



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Razvoj servisa autentifikacije zasnovanog na kombinovanju biometrije otiska prsta i lozinki

- Diplomski rad -

Mentor:
doc. dr Aleksandar Jevremović

Student:
Marko Marjanović

Br. indeksa: 2011201209

Beograd, 2013.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Marko Marjanović

Broj indeksa: 2011201209

Smer: Informatika i računarstvo

Tema: Razvoj servisa autentifikacije zasnovanog na kombinovanju biometrije otiska prsta i lozinki

Zadatak: Kombinacijom biometrijskih podataka otiska prsta i lozinke unaprediti sisteme za autentifikaciju. Korišćenjem dvo-faktorske šeme generisati kriptološke ključeve i nad njihovim sadržajem izvršiti teorijsko-informacionu analizu.

Datum odobrenja rada:
Beograd, _____._____._____.

MENTOR

Doc. dr Aleksandar Jevremović

DEKAN

Prof. dr Miroslav Lutovac

Razvoj servisa autentifikacije zasnovanog na kombinovanju biometrije otiska prsta i lozinki

Sažetak: U radu se bavimo razvojem bezbednih sistema za autentifikaciju zbog velike potrebe koja postoji u aplikacijama savremenih poslovnih okruženja. Obzirom na razvoj i potencijal biometrijskih podataka, naša ideja u radu je da ostvarimo vezu između biometrije otiska prsta i tradicionalnih lozinki. Na ovaj način servis autentifikacije obezbeđuje dvo-faktorsku šemu koja je zasnovana na nečemu što jesmo i nečemu što znamo. Naša predložena šema sadržaće detaljno objašnjenje o načinu kombinovanja ova dva faktora preko kojih se obezbeđuje sigurna autentifikacija. Zanimajući osvedočene performanse biometrijskog sistema za prepoznavanje, uticaćemo na parametre transformacione funkcije za generisanje biometrijskog obrasca koji će posedovati odgovarajuće informacione osobine za potrebe autentifikacije. Dobijanje dobre informacione vrednosti tako generisanog materijala nam omogućava kreiranje kriptoloških ključeva dobrih karakteristika. Evaluacija sistema biće izvršena na osnovu podignutog eksperimentalnog rešenja koje je zasnovano na Matlab programskom paketu i "CASIA" biometrijskoj bazi podataka.

Ključne reči: otisak prsta, lozinka, autentifikacija, kriptološki ključ.

The development of service-based authentication combining fingerprint biometrics and passwords

Abstract: This paper is the development of secure authentication systems due to the great need that exists in the application of modern business environment. Considering the development potential of the biometric data, our idea in this paper is to establish a link between fingerprint biometrics and traditional passwords. In this way the authentication service provides two-factor scheme that is based on something we are and something we know. Our proposed scheme will include a detailed explanation of how to combine these two factors over which provides secure authentication. Ignoring the demonstrated performance of biometric recognition system, we will impact parameter transformation functions for generating biometric pattern that will have the appropriate information for the authentication features. Getting appropriate informations from that kind of material we are able to generate crypto key with good performance. Evaluation of the system will be made on the basis of experimental jacked solution is based on the Matlab software package and "CASIA" biometric database.

Keywords: fingerprint, password, authentication, crypto key.

SADRŽAJ

Spisak slika.....	- 3 -
Spisak tabela	- 4 -
1 Uvod.....	- 5 -
1.1 Predmet istraživanja.....	- 5 -
1.2 Doprinosi rada.....	- 5 -
1.3 Struktura rada.....	- 6 -
2 Pregled u oblasti istraživanja	- 7 -
2.1 Dvo-faktorska autentifikacija spajanjem podataka otiska prsta i broja	- 7 -
2.1.1 Bio-hešing	- 7 -
2.1.2 Invertna WFMT funkcija.....	- 7 -
2.2 Predlog šifarskog sistema zasnovanog na biometrijskom ključu.....	- 9 -
2.2.1 Faza biometrije	- 10 -
2.2.2 Faza generisanja ključa.....	- 11 -
2.2.3 Faza šifrovanja.....	- 11 -
2.2.4 Kriterijumi razvoja.....	- 11 -
2.2.5 Eksperimentalni rezultati	- 13 -
2.3 Generisanje biometrijskog ključa za korišćenje u DES-u.....	- 15 -
2.3.1 Obrada otiska prsta	- 16 -
2.3.2 Predloženi metod	- 17 -
2.3.3 Algoritam za generisanje ključa	- 18 -
2.4 Prednosti i nedostaci biometrijskih rešenja u razvoju servisa autentifik. .	- 18 -
2.5 Razvoj dvo-faktorskih sistema autentifikacije.....	- 20 -
3 Teorijske osnove istraživanja	- 21 -
3.1 Biometrija u sistemima autentifikacije	- 21 -
3.1.1 Istorijat biometrije	- 21 -
3.1.2 Biometrijski sistemi	- 21 -
3.1.3 Autentifikacija	- 22 -

3.1.4 Verifikacija	- 23 -
3.1.5 Identifikacija	- 23 -
3.1.6 Metodi autentifikacije	- 23 -
3.1.7 Performanse biometrijskih sistema	- 24 -
3.1.8 Performanse i greške prilikom procesa upisa	- 24 -
3.1.9 Performanse i greške u procesu verifikacije	- 24 -
3.1.10 Najčešće korišćeni biometrijski sistemi	- 27 -
3.1.11 Otisak prsta	- 27 -
3.1.12 Izdvajanje minucija	- 29 -
3.1.13 Pобољшanje kvaliteta slike otiska prsta	- 30 -
3.1.14 Normalizacija	- 30 -
3.1.15 Furijer-ova transformacija	- 31 -
3.1.16 Proces kodovanja – binarizacija otiska prsta	- 32 -
3.1.17 Procena usmerenosti blokova	- 32 -
3.1.18 Segmentacija slike otiska prsta	- 33 -
3.1.19 Izdvajanje regiona interesa morfološkim operacijama	- 33 -
3.1.20 Izoštavanje teksture otiska prsta	- 34 -
3.1.21 Obeležavanje minucija	- 35 -
3.1.22 Uklanjanje lažnih minucija	- 35 -
3.1.23 Upisivanje pozicija minucija	- 36 -
3.2 Kriptološko-teorijska osnova	- 37 -
3.2.1 Kriptologija	- 37 -
3.2.2 Lozinka	- 37 -
3.2.3 Kriptološki ključ	- 38 -
3.2.4 Simetrični šifarski sistem	- 38 -
3.2.4.1 DES	- 39 -
3.2.4.2 AES	- 41 -
3.2.5 Heš funkcije	- 44 -
3.2.5.1 MD5	- 45 -

3.2.5.2 SHA.....	- 46 -
3.3 Teorijsko-informaciona analiza	- 46 -
3.3.1 Entropija	- 46 -
3.3.2 NIST testovi.....	- 46 -
3.3.3 Interliving	- 59 -
3.3.3.1 Blok interliving	- 59 -
4 Pregled predloženog rešenja.....	- 60 -
4.1 Genrička šema predloženog rešenja.....	- 60 -
4.2 Postavka i objašnjenje eksperimentalnog okruženja.....	- 61 -
4.3 Sprovedene analize	- 61 -
4.4 Pregled upotrebe predloženog rešenja	- 62 -
4.5 Performanse predloženog rešenja sa prikazanim rezultatima.....	- 67 -
4.6 Oblast primene predloženog rešenja.....	- 68 -
5 Zaključak.....	- 70 -
5.1 Sumarni ciljevi rada i ostavreni rezultati	- 70 -
5.2 Predlog za budući rad.....	- 70 -
Literatura	- 71 -

Spisak slika

Slika 1 – 2D wavelet transformacija sa jednim i tri nivoa	- 8 -
Slika 2 – Blok dijagram generisanja WFMT karakteristika.....	- 8 -
Slika 3 – Bio-hešing proces.....	- 9 -
Slika 4 – Predloženi biometrijski šifarski sistem	- 10 -
Slika 5 – Faza biometrije.....	- 13 -
Slika 6 – Optimalna kompresija.....	- 14 -
Slika 7 – Chi-Square raspodela	- 14 -
Slika 8 – Koeficijent serijske korelacije.....	- 15 -
Slika 9 – Moduli u biometrijskom sistemu	- 22 -
Slika 10 – EER tačka preseka	- 25 -
Slika 11 – Originalna i nametnuta distribucija.....	- 26 -
Slika 12 – Odnos biometrijskih tehnika u praksi	- 27 -
Slika 13 – Tipovi otisaka prstiju	- 28 -
Slika 14 – Singularne tačke.....	- 28 -
Slika 15 – Proces izdvajanja minucija	- 29 -
Slika 16 – Razlika između originalnog i histograma nakon metode pojačavanja.	- 31 -
Slika 17 – Slika otiska prsta nakon binarizacije.....	- 32 -

Slika 18 – Mapa usmerenosti blokova	33 -
Slika 19 – Oblast originalne slike	34 -
Slika 20 – Oblast nakon „Close“ operacije	34 -
Slika 21 – Oblast nakon „Open“ operacije	34 -
Slika 22 – Oblast interesa sa granicom	34 -
Slika 23 – Grananje grebena, završetak grebena, trostruko grananje	35 -
Slika 24 – Lažne minucije	36 -
Slika 25 – Pozicija minucije u koordinatnom sistemu	37 -
Slika 26 – Proces šifrovanja i dešifrovanja u simetričnim šifarskim sistemima... -	38 -
Slika 27 – DES blokovska šifra	39 -
Slika 28 – Jedna runda DES algoritma	40 -
Slika 29 – E-kutija	40 -
Slika 30 – S-kutija	41 -
Slika 31 – P-kutija	41 -
Slika 32 – ByteStub operacija	42 -
Slika 33 – ShiftRow operacija	43 -
Slika 34 – MixColumn operacija	43 -
Slika 35 – AddRowKey operacija	43 -
Slika 36 – AES funkcija runde za runde 1,2,..., n_r-1	44 -
Slika 37 – Generička šema sistema	60 -
Slika 38 – Generička šema izdvajanja biometrijskog templejta	62 -
Slika 39 – Pojačavanje histograma	63 -
Slika 40 – Brza Furijer-ova transformacija	64 -
Slika 41 – Binarizacija i usmerenost blokova	64 -
Slika 42 – Region interesa (RIO)	65 -
Slika 43 – Izoštrena slika sa uklonjenim lažnim minucijama	65 -
Slika 44 – Obeležene minucije i realne minucije	66 -
Slika 45 – Deo dobijenog tekstualnog fajla na osnovu pozicija minucija	66 -
Slika 46 – Binarni fajl nakon primene transformacione funkcije	67 -

Spisak tabela

Tabela 1 – Razlika između AES i KAES algoritma	11 -
Tabela 2 – Vrednost entropije	14 -
Tabela 3 – Kompjuterska aritmetička sredina	14 -
Tabela 4 – Monte Karlo vrednosti	15 -
Tabela 5 – Prozor 3x3	16 -
Tabela 6 – Osobina ukrštenih brojeva	17 -
Tabela 7 – Poređenje različitih biometrija	22 -
Tabela 8 – Procenat greške kod najčešćih biometrijskih karakteristika	24 -
Tabela 9 – Poređenje heš algoritama	45 -
Tabela 10 – Rezultati testa niza jedinica	27 -
Tabela 11 – Rezultati ponavljanja blokova	47 -
Tabela 12 – Ispitivanje slučajne digresije	57 -
Tabela 13 – Ispitivanje slučajne promenljive digresije	58 -
Tabela 14 – Rezultati frekvencijskog testa	67 -
Tabela 15 – Rezultati serijskog testa	67 -
Tabela 16 – Rezultati entropijskog testa	68 -

1 Uvod

Dobro je poznato da su neke osobine ljudskog tela kao što su otisak prsta, DNK, iris, karakteristične za svaku osobu. Upravo nam te činjenice govore da je potrebno iskoristiti prednosti koje nam pruža biometrija. Kako je poznato da svaki sistem ima svoje mane tako je moguće poboljšati i sisteme autentifikacije koji su zasnovani na biometrijskim uzorcima. U radu će biti detaljno objašnjeno na koji način je moguće ostvariti vezu između biometrije otiska prsta i tradicionalnih lozinki.

Poznato je da možemo izvršiti autentifikaciju na tri načina a to su: na osnovu nečega što imamo, što znamo i što jesmo. Upravo kombinacijom onoga što znamo (lozinka) i onoga što jesmo (biometrija) dolazimo do dvo-faktorske šeme koju ćemo koristiti u procesu autentifikacije. Ovakvim načinom autentifikacije postiže se znatno viši nivo bezbednosti sistema.

Materijal koji je dobijen kombinacijom biometrije i lozinke će biti iskorišćen za generisanje kriptoloških ključeva koji mogu biti korišćenih u sistemima za bezbednost podataka.

Evolucija sistema biće izvršena na osnovu podignutog eksperimentalnog rešenja koje je zasnovano na Matlab programskom kodu. Uticaćemo na parametre transformacione funkcije za generisanje biometrijskog obrasca koji će zadržati odgovarajuće informacione osobine za potrebe autentifikacije. Biometrijski uzorci otiska prsta koje ćemo koristiti su preuzeti sa CASIA baze biometrijskih uzoraka.

2.1 Predmet istraživanja

Biometrija poseduje veliki potencijal gledano sa aspekta mogućnosti dobijanja korisnih informacija iz testiranih uzoraka. Kombinovanje tako dobijenih informacija sa dodatnim parametrom kao što je lozinka dolazimo do značajnog poboljšanja sigurnosti servisa autentifikacije. U radu će biti detaljno razmatrane, teorijski i praktično ispitane i objašnjene mogućnosti dvo-faktorske biometrijske autentifikacije kao i mogućnost da se iz dvo-faktorskog materijala generišu kriptološki ključevi. Istraživanje će obuhvatiti sve prednosti i mane korišćenja biometrijskih sistema u svrhu unapređenja autentifikacionih procesa. Takođe, ispitaće se najefikasniji način kombinovanja biometrijskih i tradicionalnih sistema uz pomoć transformacione funkcije. Istraživanjem ćemo obuhvatiti i sisteme za testiranje dobijenih rezultata na osnovu kojih ispitujemo kvalitet dobijenih ključeva i funkcionalnost transformacione funkcije.

2.1 Doprinosi rada

- Generisanje kriptološkog ključa iz biometrije otiska prsta.
- Korišćenje lozinke kao dodatni faktor zaštite.
- Generisanje više ključeva na osnovu originalnog biometrijskog uzorka.
- Originalna biometrija se ne čuva u bazi podataka.
- Prilagođena transformaciona funkcija.
- Izvršena informaciono-teorijska analiza.

2.1 Struktura rada

Rad je urađen po standardnoj strukturi za izradu diplomskih radova. U uvodnom delu je opisano koji je predmet istraživanja rada kao i doprinosi koje će rad dati. Nakon togaje opisano stanje u oblasti istraživanja gde je dat osvrt na tri rada koja se bave sličnim problemom. U istom poglavlju su opisani prednosti i nedostaci biometrijskih sistema u procesu autentifikacije kao i razvoj dvo-faktorskih sistema. Treća oblast predstavlja teorijsku analizu procesa koji su korišćeni u praktičnom rešenju počevši od osnova biometrije, kriptologije kao nauke pa sve do teorijskih principa informacione analize. U četvrtoj oblasti se nalazi detaljno opisan predloženi sistem sa performansama i prikazanim rezultatima. Za kraj četvrte oblasti navedene su i oblasti primene predloženog rešenja. Zaključak nam donosi informacije o sumarnim ciljevima rada kao i jedan od predloga za buduće istraživanje.

2 Pregled u oblasti istraživanja

Tokom istraživanja trenutnog stanja u oblasti generisanja ključa na osnovu biometrije kao i dvo-faktorske autentifikacije došli smo do nekoliko radova koji se bave pomenutim temama. U daljem tekstu detaljno ćemo opisti radove i dostignuća koja su u njima postignuta.

2.1 Bio-hešing: Dvo-faktorska autentifikacija spajanjem podataka iz slike otiska prsta i nasumičnog broja dobijenog iz tokena [1]

U radu je opisan metod spajanja dva načina autentifikacije, otiska prsta i slučajnog broja dobijenog iz tokena. Uz pomoć novog pristupa dobija se jedinstven kompaktan kod za svaku osobu. Direktnim kombinovanjem odnosno množenjem pseudo-slučajnog broja i biometrijskih podataka dobijenim uz pomoć *Fourier-Melin* transformacije (FMT) predstavlja veoma pouzdan mehanizam koji pruža visok nivo pouzdanosti.

2.1.1 Bio-hešing

Bio-hešing metodologija može biti podeljena na dva dela. Prvi deo bi predstavljao integralnu transformaciju podataka dobijenih iz otiska prsta sa umerenim stepenom ofset tolerancije. Ovo bi uključivalo i korišćenje integrisanog wavelet-a i Fourier-Melin transformacionog frejmvorka, wavelet transformacija čuva lokalne ivice i smanjuje šum na nisko frekvencijski domen nakon parcelisanja slike što doprinosi manjoj osetljivosti slike otiska prsta na distorzije oblika. U skladu sa tim smanjena dimenzija slike doprinosi poboljšanoj efikasnosti izračunavanja. FMT proizvodi transformaciju i rotaciju u ravni. Linearna osobina FTM-a omogućava višestruke WFTM (wavelet FTM) koje mogu da se koriste da bi napravile referentnu inverznu funkciju koja smanjuje promenljivost ulaznih slika otisaka prsta.

Drugi deo bio-hešing metodologije je optimizacija podataka korišćenjem proizvoda nasumičnog broja dobijenog iz tokena i korisničkih podataka.

2.1.2 Invertna WFMT funkcija

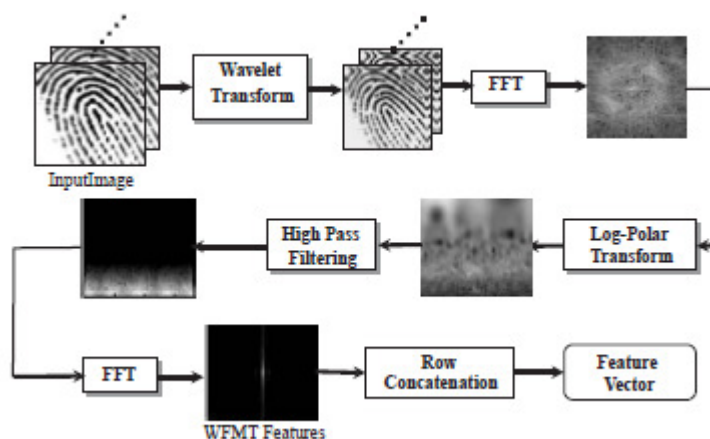
Wavelet teorija pruža mogućnost multirezolucione prezentacije za prevođenje informacija dobijenih iz slike sa dekompozicijom slike na više nivoa. Slika 1 nam prikazuje dekompoziciju slike koristeći 2D *wavelet* transformaciju (levo) kao i isti princip samo na niskim frekvencijama (desno).



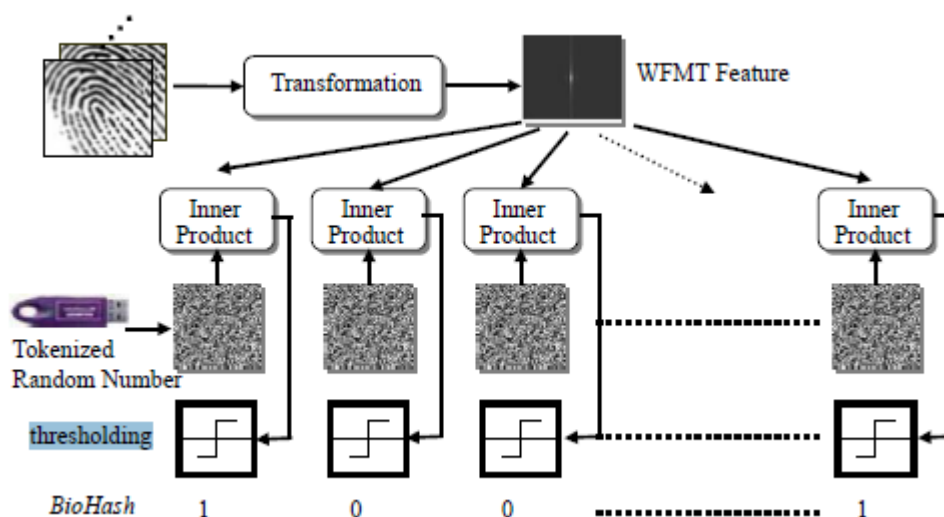
Slika 1 - 2D wavelet transformacija sa jednim(levo) i tri nivoa(desno).

Prema wavelet teoriji, wavelet transformacija čuva energiju signala i distribuira je u kompaktnijoj formi. *Subband* niskih frekvencija sadrži više energije ako se poredi sa *subband*-om visokih frekvencija tako da je bolji za prezentaciju otiska prsta. *Subband* niskih frekvencija pravi sliku koja je pogodnija za obradu zato što smanjuje uticaj šuma a takođe čuva lokalne ivice. U kojoj meri će *subband* niskih frekvencija očuvati energiju zavisi od izabranog *wavelet*-a.

Prilikom skeniranja otiska prsta dolazi do skeniranja pod različitim uglovima, iz različitih pozicija tako da to sve utiče na performanse autentifikacije. Ti problemi se mogu rešiti transformacijom slike otiska prsta u invertnu funkciju. Postoji više inverznih tehnika od kojih se u radu koristi inverzna transformacija zasnovana na integralima – FMT. FTM predstavlja rotaciju i skaliranje kao prevođenje duž korespondentnih osa parametra prostora.



Sl 2 - Blok dijagram generisanja WFMT karakteristika.



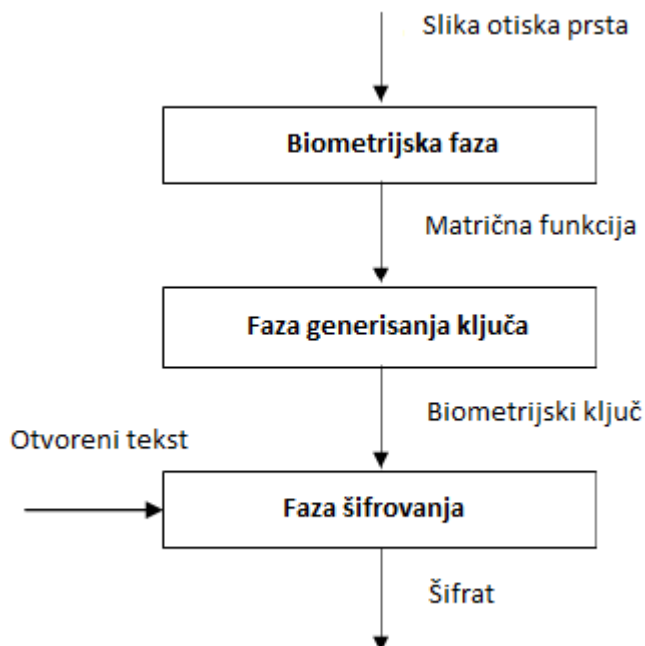
Sl 3 – Bio-hešing proces.

2.2 Predlog šifarskog sistema zasnovanog na biometrijskom ključu [2]

Sa sve većim oslanjanjem na elektronske informacije, koje treba preneti preko Interneta ili memorisati na otvorenim mrežama, kriptologija postaje veoma bitna komponenta kompjuterske sigurnosti. Predložen je šifarski sistem koji je zasnovan na ključu formiranom iz biometrijskog otiska prsta.

Postoje različiti šifarski algoritmi za bezbednost informacija: simetrični i asimetrični. Jačina šifarskog sistema zavisi od dosta faktora: dužine ključa, kompleksnosti algoritma i otpornosti na tehnike kriptanalize. Postoji najmanje dva problema kada se koriste tradicionalne šifre ili tokeni kao ključevi za neki šifarski sistem. Prvi je taj da sigurnost sistema zavisi od jačine izabrane šifre. Jaka šifra treba da bude kompleksna i dugačka što automatski dovodi do problema pamćenja takve šifre. Samim tim mnogi se opredeljuju za manje kompleksne šifre ili problem rešavaju zapisivanjem što smanjuje sigurnost sistema. Drugi problem je nedostatak direktne povezanosti šifre sa korisnikom odnosno sistem ne može po šifri da razlikuje da li je u pitanju regularan korisnik ili napadač koji se loguje na sistem sa šifrom regularnog korisnika. Alternativa šifarskoj zaštiti je povezivanje šifarskog ključa sa biometrijom. Dva popularna sistema su distribucija biometrijskog ključa i generisanje biometrijskog ključa. Kod distribucije ključ je sakriven u biometrijski otisak prilikom faze upisivanja i dostupan je u fazi autentifikacije. Kod drugog sistema ključ se generiše direktno iz otiska prsta. U ovom radu ključ se generiše iz biometrijskog otiska prsta i tako generisan ključ se koristi da se obezbedi dodatna sigurnost prilikom korišćenja šifarskog algoritma.

Generalno gledano, predloženi sistem se može podeliti u tri faze: biometrijska faza, faza generisanje ključa i faza šifrovanja.



Slika 4 - Predloženi biometrijski šifarski sistem.

U predloženom sistemu ulaz u biometrijsku fazu predstavlja sliku otiska prsta koja se dobija uz pomoć skenera otisaka prstiju. Kroz ovu fazu neke jedinstvene karakteristike otiska prsta se izdvajaju da bi se formirala biometrijska matrična funkcija. Tako formirana matrica se koristi kao ulaz za sledeću fazu u kojoj se generiše 128-bitni ključ koristeći jednu od šifarskih heš funkcija kao što je *Secure Hash Algorithm* (SHA-1) ili *Message-Digest algorithm 5* (MD5). Otvoreni tekst se zatim šifruje generisanim ključem i jednim od algoritama za šifrovanje kao što su AES ili KAES. U daljem tekstu je opisana svaka faza posebno.

2.2.1 Faza biometrije

Otisak prsta predstavlja šablon sastavljen od grebena i dolina. Takođe može biti definisan jedinstvenošću lokalnih karakteristika grebena i njihovom povezanošću. Minucije predstavljaju te lokalne karakteristike, završetke ili grananja grebena. Kod slika otisaka prstiju lošeg kvaliteta koje sadrže dosta šuma i razlike u kontrastu može doći do pojave lažnih minucija, tako da proces automatskog pronalaženja minucija postaje komplikovan. U biometrijskoj fazi se koriste sledeći koraci da bi se formirala matrična funkcija koristeći sliku otiska prsta:

- Pred-obrađivanje.
- Izvlačenje minucija.
- Post-obrađivanje.

Prvi korak koristi tri različita procesa za poboljšanje ulazne slike otiska prsta a to su: povećanje, binarizacija i segmentacija slike. Svaka etapa koristi jednu ili više procesnih metoda. Ulaz za ovaj korak predstavlja sliku otiska prsta dok na izlazu dobijamo poboljšanu sliku koja je pogodna za sledeću fazu.

U fazi izvlačenja minucija formira se okosnica slike nakon čega se sledećom metodom dolazi do minucija. Prvo se binarna slika stanji tako da debljina otiska grebena iznosi jedan piksel. Karakteristične tačke su one koje imaju vrednost piksela jedan dok jedan od okolnih piksela takođe ima vrednost jedan i to predstavlja završetak grebena dok kod račvanja grebena centralni piksel i dva okolna piksela imaju vrednost jedan. Na izlazu iz ove faze dobijamo matricu Nx3 koja sadrži x i y pozicije kao i orijentaciju minucija.

Post-obrada otklanja lažne minucije iz biometrijske matrične funkcije. Lažne minucije mogu nastati zbog prekida linije grebena koji nije mogao biti ispravljen ni nakon poboljšanja slike.

Na izlazu iz faze biometrije dobijamo Nx3 matricu koja obično sadrži informacije o ispravnim minucijama.

2.2.2 Faza generisanja ključa

U predloženom rešenju, MD5 se koristi za generisanje 128-bitnog ključa za šifrovanje koji se dobija iz biometrijske matrične funkcije. MD5 algoritam sadrži pet koraka. Na izlazu dobijamo ključ generisan MD5 algoritmom koji je pogodan za mnoge šifarske algoritme kao što su AES ili KAES.

2.2.3 Faza šifrovanja

KAES je simetrična tehnika šifrovanja koja menja AES u tehniku koja je zavisna od ključa. KAES je blokovski šifrat kod koga su veličine bloka i ključa definisane AES specifikacijom. Ključ je veličine 128,192 ili 256 bita a veličina blokova je 128 bita. U predloženoj metodi dužina ključa je 128 bita. KAES ubacuje ključ u većini algoritamskih koraka što povećava sigurnost. Glavne razlike između AES i KAES algoritma date su u sledećoj tabeli.

	AES	KAES
Funkcija runde	Poslednja runda je različita	Iste transformacije u svim rundama
S-Box	Fiksni	Zavisi od ključa
Proširivost ključa	Fiksirano S-Box-om	Generisano iz S-Box-ova
Transformacija runde	Ne zavisi od ključa	Zavisi od ključa
Pomeraj	Koristi se fiksi od 0 do 3	Oslanja se na ključ

Tabela 1 - Razlika između AES i KAES algoritma.

2.2.4 Kriterijumi razvoja

Da bi se razvila slučajnost predloženog sistema korišćeni su različiti testovi. Da bi se olakšala interpretacija eksperimentalnih rezultata dati su kratki opisi.

- **Entropija**

Entropija opisuje broj bitova po bajtu. Poznata je kao informaciona gustina fajla. Ekstremni entropijski izlaz pokazuje da je informacija u suštini slučajna. U tom slučaju optimalna kompresija ne smanjuje veličinu.

- **Najbolja optimalna kompresija**

Odražava mogućnost kompresovanja a izračunava se na osnovu entropijskog kodovanja. Na primer, ako fajl ima entropiju 4.9, optimalna kompresija (OC) bi smanjila veličinu fajla za 38%.

$$OC = 100 - (Entropija/8) * 100$$

- **Chi-Square raspodela**

Slučajnost podataka može biti testirana *chi-square* testom. *Chi-square* raspodela je kao apsolutni broj i kao procenat koja prikazuje koliko često slučajna sekvenca će preći preko izračunate vrednosti. Procenat je tumačen kao stepen do kog testirana sekvenca se sumnja da nije slučajna.

- Ako je procenat veći od 99% ili manji od 1% sekvenca gotovo sigurno nije slučajna.
- Ako je procenat između 99%-95% ili 1%-5% sekvenca je sumnjiva.
- Za procenat između 90%-95% ili 5%-10% je gotovo sigurno da je sekvenca sumnjiva.
- U ostalim slučajevima sekvenca je slučajna.

- **Vrednost aritmetičke sredine**

Aritmetička sredina za neki deo podataka se izračunava tako što se sabiraju svi bajtovi a zatim se deli sa dužinom sekvence. Ako su podaci blizu slučajnih vrednost bi trebala da bude oko 127.5. Ostale vrednosti su veoma niske ili visoke.

- **Monte Karlo vrednost za PI**

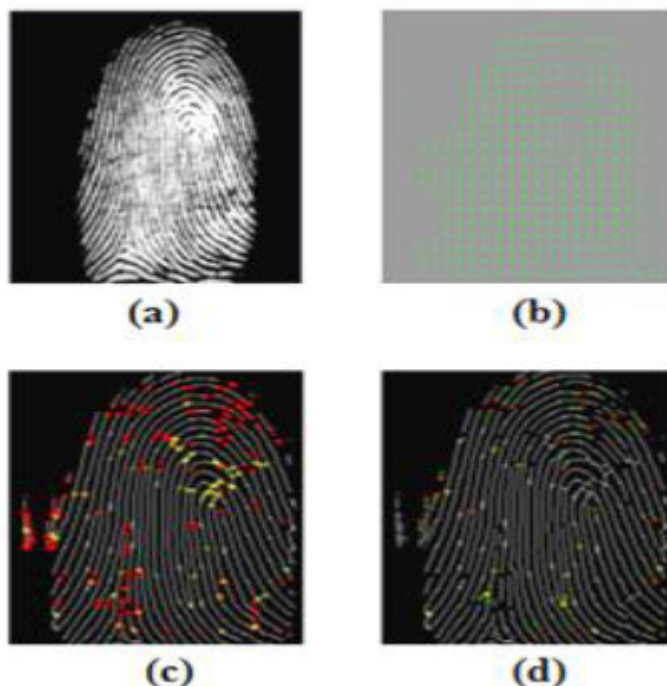
Svaki naredni niz od 6 bajtova se koristi kao 24-bitne x i y kordinate u kvadratu. Ako je razdaljina slučajno generisanih tačaka manja od radijusa kruga upisanog u kvadrat, onda se 6-bajtni niz smatra kao dobar. Procenat takvog niza može se iskoristiti da bi se izračunala vrednost PI. Ako se izračunata vrednost približava ispravnoj vrednosti PI taj niz se smatra slučajnim. Monte Karlo vrednost PI iznosi 3.143580574 (odstupanja 0.06%).

- **Koeficijent serijske korelacije**

Ovaj koeficijent izračunava stepen do kog svaki bajt niza zavisi od prethodnog bajta. Ako je vrednost (koja može biti pozitivna ili negativna) blizu nule niz je slučajan odnosno nije korelisan. U suprotnom serijska korelacija će biti veća ili jednaka 0.5.

2.2.5 Eksperimentalni rezultati

Da bi se napravila simulacija predloženog rešenja, za biometrijsku fazu je korišćen Matlab skript a za AES i KAES java program u fazi generisanja ključa. Dužina ključa je od 128 bita je fiksna za oba AES i KAES algoritma. Slika otiska prsta koja je napravljena sa *Cross Match Verifier 300* skenerom na 500 dpi je korišćena za testiranje sistema. Na slici su prikazani ulazi i izlazi programa biometrijske faze. Minucije su sačuvane kao biometrijska matrična funkcija.



Slika 5 - Faza biometrije: (a) Ulazna slika (b) Pred-obrađena
(c) Izlaz izdvajanja minucija (d) Post-obrađena

Generisani 128-bitni ključ iz biometrijske matrične funkcije kroz fazu generisanja ključa je:

```
0X9e 0Xf8 0X68 0X62
0X53 0Xd7 0X3c 0Xc5
0Xf2 0x66 00Xef 0Xde
0xb6 0Xc7 0Xbe 0X3a
```

Da bi se izvršilo testiranje korišćen je i drugi otvoreni ključ:

```
0Xb1 0Xc2 0Xf3 0X84
0X75 0Xa6 0Xd7 0X08
0X19 0X13 0X11 0X42
0X53 0X20 0X15 0X16
```

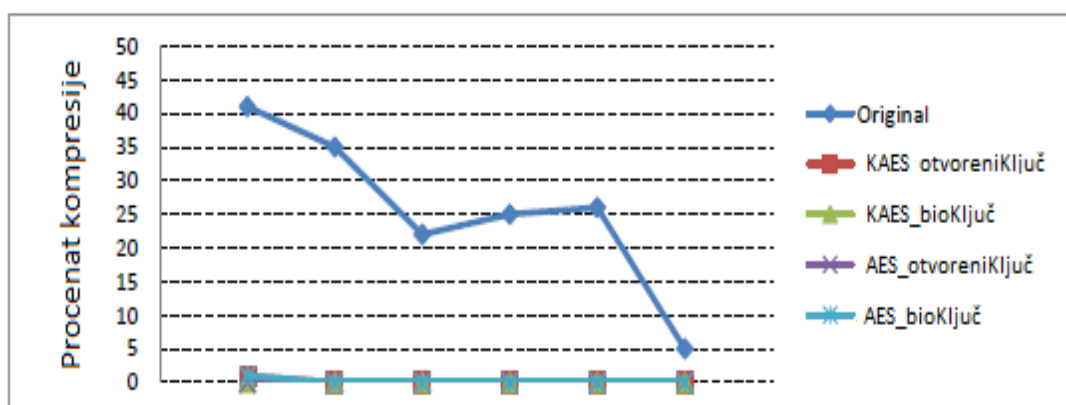
U eksperimentalnoj fazi korišćeno je 6 fajlova različitih veličina nad kojima je izvršeno šifrovanje i dešifrovanje. Slika predstavlja iskorišćenost bitova u bajtu. Može se primetiti da KAES i biometrijski KAES koristi skoro svaki bit u bajtu što

doprinosi izuzetnoj gustini fajla. Slika opisuje optimalnu “najbolju kompresiju” koja može biti postignuta. Rezultati su slični za neke testirane fajlove.

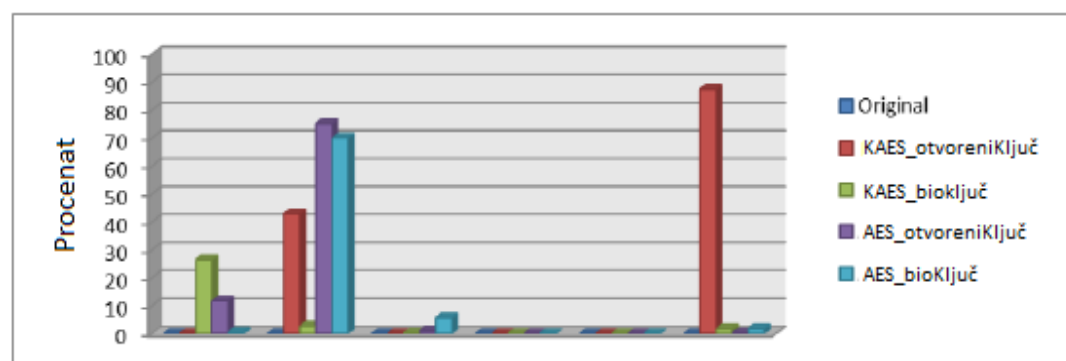
Chi-Square raspodela je prikazana na slici. Sa te slike možemo videti kolika je slučajnost predloženog sistema. Tabela prikazuje izračunatu aritmetičku sredinu i tu vidimo da su i AES i KAES blizu vrednosti 127.5. Tabela nam prezentuje izračunate Monte Karlo vrednosti broja PI koje su blizu 3.1416. Slika pokazuje da je korelacija uzastopnih bajtova veoma mala.

	T1	T2	W1	W2	Im1	Im2
Original	4.711491	5.166631	6.215379	5.963367	5.910927	7.562718
KAES_otvoreniKljuč	7.911388	7.952993	7.98213	7.986803	7.996512	7.999835
KAES_bioKljuč	7.930583	7.947021	7.983541	7.985064	7.996409	7.99978
AES_otvoreniKljuč	7.926212	7.957024	7.984306	7.983461	7.997254	7.999767
AES_bioKljuč	7.918981	7.955877	7.985193	7.985132	7.996956	7.999767

Tabela 2 - Vrednost entropije



Slika 6 - Optimalna kompresija.



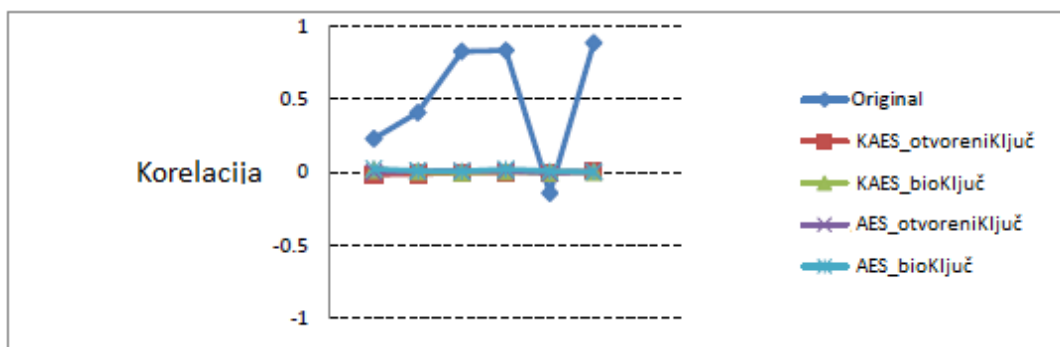
Slika 7 - Chi-Square raspodela.

	T1	T2	W1	W2	Im1	Im2
Original	85.5844	133.5031	127.0035	121.4201	65.9731	93.1652
KAES_otvoreniKljuč	127.4348	124.9963	127.1517	127.1777	127.0659	127.5825
KAES_bioKljuč	127.0274	128.4168	127.5046	128.2845	127.469	127.5014
AES_otvoreniKljuč	130.323	127.2298	127.7911	128.4338	127.58	127.6038
AES_bioKljuč	128.6254	128.1158	127.7079	127.3429	127.4235	127.6049

Tabela 3 - Kompjuterska aritmetička sredina.

	T1	T2	W1	W2	Im1	Im2
Original	4	2.824587 706	3.884057 971	3.957033 248	3.384867 591	3.865725 017
KAES_otvoreni Ključ	2.950959 488	3.166416 792	3.159420 29	3.156351 236	3.158890 29	3.136844 754
KAES_bioKljuč	3.138592 751	3.274362 819	3.157715 26	3.125660 699	3.161916 772	3.149519 89
AES_otvoreniKl juč	3.068376 068	3.076461 769	3.109974 425	3.144075 021	3.157124 842	3.136293 661
AES_bioKljuč	3.025641 026	3.148425 787	3.157715 26	3.118158 568	3.145775 536	3.136293 661

Tabela 4 - Monte Karlo vrednosti.



Slika 8 - Koeficijent serijske korelacije.

• Zaključak

Ovaj rad prezentuje biometrijski šifarski sistem kod koga se standardni ključ za šifrovanje zamenjuje ključem koji se dobija iz slike otiska prsta. KAES poboljšava sigurnost sistema omogućavajući ključu da bude glavni parametar šifarskog algoritma.

2.3 Generisanje biometrijskog ključa za korišćenje u DES-u

Kriptografija predstavlja značajno polje u oblasti šifrovanja podataka. Postoje različite šifarske tehnike, od jednostavnih do kompleksnih. Jedna od kompleksnih šifarskih tehnika zasnovanih na simetričnom ključu koristi DES algoritam. Ovaj rad istražuje jedinstveni pristup generisanju ključa preko otiska prsta. Generisani ključ se koristi kao ulazni ključ za DES algoritam.

Biometrija je nauka koja prepoznaje ljude po njihovim karakteristikama. Otisak prsta predstavlja najčešće korišćen parametar za prepoznavanje u odnosu na sve ostale biometrijske podatke. Orijentacija minucija jedinstveno prepoznaje otisak prsta. Ovakva funkcija se koristi za generisanje jedinstvenog koda za svakog pojedinca. Kod je modifikovan da obezbedi 56-bitni ključ za korišćenje u DES-u. DES je jedan od najčešće korišćenih algoritama sa simetričnim ključem. Ova tehnika šifrovanja može da se koristi za šifrovanje blokova karaktera.

2.3.1 Obrada otiska prsta

- **Izjednačavanje histograma**

Izjednačavanje histograma povećava kontrast slike. Kod ove tehnike ideja je da se obeleže nivoi sive boje zasnovani na verovatnosnoj podeli ulaznih nivoa sive boje. Izjednačavanje histograma transformiše vrednosti inteziteta slike prema sledećoj jednačini:

$$S_k = T(r_k) = \sum \Pr(r_j) = \sum n_j/n \text{ for } j=1..k.$$

U ovoj jednačini S_k je vrednost inteziteta u obrađenoj slici koja je odgovarajuća intezitetu r_k iz ulazne slike i $\Pr(r_j) = 1, 2, 3, \dots, L$ predstavlja nivo inteziteta ulazne slike otiska prsta.

- **Binarizacija**

Binarizacija slike otiska prsta predstavlja transformaciju 8-bitne sive slike otiska prsta sa nula vrednostima za grebene a jediničnim vrednostima za brazde. Minucije se izvlače iz prosvetljene, istanjene binarne slike. Jedna od tehnika pronalaženja minucija je tehnika ukrštenih brojeva.

- **Ukršteni brojevi**

Ovaj metod koristi skeletizovanu sliku gde se lokalni susedi svakog piksela grbena skeniraju koristeći prozor 3x3.

P4	P3	P2
P5	P	P1
P6	P7	P8

Tabela 5 - Prozor 3x3.

Vrednost ukrštenih brojeva (CN) se onda računa na sledeći način:

$$CN = 0.5 \sum |P_i - P_{i+1}| \text{ for } i=1 \dots 8$$

Gde je $P_9 = P_1$. Ova vrednost je definisana kao polovina sume razlike između parova susednih piksela u 3x3 prozoru. Koristeći osobine CN-a pomenute u tabeli ispod piksel grebena može biti obeležen kao završetak, grananje ili kao piksel bez značaja.

CN	Osobina
0	Izolovana tačka
1	Završetak
2	Nastavak grebena
3	Grananje
4	Tačka ukrštanja

Tabela 6 - Osobina ukrštenih brojeva.

Piksel je klasifikovan kao završetak grebena ako ima samo jedan susedni piksel u 3x3 prozoru, ako ima tri susedna piksela onda je u pitanju grananje i ako ima dva onda je nastavak grebena.

- **Standard šifrovanja podataka (DES)**

DES je blokovski šifrat zasnovan na simetričnom ključu objavljen od strane Nacionalnog Instituta za Standard i Tehnologiju (NITS). Proces šifrovanja se sastoji od dve permutacije koje se nazivaju početna i završna permutacija šesnaest *Feistel* rundi. Svaka runda koristi različiti 48-bitni ključ runde generisan od šifarskog ključa prema u napred definisanom algoritmu. DES koristi 16 rundi. Svaka runda DES-a je *Feistel* šifrat. Srce DES-a je DES funkcija koja primenjuje 48-bitni ključ u desnih 32 bita da bi se dobio 32-bitni izlaz.

2.3.2 Predloženi metod

Uzima ulaznu JPEG/JPG sliku a na izlazu daje 64-bitni ključ. Tako generisni ključ predstavlja ulaz u paritetnu drop tabelu DES generatora ključa. Ceo fokus rada je usmeren na drugi blok tj. generisanje 64-bitnog ključa od ulazne slike. Zatim se 64-bitni blok ključ generatora deli na pod blokove predstavljajući u detalje način funkcionisanja blokova. Ulazna JPEG/JPG slika se prebacuje u binarnu sliku sa dva nivoa interesa. Crni pikseli predstavljaju grebene i beli predstavljaju doline i takva slika može da se koristi za dobijanje minucija putem algoritma. Siva slika se prebacuje u binarnu nakon čega se dobija poboljšani kontrast. U procesu istanjivanja smanjuje se debljina otiska grebena na jedan piksel. Zatim sledi faza obeležavanja minucija preko metoda 3x3 prozora. Nakon toga se odklanjaju lažne

minucije. Kod završnog procesa set originalnih minucija se rekurzivno smanjuje dok se ne dobije 64-bitni ključ.

2.3.3 Algoritam za generisanje ključa

Korak 1: $NP \leftarrow$ broj minucija u regionu interesa.

Korak 2: $NP \leftarrow NP \bmod 64$

Korak 3: $NP \leftarrow NP - \text{Rem}$ // ovaj korak podešava da broj minucija bude deljiv sa 64.

Korak 4: $I \leftarrow NP/64$ // korak 4 daje broj rekurzivne interakcije da bi se obezbedila kompresija ključa na 64 bita.

Korak 5: Za 1 do I uradi sledeće: odbaci leva i desna 32 bita zatim podeli ostatak na Kl i Kg. Izvrši zamenu Kl i Kg.

- **Zaključak**

DES je jedan od najčešće korišćenih simetričnih šifarskih algoritama. Ovaj rad predstavlja nezavistan pristup generisanju ključa preko otiska prsta. Algoritam je uspešno implementiran i testiran u Matlab-u.

2.4 Prednosti i nedostaci biometrijskih rešenja u razvoju serisa autentifikacije

Elektronska povezanost ljudi u današnje vreme dostiže nivo na kome je potrebno konstantno raditi i razvijati nove tehnike sistema za autentifikaciju i bezbednost podataka. Postoji mogućnost da se autentifikujemo na osnovu tri parametara: nečim što znamo, nečim što imamo i nečim što jesmo. Ono što jesmo se reprezentuje našom biometrijom koja je jedinstvena za svaku osobu. Mogućnost korišćenja biometrije u razvoju sistema autentifikacije ima svoje prednosti kao i neke nedostatke u odnosu na klasične sisteme. Kod klasičnih sistema autentifikacije veliki problem nastaje kada je potreban visok nivo zaštite podataka. Tada je potrebno pamtiti ili bezbedno skladištiti kompleksne lozinke. Obično se biraju slabije lozinke da bi se lakše zapamtile kao što su ime, datum rođenja, ime nekog od članova porodice i td. U ispitivanju u kome je anketirano 1200 ljudi čak polovina je koristila neku od pomenutih metoda za generisanje svoje šifre. Takve šifre je lako dešifrovati da li prostim pogađanjem ili napadom putem rečnika. Bez obzira što je opšta preporuka da se za različite servise koriste različite šifre većina koristi istu tako da se kompromitovanjem jedne šifre ugrožava bezbednost svih servisa. Korisnici koji koriste kompleksnije šifre ili ih zapisuju ili nebezbedno čuvaju. Šifrovanjem se može doći do jakih šifara (šifarskog ključa) koje ne moraju da se pamte ali one su pak zaštićene jednostavnom šifrom sto dovodi u pitanje svrhu tog sistema. Veliki problem slabih šifara je taj što je napadačima dovoljno da dođu do jedne šifre da bi imali pristup nekom Intranetu tako da je sistem bezbedan koliko i najslabija šifra.

Konačno ako se šifra deli sa kolegom sistem ne može da prepozna ko je korisnik šifre. Pristup koji je baziran na nečemu što imamo je pristup uz pomoć tokena, identifikacionih kartica, kreditnih kartica ili ključeva. Tada se javlja mogućnost kompromitovanja takovog sistema ako dođe do gubitka ili krađe pomenutih predmeta.

Rešenje ovih problema se postiže korišćenjem biometrije. Biometriju ne možemo izgubiti, uvek nam je dostupna a ne moramo je pamtiti. Ako posmatramo napad metodom grube sile na biometrijski sistem, šansa da će takav napad uspeti zavisi od tačnosti poklapanja biometrijskih podataka. Predpostavićemo da je vrednost FMR-a 0.001% za određeni biometrijski sistem. Sa ovakvim podešavanjima nekoliko biometrijskih sistema (otisak prsta ili skeniranje irisa) mogu lako da budu na manje od 1% FNMR-a. Ako je vrednost FMR-a podešena na 0.001% onda je potrebno da napadač testira u proseku 100.000,00 uzoraka da bi jedan bio uspešan. Ovo se može postovetiti sa sigurnošću šifre od 5 nasumično izabranih brojeva. Da bi se napao biometrijski sistem potrebno je generisati veliku količinu biometrijskih uzoraka što je znatno teže nego generisati toliko isto nasumičnih stringova. Konačno, FMR biometrijskog sistema se može redukovati tako da pruža veći stepen sigurnosti što bi opet dovelo do povećanja FNMR-a.

Međutim, postoji i niz nedostataka koji su specifični za upotrebu biometrije u procesu autentifikacije. Jedan od najvećih nedostataka je taj da kompromitovanu biometriju ne možemo zameniti sa novom kao što je to slučaj sa šiframa ili karticama. Ako uzmemo primer ako se na aerodromima proveravaju putnici i traži se 100 najtraženijih kriminalaca (veličina baze je dakle 100 uzoraka) koristeći sistem baziran na otiscima prstiju koji radi na parametrima od 1% FNMR i 0.001% FMR. Ako sistem radi kao verifikacioni u 1% slučajeva ne bi mogao ispravno da verifikuje ispravnog putnika dok bi u 0.001% slučajeva pogrešno propustio traženog putnika. Ako je taj isti sistem postavljen kao identifikacioni sistem onda bi mu parametri bili FNMR 1% dok bi FMR bio $100 \times 0.001\% = 0.1\%$. Ovo znači da postoji 99% šanse da se uhvati traženi kriminalac ali ima i velike šanse da dođe do lažnih alarma (imajući uvidu da 200.000,00 ljudi koristi glavne aerodrome u U.S. dnevno došlo bi do 200,00 lažnih alarma).

Biometrijski sistemi imaju svoja ograničenja. Neka od najvažnijih su:

Buka u osetljivim podacima – Osetljivi podaci mogu biti puni šuma ili izvrnuti. Otisak prsta sa ožiljkom ili promukao glas su primeri podataka sa šumom. Takođe postoji mogućnost da se šum pojavi zbog neispravno montiranih senzora (zaprjani senzori) ili loši ambijentalni uslovi (loša osvetljenost) prilikom skeniranja lica. Podaci sa dosta šuma mogu dovesti do pogrešnog odbijanja.

Unutrašnje varijacije – Biometrijski podaci iste osobe se mogu značajno razlikovati odnosno nikad se ne može dobiti identičan uzorak iako se radi o istoj osobi. Npr. kod uzimanja otiska prsta položaj prsta nikad nije isti, takođe nije ni isti pritisak na skener kao i to što postoji razlika između samih skenera.

Osobnosti - Kako se očekuje da se biometrijske osobine značajno razlikuju između pojedinaca, postoje velike unutrašnje sličnosti grupe svojstava koje iskazuju te osobine.

Neuniverzalnost –Očekuje se da svaki pojedinac ima biometrijske osobine ali u stvarnosti postoji grupa ljudi koje ne možemo identifikovati na osnovu nekih biometrijskih uzoraka. Iz nekih otisaka prstiju nije moguće izvući karakteristične informacije koje su nam potrebne za identifikaciju. Problemi su loš kvalitet grebena koje poseduje 4% stanovništva i kod takvih osoba nije moguće sa standardnim senzorima dobiti dovoljno kvalitetnu sliku otiska prsta.

Napadi podmetanjem – Napadač je u mogućnosti da podmetne biometrijski uzorak legitimnog korisnika i na taj način prevari sistem. Ovakvi napadi su česti kada je u pitanju biometrija glasa[8] ili potpisa[9]. Takođe moguće je i fizičku biometriju podmetnuti. Na primer pokazano je da je moguće konstruisati veštački otisak prsta za razumno vreme [11]

2.5 Razvoj dvo-faktorskih sistema autentifikacije

Gledajući pojedinačno sisteme za identifikaciju dolazimo do zaključka da postoje velike mane kod klasičnih sistema zasnovanih na nečemu što znamo i kod sistema koji se oslanjaju na biometriju. Kako je potrebno obezbediti sisteme koji će biti daleko sigurniji od pomenutih došlo se do zaključka da se kombinovanjem ova dva načina rešava veliki broj nedostataka koji su karakteristični za unimodalne sisteme autentifikacije. Faktor autentifikacije je deo informacije koji se koristi da bi se prepoznao identitet korisnika. Koristeći dva faktora koja su nastala zasebno uvodimo dodatnu zaštitu i značajno poboljšavamo sigurnost sistema. Uobičajeni primer dvofaktorske autentifikacije možemo videti svakog dana na ATM aparatima gde se kombinuju fizički faktori sa personalnim. Dakle potrebno je fizički imati karticu kao i znati PIN da bi smo se uspešno autentifikovali.

3 Teorijske osnove istraživanja

3.1 Biometrija u sistemima autentifikacije

3.1.1 Istorijat biometrije

Biometrija (grč. *bios*-život, *metron*-mera) predstavlja skup automatizovanih metoda za jedinstveno prepoznavanje ljudi bazirano na jednoj ili većem broju njihovih fizičkih karakteristika.

Postoji nekoliko različitih mišljenja gde su začeci biometrije. Jedan od izvora kaže da su kineski trgovci u 14. veku koristili dečije dlanove i otiske nogu kako bi ih međusobno razlikovali. Sa druge strane biometrija se povezuje sa Alfonsom Bertiljanom (Alphonse Bertillon). On je radio kao činovnik u Pariskoj policiji kada je izmislio antropometriju krajem 19. veka. Po Bertiljanovom sistemu upotrebljavala se mera tela da bi se identifikovali kriminalci. Takođe, beležili su se i pokreti osumnjičenih kao i obeležja na njihovom telu, tetovaže i izrasline na koži. Mnoge razvijene policije u to vreme pre svih Britanska i Američka su prihvatile ovaj sistem i nazvale ga Bertiljinaž. One su koristile ovaj sistem da bi smanjili broj osumnjičenih koje su tražili. Ipak, merenja nisu bila precizna zato što su različiti pozornici merili na različite načine.

Bertiljanov sistem je podrazumevao i uzimanje otiska prsta ali se to nije smatralo kao važan element. Prvo čuvanje dokumenata sa otiscima prstiju se beleži od strane argentinskog policijskog zvaničnika. On je klasifikovao otiske po sistemu koji je ustanovio Ser Frensis Galton (Sir Francis Galton) antroplog koji je bio u srodstvu sa Čarlsom Darwinom. Galton je i objavio knjigu „Otisci“ koja je sadržala klasifikacioni sistem. On je prvi otkrio da ne postoje dve osobe sa istim otiskom prsta. Njegova klasifikacija detalja otiska prsta se koristi i danas.

Kompjuterske tehnike su značajno ubrzale razvoj automatizovanih biometrijskih tehnika. Ove tehnike se koriste za merenje naših ruku, prstiju, irisa, lica i glasa. Još 1985. je predložena ideja da je Iris jedinstven kao i otisak prsta. Razvoj sistema baziran na Irisu je počeo 1993. a 1994. je patentiran prvi algoritam za prepoznavanje Irisa.

3.1.2 Biometrijski sistemi

Biološke mere moraju da zadovolje sledeće uslove da bi se kvalifikovale kao biometrijske a to su:

- Univerzalnost – svaka osoba mora posedovati ovu karakteristiku.
- Jedinstvenost – karakteristika se mora razlikovati od pojedinca do pojedinca.
- Nepromenljivost – karakteristika se ne sme se menjati vremenom kao ni pri različitim uslovima prikupljanja.

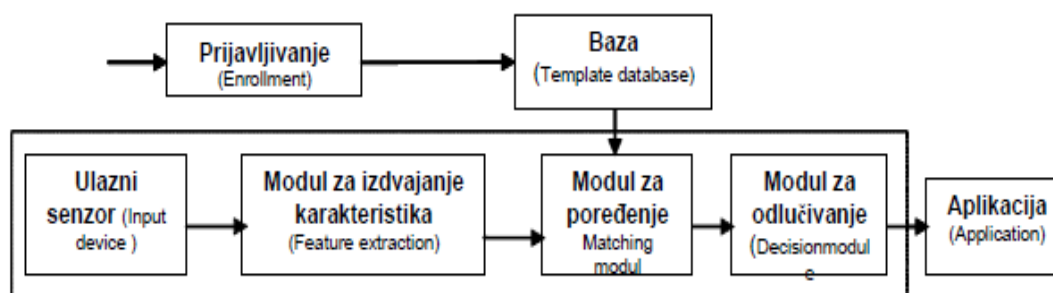
- Kolektabilnost – karakteristika mora biti prikupljiva i kvantitativno merljiva. [3]

BIOMETRIJA	univerzalnost	jedinstvenost	nepromenljivost	kolektibilnost	pozdanost	prihvatljivost	otpornost
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	S
Geometrija šake	S	S	S	V	S	S	S
Iris	V	V	V	S	V	N	V
Retina	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N

Tabela 7 - Poređenje različitih biometrija. V, S i N označavaju Visoko, Srednje i Nisko respektivno [3]

Svaki biometrijski sistem ima četiri modula:

- Senzorski modul – preko njega se beleži a zatim i digitalizuje biometrijska karakteristika.
- Modul za izdvajanje karakteristika – ovaj modul obrađuje digitalizovani podatak radi izdvajanja karakterističnih tačaka.
- Modul za poređenje – vrši se poređenje izdvojenih karakteristika sa podacima iz baze.
- Modul za donošenje odluka – kod ovog procesa identitet se prihvata ili odbija (verifikacija) ili utvrđuje na osnovu skora poređenja (identifikacija). [3]



Slika 9 - Moduli u biometrijskom sistemu [3]

3.1.3 Autentifikacija

Autentifikacija je postupak prepoznavanja osobe koja pokušava da pristupi sistemu. U kompjuterskom svetu identitet je definisan kao „jedinствeni naziv osobe, uređaja ili oba prepoznat od strane sistema“. Bezbednost svakodnevne autentifikacije je veoma bitna u današnje vreme. Postoje dva tipa autentifikacije:

- Verifikacija.
- Identifikacija.

3.1.4 Verifikacija

Verifikacijom se smatra postupak potvrđivanja identiteta neke osobe u smislu poređenja dobijenog podatka sa tačno određenim uzorkom. Ovde se vrši poređenje 1 : 1.

3.1.5 Identifikacija

Identifikacija znači upoređivanje postojećih podataka sa nepoznatom osobom koja pokušava da pristupi sistemu. Što se tiče biometrijske identifikacije tu se biometrijski otisak skladišti u bazu podataka a zatim se prilikom pokušaja da identifikacije novi dobijeni otisak poredi i traži se poklapanje. Kod identifikacije se vrši poređenje 1 : N, od osobe koja treba da se identifikuje su uzima biometrijski otisak a zatim se poredi za unapred pripremljenom bazom podataka.

Postoje pozitivna i negativna identifikacija. Cilj pozitivne je da se potvrdi da neka osoba zaista jeste ta za koju se predstavlja. Pozitivna identifikacija najčešće koristi metodu 1 : 1. Kod negativne identifikacije se polazi od suprotnih pretpostavki odnosno da osoba nije ta za koju se predstavlja i podaci biometrijski otisak se poredi sa bazom. Ovim se u stvari sprečava postojanje istih otisaka pod različitim imenom u bazi.

3.1.6 Metodi autentifikacije

Postoje tri metoda kako se možemo autentifikovati:

- Znanjem („nečim što znamo“)
- Objektom („nečim što imamo“)
- Biometrijom („nečim što jesmo“)

Autentifikacija znanjem zasniva se na tome da korisnik pamti neki podatak. Taj podatak je najčešće lozinka ili PIN kod.

Autentifikacija objektom predstavlja metod gde se koristi neki objekat kao što je ID kartica, pasoš, platna kartica, token da bi se izvršila autentifikacija.

Autentifikacija biometrijom je proces kada se koristi neki biometrijski identifikator koji pripada osobi samim rođenjem i koji se tokom života ne menja ili su promene beznačajne.

3.1.7 Performanse biometrijskih sistema

Biometrijski sistem na izlazu daje stepen poklapanja ulaznog sistema sa šablonom koji se čuva u bazi. Dva biometrijska uzorka od iste osobe ne mogu biti identična zbog uslova i vremena uzimanja tako da se ne može ni očekivati njihovo apsolutno poklapanje. Što je poklapanje veće to je sistem sigurniji da je ista osoba u pitanju. Odlučivanje se postiže granicom koja se postavlja za svaki sistem. Korišćenjem različitih vrsta parametara mogu se meriti, kvantifikovati i izražavati performanse biometrijskih sistema. Performanse i greške možemo razlikovati tokom procesa upisa, verifikacije i identifikacije.

3.1.8 Peroformanse i greške prilikom procesa upisa

Može doći do problema prilikom procesa upisa podataka. Ove poteškoće možemo meriti parametrima kao što su FTA (eng. *Failure to Acquire* – greška prilikom uzimanja podataka) i FTE (eng. *Failure to Enroll* – greška prilikom upisa).

- **FTA** – Označava procenat korisnika za koje sistem ne može prezentuje korisne biometrijske uzorke tokom procesa upisa. FTA pokriva FTE i kvalitativno prihvatanje biometrijskih podataka.
- **FTE** – Procenat korisnika za koje sistem nije u mogućnosti da generiše dovoljno kvalitetan šablon za upis, zbog ograničenosti tehnologije.

Što se tiče kvantifikacije, koristi se **TTE** (eng. *Time to Enroll*) pokazatelj, preko koga se označava trajanje procesa upisa od uzimanja biometrijskih osobina do kreiranja šablona.

3.1.9 Performanse i greške u procesu verifikacije

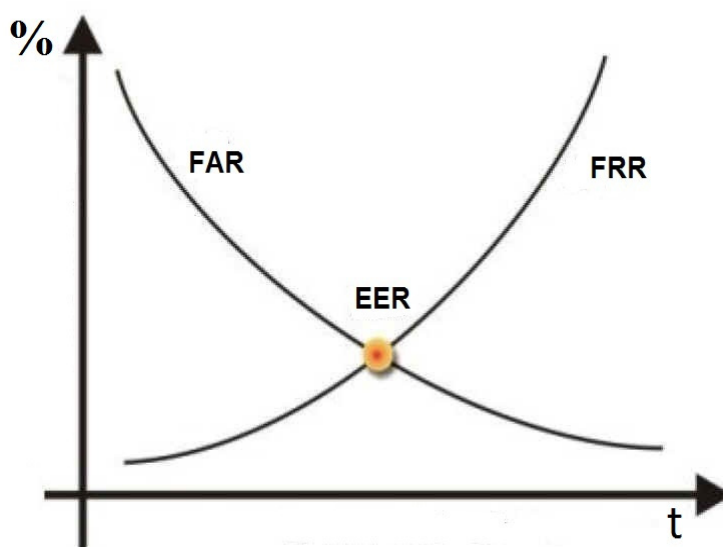
Tokom procesa verifikacije vrši se poređenje očitanih biometrijskih karakteristika sa šablonima iz baze. U tabeli ispod se vide rezultati istraživanja procenta greške koje su nastale korišćenjem biometrijskih osobina.

	Test	Parametar	Pogrešno odbijanje	Pogrešno prihvatanje
Otisak prsta	FVC 2004	Veliko deformisanje kože, rotacija prsta	2%	2%
	F _p VTE 2003	Zvanični podatak	0.1%	1%
Crte lica	FRVT 2002	Izmena osvetljenja	10%	1%
Glas	NIST 2004	Nezavisan tekst na više jezika	5-10%	2-5%

Tabela 8 - Procenat greške kod najčešćih biometrijskih karakteristika. [4]

Nakon uzimanja biometrijskog otiska sledi proces odlučivanja. U tom procesu se poredi trenutno uzeti biometrijski podatak sa podatkom koji čuvamo u bazi. Kako nije moguće da taj podatak bude identičan postavlja se granica do koje mere bi trebala da bude sličnost karakteristika dva uzorka da bi sistem nekoga prepoznao ili odbio. Rezultati odlučivanja mogu da generišu dve vrste grešaka koje možemo opisati kao:

- **FRR** – (eng. *False Rejection Rate* – greška odbijanja), poznata i kao greška prve vrste.
- **FAR** – (eng. *False Acceptance Rate* – greška prihvatanja), poznata i kao greška druge vrste.
- **EER** – (eng. *Equal Error Rate*), je veza između FAR i FRR. To je tačka preseka između FAR i FRR. Trebala bi da bude što manja što oslikava dobar balans osetljivosti sistema. [4]



Slika 10 - EER tačka preseka [5]

Ovakve greške se javljaju u pozitivnom režimu rada tj. kada se korisnik predstavlja. Što se tiče negativnog režima, razlikuju se takođe dva parametra:

- **FMR** (eng. *False Match Rate*), pokazuje kvalitet (posebnost, odlučnost) sistema.
- **FNMR** (eng. *False Non-Match Rate*), pokazuje robusnost sistema.

Neka je T sačuvani biometrijski šablon neke osobe, a i biometrijski uzorak prikupljen od te osobe. Tada imamo dve osnovne hipoteze:

$H_0: I \neq T$, ulaz ne odgovara šablonu i

$H_1: I = T$, ulaz odgovara šablonu.

Asocirane odluke u ovom slučaju su:

D0: Osoba nije ona za koju tvrdi da jeste

D1: Osoba je ona za koju tvrdi da jeste

Proces verifikacije uključuje poređenje T i I korišćenjem mere približnosti (eng. *similarity measure*) $s(T,I)$. Ako je rezultat poređenja manji od *threshold*-a (t), tada se smatra da je D0 tačno. U protivnom, prihvata se D1.

Prilikom testiranja hipoteza može doći do dve vrste grešaka:

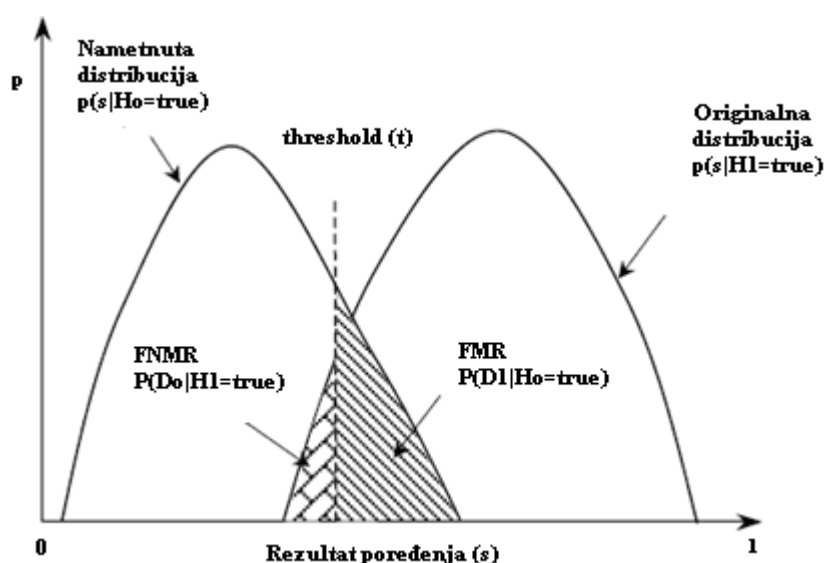
- Greška I vrste – *False Match* – kada se donese odluka D1, a tačna je hipoteza H0.
- Greška II vrste – *False Non-Match* - kada se donese odluka D0, a tačna je H1.

FMR je verovatnoća greške prve vrste, a FNMR je verovatnoća greške druge vrste:

$$\text{FMR} = P(D1 \mid H0 = \text{True})$$

$$\text{FNMR} = P(D0 \mid H1 = \text{True})$$

Da bi se procenila tačnost biometrijskog sistema, moraju se obraditi podaci velikog broja poređenja u kojima šablon odgovara uzorku (distribucija $p(s \mid H1 = \text{True})$), kao i poređenja u kojima to nije slučaj (distribucija $p(s \mid H0 = \text{True})$). U prvom slučaju distribucija se naziva originalnom (eng. *genuine distribution*), a u drugom nametnutom tj. lažnom (eng. *impostor distribution*).



Slika 11 - Originalna i nametnuta distribucija i odnos FNMR i FMR u odnosu na *threshold* [4]

FMR i FNMR su funkcije od sistemskog *threshold*-a t . Ako se t smanjuje da bi se sistem učinio tolerantnijim, tada se $\text{FMR}(t)$ povećava. Obrnuto, ako se t povećava da bi se sistem učinio sigurnijim, raste $\text{FNMR}(t)$. Dizajneri biometrijskih sistema moraju voditi računa o ovome tokom razvoja i ispitivanja. Preporučljivo je imati sistemske performanse u svim operativnim tačkama *threshold*-a. Za ovu svrhu se koristi pokazatelj-funkcija koja se naziva operativna karakteristika prijemnika (eng. *Receiver Operating Characteristic*, ROC), koja je, u osnovi, zavisnost FMR i $(1 - \text{FNMR})$ za različite vrednosti *threshold*-a.

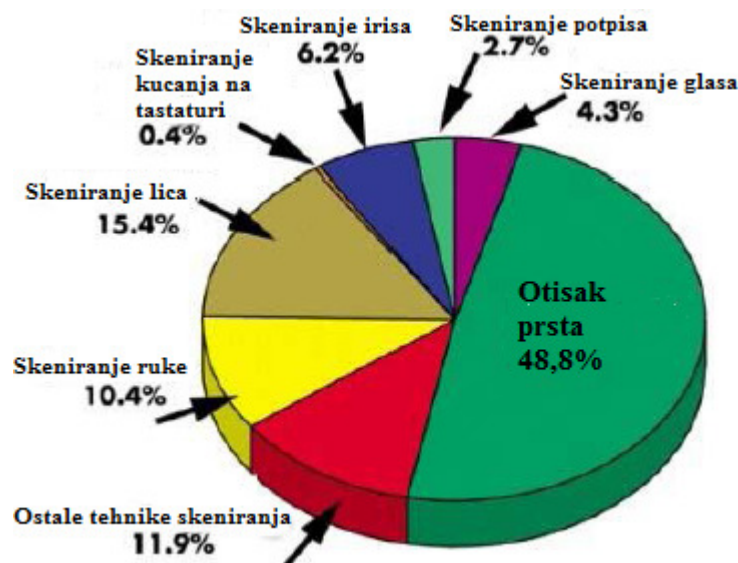
Postoje još neki „kompaktni“ pokazatelji koji se koriste da bi se sumirizovala tačnost verifikacionih sistema, od kojih se najčešće koristi EER (eng. *Equal-Error Rate*). Ovaj parametar pokazuje nivo greške za *threshold* za koji je $FMR(t) = FNMR(t)$.

Praktične performanse biometrijskih sistema primarno zavise od vrste aplikacije. Sa gledišta systemske tačnosti, veoma malo FNMR je osnovni zahtev, što je karakteristika npr. kriminoloških aplikacija. Sa druge strane, veoma malo FMR je ključno u aplikacijama za kontrolu pristupa. Između ovih krajnosti nalazi se niz aplikacija, gde se i FNMR i FMR moraju uzimati u obzir (npr. ATM card aplikacije). [4]

3.1.10 Najčešće korišćeni biometrijski sistemi

Kao što je ranije već rečeno, u biometrijskim identifikacionim sistemima prepoznavanje korisnika vrši se na osnovu njegovih fizičkih i/ili karakteristika ponašanja. Biometrijski sistemi se, shodno tome, mogu podeliti u dve osnovne kategorije i to:

- Sistemi zasnovani na prepoznavanju fizičkih karakteristika (otisak prsta, prepoznavanje lica, skeniranje irisa...).
- Sistemi zasnovani na prepoznavanju karakteristika ponašanja (prepoznavanje glasa, potpis, način hodanja...).



Slika 12 - Odnos biometrijskih tehnika u praksi [6]

3.1.11 Otisak prsta

Grana biometrije koja se bavi proučavanjem otisaka prstiju se naziva daktiloskopija. Prema njoj otisak prsta predstavlja konfiguraciju ispupčenja i udubljenja. Ispupčenja se drugačije nazivaju i papilarne linije. Ove linije se

pojavljuju još u vreme embrionog razvoja čoveka (6-7 nedelja) a u potpunosti se formiraju do 21. nedelje. Papilarne linije se razlikuju i kod jednojajčanih blizanaca.

Otiske prstiju možemo klasifikovati prema njihovim fizičkim karakteristikama odnosno prema obliku i pravcu kretanja papilarnih linija. Prema toj raspodeli postoji sedam osnovnih tipova otisaka prstiju: luk, jeloviti luk, petlja, dvostruka petlja, jamičasta petlja, spirala i mešoviti.



Slika 13 - Tipovi otisaka prstiju [7]

Nisu svi tipovi otiska prstiju podjednako zastupljeni. Petljasti tipovi čine najveći procenat od oko 60%, spiralni tip 30%, lučni tipovi i mešoviti tipovi po 5%.

Pored ovih osnovnih karakteristika otisci prstiju poseduju i singularne tačke koje su veoma bitne za prepoznavanje i razlikovanje. Kod ovih tačaka dolazi do nagle promene usmerenosti papilarnih linija. Na slici ispod su prikazane singularne tačke. [7]



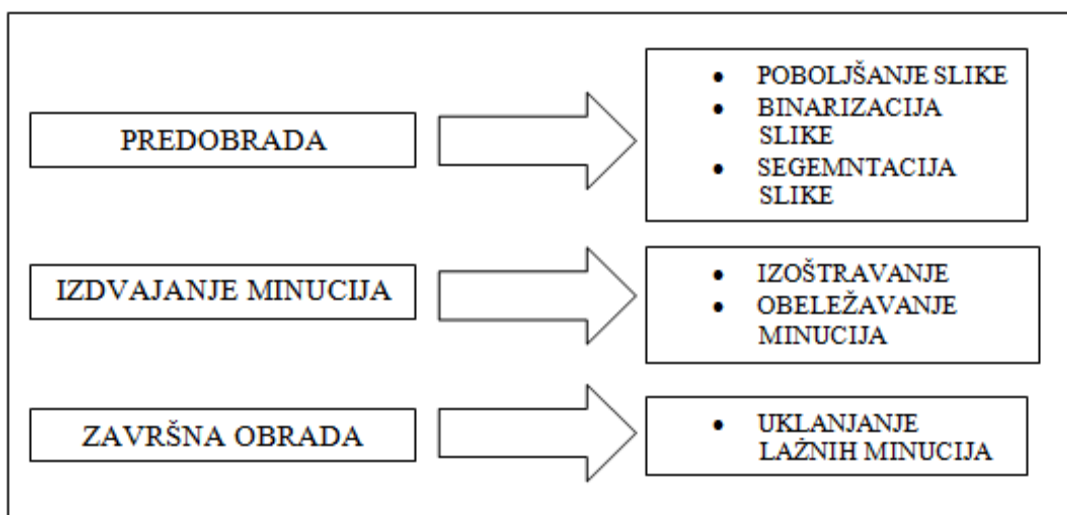
Slika 14 - Singularne tačke [7]

Verifikacija otiska odnosno svrstavanje u određeni tip se vrši uz pomoć globalnih karakteristika dok se identifikacija vrši na osnovu lokalnih odnosno detaljnih karakteristika. Te detaljne karakteristike se nazivaju minucije. Iako iz otiska prsta možemo izvući skoro 100 minucija uglavnom je dovoljno ne manje od 10-12 minucija za pozitivnu identifikaciju. Imamo nekoliko osobina papilarnih linija koje ih čine pogodnim i sigurnim pri identifikaciji. Prva od tih osobina je nepromenljivost broja i rasporeda minucija. Ne može se svojevremeno izmeniti izgled papilarnih linija jedino se mogu trajno oštetiti. Druga bitna osobina je neponovljivost. Poznati francuski matematičar Baltasar je dokazao da je verovatnoća da se podudaraju dva otiska praktično jednaka 0. Poslednja od veoma bitnih osobina je grupisanje. Ova osobina omogućava klasifikaciju na osnovu opštih sličnosti što znatno smanjuje vreme potrebno za identifikaciju. [7]

Autentifikacija otiskom prsta se zasniva na kompletnim podacima dobijenim sa otiska. Upotrebom određenog algoritma izdvaja se zapis koji je karakterističan za određeni otisak prsta. Za pretrage tipa 1:N koriste se podaci veličine 100-250 KB koji zahtevaju dosta dužu pretragu, nekoliko časova u odnosu na pretragu tipa 1:1 gde se koriste fajlovi veličine od 1 KB kod kojih se proces podudaranja završava za nekoliko sekundi. Postoji dva osnovna pristupa prilikom analize otiska prsta. Mogu se analizirati samo račvanja i završetci a može se i pratiti kompletan pravac svake papilarne linije.

3.1.12 Izdvajanje minucija

Minucije predstavljaju karakteristične tačke na otisku prsta svakog pojedinca. Na osnovu tih tačaka se vrši prepoznavanje. Proces izdvajanja minucija iz slike otiska prsta možemo podeliti u tri faze: predobrada, izdvajanje minucija, završna obrada.



Slika 15 - Proces izdvajanja minucija [8]

Za predobradu slike otiska prsta korišćena je tehnika pojačavanja histograma otiska prsta kao i Furijer-ova transformacija. Nakon toga slika se binarizuje korišćenjem lokalno prilagodivog metoda praga. Deljenje slike na

segmente se izvršava tri koraka: procena usmerenja blokova, izdvajanje na osnovu inteziteta usmerenja kao i izdvajanje regiona interesa morfološkim operacijama.

Faza izdvajanja minucija ima dva procesa od kojih se prvo vrši stanjivanje otiska grebena na debljinu koja je pogodna za dalju obradu a nakon toga se obeležavaju minucije.

Završna obrada slike otiska prsta predstavlja uklanjanje lažnih minucija da bi nakon te faze dobili prave karakteristične tačke nekog otiska prsta. [8]

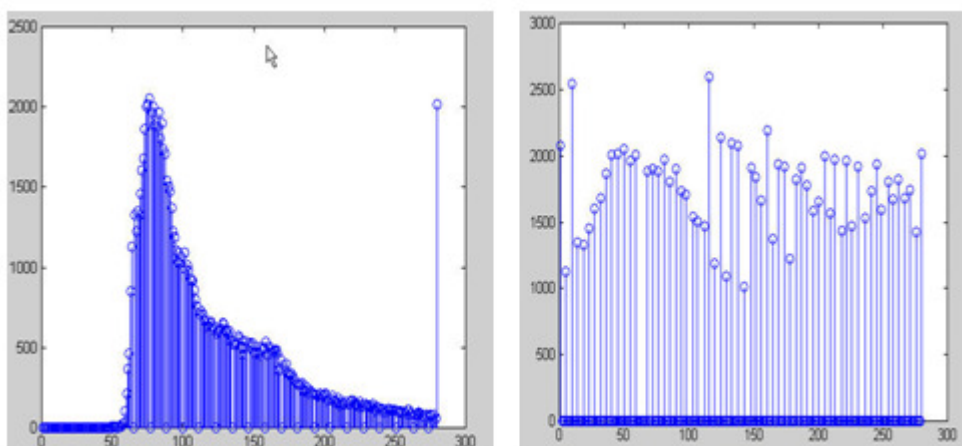
3.1.13 Poboljšanje kvaliteta slike otiska prsta

Ovo poboljšanje se vrši da bi slika bila čistija za predstojeće operacije. Posle uzimanja otiska prsta nekim od senzora koji su trenutno raspoloživi ne dobija se slika koja je odmah spremna za izdvajanje minucija iz razloga što prst može biti zaprljan, takođe može biti sam otisak oštećen kao i iz mnogih drugih razloga. Upravo iz tog razloga se vrši poboljšanje slike koje se postiže tako što se povećava kontrast između grebena i dolina kao i spajanje prekinutih linija grebena. Ovakve promene slike dovode do veće tačnosti kod procesa prepoznavanja minucija. U ovom radu su korišćene dve metode poboljšanja slike otiska prsta: pojačanje histograma i Furijer-ova transformacija. [8]

3.1.14 Normalizacija

Histogram predstavlja grafički prikaz tabelarnih frekvencija. Slika otiska prsta predstavlja digitalnu fotografiju koja je sastavljena od određenog broja piksela. Kako mi radimo sa *grayscale* fotografijom koja je sastavljena od nijansi sive boje vrednosti od 0 do 255 gde 0 predstavlja najtamniju a 255 najsvetliju nijansu, histogram takve fotografije bi bio grafički prikaz broja piksela određenih nijansi sive boje koji se nalaze na slici.

Pojačavanje histograma je metod obrade slike kojim se vrši podešavanje kontrasta slike, odnosno proširuje se distribucija vrednosti svakog piksela. Histogram slike otiska prsta je bimodalnog tip dok će nakon obrade imati vrednosti od 0 do 255 što dovodi do dosta jasnije slike otiska prsta iz koje se može dobiti više informacija. Ovako obrađena fotografija je ima daleko bolje performanse za dalju obradu.



Slika 16 - Razlika između originalnog (levo) i histograma nakon metode pojačavanja (desno). [8]

3.1.15 Poboljšanje slike Furijer-ovom transformacijom

Sledeći korak u obradi slike otiska prsta predstavlja njeno deljenje na blokove dimenzija 32x32 piksela nakon čega sledi Furijer-ova transformacija prema formuli:

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \times \exp \left\{ -j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N} \right) \right\}$$

Vrednosti: $u = 0, 1, 2, \dots, 31$ i $v = 0, 1, 2, \dots, 31$.

Da bi smo pojačali dominantnu frekvenciju određenog bloka slike množimo vrednost brze Furijer-ove transformacije FFT bloka sa njihovom dimenzijom nekoliko puta. Dimenzija originala je $FFT = \text{abs}(F(u, v)) = |F(u, v)|$.

Pojačani blok se dobija putem sledeće formule:

$$g(x, y) = F^{-1} \left\{ F(u, v) \times |F(u, v)|^k \right\}$$

gde $F^{-1}(F(u, v))$ se postiže:

$$f(x, y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) \times \exp \left\{ j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N} \right) \right\}$$

za $x = 0, 1, 2, \dots, 31$ i $y = 0, 1, 2, \dots, 31$.

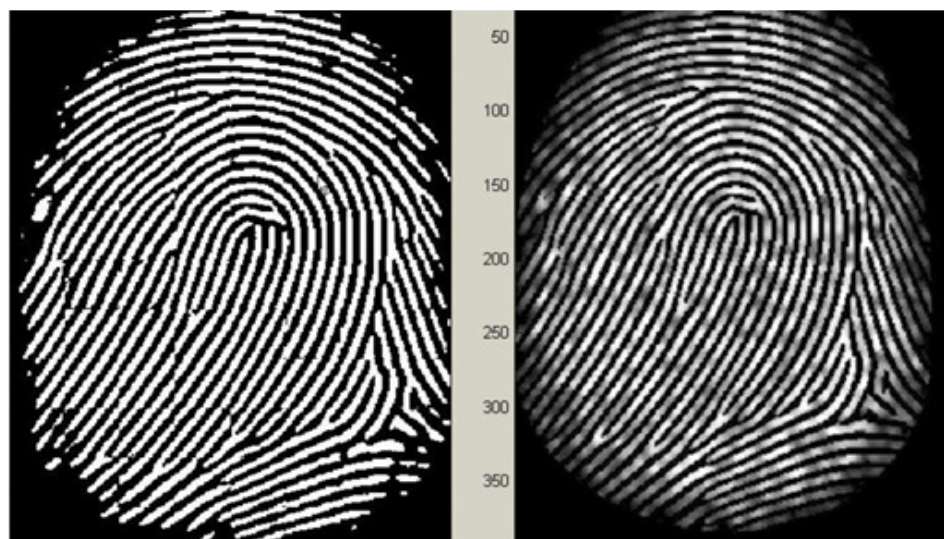
Vrednost k iz formule (2) je eksperimentalno utvrđena konstanta gde je neka optimalna vrednost $k = 0.45$. Povećanjem „ k “ dodatno bi poboljšali kvalitet otiska grebena popunjavanjem malih rupa duž linije grebena ali bi nasuprot tome imali pojavu spajanja lažnih spajanja grebena tako da bi onda završetci grebena mogli da postanu račvanje grebena što bi dovelo do lažnih minucija.

Dakle uz pomoć Furijer-ove transformacije dobili smo pobošanje slike tako što smo neke prekinute linje grebena spojili kao i to što smo eliminisali lažno spojene grebene. [8]

3.1.16 Proces kodovanja - binarizacija otiska prsta

Predstavlja proces koji transformiše 8-bitnu sivu sliku otiska prsta u 1-bitnu sliku sa vrednostima 0 za grebene a 1 za doline. Nakon ove transformacije dobijamo dosta jasniju sliku iz razloga što nema više nijansi sive boje već su grebeni predstavljeni crnom a doline belom bojom.

Lokalno prilagodiv metod binarizacije je korišćen za binarizaciju slike. Kod ovog metoda svaki piksel može da dobije dve vrednosti. Ako je vrednost osvetljaja piksela veća od srednjeg inteziteta vrednosti osvetljaja bloka dimenzija 16x16 piksela kome posmatrajući piksel pripada onda piksel dobija vrednost 1 a u suprotnom vrednost 0. [8]



Slika 17 - Slika otiska prsta nakon binarizacije (levo) [8]

3.1.17 Procena usemrenosti blokova

Slika otiska prsta se najpre deli na blokove dimanzija 16x16 piksela. Nakon toga se sledećim algoritmom procenjuje usmerenost blokova:

- Prvo se izračunava nagibna vrednost duž x i y ose za svaki piksel bloka. Ove vrenosti se računaju Sobel-ovim filterima.
- Za svaki blok koristi se sledeća formula za dobijanje aproksimacije najmanjih kvadrata smerenosti blokova:

$$tg2\beta = 2 \sum \sum (g_x * g_y) / \sum \sum (g_x^2 - g_y^2) \text{ za sve piksele u svakom bloku.}$$

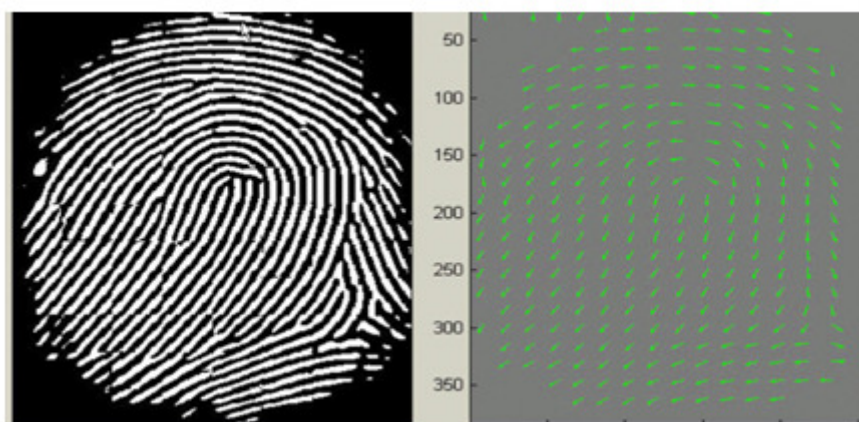
U formuli nagibne vrednosti duž x i y ose posmatramo kao kosinusne i sinusne vrednosti. Tako da tangensna vrednost usmerenosti blokova se procenjuje skoro isto kao u sledećoj formuli:

$$\tan 2\theta = 2\sin\theta \cos\theta / (\cos^2\theta - \sin^2\theta)$$

Nakon završene procene usmerenost svakog bloka, oni blokovi koji nemaju dovoljnu informaciju o grebenima i dolinama se odbacuju sledećom formulom:

$$E = \{2 \sum \sum (g_x * g_y) + \sum \sum (g_x^2 - g_y^2)\} / W * W * \sum \sum (g_x^2 + g_y^2)$$

Ako je dobijena vrednost E ispod granične vrednosti onda se posmatrani blok odbacuje u suprotnom se vrši procena usmerenosti bloka. [8]



Slika 18 - Mapa usmerenosti blokova. [8]

3.1.18 Segmetacija slike otiska prsta

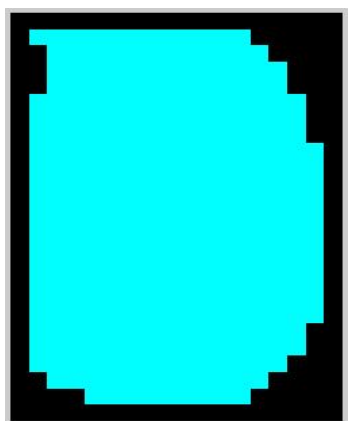
Da bi se postigli što bolji rezultati prilikom dobijanja karakteristični tačaka iz otiska prsta potrebno je te karakteristične tačke tražiti samo u delu slike na kome je otisak prsta vidljiv a ostatak slike je potrebno zanemariti. Tako posmatrani region se naziva region od interesa (RIO). Takođe, u region od interesa ne spadaju ni granični delovi otiska zato što bi oni predstavljali lažne završetke grebena odnosno lažne minucije.

Da bi se dobio RIO potrebno je proći kroz dva procesa. Prvi proces je procena usmerenosti blokova i provera promenljivosti usmerenja dok je drugi proces sastavljen od morfoloških metoda. [8]

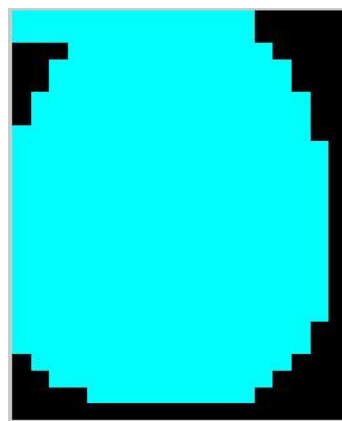
3.1.19 Izdvajanje regiona interesa morfološkim operacijama

Morfološke operacije kojima se dobija region interesa su „Open“ i „Close“. U okviru „Open“ operacije imamo dva procesa a to su erozija i dilatacija. Kod erozije svaki piksel objekta koji dodiruje pozadinu slike se menja u pozadinski

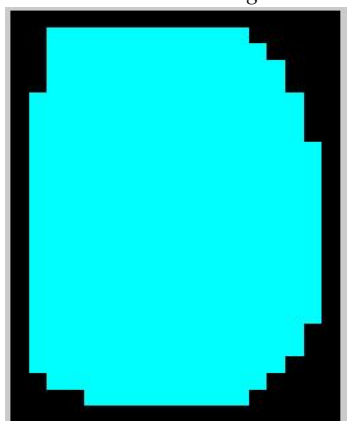
piksel, dakle objekat erodira dok kod dilatacije imamo suprotan proces gde se svaki pozadinski piksel koji dodiruje piksel objekta pretvara u piksel objekta. Kod operacije „Close“ imamo ista dva procesa samo što je redosled promenjen, prvo ide dilatacija pa erozija. Praktično to znači da ćemo koristeći operaciju „Open“ proširiti sliku i ukloniti nepotrebne tačke koje nam nisu potrebne dok se operacijom „Close“ rešavamo malih praznina.



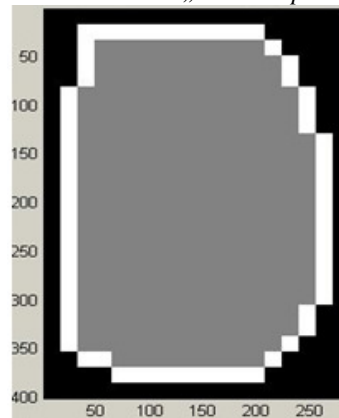
Slika 19 - Oblast originalne slike



Slika 20 - Oblast nakon „Close“ operacije



Slika 21 - Oblast nakon „Open“ operacije



Slika 22 - Oblast interesa sa granicom

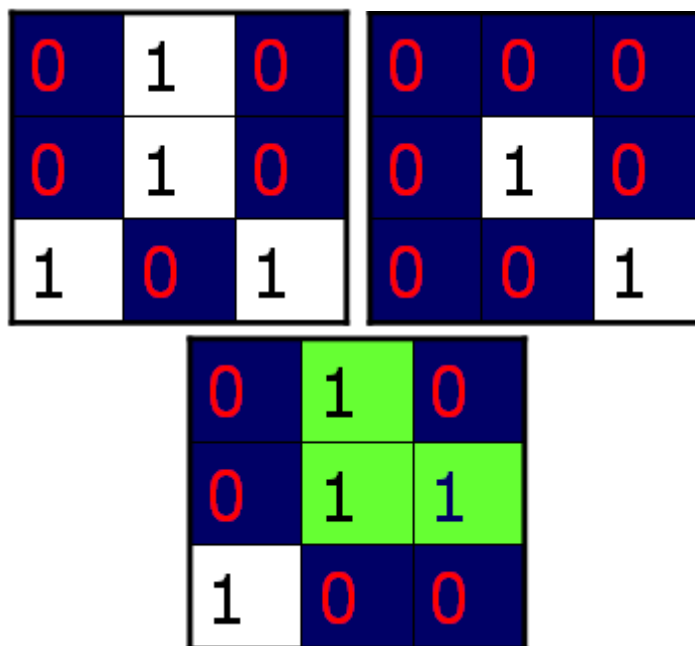
Na slici 22 je prikazana oblast od interesa koja će dalje biti razmatrana prilikom procesa prepoznavanja minucija. Granica koja predstavlja blokove između regiona interesa i pozadine se odbacuje i u obzir se uzima samo region unutar granica. [8]

3.1.20 Izoštavanje teksture otiska prsta

Stanjivanje linija se vrši da bi se eliminisali redundantni pikseli linije grebena sve dok se debljina linije ne svede na debljinu jednog piksela koristeći algoritam paralelnog stanjivanja. Prilikom svakog skeniranja cele slike otiska prsta algoritam obeležava redundantni piksel u svakom malom prozoru veličine 3x3 piksela. Nakon više skeniranja ti obeleženi pikseli se uklanjaju. Potrebno je izvršiti veći broj skeniranja kao bi algoritam dao bolje rezultate. [8]

3.1.21 Obeležavanje minucija

Posle izostravanja slike dolazi proces obeležavanja minucija. Ovaj proces nije ni malo jednostavan i može doći do obeležavanja tačaka koje imaju osobine minucija ali to u stvari nisu. Prilikom obeležavanja minucija posmatramo prozore dimenzija 3x3 piksela. Ako centralni piksel ima vrednost 1 a ima tačno tri susedna piksela sa vrednošću 1 onda centralni piksel predstavlja mesto grananja grebena odnosno minuciju. Ako centralni piksel ima vrednost 1 a ima samo jedan susedni piksel sa vrednošću 1 onda to posmatramo kao završetak grebana.



Slika 23 - Grananje grebena (gore levo), završetak grebena (gore desno), trostruko grananje.

Trostruko grananje je specijalni slučaj kada se grananje broji tri puta. Ako bi krajnji gornji i desni piksel koji su obeleženi zelenom bojom imali susedni piksel sa vrednošću 1 van posmatranog 3x3 prozora onda bi dva piksela u prozoru bila obeležena kao grane. Realno posmatrano samo se jedna grana nalazi u toj malojoj oblasti tako da se prilikom provere zahteva da se susedne grane ne računaju.

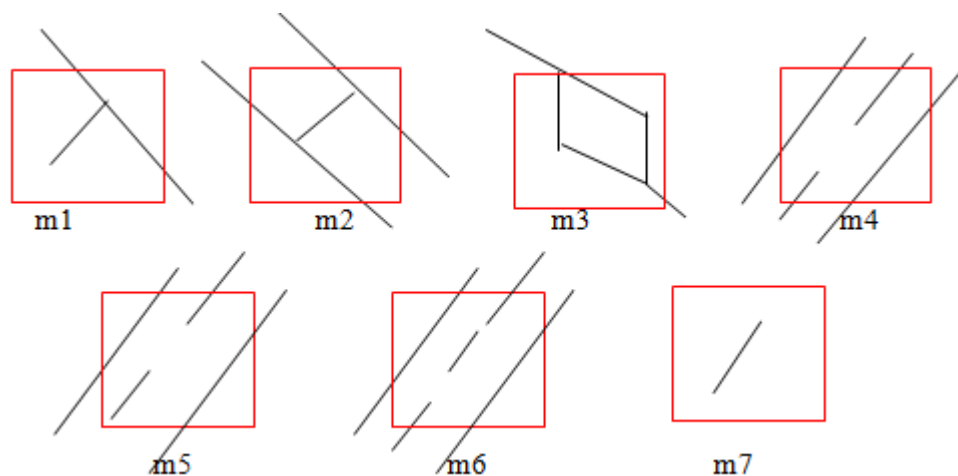
U ovoj fazi se procenjuje i prosečna širina između susednih grebena. Ova vrednost se dobija kada se saberu svi pikseli sa vrednošću jedan jednog reda istanjene slike otiska prsta nakon čega se dužina reda podeli sa tom vrednošću.

Zajedno sa obeleženim minucijama, obeležavaju se identifikacionim brojem i istanjene grebeni slike otiska prsta zbog budućih operacija. [8]

3.1.22 Uklanjanje lažnih minucija

Predprocesiranje ne obrađuje sliku perfektno tako da dolazi do određenih nepravilnosti koje je potrebno ukloniti. Na primer, pojavljuju se lažni prekidi grebena ili dolazi do pogrešnih ukrštanja grebena tako da nastaju lažne minucije koje treba odkloniti. Ukoliko se ne uklone ove lažne minucije u znatnoj meri utiču

na tačnost sistema tako da je proces uklanjanja minucija od presudne važnosti. Na slici ispod se nalazi sedam karakterističnih tipova lažnih minucija.



Slika 24 - Lažne minucije

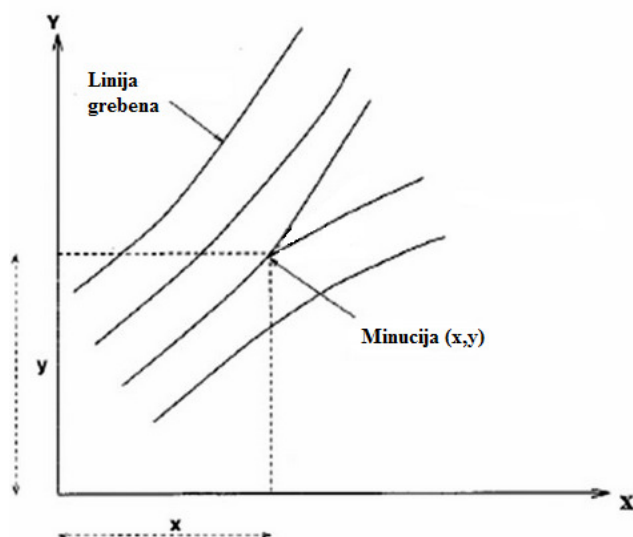
Ako pogledamo strukturu lažnih minucija možemo zaključiti da m1 predstavlja lažnu liniju preko doline koja se spaja sa grebenom. Lažno spajanje dva grebena je predstavljeno sa m2. Kod m3 imamo dva račvanja na istom grebenu. Lažni prekid linije grebena na jednom ili više mesta imamo kod m4, m5 i m6. Dok m7 predstavlja previše kratku liniju grebana.

Procedura uklanjanja lažnih minucija je sledeća:

- Ako je razmak između jednog račvanja i jednog završetka manja od vrednosti D koja predstavlja prosečnu udaljenost između susednih grebena i dve minucije se nalaze na istom grebenu (m1) otkloniti obe minucije.
- Ako je razmak između dva račvanja manji od D a nalaze se na istom grebenu ukloniti obe minucije (m2, m3).
- Ako se dva završetka nalaze u okviru distance D i prate usmerenost grebena a ispunjavaju uslov da između njih se ne nalazi ni jedan drugi završetak onda se smatraju lažnim minucijama i uklanjaju se (m4, m5, m6).
- Ako se dva završetka nalaze na kratkoj liniji grebena koja je kraća od D treba ukloniti obe minucije (m7). [8]

3.1.23 Upisivanje pozicija minucija

Kako postoji dosta varijacija prilikom prikupljanja otisaka prstiju kao što su intezitet pritiska na senzor, tip senzora, lako može doći do promene minucije iz jednog tipa u drugi. Iz tog razloga se svaka minucija kategoriše prema sledećim parametrima: kordinata na x osi, kordinata na y osi kao i orjentacija.



Slika 25 - Pozicija minucije u koordinantnom sistemu

Proračun orijentacije kod račvanja se mora posebno razmotriti. Svaki od tri grebena kod račvanja ima svoj pravac. Kako za dalji tok rada nije potreban ovaj parametar ovaj proces ćemo zanemariti.

3.2 Kriptološko-teorijska osnova

3.2.1 Kriptologija

Kriptologija je nauka o zaštiti podataka. Dugo je ova nauka bila primenljiva samo u profesionalnim sistemima koji su imali potrebu za ovakvim vidom zaštite (vojska, policija, bezbednosne agencije). Kako živimo u informacionom društvu gde svakodnevno nailazimo na veliku količinu informacija nameće se potreba da sačuvamo integritet tih podataka. Upravo ovakva situacija doprinosi ubrzanom razvoju kriptoloških mehanizama kao i razvoju načina izučavanja kriptologije.

3.2.2 Lozinka

Lozinka je unapred dogovoreni tajni signal koji se koristi kao metod raspoznavanja. U prošlosti su lozinke uglavnom bile reči koje potrebno izgovoriti da bi ste nekom dokazali da ste vi ona osoba koja se očekuje. U današnje vreme susrećemo se sa mnogim servisima koji zahtevaju da potvrdimo naš identitet nizom karaktera koji predstavlja lozinku. Idealna lozinka bi bila nešto što znamo, računar može to da potvrdi a niko drugi ne može da pogodi. U praksi ovakav scenario je skoro ne moguće postići. Da bi lozinka bila sigurna potrebno je zapamtiti a ne čuvati zapisanu. Međutim pamćenje kompleksnih lozinki nije ni malo lako tako da ljudi obično biraju manje kompleksne a samim tim i manje sigurne lozinke. Još jedan od problema predstavlja i potreba za korišćenjem više lozinki za različite sisteme što nas ponovo usmerava na korišćenje i pamćenje slabijih lozinki.

3.2.3 Kriptološki ključ

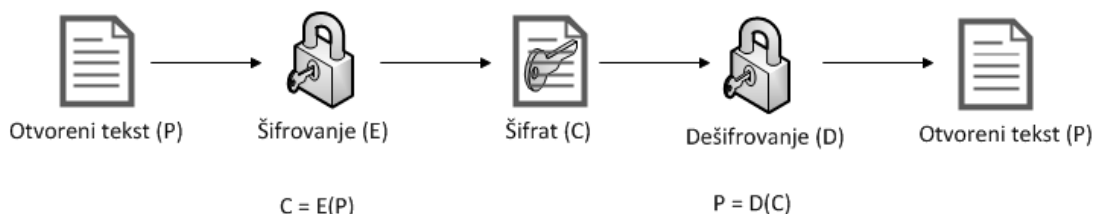
Kriptološki ključ predstavlja informacioni parametar koji određuje izlaz kriptološkog algoritma odnosno na osnovu njega otvoreni tekst prelazi u šifrat. Način dobijanja ključa je veoma bitan zato što jačina ključa određuje sigurnost kompletnog šifarskog sistema. Da bi ključ bio siguran potrebno je da bude generisan iz slučajnog niza podataka. Apsolutnu slučajnost je teško postići i njena mera se predstavlja entropijom. Izvori slučajnosti moguće je postići softverski analizirajući slučajne događaje kao što su: kretanje miša, šum elektronskih komponenti, aktivnost procesora. Međutim izvori ovakvih aktivnosti su ipak ograničeni. Generisanje ključeva iz prirode kao što je atmosferski šum, radioaktivni raspad daju mnogo bolje rezultate ali ih je teško meriti. Najpraktičnije rešenja za generisanje kriptoloških ključeva nam daje sopstvena biometrija. Nikad nije moguće zabeležiti isti biometrijski otisak što nam daje mogućnost da na osnovu npr. jednog prsta generišemo veliki broj ključeva.

Veličina ili dužina ključa je veličina koja se izražava u bitovima. Dužina ključa je direktno srazmerna jačini sigurnog sistema. Mnogi šifratni su zasnovani na javno poznatim algoritmima tako da kompletna sigurnost zavisi od dužine ključa. Kod simetričnih algoritama, koji koriste isti ključ za šifrovanje i dešifrovanje (DES, AES) je upravo takva situacija.

3.2.4 Simetrični šifarski sistem

Simetrični šifarski sistemi predstavljaju sisteme šifrovanja tajnim ključem pri čemu je ključ za šifrovanje identičan ključu za dešifrovanje. Karakterišu se relativno velikom brzinom rada i jednostavnom implementacijom.

Kod šifrovanja poruke upotrebom simetričnih sistema, tajnost i autentičnost poruke zasnivaju se na autentičnosti ključa, a sistem je bezbedniji ukoliko se ključ generiše na što slučajniji način.



Slika 26 – Proces šifrovanja i dešifrovanja u simetričnim šifarskim sistemima

Simetrični šifarski sistemi se dele na:

- Klasične
- Sekvencijalne
- Blokove

U nastavku će biti opisan rada blokovskih sistema.

Blokovske šifre se mogu posmatrati kao moderni naslednici klasičnih kodnih knjiga gde ključ određuje kodnu knjigu. Unutrašnji rad algoritama savremenih blokovskih šifara je kompleksan. Kod blokovskih šifara, otvoreni tekst i šifrat se dele na blokove fiksne dužine (64, 128, 192, 256) u bitovima, zatim se svaki blok nezavisno šifrjuje. Šifrat se dobija na osnovu otvorenog teksta iterativnom primenom funkcije runde. Ulaz u funkciju runde je ključ i izlaz prethodne runde. Blokovske šifre kombinuju svojstva konfuzije i difuzije i kompletnost. Najčešće se realizuju softverski.

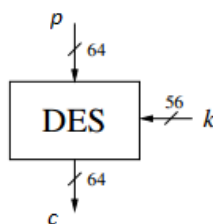
3.2.4.1 DES

Data Encryption Standard (DES) razvijen je 1970-tih godina. Predstavlja blokovsku šifru sa simetričnim ključem usvojenu od strane NIST-a (eng. *National Institute of Standards and Technology* - američka federalna agencija za standarde i tehnologiju). Pripada grupi modernih šifara.

Cilj dizajna je bio da se uvedu principi *konfuzije* i *difuzije*.

- **Konfuzija** – Šifrat treba da zavisi od otvorenog teksta i ključa na složen način.
- **Difuzija** – Svaki bit šifrata treba da je funkcija svih bitova otvorenog teksta i svih bitova ključa.

DES vrši šifrovanje blokova dužine 64 bita ključem dužine 56 bita.



Slika 27 – DES blokovska šifra

Svaki blok otvorenog teksta se transformiše u 16 rundi koje obavljaju identičnu operaciju. U svakoj rundi se koristi 48 bita ključa (podključ).

DES je Fejstel šifra. Fejstel šifra (nazvana po pioniru blokovskih šifara Horstu Fejstelu) ne predstavlja određenu šifru nego generalni princip dizajniranja šifri. Kod Fejstel šifri otvoreni tekst P se deli na blokove tako što se svaki blok deli na dva dela – levi L i desni R .

$$P = (L_0, R_0)$$

U svakoj rundi i ($i = 1, 2, \dots, n$), leva i desna strana se izračunavaju na sledeći način:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i) \end{aligned}$$

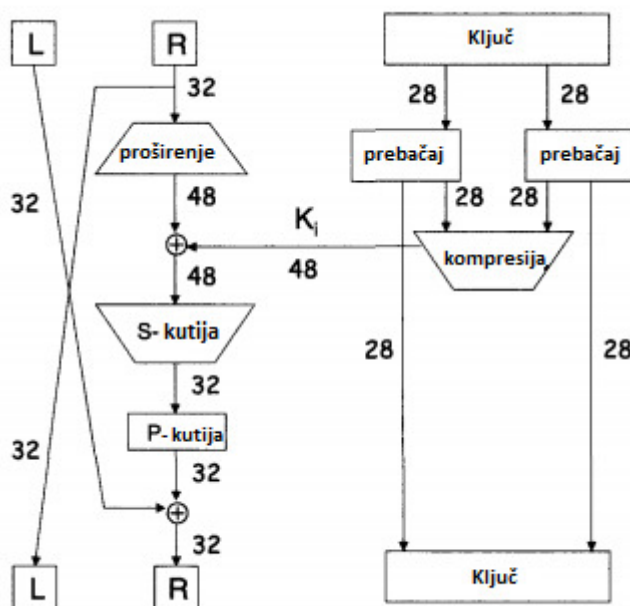
F je funkcija runde.

K_i je podključ za rundu i . Podključ je izveden iz ključa K prema specifičnom algoritmu. Izlaz iz runde je šifrat C .

$$C = (L_n, R_n)$$

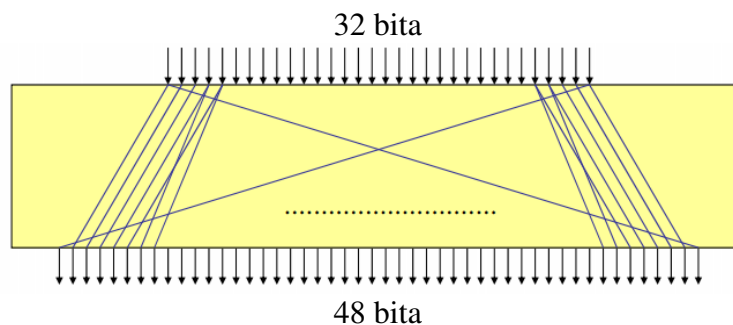
Pošto je DES Fejstel šifra, šifrovanje prati pravila prikazana u jednačini:

$$F(D_{i-1}, K_i) = P - kutija(S - kutija(proširenje(D_{i-1} \oplus K_i)))$$

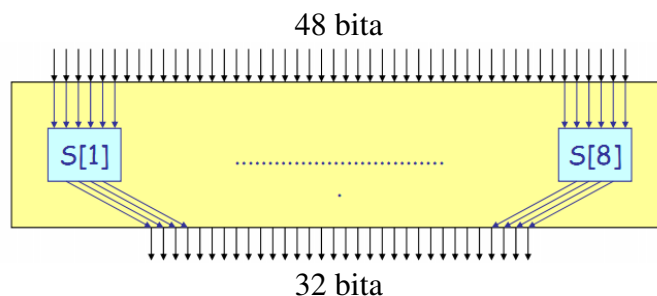


Slika 28 – Jedna runda DES algoritma

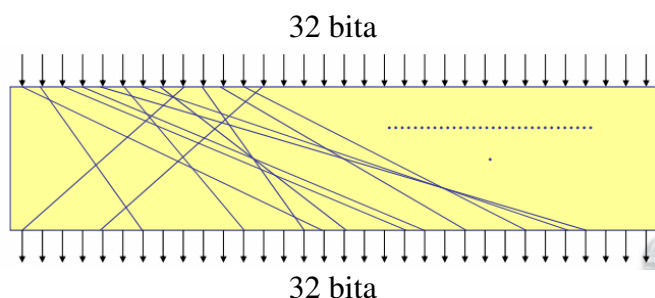
E-kutija (*expand*) proširuje i permutuje 32 ulazna bita na 48 bitova i podključ je XOR-ovan sa rezultatom. Potom S-kutije (*substitution*) kompresuju tih 48 bitova na 32 bita pre nego što se rezultat prosledi P-kutiji (*permutation*). Izlaz iz P-kutije je XOR-ovan sa starom levom polovinom da bi se dobila nova desna polovina.



Slika 29 – E-kutija



Slika 30 – S-kutija



Slika 31 – P-kutija

Trideset godina intenzivne kriptanalize nije otkrilo nikakve propuste tipa “back door”. Sa aspekta sigurnosti, danas je DES ranjiv na *brute-force* napade samo zbog male dužine ključa, a ne zato što postoji neki ozbiljniji skraćeni napad. Iako su razvijeni neki napadi koji teorijski zahtevaju neznatno manje posla u odnosu na potpunu pretragu ključeva, svi dosad napravljeni programi za razbijanje DES-a jednostavno isprobavaju sve kombinacije ključeva dok ne naiđu na onu pravu, odnosno, primenjuju potpunu pretragu ključeva.

3.2.4.2 AES

Advanced Encryption Standard (AES) je najrasprostranjenija simetrična šifra. Iako se izraz „Standard“ odnosi samo na Vladu SAD-a, AES je obavezan za upotrebu i u raznim industrijskim standardima, a takođe se koristi i u komercijalne svrhe. U komercijalne standarde koji koriste AES spadaju standard za Internet sigurnost IPsec, TLS, standard za šifrovanje Wi-Fi komunikacije IEEE 802.11i, SSH (Secure Shell) mrežni protokol, Internet komunikacija preko *Skype*-a i razni drugi sigurnosni proizvodi.

Razvijen krajem 1990-tih godina od strane NIST-a i zasnovan je na Rindael (izgovara se slično kao eng. *Rain doll*) algoritmu.

AES je kao i DES, blokovska šifra sa simetričnim ključem standardizovana od strane NIST-a. Za razliku od DES-a, nije Feistel šifra. Glavna posledica toga je da

AES operacije moraju biti povratne da bi se nešto moglo dešifrovati. Takođe, za razliku od DES-a, AES algoritam ima komplikovanu matematičku strukturu.

Otporan na poznate napade, veoma je brz, moguć je paralelni dizajn, kao i implementacija na mnogim procesorima i pametnim karticama. Do danas nisu uočeni bolji napadi od *brute-force* napada na AES.

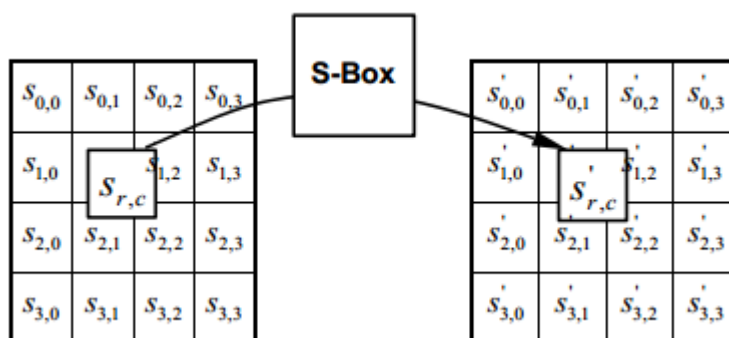
Funkcionalni parametrima AES-a su:

- Dužina bloka otvorenog teksta je 128, 192 i 256 bitova
- Dužine ključa je 128, 192 i 256 bitova
- Ima ukupno od 10 do 14 rundi, zavisno od dužine ključa
- U svakoj rundi koriste se 4 funkcije
 - Nelinearni sloj (*ByteSub*)
 - Sloj lineranog mešanja (*ShiftRow*)
 - Nelinearni sloj (*MixColumns*)
 - Dodatni sloj ključa (*AddRoundKey*).

Bitno karakteristika AES-a je da je dužina bloka otvorenog teksta u potpunosti nezavisna od dužine ključa. To znači da je moguće šifrovati blok otvorenog teksta dužine 128 bitova sa ključem dužine 256 bitova.

Sve operacije AES algoritma obavljaju se na dvodimenzionalnom nizu bitova, odnosno matrici stanja. Šifrovanje, odnosno dešifrovanje se vrši tako što se ulazni blok podatka kopira u matricu stanja nad kojom se sprovode razne operacije. Završna vrednost matrice ili stanje, kopira se u izlazni šifarski blok. AES ulazne podatke tretira kao matrice dimenzije $[4 \times 4]$.

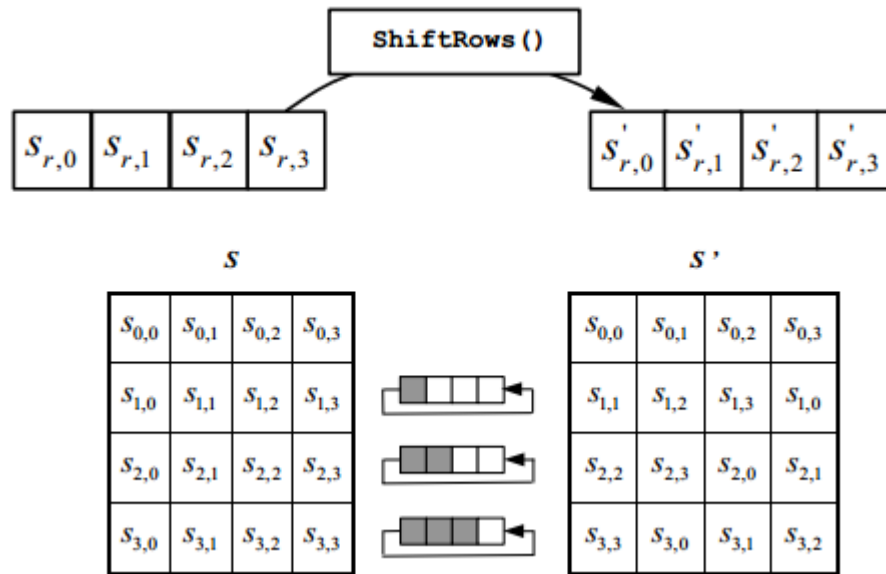
ByteStub operacija se primenjuje na svaki bajt a_{ij} tako da je $b_{ij} = \text{ByteStub}(a_{ij})$. Kao rezultat se dobija niz b_{ij} prikazan na Slika 32 – *ByteStub*.



Slika 32 – *ByteStub* operacija

ByteStub operacija je za AES isto što i S-kutija za DES. Može se posmatrati kao nelinearna, ali invertibilna, kompozicija dve matematičke operacije ili kao tabela.

ShiftRow operacija predstavlja ciklično pomeranje bajtova u svakom redu matrice 4x4. U prvom redu ne postoji pomeranje, u drugom se pomera jedan bajt, u trećem dva i u poslednjem redu tri bajta se pomeraju u levo.



Slika 33 – ShiftRow operacija

MixColumn operacija se primenjuje na svaku kolonu 4x4 matrice kao što je prikazano na Slika 34 – MixColumn .

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad \text{za } 0 \leq c < Nb.$$

Slika 34 – MixColumn operacija

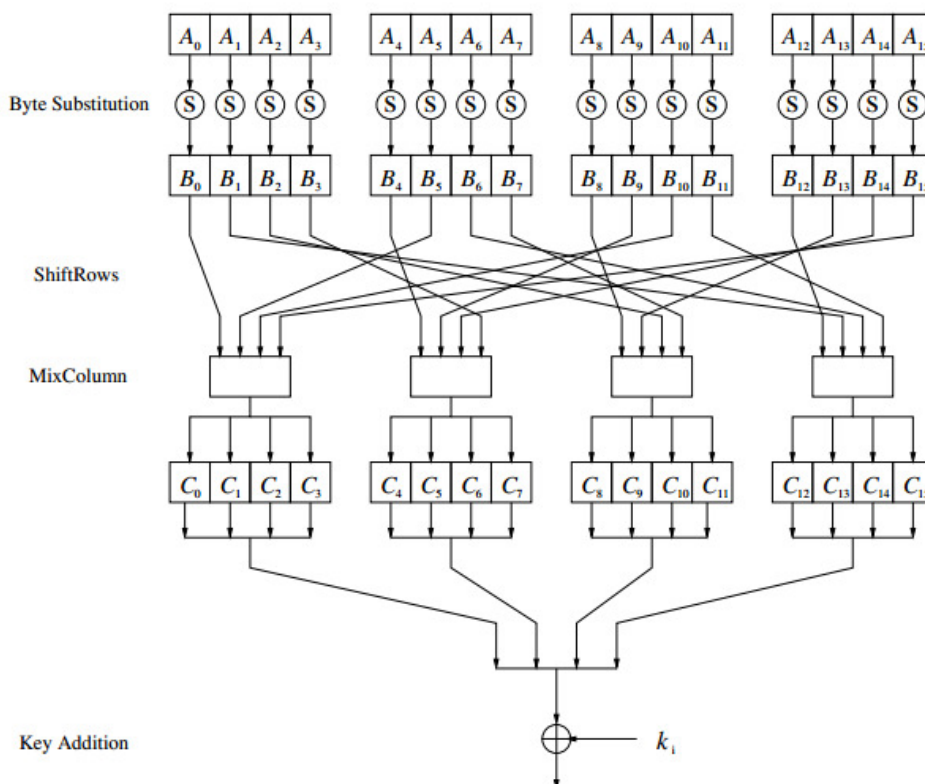
Ovu operaciju čine operacije pomeranja i XOR-ovanja.

AddRoundKey je jednostavna operacija. Kao kod DES-a, algoritam rasporeda ključa je korišćen da bi se generisao podključ za svaku rundu.

Ako je K_{ij} matrica 4x4 podključa za određenu rundu, onda se podključ XOR-uje sa trenutnom matricom 4x4 a_{ij} koja predstavlja ulaz kao što je prikazano u nastavku:

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \oplus \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Slika 35 – AddRoundKey operacija

Slika 36 – AES funkcija runde za runde 1,2,..., $n-1$

3.2.5 Heš funkcije

Heš funkcija predstavlja sumu poruke. Problem nastaje kada se iz različitih poruka dobija ista heš vrednost odnosno ista suma. Kriptografski cilj je da jedan heš odgovara samo jednoj poruci. Heš se koristi za proveru integriteta dobijene poruke. Izmena samo jednog znaka u poruci daje različitu heš vrednost. Dakle ako bi napadač promenio sadržaj presretnute poruke primalac bi mogao to da zna ako poznaje heš vrednost poruke pre slanja.

Heš funkcije se ne koriste za šifrovanje. Njihova oblast primene se svodi na integritet prenesenih podataka, autentifikaciju učesnika u komunikaciji, neporecivost transakcija i sl. Suština heš funkcija je u jednosmernosti koja predstavlja posledicu kompresije sa gubicima. Dužina heš vrednosti je konstantna za izbranu heš funkciju i ne zavisi od dužine otvorenog teksta dok je dužina šifrata uglavnom približna dužini otvorenog teksta. Takođe, ukoliko poznajemo ključ možemo izvršiti dešifrovanje dok iz heš vrednosti nije moguće dobiti poruku jer ne postoji inverzna funkcija.

Najpoznatija grupa hash funkcija je MD4 grupa. MD5, SHA i RIPEMD pripadaju ovoj grupi

3.2.5.1 MD5

MD5 (eng. *Message Digest*) predstavlja jednosmernu funkciju koja za ulaz proizvoljne dužine daje izlaz od 128 bita. Razvijena je 1991. godine od strane Rolanda Rivesta. Bio je široko rasprostranjen (za sigurnost Internet protokola, za

poređenje sačuvanih lozinki). Poznato je da ima slabosti i da nije otporna na kriptografske napade. I pored ovoga, zbog svoje brzine rada se koristi u proveru integriteta većih fajlova.

3.2.5.2 SHA

Nakon što su primećene slabosti kod MD5 funkcije, 1993. godine, NIST je uveo novi standard - SHA (eng. *Secure Hash Algorithm*). Prvi član ove porodice je nazvan SHA, iako je on danas poznat pod nazivom SHA-0. On je 1995. god. modifikovan i dobijen je SHA-1. Razlika između SHA-0 i SHA-1 ogleda se u rasporedu funkcija za kompresovanje koji obezbeđuje veću kriptografsku sigurnost.

NIST je 2002. god. uveo novu familiju algoritama (SHA-2) koje se razlikuju po dužini *hash* vrednosti: SHA-256, SHA-384 i SHA-512. SHA-224 objavljena je 2004.god. Ovi algoritmi su bezbedniji zbog dužine hash vrednosti i određenih promena u algoritmu. Takođe su kompatibilni sa AES blokvsom šifrom.

SHA-1 predstavlja industrijski standard u kriptografiji i pored toga što algoritmi iz SHA-2 porodice pružaju veću sigurnost.

SHA-0 i SHA-1 algoritmi se danas ne mogu smatrati bezbednim zato što postoje

kriptografski napadi koji su sposobni da pronađu koliziju za relativno kratko vreme.

Algoritam		Izlaz (u bitovima)	Inicijalna veličina u bitovima	Broj rundi	Kolizije
SHA-0		160			
SHA-1		160	512	80	Da
SHA-2	SHA-224	224	512	64	Za sad ne
	SHA-256	256	512	64	Ne
	SHA-384	384	1024	80	Ne
	SHA-512	512	1024	80	Ne

Tabela 9 – Poređenje heš algoritama.

3.3 Teorijsko-informaciona analiza

3.3.1 Entropija

Entropija predstavlja meru neodređenosti pridruženu slučajnoj promenljivoj. Entropiju u teoriji informacija prvi je uveo Klod Šenon i ona predstavlja očekivanu vrednost informacije sadržane u poruci. Koncept je Klod Šenon prikazao u svom čuvenom radu iz 1948. godine „Matematička teorija komunikacija“.

Šenonova entropija predstavlja apsolutnu granicu najbolje moguće kompresije bez gubitka bilo kakve komunikacije pod izvesnim ograničenjima: ako ako tretiramo poruke da su kodovane kao niz nezavisnih slučajnih promenljivih sa istom raspodelom, prva Šenonova teorema pokazuje da u graničnom slučaju, srednja dužina najkraće moguće reprezentacije za kodovanje poruka u datom alfabetu je njihova entropija podeljena sa logaritmom broja simbola u ciljanom alfabetu. [9]

3.3.2 NIST testovi

NIST-ov paket testova predstavlja statistički paket koji se sastoji od 15 testova koji su razvijeni za testiranje slučajnosti binarne sekvence koje proizvode hardver ili softver na bazi kriptografski slučajnih ili pseudoslučajnih brojeva. Ovi testovi se fokusiraju na različite vrste neslučajnosti koje bi mogle da postoje u nizu. Neki testovi su podeljeni u više podtestova.

Ispitivanje učestalosti u nizu

U fokusu ovog testa je ispitivanje odnosa jedinica i nula u nizu bitova. Cilj je uočavanje jednakosti pojavljivanja ove dve vrednosti. Potreban je približan broj jedinica i nula u sekvenci. Svi podtestovi koji proizilaze iz ovog testa direktno zavise od njegove uspešnosti.

Test se poziva preko metode **Frequency(n)** gde je n dužina bitnog uzorka. Metoda koristi i dodatni parametar ε koji predstavlja niz bitova generisanig preko RNG ili PRNG koji se testira.

Primer:

- Ulazni parametri

$\varepsilon=11001001000011111101101010100010001000010110100011000010001$
 $10100110001001100011001100010100010111000$

$n = 100$

- Obrada

$$S_{100} = -16$$

$$s_{obs} = 1.6$$

- Izlazni parametar

$$P = 0.109599$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje učestalosti u bloku

Test posmatra se odnos jedinica i nula u n-bitnim blokovima. Cilj predstavlja uočavanje jednakosti broja jedinica i nula u svakom n-bitnom bloku.

Poziv testa se vrši preko metode **BlockFrequency**(M, n) gde su

M – dužina svakog bloka

n – dužina bitnog uzorka

Kao i kod testa za ispitivanje učestalosti u nizu, koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 11001001000011111101101010100010001000010110100011000010001$
 $10100110001001100011001100010100010111000$

$$n = 100$$

$$M = 10$$

- Obrada

$$N = 10$$

$$X^2 = 7.2$$

- Izlazni parametar

$$P = 0.706438$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje uzastopnih ponavljanja istih bitova u nizu

Posmatrana karakteristika u ovom testu je ukupan broj uzastopnih ponavljanja jednog broja u nizu. Svrha ovog testa je da se odredi da li broj uzastopnih ponavljanja nula i jedinica odgovara očekivanog slučajnoj sekvenci.

Poziv testa se vrši preko metode **Runs(n)** gde je n dužina bitnog uzorka. Takođe postoji i dodatni parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 11001001000011111101101010100010001000010110100011000010001$
 $10100110001001100011001100010100010111000$

$n = 100$

$\tau = 0.02$

- Obrada

$\pi = 0.42$

$Vn(obs) = 52$

- Izlazni parametar

$P = 0.500798$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje najdužeg uzastopnog ponavljanja jedinica u bloku

U ovom testu se posmatra najduže uzastopno ponavljanje jedinica u n -bitnim blokovima. Svrha je određivanje da li se dužina najdužeg uzastopnog ponavljanja poklapa sa dužinom koja bi se očekivala u nizu slučajnih brojeva.

Poziv testa vrši se preko metode **LongestRunOfOnes(n)** gde je n dužina bitnog uzorka. Takođe postoji i dodatni parametar ε .

M – dužina svakog bloka. Test je podešen tako da za M koristi tri vrednosti: $M = 8$, $M = 128$ i $M = 104$ u skladu sa dužinom parametra n :

Minimum n	M
128	8
6272	128
750,000	104

Tabela 10 – Rezultati testa niza jedinica

Primer:

U slučaju kada je $K = 3$ i $M = 8$:

- Ulazni parametri

$\varepsilon = 11001100000101010110110001001100111000000000001001001101010$
 $1000100010011110101101000000011010111110011001110011011011000101100$
 10

$n = 128$

- Obrada

Maksimalno ponavljanje podbloka	Maksimalno ponavljanje podbloka
11001100 (2)	00010101 (1)
01101100 (2)	01001100 (2)
11100000 (3)	00000010 (1)
01001101 (2)	01010001 (1)
00010011 (2)	11010110 (2)
10000000 (1)	11010111 (3)
11001100 (2)	11100110 (3)
11011000 (2)	10110010 (2)

Tabela 11 – Rezultati ponavljanja podblokova

$v_0 = 4; v_1 = 9; v_2 = 3; v_4 = 0; x_2 = 4.882457$

- Izlazni parametar

P-value = 0.180609

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitvanje stanja binarne matrice

Svrha ovog testa je provera linearne zavisnosti između podnizova fiksne dužine iz originalnog niza.

Poziv testa vrši se preko metode **Rank(n)** gde je n – dužina bitnog uzorka. Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 11001001000011111101101010100010001000010110100011000010001$
 $10100110001001100011001100010100010111000$
 $n = 100$

- Obrada

$N_1 = 46$
 $N_0 = 47.5$
 $d = -1.376494$

- Izlazni parametar

$P = 0.168669$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje diskretne Furijerove transformacije

Fokus ovog testa predstavlja najviše vrednosti diskretne Fourier-ove transformacije niza. Svrha ovog testa je da otkrije periodične funkcije (tj. , ponavljaju obrasce

koje su blizu jedna drugoj) u testiranog nizu koja bi ukazivala na odstupanje od pretpostavke o slučajnosti . Namera je da se otkrije da li je broj najviših vrednosti koje prelaze 95% značajno različit od preostalih 5%.

Poziv testa vrši se preko metode **DiscreteFourierTransform(n)** gde je n – dužina bitnog uzorka. Koriste se i dodatni parametri:

M – broj redova u matrici
 Q – broj kolona u matrici

Primer:

- Ulazni parametri

ε = prvih 1000000 binarnih vrednosti proširenje ε

$$n = 100000$$

$$M = Q = 32$$

- Obrada

$$N = 97$$

$$F_M = 23, F_{M-1} = 60, N - F_M - F_{M-1} = 14$$

$$\chi^2 = 1.2619656$$

- Izlazni parametar

$$P = 0.532069$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje nepreklapajućih uzoraka

Karakteristika koja se posmatra u ovom testu je učestalost pojave svih mogućih n -bitnih uzoraka uz ne preklapanje u celom ispitivanom nizu. Test bi trebalo da otkrije da li je broj pojava nepreklapajućih uzoraka približno jednak broju koji se očekuje za niz slučajnih brojeva.

Poziv testa vrši se preko metode **NonOverlappingTemplateMatching(m,n)** gde su

m – dužina bita u šablonu

n – dužina bitnog uzorka

Primer:

- Ulazni parametri

$\varepsilon = 2^{20}$ bitova dobijenih preko G-SHA-1 generatora

$$n = 2^{20}$$

$$B = 000000001$$

- Obrada

$$\mu = 255.984375$$

$$\sigma^2 = 247.499999$$

$$W1 = 259; W2 = 229; W3 = 271; W4 = 245; W5 = 272; W6 = 262;$$

$$W7 = 259; i W8 = 246$$

$$\chi^2(\text{obs}) = 5.999377$$

- Izlazni parametar

$$P = 0.110434$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje preklapajućih uzoraka

Karakteristika koja se posmatra u ovom testu je učestalost pojave svih mogućih n -bitnih uzoraka uz preklapanje u celom ispitivanom nizu. Test bi trebalo da otkrije da li je broj pojava preklapajućih uzoraka približno jednak broju koji se očekuje za niz slučajnih brojeva.

Poziv testa vrši se preko metode **OverlappingTemplateMatching(m,n)** gde su:

m – dužina bita u šablonu

n – dužina bitnog uzorka

Primer:

- Ulazni parametri

ε = binarno proširenje ε do 1000000 bita

$n = 1000000$

$B = 111111111$

- Obrada

$v_0 = 329$; $v_1 = 164$; $v_2 = 150$; $v_3 = 111$; $v_4 = 78$; and $v_5 = 136$

χ^2 (obs) = 8.965859

- Izlazni parametar

$$P = 0.110434$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Maurerov univerzalni statistički test

Ispituje mogućnosti kompresije niza bez gubitka informacije. Za niz koji se može značajno kompresovati smatra se da nije niz slučajnih bitova zbog činjenice da je kompresija niza efikasnija ukoliko niz pokazuje periodična svojstva.

Poziv testa vrši se preko metode **Universal(L, Q, n)** gde su

L – dužina svakog bloka

Q – broj blokova u inicijanoj sekvenci

n – dužina bitnog uzorka

Takođe postoji i dodatni parametar ε .

Primer:

- Ulazni parametri

ε = binarno proširenje ε do 1000000 bita

$n = 1000000$

$B = 111111111$

- Obrada

$v_0 = 329$; $v_1 = 164$; $v_2 = 150$; $v_3 = 111$; $v_4 = 78$; and $v_5 = 136$

χ^2 (obs) = 8.965859

- Izlazni parametar

$P = 0.110434$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje linearne kompleksnosti

Ovaj test se koristi za dobijanje dužine linearnog pomeračkog registra (LFSR – eng. *Linear feedback shift register*). Svrha ovog testa je utvrđivanje da li je sekvenca dovoljno kompleksa da se može smatrati slučajnom.

Poziv testa vrši se preko metode **LinearComplexity(M, n)** gde su

M – dužina svakog bloka

n – dužina bitnog uzorka

Koristi se i dodatni parametar ε kao i

K – broj stepeni slobode

Primer:

- Ulazni parametri

ε = prvih 1000000 binarnih vrednosti proširenje ε

$$n = 1000000 = 10^6$$

$$M = 1000$$

- Obrada

$$v_0 = 11; v_1 = 31; v_2 = 116; v_3 = 501; v_4 = 258; v_5 = 57; v_6 = 26$$

$$\chi^2(\text{obs}) = 2.700348$$

- Izlazni parametar

$$P = 0.845406$$

- Zaključak

S' obzirom da je $P \geq 0.01$, smatra se da je sekvenca slučajna.

Serijski test

Test se koristi za utvrđivanje učestalosti svih mogućih preklapanja n-bitnog niza učitavoj sekvenci.

Poziv testa vrši se preko metode **Serial(m, n)** gde su

m – dužina svakog bloka

n – dužina bitnog uzorka

Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

ε = 1000000 bita binarnog proširenje ε

$$m = 2$$

$$n = 1000000 = 10^6$$

- Obrada

$$\#0s = 499971$$

$$\#1s = 500029$$

$$\#00s = 250116$$

$$\#01s = \#10s = 249855$$

$$\#11s = 250174$$

$$\psi^2_2 = 0.343128; \psi^2_1 = 0.003364; \psi^2_0 = 0.000000$$

- Izlazni parametar

$$\nabla\psi^2_2 = 0.339764$$

$$\nabla^2\psi^2_2 = 0.336400$$

$$P_1 = 0.843764$$

$$P_2 = 0.561915$$

- Zaključak

S' obzirom da su P_1 i $P_2 \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje približne entropije

U ovom testu posmatra se takođe učestalost pojave svih mogućih preklapajući n -bitnih uzoraka u nizu. Cilj je poređenje učestalosti preklapajućih blokova sa očekivanim rezultatima.

Poziv testa vrši se preko metode **ApproximateEntropy(m, n)** gde su

m – dužina svakog bloka

n – dužina bitnog uzorka

Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 11001001000011111101101010100010001000010110100011000010001$
 $10100110001001100011001100010100010111000$

$$m = 2$$

$$n = 100$$

- Obrada

$$\text{ApEn}(m) = 0.665393$$

$$\chi^2(\text{obs}) = 5.55079$$

- Izlazni parametar

$$P = 0.235301$$

- Zaključak

S' obzirom da jesu $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje slučajnih zbirova

Svrha ovog testa je potreba da se utvrdi da li je kumulativni zbir parcijalnih sekvenci koje se javljaju u nizu koji se testira suviše veliki ili suviše mali u odnosu na očekivano ponašanje tog kumulativnog zbira slučajnih sekvenci.

Poziv testa vrši se preko metode **CumulativeSums(mode,n)** gde su

mode – mode = 0 ili mode = 1

n – dužina bitnog uzorka

Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 11001001000011111101101010100010001000010110100011$

$00001000110100110001001100011001100010100010111000$

$n = 100$

$mode = 0 \parallel mode = 1$

- Obrada

$z = 1.6 \parallel z = 1.9$

- Izlazni parametar

$P = 0.219194 \parallel P = 0.114866$

- Zaključak

S' obzirom da jesu $P \geq 0.01$, smatra se da je sekvenca slučajna.

Ispitivanje slučajne digresije

Svrha ovog testa je da se utvrdi da li je broj određenih stanja u okviru ciklusa odstupa od onoga što bi se očekivalo od slučajne sekvence. Ovaj test je

zapravo niz od osam testova (i zaključaka), jedan test i zaključak za svako od stanja: -4, -3, -2, -1 i +1, +2, +3, +4.

Poziv testa vrši se preko metode **RandomExcursions(n)** gde je n – dužina bitnog uzorka. Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 1000000$ bita binarnog proširenje ε

$n = 1000000 = 10^6$

- Obrada

$J = 1490$

Stanje = x	x^2	P	Zaključak
-4	3.8356 98	0.5733 06	slučajan
-3	7.3187 07	0.1979 96	slučajan
-2	7.8619 27	0.1640 11	slučajan
-1	15.692 617	0.0077 79	nije slučajan
+1	2.4859 06	0.7786 16	slučajan
+2	5.4293 81	0.3657 52	slučajan
+3	2.4041 71	0.7908 53	slučajan
+4	2.3939 28	0.7923 78	slučajan

Tabela 12 – Ispitivanje slučajne digresije

- Zaključak

Za x , u sedam stanja važi da je $P \geq 0.01$, što dovodi do zaključka da je sekvenca slučajna.

Ispitivanje slučajne promenljive digresije

Svrha testa je da se utvrdi da li je ukupan broj stanja u kojima se niz nalazi, između $[-9, -1]$ i $[1, 9]$ premašuje očekivane vrednosti čisto slučajne sekvence. Ovaj test zapravo predstavlja grupu od 18 testova (i zaključaka), svaki test i zaključak za svako stanje: $-9, -8, \dots, -1$ i $+1, +2, \dots, +9$

Poziv testa vrši se preko metode **RandomExcursionsVariant(n)** gde je n – dužina bitnog uzorka. Koristi se i dodati parametar ε .

Primer:

- Ulazni parametri

$\varepsilon = 1000000$ bita binarnog proširenje ε
 $n = 1000000 = 10^6$

- Obrada

$J = 1490$

Stanje = x	x^2	P	Zaključak
-4	3.835698	0.573306	slučajan
-3	7.318707	0.197996	slučajan
-2	7.861927	0.164011	slučajan
-1	15.692617	0.007779	nije slučajan
+1	2.485906	0.778616	slučajan
+2	5.429381	0.365752	slučajan
+3	2.404171	0.790853	slučajan
+4	2.393928	0.792378	slučajan

Tabela 13 – Ispitivanje slučajne promenljive digresije.

- Zaključak

S' obzirom da jesu $P \geq 0.01$ za svako od 18 stanja za x , smatra se da je sekvenca slučajna.

3.3.3 Interliving

Interliving predstavlja metod razmeštanja ulaznih podataka da bi izgledale kao slučajno raspodeljene na izlazu. Postoje dva tipa interlivinga koji se danas koriste:

- Blok interliving.
- Konvolucionni interliving.

3.3.3.1 Blok interliving

Blok interliver prihvata skup (set) simbola, odnosno kodnih reči, i preuređuje ih bez ponavljanja ili izostavljanja bilo kog simbola u samom setu. Broj simbola u svakom setu je ustaljen za dati interliver. Operacija interlivera na setu simbola je nezavisna od operacija na svim setovima simbola. Interliver permutuje simbole prema mapiranju. Odgovarajući deinterliver koristi inverzni (obrnuti) mapping, da bi vratio originalne sekvence simbola, odnosno dovodi ih u stanje pre interlivinga. Interliver i deinterliver mogu biti od pomoći u smanjivanju grešaka koje su prouzrokovane greškama raspršivanja u komunikacionom sistemu. Svaka interliver funkcija ima odgovarajuću deinterliver funkciju. U tipičnoj upotrebi interliver/deinterliver para, ulazi deinterlivera se slažu sa interliverom, osim u podacima koji su preuređeni.

Blok interliver možemo podeliti na osnovu tipa podataka koji se dovode na njegov ulaz:

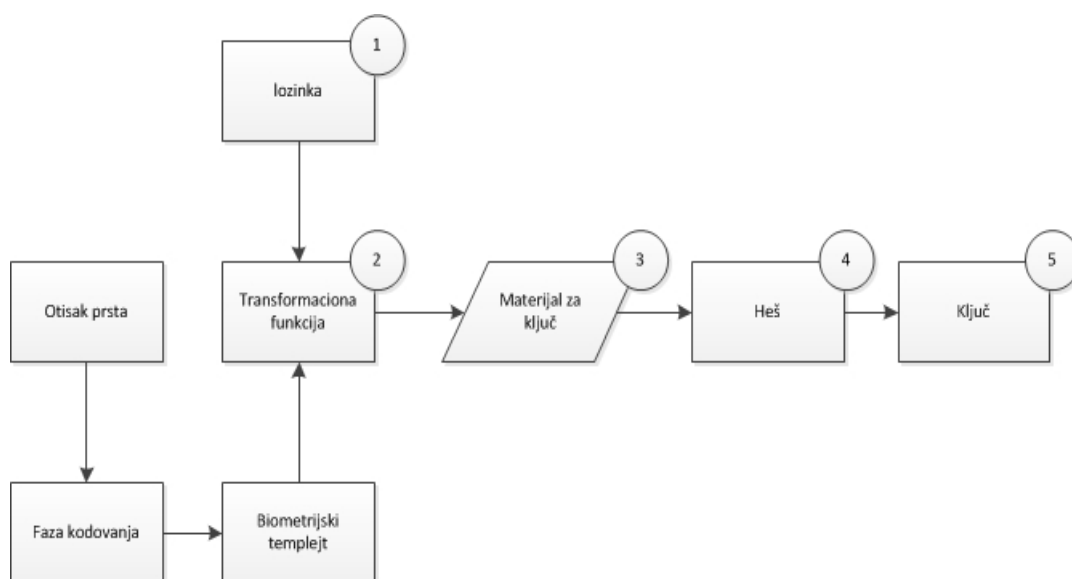
- Matrični interliver.
- Nasumični interliver.
- Algebarski interliver.

U ovom radu je iskorišćena mogućnost nasumičnog interlivera. Ovaj metod bira permutacionu tabelu na osnovu inicijalizacionog parametra što u našem slučaju predstavlja lozinka. [10]

4 Pregled predloženog rešenja

4.1 Generička šema predloženog rešenja

Dvofaktorska autentifikacija kao metod poboljšanja klasične autentifikacije predstavlja predmet istraživanja ovog rada. Kombinovanjem biometrije otiska prsta i lozinke dolazimo do ključa koji se može koristiti u servisima autentifikacije. Na generičkoj šemi može se videti raspored procesa koje je potrebno sprovesti da bi smo došli do ključa.



Slika 37 - Generička šema sistema

1. Lozinka – Generisanje ključa iz biometrije unapređuje klasične sisteme autentifikacije iz razloga što uvodi neodređenost u fazi kreiranja ključa. Da bi smo uspeli da formiramo ključ koji ima dobra svojstva što se tiče neodređenosti odnosno entropije uvodimo lozinku kao dodatni parametar. Kod predloženog rešenja lozinka predstavlja jednu vrstu inicijalizacionog vektora. Dakle, sada imamo sistem koji se oslanja na dva faktora a to je biometrija i lozinka.

2. Transformaciona funkcija - Transformacija se postiže korišćenjem funkcije *randintrlv* u programskom okruženju Matlab, kojom se elementi binarnog podatka dobijenog iz biometrije otiska prsta premeštaju nasumičnom permutacijom. Inicijalizaioni parametar za generator nasumičnih brojeva je u ovom slučaju naša lozinka koja određuje način permutacije elemenata. Funkcija je predvidiva i invertibilna za dato stanje iz razloga što se svaki put kada se pokreće Matlab eksperimentalno okruženje generator brojeva se takođe vraća na isto početno stanje ali svaka izmena inicijalizacionog parametra odnosno lozinke daje novu preraspodelu elemenata i uvodi neodređenost u načinu generisanja slučajnih brojeva odnosno u permutaciji elemenata biometrijskog templejta. Ovim smo postigli željeni efekat da i ako biometrija bude kompromitovana ne postoji način da se formira ključ bez poznavanja lozinke. Takođe, prilikom uzimanja otiska prsta nikada se ne može dobiti

isti biometrijski templejt tako da je ulaz u transformacionu funkciju uvek drugačiji tako da je ključ jako teško podvrgnuti uspešnoj kriptanalizi.

3. Materijal za ključ – Nakon primene transformacione funkcije na biometrijski templejt dobijen iz slike otiska prsta dobijamo binarni niz koji predstavlja permutaciju elemenata binarnog niza biometrijskog templejta a to je predposlednji korak za dobijanje ključa.

4. Heš – Materijal za ključ koji smo dobili ne koristimo u otvorenoj formi već se koristi heš otisak.

4.2 Postavka i objašnjenje eksperimentalnog okruženja

- Specifikacija hardverske platforme

Korišćena je sledeća hardverska platforma prilikom generisanja praktičnog rešenja:

- Procesor: Intel i5 – 2410M, 2.3GHz
- Memorija: 3GB Ram
- HDD 500GB

- Korišćena baza podataka

Za generisanje biometrijskog templejta, kao ulazni parametar sistema su korišćeni otisci prstiju iz *CASIA-FingerprintV5 (200-299)* baze podataka koja je napravljena od strane Kineske Naučne Akademije koja predstavlja opšteprihvaćenu bazu biometrijskih uzoraka.

- Razvojno okruženje

Kao razvojno okruženje korišćen je softverski alat Matlab R2011b.

4.3 Sprovedene analize i eksperimenti koji su prethodili projektovanju celokupnog rešenja

Proces dobijanja biometrijskog uzorka koji predstavlja otisak prsta je u potpunosti nasleđen. [8] U pitanju je tradicionalni sistem biometrijske autentifikacije korišćenjem biometrije otiska prsta. Preuzeti sistem koristi novi pristup prilikom procesa izdvajanja minucija zasnovan na kombinaciji najboljih predloženih rešenja za generisanje minucija iz otiska prsta. Ideja za kombinovanjem više metoda je dobijena posle intenzivne analize predloženih rešenja. Takođe, rad daje doprinos datoj oblasti koristeći morfološke operacije u procesu segmentacije, obeležavanje minucija sa posebnom pažnjom koja je posvećena trostrukom brojanju grananja linije grbena, ujedinjenje minucija posmatranjem grananja kao tri završetka kao i upisivanje pozicija minucija posle dvo-stepene transformacije.

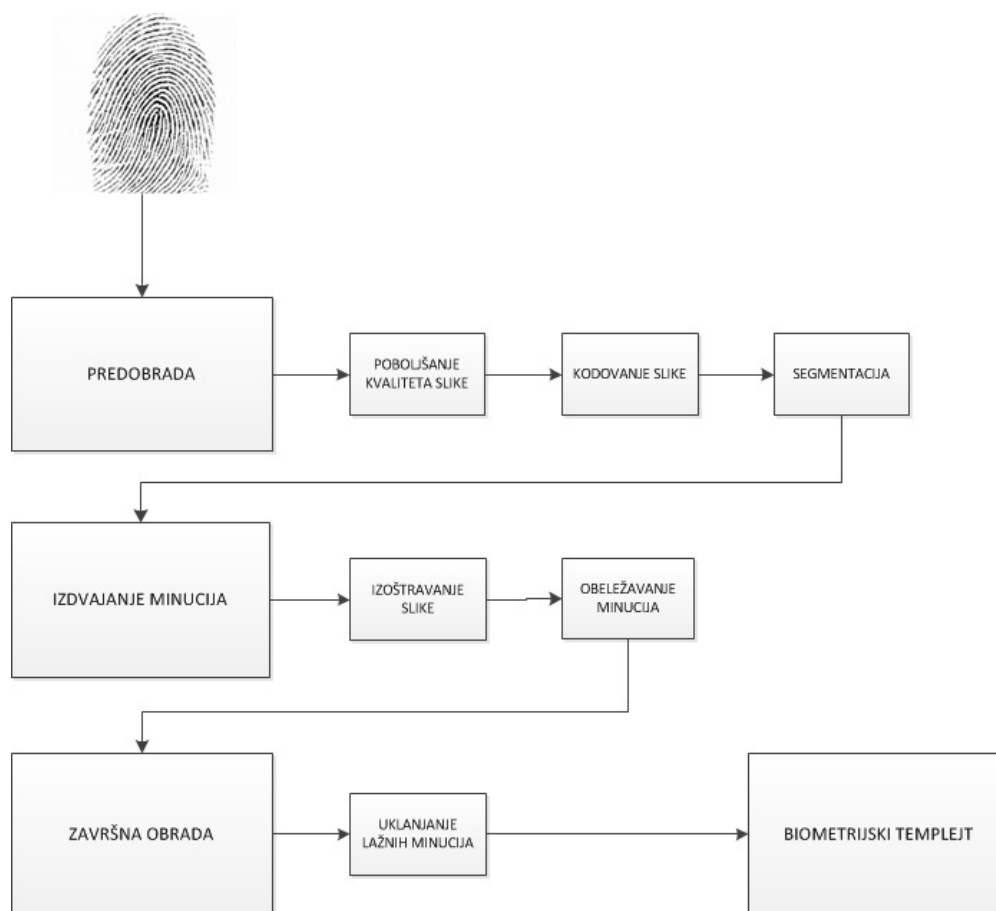
Pre nego što smo započeli razvijanje sistema koji kombinuje biometriju i lozinku morali smo da izvršimo eksperimente kojima smo potvrdili da preuzeti

tradicionalni sistem za autentifikaciju ima zadovoljavajuće performanse. To je bio ključni faktor koji je bio uslov za dalji razvoj sistema.

Testiranje tradicionalnog sistema smo izvršili upoređivanjem otisaka prstiju. Rezultati koje smo dobili su nam pokazali da ako se testira isti uzorak dobijamo poklapanje od 100% dakle sistem radi na istom principu prilikom svakog testiranja. Nakon toga testirali smo uzorke istog prsta koji su uzeti pod različitim uglom gde smo dobili poklapanje od 66% dok se poklapanje uzoraka prstiju različitih osoba svodi na sličnost od 30%. Takođe smo utvrdili da je kod sistema jako bitan kvalitet slike otiska prsta koji se testira i da od kvaliteta slike direktno zavisi i kvalitet našeg predloženog rešenja.

4.4 Pregled upotrebe predloženog rešenja

Pregled predloženog rešenja ćemo započeti generičkom šemom nasleđenog tradicionalnog sistema uz pomoć kojeg dolazimo do biometrijskog materijala koji će biti iskorišćen za generisanje kriptološkog ključa. U ovom segmentu je prikazano na koji način procesi obrade slike otiska prsta utiču na njenu promenu kao i vizuelna prezentacija tih promena.

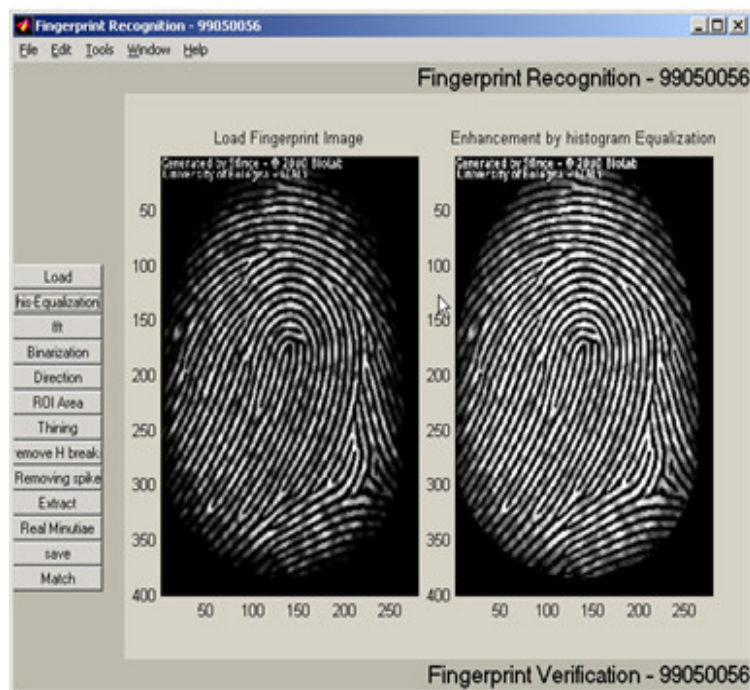


Slika 38 - Generička šema izdvajanja biometrijskog templejta.

Kod predloženog rešenja korišćen je grafički interfejs programa Matlab. Kao što se vidi sa slike na levoj strani se nalazi niz dugmića koji nam služe za pozivanje

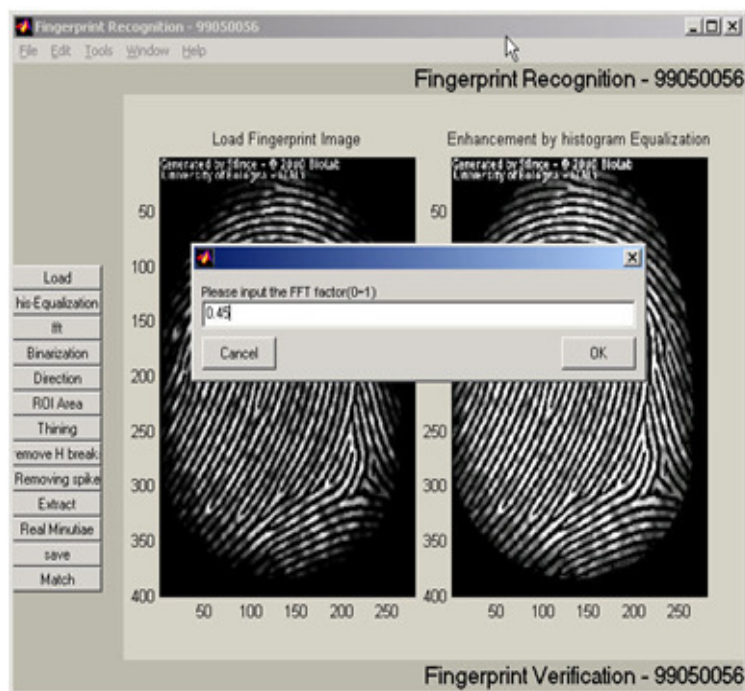
određene funkcije za obradu slike otiska prsta. U sredini se nalaze dve oblasti. Jedna predstavlja sliku otiska prsta pre a druga posle obrade preciziranom funkcijom. Sistem prihvata *grayscale* fotografije otiska prsta različitih veličina i formata. Radi dobijanja boljih rezultata kvalitet slike bi trebao da bude što viši odnosno bitno je da se što jasnije uočavaju linije grebena u odnosu na doline i pozadinu.

Na slici je jasno prikazana razlika pre i nakon procesa poboljšanja histograma. Na levom prozoru je prikazana originalna slika otiska prsta dok je na desnom nakon procesa poboljšanja.



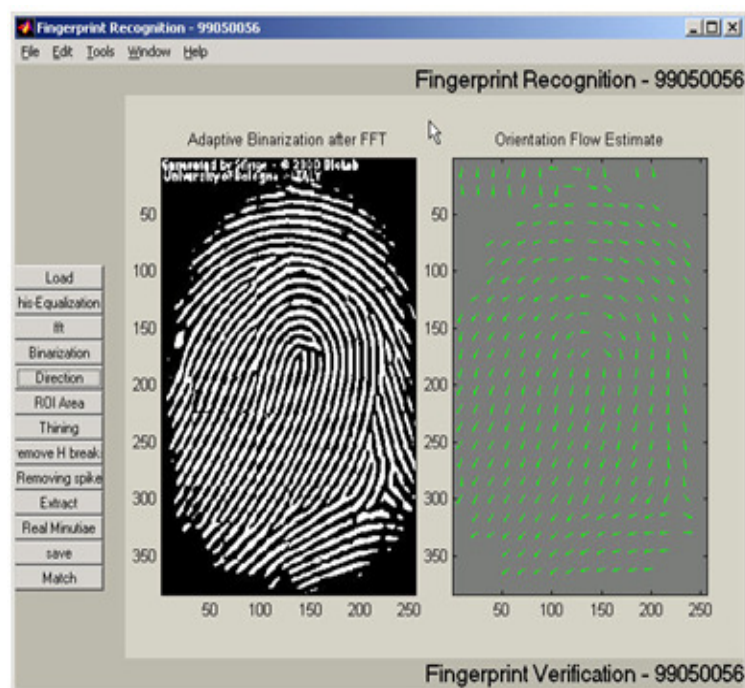
Slika 39 - Pojačavanje histograma

Slika prikazuje prozor koji dobijamo nakon što kliknemo na dugme FFT što predstavlja proces brze Furijer-ove transformacije. Tada je potrebno u predviđeno polje uneti parametar $k = 0.45$ za koji se nakon eksperimentalnog istraživanja smatra da je optimalan za ovaj tip transformacije.



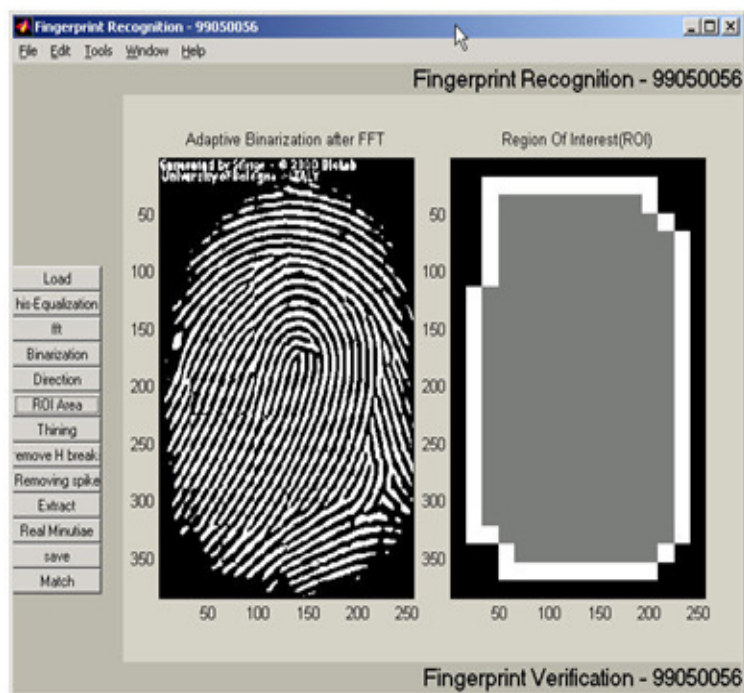
Slika 40 - Brza Furijer-ova transformacija

Slika br. 40 predstavlja primenu dve funkcije. U levom prozoru vidimo sliku nakon procesa binarizacije dok se u desnom nalaze kratke zelene linije koje predstavljaju usmerenost blokova slike otiska prsta.



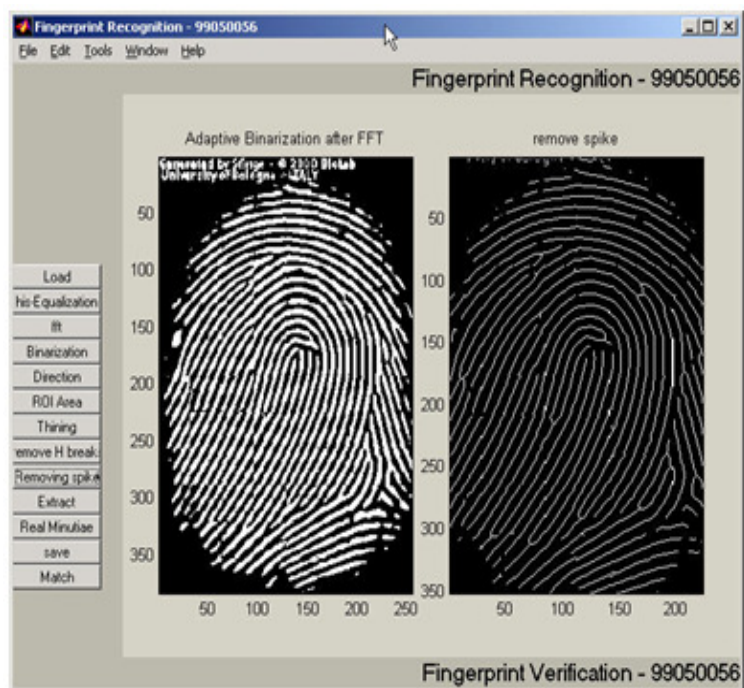
Slika 41 - Binarizacija (levo) i usmerenost blokova (desno)

Slika br.41 nam pokazuje region interesa (RIO) odnosno koji region slike ćemo dalje tretirati sledećim operacijama.



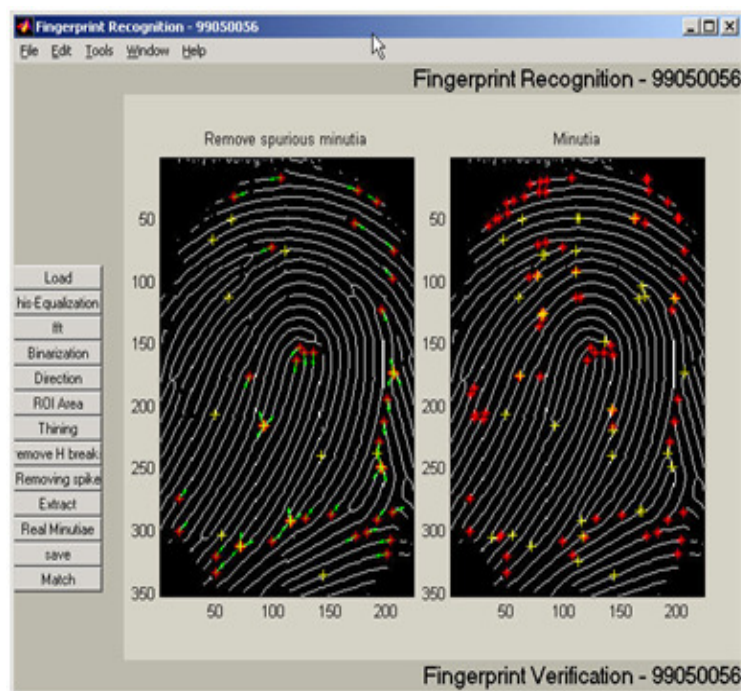
Slika 42 - Region interesa (RIO)

Na desnom prozoru sledeće slike možemo videti obrađenu sliku otiska prsta nakon procesa stanjivanja linija grebena i uklanjanja izlovanih tačaka.



Slika 43 - Izoštrena slika sa uklonjenim lažnim minucijama (desno)

Na slici se u desnom prozoru nalaze obeležene minucije od kojih će biti uklonjene one koje su lažne. Račvanja su obeležena žutom a završeci crvenom bojom. Na levom prozoru zelenom bojom su obeležene prave minucije.



Slika 44 - Obeležene minucije (desno) i realne minucije (levo)

Nakon dobijanja realnih minucija iz otiska prsta njihove koordinate na x i y osi se čuvaju u tekstualnom fajlu. Taj tekstualni fajl zatim pretvaramo u binarni.

```

3.5000000e+001 2.0500000e+002 -2.8940300e+000
1.2300000e+002 1.7000000e+001 2.2054481e+000
4.1400000e+002 3.1000000e+001 -2.5435148e+000
4.7700000e+002 1.2500000e+002 -3.0104810e+000
4.4100000e+002 6.1000000e+001 -2.6735591e+000
1.3600000e+002 1.7000000e+001 -1.0191413e+000
3.5600000e+002 1.7000000e+001 1.5049576e+000
4.8900000e+002 2.2000000e+001 2.4756264e-001
4.7800000e+002 2.3000000e+001 1.2029548e-001
4.3700000e+002 1.3800000e+002 -2.8330864e+000
4.4800000e+002 2.1100000e+002 3.0321417e+000
1.1600000e+002 7.0000000e+001 2.3102498e+000
8.1000000e+001 1.0400000e+002 2.7001636e+000
5.6000000e+001 1.3800000e+002 2.9889433e+000
1.8800000e+002 1.0700000e+002 1.8183590e+000
4.0800000e+002 9.2000000e+001 5.6743995e-001
4.2100000e+002 1.1100000e+002 -2.4319115e+000

```

Slika 45 – Deo dobijenog tekstualnog fajla na osnovu pozicija minucija.

U ovom trenutku se uvodi i drugi autentifikacioni parametar a to je lozinka. Generisanje ključa se postiže korišćenjem funkcije *interlivinga* kojom se elementi binarnog podatka dobijenog iz minucija premeštaju nasumičnom permutacijom. Inicijalizacioni parametar za generator nasumičnih brojeva je u ovom slučaju naša lozinka koja određuje način permutacije elemenata. Funkcija je predvidiva i invertibilna za dato stanje ali svaka izmena inicijalizacionog parametra odnosno lozinke daje novu preraspodelu elemenata. Ovim smo postigli željeni efekat da i ako biometrija bude kompromitovana ne postoji način da se formira ključ bez poznavanja lozinke.

```

110100100111110110011100100010010000110110011
111100101111011011100000101101101010011101101
111101101101010111010001110011101111010011111
0111010110111110111101110000111001111100011111
100010101101110011000000011001001011001001010
101111100111100110111100110101000001111101001
10100010110100101000110111110100101011101110
11011001011010100100010011011101100001111100

```

Slika 46 – Binarni fajl nakon primene transformacione funkcije.

Nakon dobijanja binarnog fajla nad kojim smo transformacionu funkciju računa se njegova heš vrednost i takav podatak se zapisuje i čuva kao ključ.

4.5 Peroformanse predloženog okruženja sa prikazom eksperimentalnih rezultata

Jaka informaciona analiza dobijenog binarnog niza je od velike važnosti iz razloga što postavlja teorijske okvire za generisanje kvalitetnog kriptološkog ključa. Performanse predloženog rešenja ćemo iskazati korićenjem aplikacije preko koje ćemo testirati dobijeni materijal. Korišćenjem Šenonove entropije dolazimo do prosečne količine informacija koje su sadržane u našem uzorku iz koga dobijamo ključ. Uzorak je potrebno analizirati i sa aspekta njegove uniformne distribucije.

Dobijeni uzorak ćemo podvrgnuti testovima za procenu informacionog sadržaja on kojih su za nas najvažniji :

- Frekvencijski test.
- Serijski test.
- Entropijski test.

Frekvencijski test predstavlja test učestalosti bitova u binarnom nizu. Dobar binarni niz ima približan broj nula i jedinica.

Frekvencijski test	Broj bitova
Vrednost bita (0)	3202
Vrednost bita (1)	4106

Tabela 14 - Rezultati frekvencijskog testa.

Serijskim testom ispitujemo koliki broj parova se nalazi u nizu. Približan broj sve četiri grupe parova u našem uzorku prikazuje da je dobijeni rezultat dobar.

Serijski test	Broj parova
Par (00)	1368
Par (01)	1833
Par (10)	1834
Par (11)	2272

Tabela 15 - Rezultati serijskog testa.

Entropija predstavlja meru neodređenosti nekog niza odnosno prosečnu količinu informacije sadržane u nizu. Kako se ovde radi o binarnom nizu jedinica

informacije je 1 bit. Dakle maksimalna entropija po jednom bitu bi iznosila 1 tako da reuzlat prikazan u tabeli nam prikazuje da je dobijena vrednost približna maksimalnoj entropiji.

Entropijski test	Vrednost
Monobit	0.9889
Bigram	0.9887
Trigram	0.9884
Matrice 4x4	0.9885

Tabela 16 – Rezultati entropijskog testa.

Uzorak koji smo testirali predstavlja binarni niz koji sadrži 7308 bita. Količina informacije koju smo dobili entropijskim testom po jednom bitu iznosu prosečno 0.988 tako da možemo dobiti količinu informacija koju sadrži niz ako pomnožimo broj bitova sa količinom informacije koju nose.

$$\text{Količina informacije niza} = 7308 \times 0.988 = 7220,3.$$

Testirali smo više dobijenih uzoraka i dobijeni rezultati entropijskog test su skoro identični prethodno navedenom (Entropija = 0.998). Dakle svi su približno maksimalnoj vrednosti entropije. Ukupna količina informacije koju je moguće iskoristiti za generisanje kriptološkog ključa je po jednom otisku u proseku 4335 bitova. Ovo je rezultat koji je dobijen nakon računanja zajedničke informacije. Tačnije, ovaj broj bitova predstavlja teorijski okvir.

Kako smo dobili teorijski okvir dužine dobijenog materijala veći od 1024 bita treba napomenuti da se nad ovim materijalom može dobiti heš vrednost velikih dužina što daje dodatnu vrednost predloženog sistema. Može se koristiti heš algoritam SHA-512 koji na izlazu daje heš vrednost dužine 512 bitova. Algoritam koristi 80 rundi za kompresovanje sa gubicima da bi došao do heš vrednosti. Za predloženi heš algoritam trenutno nije poznato d postoje kolizije.

4.6 Oblast primene predloženog rešenja

Autentifikacija na bazi biometrije obezbeđuje pogodnu i sigurnu proveru identiteta korisnika kako u lokalnom okruženju tako i preko Interneta. U koliko se zahteva visok nivo bezbednosti biometriju kombinujemo sa drugim parametrima (lozinka, token...). Predloženi sistem u ovom radu se može koristiti u takvim sistemima.

U informacionoj eri u kojoj se trenutno nalazimo sve je veća popularnost sistema koji koriste biometrijsku tehnologiju zbog praktičnosti, preciznosti i brzine napretka. Veći stepen pouzdanosti pri određivanju identiteta korisnika u odnosu na tradicionalne sisteme predstavlja iskorak što se tiče sistema autentifikacije. Korišćenje dvo-faktorske autentifikacije samo ubrzava kvalitetan razvoj bezbednosti sistema. Ovakvi sistemi se koriste u svrhu verodostojnosti a to uključuje sigurnosne sisteme za kontrolu pristupa kod finansijskih servisa (ATM i banke), vladine

institucije, granična i lokacijska kontrola pristupa, Internet bezbednost koja dalje uključuje sve segmente kriptografske bezbednosti.

Informaciono-teorijska analiza dobijenih rezultata nam dokazuje se predloženo rešenje može koristiti u svrhu generisanja kriptoloških ključeva koji se dalje koriste u svim sferama bezbednosti informacija.

5 Zaključak

5.1 Sumarni ciljevi rada i ostvareni rezultati

Razvoj servisa autentifikacije kao prevashodni cilj ovog rada je ostvaren na osnovu sistema koji nam omogućava generisanje kriptoloških ključeva korišćenjem dvo-faktorske šeme. Kombinacijom nečega što imamo (biometrija otiska prsta) i nečega što znamo (lozinka) poboljšavamo sigurnost autentifikacionih procesa koji su široko rasprostranjeni u komunikaciji putem globalne mreže.

Prilagođena funkcija interliver koja ima široku primenu u komunikacijama nam je omogućila transformacionu funkciju koja koristi lozinku kao inicijalni parametar za permutaciju podataka dobijenih iz biometrije otiska prsta. Tako dobijeni materijal nam je omogućio generisanje ključeva velikih dužina sa teorijskim okvirima.

Razvijeni sistem nam omogućava generisanje više ključeva na osnovu originalnog biometrijskog templejta. Takođe, sistem ne čuva originalnu biometriju u bazi podataka već čuva heš vrednost tako da ne može doći do kompromitovanja biometrijskog uzorka. Dakle, ne postoji referentni podatak na osnovu koga napadač može da otkrije originalnu biometriju ili ključ.

Nad dobijenim ključevima je izvršena informaciona analiza koja nam je omogućila postavljanje teorijskih okvira. Sprovedene teorijske analize količine informacija kao i njenu neuređenu raspoređenost duž kompletnog materijala predstavlja novinu analizi dobijenih rezultata.

5.2 Predlog za budući rad

Poboljšanje performansi predloženog rešenja je moguće postići korišćenjem multimodalne biometrije. Spajanje više biometrijskih uzoraka u cilju razvijanja sistema autentifikacije predstavlja polaznu tačku za budući rad. Teorijsko-informaciona analiza biometrijskih uzoraka će nam omogućiti uvođenje novina u sisteme generisanja kriptoloških ključeva korišćenjem multimodalne biometrije. Takvom analizom smo u mogućnosti da procenimo kolika je informaciona vrednost određenih delova biometrijskih uzoraka kao i procena njihove zajedničke informacije koja je idealna za generisanje ključeva.

Literatura

- [1] *Biohashing: two factor authentication featuring fingerprint data and tokenised random number*, Andrew Teoh Beng Jin, David Ngo Chek Ling, Alwyn Goh 2003.
- [2] *A proposal for a biometric key dependent cryptosystem*, K. Hassanain, M. Shaarawy, E. Hesham, 2010.
- [3] *Biometrijski sistemi – upotreba i zloupotreba*, Brankica Popović, Miodrag Popović
- [4] *Multimodalni biometrijski sistemi*, Srđan Mesarović, 2007.
- [5] www.biometrika.sk
- [6] *Savremeni trendovi u multimodalnoj biometriji*, Radovano Skendžić.
- [7] *Otisak prsta – biometrijski podaci*, Miloš Tripunović, 2007.
- [8] *Fingerprint recognition*, WuZhili, 2002.
- [9] [http://sr.wikipedia.org/sr/Entropija_\(teorija_informacija\)](http://sr.wikipedia.org/sr/Entropija_(teorija_informacija))
- [10] <http://www.mathworks.com/help/comm/ug/interleaving.html>
- [11] *Kriptologija 1- „Osnove za analizu i sintezu šifarskih sistema“ [Knjiga]- Beograd: Univerzitet Singidunum, Mladen Veinović, Saša Adamović, 2013- 1 : T. 1 : str. 247. - 978-86-7912-469-2.*