema zasnovanog na otisku prsta [2] . Prvo, značajan niz karakteristika izračunava se na osnovu otiska prsta korisnika. Zatim se primenjuje opozina transformacija za izvođenje tajnih ključeva odgovarajućih korisnika. Zatim se koristi *Diffie–Hellman* (DH) algoritam za generisanje simetričnog ključa između dve strane na osnovu tajni koje su međusobno nepoznate. Ukoliko je algoritam ispravno implementiran on će onda sadržati metode zaštite od napada, koji se u literaturi može naći pod imenom čovek u sredini (engl. *man in the middle*) ,. U ovakvim algoritmima biometrijski podaci se ne čuvaju niti se dele, što osigurava sigurnost biometrijskih podataka. Takođe, savršena tajnost prenosa postiže se pomoću ključeva sesije. U ovom radu autori su naveli da ovakvo predloženo rešenje pruža

dugoročnu zaštitu poruka prenetih između dva korisnika. Eksperimentalnom procenom izvršenom upotrebom četiri skupa podataka FVC2002, FVC 2004, NIST posebne baze podataka itd., zaključili su da predloženi okvir čuva privatnost i da se može koristiti za stvarne sisteme kontrole pristupa.

Autori *Sarkar* i *Singh* su u svom radu objavljenom 2020. godine, pod nazivom *A Novel Session Key Generation and Secure Communication Establishment Protocol Using Fingerprint Biometrics* izložili da sigurnost informacija omogućavaju razne kriptografske tehnike [3]. Šifrovanje simetričnog ključa jedna je od metoda koja zahteva komunikaciju zajedničkog tajnog ključa između dve strane. Distribucija takvog tajnog ključa je glavni izazov u kriptografiji simetričnog ključa. Potrebne su efikasne i pouzdane tehnike za distribuciju zajedničkog tajnog ključa između strana u komunikaciji. Da bi se rešio problem upravljanja ključevima i distribucije ključeva, predložili su generisanje ključa sesije zasnovanog na biometriji i to na osnovu otiska prsta i protokola uspostavljanja sigurne komunikacije. U ovoj predloženoj tehnici dva korisnika na kraju generišu 128-bitni simetrični ključ sesije, uz pomoć njihovih kombinovanih šablona otisaka prstiju koji se mogu otkazati kao i slučajnog ključa nastalog na osnovu izabranog načina spajanja šablona, ovo se izvršava na pouzdanom serveru. Server za potvrdu identiteta nalazi se između strana koje komuniciraju. Uzorci oba korisnika koji se mogu otkazati bezbedno se prenose sa jednog na drugi, koristeći kriptografiju javnog ključa. Nema potrebe da se tajni ključ deli preko nesigurnog kanala, jer strane koje komuniciraju generišu isti ključ sesije na svojoj strani. Ovaj ključ sesije važi samo za jednu sesiju komunikacije. U ovom pristupu ključ sesije se generiše iz otiska prsta, a privatnost otiska zaštićena je transformacijom uzorka otiska prsta koju je moguće otkazati od strane obe strane koje komuniciraju.

Još jedno rešenje za generisanje kriptografskih ključeva predstavili su autori *Akdoğan, Altop* i *Levi* u radu objavljenom 2019. godine pod nazivom *Secure key agreement based on ordered biometric features.* Dogovor o sigurnom ključu pomoću čisto uređene biometrije (engl. *Secure key agreement protocols: Pure biometrics and cancelable biometrics,* SKA-POB), u kom se kriptografski ključevi generišu pomoću uređenog skupa biometrijskih podataka, bez dodatnih deljenih tajnih podataka ili ključeva [4]. Predloženi pristup je predstavljen korišćenjem biometrije irisa. Protokol koristi izabrane heš funkcije i takozvani *Hash-based Message Authentication Code* (HMAC) kao jedinu kriptografsku primitivu, stoga ne zahteva kriptografske resurse. Takođe,

predložili su i integraciju strategije upoređivanja zasnovanu na prozorima i metod resetovanja prozora u SKA-POB. Na ovaj način performanse sistema se uvećavaju bez žrtvovanja sigurnosti. Pored toga, autori predlažu strategiju generisanja i distribucije lažnih blokatora kako bi sakrili prave blokatore u tranzitu, što povećava otpornost predloženog protokola protiv napada. SKA-POB protokol radi na okrugli način, omogućavajući uspešno završavanje uspostavljanja ključa što je ranije bilo moguće, tako da se smanjuje složenost kako za klijenta, tako i za server. Pored toga, koristili su više-kriterijumske analize za predloženi SKA-POB protokol i predstavili rezultate verifikacije u pogledu analize performansi zajedno sa slučajnošću, prepoznatljivošću i složenošću napada kroz sigurnosnu analizu. Rezultati pokazuju da se vrlo slučajni i računski sigurni ključevi mogu generisati sa minimalnim greškama i sa vrlo malom složenošću.

Biometrija igra značajnu ulogu u informacionoj sigurnosti, kao i u bezbednosti korisnika. Obezbeđivanje biometrijskog uzorka je oblast istraživanja od značaja. Ogleda se, između ostalog, i u aplikacijama koje u sebi koriste servise za proveru identiteta korisnika. Nedovoljna sigurnost prethodno pomenutih sistema ima vrlo negativan uticaj na sam proces biometrijske verifikacije ili identifikacije. Biometrijski uzorci mogu se zaštititi upotrebom tehnika poput transformacije ili otkazive, odnosno poništive biometrije, biometrijskih kriptosistema i hibridizacije. Većina ranjivosti ili napada otklanjaju se unapređenjem procesa hibridizacije, kao što je kombinovanje uzorka biometrije sa podatkom koji korisnik zna , poput lozinki, za sigurnu potvrdu identiteta. Izabrani izazovi u zaštiti šablona su poravnavanja šablona i izbor pseudo identifikatora i pomoćnih podataka [5]. Prethodno pomenuta tvrdnja objavljena je u radu autora *Bharathi* i *Mohana* pod nazivom: *A Review on Biometric Template Security* objavljenom 2019. godine.

Biometrijski uzorci u svom izvornom obliku podložni su napadima i neopozivi su ako su ugroženi, pa ih stoga treba zaštititi. U svom radu pod nazivom *Cancellable biometric system based on linear combination of trigonometric functions with special application to forensic dental biometrics,* objavljenom 2019. godine autori *Banday* i *Mir* predložili su pristup zaštiti šablona zasnovan na linearnoj kombinaciji trigonometrijskih funkcija koja osigurava stomatološke uzorke sačuvane u forenzičkim dokumentima i istovremeno održava performanse prepoznavanja sistema za identifikaciju. Bezbednosna analiza ove jednosmerne transformacije urađena je kroz pokušaje inverzije transformisanih šablona u prvobitni oblik, što se pokazalo efikasnim u održavanju neizbežnosti. Eksperimentalni rezultati pokazuju da je ovaj pristup praktičan sa niskom identičnom

greškom (engl. *Equal Error Rate,* EER) od 2%. Autori su pokazali da ovaj sistem ima visoku stopu prepoznavanja skoro 98% [6].

Široka primena višemodalne biometrije za potvrdu identiteta korisnika podstiče potrebu za biometrijskim sistemima sa visokim performansama prepoznavanja. Biometrijski podaci, nakon što su procurili (engl. *data leak*) ili bili ukradeni, ostaju zauvek ugroženi. Otuda je biometrijska sigurnost od najveće važnosti. Postojeće šeme zaštite biometrijskih šablona ili pogoršavaju performanse prepoznavanja ili imaju problema sa sigurnošću i brzinom. Autori *Chang, Garg, Hasan* i *Mishra* u svom radu pod nazivom *Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption,* predložili su pristup višebiometrijske potvrde identiteta koji se može otkazati gde nova šema šifrovanja po bitima transformiše biometrijski obrazac u zaštićeni obrazac pomoću tajnog ključa generisanog iz drugog biometrijskog uzorka. U potpunosti se čuva broj grešaka u bitima u originalu i zaštićenom uzorku kako bi se osigurale performanse. Uvode algoritam 1 i algoritam 2 za šifrovanje na nivou bitova, oba su definisana preko kriptografskih primitiva – šifrovanja zasnovanog na blokovskim šifarskim sistemima i funkcije heširanog ključa [7]. Profilišu ove algoritme na različitim hardverskim arhitekturama da bi izračunali efikasnost u smislu vremena potrebnog tokom faze upisa i potvrde identiteta . Za algoritam 2, zaključuju da arhitekturi radne površine od 3,3 GHz treba oko 18 milisekundi u proseku za preko 200 pokretanja da bi se potvrdio identitet korisnika. Pored toga, dali su matematički dokaz koji pokazuje da predložena šema garantuje tajnost i nepovratnost. Rezultati poređenja sa postojećim biometrijskim šemama zaštite na različitim bazama podataka lica i irisa pokazuju da predloženi rad pruža značajno dobre performanse prepoznavanja i efikasnost, dok postiže visoku sigurnost. Na kraju, značajna šema šifrovanja može se izgraditi preko komercijalnih sistema kako bi se postigla sigurnost kao i visoke performanse prepoznavanja.

Tradicionalni mehanizmi zaštite digitalnih podataka prate ili kriptografiju ili potvrdu identiteta. Primarna tačka sukoba sa ovim mehanizmima ostaje ili pamćenje ili sigurno čuvanje korisničkih podataka. Rad autora *Panchal., Samanta* i *Barman* objavljen 2017. godine pod nazivom *Biometric-based cryptography for digital content protection without any key storage,* bavi se ovim kritičnim pitanjem kroz predstavljanje mehanizma zasnovanog na biometrijskom otisku prsta kako bi se zaštitili digitalizovani dokumenti korisnika [8]. U njihovom pristupu biometrijske karakteristike se izdvajaju iz otiska prsta korisnika snimljenog biometrijskim

senzorom otiska prsta. Izdvojene karakteristike se zatim koriste za generisanje jedinstvenog koda upotrebom principa kodiranja i konvolucije. Ovaj jedinstveni kod se dalje koristi za generisanje kriptografskog ključa za šifrovanje i dešifrovanje korisničkog dokumenta. Detaljna analiza pristupa uključuje eksperimente koji sadrže razne standardne slike otisaka prstiju. Korpus slika otkriva izvesnih 95,12% istinito pozitivnih (engl. *True Positive*, TP) i 0% lažno negativnih (engl. *False Negative*, FN). Dalje, prednosti pristupa su u tome što on generiše jedinstveni ključ za svakog korisnika i uklanja potrebu za skladištenjem bilo kog biometrijskog šablona ili ključa. Pored toga, dovoljno je brži i tačniji da razvije bilo koji robustan sistem zaštite podataka.

Biometrijski modeli zasnovani na irisu su široko prepoznati kao jedan od najtačnijih oblika za potvrđivanje identiteta pojedinačnih identiteta. Karakteristike izvučene iz snimljenih slika irisa koje su pretvorene u kod dužice (engl. *Iris-Codes*) konvencionalno se čuvaju u svom izvornom formatu na uređaju za skladištenje podataka. Međutim, sa sigurnosnog aspekta, uskladišteni uzorci su veoma ranjivi na širok spektar izabranih oblika napada. Studija u ovom radu bavi se pitanjem uvođenja biometrijske šeme za zaštitu privatnosti koja se zasniva na pojmu heširanja osetljivog na lokalitet. U radu *Generation of cancelable iris templates via randomized bit sampling* objavljenom 2019. godine, autori *Sadhya* i *Raman* generisali su *Iris-Code* funkcije koje se mogu opozvati, odnosno poništiti, stvorene kao lokalno uzorkovani kod, koje istovremeno pružaju snažne potvrde sigurnosti i zadovoljavajuće performanse sistema [9]. Funkcionalnost predloženog okvira okreće se oko činjenice da su uzorci *Iris-Code* klase međusobno „bliski“, zbog čega se heširaju na istoj lokaciji. Alternativno, međuklasne karakteristike kodova dužice su relativno različite i shodno tome imaju heš na različitim lokacijama. Ispitali su suštinska svojstva LSC-a procenjujući verovatnoću sudara unutar klase i među klasama za dva različita koda dužice. Dalje, analizirali su bezbednosne garancije neinvertibilnosti, opozivosti i nepovezanosti u modelu uspostavljanjem različitih granica verovatnoće kontradiktornog uspeha. Opsežni empirijski testovi na korpusima o dužici oka CASIAv3 [10] i IITD [11] pokazali su napredne performanse predloženog modela, za koji su dobili najbolje EER od 0,105%, odnosno 1,4%.

Razvoj tehnologije prepoznavanja dužice oka, usledio je činjenicom da identifikacija na osnovu prethodno pomenutog modaliteta ima različite domene primene, kao efikasan obrazac sigurnosne potvrde identiteta. Međutim, uključivanjem većeg broja osoba u proces potvrde identiteta, uočava se da ovaj obrazac takođe može dovesti do curenja privatnosti tokom postupka

sigurnosne potvrde identiteta. Pomoću genetskih algoritama i veštačkih neuronskih mreža, moguće je regenerisati lažni uzorak na osnovu koda dužice snimljenog u bazi podataka sa šablonima. Na osnovu toga, protivnik može dovoljnu količinu informacija o dužici oka korisnika i ugroziti njegovu privatnost. Sa druge strane, protivnik takođe može dobiti šablon irisa iz druge loše upravljane aplikacije i koristi ovaj obrazac za pristup korisničkim informacijama u posebnoj aplikaciji kako bi dobio njegovu privatnost.

Autori *Lei, Lili, Bin* i *Xingchao* su u svom radu objavljenom 2019. godine pod nazivom *A Novel Privacy Protection Scheme for Iris Identification* izložili da su napadi predstavljeni u njihovom radu ozbiljno uticali na upotrebe sistema identifikacije pomoću dužice oka. Stoga, kako bi se izborili sa napadima navedenim u radu, a na osnovu koncepcije slučajne projekcije i diferencijalne zaštite privatnosti, predložili su novu šemu zaštite privatnosti koja štiti privatnosti korisnika tokom postupka identifikacije irisa [12]. U ovoj šemi se koristi slučajna projekcija u fazi sakupljanja irisa oka i izrade šablona, tako da bez šablona irisa oka ne može da se invertuje informacija o irisu. Zatim, pre očuvanja pravog uzorka, napravljeno je nekoliko lažnih šablona koji su slični pravom šablonu irisa, pa su ovi lažni šabloni narušili pravi šablon kako bi se pridržavale ograničenja ε-diferencijalne privatnosti. Stoga je pravi šablon korisnika teško identifikovati sa drugim sličnim lažnim šablonima, a protivnik ne može dobiti privatnost korisnika kroz više upita, iako je šablon irisa dobio iz drugih aplikacija. Izvršeno je nekoliko eksperimenata sa različitim parametrima, a zaštitna sposobnost je upoređena sa nekim sličnim algoritmima, a zatim su rezultati ovih eksperimenata dalje pokazali superiornost predložene šeme.

Rad autora Adamovića, Miškovica, Mačeka, Milosavljevića, Šarca, Saračevića i Gnjatovića objavljen 2020.godine, pod nazivom *An efficient novel approach for iris recognition based on stylometric features and machine learning techniques* predstavlja novi sistem prepoznavanja irisa zasnovanog na metodama mašinskog učenja. Motivacija ovog istraživanja leži u međusobnoj povezanosti biometrijskih sistema i stilometrije. Glavni cilj predloženog modela je postizanje gotovo savršene tačnosti klasifikacije, uklanjanje lažnih stopa prihvatanja i ukidanje mogućnosti ponovnog stvaranja slike irisa iz generisanog šablona [13]. Da bi to postigli, autori su izostavili talase Gabora i druge banke filtera koje su tipično upotrebljene u sistemima za prepoznavanje irisa. Umesto toga, koristili su metode mašinskog učenja koji biometrijske uzorke klasifikuju kao numeričke karakteristike. Biometrijski uzorci se generišu pretvaranjem

normalizovane slike irisa u jednodimenzionalni skup kodova fiksne dužine, koji zatim prolazi kroz izdvajanje stilometrijskih karakteristika. Izdvojene osobine se dalje koriste za klasifikaciju pomoću izabranih metoda mašinskog učenja. Nova metoda prepoznavanja razvijena je pomoću baze podataka CASIA iris, a njena generalizacija se demonstrirala odvojeno na bazama podataka MMU i IITD iris, kao i na njihovom objedinjavanju sa bazom podataka CASIA, primenom preuzorkovanja pre i tokom postupka unakrsne validacije. Eksperimentalna procena pokazuje da sistem radi onako kako je predviđeno. Pored toga, računarski troškovi su znatno smanjeni u odnosu na tradicionalne sisteme, što zauzvrat smanjuje ukupnu složenost sistema prepoznavanja, čineći ga pogodnim za upotrebu u praktičnim primenama.

Rad autora *Abikoye, Ojo, Awotunde* i *Ogundokun* pod nazivom *A safe and secured iris template using steganography and cryptography* kombinuje algoritme kriptografije (*Twofish* [14] i trostruko šifrovanje podataka 3DES [15] i steganografije (najmanje značajni bitovi) da bi se rešio problem napada ili hakovanja biometrijskog šablona za zlonamerno delo, što je postalo veliki problem u sistemu prepoznavanja irisa [16]. *Twofish* koji je matematički siguran i zaštićen algoritam i trostruko šifrovanje podataka koje je nastalo na osnovu DES algoritma koriste za promenu čitljivih tajnih podataka (obična slika) u nečitljiv format (šifrat slike), dok su najmanje značajni bitovi (LSB) steganografski algoritam koji šifriranu sliku ugrađuju direktno u naslovnu sliku da bi se dobila slika poznata kao stego slika. U ovom radu, Hafova transformacija, model Dagmanovog rubber sheet modela i izabranog logaritamskog Gaborovog filtra korišćeni su za segmentaciju slike irisa, normalizaciju i izdvajanje karakteristika, a generisani šablon irisa je šifrovan pomoću algoritama 3DES i *Twofish*. Šifrat slike je zatim ugrađen u naslovnu sliku da bi se dobila stego slika pomoću LSB-a. Rezultat ovog rada blago menja glavnu datoteku nakon ugradnje tajne slike (stego datoteka) koju ljudsko oko ne može identifikovati, a samo je JPEG slika korišćena kao glavna ili druga datoteka. Dva nivoa prethodno pomenute sigurnosne tehnike, shodno autorima obezbeđuju visok kapacitet i kompleksnost analize u odnosu na napadača.

U radu autora *Abozaid, Haggag, Kasban* i *Eltokhy* objavljenom 2019. godine pod nazivom *Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion,* predstavljen je efikasan pristup multimodalnoj biometrijskoj identifikaciji kao alatu za potvrdu identiteta čoveka zasnovan na spajanju prepoznavanja lica i glasa. Za izdvajanje karakteristika prepoznavanja glasa koriste se koeficijenti Mel-Cepstral i statistički koeficijenti,

koji se zatim upoređuju. Funkcije prepoznavanja lica izdvajaju se koristeći različite tehnike ekstrakcije, analizu svojstvenih površina i principa prepoznavanja glavnih komponenti (eng. *Principal Component Analysis*, PCA) i rezultati se upoređuju. Modaliteti prepoznavanja glasa i lica izvode se pomoću različita tri klasifikatora, gausovski modeli mešanja (engl. *Gaussian Mixture Model*, GMM), veštačke neuronske mreže (engl. *Artificial Neural Network*, ANN) i metode vektora oslonca (engl. *Support Vector Machine*, SVM). Kombinacija biometrijskih sistema, glasa i lica, u jedan multimodalni biometrijski sistem vrši se korišćenjem spajanja karakteristika i rezultata spajanja. Eksperimenti računarske simulacije pokazuju da se dobijaju bolji rezultati u slučaju korišćenja cepstralnih koeficijenata i statističkih koeficijenata za prepoznavanje glasa, a u slučaju lica eksperiment Ejgen-lice (deut. *Eigenface*) i SVM daje bolje rezultate za prepoznavanje lica [17]. Takođe, u predloženom multimodalnom biometrijskom sistemu spajanje rezultata daje bolje rezultate od ostalih scenarija.

U svom radu, autori Maček, Adamović, Milosavljević, Jovanović, Gnjatović i Trenkić, pod nazivom *Mobile banking authentication based on cryptographically secured Iris biometrics* pokazali su da je biometrijska potvrda identiteta postupak uspostavljanja korisničkog identiteta zasnovan na fiziološkim ili bihevioralnim osobinama osobe. Biometrija se može shvatiti kao konačno rešenje za potvrdu identiteta: korisnici ne moraju da pamte lozinke ili da nose tokene, a biometrijske osobine su prepoznatljive i nepovratne prirode, nudeći tako neodbijanje. Kao i bilo koji lični podaci, biometrijski uzorci mogu se presresti, ukrasti, ponovo reprodukovati ili izmeniti ako je nesigurni biometrijski uređaj povezan na mrežu ili ako vešti protivnik dobije fizički pristup uređaju koji ne koristi anti-forenzičke tehnike koje bi sprečile izdvajanje osetljivih podataka (tj. nezaštićeni uzorci). Zbog neopozivosti biometrijskih podataka, napadi mogu dovesti do krađe identiteta. Imajući to u vidu, postaje jasno da biometrijski sistemi rade sa osetljivim ličnim podacima i da su bezbednost i privatnost šablona važna pitanja kojima treba obratiti pažnju prilikom dizajniranja sistema za potvrdu identiteta. Da bi se falsifikovala krađa identiteta, ne treba se oslanjati na identifikaciju zloupotrebe nakon počinjenog dela (engl. *post-mortem*) - to treba sprečiti tehnološkim protivmerama koje pružaju snažnu sigurnost šablona i zaštitu privatnosti korisnika [13]. Pored toga, performanse biometrijskog sistema treba smanjiti na razumni nivo nakon uvođenja ovih protivmera u sistem, tj. od njih se očekuje da neće pogoršati tačnost verifikacije na neprihvatljiv nivo ili uvesti ozbiljne računske troškove ili zahteve za skladištenjem.

Autori *Kaur* i *Khanna* su 2020. objavili rad pod imenom *Remote Multimodal Biometric Authentication using Visual Cryptography* u kom su predstavili arhitekturu za višemodalne sisteme za biometrijsko prepoznavanje gde su korisnik, sistem prepoznavanja i baza podataka šablona udaljeni preko mreže. Kako je broj biometrijskih podataka ograničen, a kada se jednom izgube, zauvek su ugroženi. Imperativ je dizajnirati sisteme koji optimizuju stope prepoznavanja, a takođe se bave pitanjima bezbednosti i privatnosti za šeme autentifikacije sa omogućenom biometrijom. Predložena arhitektura omogućava opoziv multimodalnim biometrijskim šablonima i osigurava njihovo skladištenje i prenos preko udaljene mreže uz pomoć tehnike vizuelne kriptografije. Predložena arhitektura daje dobre performanse podudaranja i takođe ispunjava četiri kriterijuma zaštite uzorka, tj. sigurnost, raznolikost, opozivosti i performanse [18]. Takođe se obrađuju različiti scenariji napada kao što su „pecanje“ (engl. *phishing*), ponovna reprodukcija (engl. *replay attack*), napadi na baze podataka (presretanje između modula ili izmena podataka u bazi), „posrednik“ i napad putem mnoštva zapisa. Više informacija o napadima na ovakve sisteme mogu se pronaći u uvodnom delu doktorske disertacije *Battista Biggio* [19].

Kratak pregled u oblasti istraživanja dat je sa ciljem da čitaocu pruži mogućnost da iz probranih izbora dođe do dodatnih informacija koje su navedene u disertaciji. Molim čitaoce da u slučaju potrebe, kontaktiraju autora referenci navedenim u poglavlju Literatura.

„The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. “

Claude Shannon

3. Generisanje i distribucija kriptoloških ključeva

U trećem poglavlju ove disertacije date su osnovne definicije kriptologije kao nauke i njenih oblasti koje su sastavni deo nje. Objašnjen je pojam savršene tajnosti kao uvod u kriptološke algoritme nakon čega su objašnjeni pojmovi generisanja i distribucije kriptoloških ključeva.

Komunikacija između dve ili više osoba predstavlja njihovu međusobnu aktivnost koja ima za cilj ili se sastoji od razmene nekih informacija. Tokom samog procesa razmena informacija, osobama koje učestvuju u datoj komunikaciji često i nije bitno da li će njihovu komunikaciju neko razumeti ili prekinuti, no naravno postoje i obrnute situacije kada je bitno da celokupna komunikacija bude razumljiva samo učesnicima iste. Često se i u svakodnevnom životu susrećemo sa pojmom tajne komunikacije. Za ovakvu komunikaciju očekujemo da niko sem samih učesnika ne zna o čemu je zapravo reč. U ovakvim situacijama potrebno je koristiti neke načine da razmena informacija bude prikrivena.

Načini kako čovek ostvaruje komunikaciju su: kroz govor, putem pisanja i vizuelno gde možemo podrazumevati slike ili simbole. Osobe koje u datom trenutku obavljaju samu komunikaciju mogu biti na istom mestu u isto vreme ili na različitim mestima u isto vreme.

Kroz istorijsku analizu komunikacije, uočava se i potreba za razvojem načina prenosa informacija. Primećuje se i potreba da se informacija za što kraće vreme prenese između učesnika, te je i jasan razvoj informacionih tehnologija kao način za realizaciju iste. Istovremeno zapaža se i praksa da poruke koje se prenose treba da budu tajne, odnosno da se na neki način prikriju. Kako sam prenos poruka tako su se i načini njihovih prikrivanja razvijali vekovima unazad.

Oblast nauke koja se bavi tehnikama održavanja da informacija bude i ostane tajna zove se Kriptografija. Počeci razvoja ove nauke, iako se najčešće vezuje za oblast informacionih tehnologija, datiraju još iz perioda pre nove ere.

Mnoge važne istorijske ličnosti koristile su kriptografiju, neki od njih su:

- Gaj Julija Cezar koji je pomeranjem slova za određen broj mesta dobijao nov tekst koji je u potpunosti nečitljiv i nerazumljiv svima koji ne znaju broj pomeranja slova. Dakle, ako bi definisao da se sva slova pomeraju za 3 mesta to bi značilo da će se slovo A predstavljati sa slovom D. Ovo je tehnika koja je u kriptografiji poznata pod imenom Cezarova šifra [20].
- Slikar Leon Batista Alberti, italijanski slikar, je koristio dva kruga alfabeta i brojao redosled slova, u zavisnosti od pozicije posmatranog slova u alfabetu, dakle parna ili neparna pozicija, koristio je jedan od krugova alfabeta. Slova od kojih počinje alfabet predstavljaju ključ i deo su teksta koji treba da se sakrije.
- Fransis Bejkon, engleski filozof, je dao veliki doprinos nauci popularizujući induktivnu metodu kao i pojam eksperimenta odnosno princip istraživanja na osnovu iskustva. Pored filozofije deo svog života je bio u politici gde je bio jedan od učesnika formiranja engleske tajne službe odnosno same špijunaže.
- Tomas Džeferson je slova alfabeta ređao kao diskove i dobio oblik valjka, svaki disk je sadržao abecedu čija su slova počinjala različitim redosledom. Ključno je bilo znati redosled po diskovima za raspoznavanje poruke koja se šalje.

Postoje brojne knjige posvećene isključivo istoriji same kriptografije, među njima su i autori Dejvid Kan [21] i Sajmon Sing [22]. Međutim, kriptografija se ne bazira samo na istorijskom akcentu, većina nas koristi kriptografske metode prilično često, često bez znanja ili razmišljanja o tome, na primer, kada se vrši kupovina preko kreditne kartice ili slanje poruka korišćenjem elektronske pošte.

3.1. Osnovni pojmovi

U oblasti bezbednosti informacija, termini kriptografija, kriptoanaliza i kriptologija imaju suptilno različita značenja. Proces razvoja sistema za prikrivanje informacija tako da ih u idealnom slučaju ne može razumeti niko osim ciljanog primaoca informacije naziva se kriptologija, a metoda

dizajnirana da izvrši ovaj proces naziva se kriptografija [23]. Kriptoanaliza se odnosi na proces otkrivanja prikrivene informacije kroz pokušaje da se razume i sazna ključ. Često kriptoanaliza pored same analize jednog kripto sistema podrazumeva i napade na isti. Kriptologija je sveobuhvatan termin koji uključuje kriptografiju, kriptoanalizu i interakciju između njih.

Kada dve strane koriste šifru za razmenu informacija, neprikrivene informacije nazivaju se otvorenim tekstom, a prikrivene informacije se naziva šifrovani tekst ili šifrat. Proces pretvaranja otvorenog teksta u šifrovani tekst naziva se šifrovanje. Po prijemu šifrovanog teksta, primalac mora ukloniti ključ, ovaj proces se naziva dešifrovanje. Da bi mogli efikasno da šifruju i dešifruju poruke, dva učesnika u komunikaciji obično moraju da dele znanje o tajnom ključu, koji se koristi u takozvanom dogovorenom šifrovanju. Tačnije, ključ za šifru je informacija koja je obično poznata samo pošiljaocu i nameravanom primaocu poruke, koju pošiljalac koristi za šifrovanje otvorenog teksta, a primalac za dešifrovanje šifrovanog teksta [24].

Shodno navedenom, bitno je naglasiti da kriptografija nije teorija kodovanja. Za razliku od kriptografije, u kojoj je cilj prvenstveno prikrivanje informacija, kod kodova je cilj pouzdan i efikasan prenos informacija preko komunikacionog medija.

U praksi se obično pretpostavlja da kada par učesnika u komunikaciji koristi šifru za poverljivu komunikaciju, način šifrovanja koji se koristi poznat je svim protivnicima koji žele da otkriju sadržaj poruke. Dakle, sigurnost šifrovanja se može opisati kao mera koliko bi protivniku bilo teško da razbije šifru, odnosno koliko bi protivniku bilo teško da pronađe ključ za šifru.

Različite vrste šifrovanja koje su korišćene i koje se koriste u praksi podeljene su u dve široke kategorije:

- Šifrovanje sa simetričnim ključem i
- Šifrovanje sa javnim ključem poznato i kao asimetrično šifrovanje.

Šifre sa simetričnim ključem, jedina vrsta koja je postojala pre 1970-ih, takođe se ponekad nazivaju šiframa sa privatnim ključem. Kada se koristi šifra sa simetričnim ključem, pošiljalac poruke i nameravani primalac poruke moraju čuvati ključ u tajnosti od protivnika. Ova vrsta šifrovanja se često u literaturi naziva klasično šifrovanje [25]. Nedostatak kod šifrovanja sa simetričnim ključem je u tome što učesnici u komunikaciji moraju imati način da razmene ključeve u tajnosti i nezavisno od poruke koju šalju.

Pronalazak šifrovanja sa javnim ključem je revolucionirao otkriće u okviru kriptologije. Kod šifrovanja sa javnim ključem se koristi par ključeva, jedan za šifrovanje i jedan za dešifrovanje [26]. Kada se koristi šifrovanje sa javnim ključem, željeni primalac poruke kreira i ključ za šifrovanje i ključ za dešifrovanje, objavljuje ključ za šifrovanje tako da svako može da ga zna, ali čuva ključ za dešifrovanje u tajnosti. Na ovaj način, pošiljalac poruke može znati ključ za šifrovanje, koji mu je potreban za šifrovanje otvorenog teksta, ali samo primalac zna ključ za dešifrovanje. Iako se čini se da je nedostatak u šiframa sa javnim ključem baš taj što protivnici mogu da znaju ključeve za šifrovanje, obično nije realno moguće pronaći ključeve za dešifrovanje na osnovu znanja koje se poseduje o ključevima za šifrovanje [27].

Razvoj šifrovanja sa javnim ključem ipak nije doveo do propasti šifrovanja sa simetričnim ključem [28]. Glavni razlog tome proizilazi iz činjenice da šifrovanje sa javnim ključem obično radi mnogo sporije nego simetrično.

Mnogi zaista fascinantni istorijski zapisi o kriptologiji uključuju uspešne kriptoanaliza. Jedan od takvih je i napad na nemačku mašinu Enigma od strane savezničkih kripto-analitičara u Engleskoj, tokom Drugog svetskog rata. Cilj kriptoanalize je često određivanje odnosno izračunavanje kriptološkog ključa. Najočigledniji metod za određivanje, poznat kao napad grubom silom, uključuje testiranje svakog mogućeg ključa dok se ne pronađe onaj koji radi. Neki tipovi šifrovanja imaju relativno mali broj mogućih ključeva i stoga mogu biti napadnuti grubom silom. Međutim, gruba sila nije legitiman metod napada [29]. Na primer, za *Advanced Encription Standard*, koji je jedan od algoritama za simetrično šifrovanje minimalni broj mogućih ključeva je 3,4x1038, za šta bi bilo potrebni milioni godina da se testira računajući na korišćenje najnaprednije trenutne tehnologije. Sigurnost šifre nije uvek direktno vezana za broj mogućih ključeva iako je broj mogućih ključeva za šifrovanje zamenom veći od 4x1026 pokazano je da se šifrovanje zamenom ponekad može relativno lako razbiti pomoću tehnike koja se zove analiza frekvencije.

Sigurnost komunikacije se ne ogleda samo u tajnosti teksta već i u proveri identiteta korisnika koji u komunikaciji učestvuju. Poseban akcenat je na proveri da li je šifrovani tekst koji je primljen elektronskim putem zaista poslat od strane osobe koja tvrdi da ga je poslala, i da ključevi identifikovani elektronski zaista pripadaju osobi koja tvrdi da ih poseduje. Naročito u našem digitalnom dobu, potvrda da neko komunicira bas sa određenom osobom, može biti jednako važna kao i poruka koja se zapravo razmenjuje tokom komunikacije.

U kriptografiji se za procese šifrovanja i dešifrovanja koriste različite matematičke metode. Na osnovu toga moguće je čuvanje ili prenos tajnih podataka preko nesigurnih mreža poput Interneta. Podaci su dostupni samo ciljanim odnosno znanim primaocima poruka.

3.1.1. Ciljevi kriptografije

Glavni ciljevi kriptografije na osnovu navedenog su, dakle ono što kriptografija omogućava:

- Privatnost podataka, odnosno njihova poverljivost;
- Autentičnost podataka, odnosno potvrda da je poruka došla odakle se i tvrdi i
- Integritet podataka, odnosno da nije modifikovan toko prenosa.

Poverljivost podataka je ujedno i najčešći cilj. Realizuje se tako što se značenje poruke prikriva njenim kodiranjem. Dakle, pošiljalac šifruje poruku koristeći kriptografski ključ dok primalac dešifruje poruku koristeći kriptografski ključ koji može ili ne mora biti isti kao onaj koji koristi pošiljalac.

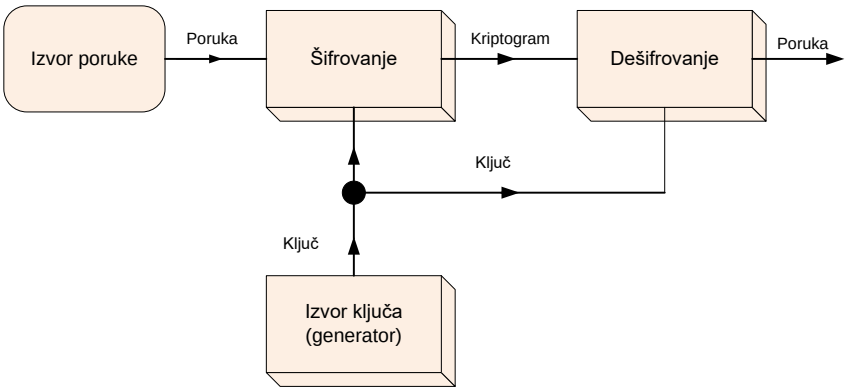
Autentičnost podataka se realizuje na način da korisnik ili sistem može dokazati svoj identitet drugome ko nema lično znanje o njihovom identitetu. Jedan od načina je korišćenje digitalnih sertifikata.

Integritet podataka kao jedan od ciljeva, osigurava da je primljena poruka ista kao poruka koja je poslata. Za realizaciju se koristi heširanje i kreira se jedinstvena sažeta poruka od poruke koja se šalje, zajedno sa porukom. Sa druge strane, primalac koristi istu tehniku da napravi drugi sažetak poruke da bi se uporedio sa originalnim. Bitno je naglasiti da integritet podataka samo štiti od nenamerne izmene poruke. Osnova svega navedenog je očuvanje tajnosti podataka.

3.2. Uslovi savršene tajnosti

Klod Šenon (Claude Shannon) je definisao uslove savršene tajnosti [30]. Kao prvi korak u matematičkoj analizi kriptografije, neophodno je da se situacija na odgovarajući način idealizuje i

da se na matematički prihvatljiv način definiše šta podrazumevamo pod sistemom tajnosti. Šenon je za početak definisao blok dijagram savršenog sistema tajnosti.



Slika 3-1: Blok dijagram savršenog sistema

Kod ovako definisanog sistema postoje dva izvora informacija, jedan koji predstavlja izvor poruke i drugi koji je izvor ključa- generator ključeva. Uloga izvora ključa je da proizvodi određeni ključ među onima koji su mogući u sistemu. Bitno je naglasiti da se ključ prenosi na neki drugi način u odnosu na poruku primaocu. Ovaj način prenosa nije presretljiv. Ova dva izvora će zajedno generisati novu poruku, kriptogram, koja će se prenositi komunikacionim kanalom u kom je moguće presretanje same nove poruke. Na prijemnoj strani, poslati ključ se kombinuje sa dobijenom porukom, dakle dešifruje se i dobija se početna poruka.

Šenon je pošao od pretpostavke da ne treba šifrovanje realizovati kao funkciju sa dve promenljive, već kao skup operacija ili transformacija. Transformacija primenjena na poruku proizvodi kriptogram. Pretpostavio je, takođe, da postoji samo konačan broj mogućih ključeva i da svaki ima odgovarajuću verovatnoću. Dakle, izvor ključa može biti statistički proces ili uređaj koji bira jednu iz skupa transformacija sa odgovarajućim verovatnoćama. Slično ovome, pretpostavio je da postoji i konačan broj mogućih poruka sa pridruženim verovatnoćama. Ovo je objasnio time da su slova koja su naređana jedna do drugih imaju određenu dužinu, misleći na reči koje predstavljaju poruku, dok frekvencija pojavljivanja ovih slova i reči predstavlja njihove pridružene verovatnoće.

Na prijemnom delu sistema, mora biti moguća transformacija koja će kriptogram vratiti u originalnu poruku. Dakle transformacije na prijemu je u stvari primena inverzne funkcije od transformacije na predajnoj strani sistema.

Šenon je na osnovu navedenog definisao da bi jedan sistem ispunio uslove tajnosti on mora funkcionisati kao suma jedinstveno reverzibilnih transformacija koja transformiše skup mogućih poruka u skup kriptograma, pri čemu svaka transformacija ima odgovarajuću verovatnoću [31].

Pretpostavio je da ako su poruke konačnog broja $P_1, P_2 \ldots P_n$, ako imaju a priori verovatnoće $V(P_1), V(P_2) \ldots V(P_n)$, ako su šifrovane u moguće kriptograme $K_1, K_2 \ldots K_m$, tako da je $K = T_i P$, gde je T transformacija koja se primenjuje u procesu šifrovanja.

Kripto analitičar presreće određen kriptogram, on može izračunati a posteriori verovatnoće za različite poruke $V_K(P)$.

Savršena tajnost se može definisati pod uslovom da su za sve kriptograme a posteriori verovatnoće jednake a priori verovatnoćama nezavisno od vrednosti samih kriptograma. U ovom slučaju, presretanje poruke neće dati nikakve informacije o poruci kripto analitičaru. Svaka njegova akcija koja zavisi od informacije sadržane u kriptogramu ne može se promeniti, za sve njegove verovatnoće ono što kriptogram sadrži ostaje nepromenjeno. Sa druge strane, ako uslov nije zadovoljen, postojaće situacije u kojima će kripto analitičar imati određene a priori verovatnoće, ili određene poruke što može uticati na njegove postupke čime se neće postići savršena tajnost. Pokazao je da potreban i dovoljan uslov za savršenu tajnost sledi iz Bajesove teoreme [32]:

$$V_K(P) = \frac{V(P)V_P(K)}{V(K)}$$

U navedenoj formuli:

- $V(P)$= *a priori* verovatnoća poruke.
- $V_P(K)$= uslovna verovatnoća kriptograma ako je poruka izabrana, ili suma verovatnoća svih ključeva koji proizvode kriptogram iz poruke.
- $V(K)$= verovatnoća dobijanja kriptograma iz bilo kog razloga.
- $V_K(P)$= *a posteriori* verovatnoća poruke ako je kriptogram presretnut.

Za savršenu tajnost a posteriori verovatnoća i a priori verovatnoća poruke moraju biti jednake, što dovodi konačno do definicije koja važi za sve poruke i kriptograme pod uslovom da je a posteriori verovatnoća nezavisna od poruke [31]:

$$V_P(K) = V(K)$$

Definisao je niz različitih kriterijuma koje treba primeniti u proceni sistema tajnosti. Najvažniji od njih su:

- količina tajnosti – za savršeni sistem je karakteristično da i posle velikog broja pokušaja , kripto analitičar nema jedinstveno rešenja kako da kriptogram transformiše u poruku. Šenonov predloženi sistem ne treba da bude savršen po pitanju tajnosti, već takav da dajući neke informacije, ne daje jedinstveno rešenje. Dakle, potrebno je da postoje velike varijacije u količini rada potrebnog da se dođe do rešenja i u količini kriptograma koji se moraju presresti da bi rešenje postalo jedinstveno.
- veličina ključa – ključ se mora preneti na nepresretljiv način do primaoca. Ponekad se mora zapamtiti. Stoga je poželjno je da ključ bude što manji, najmanja vrednost je jednaka dužini poruke.
- složenost operacija šifrovanja i dešifrovanja – šifrovanje i dešifrovanje bi, naravno, trebalo da bude što jednostavnije. Ako se radi ručno, složenost dovodi do gubitka vremena kao i do grešaka jer je prisutan ljudski faktor. Sa druge strane, ako se automatizuje uz pomoć računara složenost može zahtevati upotrebu velikih skupih mašina.
- propagacija grešaka – kod određenih tipova šifri, greške koje nastaju zbog jednog slova u šifrovanju ili u procesu prenosa dovode do velikog broja grešaka u dešifrovanom tekstu. Ovo dovodi do gubitka velikog broja informacija i potrebe za velikim brojem ponavljanja kriptograma. Propagacija ili širenje grešaka se takođe mora svesti na minimum.
- proširenje poruke – u određenim sistema, veličina poruke se povećava procesom šifrovanja. Ovaj neželjeni efekat se može videti u sistemima gde se u procesu šifrovanja dodaju nule ili gde se koristi više različitih zamena.

Na osnovu ovih definicija i dokaza razvijaju se razni matematički modeli koji će vršiti šifrovanje odnosno dešifrovanje sa jedne strane, a sa druge strane razvijaju se i različiti načini da se generišu ključevi.

3.3. Algoritmi

Ukoliko se neki matematički model ili funkcija primeni na poruku i dobije se kriptogram i ako se ovakav obrazac ponavlja konačan broj puta dobija se procedura odnosno način kako se poruka šifruje. U literaturi ovaj postupak se definiše kao kriptografski algoritam ili algoritam za šifrovanje [33]. Najjednostavnija definicija algoritma bi bila da je to automat konačnih stanja koji se inicijalizuje na bazi šifarskih ključeva, a zatim radi po automatizmu. Algoritam u sebi sadrži različite korake, svaki korak je unapred definisana operacija, sve one zajedno čine da algoritam bude konačan, a rezultat koji proizilazi iz njegovog rada treba da bude jedinstven.

Različite vrste šifrovanja definišu algoritme koji se za to koriste. Kako je već navedeno da šifrovanje može biti simetrično i asimetrično tako se i u literaturi definišu: simetrični algoritmi i asimetrični algoritmi [33].

Kriterijumi na osnovu kojih se mogu analizirati različiti algoritmi su:

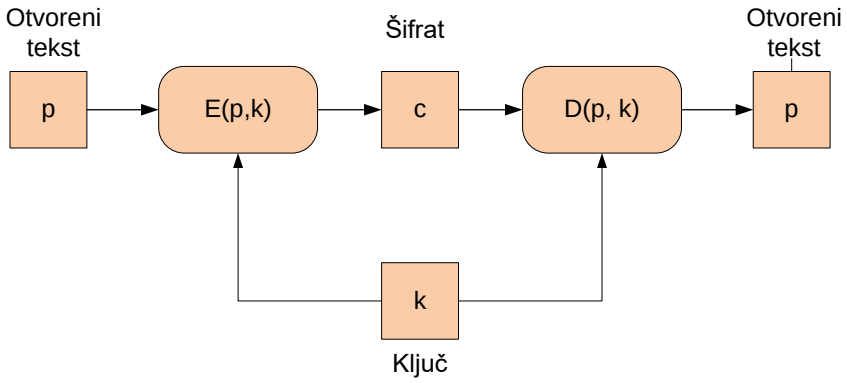
- *Arhitektura* - definiše strukturu i operacije koje algoritam može da izvede, njegove karakteristike i način na koji se implementiraju. Takođe određuje da li je algoritam simetričan ili asimetričan, odnosno da li koristi tajni ili javni ključ za šifrovanje i dešifrovanje.
- *Sigurnost* - afirmativna mera snage sistema u odupiranju napadu je poželjan element svakog algoritma šifrovanja. Bezbednost algoritma za šifrovanje zavisi od veličine ključa koji se koristi za izvršenje šifrovanja: generalno, što je veća veličina ključeva realizovaće se snažnije šifrovanje.
- *Fleksibilnost* - definiše da li je algoritam u stanju da izdrži manje modifikacije u skladu sa zahtevima.

- *Skalabilnost* - skalabilnost zavisi od određenih parametara kao što su upotreba memorije, brzina šifrovanja, performanse hardvera i softvera, efikasnosti računara i drugi.
- *Ograničenja* - definišu koliko fino algoritam funkcioniše korišćenjem računarskih resursa koji su mu dostupni. Odnosno definiše koliko je algoritam ranjiv pri čestim napadima

Da bi se primenio odgovarajući algoritam potrebno je poznavati njegovu snagu i ograničenja. Zbog toga je neophodna procena različitih postojećih algoritama na osnovu određenih parametara. Parametri mogu da obuhvataju arhitekturu, bezbednost, skalabilnost (u smislu brzine šifrovanja, korišćenja memorije, hardverskih performansi softvera i vremena računanja), ograničenja i fleksibilnost.

3.3.1. Simetrični algoritmi

Šifrovanje sa jednim ključ se realizuje tako što se koristi tajni ključ i poznati algoritam za izvršavanje procesa šifrovanja odnosno dešifrovanja. Neki popularni simetrični algoritmi su DES (engl. Data Encryption Standard), AES (engl. Advanced Encryption Standard), IDEA (engl. International *Data Encryption Algorithm*), Blowfish, Twofish i drugi.

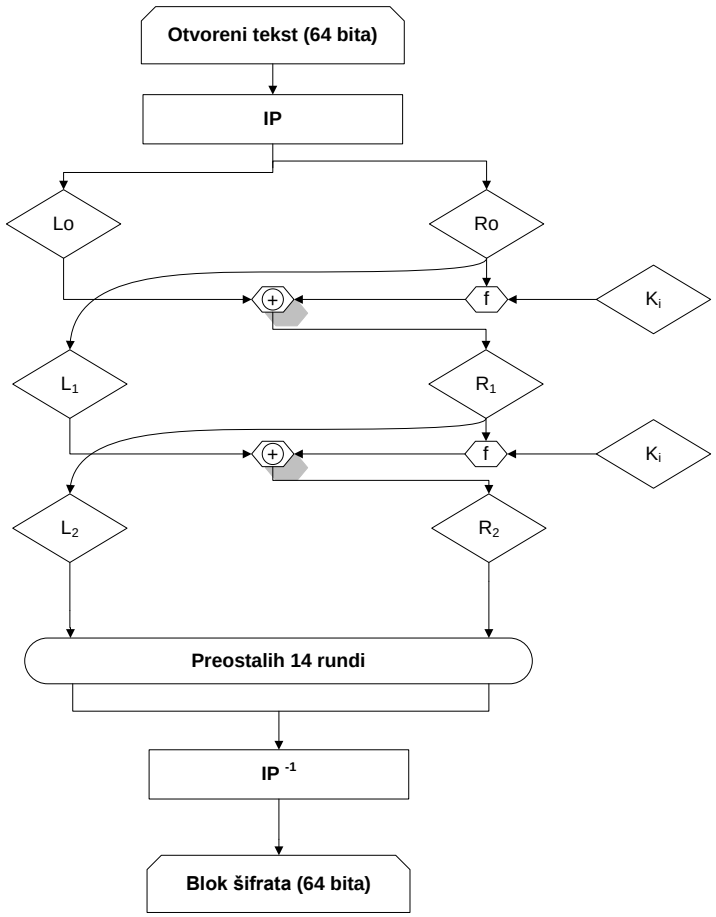


Slika 3-2 Simetrični algoritmi

3.3.1.1. DES algoritam za šifrovanje i dešifrovanje podataka

DES standard za šifrovanje podataka je razvijen 1974. godine, IBM ga je dizajnirao na osnovu njihove Luciferove šifre, bio je prvi standard šifrovanja koji je objavio NIST [34].

DES (*Data Encryption Standard*) se u početku smatrao jakim algoritmom, ali danas velika količina podataka i kratka dužina ključa DES-a ograničava njegovu upotrebu [35]. Operacije šifrovanja i dešifrovanja se zasnivaju na binarnom broju koji se zove ključ. Ključ se sastoji od 64 binarne cifre, od kojih se 56 bitova koristi za algoritam, a 8 bitova se koristi za otkrivanje greške. Algoritam u sebi sadrži tri faze: početnu permutaciju (engl. *Initial permutation*), zatim obrada podataka koja se obavlja u 16 etapa i poslednji korak je inverzna permutacija. Faze algoritma su prikazane na slici 3.2.



Slika 3-3 DES algoritam [36]

Početni blok pod nazivom otvoreni tekst, u sebi sadrži tekst koji treba šifrovati i veličine je 64 bita. Potom je faza početne permutacije gde se dobija nov 64-bitni niz y_0. Sadržaj ovog niza se deli na pola, te se dobijaju dva nova niza, V_0 i N_0. Prvi niz čine 32 viša bita dok drugi niz čine 32 niža bita y_0. Ovim je prva faza završena.

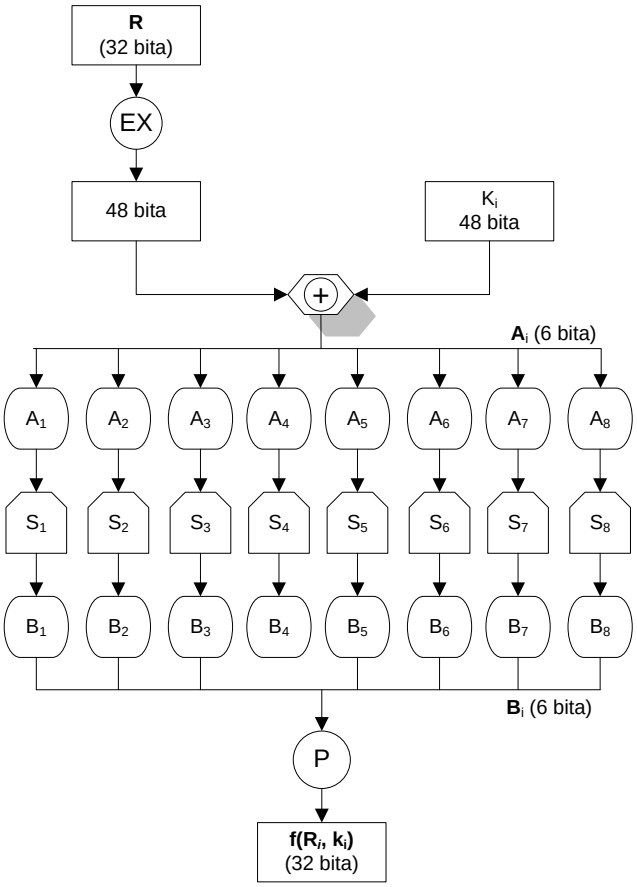
U narednoj fazi se 16 puta ponavljaju sledeće operacije:

- niži set bitova postaje tako što se iz prethodne iteracije uzima viši set bitova: $N_i = V_{i-1}$; dodatno parametar i predstavlja moguć broj iteracija odnosno maksimalna vrednost mu je 16.
- viši set bitova se dobija tako što se iz prethodne iteracije uzima niži set bitova i primeni se logička operacija ekskluzivno ili (engl. *XOR*) sa rezultatom funkcije nad višim bitovim prethodne iteracije i ključevima trenutne iteracije $V_i = N_{i-1} \oplus f(V_{i-1}, k_i)$

Poslednja faza , zvana inverzna permutacija radi zamenu nižih i viših bitova i na izlazu se dobija šifrat dužine 64 bita.

Operacije koje se izvode u okviru funkcije $f(V_{i-1}, k_i)$, nazivaju se i Fistelovo šifrovanje (engl. *Feistel Cipher*) [36] , ilustrovane su na slici 3.3.

Kao što se može uočiti prvo se proširuju dužine viših bitova prethodne iteracije i primeni se logička operacija xor nad ključem date iteracije. Nova dužina niza se deli na 8 jednakih celina i dobijaju se blokovi sa imenom A1 do A8. Nad svakim blokom se izvrši zamena vrednosti u okviru S blokova (engl. *supstitution box)* novodobijeni nizovi se smeštaju u B kutije svaki je dužine 4 bita, njihovim spajanjem zatim permutovanjem dobija se rezultat $f(V_{i-1}, k_i)$.



Slika 3-4 DES algoritam, Fistelovo šifrovanje [36]

U procesu dešifrovanja, obzirom da je DES simetrični algoritam, faze su identične. Naravno sada je na ulazu šifrat, prolazi se kroz iste faze kompletnog algoritma sa jedinom razlikom u samom ključu. Iteracije ključa koje se koriste, k_i idu obrnuto, dakle kreće se sa poslednjim koji se koristio u šifrovanju a završava sa prvim. Na ovaj način se dobija otvorena poruka.

TDES ili (3DES) je bila mnogo komplikovanija verzija DES-a koja je postizala visok nivo bezbednosti šifrovanjem podataka koristeći DES tri puta i koristeći tri različita nepovezana ključa. 3DES je i dalje odobren za upotrebu od strane vladinih sistema SAD, ali je zamenjen sa AES algoritmom.

3.3.1.2. AES algoritam za šifrovanje i dešifrovanje podataka

Algoritam (engl. *Advanced Encryption Standard*) je nastao tokom 1990-tih kao rezultat konkursa za algoritam koji bi zamenio DES, a koji je bio raspisan od strane američkog NIST instituta. Pobednik je bio *Rijndael* algoritam, koji je kasnije prihvaćen kao AES algoritam.

Poput DES-a, i AES je algoritam koji radi nad blokovima podataka i koji proces kodiranja izvršava kroz određeni broj rundi, međutim AES ne koristi Fistelovo šifrovanje. Posledica toga je da procesi šifrovanja i dešifrovanja nisu ekvivalentni. Zapravo, ovde su dešifrovanje i šifrovanje inverzni procesi. U odnosu na DES, AES je, sa matematičke tačke gledišta, izuzetno složen.

Ukratko, osnovne osobine standardnog AES algoritma su sledeće:

- Veličina bloka može biti 128 bita, 192 bita i 256 bitova.
- Dužina ključa, iako nije zavisna od dužine bloka, je iste dužine kao blok.
- Broj ponavljanja je od 10 do 14 puta a uslovljeno je jedino dužinom ključa.

U inicijalnoj rundi se postavljaju vrednosti ključa (*AddRoundKey* operacija). U svakoj od narednih (regularnih) rundi obavljaju se sledeće akcije(koraci):

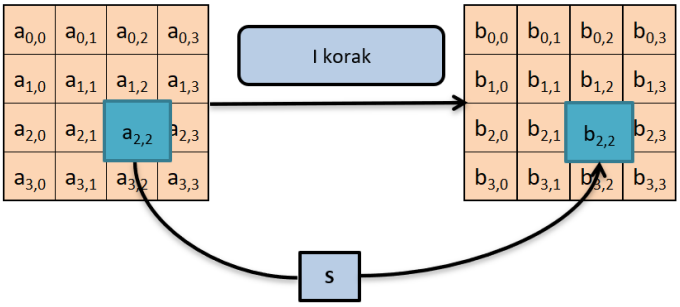
- I korak - SubBytes
- II korak - ShiftRows
- III korak - MixColumns
- IV korak - AddRoundKey

U finalnoj rundi izostavlja *MixColumn*s korak. Distribucija ključa se obavlja po Rijndelovom algoritmu za distribuciju ključa.

SubBytes operacija

Ulaz u *SubBytes* operaciju su bajtovi podataka koji treba da budu šifrovani, i oni su na slici 3.4 označeni kao elementi matrice A. U ovom koraku svaki ulazni bajt menja svoju vrednost nakon interakcije sa odgovarajućim elementom iz osmobitne supstitucione matrice. Ova operacija obezbeđuje nelinearnost dobijenog koda i obezbeđuje da takozvani linearni algebarski napadi

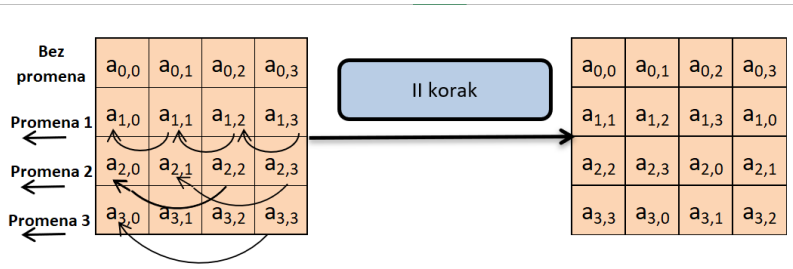
nemaju efekta protiv ovog algoritma. S-matrica koja se ovde koristi je zapravo originalna Rijndaelova S-matrica.



Slika 3-5 I korak - zamena bajtova

ShiftRows operacija

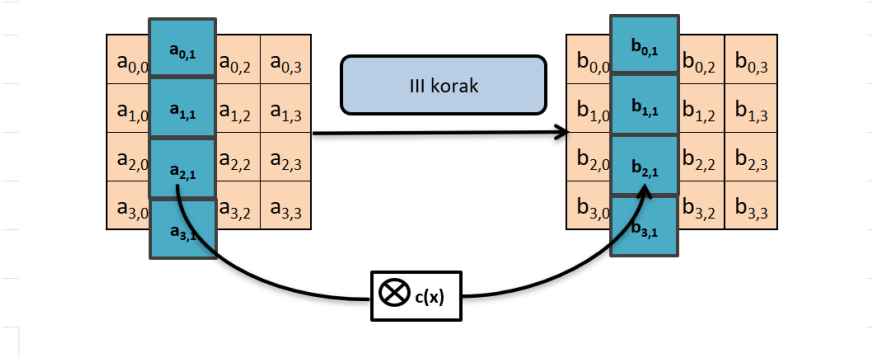
Ulaz u ovu operaciju je matrica koja predstavlja rezultat prethodnog koraka. Ta matrica je označena sa A. Operacija *ShiftRows* radi nad elementima jednog reda matrice tako što ih ciklično pomera za odgovarajuću vrednost koja se naziva *offset.* U ovom slučaju prvi red ostaje isti dok se svaki naredni red pomera za po jedno mesto u levo što se vidi na slici 3.5. Posle završenih operacija dobija se nova promenjena matrica A.



Slika 3-6 AES II korak - Pomeranje reda

MixColumns operacija

Ulaz u ovaj korak je matrica koju smo dobili kao rezultat *ShiftRows* koraka. Označićemo je sa A. U koraku *MixColumns* sva četiri bajta svake kolone promene mesta koristeći neku inverznu linearnu transformaciju. Dakle, *MixColums* operacija uzima četiri bajta kao ulaz i vraća četiri bajta na izlazu. Zajedno sa *ShiftRows* ovaj korak obezbeđuje difuziju podataka u ovom kodnom sistemu.

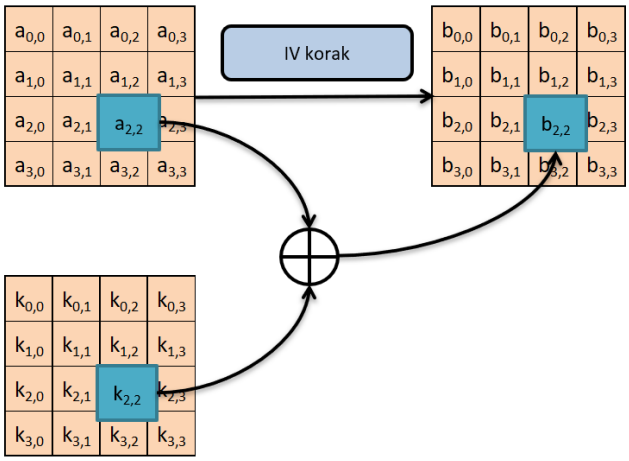


Slika 3-7 III korak - Mešanje podataka po kolonama

Svaka kolona se ovde tretira kao polinom nad **GF**(2^8) poljem i predstavlja rezultat množenja modula po $x^4 + 1$ i fiksnog polinoma $c(x) = 3x^3 + x^2 + x + 2$ (slika 3.6).

AddRoundKey Operacija

Ulaz u ovaj korak je matrica dobijena nakon *MixColumn* Operacije. Nazovimo tu matricu A. Da bi se dobila kriptovana matrica (označićemo je sa B) iskombinovaćemo matricu A sa matricom koja sadrži ključ koristeći XOR operaciju nad odgovarajućim bajtovima (slika 3.7). Za svaku rundu se generiše poseban ključ koji se generiše na osnovu polaznog ključa po Rijndaelovom algoritmu za distribuciju ključeva. Svaki podključ je matrica koja je po dimenzijama jednaka matrici A.



Slika 3-8 AES IV korak - dodavanje podključa

Rijndael algoritam za distribuciju ključeva

Algoritam koji se koristi za distribuciju ključeva u okviru AES algoritma u originalu se zove *Rijndael key schedule* algoritam**.** Pomoćne operacije koje se koriste u ovom algoritmu su rotacija, *Rcon* preslikavanje, *S-box* preslikavanje i osnovna raspodela ključeva.

Operacija rotacije ima funkciju 32-bitnog kružnog pomeračkog registra na levo. Ako je ulazna reč 1d2c3a4f, nakon *RotWord* operacije reč će biti transformisana u 2c3a4f1d, ako su članovi stringa ASCII karakteri.

Rcon preslikavanje se vrši na osnovu *Rcon* matrice. Opis kako je *Rcon* matrica dobijena ovde će biti izostavljen. Za svaki bajt se može izračunati odgovarajuća *Rcon* vrednost direktnim čitanjem iz *Rcon* tabele. Ako je vrednost ulaznog bajta označena sa B, njegov *Rcon* ekvivalent se računa kao RB = *Rcon* [B].

Osnovna raspodela ključeva je operacija koja se odvija u unutrašnjoj petlji algoritma za raspodelu ključeva *i* za nju je karakteristično sledeće:

- Ulaz je 32-bitna reč, i redni broj iteracije *i*. Izlaz je 32-bitna reč.
- Izlazna reč zamenjuje ulaznu u daljim računanjima.

Prethodno navedena *RotWord* operacija se primenjuje na svaku grupu od 32 bita izlazne reči.

Primeni se S-box preslikavanje na svaki bajt izlazne reči.

Primeniti *Rcon* operaciju nad vrednosti *i*, pa onda uraditi XOR nad izlazom iz pomenute *Rcon* operacije i prvog bajta izlazne reči.

Raspodela ključa

Pošto je distribucija ključa vrlo slična za svaku od mogućih dužina ključeva (i za 128 bita, i za192 i za 256-bit), kao i sam proces šifrovanja definisaćemo sledeće konstante koje zavise od dužine ključa:

- *n* – predstavlja broj bajtova u osnovnom ključu i ima vrednost: 16 za ključ od 128 bita, 24 za 192 bita u ključu i 32 za 256-bitne ključeve
- *b* – predstavlja broj bitova u proširenom ključu i ima vrednost: 176 za 128-bitni ključ, 208 za 192-bitne i 240 za 256-bitne.

Opis distrubucije ključeva

Rijndaelova distribucija ključeva se odvija po sledećim koracima:

- Prvih *n* bajtova proširenog ključa je zapravo uneti kodni ključ
- Vrednost *i* koja se koristi za *Rcon* iteracije je postavljena na 1.

Sve dok ne dobijemo svih *b* bajtova proširenog ključa, radimo sledeće kako bi generisali nedostajuće bajtove:

Sledeće korake izvodimo kako bi generisali po 4 nedostajuća bajta u ključu:

1. Kreiramo privremenu četvorobajtnu promenljivu *t*.
2. Prethodna 4 bajta u proširenom ključu dodelimo bajtovima u promenljivoj *t*.
3. Izvedemo osnovnu raspodelu ključeva nad *t*, gde i koristimo kao *Rcon* ulaznu vrednost.
4. Uvećamo *i* za 1.

Opisan je način kako rade dva najpoznatija algoritma za šifrovanje simetričnim ključem. U okviru dostupne literature na kraju disertacije, mogu se naći izvori koji daju više informacija o

ostalim algoritmima. U nastavku je prikazana tabela sa pregledima raznih simetričnih algoritama, koje mogu biti dovoljne za osnovne informacije o njima.

Ime	Struktura	Dužina osnovnog teksta	Dužina ključa	Broj *S box*	Broj ponavljanja
3DES	Fistelovo šifrovanje	64 bita	168	8	48
Blowfish	Fistelovo šifrovanje	64 bita	128-448	8	16
IDEA	*Substitution-Permutation*	64 bita	128	nema	8
TEA	Fistelovo šifrovanje	64 bita	128	nema	64 (32 kruga)
CAST	Fistelovo šifrovanje	64 bita	40-128	4	12 do 16
RC6	Fistelovo šifrovanje	128 bita	128, 192, 256	nema	20
Serpent	Fistelovo šifrovanje	128 bita	128, 192, 256	8	32
Twofish	Fistelovo šifrovanje	128 bita	128, 192, 256	4	16
MARS	Fistelovo šifrovanje	128 bita	128-448	1	32

Tabela 3-1 Pregled simetričnih algoritama

3.3.2. Asimetrični algoritmi

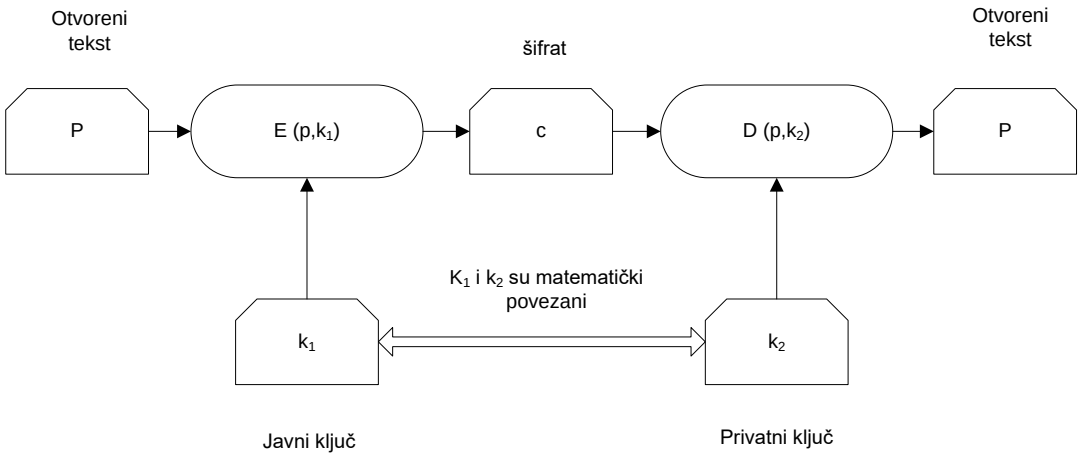
U ovom delu disertacije razmatraće se različiti algoritmi za šifrovanje sa javnim ključem, poznati pod imenom asimetrično šifrovanje. U sistemima za šifrovanje sa javnim ključem svaki entitet A ima javni ključ *j* i odgovarajući privatni ključ *p*. U sigurnim sistemima, zadatak izračunavanja privatnog ključa datog javnog ključa je računski neizvodljiv. Javni ključ definiše transformaciju šifrovanja , dok privatni ključ definiše pridruženu transformaciju dešifrovanja.

Svaki entitet B koji želi da pošalje poruku entitetu A dobija autentičnu kopiju A-ovog javnog ključa, koristi transformaciju šifrovanja da dobije šifrovani tekst zatim se vrši prenos šifrovanog teksta zajedno sa javnim ključem. Da bi dešifrovao, primenjuje se inverzna transformaciju kako bi se dobila originalna poruka. Javni ključ ne mora da se čuva u tajnosti, on može biti široko dostupan ali je potrebna potvrda njegove autentičnosti za garanciju da je A zaista jedina strana koja zna odgovarajući privatni ključ.

Osnovna prednost ovakvih sistema je u činjenici da je obezbeđivanje autentičnih javnih ključeva generalno lakše nego bezbedna distribucija tajnih ključeva poput distribucije ključa u sistemima sa simetričnim ključevima.

Glavni cilj šifrovanja sa javnim ključem je da obezbedi privatnost ili poverljivost. Pošto je A-ova transformacija šifrovanja poznata javnosti, samo šifrovanje sa javnim ključem ne obezbeđuje autentifikaciju porekla podataka ili integritet podataka.

Takve garancije moraju biti obezbeđene korišćenjem dodatnih tehnika, uključujući kodove za autentifikaciju poruka i digitalne potpise. Algoritmi šifrovanja sa javnim ključem su obično znatno sporiji od algoritama šifrovanja sa simetričnim ključem kao što je DES. Iz tog razloga, šifrovanje javnim ključem se najčešće koristi u praksi za transport ključeva koji se kasnije koriste za masovno šifrovanje podataka simetričnim algoritmima i drugim aplikacijama, uključujući integritet podataka i autentifikaciju, i za šifrovanje malih podataka.



Slika 3-9 Algoritam sa javnim ključem

3.3.2.1. RSA Algoritam

Jedan od algoritama za asimetrično šifrovanje je RSA algoritam. Njegova bezbednost se zasniva na neuhvatljivosti celobrojne faktorizacije. Postupak generisanja privatnog i javnog ključa je opisan kroz naredne korake:

1. Prvo se generišu p i q – ovo su dva približno iste veličine prosta broja.
2. Oni se potom pomnože tako da faktorizacija bude: $n = \frac{p \cdot q}{t} = (p-1)(q-1)$
3. Potom treba izabrati nov prost, e, za ovaj broj važi sledeća osobina $1 < e < t$, pri čemu izabran broj e i broj t ispunjavaju uslov da su uzajamno prosti.
4. Poslednji korak je izračunavanje broja d, ovaj broj se dobija primenom Euklidovog algoritma tako da proizvod e i d po modulu t, daje rezultat 1.
5. Na osnovu ovih koraka javni ključ predstavlja (n, e) dok je rezultat koraka broj 4 privatni ključ (d).

3.3.3. Funkcija za sažimanje – heš funkcija

Heš funkcije koriste poruku kao ulazni podatak zatim uz pomoć određenih operacija generišu izlazni podatak koji se u literaturi može naći pod sledećim imenima: heš kod, heš-rezultat, heš-vrednost ili jednostavno heš. Tačnije, heš funkcija h preslikava nizove bitova proizvoljne konačne dužine u nizove fiksne dužine od n bitova. Za domen D i opseg R sa h : D→R i |D| > |R|, funkcija je oblika više-prema-jedan, što implicira da je postojanje kolizija neizbežno. Zaista, ograničavajući h na domen t-bitnih ulaza (t > n), ako je h „slučajan“ u smislu da su svi izlazi u suštini jednako verovatni, tada bi se oko 2^{t-n} ulaza preslikalo na svaki izlaz, a dva nasumično izabrana ulazi bi dali isti izlaz sa verovatnoćom 2^{-n} (nezavisno od t). Osnovna ideja kriptografskih heš funkcija je da heš vrednost služi kao kompaktna reprezentativna slika (ponekad se naziva otisak, digitalni otisak ili sažetak poruke) ulaznog niza i može se koristiti da se jedinstveno identifikuje niz.

Heš funkcija (u neograničenom smislu) je funkcija h koja ima minimalno sledeća dva svojstva:

1. kompresija — h mapira ulaz k proizvoljne konačne dužine bita u izlaz h(k) koji je fiksne dužine.
2. lakoća izračunavanja— s obzirom na h i ulaz k, h(k) je lako izračunati.

Jedan od algoritama koji koristi heš funkcije je SHA 1 skraćenica je nastala od *Secure Hash Algoritam*. Algoritam se sastoji od pet heš funkcija, dizajnirala ga je Agencija za nacionalnu bezbednost (NSA) a objavio Nacionalni institut za standarde i tehnologiju (NIST). SHA 1 proizvodi 160-bitni sažetak poruke za poruku čija je maksimalna dužina 264. Sažetak poruke je izlaz poruke fiksne dužine. Sažetak poruke se zatim unosi u algoritam digitalnog potpisa, koji će zatim generisati potpis za poruku. Potpisivanje sažetka poruke umesto poruke nudi poboljšane performanse jer će sažetak poruke biti mnogo manji od poruke. Primalac poruke će tada koristiti isti heš algoritam za verifikaciju potpisa. Svaka promena koja se dogodi tokom tranzita će rezultirati drugačijim sažetkom poruke i, prema tome, potpis neće biti verifikovan. Kada se potvrdi da je tačna, primalac može da otključa poruku. Ovaj metod sprečava neovlašćene korisnike da pregledaju poruke koje nisu namenjene njima.

Digitalni potpis je niz podataka koji povezuje poruku (u digitalnom obliku) sa nekim izvornim entitetom. Algoritam za generisanje digitalnog potpisa (ili algoritam za generisanje potpisa) je metoda za proizvodnju digitalnog potpisa. Algoritam za verifikaciju digitalnog potpisa (ili algoritam za verifikaciju) je metod za proveru da li je digitalni potpis autentičan (tj. da ga je zaista kreirao navedeni entitet). Šema (ili mehanizam) digitalnog potpisa sastoji se od algoritma za generisanje potpisa i pridruženog algoritma za verifikaciju. Proces (ili procedura) potpisivanja digitalnog potpisa sastoji se od (matematičkog) algoritma za generisanje digitalnog potpisa, zajedno sa metodom za formatiranje podataka u poruke koje se mogu potpisati. Proces (ili procedura) verifikacije digitalnog potpisa sastoji se od algoritma verifikacije, zajedno sa metodom za oporavak podataka iz poruke.

Prenos ključa može se smatrati posebnim slučajem autentifikacije poruke sa privatnošću, pri čemu poruka uključuje kriptografski ključ. Mnogi protokoli za razmenu ključeva, zasnovani na tehnikama javnog ključa, koriste digitalne potpise za autentifikaciju, dok su drugi usko povezani sa tehnikama za identifikaciju.

3.3.4. Uspostavljanje i prenos ključa

Autentifikacija i uspostavljanje ključa su osnovni koraci u uspostavljanju bezbedne komunikacije. Autentifikacija se odnosi na saznanje da ispravne strane komuniciraju;

uspostavljanje ključeva se bavi dobijanjem dobrih kriptografskih ključeva za zaštitu komunikacija, posebno za obezbeđivanje poverljivosti i integriteta saopštenih podataka. Budući da se savremeni svet sve više oslanja na digitalne mreže, bezbednost komunikacija je kritičan element u funkcionisanju društva danas, a u budućnosti će postati samo važnija. Protokoli za autentifikaciju i uspostavljanje ključa stekli su reputaciju da ih je teško analizirati i pravilno dizajnirati [37].

Protokol za razmenu ključeva se definiše kao algoritam sačinjen od niza koraka koji precizno definišu akcije koje su potrebne od strane korisnika da bi se postigao određeni cilj. Uspostavljanje ključa je proces ili protokol kojim zajednička tajna postaje dostupna dvema ili više strana, za naknadnu kriptografsku upotrebu. Uspostavljanje ključa se može široko podeliti na: prenos ključa i dogovor oko ključa [38]. Protokol ili mehanizam za transport ključa je tehnika uspostavljanja ključa gde jedna strana kreira ili na drugi način dobija tajnu vrednost i bezbedno je prenosi drugoj. Protokol ili mehanizam dogovora oko ključa je tehnika uspostavljanja u kojoj dve strane izvode zajedničku tajnu kao funkciju informacija koje su doprinele ili su povezane, tako da nijedna strana ne može unapred da odredi rezultujuću vrednost.

Autentifikacija i uspostavljanje ključa se obično dešavaju na početku komunikacione sesije, koju često nazivamo jednostavno sesijom. Autentifikacija omogućava onim stranama aktivnim u sesiji da saznaju identitet drugih strana u sesiji [39]. Uspostavljanje ključa se koristi za podešavanje ključa sesije, koji se koristi za naknadnu zaštitu podataka koji se komuniciraju tokom sesije uz pomoć kriptografskih mehanizama koji su izabrani. Kao stvar opšteg principa, nije moguće uspostaviti ključ sesije bez već dostupnih postojećih sigurnih kanala. Stoga, osim mogućnosti bezbednog fizičkog uspostavljanja ključeva, od suštinskog je značaja ili da se ključevi već dele između različitih korisnika ili da su autentični javni ključevi dostupni. Stoga protokol za uspostavljanje ključa uvek sadrži dve vrste ključeva: ključevi sesije, koji se uspostavljaju tokom protokola; dugoročni ključevi, koji postoje pre pokretanja protokola. Ključevi sesije su skoro uvek ključevi za upotrebu sa kriptografijom sa simetričnim ključem i dele se između strana u protokolu nakon završetka protokola. U praksi je uobičajeno da se iz ključa sesije izvede veći broj daljih ključeva, na primer dobijati različite ključeve za svaki pravac dvosmernog bezbednog kanala [40].

Dugoročni ključevi često dolaze u različitim tipovima:

- *Zajednički ključevi*. Strane protokola mogu unapred da dele ključeve za kriptografiju sa simetričnim ključem (i često se nazivaju unapred deljeni ključevi). Oni se mogu deliti na osnovu parova između strana, što može uključivati servere od poverenja kao i obične korisnike protokola [41].
- *Javni-privatni ključevi*. Strane u protokolu mogu imati dugoročne javne ključeve za koje poseduju odgovarajući privatni ključ. Obično to znači da infrastruktura javnog ključa mora biti uspostavljena tako da strane mogu potvrditi javne ključeve putem sertifikata [41] .

3.3.4.1. Diffie-Hellmanov protokol za razmenu ključeva

Diffie-Hellmanov protokol za razmenu ključeva je kriptografski protokol koji dozvoljava uspostavu zajedničkog tajnog ključa preko nesigurnog komunikacionog kanala . Obe strane, zatim koriste ovaj ključ za šifrovanje narednih komunikacija koristeći šifrovanje sa simetričnim ključem. Šemu su prvi javno objavili *Vhitfield Diffie* i *Martin Hellman* 1976. godine, *Diffie-Hellman* protokol za razmenu ključeva je sam po sebi anoniman protokol koji pruža osnovu za različite protokole za autentifikaciju. U originalnim opisima, *Diffie-Hellman* razmena sama po sebi ne obezbeđuje autentifikaciju strana koje komuniciraju i stoga je podložna napadu tipa čoveka u sredini. Matematički model njihovog algoritma je u osnovi sveden na rešavanje logaritma [42].

Karakteristike Diffie-Hellman protokola [43]

- Tajni ključevi se kreiraju samo po potrebi te nema razloga za njihovo čuvanje na duži vremenski period.
- Prilikom razmene potrebna infrastruktura zahteva samo globalne parametre.

Neke od slabosti *Diffie-Helman-ovog* algoritma su:

- ne pruža nikakve informacije o identitete obe strane. Dakle, ranjivo je na napad lažnog predstavljanja,
- računarski je intenzivan,

- ne može sprečiti ponovni napad i
- podložan je napadu čoveka u sredini.

3.4. Generisanje kriptografskih ključeva

Generisanje ključeva se u literaturi definiše kao proces koji obezbeđuje ključeve u jednom kriptografskom sistemu [44]. Bez obzira na postupak izbora koji se koristi za generisanje, iskustvo je pokazalo da treba izbegavati organizovane i predvidljive metode za izbor bitova ključa. Svaki postupak odabira na osnovu nečijeg broja telefona, imena i adrese, datuma rođenja ili slično, toliko je krhak da se ne može smatrati sigurnim. Takođe, programi za generisanje pseudoslučajnih brojeva dostupni na mnogim računarskim sistemima suviše su predvidljivi da bi se koristili u ove svrhe i trebalo bi ih izbegavati. Glavni ključ, bilo direktno ili preko jedne od njegovih izvedenih varijanti, obezbeđuje zaštitu (kroz šifrovanje) za sve ostale ključeve uskladištene u sistemu. Glavni ključ treba da bude nepromenljiv u sistemu tokom dužeg perioda, stoga se velika pažnja mora posvetiti njegovom načinu generisanja.

Potencijalno, veliki broj ključeva za šifrovanje koji bi mogli biti korišćeni u kripto sistemu povećava verovatnoću da će najmanje jedan od njih postati poznat protivniku. Stoga, procedura generisanja ključa mora biti dizajnirana tako da ako jedan ili više ključeva budu kompromitovani, proces generisanja mora biti takav da obezbedi dovoljnu zaštitu za preostale ključeve. Preporuka je da se za generisanje ključa iskoristi glavni ključ, ili jedna od njegovih varijanti, tako što se doda jedna ili više operacija upravljanja kriptografskim ključevima.

U procesu inicijalizacije bitova, za generatore pseudoslučajnih brojeva mogu se koristiti slučajni brojevi. Za kriptografske aplikacije ključno je da se generišu slučajni bitovi koji će biti nepredvidivi za protivnika čak i pri izlaganju delimičnih informacija. Dakle, potrebno je osigurati nepredvidljivost brojeva u generisanom nizu. Karakteristike ovakvih generatora se uglavnom opisuju preko dužine generisanog niza koji u sebi sadrži slučajne brojeve. Inicijalizacija ovog generisanja mora biti zasnovana na slučajnosti u smislu da se ne može odrediti u realnom vremenu.

Da bi ispitali generator slučajnih brojeva moramo ispitati generisani niz. Postoji mnogo testova, ali se na osnovu testiranja niza generisanih brojeva generator ne može proglasiti

generatorom slučajnih brojeva. Testiranjem se sa sigurnošću može utvrditi da niz generisanih bitova nije slučajan, odnosno da generator ne generiše slučajne brojeve ili u suprotnom utvrditi sličnosti sa nizom bitova generisanih pomoću idealnog generatora (npr. čovek koji baca novčić). Ako se izmerene statističke vrednosti nalaze u ekstremnim delovima krivih raspodele, možemo zaključiti da niz koji ispitujemo nije niz slučajnih brojeva.

Danas postoje različiti skupovi testova kojima se testira slučanost, poput: FIPS 140-1 testova, NIST testova, DIEHARD testova i drugih. NIST (*National Institute of Standards and Technology*) preporučuje skup testova koji su navedeni u NIST-ovoj dokumentaciji zajedno sa matematičkom pozadinom. Svi testovi se vrše nad nizom bitova ali se zaključak izveden nad tim nizom može primeniti i na generator. Uslov koji se zadaje za dužinu je 100 karaktera.

Dat je kratak opis svih 14 testova.

- *The Frequency (Monobit) Test* - je test ispitivanja frekvencije pojavljivanja jedinica i nula, ima za svrhu utvrđivanje da li dobijenom nizu egzistira približno jednak broj nula i jedinica. Ovo je jedan od osnovnih testova mada sam nije dovoljan za pokazivanje da li je niz slučajan ili nije.
- *Frequency Test within a Block* - je test ispitivanja sume jedinica u odnosnu na sumu nula u blokovima bita koji su iste dužine.
- *The Runs Test* - je test ispitivanja uzastopnih ponavljanja istih bitova u nizu, kao rezultat daje broj ponavljanja dva ili više istih brojeva zaredom.
- *Test for the Longest-Run-of-Ones in a Block* - je test ispitivanja najdužeg ponavljanja jedinica u bloku kroz poređenje sa dužinom niza za koji se zna da je slučajan.
- *The Binary Matrix Rank Test* - je test ispitivanja ranga matrica podnizova koji su u sastavu niza.
- *The Discrete Fourier Transform (Spectral) Test* - je test spektralnog ispitivanja amplituda u diskretnoj Furijeovoj transformaciji ispitivanog niza sa ciljem otkrivanja eventualnih periodičnih pojava u tom nizu koje ukazuju na odstupanje posmatranog niza od niza slučajnih bitova.

- *The Non-overlapping and Overlappin Template Matching Test* - je test ispitivanja broja ponavljanja unapred određenog uzorka generisanog niza. Kontinuitet u ponavljanju ukazuje na odstupanje posmatranog niza od niza slučajnih bitova.
- *Maurer's "Universal Statistical" Test* - je test ispitivanja broja bitova unutar uzoraka i pokazuje dokle se niz može kompresovati. Cilj je ispitati da li se posmatrani niz može značajno kompresovati bez gubitka informacija. Ukoliko je to moguće smatra se da se ne radi o slučajnom nizu.
- *The Lempel-Ziv Compression Test* - je test ispitivanja broja različitih uzoraka na osnovu čega se procenjuje da li se niz može značajnije kompresovati ili ne (da li nije slučajan ili jeste).
- *The Linear Complexity Test* - je test ispitivanja linearne složenosti.
- *The Serial Test* - je test ispitivanja preklapajućih uzoraka odnosno ispitivanje frekvencije pojavljivanja svih mogućih m-bitnih uzoraka u celom nizu.
- *The Approximate Entropy Test* - je test ispitivanja približne entropije.
- *The Cumulative Sums (Cusums) Test* - je test ispitivanja kumulativne sume i predstavlja najveće odskakanje od nule sume koja nastaje sabiranjem članova modifikovanog niza. Modifikovani niz se dobije tako što vrši zamena nula sa negativnim jedinicama
- *The Random Excursions Test* - je test koji se vrši na modifikovanom nizu. Stanje je predstavljeno sumom svih bita do trenutne pozicije. Određuje se u kojoj meri pojavljivanje stanja u jednom ciklusu, odstupa od očekivanog broja kada se poredi sa nizom za koji se smatra da je slučajan.

Pseudoslučajno generisanje bita PRBG

Pseudoslučajne bite možemo generisati tako što prvo izabere slučajna početna vrednost *s* zatim primenimo jednosmernu funkciju koja se primenjuje na nastale uzastopne sekvence. Na izlazu se zbog izbegavanja eventualne korelacije uzimaju samo neke od bitova sekvenci. Ovakav način generisanja obično se ne smatra sigurnim ali praktično jeste primenljiv.

ANSI X9.17 generator

ANSI X9.17 standard koji se koristi u DES algoritmu za trostruko šifrovanje sa dva ključa na sledeći način:

$$E(x) = E_{k1}\left(D_{k2}\left(E_{k1}(x)\right)\right)$$

Ulazni podaci generatora su: slučajni tajni 64-bitni broj s, celi broj m i DES ključ koji bi trebao da se koristi samo u ovom algoritmu, a ne i za DES šifrovanje/dešifrovanje nakon generisanja ključeva tj. inicijalnih vektora. Algoritam se odvija na sledeći način: izračuna se $I = E_k(D)$ gde je D 64-bitna reprezentacija trenutnog vremena izvrši se m sledećih ciklusa:

$$x_i = E_k(I \oplus s), \text{ odnosno}$$

$$s = E_k(x_i \oplus I)$$

Rezultat je niz x od m 64-bitnih slučajnih brojeva koji se mogu koristiti kao inicijalizacioni vektori za DES šifrovanje/dešifrovanje. Da bi se neki od brojeva $x_1 \ldots, x_m$ koristio kao ključ za DES algoritam, osmi bit treba postaviti tako da ukupan broj jedinica u x_i bude neparan.

FIPS 186 generator

FIPS 186 je generator pseudoslučajnih brojeva, upotrebljava se prilikom generisanja ključa u algoritmu DSA (*Digital Signature Algorithm*). Koristeći slučajno generisanu početnu vrednost s i jednosmernu funkciju zasnovanu na SHA-1 (algoritam A1) ili DES (algoritam A2) algoritmu, vrši se generisanje [45] . Opisaćemo prvo pomoćne algoritme zasnovane na SHA-1 i DES algoritmima.

<u>Algoritam A1</u> (koristi SHA-1):

ULAZ: 160-bitni string t i b-bitni string c takvi da je b dužine od 160 do 512

IZLAZ: G(t,c) koji je dužina 160 bita

podeliti t na pet 32-bitnih blokova $t=H_1 \| H_2 \| H_3 \| H_4 \| H_5$

dopuniti c sa nulama tako da bude dužine 512 bita, čime se dobije X $X=c \| 0^{512-b}$

podeliti X na 16 reči $x_0, \ldots, x_{15}$ dužine 32 bita

primeniti SHA-1 algoritam na x_0, ..., x_{15} i H_1,H_2,H_3,H_4,H_5

Algoritam A2 (koristi DES):

ULAZ: 160-bitni stringovi t i c

IZLAZ: 160-bitni string G(t,c)

t se podeli na pet 32-bitnih blokova

c se podeli pet 32-bitnih blokova

$x_0=t_0 \oplus c_0$, $x_1=t_1 \oplus c_1$, $x_2=t_2 \oplus c_2$, $x_3=t_3 \oplus c_3$, $x_4=t_4 \oplus c_4$

u četiri ciklusa (i=0,4) uraditi sledeće:

$$b_1 = c_{(i+4) \bmod 5}, b_2 = c_{(i+3) \bmod 5}$$

$$a_1 = x_1;\ a_2 = x_{(i+1) \bmod 5} \oplus x_{(i+4) \bmod 5}$$

$$A = a1 \| a2, B = msb24(b1) \| b2$$

- primeniti DES sa ključem B za šifrovanje A tj. $y_i=DES_B(A)$

- podeliti y_i na dva 32-bitna bloka $y_i = L_i \| R_i$

u četiri ciklusa (i=0,4) uraditi sledeće: $y_i=L_i \oplus R_{(i+2) \bmod 5} \oplus L_{(i+3) \bmod 5}$

FIPS 186 algoritam

Ulaz za ovaj algoritam su: celi broj m i 160-bitni prost broj q.

Izlaz je m pseudoslučajnih brojeva $a_1,a_2,...a_m$ iz intervala [0,q-1] koji mogu biti upotrebljeni kao privatni ključevi za DSA algoritam ako se koristi A1 odabrati proizvoljan broj $160 \leq b \leq 512$, a ukoliko se koristi A2 onda uzeti b=160 generisati slučajnu i tajnu b-bitnu inicijalnu vrednost s neka je t string dužine 160 bita, u m ciklusa (i=1,m) uraditi sledeće: - ili omogućiti korisniku da unese b-bitni string y_i ili uzeti $y_i=0$ - $z_i=(s+y_i) \bmod 2^b$ - $a_i=G(t, y_i) \bmod q$ gde je G algoritam definisan u A1 ili A2 - $s=(1 + s + a_i) \bmod 2^b$ rezultat je niz brojeva $a_1,a_2,...a_m$

Kriptografski sigurno pseudoslučajno generisanje bita CSPRBG

Kao što je već rečeno CSPRBG (engl. *Cryptographically secure pseudorandom number generator*) generatori su znatno sporiji od PRBG generatora, a uzrok tome je modularno množenje koje koriste ovi generatori.

RSA generator - rezultat RSA generatora je pseudoslučajna sekvenca bita $z_1,z_2,...z_l$.

Generisanje sekvence se odvija na sledeći način [46]:

generisati dva prosta broja p i q i izračunati $n = p \cdot q, \phi = (p-1) \cdot (q-1)$

izabrati slučajan broj e takav da je $1 < e < \phi$ i da je NZD$(e, \phi) = 1$

izabrati slučajan broj x_0 iz intervala $[1, n-1]$

u ℓ ciklusa (i=1, ℓ) uraditi sledeće:

$x_i = x_{i-1}{}^e mod n$

z_i=lsb(x_i) najmanje značajnih bita od x_i

rezultat je sekvenca bita $z_1 \dots z_\ell$

Micali-Schnorr generator - predstavlja modifikovani RSA generator. Ovim modifikacijama postižu se bolje performanse u odnosu na RSA generator. Rezultat je pseudoslučajna sekvenca bita $z_1,z_2,...z_l$, a generisanje sekvence se odvija na sledeći način [47]:

generisati dva prosta broja p i q, pa izračunati $n = p \cdot q, \phi = (p-1) \cdot (q-1)$

neka je $N = [\log_2 n] + 1$ bitska dužina od n

izabrati slučajan broj e takav da je $1 < e < \phi$ i da je NZD$(e, \phi) = 1, 80e \leq N$

neka je $k = \left\lceil N\left(1 - \frac{2}{e}\right)\right\rceil$ i $r = N - k$

odabrati slučajnu početnu sekvencu x_0 bitske dužine r

u ℓ ciklusa (i=1, ℓ) uraditi sledeće:

$$y_i = x_{i-1}^e mod \text{ n}$$

$$x_i = MSB_r(y_i)$$

$$z_i = LSB_k(y_i)$$

Gde su r i k bitovi od niza y_i

Blum Blum Shub generator - Ovaj generator je poznat još pod nazivima x^2 generator ili BBS generator. Generisanje sekvence bita $z_1,z_2,...z_l$ se odvija na sledeći način:

generisati dva velika tajna broja p i q (takvi da daju ostatak 3 pri deljenju sa 4)

$n = p \cdot q$

iz intervala [1,n−1] bira se slučajan broj s, takav da je NZD(s,n)=1; $x_0=s^2$ mod n

u ℓ ciklusa (i=1, ℓ) se generiše sekvenca bita z_i na sledeći način: $x_i = x_{i-1}^2 mod$ n,

odnosno $z_i = LSB(x_i)$

3.4.1. Životni vek ključeva

Generisanje ključa je pred faza u životnom veku ključa. U ovoj fazi zaključujemo da je pored korišćenja ključa za kriptografsku obradu (npr. šifrovanje ili proveru autentičnosti) podataka, bitnije koristiti ga kao glavni ključ za izvođenje podključeva a nakon toga koristiti podključeve za stvarnu kriptografsku obradu. Ova popularna paradigma se zove ponovno ključanje (engl. *re-keying*) i pokazala se dobra s aspekta bezbednosti, efektivno produžavajući životni vek glavnog ključa i donoseći značajne, dokazive koristi u bezbednosti u praktičnim situacijama. Sigurnost koju pružaju različiti procesi ponovnog ključa se kvantifikuju kroz funkciju bezbednosti primitiva. Na ovaj način se postiže mogućnost izbora u različitim procesima generisanja ponovnog ključa s obzirom na ograničenja aplikacija za generisanje.

Faze u životnom ciklusu ključeva su:

- generisanje ključeva. Ova faza se u pojedinoj literaturi navodi i kao pred faza;
- distribucija ključeva;

- opoziv ključeva;
- kraj validnosti ključeva, uništavanje ključeva i eventualno arhiviranje.

Kada se ključevi formiraju oni se pakuju, obeležavaju, dodaje im se heš ili RSA digitalni potpis (očuvanje integriteta). Kod distribucije ključeva mora se voditi računa o tome da li su ključevi simetrični, tajni ili javni. Simetrični ključevi se ne mogu distribuirati istim komunikacionim kanalom kojim se šalje šifrat. Ne smeju se ni čuvati zajedno sa otvorenim tekstom ili šifrovanim tekstom. Kod simetričnih ključeva može se dodati heš zbog sažimanja, privatni i javni ključevi se obavezno potpisuju sa RSA digitalnim potpisom.

3.4.2. Generisanje ključeva – matematičke osnove

Za generisanje: simetričnih ključeva, RSA prostih brojeva, D-H tajne vrednosti i dr. neophodno je koristiti slučajne brojeve. Kriptografski slučajni brojevi moraju biti statistički slučajni i nepredvidivi. Pseudoslučajni brojevi su prediktabilni, samo je pitanje koliko od izlaznog niza moramo poznavati da bi smo otkrili celokupni mehanizam generisanja. Za razliku od pseudoslučajnih, kriptološki nizovi nisu jednostavno prediktabilni.

Nizovi "istinski" slučajnih brojeva dobijaju se praćenjem prirodnih pojava čiji je ishod nepredvidiv kao što su, na primer, bacanje novčića, igre kartama, bacanje kockica, rulet, odvajanje štapića. Ovakvi nizovi brojeva ne prate nikakve obrasce i potpuno su nasumični. Mada su ovi nizovi jedini zaista slučajni, metodi kojima se oni dobijaju su previše spori za potrebe statistike i kriptografije.

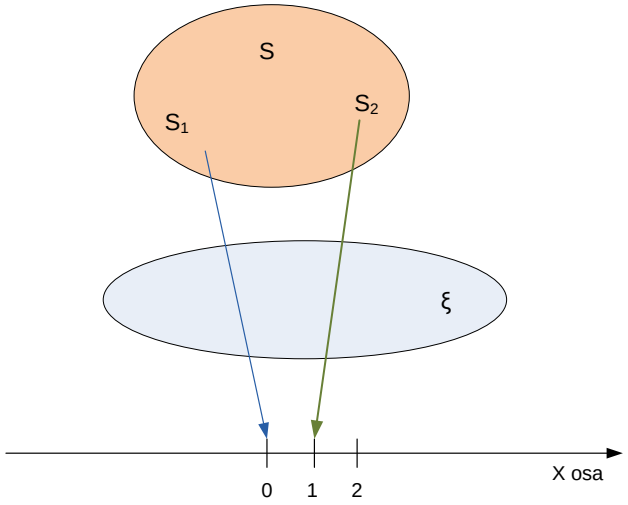
Druge pojave koje se posmatraju su svi fenomeni koji se pokoravaju zakonima kvantne mehanike, radioaktivno raspadanje, buka. Na primer, ispuštena kocka sigurno će pasti, ali na koju od šest strana , nemoguće je predvideti, stoga sledi, da je pad kocke na pojedinu stranu posledica slučaja. Nije nam poznat uzrok koji u datom momentu dovodi do pada kocke na određenu stranu, a kako uzrok, dakle nije poznat , nije moguće niti delovati na proces u smislu ostvarenja jednog od mogućih događaja. Posmatranje takvih " slučajnih " događaja ostvarenih pri velikom broju ponovljenih uslova njihove realizacije, ukazuje na činjenicu: iako ne postoji mogućnost

predviđanja u kojem smislu i u kolikoj će meri delovati slučaj u konkretnom primeru, ipak se delovanje slučaja pokorava određenim zakonitostima, koji vrede za skup događaja kao celina. Proučavanje zakona koji vladaju između slučajnih događaja kao celine vršimo pomoću matematičke obrade podataka. Podatke dobijamo merenjem masovnih pojava (npr. rođenje dečaka ili devojčića, pad novčića na " grb" ...).

3.4.2.1. Matematičko predstavljanje

Sa matematičke tačke gledišta je poželjno da se svakom mogućem ishodu nekog eksperimenta pridruži neki odgovarajući broj. Ovo se postiže uvođenjem slučajne promenljiva. Slučajna promenljiva se dakle, definiše kao funkcija koja preslikava prostor događaja S na realnu osu x. Pri tome je moguće da se više od jedne tačke iz S preslikava u jednu vrednost slučajne promenljive, ali svaka tačka u S mora odgovarati samo jednoj vrednosti slučajne promenljive ξ [32].

Najčešće viđen primer u literaturi je eksperiment bacanja novčića gde kao moguće ishode imamo dve strane novčića: pismo i glava. Ova dva ishoda se matematički mogu predstavljaju s_1 i s_2 respektivno. Skup svih ishoda eksperimenta, definiše se kao prostor događaja i matematički se definiše $S = \{s_1, s_2\}$. Za moguće ishode definišu se vrednosti slučajnih promenljivih $\xi(s_1) = 1;\ \xi(s_2) = 0.$ ξ preslikava prostor događaja S u tačke 0 i 1 na x osi što je prikazano na slici 3 - 10.



Slika 3-10 Predstavljanje slučajnih promenljivih

Vrednost 0 i 1 predstavljaju rang slučajne promenljive ξ, u literaturi se može susresti i pojam opseg odnosno domen.

Slučajna promenljiva predstavljena kroz primer bacanja novčića je diskretna promenljiva, jer u konačnom intervalu uzima samo pojedinačne, diskretne vrednosti. Osobina diskretne slučajne promenljive je da uzima vrednosti iz prebrojivog skupa ishoda koji se preslikava u prebrojiv skup verovatnoća. Slučajna promenljiva može biti kontinualna, takva promenljiva uvek ima definisanu vrednost u posmatranom intervalu na x osi. Kontinualna slučajna promenljiva ima osobinu da se na neprebrojivom skupu ishoda preslikava u funkciju definisanu na beskonačnom domenu.

Prostor događaja predstavljena kroz primer bacanja novčića S, takođe je diskretan. Međutim, u opštem slučaju prostor događaja za diskretnu promenljivu može biti i kontinualan i mešovit. Za kontinualnu promenljivu, prostor događaja mora biti kontinualan jer svaka tačka u prostoru S mora odgovarati samo jednoj vrednosti slučajne promenljive.

3.4.2.2. Funkcija raspodele verovatnoće

Da bi se promenljiva opisala, pored poznavanja vrednosti, potrebno je znati koliko često, odnosno sa kojom verovatnoćom se pojavljuju te vrednosti. Zakonom raspodele se naziva bilo

koje pravilo koje omogućuje da se nađu verovatnoće svih mogućih događaja vezanih za tu slučajnu promenljivu.

Najprostiji zakon raspodele je tzv. funkcija raspodele verovatnoće ili kraće funkcija raspodele. Neka je data slučajna promenljiva ξ i proizvoljni realni broj x. Verovatnoća da slučajna promenljiva uzme vrednosti manje od x, naziva se funkcija raspodele [32], matematičko predstavljanje date funkcije je $P_\xi(x)=p(\xi \le x)$. Argument x je bilo koji broj u opsegu $(-\infty, +\infty)$.

Funkcija raspodele ima sledeće osobine:

1. $0 \le P_\xi(x) \le 1$
2. $P_\xi(-\infty)=0;\ P_\xi(\infty)=1$
3. $P_\xi(x_1) \le P_\xi(x_2)$, за $x_1<x$
4. $p(x_1< \xi \le x_2) = P_\xi(x_2)- P_\xi(x_1)$
5. $P_\xi(x^+) = P_\xi(x)$.

Prva osobina se odnosi na verovatnoću funkcije P_ξ. Sledeća osobina sledi iz činjenice da $P_\xi(-\infty)$ uključuje nemoguće događaje, dok $P_\xi(\infty)$ uključuje sve moguće događaje. Treća osobina pokazuje da je funkcija raspodele neopadajuća. Četvrta kaže da su događaji međusobno isključivi pa se verovatnoća može izraziti i kao suma . Poslednja osobina pokazuje da je funkcija raspodele kontinualna funkcija s desna (oznaka (x^+) predstavlja $(x+\xi)$,gde je $\xi>0$ i $\xi \to 0$) . Druga, treća i četvrta osobina služe za testiranje da li je neka funkcija od x funkcija raspodele neke slučajne promenljive i ako jeste sva tri uslova moraju biti ispunjena.

Funkcija raspodele diskretne slučajne promenljive ima stepenasti oblik

$$p\xi(x) = \sum_{i=1}^{N} P\{\xi = xi\}u(x - xi) = \sum_{i=1}^{N} P(xi)u(x - xi)$$

gde u(x) predstavlja jediničnu step funkciju definisanu kao u(x)={0, za $x\le1$; 1, za $x\ge0$ }, a N predstavlja ukupan broj mogućih vrednosti x_i , koji može biti i beskonačan. Amplituda stepa u nekoj tački x_i odgovara $P(x_i)$.

Slučajna promenljiva ima samo dve moguće vrednosti: 0 i 1. Verovatnoća pojave 0 jednaka je q, a verovatnoća pojave 1 jednaka je p.

- Za x≥1 događaj { ξ ≤x} siguran je događaj, pa je P { ξ ≤x }=1.
- Za 0≤x<1 verovatnoća događaja { ξ ≤x } odgovara verovatnoći događaja { ξ =0}, odatle je P { ξ ≤x }= P (ξ=0)=q.
- Za x<0 događaj {ξ ≤x} je nemoguć, pa je P { ξ ≤x }=0.

Dakle, $P_{\xi}(x)$= {1 za x≥1; q za 0≤x<1 ;0 za x<0}.

3.4.2.3. Jednosmerne funkcije

Ukoliko bi smo imali dva proizvoljna skupa O i S , preslikavanje, uz određenu zakonitost, pomoću koje se proizvoljnom elementu skupa O dodeljuje neki element iz skupa S predstavlja funkciju. Element iz skupa O se naziva original dok se njegov dodeljen element iz skupa S naziva Slika. Ukoliko neka funkcija F ima svoju Inverznu funkciju f^{-1}, to znači da postoji inverzno preslikavanje elemenata.

Funkcije kod kojih je moguće inverzno preslikavanje imaju sledeće osobine:

- Preslikavanje mora biti obostrano jednoznačno što znači da svakom elementu iz O skupa odgovara tačno jedan element iz S skupa

$$(\forall x_{1,} x_2 \in O)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$$

- Funkcije kod kojih je ispunjen uslov ovako definisanog preslikavanja se nazivaju injektivne funkcije.
- Preslikavanje mora biti i NA što znači da za svaki element iz skupa S dakle $y \in S$, postoji jedan element u skupu O, dakle $x \in O$, za koji važi $f(x) = y$.

$$(\forall y \in S)(\exists x \in O)(f(x) = y)$$

- Funkcije je surjektivna ako svi elementi kodomena f imaju svoj original u domenu f.

- Ukoliko je funkcija f funkcija koja je i injektivna i surjektivna, onda je kod ovakve funkcije ispunjeno bijektivno preslikavanje.
- Ako je f preslikavanja elemenata iz skupa O u skup S bijektivno preslikavanje , onda sa f^{-1}označavamo preslikavanje elemenata iz skupa S u skup O.

U ovakvom preslikavanju, ukoliko je ispunjen uslov $f^{-1} \circ f = f \circ f^{-1} = i_o$, gde sa i_o predstavlja preslikavanja skupa O na sebe. Pod ovako ispunjenim uslovima u procesu preslikavanja, f^{-1} nazivamo inverznim preslikavanjem. Ukoliko kao rezultat preslikavanja dobijamo novu funkciju tu funkciju nazivamo inverzna funkcije

Jedna od osnovnih definicija jednosmernih funkcija glasi: Funkcije kod koji se ne može na jednostavan i lak način iz inverzne funkcije odrediti osnovni oblik funkcije, dok je sa druge strane, način izračunavanja inverzne funkcije veoma jednostavan.

Da bi se formalizovala definicija, potrebno je prvo definisati pojam zanemarljive funkcije koju ćemo zvati $\in$. Funkcija $\in: N \to [0,1]$ je zanemarljiva ako za svaku konstantu c postoji n_0 takvo da je $\in(n) \leq \frac{1}{n^c}$ za svako $n \geq n_0$, ovakva funkcija monotono opada mnogo pre nego polinomska funkcija, takođe ovo je funkcija za koju važi da $\lim_{n\to\infty} \in(n) = 0$.

Dakle ako imamo injektivnu funkciju, ta funkcija je jednosmerna, ako zadovoljava sledeće uslove:

- Funkcija koja se u konačnom vremenu može izračunati.
- Funkcija za koju je teško u konačnom vremenu odrediti inverznu funkciju. Za svaki probabilistički polinomski algoritam $Pr[A(f(x)) = x]$, postoji zanemarljiva funkcija $\in$ takva da $Pr[A(f(x)) = x] \leq \in(n)$, pri čemu se verovatnoća odnosi na slučajni izbor ulaza x dužine n na uniformni način i slučajne izbore algoritma A.

Radi jednostavnosti, data je definicija jednosmerne funkcije samo ako je funkcija injektivna. Bez ispunjenog uslova da je funkcija injektivna , definiciju treba da se prilagodi problemu nalaženja nekog originala za $f(x)$, odnosno definisati da verovatnoća da $A(f(x)) \in f^{-1}(f(x))$

bude zanemarljiva. Dodatno, iz tehničkih razloga definisanja algoritma A, treba ograničiti da $f(x)$ ne smanjuje previše svoj ulaz, odnosno da su dužina $|f(k)|$ i dužina $|k|$ povezani polinomom (u oba smera.)

Ulazna dužina n se može smatrati odgovarajućom kao dužina ključa u kriptografskom protokolu u okviru funkcije f . Pod pretpostavkom da je f jednosmerna funkcija , očekuje se da dovoljno dugačko n otežava i proces izračunavanja inverzne funkcije od izračunavanja same funkcije. Dakle, kako bi se znalo kolika je dužina ulaznog n, potrebno je znati konkretan algoritam čija je maksimalna verovatnoća uspeha ∈ definisana za algoritam A određena vremenom izvršenja, dužinom n i matematičkog modela koji se implementira.

Primeri jednosmernih funkcija

Funkcije kojima se najčešće objašnjava pojam i definicije jednosmernih funkcija su navedene u nastavku:

- Množenje $f(p,k) = p \cdot k$, gde su p, k prosti brojevi jednake dužine. Dakle jednostavno je i vremenski ograničeno odrediti proizvod dva prosta broja jednakih dužina. Izračunavanje inverzne funkcije je u stvari rastavljanje na proste činioce, matematički definisan pojam
- Faktorizacije elemenata. Ono što je bitno da sam proces faktorizacije se razlikuje od vrste proizvoda, brojevi se dele sa najmanjim prostim brojem sa kojim je proizvod deljiv , proces se ponavlja dok se ne dobiju svi prosti brojevi i nakon toga se definišu brojevi od kojih je nastao traženi proizvod. Polinomi se faktorizuju ili deljenjem sa linearnim polinom ili izvlačenjem zajedničkog sadržalaca. Uočava se da je jako teško, gotovo nemoguće uraditi faktorizaciju povećanjem dužine prostih brojeva, ili korišćenjem složenih polinoma.
- Zbir podskupa $f(x_1, \ldots . x_n, S) = (x_1, \ldots . x_n, \sum_{i \epsilon S} x_i)$. Ovde je svako x_i n-bitni ceo broj i broj $S \subseteq [n]$. Izračunavanje inverzne funkcije je problem zbira podskupa koji se opisuje kao nalaženje nepraznog podskupa čiji je zbir elemenata nula u okviru skupa celih brojeva. Načini za rešavanje problema zbira podksupa su različiti, neki od njih

su: Naivni algoritmi, algoritmi aproksimacije u polinomijalno vreme, dinamičko programiranje i drugi.

- Diskretni logaritmi $f_{G,g}(x) = g^x$, ova funkcija je definisana na skupu celih brojeva i ona može i ne mora da ima rešenje. Ako je G konačna ciklična grupa reda n, za diskretni logaritam $\log_g G$ dobija se jedinstveni celi broj x, takav da je $0 \leq x \leq n-1$. Uočava se da u konačnom skupu G reda n lako možemo izračunati funkciju , dok je pronaći x kojim treba stepenovati g teško.
- RSA Algoritmi , koriste se veliki prosti brojevi istih dužina p i q nad kojim se primenjuju određene matematičke operacije te se sama sigurnost RSA zasniva se na složenosti faktorizacije velikih brojeva. Predlaže se i da se u izboru para ključeva koriste jaki prosti brojevi p i q za generisanje n. Jaki prosti brojevi imaju određene osobine koje čine proizvod n teško faktorizovanim. Razlog za ovakav izbor je to što su neke od metoda faktorizacije, kao što su Polardove $(p-1)\cdot(p+1)$ metode, naročito pogodne za proste brojeve p za koje $(p-1)$ili $(p+1)$ imaju samo male proste faktore. Jaki prosti brojevi su otporni na ovakve napade. Računa se $n = p \cdot q$ i Ojlerova funkciju $\phi(n) = (p-1)\cdot(q-1)$. Zatim se bira celobrojna vrednost c takva da je $1 < c < \phi(n)$, zatim se računa r po formuli $r \cdot c \equiv mod\ \phi(n)$ Javni ključ je uređeni par (n, c) a privatni ključ je par (n, r).
- Rabinova šema za generisanje digitalnog potpisa $f_{n,e}(x) \equiv x^2 mod\ n$, gde je n proizvod dva prosta broja i $x \in \sum_i^n Z$. Računanje inverzne funkcije se i u ovom slučaju svodi na faktorizaciju.
- Heš funkcija ili algoritam je svaki algoritam koji ulazni podatak proizvoljne dužine transformiše u izlazni podatak fiksne dužine, na ovaj način dobijamo heš vrednost. U samoj definiciji se vidi analogija sa definicijom jednosmernih funkcija.

Može se zaključiti da su jednosmerne funkcije sastavni deo:

- Definisanja sigurnosnih kanala komunikacije;
- Definisanja generatora pseudoslučajnih brojeva;

- Definisanja pseudoslučajnih funkcija;
- Realizacije simetričnih kriptosistema;
- Realizacije šema digitalnog potpisa.

Za neke zadatke u kriptografija, pre svega šifrovanje sa javnim ključem, jednosmerne funkcije obično nisu dovoljne već je potrebno koristiti i neko njihovo dodatno svojstvo na ovome se zasnivaju takozvane *Trapdoor* funkcije. Ovakve funkcije se lako mogu invertovati i lako se može izračunati početna funkcija ako se zna određena osobina koja ujedno predstavlja i prečicu za izračunavanje. Primeri ovakvih funkcija su RSA algoritam i Rabinova šema generisanja.

3.4.2.4. Entropija informacije

Entropiju informacija (informacionu teorijsku entropiju) je prvi uveo Šenon 1948. godine [31]. Ona se može se pripisati slučajnoj promenljivoj kao prosečan nivo samoinformacije u svakom mogućem događaju promenljive, što pokazuje nužni nivo neizvesnosti ili iznenađenja u događaju. U Šenonovoj teoriji, za slučajnu promenljivu x, samoinformacija I_X događaja sa verovatnoćom $P_X(x_i)$ je definisana kao:

$$I_X(x_i) = -\log_b P_X(x_i)$$

U navedenoj jednačini baza logaritma određuje jedinicu informacije. Konkretno, ako je b=2, tada se $I_X(x_i)$ izračunava u bitovima. Entropija $H(X)$ je definisana kao:

$$H(X) = E[I_X] = \sum_I P_X(X_I) I_X(X_I) = \sum_i -P_X(x_i) \log_b P_X(x_i)$$

U navedenoj jednačini, $E[I_X]$ je matematičko očekivanje od I_X . Fon Nojman je predložio naziv "entropija" za koncept koji je uveo Šenon zbog njegove sličnosti sa termodinamičkom entropijom u pojmu, kao i srodnim jednačinama. U stvari, informaciono-teorijska entropija se koristi kao mera slučajnosti, nereda i nedostupnih informacija, kao što je slučaj termodinamičke entropije. Šenon je raspravljao o ulozi entropije i srodnim konceptima u modeliranju kriptosistema.

Dostupni su razni naučni radovi koji se bave ulogom entropije u dizajnu, implementaciji i analizi kriptosistema, kao i kriptografskih aplikacija, okruženja i drugih. Na primer, ulogu entropije u izračunavanju donjih granica veličine ključa, kao i odnos između entropije i savršene tajnosti proučavao je *Maurer* [48]. Štaviše, *Reyzin* je predstavio kratak uvod u neke pojmove u vezi sa entropijom u kriptosistemima [49]. Odnos između entropije i prave slučajnosti, kao i ključne nepredvidljivosti, proučavali su *Vassilev* i *Hall* [50] .

„Information is the resolution of uncertainty. „

Claude Shannon

4. Pojam i definicije biometrije

U ovom poglavlju prikazaće se osnovni pojmovi u oblasti biometrije. Definisaće se i biometrijska provera identiteta kroz postupke prikupljanja određenih karakteristika zatim njihove analize. Pokazaće se kako se vrši odabir karakteristika za koje vazi da se teško mogu oponašati odnosno da skoro jednoznačno identifikuju osobu.

Zatim će se definisati biometrijski uzorak, kroz načine njihovih prikupljanja uz pomoć specijalnih uređaja, proces digitalizacije kao i dalje softverske obrade. Na osnovu navedenog, definisaće se biometrijski sistemi za autentifikaciju zatim sistemi za generisanje kriptoloških ključeva, a sve u cilju podizanja bezbednosti i zaštite identiteta osobe.

Primena različitih strategija fuzije za kombinovanje više biometrijskih izvora. Principi donošenja odluke u slučaju primene u servisima autentifikacije.

Biometrija se odnosi na merenje jedinstvene lične karakteristike pojedinca a sve sa ciljem da se identifikuje i to sa visokim stepenom sigurnosti, čime se obezbeđuje osnova za poverenje. Na osnovu toga da li se biometrija primenjuje na karakteristike korisnika ili na njegovo ponašanje definišu se i različiti tipovi na kojima biometrije zasniva, a to su :

- na fizičkim karakteristikama i
- na karakteristikama ponašanja.

U skladu sa vrstama korišćenja biometrije definišu se i različiti oblici biometrijskih sistema. Ukoliko sistem koristi jednu od biometrijskih karakteristika osobe, takav se sistem u literaturi definiše kao unimodalni biometrijski sistem, ukoliko sistem kombinuje dve ili više biometrijske karakteristike onda se on definiše kao višemodalni biometrijski sistem.

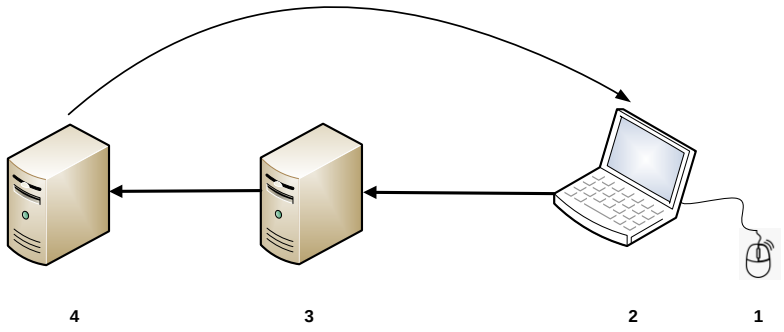
4.1. Biometrija zasnovana na fizičkim karakteristikama

Ukoliko se govori o provera identiteta uz pomoć biometrije, u dostupnoj naučnoj literaturi, proces predstavlja prikupljanje i analizu fizičkih karakteristika. Tako prikupljeni podaci postaju biometrijski uzorci oni identifikuju osobu jednoznačno. Proces postanka uzorka predstavlja digitalizaciju karakteristika da bi se dalje mogle matematički obrađivati. Ukoliko koristimo biometrijske uzorke najčešće se to radi u biometrijskim sistemima. Ovakvi sistemi, kao i svi drugi imaju zadatak da ulazne podatke obrade na određen način kako bi se generisao izlazni podatak. Shodno ulaznim podacima, definiše se i namena ovakvih sistema u domenu zaštite .

4.1.1. Autentifikacija uz pomoć otiska prsta

Istorijski gledano, u primenama za sprovođenje zakona, dobijanje slika otiska prsta je vršeno korišćenjem takozvane „tehnike mastila“: prsti subjekta su premazani crnim mastilom i pritisnuti ili umotani na papirnu karticu; kartica je zatim skenirana korišćenjem skenera opšte namene, stvarajući digitalnu sliku. Danas, se radi takozvano skeniranje, gde se otisak dobija uz pomoć elektronskog skenera otiska prsta (koji se naziva i čitač otiska prsta).

Opšta struktura tipičnog skenera otiska prsta realizovana je kroz senzor koji očitava šaru na površini prsta i pretvara analogno očitavanje u digitalni oblik preko A/D (analogno digitalnog) pretvarača; interfejs modul je odgovoran za komunikaciju (slanje slika, prijem komandi, itd.) sa spoljnim uređajima (npr. personalni računar). Otisak prsta je ono što je za svakog pojedinca jedinstveno, takođe, nastaje i pre rođenja [51].



Slika 4-1 Jedno rešenje za proveru korisnika

Na slici je prikazano jedno od mogućih rešenja za proveru korisnika, ovo rešenje se može primeniti prilikom izrade određenih aktivnosti. Bez prisustva (3) servera za biometrijsku proveru , korisniku (2) se proverava identitet prilikom pristupa (4) serveru na kome je smešten sistem za elektronsko učenje i dokle god traje sesija ne vrši se provera. Provera je obično sastavljena od unosa tačnog korisničkog imena i lozinke. Uz primenu (1) provera se može vršiti periodično u toku trajanja sesije [52].

Osnovni koraci biometrijskih potvrda identiteta otiskom prsta su uobičajeni za većinu web aplikacija i mogu se grupisati na sledeći način [53]. Kreiranje korisničkog imena i lozinke za svakog korisnika, skeniranje palca svakog korisnika i njihovo skladištenje u sigurnom serveru.

- Prijavljivanje korisnika na sajt koristeći definisano korisničko ime i lozinku.
- U slučaju pristupa osetljivim podacima, skenira se otisak palca na osnovu poklapanja otiska omogućava se pristup podacima.
- Ukoliko se ne pokaže poklapanje, korisnik neće moći da pristupi osetljivim podacima.

Analiza biometrijske metode kroz ocenu ispunjenosti aspekata

- Jedinstvenost: visok stepen ispunjenosti
- Trajnost: visok stepen ispunjenosti
- Prikupljivost: srednji stepen ispunjenosti
- Izvodljivost: visok stepen ispunjenosti
- Prihvatljivost: srednji stepen ispunjenosti

Provera autentičnosti zasnovana na biometriji može da pruži snažnu bezbednosnu garanciju o identitetu korisnika. Bezbednost biometrijskih podataka je posebno važna obzirom da ako se jednom podaci kompromituju ostaju kompromitovani trajno. Prilikom upotrebe biometrije sledeće činjenice moramo imati u vidu:

- Biometrija je autentična, ali nije tajna: Za razliku od lozinki i kriptografskih ključeva koji su poznati samo korisniku, biometrija kao što su glas, lice, potpis, pa čak i otisci

prstiju mogu se lako snimiti i potencijalno zloupotrebiti bez pristanka korisnika. Biometrija lica i glasa je na sličan način podložna snimanju bez eksplicitnog znanja korisnika. Nasuprot tome, korisnik mora voljno da deli tokene i znanje da bi bili kompromitovani.

- Biometrijski podaci se ne mogu opozvati ili otkazati: lozinke, PIN-ovi, itd., mogu se resetovati ako su ugroženi. Tokeni kao što su kreditne kartice i značke mogu se zameniti ako su ukradeni. Međutim, biometrija je trajno povezana sa korisnikom i ne može se opozvati ili zameniti ako je ugrožena. Iako korisnik može sukcesivno da registruje različite otiske prstiju opet je ograničen brojem svojih prstiju. Ovaj izbor ne postoji za druge biometrijske modalitete.
- Ako se biometrija jednom izgubi, ona je zauvek ugrožena: biometrija pruža prednosti upotrebljivosti jer otklanja potrebu za pamćenjem i upravljanjem više lozinki/identiteta. Međutim, ovo takođe znači da ako je biometrija ugrožena u jednoj aplikaciji, u suštini sve aplikacije u kojima se koristi određena biometrija su ugrožene.
- Unakrsno uparivanje se može koristiti za praćenje pojedinaca bez njihovog pristanka: Pošto se ista biometrija može koristiti za različite aplikacije i lokacije, korisnik se potencijalno može pratiti ako se organizacije dogovaraju i dele svoje odgovarajuće baze biometrijskih podataka. Sa tradicionalnim šemama autentifikacije, korisnik može da održava različite identitete/lozinke da bi to sprečio. Činjenica da biometrija ostaje ista predstavlja zabrinutost za privatnost.

Uočava se da „anonimna biometrija“ kao tehnologija treba da se koristi u cilju poboljšanja privatnosti. Tehnike koje mogu da ispune ove zahteve nazivaju se i poništava biometrija.

Neinvertibilne (poništive) transformacije su jedno od rešenja biometrijske autentifikacije koja čuvaju privatnost. Umesto čuvanja originalne biometrije, ona se transformiše korišćenjem određene jednosmerne funkcije. Transformisana biometrija i transformacija se čuvaju ili na pametnoj kartici ili centralno u bazi podataka. Kako primenom jednosmernih funkcija u procesu transformacije dovode do generisanja novog podatka (konstrukta) za koji važi da čuva privatnost jer neće biti moguće (ili računarski veoma teško) povratiti originalni biometrijski šablon koristeći

tako transformisanu verziju. Ako je biometrija ugrožena, može se jednostavno ponovo upisati koristeći drugu funkciju transformacije, čime se obezbeđuje opoziv. Konstrukt takođe sprečava unakrsno podudaranje između baza podataka, pošto svaka aplikacija koja koristi istu biometriju koristi drugačiju transformaciju. Još jedna prednost ovog pristupa je što se reprezentacija obeležja ne menja (i u transformaciji domena signala i u domenu obeležja). Ovo omogućava korišćenje postojećih algoritama za ekstrakciju karakteristika i uparivanje. Štaviše, pristup je kompatibilan sa prethodnim instalacijama za biometrijsku autentifikaciju.

4.1.1.1. Poništivi šabloni za biometriju otiska prsta

Tehnike za dizajniranje poništivih šablona za biometriju otiska prsta, funkcionišu tako što uz pomoć jednosmernih funkcija transformišu originalne karakteristike, lokacije i orijentacije otiska i dobija se potpuno novi podatak za koji važi pravilo jednosmernih funkcija a to je da je gotovo nemoguće povratiti izvorni podatak .

Algoritam koji poredi dve biometrije x_1 i x_2 daje rezultat podudarnosti ili sličnosti u opsegu $0 \leq \mu(x_1, x_2) \leq 1$, u skladu sa tim postoji nekoliko faktora koje treba uzeti u obzir prilikom dizajniranja poništive transformacije čiji je zadatak da transformiše biometriju x_1 u biometrijski poništivi šablon $\mathrm{C}(x_1)$ [54]. Karakteristike takvog algoritma se ogledaju u sledećim fazama:

1. Registracija- Da bi poništiva transformacija C bila ponovljiva od jedne instance y_1 biometrije u sledeću instancu y_2 iste biometrije, biometrijski signali y_1 i y_2 moraju svaki put biti pozicionirani u istom koordinatnom sistemu. Za otiske prstiju, to znači da i y_1 i y_2 moraju prvo da se rotiraju i prevedu pomoću koordinatne transformacije T_1 i T_2, respektivno, tako da se signali $x_1 = T_1(y_1)$ i $x_2 = T_2(y_2)$ preklapaju. Dakle, potrebno je da se, pre poništive transformacije C, otisci y_1 i y_2 registruju tako da se odgovarajuće minucije podudaraju što je moguće bolje.
2. Tolerancija varijabilnosti unutar korisnika - Još jedan problem sa kojim se treba boriti, čak i nakon registracije, je varijabilnost unutar korisnika koja je prisutna u biometrijskim signalima. Karakteristike dobijene nakon transformacije treba da budu robusne u odnosu na ovu varijaciju, tako da verovatnoća lažnog odbijanja idealno ne bi trebalo da se

povećava u transformisanom domenu, tj. kada se x_1 i x_2 poklapaju $\mu(x_1, x_2) > t \Longrightarrow \mu\big(\mathrm{C}(x_1), \mathrm{C}(x_2)\big) > t$

3. Zadržavanje entropije - Transformisana verzija ne bi trebalo da izgubi bilo kakvu individualnost. Unutrašnja snaga transformisane biometrije $\mathrm{C}(x)$ treba da bude uporediva sa originalnom biometrijom x, odnosno verovatnoća lažnog prihvatanja ne bi trebalo da se povećava u transformisanom domenu. U idealnom slučaju, trebalo bi da imamo, ako se x_1 i x_2 ne poklapaju, $\mu(x_1, x_2) \leq t \Longrightarrow \mu\big(\mathrm{C}(x_1), \mathrm{C}(x_2)\big) \leq t$, gde je t prag odluke.
4. Dizajn funkcije transformacije - Transformacija C mora dalje da zadovolji sledeće uslove:
5. Transformisana verzija $\mathrm{C}(x)$ biometrije x ne bi trebalo da se podudara sa originalom, tj. $\mu(\mathrm{C}(x), x) \leq t$, gde je, opet, t prag odluke za uparivanje algoritma μ.

Više transformisanih biometrija $\mathrm{C}(x_1)$ i $\mathrm{C}(x_2)$ generisane iz istog šablona x iste biometrije ne bi trebalo da se poklapaju $\mu\big(\mathrm{C}_1(x), \mathrm{C}_2(x)\big) \leq t$. Time se sprečava unakrsno podudaranje između baza podataka kada se koriste različite poništive transformacije C_1 i C_2 naravno podrazumeva se da se i same transformacije razlikuju.

Originalni biometrijski ili šablon x ne bi trebalo da se povrati iz transformisanog $\mathrm{C}(x)$ obzirom da po definiciji jednosmerne funkcije ne postoji njena inverzna, te inverzna transformacija C^{-1} ne bi trebalo da postoji. Ovo svojstvo čuva privatnost originalnog šablona x pošto se ne čuva.

4.1.1.2. Neinverzibilnost

Da bi određena funkcija bila jednosmerna funkcija odnosno neinvertibilna, za takvu funkciju mora da važi pravilo da se ne može uz pomoć određenih matematičkih funkcija vratiti odnosno transformisati u svoju originalnu funkciju.

Dakle, neivertibilnost kod otisaka prsta se ogleda u činjenici da je nemoguće kreirati funkciju koja uzima transformisanu tačku i regeneriše jedinstvenu ulaznu tačku. Za transformaciju preklapanja površine, ovo se može realizovati na dva načina: Prvo, ako oblast prostora (recimo, kvadrat od 50 50 piksela) mapiramo na manji deo prostora (recimo, kvadrat od 20 20 piksela), ovo

„smanjenje regiona“ može da unese nejasnoću između tačaka. Dve obližnje tačke na ulaznoj slici mogu se mapirati na potpuno istu (kvantizovanu) tačku na izlaznoj slici. Međutim, detaljne tačke su retko bliže od jednog razmaka grebena, tako da je uticaj ovog fenomena minimalan. Interesantniji je slučaj kada se površina slike uvija savijanjem, odnosno zgužva.

U ovakvim transformacijama dva relativno velika regiona ulazne slike se preklapaju u izlaznoj slici, Vizuelno na slici koja je zgužvana minucije izgledaju kao da su bliže jedna drugoj. Dakle, ako se izabere neka tačka na transformisanoj slici koja leži u takvom regionu, nemoguće je reći kom od ova dva originalna disjunktna ulazna regiona pripada tačka čime se povećava neivertibilnost [55]. Da bismo izmerili stepen takvog „savijanja“ u transformaciji, izračunavamo četiri najbliža suseda svake tačke minucija pre i posle transformacije. Koristeći ove lokalne informacije, može se konstruisati kompletna mreža tačaka detalja. Ako mreže pre i posle transformacije imaju istu povezanost, invertovanje transformacije je jednostavno stvar gužvanja slike.

4.1.2. Autentifikacija prepoznavanjem lica

U literaturi problem prepoznavanja lica može biti formulisan kao:

- prepoznavanje lica sa date statične (fotografije) ili video slike scene,
- identifikacija ili verifikacija jedne ili više osoba na sceni upoređivanjem sa licima sačuvanim u bazi podataka.

Kada se upoređuje verifikaciju lica sa prepoznavanjem lica, postoji nekoliko aspekata koji se razlikuju [56]. Prvo, pretpostavlja se da je osoba – ovlašćeni korisnik sistema lične identifikacije odnosno da zahteva proveru identiteta. Računarski to znači da nije potrebno konsultovati kompletan set slika baze podataka da bi se potvrdila tvrdnja. Dolazna slika (koja se naziva probna slika) se stoga upoređuje sa malim brojem slika modela osobe čiji se identitet tvrdi, a ne, kao u scenariju prepoznavanja, sa svakom slikom (ili nekim deskriptorom slike) u potencijalno velika baza podataka.

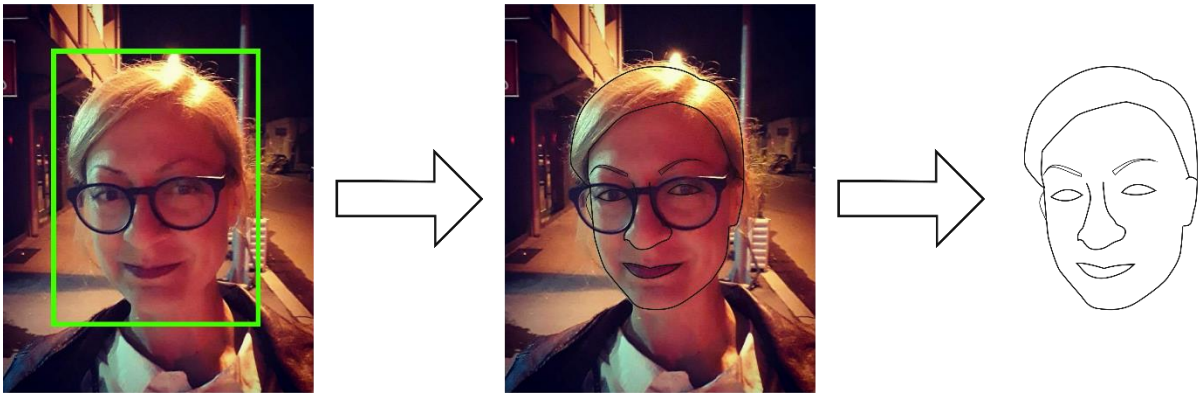
Drugo, automatski sistem autentifikacije mora da radi u skoro realnom vremenu da bi bio prihvatljiv za korisnike. Konačno, u eksperimentima prepoznavanja, samo slike ljudi treniranog seta podataka su već nalaze u sistemu.

Generalno, biometrijski uređaji se mogu objasniti u tri koraka:

1. senzor vrši posmatranje. Vrsta senzora i njegovo posmatranje zavise od vrste biometrijskog uređaja. Ovakav zapis daje biometrijski potpis pojedinca.
2. kompjuterski algoritam normalizuje biometrijski potpis tako da bude u istom formatu (veličina, rezolucija, prikaz, itd.) kao uzorci u bazi podataka sistema. Normalizacija biometrijskog potpisa daje normalizovani potpis pojedinca.
3. uparivač upoređuje normalizovani potpis sa skupom (ili podskupom) normalizovanih potpisa u bazi podataka sistema i pruža „ocenu sličnosti“ koja upoređuje normalizovani potpis pojedinca sa svakim potpisom u skup baze podataka.

Šta se dalje radi sa sličnošću rezultati zavisi od primene biometrijskog sistema.

Prepoznavanje lica počinje otkrivanjem obrazaca lica, nastavlja normalizacijom lica slike koje uzimaju u obzir geometrijske promene i promene osvetljenja, eventualno koristeći informacije o lokaciji i izgledu orijentira na licu. Zatim se identifikuje lice koristeći odgovarajuće klasifikacione algoritme i obrađuje rezultate koristeći šeme zasnovane na modelu.



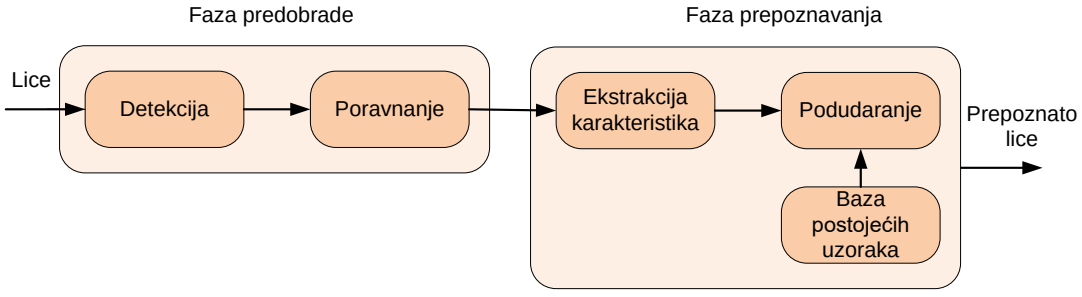
Slika 4-2: Jedan način detekcije lica

Svi algoritmi za prepoznavanje lica funkcionišu kroz dve segmenta: (1) detekcija i normalizacija lica i drugi segment identifikacija lica. Algoritmi koji se sastoje iz oba segmenta se nazivaju potpuno automatski algoritmi dok se oni koji se sastoje samo iz drugog segmenta nazivaju delimično automatskim algoritmi.

Razvoj prepoznavanja lica tokom proteklih godina razvio je različite načine za prepoznavanje: na frontalni, profilni i tolerantno na pogled prepoznavanje. U zavisnosti od vrste slika koriste se drugačiji algoritmi za prepoznavanje. Dok frontalno prepoznavanje svakako jeste klasični pristup, obično će algoritmi tolerantni na pogled izvršiti prepoznavanje na sofisticiraniji način uzimajući u obzir neke osnovne postulate fizike, geometrije, i statistike.

Prepoznavanje sa profila kao samostalni sistemi ima prilično marginalni značaj za identifikaciju. Međutim, oni su veoma praktični ili za brze grube pretraga velike baze podataka lica da bi se smanjila računarsko opterećenje za naknadne algoritme, ili kao deo hibridne šeme prepoznavanja. Postoje takođe i hibridni pristupi, oni imaju poseban status među prepoznavanjem lica sistema jer kombinuju različite pristupe prepoznavanju u cilju prevazilaženja nedostatka pojedinačnih komponenti.

Tok obrade prepoznavanja lica, prikazan na slici 4-2, sastoji se od četiri modula: detekcija, poravnanje, ekstrakcija karakteristika, i podudaranje. Uopšteno govoreći, koraci toka obrade se mogu podeliti u dve glavne etape: faza predobrade i faza prepoznavanja. Prva faza uključuje detekciju lica i usklađivanje ili lokalizaciju i normalizaciju. Ekstrakcija crta lica i usklađivanje čine poslednju fazu.



Slika 4-3: Prepoznavanje lica opisano kroz faze

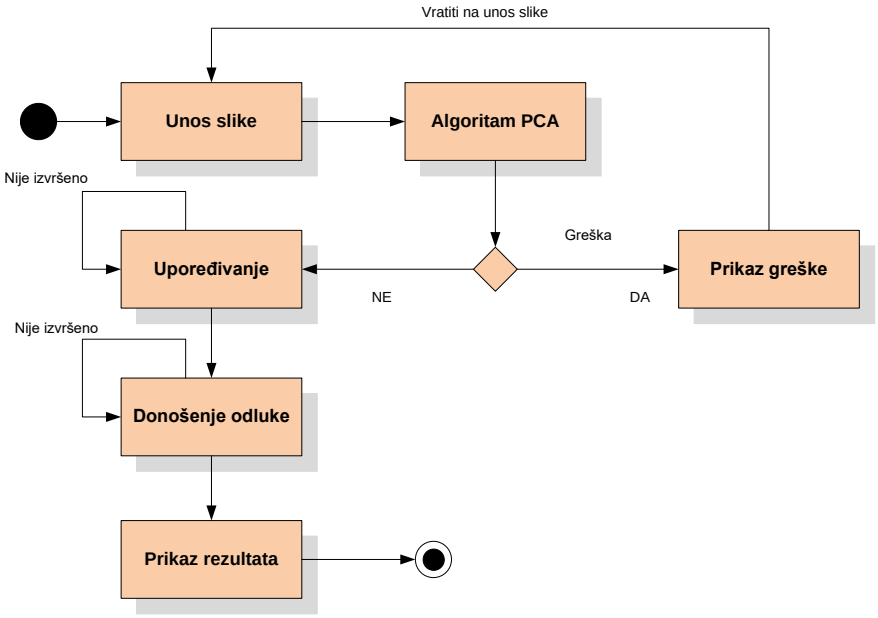
Fokusiranje na aspekt promenljivosti poze lica, prepoznavanje lica pristupi se mogu podeliti u dve kategorije: globalni pristup i pristup zasnovan na komponentama. U globalnom pristupu, jedan vektor obeležja koji predstavlja celinu slike lica se koristi kao ulaz u klasifikator. U literaturi se predlaže nekoliko klasifikatora poput: minimalnog rastojanja, klasifikacija u sopstvenom prostoru Fišerova diskriminaciona funkcija i neuronske mreže.

Globalne tehnike dobro rade za klasifikaciju frontalnih pogleda lica. Međutim, oni nisu otporne na promene položaja lica obzirom da su globalne karakteristike veoma osetljive na translaciju i rotaciju lica. Jedan od načina kako se ovaj problem može izbeći je uvođenje faze poravnavanja pre same klasifikacije. Poravnavanje ulazne slike lica sa referentnom slikom lica zahteva kompjutersku korespondenciju između dve slike lica. Korespondencija je obično određena za mali broj istaknutih tačaka na licu kao centar oka, nozdrve ili uglovi usta. Na osnovu ovih korespondencija, ulazna slika lica može se izobličiti na referentnu sliku lica. U procesu poravnanja mogu se koristite sledeće tehnike: Afina transformacija, modeli aktivnih oblika (engl. *Active shape models*), metode vektora oslonca (engl. *Support Vector Machine*, SVM).

Alternativa globalnom pristupu je klasifikacija lokalnih komponenti lica. Glavna ideja u ovom vidu klasifikacije je da se kompenzuju promene poze omogućavajući fleksibilan geometrijski odnos između komponenata u fazi klasifikacije. U literaturi se mogu naći rešenja gde se prepoznavanje lica vrši nezavisno za tri regije lica (oči, nos i usta). Konfiguracija komponenti tokom klasifikacije tada nije ograničena pošto sistem ne sagledava geometrijski model lica. Mogu se takođe naći i radovi koji koriste pristup prepoznavanja uz upotrebu dodatnog stepena poravnanja.

U fazi prepoznavanja može se koristiti analiza svojstvenih površina i princip prepoznavanja glavnih komponenti (eng. *Principal Component Analysis*, PCA). Svojstvene površine se slože tako da predstavljaju različite količine varijacije, respektivno, između lica. Svako lice može biti tačno predstavljeno linearnom kombinacijom svojstvenih površina. Takođe se mogu aproksimirati korišćenjem samo najboljih svojstvenih površina. Najbolje svojstvene površine konstruišu više dimenzionalni prostor, odnosno prostor lica. Razne druge tehnike su opisane i dostupne u različitim naučnim časopisima, neki od njih su u literaturi [57], [58].

U procesu provere podudaranja veliki uticaj ima dostupna baza postojećih uzoraka sa kojom se vrši poređenje. Postojeće javno dostupne baze podataka lica sadrže slike lica sa širokim spektrom poza, uglova osvetljenja, gestove, ove slike umeju nekad da budu neadekvatno obeležene, čime se ograničava njihovo korišćenje za procenu relativnih performansi lica algoritmi detekcije. Na primer, mnoge slike u postojeće baze podataka nisu označene tačnim uglovima položaja na kojoj su odvedeni. Da bismo uporedile performanse različitih lica algoritama za prepoznavanje baze podataka treba da budu sistematične, sa velikim brojem dostupnih uzorka čiji su dostupni podaci dobro struktuirani.



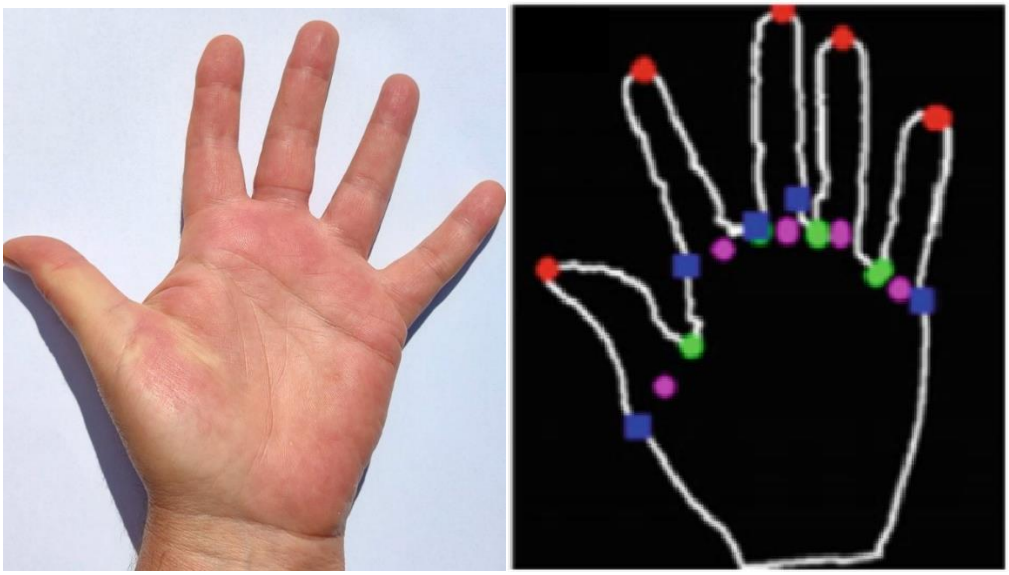
Slika 4-4: Dijagram aktivnosti

Analiza biometrijske metode kroz ocenu ispunjenosti aspekata

- Jedinstvenost: srednji stepen ispunjenosti
- Trajnost: srednji stepen ispunjenosti
- Prikupljivost: visok stepen ispunjenosti
- Izvodljivost: srednji stepen ispunjenosti
- Prihvatljivost: visok stepen ispunjenosti

4.1.3. Autentifikacija otiskom dlana

Čovekov dlan predstavlja jednu od njegove jedinstvenosti. Jedinstvenost se ogleda u širini i dužini dlana, rasporedu dužini i dubini papilarnih linija koje se na njemu nalaze, ukrštene papilarne linije koje postoje u korenu prstiju. Bitno je naglasiti da se sve navedene karakteristike dlana kod odraslih osoba ne menjaju tokom vremena, sem u slučaju povreda.



Slika 4-5 Otisak dlana

Slike otiska dlana mogu se snimiti i pomoću jeftinih kamera niske rezolucije, no naravno mogu se iskoristiti i savremeni multispektralni sistemi koji uz pomoć određenih talasnih dužina generišu slike dlana .

Kao i kod otiska prsta, pošto se slike generišu primenjuju se neke od metoda za njihovu obradu, izdvajaju se određena obeležja i upoređuju [59]. Poređenja se mogu vršiti na osnovu klasifikacionih tehnika kada ceo dlan posmatramo kao visedimenzioni vektor, zatim se mogu porediti samo određene karakteristike na dlanu na osnovu šablona, a mogu se koristiti i

kombinacije navedenih metoda. Nad snimkom uzorka se primenjuju određeni algoritmi i generiše se šablon.

Iako dlan sadrži dosta karakteristika, sa aspekta biometrije njega karakteriše niska pouzdanost jer je količina informatičkog sadržaja koja se može dobiti mala.

Analiza biometrijske metode kroz ocenu ispunjenosti aspekata:

- Jedinstvenost: nizak stepen ispunjenosti
- Trajnost: srednji stepen ispunjenosti
- Prikupljivost: visok stepen ispunjenosti
- Izvodljivost: srednji stepen ispunjenosti
- Prihvatljivost: nizak stepen ispunjenosti

Ova metoda se zahvaljujući napretku informacionih tehnologija, modifikovala, te dovela do toga da se upotrebom različitih LED skenera, skenira raspored vena na dlanu. Vene su zbog svoje različitosti u smislu debljine i rasporeda dobar biometrijski izbor koji ne može dovesti do generisanja istih šablona za različite osobe.

Tipičan sistem za prepoznavanje rasporeda vena na dlanu sastoji se od četiri koraka [60]: akvizicija slike vena na dlanu, predobrade, posebno na lokaciji sredine dlana (engl. *region of intrest*, ROI), ekstrakcija i uparivanje karakteristika. Akvizicija slike vena na dlanu prikuplja slike vena na dlanu. Predobrada segmentira deo slike vene dlana za ekstrakciju obeležja. Ekstrakcija karakteristika dobija efikasne karakteristike iz prethodno obrađenih vena dlana. Uparivač upoređuje dve karakteristike vena na dlanu i baza podataka čuva registrovane šablone.

4.1.4. Autentifikacija uz pomoć oka

Još jedna od osobenosti čoveka su oči, sa aspekta biometrije određeni delovi oka predstavljaju dobar biometrijski izvor. U procesu autentifikacije uz pomoć oka, koriste se dve metode skeniranje retine i skeniranje irisa.

Prilikom procesa skeniranja irisa, prvi deo se odnosi na njegovo pronalaženje u odnosu na ostale delove oka, odnosno lokalizaciju sa fotografije. Preciznost koja je ovde neophodna, utiče direktno na kvalitet uzorka. Za sam proces lokalizacije se koriste neki od već postojećih algoritama kao što je Hafova transformacija. Hafova transformacija određuje kružnicu koje locira iris. Nakon toga veliku ulogu ima kvalitet same slike, jer je sledeći korak normalizacija slike irisa.

4.1.4.1. Prepoznavanje dužice oka (Irisa)

Pouzdano automatsko prepoznavanje osoba odavno predstavlja primamljiv cilj. Kao i u svim problemima prepoznavanja obrazaca, ključno pitanje jeste odnos između međuklasne i unutar klasne varijabilnosti: objekti se mogu pouzdano klasifikovati samo ako je varijacija između različitih instanci date klase manja od varijacije između različitih klasa. Na primer, prilikom prepoznavanju lica, poteškoće nastaju zbog činjenice da je lice promenljivi društveni organ koji prikazuje različite izraze, tj. predstavlja aktivan 3D objekat čija slika varira u zavisnosti od ugla gledanja, poze, osvetljenja, aksesoara i starosti [61]. Pokazalo se da čak i za slike koje su snimljene u razmaku od najmanje jedne godine, čak i kada je reč o fotografijama za zvanična dokumenta čak i najbolji algoritmi imaju neprihvatljivo velike stope grešaka. Nasuprot ove varijacije unutar klase (isto lice), varijacije među klasama su ograničene jer različita lica poseduju isti osnovni skup karakteristika, u istoj kanonskoj geometriji.

Prateći osnovni princip da varijacije među klasama treba da budu veće od varijacija unutar razreda, šare dužice nude moćan alternativni pristup pouzdanom vizuelnom prepoznavanju osoba kada se slikanje može uraditi na udaljenosti od oko metar ili manje, a posebno kada postoji potreba za pretraživanjem veoma velike baze podataka bez ikakvih lažnih podudaranja uprkos ogromnom broju mogućnosti da se to dogodi. Iako mala, prečnik 11 mm, i ponekad problematična za snimanje, iris ima veliku matematičku prednost u tome što je njena varijabilnost uzorka među

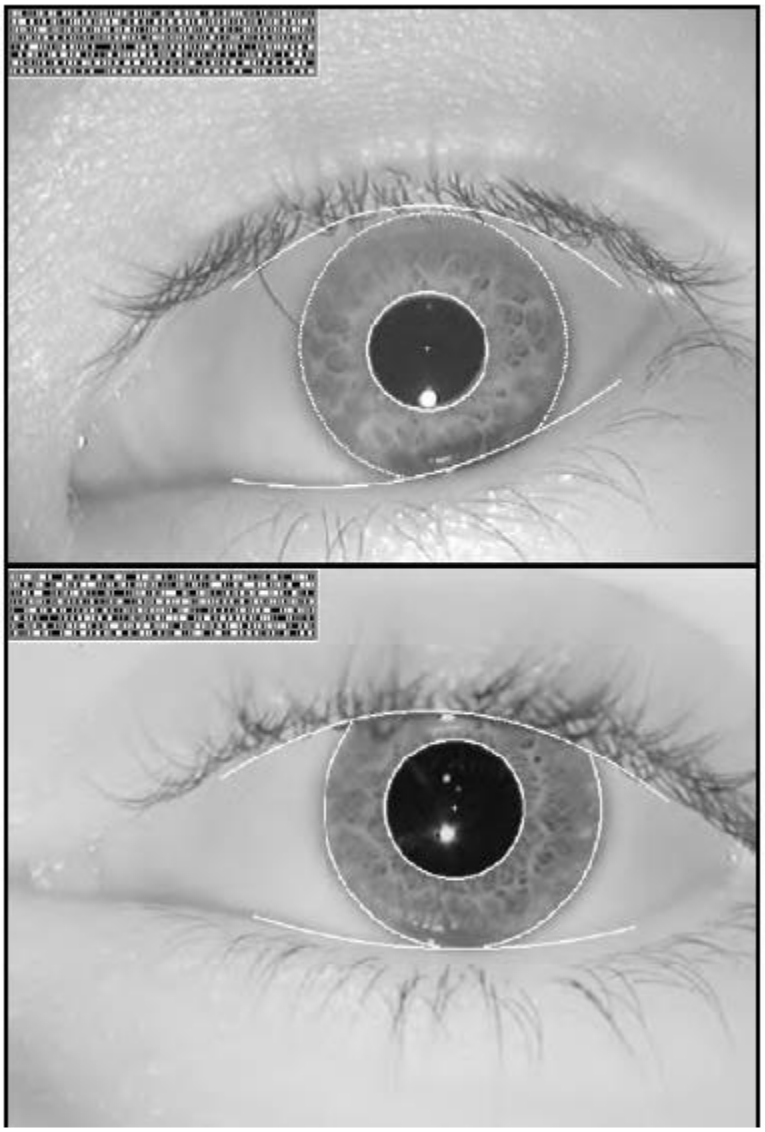
različitim osobama ogromna. Pored toga, kao unutrašnji (ali spolja vidljiv) organ oka, iris je dobro zaštićena od okoline i stabilna tokom vremena. Kao ravan objekat, njena slika je relativno neosetljiva na ugao osvetljenja, a promene ugla gledanja izazivaju samo nesrodne transformacije; čak i nesrodno izobličenje uzorka uzrokovano dilatacijom zenice je lako reverzibilno u fazi kodiranja slike. Na kraju, lakoća lokalizacije očiju na licima i prepoznatljiv prstenasti oblik dužice omogućavaju pouzdanu i preciznu izolaciju ove osobine i kreiranje prikaza nepromenljive veličine.

Iris počinje da se formira u trećem mesecu trudnoće [51] i strukture koje stvaraju njen obrazac su uglavnom završene do osmog meseca, iako se akrecija pigmenta može nastaviti u prvim postnatalnim godinama. Njena složena šara može da sadrži mnoge karakteristične odlike kao što su lučni ligamenti, brazde, grebeni, kripte, prstenovi, krug, pege i cik-cak venac, od kojih se neke mogu videti na slici 4-5. Boja dužice je određena uglavnom gustinom pigmenta melanina u njegovom prednjem sloju, dok plave dužice predstavljaju rezultat odsustva pigmenta [62]. Svetlost duže talasne dužine prodiru, dok se kraće talasne dužine rasipaju kroz prednji sloj dužice (stromu). Poprečna trabekularna mreža elastičnog pektinatnog ligamenta stvara preovlađujuću teksturu pod vidljivom svetlošću, dok u bliskim infracrvenim (NIR) talasnim dužinama koje se koriste za nenametljivo snimanje, dublje i nešto sporije modulisane karakteristike strome dominiraju šarom zenice. U NIR talasnim dužinama, čak i tamno pigmentisane šarenice otkrivaju bogate i složene karakteristike [62].

4.1.4.2. Lokalizovanje dužice i njena ograničenja

Kako bi se uhvatilo sto više i što boljih detalja šare dužice, sistem za snimanje treba da razreši najmanje 70 piksela u prečniku irisa. U većini slučajeva primene ovih algoritama do danas, razrešeni radijus dužice je obično iznosio 80 do 130 piksela. Monohromne CCD kamere (480 × 640) su korišćene jer je NIR osvetljenje u opsegu 700 *nm*–900 *nm* bilo potrebno kako slikanje ne bi izazivalo nelagodu kod ljudi. Neke platforme za snimanje su koriste široko ugaonu kameru za grubu lokalizaciju očiju na licu da bi upravljale optikom usko ugaone pan/tilt kamere koja je dobijala slike očiju veće rezolucije. Postoji mnogo alternativnih metoda za pronalaženje i praćenje crta lica, kao što su oči, i o ovoj dobro istraženoj temi ovde se neće dalje raspravljati. Većina slika

u sadašnjoj bazi podataka je dobijena bez upotrebe aktivne optike pan/tilt kamere, umesto toga korišćena je vizuelnu povratnu informaciju preko ogledala ili video slike kako bi omogućili subjektima koji sarađuju da pozicioniraju svoje oči unutar vidnog polja jedne kamere sa uskim uglom.



Slika 4-6: Primer šara dužice(irisa) [63]

Primeri ljudskih šara dužice, monohromatski prikazani na udaljenosti od oko 35 cm. Prekrivači obrisa pokazuju rezultate lokalizacije dužice i zenice i koraka detekcije očnih kapaka. Nije moguće pretpostaviti da su granice dužice koncentrične ili čak kružne. Tokovi bitova na slici

su rezultat demodulacije sa 2D Gaborovim talasima kompleksne vrednosti za kodiranje fazne sekvence svake šare dužice.

Procena fokusa slike se vrši u realnom vremenu (brže od brzine kadrova u video snimku) merenjem spektralne snage u srednjim i gornjim frekventnim opsezima 2D Furijeovog spektra svakog okvira slike i nastojanjem da se ova količina maksimizira bilo pomeranjem aktivnog sočiva ili obezbeđivanjem audio povratne informacije subjektima kako bi na odgovarajući način prilagodili svoj opseg. Brzina izvršenja video brzine procene fokusa (tj. u roku od nekoliko milisekundi na ARM uređaju) se postiže korišćenjem jezgra 2D filtera propuštanja opsega koji zahteva samo sumiranje i razlikovanje piksela, i bez množenja, unutar potrebne 2D konvolucije neophodne za procenu snage u odabrane 2D spektralne trake.

Slike koje zadovoljavaju kriterijum minimalnog fokusa se zatim analiziraju da bi se pronašla dužica, sa inicijalno kružnim aproksimacijama njenih granica korišćenjem strategije od grube do fine koja se završava procenama koordinata centra i radijusa irisa i zenice. Iako rezultati pretrage dužice u velikoj meri ograničavaju pretragu zenice, ne može se pretpostaviti koncentričnost ovih granica. Vrlo često je centar zenice nazalan i inferioran u odnosu na centar dužice. Njegov radijus može da se kreće od 0,1 do 0,8 radijusa irisa. Dakle, sva tri parametra koja definišu zenicu kada se aproksimira kao krug moraju se proceniti odvojeno od parametara irisa. Veoma efikasna formula za određivanje ovih parametara je [64]:

$$\max_{(r,x_0,y_0)} \left| G\sigma(r) * \frac{\partial}{\partial_r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

gde je $I(x,y)$slika kao što je slika 4-6, koja sadrži oko. Formula traži preko domena slike (x,y) maksimum u zamućenoj parcijalnoj derivaciji u odnosu na povećanje radijusa r normalizovanog konturnog integrala $I(x,y)$ duž kružnog luka ds poluprečnika r i koordinata centra (x_0,y_0). Simbol * označava konvoluciju, a $G\sigma(r)$ je funkcija izglađivanja konkretno Gausova funkcije. Kompletan operator se ponaša kao kružni detektor ivica, zamagljen na skali postavljenoj sa σ, tražeći iterativno maksimalnu konturnu integralnu derivaciju na sukcesivno finijim skalama analize kroz tri parametarska prostora koordinata centra i radijusa $(r,x_0,y_0))$ koji definišu put konturne integracije.

Formula služi da pronađe i granicu zenice i spoljnu (limbus) granicu irisa na način koji se međusobno pojačava. Jednom kada iterativne pretrage od grubog do finog za obe ove granice dostignu jednopikselnu preciznost, onda se sličan pristup detektovanju krivolinijskih ivica koristi za lokalizaciju i gornje i donje granice očnog kapka. Put integracije konture u datoj formuli je promenjen iz kružnog u lučni, sa parametrima spline prilagođenim metodama statističke procene za modeliranje svake granice očnog kapka. Slike sa manje od 50% šarenice vidljive između postavljenih izbočina očnih kapaka smatraju se neadekvatnim, na primer, u treptaju. Učinak svih ovih procesa detekcije je filtriranje tkiva šarenice od drugih regiona slike.

Pošto unutrašnje i spoljašnje granice dužice često nisu pravi krugovi, učinak u prepoznavanju dužice je značajno poboljšan ublažavanjem obe ove pretpostavke, zamenjujući ih disciplinovanijim metodama za verno otkrivanje i modelovanje tih granica bez obzira na njihov oblik, i definisanjem fleksibilnijeg generalizovanijeg koordinatnog sistema na njihovoj osnovi. Budući da je spoljna granica dužice često delimično prekrivena kapcima, a unutrašnja granica dužice može biti delimično prekrivena refleksijama od osvetljenja, a ponekad obe granice takođe mogu biti delimično zaklonjene refleksijama od naočara, neophodno je postaviti fleksibilne konture koje mogu tolerisati smetnje i nastaviti svoju putanju preko njih na principijelnoj osnovi, nekako vođeni podacima koji postoji negde drugde. Dalje ograničenje je da i unutrašnji i spoljašnji granični model moraju formirati zatvorene krive. Konačni cilj je težnja da se nametne ograničenje u smislu glatkoće, na osnovu verodostojnosti bilo kog dokaza za neglatku krivinu.

Odličan način da se postignu svi ovi ciljevi je opisivanje unutrašnjih i spoljašnjih granica dužice u smislu „aktivnih kontura“ na osnovu diskretnih razvoja Furijerovih serija podataka o konturi. Korišćenjem Furijerovih komponenti čije su frekvencije celobrojni uzorci od $1/2\pi$, obezbeđena je zatvorenost, ortogonalnost i potpunost. Odabir broja frekvencijskih komponenti omogućava kontrolu nad stepenom glatkoće koja se nameće i nad vernošću aproksimacije. U suštini, skraćivanje diskretnog Furijeovog reda nakon određenog broja termina predstavlja nisko propusno filtriranje podataka o graničnoj krivini u aktivnom modelu konture. Procedura procene je izračunavanje Furijeove transformacije N pravilno raspoređenih ugaonih uzoraka radijalnih podataka o ivicama gradijenta $\{r_\theta\}$ za $\theta = 0, \ldots, N-1$. Skup M diskretnih Furijerovih koeficijenata $\{C_k\}$ za $k = 0, \ldots, M-1$, izračunavaju se iz niza podataka $\{r_\theta\}$ na sledeći način:

$$C_k = \sum_{\theta=0}^{N-1} r_\theta e^{-2\pi ik\theta/N}$$

Koeficijent nultog reda ili jednosmerna komponenta C_0 izdvaja informacije o prosečnoj krivini granice (zenice ili spoljašnje dužice), drugim rečima, o njenom poluprečniku kada se aproksimira samo kao jednostavan krug.

Iz ovih M diskretnih Furijerovih koeficijenata, dobija se aproksimacija odgovarajuće granice dužice, bez prekida i sa rezolucijom koju određuje M, kao novi niz $\{r_\theta\}$ za $\theta = 0, \ldots, N-1$.

$$R_\theta = \frac{1}{N} \sum_{k=0}^{M-1} C_k e^{2\pi ik\theta/N}$$

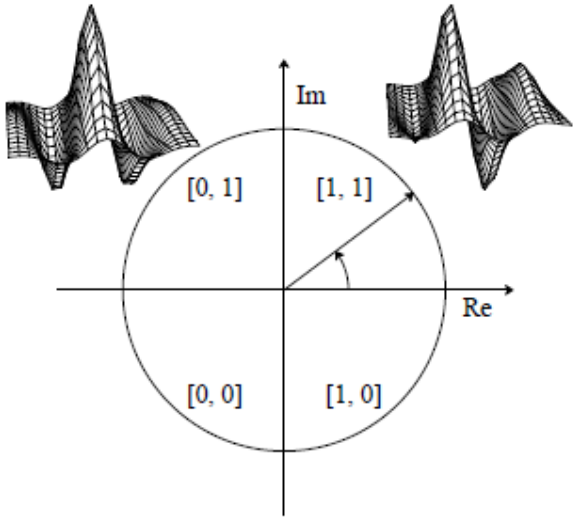
Za metode aktivne konture, postoji kompromis između toga koliko precizno neko želi da model odgovara svim podacima (poboljšano povećanjem M), u odnosu na to koliko se želi nametnuti ograničenja kao što je održavanje modela jednostavnim i niskodimenzionalna zakrivljenost (postignuta smanjenjem M , na primer M = 1 primenjuje kružni model). Dakle, broj M aktiviranih Furijerovih koeficijenata je specifikacija za broj stepeni slobode u modelu oblika. Dobar izbor M za snimanje prave granice zenice sa odgovarajućom vernošću je M = 17, dok je dobar izbor za spoljnu granicu dužice gde su podaci često mnogo slabiji je M = 5. Takođe je korisno da se nametnu monotono opadajuće težine izračunatim Furijeovim koeficijentima C_k kao dalju kontrolu rezolucije aproksimacije $\{R_\theta\} \approx \{r_\theta\}$, koja se svodi na niskopropusno filtriranje zakrivljenosti u njenoj Furijevoj predstavi. Sve u svemu, ove manipulacije, posebno dva različita izbora za M, implementiraju princip kompjuterskog vida da se jaki podaci (granica zenice) mogu modelovati samo sa slabim ograničenjima, dok slabi podaci (spoljna granica) treba da se modeluju sa jakim ograničenjima.

Aktivni modeli kontura za unutrašnje i spoljašnje granice dužice podržavaju izometrijsko mapiranje tkiva dužice između njih, bez obzira na stvarne oblike kontura, i sa otpornošću na praznine kao one koje su posledica prekida uzrokovanih očnim kapcima.

4.1.4.3. Kodiranje odlika dužice pomoću 2D Gaborove talasne demodulacije

Svaki izolovani uzorak dužice se zatim demoduliše da bi se izdvojila informacija o fazi pomoću kvadratnih 2D Gaborovih talasa [64]. Ovaj proces kodiranja je ilustrovan na slici 4-7. On se svodi na faznu kvantizaciju šare dužice u slojevima, identifikujući u kom kvadrantu kompleksne ravni leži svaki rezultujući fazor kada se dato područje dužice projektuje na 2D Gaborove talase kompleksne vrednosti:

$$h_{\{Re,Im\}} = sgn_{\{Re,Im\}} \int_{\rho} \int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} \cdot e^{-(r_0-\rho)^2/\alpha^2} \cdot e^{-(\theta_0-\phi)^2/\beta^2} \, \rho \, d\rho d\phi$$



Slika 4-7: 2D Gaborovi talasi

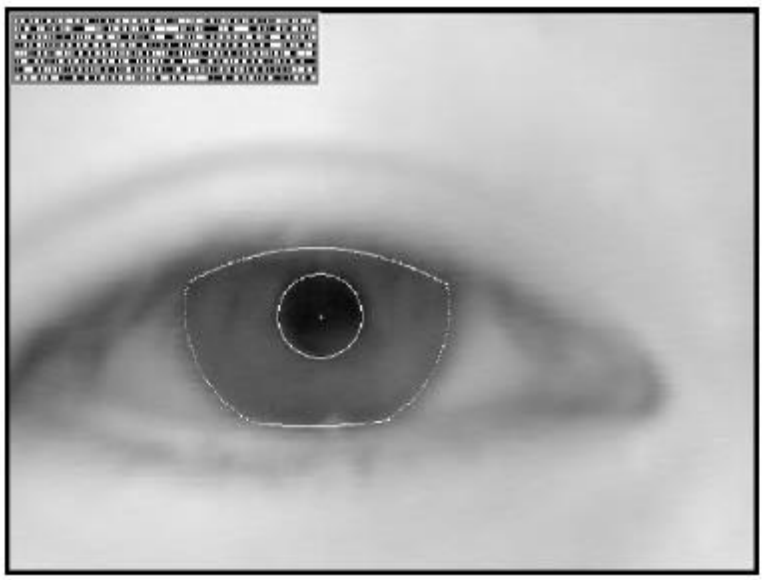
Proces fazne demodulacije koji se koristi za kodiranje šara dužice. Lokalni delovi dužice se projektuju na kvadratne 2D Gaborove talase, generišući koeficijente kompleksne vrednosti gde realni i imaginarni delovi određuju koordinate fazora u kompleksnoj ravni. Svaki fazor, odnosno njegov ugao je kvantovan u jednom od četiri kvadranta, definišući 2 bita informacije o datoj fazi. Sam proces se vrši po celom irisu definiše se veliki broj fazora kako bi se izdvojilo 2048 bita, gde se $h_{\{Re,Im\}}$ može posmatrati kao bit čija je vrednost kompleksan broj, kod koga je realni i imaginarni deo uslovljen predznakom 2D integrala; $I(\rho,\phi)$ je neobrađena slika dužice u koordinatnom sistemu koji je nepromenljiv u veličini i translaciji, i koji takođe ispravlja proširenje zenice, α i β su parametri veličine 2D talasa na više skala, koji obuhvataju osmostruki opseg od

0,15 mm do 1,2 mm na irisu; ω je talasna frekvencija, koja obuhvata 3 oktave u obrnutoj proporciji sa β; i sa (r_0, θ_0) su definisane, u za svaki region irisa, polarne koordinate na osnovu kojih se dobijaju $h_{\{Re,Im\}}$. Takve sekvence kodiranja faznog kvadranta su ilustrovane za dve dužice pomoću tokova bitova prikazanih grafički na slici 4-6. Poželjna karakteristika definicije faznog koda date na slici 4-7 je da je to ciklični ili sivi kod: pri rotiranju između bilo kojih susednih faznih kvadranata, menja se samo jedan bit, za razliku od binarnog koda u kome se 2 bita mogu promeniti, čineći neke greške proizvoljno skuplje od drugih. Ukupno 2048 takvih faznih bitova (256 bajtova) se izračunava po svakom irisu, ali u velikom poboljšanju u odnosu na ranije algoritme, sada se takođe izračunava jednak broj maskirnih bitova da bi se označilo postoji li neki region dužice koji je zaklonjen kapcima, postoje li neke okluzije trepavica, spekularne refleksije, granične artefakte tvrdih kontaktnih sočiva ili sadrži loš odnos signal-šum i stoga ga treba zanemariti u kodu za demodulaciju kao artefakt.

2D Gaborovi talasi su izabrani za ekstrakciju informacija o irisu zbog lepih svojstava optimalnosti ovih talasa. Prateći Hajzenbergov princip nesigurnosti koji se generalno primenjuje na matematičke funkcije, filteri koji su dobro lokalizovani po frekvenciji su loše lokalizovani u prostoru (ili vremenu), i obrnuto. 2D Gaborovi talasi imaju maksimalnu zajedničku rezoluciju u dva domena istovremeno [64], što znači da se i „šta“ i „gde“ informacije o karakteristikama dužice ekstrahuju sa optimalnom simultanom rezolucijom. Još jedno lepo svojstvo 2D Gaborovih talasa je da, pošto su kompleksne vrednosti, dozvoljavaju definisanje i dodeljivanje faznih promenljivih bilo kojoj tački na slici.

Samo informacije o fazi se koriste za prepoznavanje iris jer informacije o amplitudi nisu veoma diskriminirajuće i zavise od kontrasta same slike, osvetljenje i drugih. Podešavanja faznih bitova koja kodiraju sekvencu projekcijskih kvadranta kao što je prikazano na slici 4-7, obuhvataju informacije o prelasku talasa u nulu, kao što je jasno iz formule. Ekstrakcija faze ima dalju prednost u tome što fazni uglovi ostaju definisani bez obzira na to koliko loš može biti kontrast slike, kao što ilustruje slika koja je izuzetno van fokusa na slici 4-8. Njegov fazni tok bitova ima statistička svojstva kao što su dužine slična onima kodova za pravilno fokusirane slike oka na slici 4-5 (Slika 4-7 takođe ilustruje robusnost operatora za pronalaženje dužice i zenice i operatora detekcije očnih kapaka, uprkos lošem fokusu.) Prednost koja proizilazi iz činjenice da su fazni bitovi podešeni i za slabo fokusiranu sliku, kao što je prikazano ovde, čak i ako se zasniva samo na nasumičnom

CCD termičkom šumu, različite loše fokusirane dužice nikada ne budu pomešane jedna sa drugom kada se uporede njihovi fazni kodovi. Nasuprot tome, slike različitih lica izgledaju sve sličnije kada je rezolucija loša i moguće ih je pomešati algoritmima za prepoznavanje lica zasnovanim na izgledu.



Slika 4-8: Izdvajanje irisa iz mutne slike

Ovim se ilustruje da su čak i za loše fokusirane slike oka, bitovi sekvence faze demodulacije i dalje postavljeni, prvenstveno nasumičnim CCD šumom. Ovo sprečava da se loše fokusirane slike oka pogrešno podudaraju, jer mogu biti u prikazima zasnovanim na amplitudi.

4.1.4.4. Prepoznavanje dužice oka – univerzalni metod

Robusne reprezentacije za prepoznavanje obrazaca moraju biti nepromenljive u odnosu na promene u veličini, položaju i orijentaciji obrazaca. U slučaju prepoznavanja dužice, to znači da se mora kreirati reprezentacija koja je invarijantna:

- optičkoj veličini dužice (koja zavisi od udaljenosti od oka i faktora optičkog uvećanja kamere);
- veličini zenice unutar dužice (što uvodi nesrodnu deformaciju uzorka);

- lokacija dužice unutar slike i
- orijentacija dužice.

Gore navedeno, zavisi od nagiba glave, torzione rotacije oka unutar njegovog ležišta i uglova kamere, u kombinaciji sa snimanjem pomoću fokusa za pronalaženje očiju pomeranjem/nagibom koja uvode dodatne faktore rotacije slike kao funkciju položaja oka , položaja kamere i uglova ogledala.

Za slike na osi, ali moguće rotirane dužice, prirodno je koristiti projektovani pseudopolarni koordinatni sistem. Koordinatna mreža nije nužno polarna niti simetrična, pošto se ne pretpostavljaju kružne granice i kod većine očiju zenica nije centralna u irisu; nije neuobičajeno da njegovo nazalno pomeranje iznosi čak 15%. Ovaj koordinatni sistem se može opisati kao dvostruko bezdimenzionalni: ugaona promenljiva je sama po sebi bezdimenzionalna, ali je u ovom slučaju i radijalna promenljiva bezdimenzionalna, jer se kreće od granice zenice do limbusa uvek kao jedinični interval [0, 1]. Dilatacija i stezanje(skupljanje) elastične mreže dužice kada zenica promeni veličinu je suštinski modelovana ovim koordinatnim sistemom kao istezanje homogene gume folije, koji ima topologiju prstena ukotvljenog duž svog spoljašnjeg perimetra, sa snagom vuče (napetosti) koju kontroliše (izvan središta) unutrašnji prsten promenljivog radijusa.

Model homogene gumene folije svakoj tački na irisu, bez obzira na njenu veličinu i proširenje zenice, dodeljuje par realnih koordinata (r, θ) gde je r na jediničnom intervalu [0, 1], a θ ugao [0, 2π]. Ova normalizacija ili ponovno mapiranje slike dužice $I(x, y)$ iz neobrađenih kartezijskih koordinata (x, y) u bezdimenzionalni pseudopolarni koordinatni sistem (r, θ)može se predstaviti kao [63]

$$I\big(x(r,\theta), y(r,\theta)\big) \rightarrow I(r,\theta)$$

gde su $x(r, \theta)$ i $y(r, \theta)$definisani kao linearne kombinacije skupa graničnih tačaka zenice $\big(x_p(\theta), y_p(\theta)\big)$ i skupa graničnih tačaka limbusa duž spoljašnje peri metra irisa $\big(x_s(\theta), y_s(\theta)\big)$ koji se graniči sa okvirom , kao što je određeno aktivnim modelima konture koji su inicijalizovani maksimumima iz formule

$$\max_{(\mathrm{r},\mathrm{x_0},\mathrm{y_0})} \left| \mathrm{G}\sigma(\mathrm{r}) * \frac{\partial}{\partial_\mathrm{r}} \oint_{\mathrm{r},\mathrm{x_0},\mathrm{y_0}} \frac{\mathrm{I(x,y)}}{2\pi\mathrm{r}} \mathrm{ds} \right|.$$

Sledi da je [64]:

$$x(r,\theta) = (1-r)x_p(\theta) + rx_s(\theta), \text{ odnosno } y(r,\theta) = (1-r)y_p(\theta) + ry_s(\theta).$$

Pošto se radijalna koordinata prostire od unutrašnje granice dužice do njene spoljne granice kao jedinični interval, ona inherentno koriguje deformaciju elastičnog uzorka u irisu kada se zenica promeni u veličini.

Lokalizacija dužice i gore opisani koordinatni sistem postižu nepromenljivost 2D položaja i veličine dužice i proširenja zenice unutar nje. Međutim, to ne bi bilo nepromenljivo u odnosu na orijentaciju dužice unutar ravni slike. Najefikasniji način da se postigne prepoznavanje dužice sa invarijantnošću orijentacije nije da se rotira sama slika, već da se izračuna fazni kod dužice u jednoj kanonskoj orijentaciji, a zatim da se ova veoma kompaktna reprezentacija u mnogim diskretnim orijentacijama uporedi cikličkim pomeranjem njegove ugaone promenljive [63].

Neka je funkcija $f(x)$ neobrađena (sirova) raspodela gustine dobijena za Hemingovo rastojanje između različitih irisa nakon njihovog poređenja samo u jednoj relativnoj orijentaciji. U slučaju da funkcija $f(x)$ sadrži binomnu raspodelu integral funkcije u opsegu od [0, x] predstavlja verovatnoću dobijanja lažnog podudaranja u testu kada se koristi Hemingovo rastojanje kao kriterijum prihvatanja x:

$$F(x) = \int_0^x f(x)\,dx$$

Verovatnoća da se ne napravi lažno podudaranje je $1 - F(x)$ i to nakon jednog testa. Za izvođenje *n* takvih testova nezavisno, verovatnoća se predstavlja $\big(1 - F(x)\big)^n$. Iz toga sledi da je verovatnoća lažnog podudaranja nakon „najboljeg od *n*“ testa slaganja, kada se koristi Hemingovo rastojanje kriterijum x, bez obzira na stvarni oblik neobrađene nerotirane distribucije *f(x)*,

$$F_n(x) = 1 - \big(1 - F(x)\big)^n$$

U radovima različitih autora nalazi se da za identifikaciju ljudi po irisu za visok stepen tačnosti, treba da zahtevati stepen podudarnosti Hemingovog rastojanje bude manji ili jednak od 0,32 [65].

Hemingovo rastojanje – osnovni pojmovi

Hemingovo rastojanje između dve kodne reči je jednostavno broj pozicija bitova u kojima se one razlikuju. Ako je Hemingovo rastojanje R između dve kodne reči K_1 i K_2, pri čemu je kodna reči K_1 ona koja se prenosi, tada bi se moralo pojaviti R grešaka da bi se kodna reč K_2 primila.

Uopšteno govoreći, ako je minimalna Hemingova udaljenost između kodne reči K_1 i bilo koje druge važeće kodne reči Rm, tada primljena kodna reč neće biti važeća kodna reč ako dođe do greške između opsega [1, Rm-1].

Sa druge strane, pod pretpostavkom da je primljena nevažeća kodna reč, rastojanje odnosno broj neslaganja između nje i svih važećih kodnih reči može se izračunati na prijemnoj strani. Neka rastojanje između primljene kodne reči i važeće kodne reči K_n bude Rn. Ako se utvrdi da je jedno od ovih rastojanja Rn manje od svih ostalih, onda je uz pretpostavku slučajnih grešaka realnije da je preneta kodna reč bila K_n od bilo koje druge. Dekoder bi se stoga mogao naterati da emituje „najverovatnije tačnu“ kodnu reč K_n; ovo je poznato kao korekcija greške maksimalne verovatnoće ili minimalne udaljenosti. Takva korekcija greške je moguća samo ako je broj grešaka manji od R/2, jer bi u suprotnom rastojanje do dve kodne reči moglo biti jednako, ili bi rastojanje do pogrešne kodne reči moglo biti manje od rastojanja do ispravne.

Postoji mogućnost otkrivanja grešaka i ispravljanja; kod koji je potreban da omogući ispravljanje G_K grešaka i detekciju daljih G_D grešaka mora imati minimalno rastojanje

$$R_n = 2G_K + G_D + 1$$

Određivanje minimalne udaljenosti koda upoređivanjem svakog para kodnih reči na osnovu navedene formule bilo bi dugotrajno za velike dužine kodnih reči. Stoga je uvedena minimizacija oblika da samo 2k važećih kodnih reči treba da se provere i da na osnovu toga minimalna Hemingova udaljenost linearnog bloka kodnih reči jednaka je minimalnoj Hemingovoj težini među njegovim kodnim rečima koje nisu nula. Hemingova težina kodne reči je jednostavno broj jedinica u njoj.

Hafova (Hough) transformacija - Osnovni pojmovi

Hafova transformacija je robusna tehnika procene parametara zasnovana na principu glasanja. Patentirao je *Paul Hough* 1962. godine kao metod određivanja orijentacije. U kompjuterskom obliku, Hafova transformacija pronalazi parametre nesavršenih primeraka date klase oblika. Prvobitno je korišćen za otkrivanje pravih linija, a kasnije je proširen na neke složenije parametarske oblike kao što su krugovi i elipse. Generalizovana Hafova transformacija, koju je opisao D. H. Ballard 1979. godine, generalizovana je za detekciju proizvoljnih parametarskih oblika [66]. Pre same detekcije oblika, šum na slici se obično uklanja i tražene informacije se naglašavaju filtriranjem, detekcijom ivica ili nekim drugim metodama. Primerci klase oblika su definisani n-tim parametrima. Svaki element slike (piksel) glasa za parametre svih oblika kojima bi mogao da pripada. Glasovi se sabiraju u akumulacionom polju čija dimenzionalnost zavisi od broja parametara koji definišu oblik. Traženi oblici se konačno nalaze kao maksimumi tog polja.

Karakteristike Hafove transformacije

Hafova transformacija u osnovi uključuje tri koraka. Prvi korak je pripremna obrada slike, odnosno otkrivanje primitivnih elemenata forme. Ne sadrže svi elementi slike podjednako vredne informacije. Stoga se pre procesa glasanja elemenata slike, po pravilu, na slici naglašavaju korisne informacije. Konkretno, na osnovu nekih lokalnih karakteristika izdvajaju se elementi koji bi mogli pripadati oblicima koji se otkrivaju. Najčešće se koristi detekcija ivica. Drugi korak je transformacija slike u parametarski prostor. Svaki od elemenata slike ekstrahovan u prvom koraku je mapiran u parametarski prostor predstavljen poljem akumulacije. Ako otkrijemo pravce Hafovom transformacijom, akumulaciono polje je dvodimenzionalno, ali dimenzionalnost polja raste sa povećanjem broja parametara koji definišu traženi oblik. Preslikavanje parametara oblika u polje akumulacije se postiže procesom glasanja. Najjednostavniji postupak glasanja je povećanje vrednosti u polju akumulacije na mestu čije su koordinate jednake paru (ili n-momentu) parametara traženog oblika. Treći i poslednji korak je detekcija lokalnih maksimuma. Rezultat drugog koraka je akumulaciono polje u kome se nalaze lokalni maksimumi na koordinatama koje predstavljaju parametre traženog oblika. Najlakši način da se izvuku takvi maksimumi je da se izdvoje sve vrednosti polja akumulacije koje prelaze datu graničnu vrednost. Zbog prisustva šuma i izobličenja

oblika, sami maksimumi mogu da se protežu kroz nekoliko elemenata akumulacionog polja, pa se često koriste metode za rast površine [67] Hafova transformacija može istovremeno otkriti više oblika na jednoj slici. Svaki maksimum polja akumulacije koji se uzima u obzir odgovara određenom broju parametara koji definišu pojedinačni detektovani oblik. Generalno razlikujemo dva oblika Hafove transformacije: jedan prema više (1: m) i više prema jednom (m: 1).

U obliku (1: m) svaki karakteristični element (x,y) prostora slike je povezan sa skupom od m elemenata u parametarskom prostoru koji predstavljaju m mogućih oblika koji prolaze kroz element (x,y). Ako se radi o detekciji pravolinijskih segmenata, idealno bi bilo da ova procedura dodeljuje svaki pravolinijski segment sastavljen od n elemenata tački (p, θ), koja ima vrednost n u prostoru parametara.

U obliku (m:1), m predstavlja broj elemenata potrebnih da se nedvosmisleno definiše parametarski oblik. Za pravolinijske segmente m je jednako 2 pošto su dve tačke dovoljne da se nedvosmisleno definiše pravac. Stoga je svaki par elemenata u prostoru slike povezan sa jednim elementom (p, θ), u parametarskom prostoru. Element (p, θ), određuje pravac koji prolazi kroz obe tačke u prostoru slike. U idealnom slučaju, pravolinijski segment u prostoru slike sastavljen od n elemenata slike je povezan sa jednom tačkom u prostoru parametara čija je vrednost jednaka $\frac{n \cdot (n+1)}{2}$ [67].

Jedna od ključnih prednosti Hafove transformacije je robusnost. Oblici na slici retko su potpuni prikazi oblika koje tražimo zbog zamućenja, šuma, ugla snimanja ili sličnih smetnji. Pored toga, prethodna obrada slike koja uklanja nepotrebne informacije sa slike generalno takođe uklanja neke korisne informacije. Sa Hafovom transformacijom, oblici se mogu pronaći čak i kada je dostupno znatno manje od polovine slikovnih elemenata koji ih definišu. Zahvaljujući ovoj osobini, moguće je pronaći potrebne oblike čak i kada su delimično prekriveni, zamućeni ili samo delimično odvojeni u pripremnoj obradi slike. Međutim, posledica takve robusnosti je velika verovatnoća pronalaženja malih nasumičnih struktura [68]. Takva pogrešna detekcija se može sprečiti ili smanjiti pažljivom analizom i pripremom korišćenih slika, kao i podešavanjem detekcije maksimuma lokalnog akumulacionog polja.

Pored robusnosti, jedna od prednosti Hafove transformacije je i mogućnost paralelnog računanja. Svaki element slike se obrađuje nezavisno od ostalih. Zahvaljujući tome, elementi slike

se mogu obraditi paralelno, što omogućava računanje u realnom vremenu na paralelnoj arhitekturi [67].

Najveći nedostatak Hafove transformacije su veliki zahtevi za raspoloživom memorijom. Zahtevi za transformaciju brzo rastu sa brojem parametara koji definišu traženi oblik. Prave imaju dva parametra, krugovi tri, a elipse čak 6, što znači da je akumulacijsko polje za detekciju elipsi 6-dimenzionalno. Računski zahtevi mogu se umanjiti korišćenjem informacija sa slike radi ograničavanja raspona mogućih parametara. *Ballard* [66]. opisuje kako optimizovati detekciju krugova koristeći gradijenta. Memorijski zahtevi se mogu redukovati podelom visoko dimenzionalnih problema u odvojene niže dimenzionalne. Metode redukovanja parametara takođe smanjuje memorijske zahteve.

Hafova transformacija za krugove

Elementi krive su definisani sa n parametara $\alpha_1 \dots \dots \alpha_n$, mogu se definisati jednakošću oblika:

$$f\big((\alpha_1 \dots \dots \alpha_n), (x, y)\big) = 0$$

Prateći gornju jednačinu, element slike (x,y) u prostoru parametara definiše hiper ravninu u n-dimenzionalnom prostoru parametara $(\alpha_1 \dots \dots \alpha_n)$.

Presek dobijenih hiper ravni predstavlja parametre koji najverovatnije karakterišu instancu željenog oblika u prostoru slike.

Za pravac, jednakost ima sledeći oblik:

$$f\big((\rho, \theta), (x, y)\big) = \rho - xcos\theta - ysin\theta = 0$$

$$f\big((x_c, y_c, r), (x, y)\big) = (x - x_c)^2 + (y - y_c)^2 - r^2 = 0$$

Tačke kruga (x,y) definisane su koordinatama centra (x_c, y_c) i poluprečnikom r tog kruga kao što je prikazano u jednačini.

$$f\big((x_c, y_c, r), (x, y)\big) = (x - x_c)^2 + (y - y_c)^2 - r^2 = 0$$

Parametarski možemo predstaviti jednačinu kruga kao:

$$x = x_0 + rcos\theta$$

$$y = y_0 + rsin\theta$$

Prema tome, koordinate u polju akumulacije mogu se izračunati pomoću jednačine:

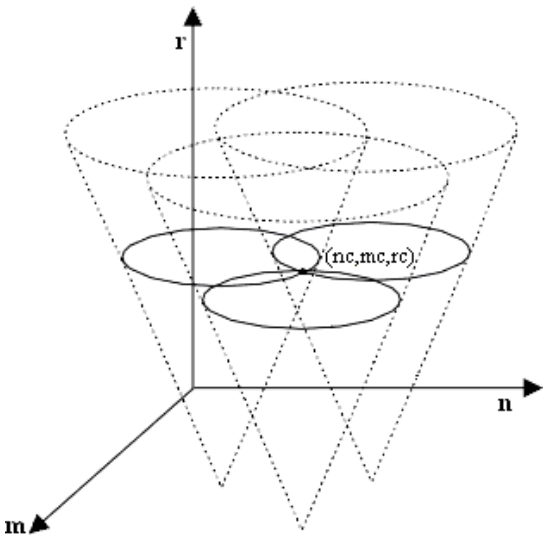
$$x_0 = x - rcos\theta$$

$$y_0 = y - rsin\theta$$

Gde je θ element iz intervala [0, 360], x_0 i y_0 su koordinate u akumulacionom polju, k i i su koordinate elemenata na slici, a r je poluprečnik kruga.

Na osnovu jednačine , svaki element (x,y) prostora slike pridružuje se konusnom omotaču koji u (x_c, y_c, r) parametarskom prostoru predstavlja sve kružnice koje prolaze kroz tačku (x,y). Svaki mogući poluprečnik odgovara tačno jednom krugu konične površine kao što je prikazano na slici 4-8.

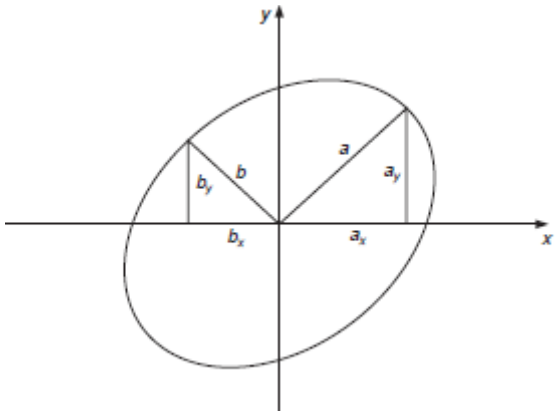
Hafova transformacija za krug u njegovom osnovnom obliku zahteva trodimenzionalno polje akumulacije (m, n, r), gde je $m \times n$ veličina slike, a r broj mogućih poluprečnika.



Slika 4-9 Hafova transformacija kružnica

Hafova transformacija za elipse

Slično krugu, elipsa se može parametrizovati sledećim vrednostima: $(x_0, y_0, a_x, b_x, a_y, b_y)$ kao što je prikazano na slici 4-9, [69]. Pošto je za definisanje elipse potrebno 6 parametara, Hafova transformacija za elipsu zahteva 6-dimenzionalni prostor parametara.



Slika 4-10 Hafova transformacija elipsa

Tačke elipse (x,y) definisane su koordinatama centra (x_c, y_c) i male i velike poluose a i b kao što je prikazano u jednačini.

$$\frac{(x - x_c)^2}{a^2} + \frac{(y - y_c)^2}{b^2} = 1$$

Parametarski, možemo prikazati jednačinu elipse kao:

$$x = x_0 + a_x cos\theta - b_x \sin\theta$$

$$y = y_0 + a_y cos\theta - b_y \sin\theta$$

Prema tome, koordinate u polju akumulacije mogu se izračunati pomoću jednačine:

$$x_0 = x - a_x cos\theta + b_x \sin\theta$$

$$y_0 = y - a_y cos\theta + b_y \sin\theta$$

Uspešnost Hafove transformacije

Uspeh Hafove transformacije zavisi od velikog broja konfiguracionih parametara. Ako posmatramo kružnicu , jedan od parametara je interval boja pri odvajanju elemenata slike, odnosno intervali nijanse, zasićenosti i intenziteta boje. Ako povećamo intervale parametara boje, algoritam će takođe pronaći znakove koji nisu jasno definisani bojom zbog različitih uticaja, ali će se tada pojaviti više smetnji. Pored boje, na rezultate utiče i podrazumevani radijus krugova koje tražimo.

Sledeći parametar od koga zavise rezultati je osetljivost na intenzitet slike pri izdvajanju centra kruga u akumulacionom polju. Ova osetljivost zapravo ukazuje koliko elemenata slike mora da glasa za centar da bismo ga izdvojili. U idealnim uslovima za krug sa debljinom ivice od jednog elementa slike (piksela), ova vrednost bi trebalo da bude oko $2r\pi$. Ako debljinu obima kruga označimo sa d, vrednost maksimuma za potpuno odvojen krug bi bila oko $d\pi(2r - d)$. Smanjenjem broja piksela koji moraju da glasaju za centar, algoritam postaje manje osetljiv na promene u prečniku, ali tada postaje i osetljiviji na smetnje. Takođe u slučaju smanjenja broja potrebnih glasova, algoritam će moći da detektuje znakove koji su zamućeni, imaju smetnje ili zbog kriterijuma boje ne mogu svi pikseli da glasaju za njih.

Minimalna veličina maksimalne površine u polju akumulacije koju biramo je kriterijum kojim generalno smanjujemo verovatnoću otkrivanja poremećaja kao znakova. Zavisi i od kvaliteta slike i veličine karaktera, a smanjenjem algoritama pronalazi manje uočljive karaktere, ali i druge smetnje sličnih boja.

4.2. Biometrija zasnovana na karakteristikama ponašanja

Biometrija zasnovana na karakterističnom ponašanju se opisuje kao nešto što korisnik može, ume, radi i slično. Za realizaciju se ne očekuje njegova osobenost koju poseduje rođenjem (otisak prsta, iris) već način kako izvršava neku karakterističnu radnju.

4.2.1. Autentifikacija na osnovu brzine kucanja

Brzina kucanja (*Keystroke dynamics authentication*) se zasniva na činjenici da je ritam i brzina kucanja različita od korisnika do korisnika i da kao takva može biti jedan od dobrih metoda za autentifikaciju zasnovanu na karakteristikama ponašanja. Ovaj pristup su predložili autori [70] uključuje pet karakteristika za identifikaciju korisnika

- *Typing speed* - brzina kucanja se meri brojem karaktera u minuti,
- *Flight time* - je vreme između pritiska dva tastera.
- *Keystroke seek time* - vreme koliko je taster pritisnut.
- *Characteristic sequences of keystrokes*- često kucane sekvence tastera za identifikaciju korisnika.
- *Characteristic errors*- meri zajedničke greške napravljene od strane korisnika koje se mogu identifikovani.

Na osnovu ovih karakteristika kreira se obrazac za poređenje koji se koristi za merenje sličnosti između karakteristika sačuvanih kao šabloni trenutnih merenja kao u jednačini [71].

$$r = \frac{\sum_{i=1}^{n}(k_i * t_i)}{\sqrt{\sum_{i=1}^{n} k_i^2 * \sum_{i=1}^{n} t_i^2}}, \text{ gde } i \in k, t$$

k je vektor dužine n koji memoriše karakteristike sačuvane kao šablon

t je vektor dužine n koji memoriše karakteristike trenutnih merenja

Analiza biometrijske metode kroz ocenu ispunjenosti aspekata

- Jedinstvenost: nizak stepen ispunjenosti
- Trajnost: nizak stepen ispunjenosti
- Prikupljivost: srednji stepen ispunjenosti
- Izvodljivost: visok stepen ispunjenosti
- Prihvatljivost: visok stepen ispunjenosti

4.2.2. Autentifikacija na osnovu stila pisanja

Stil pisanja je nesvesna navika i obrazac rečnik i gramatika mogu biti pouzdan indikator autorstva. Istraživanja stilometrijom obično ciljaju na tri različita problema, uključujući, identifikaciju autorstva odnosno autentičnost, verifikaciju autorstva, profilisanje ili karakterizaciju autorstva.

Autentičnost se sastoji od određivanja najverovatnijeg autora u određenom dokumentu od liste poznatih pojedinaca odnosno mogućih autora. Najstariji uspesi u pokušaju otkrivanja autentičnosti pisanja vezana su za autorstva Šekspirovih dela, rešena od strane Mendenhalla 1887. godine zatim studije od strane Mostlera i Wallace 1964. godine koji su ispitivali autentičnosti autorstva 12 poznatih engleskih pisaca primenom određenih statističkih metoda.

Studije o autentičnosti u današnje vreme su više koncipirane na istraživanja o načinima identifikovanja terorističkih komunikacija , otkrivanja autora određenih e-mail poruka, načinima sakupljanja digitalnih dokaze za forenzičke istrage ili rešavanje spornog književnog, istorijskog ili muzičkog autora

Treba napomenuti da verifikacija autorstava i otkrivanje plagijarizma nije isti zadatak. Verifikacijom autorstva utvrđuje se da li su dva dokumenta napisana od strane istog autora, dok kod detekcije plagijarizma, utvrđuje se stepen sličnosti između dva dokumenta koja su često ili skoro uvek iste tematike.

Verifikacija autorstva sastoji se od provere da li je ciljni dokument napisan ili ne od strane određenog autora. Postoji nekoliko radova o verifikaciji autora, a većina njih se fokusira na opšti

tekstualni dokument. Danas se često susrećemo sa pojmom autorskih prava naročito za dokumenta koja su objavljena na Internetu. Na uspešnu verifikaciju autorskog prava za *online* dokumenta utiče više faktora neki od njih su: veličina teksta, broj autora u tekstu, broj objavljenih tekstova autora odnosno uzorak, kao i činjenica da su dokumenti različito struktuirani za razliku od književnih radova.

Pretpostavka je da se verifikacija autorstva zasniva na proceni biometrijske informacije, gde posmatrani tekstovi predstavljaju biometrijski izvor, osnova za generisanje biometrijskog šablona tj. obeležja (engl. *features*), a metode za njihove odabire generišu se iz podgrupe obeležja koji imaju najmanju uzajamnu informaciju između tekstova različitih autora i maksimalnu uzajamnu informaciju za tekstove jednog autora [16]. Dobijena informacija predstavlja jedinstveni otisak ili karakteristiku određenog autora na osnovu koje je moguće verifikovati ili autentifikovati autora. Na primer, ako je uzajamna informacija velika, tada oba teksta pripadaju istom autoru ili ako je uzajamna informacija mala, tada tekstovi ne pripadaju istom autoru. Takođe, treba uzeti u obzir uzajamnu informaciju koja prirodno postoji između različitih autora.

Kompletan ovaj proces možemo lako uporediti sa biometrijskom autentifikacijom. Imajući na umu da možemo uz pomoć stilometrije da potvrdimo da dva teksta pripadaju istom autoru, to omogućava razvoj servisa autentifikacije na osnovu tekstova koje posedujemo i teksta na osnovu koga želimo da prepoznamo autora. Na osnovu svega navedenog, stilometriju ili stilometrijsku informaciju okarakterisaćemo kao još jedan potencijalni izvor biometrijske informacije na osnovu koje je moguće verifikovati autora. S tim, što količina informacije zavisi od dužine teksta, i iz tog razloga je jako važno pronaći uzorke koji će davati maksimalnu količinu informacije iz posmatranog teksta.

4.3. Biometrijski sistemi

Precizna automatska lična autentifikacije postaje sve važnija za rad elektronski povezanog informacionog društva. Sistemi kojima se pristupa zahtevaju potvrđivanje identiteta osobe pre nego što pristupi resursima. Biometrija je dugo bila poznata kao robustan pristup za autentifikaciju osoba. Sa novim napretkom tehnologije, biometrija postaje nova tehnologija za autentifikaciju pojedinaca. Biometrijski sistem identifikuje ili verifikuje osobu na osnovu njenih fizioloških karakteristika, kao što je otisak prsta, lice, otisak dlanova, ili karakteristike ponašanja kao što su glas, stil pisanja i hod.

Teoretski, bilo koja ljudska fiziološka karakteristika ili karakteristika ponašanja može se koristiti za stvaranje ličnosti identifikacija sve dok zadovoljava karakteristike kao što su univerzalnost, jedinstvenost, trajnost i konačno sakupljanje.

Za razliku od šema identifikacije zasnovanih na posedovanju i znanju, biometrijske identifikatori se ne mogu pogrešno postaviti, zaboraviti, pogoditi ili lako falsifikovati, neki primeri biometrijskih sistema su prepoznavanje otiska prsta, prepoznavanje lica, prepoznavanje otiska dlanova, glas prepoznavanje itd. Tradicionalni sistemi lične identifikacije zasnovani su na „Nešto što imamo ”npr. Ključ ili „Nešto što znamo“ npr. Lični identifikacioni broj [PIN], ali biometrija se oslanja na „nešto što jesmo“. Biometrijski sistemi koji se koriste u aplikacijama u stvarnom svetu su unimodalni.

Ovi unimodalni biometrijski sistemi oslanjaju se na dokaze jednog izvora podatke za autentifikaciju lica. Iako ovi unimodalni biometrijski sistemi imaju mnogo prednosti, mora se suočiti sa raznim problemima kao što su [72]:

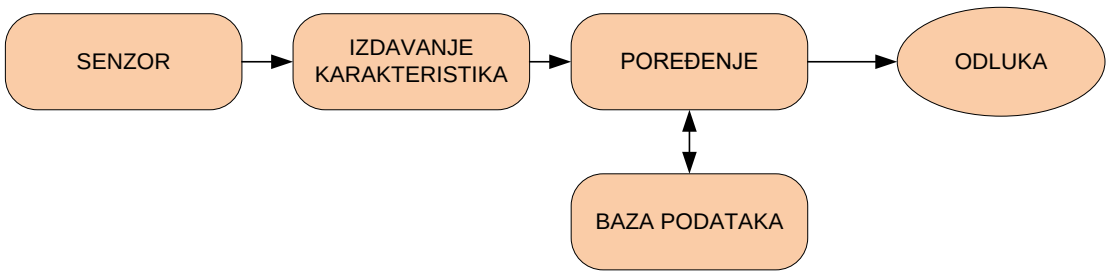
- Netačni podaci - podložnost biometrijskih senzora na buku dovodi do netačnog podudaranja, takvi podaci mogu dovesti do lažnog odbijanja.
- Varijacije unutar klase - biometrijski podaci prikupljeni tokom verifikacije neće biti identični na podatke koji se koriste za generisanje šablona tokom upisa pojedinca. Ovo je poznato kao varijacija unutar klase. Velike varijacije unutar klase povećavaju stopu lažnih odbijanja (FRR) biometrijskog sistema.

- Sličnosti među klasama - sličnost među klasama odnosi se na preklapanje prostora karakteristika odgovara više pojedinaca. Velike sličnosti među klasama povećavaju laž Stopa prihvatanja (FAR) biometrijskog sistema.
- Neuniverzalnost - neke osobe ne mogu obezbediti potrebnu samostalnu biometrijsku vrednost, zbog bolesti ili invaliditeta.
- Lažno predstavljanje - unimodalna biometrija je podložna lažiranju gde se podaci mogu imitirati ili duplirati.

Najbolje rešenje za prevazilaženje ovih problema sa unimodalnim biometrijskim sistemom je upotreba multimodalnog biometrijskog sistema koji se zasniva na više izvora informacija za ličnu autentifikaciju.

4.3.1. Teorijska osnova o biometrijskim sistemima

Biometrijski sistem je u suštini sistem za prepoznavanje uzorka biometrijskih podatka pojedinca. Sistem izdvaja skup značajnih karakteristika iz podataka, upoređuje ovaj skup uzoraka sa skupovima uzoraka sačuvanim u bazi podataka, i izvršava radnju na osnovu rezultata poređenja. Izgled biometrijskog sistema prikazan kroz module dat je na slici 4-11. Dakle, generički biometrijski sistem se može posmatrati kao da ima četiri glavna modula: cenzorski modul; modul za procenu kvaliteta i izdvajanje karakteristika; modul za poređenje; i modul baze podataka u kome su sačuvani uzorci [73].



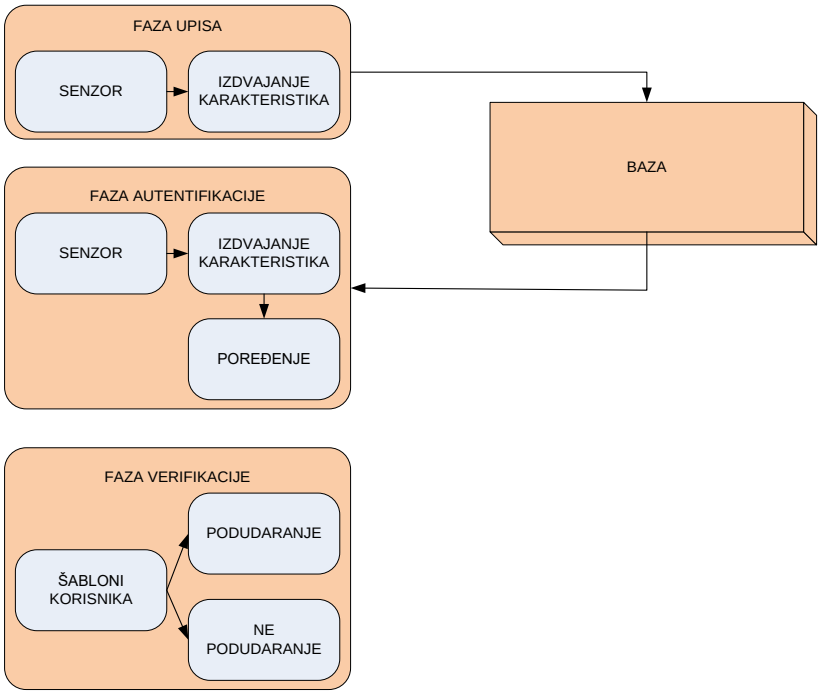
Slika 4-11 Biometrijski sistemi – moduli

U zavisnosti od uloge sistema, on može da funkcioniše u režimu verifikacije ili autentifikacije, primer sistema dat je na slici 4-12. U režimu verifikacije, sistem potvrđuje identitet osobe upoređivanjem snimljenih bioloških uzoraka sa sopstvenim biometrijskim šablonom ili šablonima koji su smešteni u sistemskoj bazi podataka. U takvom sistemu, pojedinac koji želi da bude verifikovan polaže pravo na identitet obično preko PIN-a, korisničkog imena ili pametne kartice, a sistem sprovodi poređenje jedan na jedan da bi se utvrdilo da li je tvrdnja istinita ili ne. Verifikacija se obično koristi za pozitivno prepoznavanje, odnosno cilj verifikacije je sprečavanje mogućnosti korišćenja istog identiteta od strane više osoba.

U režimu autentifikacije, sistem prepoznaje pojedinca pretraživanjem bioloških uzoraka svih korisnika u bazi podataka za podudaranje. Dakle, sistem sprovodi poređenje jedan-prema-više da bi ustanovio identitet. Autentifikacija je ključna komponenta u realizaciji negativnog prepoznavanja. u kojima sistem utvrđuje da li je to ta osoba (implicitno ili izričito). Nasuprot pozitivnom prepoznavanju, svrha negativnog prepoznavanja ogleda se u sprečavanju mogućnosti korišćenja različitih identiteta od strane iste odnosno jedne osobe.

Dok tradicionalne metode ličnog prepoznavanja kao što su lozinke, PIN-ovi, ključevi i tokeni mogu funkcionisati, uz pomoć biometrije se jedino mogu utvrditi pozitivno i negativno prepoznavanje.

Da bi ove dve navedene faze mogle da se realizuju, bitna je prvo realizacije faze upisa. Faza upisa je jedina faza koja ne radi nikakav vid provere. U ovoj fazi korisnik prilaže svoju biometrijsku jedinstvenost. Ovo se realizuje uz pomoć određenih senzora u zavisnosti od tipa biometrijskog sistema. Dobijena slika se pretvara u uzorak koji se uz određene informacije o samom korisniku, smešta u bazu podataka [73].



Slika 4-12: Biometrijski sistemi- faze

4.3.2. Performanse biometrijskih sistema

Stepen sličnosti između dva biometrijska skupa obeležja je naznačen ocenom sličnosti (engl. *matching score*). Rezultat podudaranja sličnosti je poznat kao pravi ili autentičan rezultat i dobija se kao rezultat podudaranja dva uzorka iste biometrijske osobine korisnika. Sa druge strane može se dobiti i rezultat nepodudaranja ukoliko se porede dva biometrijska uzorka koja potiču od različitih korisnika. Rezultat nepodudaranja koji premašuje prag prihvatanja μ (engl. *threshold)* zove se lažno prihvatanje (ili, lažno podudaranje), dok se rezultat podudaranja koji pada ispod praga prihvatanja μ zove lažno odbijanje (ili, lažno nepodudaranje).

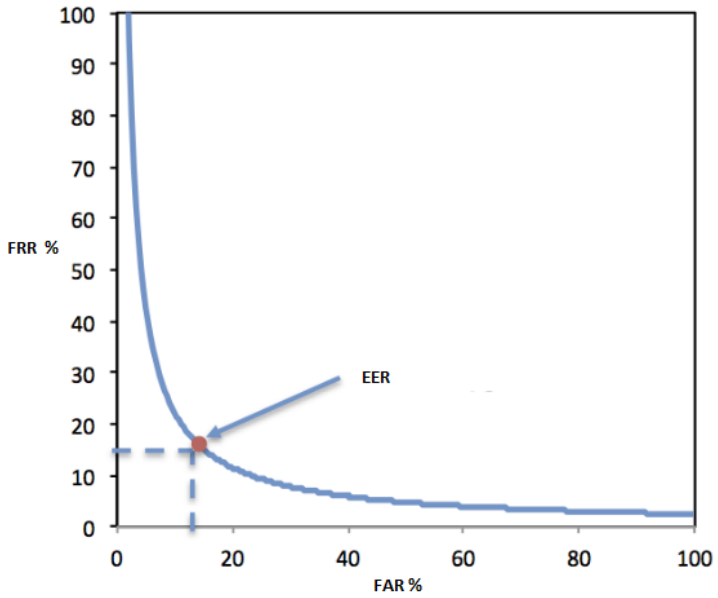
Stopa lažnog prihvatanja (FAR) ili stopa lažnog podudaranja (FMR) biometrijskog sistema se stoga može definisati kao deo rezultata prevaranta koji prelazi prag prihvatanja μ. Slično tome, stopa lažnog odbijanja (FRR) ili lažna stopa nepodudaranja (FNMR) sistema može se definisati kao deo pravih rezultata koji pada ispod praga prihvatanja μ. Striktno govoreći, u literaturi FMR i FNMR nisu uvek sinonim za FAR i FRR, respektivno.

Genuine Accept Rate (GAR) je deo pravih rezultata koji premašuju prag prihvatanja μ. Dakle, GAR = 1 – FRR.

Regulisanjem vrednosti praga prihvatanja μ menjaju se vrednosti FRR i FAR. Za biometrijski sistem nije moguće smanjiti obe ove greške istovremeno.

FAR i FRR pri različitim vrednostima praga prihvatanja μ mogu se sumirati pomoću *Detection Error Tradeoff* (DET) krive [74] koja prikazuje FRR u odnosu na FAR na različitim pragovima na skali normalnog odstupanja i interpolira između ovih tačaka.

Kada se linearna, logaritamska ili polu-logaritamska skala koristi za crtanje ovih stopa greške, onda je rezultujući grafikon poznat kao kriva radne karakteristike prijemnika (ROC) [75]. U mnogim slučajevima, ROC kriva prikazuje GAR (umesto FRR) u odnosu na FAR. Primarna razlika između DET i ROC krive je upotreba skale normalnog odstupanja u DET. Važno je napomenuti da pojava lažnih prihvatanja i lažnih odbijanja nije ravnomerno raspoređena među korisnicima biometrijskog sistema. Primer ROC krive dat je na slici u nastavku.



Slika 4-13Primer ROC krive [8]

Jedna od mera performansi koja se može dobiti na osnovu ROC krive je jednaka stopa greške (EER), koja odgovara tački gde FRR i FAR imaju istu vrednost.

Postoje inherentne razlike u prepoznatljivosti različitih korisnika. U literaturi se mogu pronaći četiri kategorije biometrijskih korisnika na osnovu ovih inherentnih razlika [76].

- Postoje korisnici čiji su biometrijski skupovi karakteristika veoma karakteristični i pokazuju male varijacije unutar klase. Stoga se od ovih korisnika očekuje da imaju mali broj grešaka lažnog prihvatanja i lažnog odbijanja.
- Postoje korisnici koji su skloni lažnim odbijanjima. Skupovi biometrijskih karakteristika takvih korisnika obično pokazuju velike varijacije unutar klase.
- Korisnici čiji se skup biometrijskih karakteristika u velikoj meri preklapa sa onima drugih pojedinaca. Biometrijski skupovi karakteristika ovih korisnika imaju male varijacije među klasama. Stopa lažnog prihvatanja povezana sa ovim korisnicima je obično visoka.
- Korisnici koji su uspešni u manipulisanju svojim biometrijskim osobinama (naročito osobinama ponašanja) kako bi se lažno predstavljali za legitimno upisane korisnike sistema. Stoga, ovi korisnici mogu povećati stopu lažnog prihvatanja sistema.

Performanse upisa se najbolje opisuju kroz vreme upisa (engl. *Time to Enroll*, TTE), predstavlja vreme koje je potrebno da se od početka procesa skeniranja dobije uzorak pojedinca u bazi podataka.

Greške na koje može naići jedan biometrijski sistem u fazi upisa a koje direktno utiču i na TTE su:

- Stopa neuspeha pri uzimanju informacija o korisniku (engl. *Failure to Acquire* , FTA), poznata je i kao neuspeh pri snimanju (FTC) označava odnos vremena kada biometrijski uređaj ne uspe da snimi uzorak i vremena dok traje preuzimanje karakteristika na uređaju. Ovaj tip greške je direktno vezan za same senzore koji se koriste u sistemu odnosno njihove karakteristike, habanja i slično
- Stopa neuspeha pri upisu (engl. *Failure to Enroll*, FTE) definiše se poput udela korisnika koji se ne mogu uspešno upisati u jedan biometrijski sistem. Obuka korisnika

može biti neophodna kako bi se osiguralo da pojedinac na odgovarajući način pristupi (u smislu korišćenja senzora) biometrijskom sistemu kako bi se olakšalo sticanje biometrijskih podataka dobrog kvaliteta. Ovo zahteva dizajn robusnih i efikasnih korisničkih interfejsa koji mogu pomoći pojedincu tokom upisa.

U sistemima mora postojati kompromis između FTE i same tačnosti sistema merene kroz greške FAR/FRR. FTE greške se obično javljaju kada sistem odbije unose lošeg kvaliteta tokom upisa, shodno tome, ako je prag kvaliteta visok, sistemska baza podataka sadrži samo šablone dobrog kvaliteta i percipirana tačnost sistema se poboljšava.

Sve navedene greške (tj. FTE, FTC, FAR, FRR) predstavljaju važne specifikacije performansi biometrijskog sistema i kao takve se koriste tokom evaluacije sistema.

Performanse biometrijskog sistema se takođe mogu sumirati korišćenjem drugih mera kao što je identična greška (engl. *Equal Error Rate*, EER) i indikator osetljivosti (engl. *d-prime value*). EER se odnosi na onu tačku na DET krivoj gde je FAR jednak FRR, dakle zaključuje se da niža EER vrednost, ukazuje na bolje performanse sistema.

Indikator osetljivosti meri razdvajanje između srednje vrednosti raspodele verovatnoća pravog i pogrešnog i njihovih standardnih devijacija, definisana je kao

$$d' = \frac{\sqrt{2}\left(\mu_{pravog} - \mu_{pogrešnog}\right)}{\sqrt{\sigma_{pravog}^2 + \sigma_{pogrešnog}^2}}$$

U formuli, vrednosti μ i σ su srednje vrednosti i standardne devijacije, respektivno, pravih i pogrešnih raspodela verovatnoća.

Veća vrednost indikatora osetljivosti ukazuje na bolje performanse. Ako obe raspodele zaista prate normalnu (Gausovu) distribuciju sa jednakom varijansom što je gotova nemoguća situacija u praktičnom biometrijskom domenu, onda se vrednost indikatora osetljivosti smanjuje na vrednost normalnog odstupanja.

Odnos greške se može definisati

$$F = \frac{\mu_{pravog} - \mu_{pogrešnog}}{\sigma_{pravog} + \sigma_{pogrešnog}}$$

Ako obe raspodele zaista prate normalnu (Gausovu) distribuciju onda se definiše zavisnost između EER i F kao

$$EER = \frac{1}{2} - \frac{1}{2} fg\left(\frac{F}{\sqrt{2}}\right)$$

U ovoj formuli $fg\left(\frac{F}{\sqrt{2}}\right)$ je funkcija greške, funkcija greške u zavisnosti od promenljive x glasi: $fg(x) = \frac{2}{\pi}\int_0^x e^{-t^2}\, dt$.

U slučaju autentifikacije, upoređuje se ulazni skup karakteristika sa svim šablonima dostupnim u bazi podataka kako bi se odredilo najbolje podudaranje. Najbolje podudaranje se može utvrditi ispitivanjem rezultata podudaranja, koji se odnose na sva poređenja i izveštavanjem o identitetu šablona koji odgovara najvećem rezultatu sličnosti. Stopa identifikacije pokazuje koliko puta je prethodno upisana osoba uspešno mapiranja na tačan identitet u sistemu.

	Biometrijski sistemi					
Faktori						
	Otisak prsta	**Lice**	**Dlan**	**Iris**	**Glas**	**Potpis**
Tačnost	Visok	Nizak	Visok	Visok	Srednji	Srednji
Jednostavan za korišćenje	Visok	Srednji	Srednji	Srednji	Visok	Visok
Cena	Nizak	Srednji	Visok	Visok	visok	Nizak
Privatnost	Visok	Visok	Srednji	Visok	Visok	Visok
Posebnost	Visok	Nizak	Visok	Visok	Nizak	Srednji
Faktori koji uzrokuju grešku	Godine	Okluzija	Godine	Ugao oka	Bolest	Nedoslednost
Prepreke za univerzalnost	Pohabanost grebena	Operacije	Pohabanost otiska	Oštećenje vida	Oštećenje govora	Falsifikovanje

Tabela 4-1: Pregled uticaja različitih faktora biometrijskog sistema

4.3.3. Multimodalni biometrijski sistemi

Multimodalni biometrijski sistemi kombinuju dve ili više biometrijskih osobina za prepoznavanje korisnika. Korišćenje dve ili više biometrijske poboljšava stopu uspešnosti procesa prepoznavanja korisnika. Multimodalni biometrijski sistem koriste senzore za prikupljanje i čuvanje neobrađenih podataka o korisniku. Različite vrste i složenost samih senzora omogućava da uzorci budu jedna ili više biometrijskih osobina. Na osnovu navedenog, za ovakve sisteme se može reći da su pouzdaniji u odnosu na sisteme koji koriste samo jednu biometrijsku osobinu.

U literaturi se mogu naći različite podele višemodalnih biometrijskih sistema. Jedna od podela koja se odnosi na interpretaciju ulaznih podataka data je u nastavku.

a) Sistemi sa više senzora - sistem sa više senzora koristi samo jedna određenu biometrijsku osobina sa tim što se ta osobina unosi u sistem putem više različitih senzora.

b) Sistem sa više jedinica - sistem sa više jedinica koristi više karakteristika sličnog dela tela kao biometrijske podatke. Sličnost dela tela se odnosi na: prste leve ruke, prste desne ruke, palac leve i desne ruke i slično.

c) Sistem sa različitim algoritmima - ovo je oblik sistema koji koriste iste ulazne podatke ali se obrađuju uz pomoć različitih algoritama.

d) Sistem sa više uzoraka - sistem sa više uzoraka koristi jednu određenu biometrijsku osobinu, ali dobija višestruku kopije istih biometrijskih podataka za klasifikaciju varijacije.

e) Višemodalni sistem - multimodalni sistem koristi dva ili više od dva različita biometrijska posebnost za identifikaciju pojedinca.

Multimodalni sistem ima tri različita režima rada.

- Serijski režim rada - u serijskom režimu rada identifikacija se vrši koristeći pojedinačne biometrijske podatke. Ako sistem ne može da identifikuje, koristi sledeću biometrijsku osobinu za identifikaciju.

- Paralelni režim rada - u paralelnom režimu, sistem koristi oba biometrijske osobine istovremeno za identifikaciju.

- Hijerarhijski režim rada - hijerarhijski režim podseća na struktura u obliku drveta. Ovaj režima je primenljiv kada je broj klasifikatora ogroman.

Primarni problem višemodalnog biometrijskom sistema je podešavanje tipa podataka koji treba da se na neki način sjedine, odnosno pomešaju (engl. *fusion*). U višemodalnom biometrijskom sistemu, fuzija može biti urađena u bilo kom od četiri biometrijska modula: u ulaznom modulu odnosno senzoru, modulu za izdvajanje karakteristika, u modulu za poređenje, u modulu za donošenje odluke.

Na osnovu navedenog proces sjedinjavanja odnosno fuzija se grubo može kategorisati na osnovu realizacije u različitim modulima, na:

1) fuzije pre modula za poređenje. Ova vrsta fuzije je primenljiva u fazi upisa i u fazi autentifikacije, što se postiže sjedinjavanje na nivou senzora ili na nivou izdvajanja karakteristika.

   - Fuzija na nivou senzora – ovaj vid sjedinjavanje se realizuje pošto se sirovi biometrijski podaci (engl. *raw data*) preuzmu sa različitih tipova senzora. Ovako ne obrađeni biometrijski podaci se spajaju pre njihove klasifikacije. Ova vrsta fuzije je pogodna samo za sisteme sa više senzora ili višemodalne biometrijske sisteme. Karakteristika ovakvog tipa fuzije je da se od sirovih podataka može kreirati biometrijski podatak poput slagalice ili mozaika (engl. *mosaicing*) [77].
   - Fuzija na nivou izdvajanja karakteristika – kod ove vrste fuzije izdvajaju se dva različita skupa biometrijskih podataka. Ova vrsta izdvaja dva različita skupa karakteristika. U ovom tipu fuzije konvertuje se konačan skup od N karakteristika u nov, drugačiji set karakteristika. Da bi se konverzija desila koriti se određeni algoritam ili algoritmi za izdvajanje i kreiranje novog seta karakteristika. Ako se izdvaja biometrijsku skup koristeći isti algoritam kaže se da su u pitanju homogene karakteristike , ako se koriste različite algoritam za izdvajanje karakteristika nazivaju se nehomogene.

2) fuzija nakon modula za poređenje. Ova vrsta fuzije je primenljiva samo tokom faze autentifikacije. Spajanje podataka nakon poređenja može realizovano na sledećim nivoima:

   - Fuzija na nivou rezultata (engl. *Score Level Fusion*) - rezultati podudaranja koje izlaze više biometrijskih uparivača koji su sređeni (unapred definisani) da bi se donela odluka o identitetu pojedinca. Rezultat podudaranja je rezultat poređenja dva skupa karakteristika ekstrahovanih korišćenjem istog ekstraktora. Tipično, ova procedura konsolidacije ima za cilj generisanje jednog skalarnog rezultata koji biometrijski sistem kasnije koristi [78].

   - Fuzija na nivoa opsega (engl. *Rank Level Fusion*) je metoda konsolidovanja više od dva rezultata identifikacije da bi se povećala pouzdanost lične identifikacije. U multimodalnim biometrijskim sistemima, ovaj model fuzije se može koristiti za kombinovanje biometrijskih poklapanja nastalih sa različitih biometrijskih modaliteta, na primer lice, otisak prsta, otisak dlana. Može se koristiti i za poboljšanje performansi u unimodalnom biometrijskim sistemima kroz kombinovanje višestrukih izlaza klasifikatora koji koriste različite klasifikatore, setove za obuku, različite arhitekture i slično [78].

   - Fuzija na nivou odluke (engl. *Decision Level Fusion*) – metoda u multimodalnoj biometriji sistema kod koje se kombinacija biometrijskih osobina radi na nivou odluke. Odluke se definiše uz pomoć logičke I ili logičke ILI operacije Rezultat logičkog I daje „Poklapanje“ (engl. *True*) samo kada su svi elementi uparivača isti kao ulazni podaci. Rezultati logičkog ILI daje rezultate „Poklapanje“ ukoliko je makar jedan element uparivača isti kao ulazni podaci [78].

Performanse multimodalnog biometrijskog sistema

Kroz radove različitih autora gde su data rešenja različitih multimodalnih biometrijskih sistema pokazano je da multimodalna biometrija ima potencijal da prevaziđe ograničenja bilo koje pojedinačne biometrijske tehnologije u poboljšanju nivoa bezbednosti sistema i sprečavanju lažiranja. Tehnologija fuzije informacija može se primeniti na različitim nivoima i na različite načine u multimodalnim biometrijskim aplikacijama. Izazov leži u pronalaženju smislenog

operativnog opsega da ne umanji udobnost korisnika ali da poveća tačnosti uzoraka. Procenjene su stope greške biometrijske fuzije. Rezultati pokazuju da je učinak sumarnog pristupa superiorniji u odnosu na spajanje dva modaliteta nezavisno. Dalja istraživanja ukazuju da rezultat zavisi od različitih pristupa multimodalne biometrijske fuzije, da treba proceniti stope grešaka pre nego što se integrišu različite fuzije u biometrijskim aplikacijama.

U praksi postoji mnogo multimodalnih biometrijskih sistema za prepoznavanje pojedinca, izbor odgovarajućeg modela, izbor optimalnog nivoa fuzije i redundantnost ekstrahovanih karakteristika i dalje su neki od nedostataka sa kojima se različiti autori u svojim radovima suočavaju.

U disertaciji su razmotreni različiti pristupi koji su mogući u multimodalnim biometrijskim sistemima, odgovarajući nivoi fuzije i strategije integracije koje se mogu izabrati za konsolidaciju informacija. Multimodalna biometrija takođe rešava problem lažiranja što se tiče sa više osobina ili modaliteta, prevarantu bi bilo veoma teško da prevari ili napadne više osobina istinskog korisnika istovremeno. U principu, stopa stvarne prihvatljivosti [GAR], stopa lažnih odbijanja [FRR], stopa lažnog prihvatanja [FAR] i jednaka stopa grešaka [ERR] koriste se za merenje tačnosti sistema.

Kombinacija više od jedne biometrije može se primeniti za poboljšanje bezbednosti. Performanse i napredni nivo bezbednosti učinili su multimodalne biometrijske sisteme popularnim u današnje vreme. Visoka tačnost se može postići korišćenjem različitih metoda u procesu selekcije karakteristika.

„ I just wondered how things were put together. “

Claude Shannon

5. *Predlog sistema za generisanje kriptoloških ključeva na osnovu više biometrijskih modaliteta*

U petom poglavlju disertacije predstavljena je jedna klasa biometrijskog sistema koji koristi više biometrijskih modaliteta u svrhu generisanja kvalitetnih kriptoloških ključeva dovoljnih dužina za primenu u kriptografskim šiframa u 21 veku. Analizirane su pojedinačne komponente sistema merenjem performansi u cilju pokazivanja da je ovaj sistem prihvatljiv za upotrebu. Prikazani su svi eksperimentalni rezultati. Urađena je bezbednosna analiza sistema.

U ovom poglavlju predstavljen je novi hibridni višemodalni biometrijski sistem. Predloženi sistem koristi jedan biometrijski izvor za generisanje kvalitetnog kriptografskog ključa i drugi biometrijski izvor za servis autentifikacije. Na ovaj način ostvareni su pozitivni efekti na robusnost, privatnost i nisku stopu lažnog prihvatanja.

U skladu sa ciljevima dizajna, sistem koristi tabelu u kojoj čuva heš vrednosti ključeva generisanih tokom faze upisa i biometrijske šablone koji se mogu poništiti, a koriste se za autentifikaciju. Ovim je postignuta veća bezbednost sistema, a prevashodno se ogleda u činjenici da napadač ne može dobiti tajni ključ ili biometriju namenjenu za autentifikaciju, jer se podaci skladišteni u tabeli transformišu neinverzibilnim funkcijama.

Evaluacija predloženog okvira sistema koji koristi iris biometriju za generisanje ključa i biometriju otisaka prsta za servis autentifikacije, sprovedena je preko biometrijskih uzoraka iz CASIA baze podataka.

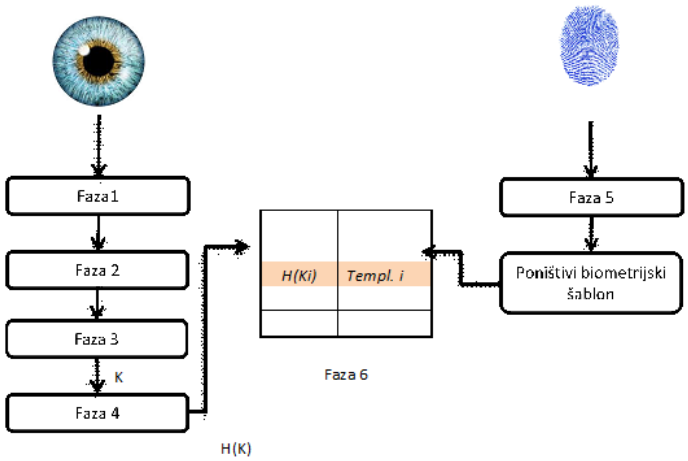
Glavni doprinos predloženog rešenja je kombinovanje dva unimodalna sistema čime je stvoren višemodalni sistem za autentifikaciju i generisanje ključa.

5.1. Predloženo rešenje

U ovom delu detaljno je objašnjena generička šema predloženog rešenja. Okvir predloženog rešenja postiže visok nivo tačnosti u svim svojim funkcionalnostima. Na slici 5-1 predstavljena je faza upisa, a na slici 5-2 faza autentifikacije. Tokom faze upisa, korisnik sistema prosleđuje dva biometrijska uzorka za funkcionalnost sistema. Funkcija jednog je generisanje tajnog ključa, dok je drugi u funkciji servisa autentifikacije.

Faza upisa korisnika sistema se sastoji od sledećih koraka koji su navedeni na slici:

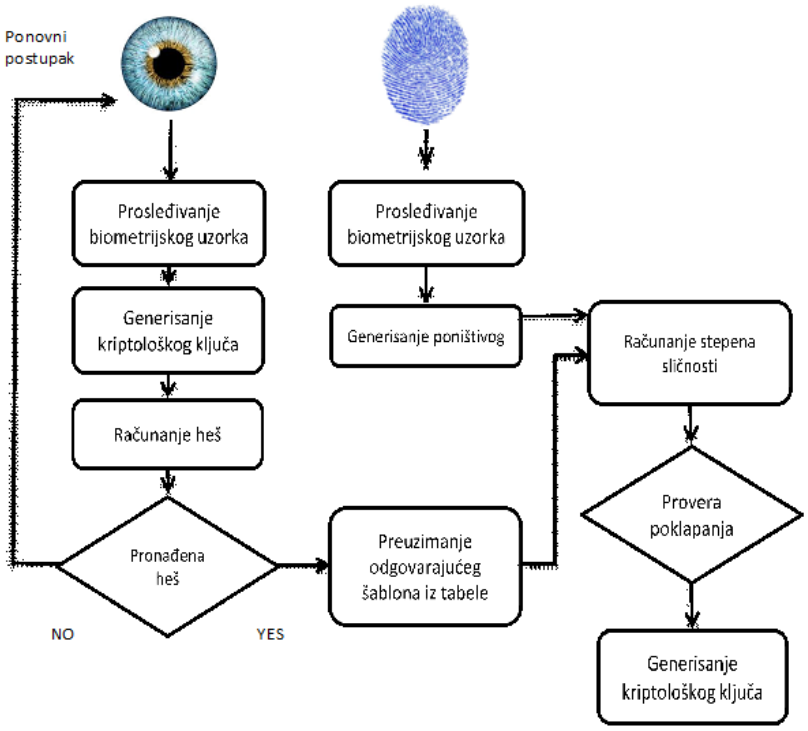
- Faza 1 - uz upotrebu senzora očitavaju se biometrijski podaci koji se koriste za generisanje ključa;
- Faza 2 - obrađuju se podaci, izdvaja se biometrijska informacija;
- Faza 3 - generiše se ključ iz poništivog biometrijskog šablona;
- Faza 4 - računa se heš vrednost generisanog ključa;
- Faza 5 - uz upotrebu senzora očitavaju se biometrijski podaci koji se koriste za proces autentifikacije;
- Obrađuju se podaci, izdvaja se biometrijska informacija i generiše se poništivi biometrijski šablon primenom neinvertibilne funkcije.
- Faza 6 - heš vrednost generisanog ključa i generisan poništivi biometrijski šablon se potom skladište u memoriju - namensku bazu podataka.



Slika 5-1 Predloženo rešenje – faza upisa

U fazi autentifikacije, korisnik prosleđuje sistemu dve biometrije sa dva različita modaliteta. Sistem obavlja jednake operacije kao i u fazi upisa korisnika u sistem. Jednom kada je generisana heš vrednost ključa i poništivi biometrijski uzorak, iz prosleđenog biometrijskog uzorka sistem zahteva odgovarajući heš .

Ako nema poklapanja heš vrednosti, sistem odbija korisnika ili zahteva ponavljanje istog procesa. U drugom slučaju, sistem računa stepen sličnosti između biometrijskih uzoraka. Na osnovu stepena sličnosti sistem odlučuje da li da regeneriše ključ ili ne.



Slika 5-2 Faza autentifikacije

Možemo zaključiti da se ključ generiše pod sledećim uslovima:

- izračunata heš vrednost iz biometrijskog uzorka nalazi se u tabeli koja pamti heš vrednost ključa;
- da procenat sličnosti, izračunat između generisanog šablona i one zapamćene u *look-up* tabeli, bude manji u odnosu na definisani prag.

5.2. Implementacija predloženog rešenja

U predloženom rešenju upotrebljena su dva biometrijska izvora, iris i otisak prsta. Kao što je već opisano, iris se koristi za generisanje tajnog kriptološkog ključa, dok se otisak prsta koristi za autentifikaciju korisnika. Konvencionalne metode koje su iskorišćene za generisanje ključa na osnovu iris biometrije, kao i izdvajanje karakterističnih tačaka iz otiska prsta, su dobro poznate i najčešće korišćene metode, takođe, detaljno opisane u radovima mnogih istraživača koji se bave ovom naučnom oblasti.

Poništivi šablon se generiše iz uzorka i efikasne neinvertibilne ćelije pomešan po predlogu autora, što je modifikacija bez ključa Dekartove transformacije.

5.2.1. Generisanje tajnog ključa na osnovu biometrije irisa

Iris predstavlja biometrijski izvor koji sadrži najveću količinu informacije u poređenju sa drugim modalitetima koji su danas aktuelni i koriste se u svrhu razvoja različitih sistema. U pogledu karakteristika, iris prema *Dagmanu* [63] raspolaže sa više od 250 stepeni slobode (engl. *Degrees of freedom*) u informativnom smislu. To je neuporedivo više u odnosu na otisak prsta za koji se u novijim istraživanjima mogu naći podaci do 26 stepena slobodne za sve prste jedne šake [12]. Međutim, zahtevani su određeni predprocesi koji su uslov za generisanje tajnog ključa irisa.

Ukratko, spoljašnji radijus uzorka irisa i zenica su prvo lokalizovane sa *Hafovom* transformacijom koja uključuje pametan detektor ivice da generiše mapu ivica. Slabo lokalizovan iris rezultovaće neuspešnom podelom, a to će uvesti veliki šum u podacima, a sve to će se odraziti na proces regenerisanja ključa. Ovaj korak je od izuzetne važnosti u fazi upisa, iz razloga što može uticati negativno na stopu lažnog odbacivanja (*FRR*) za legitimne korisnike i izazvati nešto što se može manifestovati u pogledu opterećenja računarskog resursa slično *DOS* napadu.

Hafova transformacija identifikuje pozicije krugova i elipsa [66]: locira konture u n - dimenzionalnom prostoru ispitivanjem da li leže na krivama određenog oblika. *Hafova* transformacija za granice spoljašnjeg i unutrašnjeg kruga i seta od n oporavljenih tačaka (x_i, y_i) se definiše na sledeći način:

$$H(x_c, y_c, r) = \sum_{i=1}^{n} h(x_i, y_i, x_c, y_c, r)$$

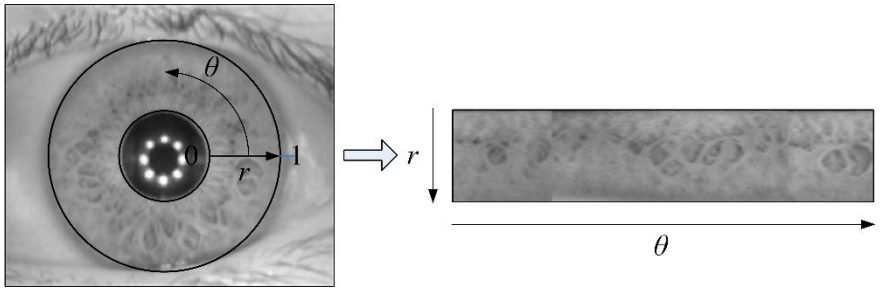
$$h(x_i, y_i, x_c, y_c, r) = \begin{cases} 1, (x_i - x_c)^2 + (y_i - y_c)^2 - r^2 = 0 \\ 0, (x_i - x_c)^2 + (y_i - y_c)^2 - r^2 \neq 0 \end{cases}. \quad (1)$$

Krug (x_c, y_c, r) koji prolazi kroz svaku tačku ivice (x_i, y_i) je definisan kao

$$(x_i - x_c)^2 + (y_i - y_c)^2 = r^2.$$

Triplet koji maksimizuje $H(x_c, y_c, r)$ je zajednički za većinu tačaka ivica i odgovoran je za izbor koji predstavlja konturu od interesa. Slična tehnika koja koristi parabolične lukove koristi se za otkrivanje gornjih i donjih kapaka. Jednom kada se lokalizuje slika irisa, region od interesa je definisan i transformiše se unutar pravougaone slike fiksne veličine. Proces normalizacije obavlja se uz pomoć *Dagmanov - rubber sheet* modela koji preslikava sliku irisa $I(x, y)$ iz dekartovog (x, y) u polarni koordinatni sistem (r, θ) :

$$I\big(x(r,\theta), y(r,\theta)\big) \rightarrow I(r,\theta)$$



Slika 5-3 Preslikavanje slike irisa iz dekartovog u polarni koordinatni sistem [64]

Parametar r je u granicama od [0, 1] a θ je ugao u opsegu [0, 2π]. Ako su iris i zenica u granicama θ zapisuju se kao (x_i, y_i) i (x_p, y_p), redom, transformacija se vrši prema:

$$x(r,\theta) = (1 - r)x_p(\theta) + x_i(\theta),$$

$$y(r,\theta) = (1 - r)y_p(\theta) + y_i(\theta).$$

Iako se u literaturi navode različite metode ekstrakcije, diskriminantne osobine se ekstraktuju iz normalizovanog irisa koristeći konvencionalnu metodu baziranu na *Gabor* filterima. Ova metoda je pokazana i priznata kao pogodna metoda izdvajanja u različitim istraživanjima drugih autora. Normalizovana slika je razbijena u broj 1-D signala koji su savijeni sa 1-D Gabor talasima. Frekvencijski odziv 1-D log-Gabor filtera [64], dat je sa

$$G(f) = e^{\frac{-\left(\log\frac{f}{f_0}\right)^2}{2\left(\log\frac{\sigma}{f_0}\right)^2}},$$

gde f_0 predstavlja centralnu frekvenciju , a σ predstavlja opseg filtra. Kvantizacija je primenjena na 4 nivoa filtriranja izlaza (svaki nivo kreira 2 bita podataka za svaki fazor). Kvantizacioni nivoi se koriste za kodovanje uzoraka irisa biometrijskog šablona. EER se generise korišćenjem *Reed-Solomonovog* algoritma a šablon se pretvara u ključ. Broj bitova u biometrijskom uzorku zavisi od ugaone i radijalne rezolucije i broja korišćenih filtera, dok entropija šablona zavisi od broja korišćenih filtera, njihovih centralnih frekvencija i parametara filtra.

5.2.2. Izdvajanje karakterističnih tačaka

Karakteristične tačke se izdvajaju iz otiska prsta pre generisanja poništivog biometrijskog šablona. Ova procedura se sastoji od nekoliko koraka: predobrada, segmentacija, procena orijentacionog polja, poboljšanje slike i ekstrakcija detalja. Prva operacija primenjena na dobijeni uzorak je izjednačavanje histograma, što povećava lokalni kontrast slike. Vinerov filter uklanja zamućenje i aditivni šum sa slike bez promene strukture biometrijskog uzorka otiska prsta. Neka $H(u,v)$ označava Furijeovu transformaciju tačke rasprostiranja funkcije $h(x,y)$ i neka $H^*(u,v)$ označava konjugovano kompleksnu funkciju degradacije, Vinerov filter [79] u frekventnom domenu se može predstaviti:

$$W(u,v) = \frac{H^*(u,v)}{|H(u,v)|^2 + \frac{P_n(u,v)}{P_s(u,v)}}$$

gde $P_n(u, v)$ označava spektar šuma i $P_s(u, v)$ je spektar slike $f(x, y)$. Ako je zamućenje zanemarljivo i potrebno je ukloniti samo aditivni šum, filter ima oblik:

$$W(u,v) = \frac{P_s(u,v)}{P_s(u,v)+{\sigma_n}^2},$$

gde σ_n^2 predstavlja varijansu šuma. Izlaz Viner filtera je podeljen na blokove koji se ne preklapaju i koji su jednakih veličina. Neka N označava veličinu bloka i $\mu(I)$ srednju vrednost piksela bloka. Blok I se smatra blokom u prvom planu ako je njegova varijansa veća od praga τ_s:

$$\sigma^2(I) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\big(I(i,j) - \mu(I)\big)^2 > \tau_s.$$

Ovaj proces se naziva segmentacija i koristi se za razdvajanje interesnih regiona od ostatka slike. Sledeći korak u procesu ekstrakcije je procena orijentacionog polja. Pristup proceni polja orijentacije koji se koristi u ovom istraživanju zasniva se na gradijentu. Gradijenti vektori ukazuju na najveće odstupanje intenziteta sive boje koje je normalna na ivicu . Neka g_x i g_y označavaju gradijente vektore bloka centriranog u piksel (i, j) u horizontalnom i vertikalnom pravcu. Orijentacija θ svakog bloka je data:

$$\theta = \frac{1}{2}tan^{-1}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}2g_x(i,j)g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\big({g_x}^2(i,j)-{g_y}^2(i,j)\big)}\right) + \frac{\pi}{2}.$$

Slika je poboljšana Gausovim niskopropusnim filtrom, a zatim 2-D Gabor filtrom. Neka f_0 označava frekvenciju opsega, θ orijentaciju filtera, σ_x i σ_y standardne devijacije Gausove anvelope duž x i y ose, i [x_θ, y_θ] koordinate [x, y] nakon rotacije u smeru kazaljke na satu oko Dekartove ose sa 0.5π–θ. 2-D Gabor-ov filter daje:

$$G(x,y,\theta,f_0) = e^{-\frac{1}{2}\left(\frac{{x_\theta}^2}{{\sigma_x}^2}+\frac{{y_\theta}^2}{{\sigma_y}^2}\right)}cos(2\pi f_0 x_\theta),$$

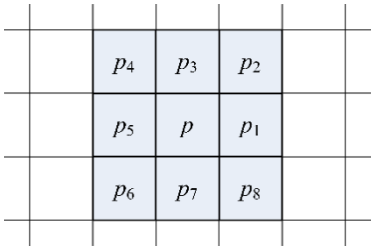
$$x_\theta = x\,sin\,\theta + y\,cos\,\theta,$$

$$y_\theta = -x\,cos\,\theta + y\,sin\,\theta.$$

Kako algoritmi za ekstrakciju karakterističnih tačaka rade na binarnim slikama, izlaz za filtriranje je binarizovan. Nivo sivila svakog piksela se upoređuje sa globalnim pragom, što dovodi do toga da slika ima dva nivoa od interesa: crni pikseli i beli pikseli. Morfološki operatori se dalje primenjuju na binarizovanu sliku kako bi se eliminisao šum koji nastaje zbog prekida linija.

Algoritam stanjivanja smanjuje širinu karakterističnih linija. Slika se segmentira na dva podpolja kao u šablonu na šemi.

Neka p_1, p_2, ... p_8 [0, 1] označavaju susedne piksele piksela p, kao što je prikazano na slici 5-4, i neka b_i=1 ako: $p_{2i-1} = 0 \wedge (p_{2i} = 1 \vee p_{2i+1} = 1)$.



Slika 5-4 Susedni pikseli u odnosu na p

Broj prelaza $X_H(p)$, je broj puta kada se prelazi iz bele do crne tačke, kada se tačke prelaze redom. Četiri uslova uklanjanja piksela koji se koriste u iteracijama algoritma definisani su na sledeći način:

$$X_H(p) = \sum_{i=1}^{4} b_i = 1.$$

$$2 \leq min\{(\sum_{i=1}^{4} p_{2i-1} \vee p_{2i}), (\sum_{i=1}^{4} p_{2i} \vee p_{2i+1})\} \leq 3.$$

$$(p_2 \vee p_3 \vee \overline{p_8}) \wedge p_1 = 0.$$

$$(p_6 \vee p_7 \vee \overline{p}) \wedge p_5 = 0.$$

Uslov XH(p)=1 podrazumeva da je p konturna tačka. Svaka iteracija algoritma ima dve poditeracije. Piksel p se briše iz prvog podpolja u prvoj pod-iteraciji samo ako su zadovoljeni uslovi u prve tri formule Piksel p se briše iz drugog podpolja u drugoj poditeraciji samo ako su zadovoljeni uslovi prve dve i poslednja formula. Rezultat algoritma je slika sastavljena od linija širine jednog piksela, sa jasno vidljivim završecima grebena i bifurkacijskim tačkama. Broj prelaza XR(p) se izračunava za svaki piksel u rezultujućoj slici, prema definiciji Rutovitza, kao broj prelaza iz bele u crnu i obrnuto kada se tačke prelaze redom.

Piksel p je identifikovan kao tačka završetka grebena ako:

$$X_R(p) = \sum_{i=1}^{8} |p_{i+1} - p_i| = 2.$$

Piksel p je identifikovan kao bifurkaciona tačka ako:

$$X_R(p) = \sum_{i=1}^{8} |p_{i+1} - p_i| = 6.$$

5.2.3. Generisanje poništivog šablona

Neinvertibilne transformacije se koriste za očuvanje privatnosti biometrijskih šablona. Transformacija proizvodi poništivi šablon koji ne odgovara pravoj biometriji, a original se ne može rekonstruisati iz poništivog šablona, što odgovara rezultatu jednosmernih funkcija. Ako je uskladišteni šablon kompromitovan, novi poništivi šablon generiše se promenom parametara, tj. karakteristika izobličenja neinvertibilne transformacije. Transformacija koja se primenjuje na šablonu otiska prsta je invertibilna ako su pozicije post-transformacionih detalja nakon toga visoko korelisane sa pozicijama karakterističnih tačaka pre transformacije. Prema pomenutom, cilj transformacije je da se maksimalno eliminiše korelisanost karakterističnih tačaka. Pored toga, potrebna je tolerancija na napade grubom silom.

Neka (xi, yi), i=1, ... n označavaju koordinate karakterističnu tačku i za n identifikovanih karakterističnih tačaka. Dvodimenzionalni vektori ekstraktovanih karakterističnih tačaka je dat kao:

$$F = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}.$$

Neinvertibilnost z predložene transformacije dolazi od premeštanja ćelija. Koordinatni sistem je podeljen na N_x x N_y ćelija, od kojih svaka sadrži n_{xy} karakterističnih tačaka. Ćelije se mešaju na sledeći način: klizno pomeranje na desno se izvodi za svaku ćeliju prema broju karakterističnih tačaka u toj ćeliji. Kada se završi ova faza, na isti način se vrši rotiranje. Više od jedne ćelije se može preslikati u istu ćeliju nakon transformacije, pošto pomeranje zavisi od broja tačaka u ćeliji i nijedan ključ se ne koristi kao matrica transformacije. Transformacija u ovom trenutku nije obrnuta, jer je nemoguće odrediti originalnu ćeliju karakteristične tačke.

Ova transformacija takođe zadovoljava uslove lokalnog omekšanja. Snaga transformacije zavisi od broja ćelija: protivnik koji izvodi brutalni napad mora pokušati $(N_x N_y)^{NxNy}$ mogućnosti.

(x^T_i, y^T_i), i=1, ... n označavaju koordinate karakterističnih tačaka i nakon premeštanja ćelija. Generisanje poništivog šablona dato je :

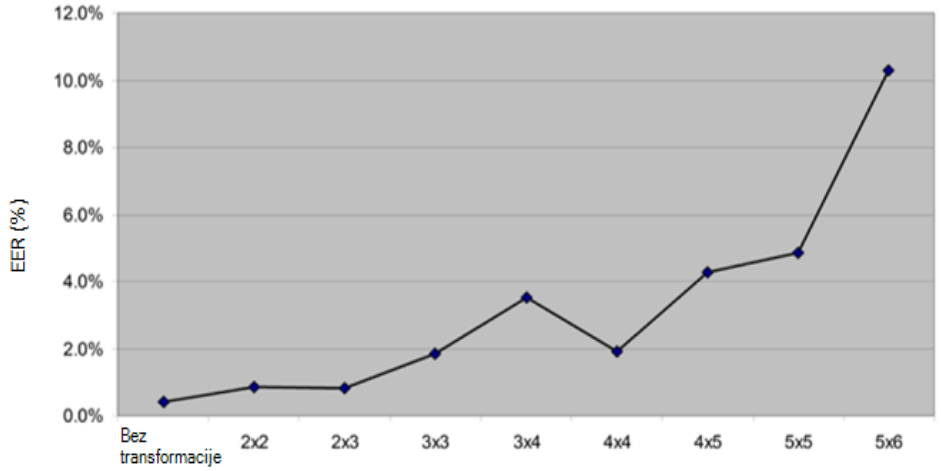
$$F^T = \{(x^T{}_1, y^T{}_1), (x^T{}_2, y^T{}_2), \ldots, (x^T{}_n, y^T{}_n)\}.$$

Šabloni se uparuju u fazi autentifikacije odbacivanjem nedostajućih tačaka, izračunavanjem sume kvadratnih razlika između dva vektora, normalizovanih sa brojem preostalih vrednosti koje nisu odbačene, i poređenjem rezultata podudaranja sa pragom.

5.3. Eksperimentalni rad

Evaluacija predloženog sistema je eksperimentalno sprovedena u razvojnom okruženju MATLAB-a (verzija R2011b). Eksperimentalni rad ne uključuje hardver namenjen za prikupljanje biometrijskih uzoraka. Za potrebe eksperimenta, ulazni podaci su preuzeti iz biometrijskih korpusa CASIA-IrisV4 i CASIA-FingerprintV5 [10], koje je prikupio Institut za automatizaciju Kineske akademije nauka. Treba napomenuti da različita eksperimentalna okruženja mogu dovesti do pozitivnih ili negativnih efekata u varijaciji u parametra FAR, i entropiju sistema koja je ključni parametar za postizanje visokog kvaliteta u svim radnim režimima. Podskup slike irisa koji je korišćen u eksperimentima sadrži 500 uzoraka od 50 osoba. Svaka slika se normalizuje u 8-bitnu sliku od 240x20 piksela, a zatim se primenjuje 1-D log-Gabor filter sa σ=0,5 i centralnom talasnom dužinom od λ=12 piksela, što rezultuje šablonom od 9600 bita. Utvrđeno je da ovi parametri obezbeđuju visoku lokalnu entropiju (u biometrijskoj informaciji) i optimalno kodovanje u bazi podataka CASIA.

Podskup slika otiska prsta koji se koristio u eksperimentima sadrži 500 uzoraka od 50 osoba, sa rezolucijom od 328x356 piksela. Optimalan broj ćelija korišćenih u neinvertibilnoj transformaciji je izabran kao kompromis između bezbednosti šablona za napade grubom silom i jednake stope grešaka EER, kao što je prikazano na slici 5-5.



Slika 5-5 Određivanje optimalnog broja ćelija u neinvertibilnoj transformaciji

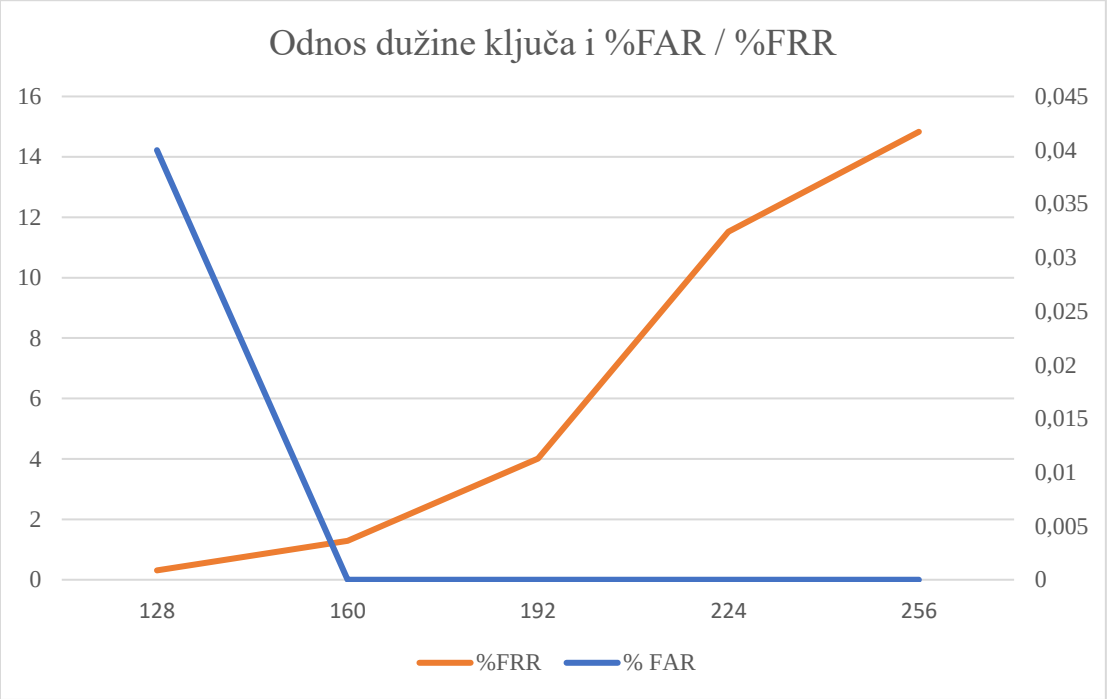
Na osnovu slike, može se zaključiti da je optimalan broj ćelija koje se koriste u neinvertibilnoj transformaciji 4x4, uočava se da je za navedenu transformaciju EER skoro 2% (1 odbijanje u 50 pokušaja autentifikacije) i dovoljnim nivoom sigurnosti biometrijskog šablona.

Generisano je inicijalno pet look-up tabela za različite dužine ključeva, od kojih svaka sadrži 50 redova heš vrednosti za ključeve, ispravne kodove iz izlaza Red-Solomon algoritma i poništive šablone generisane iz jedne slike otiska prsta za svaku osobu.

Inicijalna evaluacija sistema odnosi se na parametar FAR i FRR koji su od velikog značaja za stvarnu primenu ovakvih sistema. U tabeli ispod prikazane su vrednosti dobijene za različite dužine ključeva u bitovima, bez verifikacije heš vrednosti.

Dužina ključa	**% FAR**	**%FRR**
128	0,04	0,31
160	<0,01	1,29
192	0,00	4,01
224	0,00	11,52
256	0,00	14,83

Tabela 5-1 % FAR i % FRR u odnosu na dužinu ključa

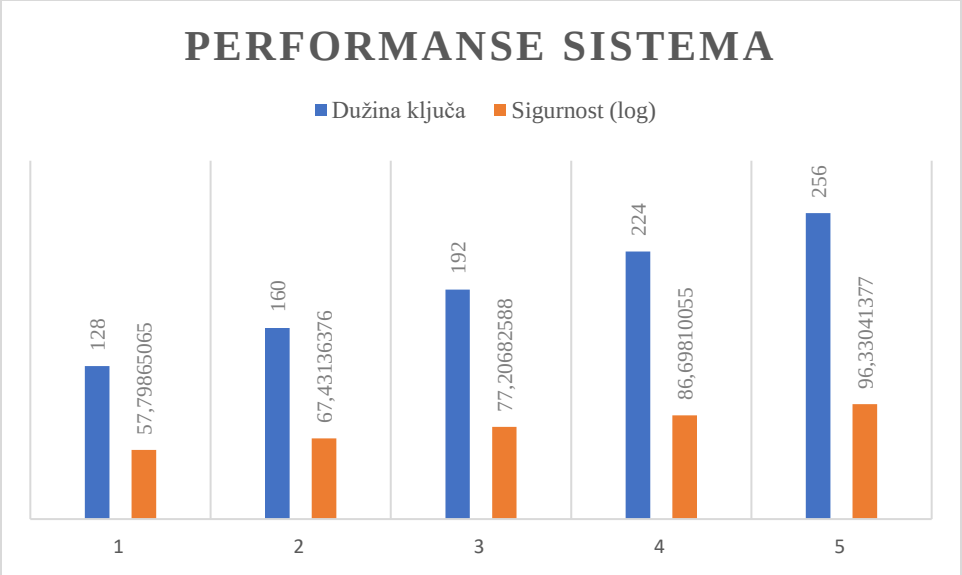


Slika 5-6 Grafički prikaz dužine ključa u odnosu na % FAR i %FRR

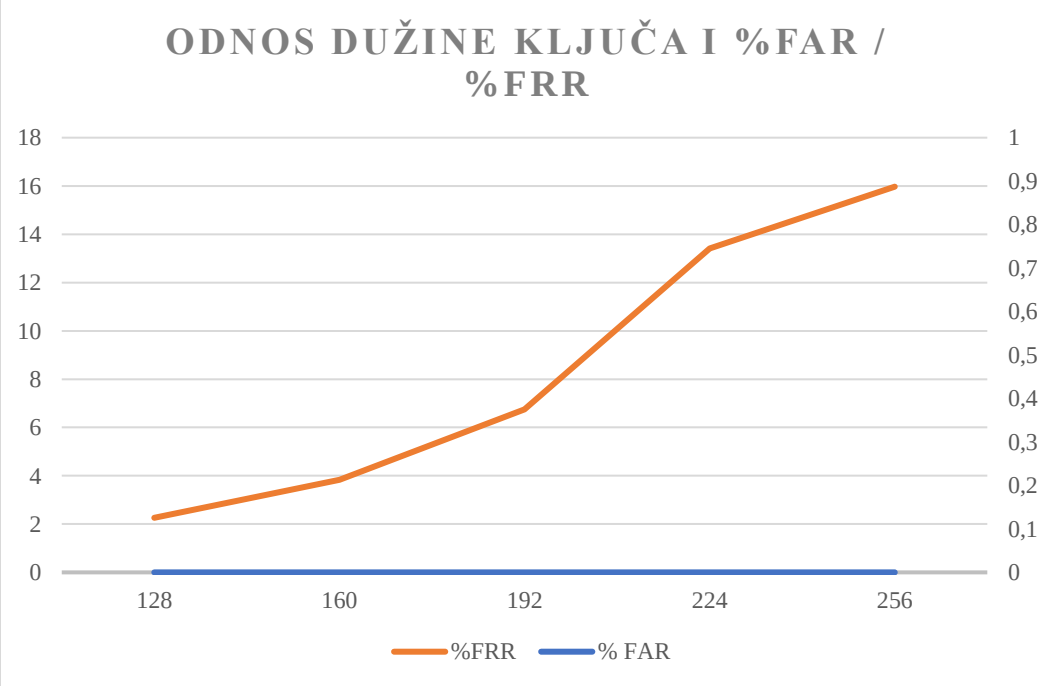
Ukupne performanse na nivou sistema su date u tabeli 5-2.

Dužina ključa	**Haš**	**Sigurnost**	**% FAR**	**%FRR**
128	RIPEMD -160	$6.29x10^{57}$	0,00	2,26
160	RIPEMD -160	$2.70x10^{67}$	0,00	3,83
192	SHA-224	$1.61x10^{77}$	0,00	6,75
224	SHA-224	$4.99x10^{86}$	0,00	13,41
256	SHA-256	$2.14x10^{96}$	0,00	15,97

Tabela 5-2 Performanse predloženog rešenja



Slika 5-7 Grafički prikaz performansi predloženog rešenja kroz aspekt sigurnosti



Slika 5-8 Grafički prikaz % FAR i % FRR

Iz ugla napadača ili ako sprovedemo bezbednosnu analizu koja se odnosi na različite vrste napada, u svim radnim režimima predloženog rešenja ostavljena je mogućnost procene napadača

na osnovu primene grube sile bez postojanja skraćenog napada. Iz kriptografskog ugla zadovoljen je jedan o Kerkehofih principa kada je reč o proceni bezbednosti jednog kripto sistema.

5.4. Evaluacija bezbednosti predloženog rešenja

Široka primena rešenja zasnovanih na biometrijskim podacima uticala je na pojavu više vrsta napada koji mogu da eksploatišu ili kompromituju biometriju u različitim segmentima primenjenog rešenja.

Iz tog razloga u nastavku su navedeni neki od poznatih napada na biometrijske sisteme:

- Lažna biometrija – napadač pokušava da kompromituje sistem sa lažnom biometrijom. Potencijalni vid zaštite bio bi detektor koji treba da utvrdi da li se radi o sintetičkom biometrijskom uzorku. Danas su aktuelni detektori koji koriste neuronske mreže.
- Ponovno slanje podataka – napadač uspeva da opservira komunikacioni kanal i izvodi napad ponovnim slanjem. Potencijalni vid zaštite bio bi parametar koji čuva svežinu biometrije, po uzoru na sisteme autentifikacije koji koriste slučajno generisane brojeve u vidu izazova.
- Napad na ekstraktor biometrijskog templejta – napadač uz posebno odabrane alate kompromituje ekstraktor biometrijskih templejta i tako iskorišćava odabrane vektore. Potencijalni vid zaštite je definisan u zavisnosti od korišćene biometrije i metoda koji se koriste za ekstrakciju biometrijskih karakteristika.
- Upotreba sintetičkih ekstraktora – ovaj vid napada koristi najčešće veštačku inteligenciju za razvoj metoda koji će omogućiti reverzno inženjerstvo, na način da od originalnog biometrijskog templejta regeneriše biometrijski uzorak. Potencijalni vid zaštite podrazumeva primenu veštačke inteligencije kao odgovor na napade iz istog domena.
- Narušavanje integriteta – napadač menja biometrijske podatke u bazama podataka. Potencijalni vid zaštite podrazumeva razvoj i primenu naprednih biometrijskih sistema koji ne skladište originalnu biometriju u bazama podataka, već se biometrija trajno čuva

u pomoćnim podacima koji će omogućiti u legitimnim uslovima regenerisanje originalne biometrije samo uz prisustvo vlasnika biometrije.

- Napad čovek u sredini – ova vrsta napada je dobro poznata i iz tog razloga postoji veliki broj različitih bezbednosnih protokola koji mogu biti iskorišćeni za ovaj vid bezbednosnog problema.
- Kompromitovano programsko rešenje – napadač stiče administratorske privilegije koje mu omogućavaju da utiče na krajnju odluku sistema u kritičnim fazama, tj. faze u kojima se regeneriše ključ ili autentifikuje korisnik.

U našem slučaju, uzeti su u obzir svi pomenuti napadi, kao i dodatne metode zaštite u različitim delovima sistema koji nisu detaljno uzeti u razmatranje u ovoj disertaciji. Detaljnom analizom sistema, sistem je u svim svojim radnim režimima visoko otporan na sve pomenute vrste napada. Imajući na umu, da je sinteza našeg sistema urađena na osnovu više modaliteta, te da je u određenim fazama stečena zavisnost u vidu fuzije, zaključujemo da na ovaj način dodatno podižemo nivo bezbednosti i štitimo sistem od kompromitacije biometrije i na kraju krađe identiteta. Sa druge strane, kada je reč o performansama sistema, multimodalni sistemi podižu nivo tačnosti i smanjuju mogućnost uspešnog izvođenja napada.

„ I am very seldom interested in applications.

I am more interested in the elegance of a problem.

Is it a good problem, an interesting problem? “

Claude Shannon

---

6. *Zaključak i predlozi za budući rad*

U poslednjem, šestom delu rada dat je zaključak. Sumirani su svi ciljevi koji su postavljeni na početku istraživanja. Dati su svi ostvareni rezultati i doprinosi u radu. Kao osnovne oblasti primene identifikovani su skoro svi kripto sistemi, prvenstveno oni sistemi koji su od izuzetne važnosti za informacionu bezbednost jedne države u skladu sa postojećim softverskim i hardverskim rešenjima.

Biometrijski servisi za prepoznavanje osoba koriste karakteristike ponašanja ili fizičke karakteristike. Ovakvi sistemi mogu da koriste jedan ili više biometrijskih modaliteta. Pokazano je da se snaga sistema zaštite koji se danas koriste procenjuje u odnosu na računarsku snagu sa kojom raspolaže potencijalni napadač. Zaključuje se da upotreba jednog biometrijskog izvora nije dovoljna i da je potrebno istovremeno uključiti i druge biometrijske izvore. Korišćenjem više biometrijskih izvora treba obezbediti dovoljnu količinu informacije koja je neophodna za zaštitu sistema sa ciljem prevazilaženja samo komercijalne primene. Rešenja koja se koriste u vojnim, policijskim i drugim službama iziskuju primenu sistema koji poseduju svojstva perfektnih šifarskih sistemima u domenu biometrijske kriptografije.

Sve ovo je uticalo na razvoj novih trendova u ovoj oblasti biometrijske kriptografije, gde se sinteza multimodalnih sistema vrši na nivou karakteristika, odluke, rezultata i drugih hibridnih fuzija. Jedan od doprinosa u ovom radu jeste razumevanje pomenutih trendova, kao i njihova primena u predloženom rešenju.

U dosadašnjim istraživanjima koja se bave sa multimodalnim biometrijskim sistemima, dobijeni rezultati, kao i celokupne performanse u pogledu bezbednosti ukazuju na veliki potencijal i široku primenu ovakvih sistema. Dalja istraživanja i razvoj novih sistema je neizostavan, jer se stalno otvaraju nova pitanja koja se uglavnom odnose na privatnost biometrijskih podataka, a to je preduslov njihove šire primene i društvene prihvatljivosti.

Istraživanje u ovoj disertaciji je potvrda da je moguće razviti biometrijski sistem koji se oslanja na pomenute principe koje možemo okarakterisati kao „anonimna ili poništiva biometrija“,

što je preduslov u pogledu privatnosti i zaštite biometrijskih podataka. U praktičnom smislu, koriste se funkcije transformacije koje originalnu biometriju preslikavaju u podatak druge strukture koji ne odaje originalnu biometriju, a u pogledu performansi ostaje dosledan.

Opšta hipoteza glasi da su biometrijski modaliteti kao izvori bio informacije dovoljno kvalitetni za sintezu sistema iz domena biometrijske kriptografije, u svrhu generisanja i distribucije kriptoloških ključeva, što je dokazano u ovoj tezi. Eksperimentalnim rezultatima je potvrđeno da je optimalan broj ćelija koje se koriste kao argument u neinvertibilnoj transformaciji (4x4), te se zaključuje da je za navedenu transformaciju parametar EER približno 2% ili u proseku jedno odbijanje u 50 pokušaja.

Kombinovanjem više biometrijskih modaliteta pokazalo se da je moguće poboljšati performanse navedenog sistema i učiniti da rad sistema bude pouzdan i bezbedan. Ova posebna hipoteza je dokazana putem empirijskih istraživanja gde je potvrđeno da višemodalni sistem za generisanje tajnih ključeva ne dozvoljava lažno prihvatanje, to znači da je parametar FAR u svim radnim režimima sistema jednak nuli, što čini ovaj sistem društveno prihvatljivim iz ugla korišćenja i u pogledu bezbednosti.

Naučni doprinosi disertacije

Rešenje prikazano u ovoj doktorskoj disertaciji kroz eksperimentalni rad koji je izložen u petom poglavlju ukazuje na ispunjenost Kerkhofovih principa koji se odnose na snagu šifarskog sistema. Pokazano je da je kvalitet kriptoloških ključeva značajno bolji u informaciono-teorijskom smislu. Sistem je u stanju da ekstraktuje ključeve dužine od 128 do 256 bitova. Treba napomenuti da se ključ od 256 bitova smatra izuzetno jakim ključem i da po NIST-ovim standardu ovaj ključ može biti predmet eksploatacije narednih 30 do 50 godina.

Primenom dobre strategije fuzije razvija se sistem visokih performansi. Sa aspekta sigurnosti, predloženo rešenje u ovoj tezi sprečava sve poznate metode napada na biometrijske sisteme, što je elaborirano u petom poglavlju koje se odnosi na evaluaciju bezbednosti predloženog rešenja. Ukoliko se napad ne može sprečiti, predloženo rešenje će smanjiti mogućnosti izvođenja, odnosno umanjiće efekte samih napada.

U predloženom rešenju, na robusnost ne utiče broj korisnika koji će koristiti sistem kao i da su vrste biometrijskih osobina koje je potrebno steći već poznate i teorijski dokazive te da kao takve predstavljaju reprezentativni biometrijski uzorak.

Za realizaciju datog rešenja u skladu sa kontinuiranim razvojem informacionih tehnologija i dostupnošću uređaja za izdvajanje biometrijskih karakteristika ovaj sistem predstavlja kompromis između troškova razvoja i njegovih performansi i omogućava primenu na standardnim hardverskim platformama za akviziciju biometrijskih uzoraka koji su danas u upotrebi.

Predlog budućih istraživanja

Dalja istraživanja mogu krenuti i od pretpostavke da će multimodalni biometrijski sistemi poboljšati tačnost autentifikacije i verifikacije kroz korišćenje i usaglašavanje više od dva izvora informacija ponaosob.

Očekuje se da će rezultirati rane fuzije na nivou karakteristika biti boljeg učinka od fuzije na nivou rezultata. Međutim, teško je predvideti povećanje performansi zbog svake od ovih strategija pre pozivanja na metodologiju fuzije.

Kako dostupnost više izvora biometrijskih informacija (koji se odnose ili na jednu osobinu ili na više osobina) ukazuje na korišćenje fuzije, korelacija između izvora mora biti detaljnije ispitana pre nego što bi se utvrdila njihova pogodnost za fuziju. Međutim, definisanje odgovarajuće mere raznovrsnosti za proračunavanje performansi fuzije do sada nije dovoljno naučno istraženo.

Druge teme istraživanja u multimodalnoj biometriji mogu biti orijentisane ka sledećim pravcima: zaštita šablona, indeksiranje multimodalne baze podataka, integracije biometrijskih izvora u veoma neograničenim okruženjima, projektovanje dinamičke fuzije kroz primenu algoritama za rešavanje problema nepotpunih ulaznih podataka, predikcija odgovarajućih performansi multimodalnih sistema.

7. Literatura

[1] N. Maček, B. Đorđević, J. Gavrilović and K. Lalović, "An Approach to Robust Biometric Key Generation System Design," *Acta Polytechnica Hungarica,* vol. 12, no. 8, pp. 43-60, 2015.

[2] R. Dwivedi, S. Dey, A. M. Sharma and A. Goel, "A fingerprint based crypto-biometric system for secure communication.," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-15, 2019.

[3] A. Sarkar and B. Singh, A Novel Session Key Generation and Secure Communication Establishment Protocol Using Fingerprint Biometrics, Springer, 2020.

[4] D. Akdoğan, K. Altop and A. Levi, "On the Use of Ordered Biometric Features," *Computer Networks,* vol. 163, no. 1, 2019.

[5] R. K. Bharathi and S. D. Mohana, "A Review on Biometric Template Security.," in *International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT),* Mandya, 2019.

[6] C. Donghoon , G. Surabhi , H. Munawar and M. Sweta , "ancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption," *IEEE Transactions on Information Forensics and Security,* vol. 15, pp. 3152-3167, 2020.

[7] B. Mahroosh and H. . M. Ajaz , "Cancellable biometric system based on linear combination of trigonometric functions with special application to forensic dental biometrics," *International Journal of Biometrics,* vol. 11, no. 4, pp. 342-371, 2019.

[8] P. Gaurang , S. Debasis and B. Subhas , "Biometric-based cryptography for digital content protection without any key storage," *Multimedia Tools and Applications,* pp. 1-22, 2017.

[9] S. Debanjan and R. Balasubramanian , "Generation of Cancelable Iris Templates via Randomized Bit Sampling," *IEEE Transactions on Information Forensics and Security,* pp. 2972-2986, 2019.

[10] C. v3, "CASIA v3," [Online]. Available: http://biometrics.idealtest.org/.

[11] I. Delhi, "IIT," [Online]. Available: https://opendata.iiitd.edu.in/.

[12] L. Zhang, Y. Lili, W. Bin and B. Xingchao, "A Novel Privacy Protection Scheme for Iris Identification," *Wireless Personal Communications volume,* no. 109, p. 2411–2425, 2019.

[13] S. Adamović, V. Miškovic, N. Maček, M. Milosavljević, M. Šarac, M. Saračević and M. Gnjatović, "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," *Future Generation Computer Systems,* vol. 107, pp. 144-157, 2020.

[14] B. Schneier, J. Kelsey, D. Whiting and D. Wagner, "https://www.schneier.com/academic/archives/1998/06/twofish_a_128-bit_bl.html," Twofish: A 128-Bit Block Cipher. [Online].

[15] Wikipedia, "Triple DES," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Triple_DES.

[16] C. A. Oluwakemi and A. O. Umar , "A safe and secured iris template using steganography and cryptography," *Multimedia Tools and Applications,* no. 79, pp. 1-24, 2020.

[17] A. Abozaid, A. Haggag, H. Kasban and Mostafa, "Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion," *Multimedia Tools and Applications,* no. 78, p. 16345–16361, 2019.

[18] P. K. Harkeerat Kaur, "Remote Multimodal Biometric Authentication using Visual Cryptography," in *Proceedings of 3rd International Conference on Computer Vision and Image Processing*, Singapure, 2020.

[19] B. Biffio, *Adversarial Pattern Classification - Phd Thesis,* Cagliary: University of Cagliary, 2010.

[20] . J. Russell and R. Cohn, Caesar Cipher, Book on Demand Ltd., 2012.

[21] D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, New York: Scribner, 1996.

[22] S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, New York: Anchor , 2000.

[23] J. Buchmann , Introduction to cryptography, New York: Springer, 2004.

[24] B. Forouzan and . D. Mukhopadhyay, Cryptography and network security., New York: Mc Graw Hill Education (India) Private Limited, 2015.

[25] J.-P. Aumasson, Serious cryptography: a practical introduction to modern encryption., San Francisco: No Starch Press, 2017.

[26] W. Diffie and M. Hellman, "Privacy and authentication: An introduction to cryptography," *Proceedings of the IEEE,* vol. 67, no. 3, pp. 397-427, 1979.

[27] N. Koblitz, . A. Menezes, Y.-H. Wu and R. Zuccherato, Algebraic aspects of cryptography, Heidelberg: Springer-Verlag, 1998.

[28] A. Salomaa, Public-key cryptography, Heidelberg: Springer-Verlag, 1996.

[29] C. Deavours and L. Kruh, Machine cryptography and modern cryptanalysis, London: Artech House, Inc., , 1985.

[30] M. Veinović and S. Adamović, Kriptologija 1, Beograd: Univerzitet Singidunum, 2014.

[31] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.,* vol. 28, pp. 656-715, 1949.

[32] M. Merkle, Verovatnoć i statistika za inžinjere i studente tehnike, Beograd: Akademska misao, 2016.

[33] J. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE,* vol. 76, no. 5, pp. 533-549, 1988.

[34] N. i. z. s. i. tehnologiju, "National Institute of Standards and Technology (NIST)," [Online]. Available: https://www.nist.gov/.

[35] F. I. P. Standard, *Data Encryption Standard,* Washington: National Bureau of Standards, U.S. Department of Commerce,, 1977.

[36] A. J. Menezes, J. Katz, P. C. v. Oors and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[37] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198-208, 1983.

[38] R. Merkle, "Protocols for public key cryptosystems," *Secure communications and asymmetric cryptosystems,* pp. 73-104, 2019.

[39] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International conference on the theory and applications of cryptographic techniques. Springer*, Heidelberg, 2001.

[40] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," *Proceedings 42nd IEEE Symposium on Foundations of Computer Science. IEEE,,* pp. 136-145, 2001.

[41] C. Boyd, A. Mathuria and D. Steblia, Protocols for authentication and key establishment, Heidelberg: Springer, 2003.

[42] L. Nan, "LI, Nan. Research on Diffie-Hellman key exchange protocol.," *Processing 2nd International Conference on Computer Engineering and Technology. IEEE,* vol. 4, pp. 634-637, 2010.

[43] S. Blake-Wilson and A. Menzes, "Authenticated Diffe-Hellman key agreement protocols," in *International Workshop on Selected Areas in Cryptography*, Heidelberg, 1998.

[44] S. Matyas and C. Meyer, "Generation, distribution, and installation of cryptographic keys," *IBM Systems Journal, ,* vol. 17, no. 2, pp. 126-137, 1978.

[45] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudorandom bits," *SIAM journal on Computing,* vol. 13, no. 4, pp. 850-864, 1984.

[46] M. Bellare and P. Rogaway, "The exact security of digital signatures-How to sign with RSA and Rabin," in *International conference on the theory and applications of cryptographic techniques*, Heidelberg, 1996.

[47] A. Topuzoglu and . A. Winterhof, "Pseudorandom sequences," *Topics in geometry, coding theory and cryptography. Springer, Dordrecht,*, vol. 6, pp. 135-166, 2006.

[48] U. Maurer, "The role of information theory in cryptography," in *Fourth IMA Conference on Cryptography and Coding.*, 1993.

[49] . L. Reyzin, "Some notions of entropy for cryptography," in *International Conference on Information Theoretic Security*, Springer, Berlin, Heidelberg, 2011.

[50] A. Vassilev and T. Hall, "The importance of entropy to information security," *Computer,* vol. 47, no. 2, pp. 78-81, 2014.

[51] K. Lalović, N. Maček, M. Milosavljević, M. Veinović, I. Franc, J. Lalović and Tot Ivan, "Biometric Verification of Maternity and Identity Switch Prevention in Maternity Wards," *Acta Polytechnica Hungarica.*, vol. 13, no. 1, pp. 65-81, 2016.

[52] Z. Aasim, H. Syed and T. Mohamed Salim, "Towards Secure m-Learning: An Analysis," *Magnt Research Report,* vol. 2, no. 5, pp. 148-159, 2014.

[53] G. Atul, "Secure Web Access Model For Sensitive Data," *International Journal of Computer Science and Communication,* vol. 1, pp. 13-16, 2010.

[54] N. Kumar and M. Kumar, "Cancelable biometrics: a comprehensive survey.," *Artificial Intelligence Review, ,* vol. 53, no. 5, pp. 3403-3446, 2020.

[55] A. K. Trivedi, D. M. Thounaojam and S. Pal, "Non-Invertible cancellable fingerprint template for fingerprint biometric," *Computers & Security,* vol. 90, pp. -, 2022.

[56] M. Farhan, M. Aslam, J. Sohail, K. Shehzad and K. Mucheol, "Real-Time Imaging-Based Assessment Model for Improving Teaching Performance and Student Experience in e-Learning," *Journal of Real-Time Image Processing,* vol. 13, no. 3, p. 91–504, 2017.

[57] A. Jain and S. Li, Handbook of face recognition, New York: Springer, 2011.

[58] . S. Karamizadeh, S. Abdullah, A. Manaf, Z. Mazdak and A. Hooman, "An overview of principal component analysis," *Journal of Signal and Information Processing,* vol. 4, no. 3, pp. 173-175 , 2020.

[59] A. S. AL-Jaberi and A. M. AL-Juboori, "Palm vein recognition, a review on prospects and challenges based on CASIA's dataset.," *13th International Conference on Developments in eSystems Engineering (DeSE). IEEE,* pp. 169-176, 2020.

[60] Y. Wu and T. Huang, "Vision-based gesture recognition: A review.," in *International gesture workshop. Springer, Berlin,* Heidelberg, 1999.

[61] B. Wang, W. Li, W. Yang and Q. Liao, "Illumination Normalization Based on Weber's Law With Application to Face Recognition," *IEEE Signal Processing Letters,* vol. 18, no. 8, pp. 462-465, 2011.

[62] J.-P. Ortonne, "Photoprotective properties of skin melanin," *British Journal of Dermatology,* vol. 146, pp. 7-10, 2022.

[63] J. Daugman, "Recognizing people by their iris patterns," *Information Security Technical Report,* vol. 3, no. 1, pp. 33-39, 1998.

[64] . J. Daugman, "Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression," *IEEE Transactions on acoustics, speech, and signal processing,,* vol. 36, no. 7, pp. 1169-1179, 1988.

[65] K. Hollingsworth, K. Bowyer and P. Flynn, " The best bits in an iris code," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 31, no. 6, pp. 964-973, 2008.

[66] D. Ballard, "Generalizing the Hough Transform to Detect Arbitrary Shapes," *Pattern Recognition,* vol. 13, no. 2, pp. 111-122, 1989.

[67] J. Llados and D. Blostein, "Special issue on graphics recognition," *International Journal on Document Analysis and Recognition (IJDAR),* vol. 9, pp. 1-2, 2007.

[68] C. Stewart, "Robust Parameter Estimation in Computer Vision," *SIAM Review - Society for Industrial and Applied Mathematics,* vol. 41, no. 3, p. 513–537, 1999.

[69] M. S. Nixon and A. S. Aguado, Feature Extraction & Image Processing for Computer Vision - 4th Editions, : Academic Press, Elsevier, 2019.

[70] R. Shikder, S. Rahaman, F. Afroze and A. Al Islam, "Keystroke/mouse usage based emotion detection and user identification," *International Conference on Networking, Systems and Security (NSysS),* pp. 96-104, 2017.

[71] A. Arwa, K. Warwick and H. Wei, Non-Conventional Keystroke Dynamics for User Authentication, USA: Elsevier Science Inc., 2017.

[72] D. Zhang, Automated biometrics: technnologies and systems, Springer Science & Business Media, 2000.

[73] M. Milosavljević and S. Adamović, Kriptologija 2, Beograd: Univerzitet Singidunum, 2014.

[74] A. Adler and M. Schuckers, "Calculation of a composite DET curve," *International Conference on Audio-and Video-Based Biometric Person Authentication.,* vol. 3546, p. 860868, 2005.

[75] J. C. Wu, A. Martin and R. Kacker, "Measures, uncertainties, and significance test in operational ROC analysis," *Journal of Research of the National Institute of Standards and Technology,* vol. 116, no. 1, p. online, 2011.

[76] G. Doddington, M. Przybocki, A. Martin and D. Reynolds, "The NIST speaker recognition evaluation – Overview, methodology, systems, results, perspective," *Speech Communication,* vol. 31, no. 2-3, pp. 225-254, 2000.

[77] J. Anil and R. Arun, "Fingerprint mosaicking," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, , 2002.

[78] A. K. Jain, P. Flynn and . A. A. Ross, Handbook of Biometrics, New York: Springer, 2008.

[79] H. Furuya, S. Eda and T. Shimamura, "Image restoration via Wiener filtering in the frequency domain," *WSEAS transactions on signal processing*, vol. 5, no. 2, pp. 63-73, 2009.

[80] J. Gaurav , K. Amit and N. Ravinder, "Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry," in *Computational Intelligence: Theories, Applications and Future Directions - Volume II. Advances in Intelligent Systems and Computing*, Singapore, Springer, Singapore, 2019, pp. 557-570.