Jedna klasa biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama

By Srđan Barzut

WORD COUNT	37998	TIME SUBMITTED	18-NOV-2021 12:40PM
		PAPER ID	82067373

UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

Jedna klasa biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama

- Doktorska disertacija -

Mentor:

Prof. dr Milan Milosavljević

Kandidat:

Srđan Barzut

Beograd, 2021.

Mentor:
Prof. dr Milan Milosavljević
Univerzitet Singidunum

Članovi komisije:
Prof. dr Milan Milosavljević
Univerzitet Singidunum

Prof. dr Saša Adamović
Univerzitet Singidunum

Dr Branko Kovačević, profesor emeritus
Univerzitet u Beogradu – Elektrotehnički fakultet

Datum odbrane:

_____

Zahvaljujem se mentoru,

prof. dr Milanu M. Milosavljeviću,

na nesebičnoj pomoći, korisnim savetima i

velikoj podršci tokom izrade ove disertacije.

Sažetak: U ovoj doktorskoj disertaciji predložen je novi biometrijski kriptosistem otisaka prstiju baziran na sistemu fazi povezivanja i dubokih konvolucionih neuronskih mreža. Centralni doprinos rada predstavlja novi pristup automatskom izdvajanju obeležja fiksne dužine iz otisaka prstiju, u potpunosti zasnovanom na konvolucionim neuronskim mrežama. Predloženom kvantizacijom obeležja kodovanjem sa dva bita, biometrijski šabloni su prevedeni u binarni domen, što je omogućilo primenu XOR biometrije i razvoj biometrijskog kriptosistema koji se može koristiti za upravljanje ključevima (engl. *key-release*) ili za zaštitu šablona. Problem varijabilnosti biometrijskih podataka marginalizovan je primenom BCH koda za korekciju grešaka, koji radi na nivou bloka što ga čini otpornim na poznate statističke napade. Predloženi biometrijski kriptosistem sistem može upravljati dužinom ključeva od 265 bita, što zadovoljava potrebe savremenih kriptografskih sistema, uz prihvatljivu marginu EER greške od 1%. Evaluacija eksperimentalnih rezultata potvrđuje značajan napredak u odnosu na druge biometrijske kriptosisteme i sisteme za poređenje otisaka na osnovu njihove teksture.

Ključne reči: biometrija, prepoznavanje otisaka prstiju, zaštita biometrijskih šablona, biometrijski kriptosistemi, šema fazi povezivanja, konvolucione neuronske mreže

Abstract: In this doctoral dissertation a novel fingerprint biometric cryptosystem based on the fuzzy commitment scheme and deep convolutional neural networks is proposed. The main contribution in this paper is novel approach to automatic discretization of fingerprint texture descriptors, entirely based on convolutional neural network, and designed to generate fixed-length templates. With the proposed quantization of the extracted features by two-bit coding, biometric templates are converted to a binary domain, which allows the application of XOR biometrics and the development of a biometric cryptosystem that can be used for key-release or as a template protection mechanism in fingerprint matching systems. The problem of biometric data variability is marginalized by applying the secure block-level Bose–Chaudhuri–Hocquenghem error correction code resistant to statistical-based attacks. The proposed biometric cryptosystem can manage a key length of 265 bits, which meets the requirements of modern cryptographic systems, with an acceptable EER of 1%. The evaluation shows significant performance gains when compared to other texture-based fingerprint matching and biometric cryptosystems.

Keywords: Biometrics, Fingerprint Recognition, Biometric Template Security, Biometric Cryptosystems, Fuzzy Commitment Scheme, Convolutional Neural Networks

SADRŽAJ

1. Uvod i metodologija naučno-istraživačkog rada 1
1.1. Uvod 1
1.2. Predmet istraživanja i očekivani naučni doprinos 2
1.3. Ciljevi i metode istraživanja 4
1.4. Hipoteze istraživanja 5
1.5. Struktura rada 6

2. Biometrija 8
2.1. Uvod 8
2.2. Biometrijski autentifikacioni sistemi 9
2.3. Biometrijske karakteristike 11
2.3.1. Otisak prsta 13
2.3.2. Dužica oka 22
2.3.3. Karakteristike lica 28
2.3.4. Pregled ostalih značajnijih biometrijskih karakteristika 32
2.4. Multibiometrija 36
2.4.1. Odabir biometrijskih podataka 37
2.4.2. Prikupljanje i obrada podataka 39
2.4.3. Sjedinjavanje biometrijskih podataka 39
2.4.4. Prednosti upotrebe multibiometrijskih sistema 45

3. Sigurnost biometrijskih sistema 47
3.1. Interni napadi na biometrijske sisteme 49
3.2. Napadi na infrastrukturu biometrijskog sistema 50
3.3. Zaštita biometrijskih šablona 54
3.3.1. Klasični šifarski algoritmi za zaštitu biometrijskog šablona 55
3.3.2. Transformacije obeležja u šablonu 56
3.3.3. Biometrijski kriptosistemi 58
3.4. Multimodalni biometrijski kriptosistemi 62

4. Jedna klasa biometrijskih kriptosistema zasnovana na konvolucionim neuronskim mrežama 64
4.1. Prethodni radovi 64
4.2. Određivanje referentne tačke i poboljšanje slike 77
4.3. Segmentacija regiona od interesa i formiranje skupa za obučavanje 80
4.4. Izdvajanje obeležja primenom konvolucione neuronske mreže i diskretizacija 81
4.5. Formiranje biometrijskog kriptosistema 88
4.6. Eksperimentalni rezultati 93

5. Zaključak 101
5.1. Sumarni pregled istraživanja 101
5.2. Pregled naučnih doprinosa 103
5.3. Predlog budućih istraživanja 104

Literatura 105

Spisak slika

Slika 1 – Opšti model biometrijskog autentifikacionog sistema 11
Slika 2 – Međusobna zavisnost FRR i FAR grešaka 13
Slika 3 – Purkinjeova klasifikacija otisaka prstiju 14
Slika 4 – Određivanje polja orijentacije 16
Slika 5 – Jezgro i delta u otiscima prstiju (leva petlja, desna petlja i spirala) 18
Slika 6 – Poenkareov indeks 19
Slika 7 – Najznačajnije vrste minucija 19
Slika 8 – Princip detekcije prekida i račvanja papilarnih linija 20
Slika 9 – Određivanje pravca papilarne linije i ugla minucije 20
Slika 10 – Blok dijagram sistema za prepoznavanje dužice oka 23
Slika 11 – Princip konverzije dužice Dougmanovim modelom 24
Slika 12 – Dobijanje koda dužice faznom demodulacijom 26
Slika 13 – Raspodela HD poređenja više od devet miliona različitih dužica oka 28
Slika 14 – Pristup izdvajanja obeležja kod različitih tehnika 31
Slika 15 – Otisak dlana i geometrija šake 32
Slika 16 – Vaskularni obrasci prsta 33
Slika 17 – Prikaz veličine podataka jednog otiska prsta nakon svakog modula 40
Slika 18 – Primer sjedinjavanja na nivou senzora dva parcijalna otiska 41
Slika 19 – Primer homogenog sjedinjavanja dva parcijalna otiska 42
Slika 20 – Hijerarhijska klasifikacija potencijalnih napada na biometrijski sistem 48
Slika 21 – Ranjivost infrastrukture biometrijskog sistema 50
Slika 22 – Različiti pristupi načinu zaštite biometrijskog šablona 55
Slika 23 – Primena klasičnih šifarskih algoritama za zaštitu biometrijskog šablona 56
Slika 24 – Pristup transformacije obeležja u šablonu 57
Slika 25 – Neinvertibilne transformacione funkcije otiska prsta 58
Slika 26 – Koncept povezivanja ključa u biometrijskim kriptosistemima 60
Slika 27 – Koncept generisanja ključa u biometrijskim kriptosistemima 61
Slika 28 – Fazi povezivanje dvoslojnom metodom kodova za korekciju grešaka 65
Slika 29 – Fazi trezor šema za otiske prstiju 66
Slika 30 – ROI podeljen na sektore 68
Slika 31 – Region od interesa konvoluiran sa Gaborovim filtrom u osam uglova 69
Slika 32 – Raspodela Hemingovog rastojanja sa primenom tehnike odstranjivanja nepouzdanih bita na šablonu dužine 512 bita 73
Slika 33 – Raspodela Hemingovog rastojanja sa primenom tehnike odstranjivanja nepouzdanih bita na šablonu dužine 1024 bita 73
Slika 34 – Koncept FCS sa otiscima prstiju 74
Slika 35 – LBP kodovanje 75
Slika 36 – Horizontalni i vertikalni Sobelov operator 77
Slika 37 – Normalizacija regiona od interesa 79
Slika 38 – Poboljšanje slike otiska prsta 80
Slika 39 – Generisanje obučavajućeg skupa jednog uzorkovanog otiska 81
Slika 40 – Obuka *AlexNet* neuronske mreže 82
Slika 41 – Arhitektura modifikovane *AlexNet* neuronske mreže 83
Slika 42 – Obuka *GoogLeNet* neuronske mreže 83
Slika 43 – Arhitektura *GoogLeNet* neuronske mreže 84

Slika 44 – Obuka *ResNet* neuronske mreže 85
Slika 45 – Uporedni prikaz klasične i rezidualne arhitekture neuronske mreže 86
Slika 46 – Blok šema predloženog biometrijskog kriptosistema 89
Slika 47 – Odnos FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 94
Slika 48 – Odnos FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita 94
Slika 49 – Odnos FAR i FRR primenom *GoogLeNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 95
Slika 50 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 96
Slika 51 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita 97
Slika 52 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 265 bita 97
Slika 53 – ROC dijagram predloženih šema 98
Slika 54 – Uporedni prikaz dva uzorka istog identiteta 99

Spisak tabela

Tabela 1 – Zastupljenost tipova otiska prstiju po Henrijevoj kategorizaciji 14
Tabela 2 – Verovatnoća greške u zavisnosti od različitih vrednosti HD 28
Tabela 3 – Uporedni pregled rezultata različitih metoda sjedinjavanja na nivou rangiranja 44
Tabela 4 – FAR i FRR vrednosti ostvarene u [79] 70
Tabela 5 – FAR i FRR vrednosti ostvarene u [80] 71
Tabela 6 – FAR i FRR vrednosti ostvarene u [81] 74
Tabela 7 – FAR i FRR vrednosti ostvarene u [82] 75
Tabela 8 – Karakteristike korišćenih konvolucionih neuronskih mreža 82
Tabela 9 – Uporedni pregled tačnosti klasifikacije 87
Tabela 10 – Prikaz odnosa dužine ključa i mogućnosti korekcije grešaka za BCH kôd dužine 2047 bita 91
Tabela 11 – Rezultati FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 93
Tabela 12 – Rezultati FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita 94
Tabela 13 – Rezultati FAR i FRR primenom *GoogLeNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 95
Tabela 14 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita 96
Tabela 15 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita 96
Tabela 16 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 265 bita 96
Tabela 17 – Komparativni pregled rezultata 99

1. Uvod i metodologija naučno-istraživačkog rada

1.1. Uvod

Kao najstariji i najpoznatiji primer primene biometrijskih (engl. *biometrics*) fizičkih karakteristika može se reći da je to svakodnevno prepoznavanje drugih ljudi na osnovu lica, koje nesvesno koristimo od rođenja. Slično se može reći i za glas, ali i za neke od karakteristika ponašanja. Proučavanje merljivosti fizičkih karakteristika čoveka dugo predstavlja predmet naučnih istraživanja. Otisci prstiju su prvi od biometrijskih karakteristika koji su privukli pažnju, da bi se daljim istraživanjima i razvojem informacionih tehnologija, otkrila jedinstvenost i primenljivost mnogih drugih fizičkih osobina, kao i karakteristika ponašanja čoveka. Prva istraživanja o otiscima prstiju uradio je italijanski profesor anatomije Marčelo Malfigi (*Marcello Malpighi*) 1686. godine, u kojima se bavio oblikom, strukturom i funkcijom brazdi na koži prstiju. Od tada, veliki broj istraživača počeo je da se bavi istraživanjem otisaka prstiju, da bi 1880. godine škotski lekar Henri Folds (*Henry Faulds*) prvi sugerisao individualnost otiska, na osnovu svojih empirijskih zapažanja. Policijski službenik Alfons Bertiljon (*Alphonse Bertillon*) razvio je 1888. godine u Parizu antropometrijski (engl. *anthropometry*) sistem od deset mera telesnih karakteristika – Bertiljonov sistem [1] i koristio ga je za identifikaciju, prvenstveno kriminalaca povratnika. Nešto kasnije je otisak prsta pridodat u skup karakteristika na predlog Fransisa Galtona (*Sir Francis Galton*), mada se njemu nije poklanjala posebna pažnja. Galton se posvetio naučnim istraživanjima o otiscima prstiju i u svojoj knjizi [2] je napravio klasifikaciju otisaka, procenio jedinstvenost i perzistentnost, uveo primenu karakteristike minucija (lat. *minutiae*) za poređenje otisaka i pokušao da dokaže dokaznu vrednost otisaka prstiju. Bertiljonov sistem, proširen otiscima prstiju, prvi je u upotrebu uveo Ivan Vučetić (*Juan Vucetich*), argentinski antropolog i policijski inspektor 1891. godine, da bi već 1892. godine na osnovu otisaka prstiju bila izvršena prva identifikacija u jednom slučaju ubistva. U literaturi se ovo navodi kao prvi slučaj gde su otisci prstiju korišćeni tokom istrage, a kasnije kao osnovni dokaz na sudu. To se ujedno smatra i početkom daktiloskopije (gr. *dactilo* - prst i lat. *scopein* - gledati), kao discipline kriminalističke tehnike.

Značaj biometrijskih karakteristika je u prošlosti stidljivo prihvatana, pre svega zbog veoma teškog i komplikovanog procesa obrade, samim tim dokazivanja osobine jedinstvenosti i opšteg prihvatanja njene vrednosti. U visokoprofilnim slučajevima, kada konvencionalne metode dokazivanja nisu dale rezultate, biometrijske karakteristike su postale glavni dokaz na sudu, pa je biometrija tako postala prihvaćena od strane društva. Biometrija nije apsolutno tačna i precizna, pa se može reći da još uvek nije ispunila sva očekivanja. Zbog toga je ova oblast predmet interesovanja naučne javnosti i na njenom

razvoju i usavršavanju se svakodnevno radi. Osnovni problem koji se javlja prilikom biometrijske autentifikacije je varijabilnost biometrijskih karakteristika usled: šuma senzora, varijacije osvetljenja i pozicioniranja, promene karakteristika usled starosti i sl., a dodatni problem kod nekih karakteristika predstavljaju genetske sličnosti. Poboljšanje performansi biometrijskog sistema postiže se kombinovanjem više biometrijskih izvora, čime se formira multibiometrijski sistem autentifikacije. Izvori podataka mogu biti iste biometrijske osobine (otisci različitih prstiju, skeniranje dužice oba oka itd.), a mogu se koristiti različite biometrijske osobine (modaliteti) u multimodalnim biometrijskim sistemima. U multibiometrijskim sistemima, korišćenjem više nezavisnih biometrijskih izvora, različitih biometrijskih karakteristika ili tehnika obrade podataka, međusobno se kompenzuju njihovi nedostaci, čime je moguće povećati: preciznost i bezbednost sistema, primenljivost u pogledu njegove univerzalnosti i stepen društvene prihvatljivosti. Slično Bertiljonovom sistemu, gde se za svaku osobu prikupljalo više antropometrijskih karakteristika, danas se prave automatizovane baze podataka koje objedinjavaju više biometrijskih karakteristika. Multimodalne baze biometrijskih podataka postale su neizostavan deo procesa verifikacije identiteta pri kontroli granica i drugih nacionalnih projekata od velikog značaja, koji uključuju celokupnu populaciju jedne države. Danas, načelo prihvatljivosti kod korisnika, pored poverenja u tačnost sistema, u velikoj meri uključuje uverenost u svojstva privatnosti biometrijskog sistema, kako bi prihvatili korišćenje svojih biometrijskih osobina u svrhe autentifikacije. Na taj način, privatnost otvara pitanje sigurnosti biometrijskih podataka koji su uskladišteni u sistemu.

Ni jedan sistem nije apsolutno bezbedan i otporan na obmane ili upade. Pod određenim okolnostima, sa dovoljno resursa i raspoloživog vremena, svaki sigurnosni sistem se može savladati. Analiziranjem ranjivosti biometrijskih sistema formira se model pretnji, s ciljem da se identifikuju mogući napadi i otkriju potencijalne slabosti, radi preduzimanja preventivnih radnji i odgovarajućih protivmera. Uspešnim napadom na biometrijski sistem, osim proboja sigurnosti, može doći do krađe biometrijskih podataka. Time se krši osnovni princip poverljivosti, a mogu biti ugroženi drugi biometrijski sistemi koji su bazirani na istim biometrijskim karakteristikama. Zbog toga, poseban izazov u biometrijskim sistemima predstavlja zaštita biometrijskih podataka, što je jedan od polaznih izazova u predmetu istraživanja ovog rada.

1.2. Predmet istraživanja i očekivani naučni doprinos

Biometrija se već dugo primenjuje u kriminalistici u forenzičke svrhe, dok je poslednjih godina u velikoj meri implementirana u državnim projektima za povećanje nacionalne bezbednosti kroz: biometrijska dokumenta, kontrolu identiteta prilikom glasanja, kontrolu granica itd., dok se sve više primenjuje u komercijalnom sektoru za kontrolu pristupa, evidenciju radnog vremena, autentifikaciju na prenosnim uređajima,

bankomatima, u mobilnom bankarstvu i elektronskoj trgovini. Iz navedenog sledi da je izuzetno značajno istraživanje daljeg razvoja biometrijskih tehnika autentifikacije i sistema zaštite biometrijskih podataka, s obzirom na to da od sigurnosti biometrijskih sistema može zavisiti celokupna sigurnost drugih sistema, počev od pojedinačne finansijske transakcije do celokupnog bankarskog ili korporativnog sistema, pa i sigurnosti cele države. Brojna literatura je posvećena teorijsko–naučnim osnovama biometrije i njenoj potencijalnoj primeni u kriptografiji, što je dodatni dokaz aktuelnosti i značaja ove teme.

Predmet ovog naučno-istraživačkog rada su biometrijski kriptosistemi u funkciji zaštite biometrijskih karakteristika korisnika i njihovog povezivanja sa kriptološkim ključevima, radi uspostavljanja *key-release* sistema upravljanja ključevima na osnovu biometrije. Analizirana je mnogobrojna naučna građa iz ove oblasti i izdvojena su najznačajnija dosadašnja dostignuća, koja su upotrebljena kao polazna osnova za definisanje usmerenih ciljeva i uspostavljanje hipoteza, u skladu sa kojima je napravljen plan daljeg istraživanja, koje je sprovedeno i sumirano u ovom radu.

U radu su prezentovani rezultati navedenih istraživanja o poznatim tehnikama i različitim pristupima automatizovane autentifikacije na osnovu biometrijskih podataka, kao i potencijalnim pretnjama i napadima na njih. Kao proizvod uspešno obavljenog istraživanja, na osnovu intenzivnog eksperimentalnog testiranja postavljenih hipoteza i ideja, u disertaciji je iznet predlog jedne klase biometrijskog kriptosistema za autentifikaciju sa zaštitom šablona i biometrijski zavisnim oslobađanjem kriptografskog ključa. Jedan od glavnih doprinosa je nov pristup automatskom izdvajanju obeležja iz teksture otiska prsta, zasnovanog na konvolucionim neuronskim mrežama. Pored toga, predložena je kvantizacija kodovanjem sa dva bita, kako bi se obeležja prevela u binarni domen u skladu sa postavljenim ciljem da se omogući primena XOR biometrije. Primenom odgovarajuće tehnike ispravljanja grešaka, koja zadovoljava bezbednosne zahteve, formirana je šema fazi povezivanja sa dužinom kriptološkog ključa koji se može koristiti u drugim savremenim kriptografskim sistemima. Evaluacija eksperimentalnih rezultata potvrđuje efektivnost predloženog pristupa.

Tema doktorske disertacije je aktuelna, a naučni doprinos prezentovanog istraživanja i predloženog praktičnog rešenja ogleda se u povećanju sigurnosti biometrijskih podataka i njihove primene u vrhunskim autentifikacionim sistemima, kao i u drugim kriptografskim sistemima prilikom čuvanja kriptoloških ključeva. Očekuje se da će prezentovana analiza mnogobrojnih sistema, kao i inovativni doprinos ove disertacije poslužiti kao polazna osnova za dalja istraživanja, unapređenje ovog i drugih postojećih sistema, kao i da će biti inspiracija za nova rešenja.

1.3. Ciljevi i metode istraživanja

Naučni ciljevi istraživanja sastoje se od objedinjenih deskripcija određenih naučno–teorijskih kategorija, njihovih relacija i međusobne zavisnosti svih činilaca sadržanih u radu, uz poštovanje metoda za izradu naučno–istraživačkog rada. Konkretan cilj istraživanja ujedno je i teorijski cilj, a podrazumeva uspostavljanje teorijskih okvira sistematičnom i kritičnom analizom literature i aktuelnih naučnih radova iz oblasti biometrijskih tehnika i sistema, različitih načina implementacije, s posebnom pažnjom usmerenom na sigurnost ovih sistema i potencijal za primenu biometrije u kriptografskim sistemima. Postavljeni cilj ovog istraživanja je da se ostvari visok nivo zaštite biometrijskih podataka otisaka prstiju i pridruženih asociranih kriptoloških ključeva u biometrijskim kriptosistemima. Za ostvarenje ovog cilja presudno je izvršiti transformaciju izdvojenih biometrijskih karakterističnosti u skup fiksnog broja elemenata, koji se diskretizacijom može prevesti u binarni domen. Na taj način omogućena je ravnopravna primena globalnih i lokanih informacija o teksturi otiska prsta, u poređenju sa minucijama koje su do sada primarno korišćene u sistemima za prepoznavanje otisaka prstiju. U okviru eksperimentalnog dela istraživanja dokazana je uspešnost predloženog rešenja.

Za naučni i istraživački rad primenjivane su brojne metode s ciljem zadovoljenja osnovnih metodoloških zahteva: objektivnosti, pouzdanosti, opštosti i sistematičnosti. Na osnovu odabrane problematike, definisanih ciljeva istraživanja i postavljenih naučnih hipoteza, s ciljem da se definišu naučni i stručni zaključci i predlozi potencijalnih rešenja, sprovedena je teorijska analiza korišćenjem rezultata istraživanja iz međunarodne naučno-stručne građe. U disertaciji su predstavljena istraživanja naučno-teorijskih saznanja, relevantne literature i savremene poslovne prakse, primenom mnogobrojnih metoda kao što su: indukcija i dedukcija, analiza i sinteza, generalizacija i specijalizacija, metode dokazivanja i opovrgavanja, istorijske metode, kao i metode kompleksnog posmatranja i analize sadržaja.

Primenom istorijskog metoda prikupljeni su i analizirani rezultati brojnih istraživanja iz oblasti biometrije, izdvajanja karakterističnih detalja i obeležja, fazi povezivanja, kriptosistema, tehnika za korekciju grešaka i sigurnosnih analiza svega navedenog. Pribavljeni podaci potiču iz doktorskih disertacija i naučnih radova iz ove oblasti.

Statističke metode: U radu su korišćeni statistički podaci vodećih međunarodnih institucija, koje se bave organizacijom uporednih testiranja, prikupljanjem i prezentovanjem podataka o biometrijskim tehnologijama.

Metoda analize i sinteze: U radu je analiziran biometrijski sistem koji predstavlja celinu iz ugla njegovih modula za: akviziciju, izdvajanje obeležja, poređenje i donošenje odluke, kao i prateće infrastrukture za komunikaciju i skladištenje. U takvim sistemima

analizirani i ispitivani su uticaji pojedinih činilaca na sveobuhvatnu sigurnost ovih sistema. Posebno je analizirana sigurnost biometrijskih podataka i njihovog skladištenja, s obzirom na to da je iz ugla korisnika privatnost podataka najznačajniji potencijalni problem ovih sistema. Ujedno, zloupotreba podataka ili mogućnost njihove estimacije, predstavlja veliku ranjivost samog sistema. Sistematizacijom znanja i sintezom rezultata analize, prezentovan je princip rada i zaštite aktuelnih rešenja.

Metoda kompleksnog posmatranja i analize sadržaja primenjivana je tokom sagledavanja rezultata preuzetih iz drugih istraživanja u cilju definisanja pravca istraživanja i razvoja nove klase biometrijskog kriptosistema.

Metod komparacije: U cilju sagledavanja mogućnosti koje ova tehnologija pruža i njene primene, urađena je komparacija različitih postojećih rešenja. Primenom eksperimentalnog metoda urađena je simulacija predloženog biometrijskog kriptosistema i njegovog rada na javno dostupnim bazama otisaka prstiju, kako bi se izvršila njegova evaluacija i komparacija sa postojećim rešenjima. Na ovaj način primenjene su metode dokazivanja i opovrgavanja.

1.4. Hipoteze istraživanja

Hipoteza predstavlja definisanje pretpostavke s ciljem da se upotpuni oskudno empirijsko saznanje. S obzirom na to da je cilj ovog rada da definiše teorijski okvir predmetne teme i ustanovi načela primene biometrije u kriptografiji, opšta hipoteza disertacije od koje se krenulo u istraživanje glasi: „Biometrijske karakteristike ljudi mogu se primeniti u kriptografiji“. Posebna hipoteza koja proizilazi iz opšte je: „Reprezentaciju fizičkih osobina i karakteristika ponašanja čoveka možemo prilagoditi uspostavljenim kriterijumima i potrebama kriptografije, kako bismo ih iskoristili za upravljanje kriptološkim ključevima“. Pojedinačne hipoteze koje su nadalje korišćene u disertaciji glase:

1. Informacije o teksturi otisaka prstiju mogu se upotrebiti za formiranje biometrijskog kriptosistema;
2. Za izdvajanje biometrijskih obeležja moguće je upotrebiti duboke konvolucione neuronske mreže;
3. Izdvojena biometrijska obeležja otisaka prstiju moguće je konvertovati u binarni domen radi formiranja XOR biometrije;
4. Biometrijski kriptosistem može se upotrebiti za zaštitu biometrijskih šablona i kriptoloških ključeva.

1.5. Struktura rada

Pored uvodnih razmatranja, kratkog pregleda oblasti i prezentacije metodološkog pristupa i postavljenih hipoteza u prvom poglavlju, rad se sastoji od još četiri poglavlja.

U drugom poglavlju dat je pregled i podela biometrijskih sistema za autentifikaciju, kao i poređenje sa sistemima autentifikacije zasnovanih na znanju i objektu. Definisan je konceptualni model jednog biometrijskog sistema, kao i njegovi parametri kojima se performanse mere, kvantifikuju i izražavaju. U nastavku poglavlja detaljno su istražene i analizirane biometrijske tehnike za autentifikaciju na osnovu: otiska prsta, dužice oka i crta lica, dok su osnovni principi ostalih najzastupljenijih biometrijskih osobina ukratko objašnjeni. Prezentovani su rezultati analize upotrebe više biometrijskih izvora podataka istovremeno, formirajući tako multibiometrijski sistem. Ključno pitanje kod ovih sistema je način sjedinjavanja podataka, pa je izvršena podela i komparativna analiza svih pristupa. Razmatrani su razlozi ovakvog pristupa autentifikaciji i identifikovane su prednosti i mane, koje se javljaju u svakoj mogućoj implementaciji.

Treće poglavlje posvećeno je sigurnosti sistema i biometrijskih podataka koji se koriste u njemu. Analizirana je sigurnost biometrijskog sistema, na osnovu čega je formiran model pretnji. Istraženi su postojeći najpoznatiji napadi, posledice koje proističu iz njih, kao i odgovarajuće protivmere. Posebna pažnja je posvećena zaštiti biometrijskih podataka i privatnosti korisnika, pa su posebno analizirani načini zaštite biometrijskih šablona. Rešavajući probleme zaštite biometrijskih šablona i upravljanja kriptografskim ključevima, nastali su biometrijski kriptosistemi, koji su predstavljeni u ovom poglavlju. Dat je aktuelni pregled ovih sistema i analizirane su njihove mogućnosti u pogledu zaštite tajnih ključeva biometrijom i generisanja kriptografskih ključeva na osnovu biometrijskih podataka.

Četvrto poglavlje se nadovezuje na treće i u njemu je dat predlog nove klase biometrijskog kriptosistema zasnovanog na novopredloženom rešenju da se primene konvolucione neuronske mreže za izdvajanje obeležja. Kako bi se ostvario visok nivo zaštite biometrijskih podataka, predloženo je da se formira biometrijski kriptosistem zasnovan na fazi povezivanju. Osnovni preduslov za formiranje ovog sistema je da se iz biometrijskih podataka otisaka prstiju formira binarna reprezentacija fiksne dužine. Predloženo je efikasno rešenje za diskretizaciju, kojom je izvršena transformacija izdvojenih obeležja u binarni domen, čime se omogućuje primena XOR biometrije. Rezultujući binarni šabloni fiksne dužine, testirani su u režimu autentifikacije sa integrisanim sistemom upravljanja kriptološkim ključevima, baziranim na tehnikama za korekciju grešaka. Izbor adekvatnog koda za korekciju grešaka predstavlja sigurnosni izazov zbog mogućih statističkih napada. Usled toga je, pored efikasnosti koda da ispravi greške izazvane biometrijskom varijabilnošću, uzeto u razmatranje i pitanje otpornosti na

sigurnosne pretnje ove vrste. U ovom poglavlju analizirani su eksperimentalni rezultati predložene klase biometrijskog kriptosistema.

Na kraju disertacije izveden je kritički osvrt na prezentovane rezultate, izvedeni su zaključci i njihovo poređenje sa postavljenom opštom hipotezom i ciljevima istraživanja. Dati su predlozi mogućih pravaca daljih istraživanja i unapređenja iz ove oblasti, kao i spisak referentne literature.

2. Biometrija

2.1. Uvod

Biometrijom se izučavaju merljive fizičke osobine i karakteristike ponašanja [3]. Naziv je nastao od grčkih reči *bios* – život i *metron* – meriti, dok su međunarodna tela za standardizaciju biometriju definisala kao: „automatizovano prepoznavanje pojedinaca na osnovu njihovog ponašanja i bioloških osobina“[1]. Iz ugla iskazanog naučno-istraživačkog interesovanja, u najistaknutije biološke osobine spadaju: otisci prstiju, dužica oka, mrežnjača oka, geometrija šake, crte lica, termografija lica, vaskularni obrasci (raspored vena), miris i DNK, dok se od biometrija karakterističnosti ponašanja izdvaja dinamika: potpisivanja, govora, hoda i kucanja na tastaturi [4].

Biometrijske karakteristike mogu biti primenjene u različitim sigurnosnim sistemima, u zavisnosti od definisanih zahteva, načina akvizicije koji su na raspolaganju i nivoa neophodne sigurnosti. Sve biometrijske karakteristike poseduju izvesne prednosti i nedostatke, stoga je odabir najbolje biometrije za neku konkretnu implementaciju uslovljen analizom više različitih faktora. Prilikom izbora biometrijske karakteristike za primenu u nekom biometrijskom sistemu, poželjno je da ona bude [5]:

- Univerzalna – svi korisnici obuhvaćeni sistemom poseduju izabranu karakteristiku;
- Jedinstvena – nad primenjenom populacijom odabrana biometrija mora biti jednoznačna za svakog korisnika;
- Postojana – nepromenljivost izabrane biometrije u vremenu;
- Merljiva – iz željene karakteristike moguće je izdvojiti specifična obeležja i digitalno ih reprezentovati;
- Zadovoljavajućih performansi – neophodno je da preciznost i odziv sistema zadovoljavaju definisane potrebe i eventualno postojeća ograničenja;
- Prihvatljiva – korisnici sistema moraju biti uvereni u poštovanje načela privatnosti i sigurnosti svojih biometrijskih podataka, kako bi bezrezervno prihvatili njihovo korišćenje;
- Sigurna – poverenje u sistem, na osnovu procene mogućnosti njegove obmane i primenjenih protivmera.

Biometrijski sistemi mogu biti bazirani samo na jednoj biometrijskoj osobini, a mogu se koristiti dve ili više različitih biometrijskih osobina u multimodalnim biometrijskim

[1] Definicija po ISO/IEC JTC1 (*Joint Technical Committee 1*) SC (*SubCommittee*) 37 – Telo za standardizaciju biometrije

sistemima. Takođe, moguće je višestruko korišćenje jednog istog biometrijskog izvora, s tim da se razlikuje način akvizicije ili način obrade podataka. Kod biometrijskih osobina, koje poseduju takvu mogućnost, moguće je korišćenje više instanci iste biometrijske osobine (npr. upotreba različitih prstiju ili oba oka). Svi ovi sistemi, koji koriste više od jednog biometrijskog izvora podataka, zovu se multibiometrijski sistemi.

2.2. Biometrijski autentifikacioni sistemi

Sigurnost informaciono-komunikacionih sistema se obično realizuje kroz tri procesa:

- autentifikacija (engl. *authentication*) – utvrđivanje identiteta,
- autorizacija (engl. *authorization*) – utvrđivanje ovlašćenja i
- neporecivost (engl. *non-repudiation*).

Autentifikacija predstavlja proces utvrđivanja ili potvrde nečijeg identiteta. Posedovanje nekog oblika jednoznačnosti omogućava autentifikaciju neke osobe ili uređaja u nekom sistemu. Autentifikacija se može podeliti na:

- identifikaciju i
- verifikaciju.

Verifikacija predstavlja postupak potvrde predloženog identiteta nekog korisnika, uređaja ili nekog drugog sistema, na osnovu upoređivanja priloženih obeležja i odgovarajućeg uzorka koji se čuva u bazi podataka autentifikacionog sistema. Ovaj oblik autentifikacije je sistem 1:1, jer se poređenje radi samo sa jednim ciljanim uzorkom.

Biometrijska identifikacija predstavlja proces pronalaženja identiteta neke osobe, uređaja ili sistema, upoređivanjem prezentovanih ili pronađenih specifičnih obeležja sa svim uskladištenim uzorcima u bazi biometrijskih podataka. Ovaj oblik autentifikacije je sistem 1:N, jer se poređenje radi sa više uzorka. Postoji pozitivna i negativna identifikacija, odnosno kada u zavisnosti od potrebe potvrđujemo nečiji identitet ili isključujemo postojanje tog identiteta u nekoj bazi podataka, kao na primer u bazi lica za kojima je raspisana poternica.

Autentifikacijom isključivo pronalazimo ili potvrđujemo neki identitet. Ovim procesom se ne definišu prava pristupa koja pripadaju tom identitetu. Autorizacijom se proveravaju prava nad objektima za subjekat potvrđenog identiteta.

Neporecivost predstavlja načelo kojim se sprečava lažno poricanje neke radnje nad nekim objektom, generisanja neke poruke ili dokumenata, izmene bilo kakvih podataka u

sistemu, odnosno predstavlja mogućnost da je uvek moguće dokazati da poruke, dokumenti ili izmene proističu od nekog entiteta, iako on to poriče. Za obezbeđenje neporecivosti akcija nad objektima koristi se evidentiranje – čuvanje podataka o svim akcijama subjekata. U računarskim komunikacijama (npr. elektronska trgovina) primenjuju se kriptografske tehnike digitalnog potpisivanja ili šifrovanja, kojima se postiže autentičnost i neporecivost.

Metode autentifikacije mogu biti zasnovane na [3]:

- znanju (lozinka, LIB i dr.),
- objektima (pametna kartica, RFID token i dr.) i
- biometrijskim karakteristikama.

Lozinke predstavljaju najjednostavniju i najpopularniju vrstu autentifikacije. Razlog leži u činjenici da za njihovo korišćenje nije potrebna nikakva dodatna oprema u računarskim sistemima i da su jednostavne za upotrebu. Međutim, porastom snage računarskih sistema lozinke postaju sve manje sigurne. Ako se uzme u obzir i ljudski faktor, kao najslabija karika u lancu sigurnosti, lozinke više nisu primenljive za sigurnost važnijih sistema. Lozinke bi trebalo da budu različite za svaki servis koji se koristi, da zadovoljavaju određenu kompleksnost i da se često menjaju. Kako su ljudi danas izloženi velikom broju sistema i servisa koji zahtevaju lozinku, poštovanje navedenih sigurnosnih pravila jednostavno nije moguće. Uz eventualne manje varijacije, često se koristi jedna ista lozinka za sve potrebe. U boljem slučaju koriste se dve do tri lozinke u zavisnosti od značajnosti servisa, odnosno sistema. Neretko se koriste servisi za generisanje kompleksnih lozinki, njihovo čuvanje i automatsko popunjavanje pristupnih kredencijala. Kompromitacijom sigurnosti takvog sistema, kompromitovanost korisnika se lančano prenosi. Značajan pritisak na sigurnost autentifikacije bazirane na znanju predstavljaju automatizovani sistemi za krađu akreditiva za pristup, najčešće metodom fišinga (engl. *phishing*) [6]. Krađa identiteta, zahvaljujući slabostima ove vrste autentifikacije, sve više potiskuje upotrebu lozinki za pristup sistemima od velike važnosti.

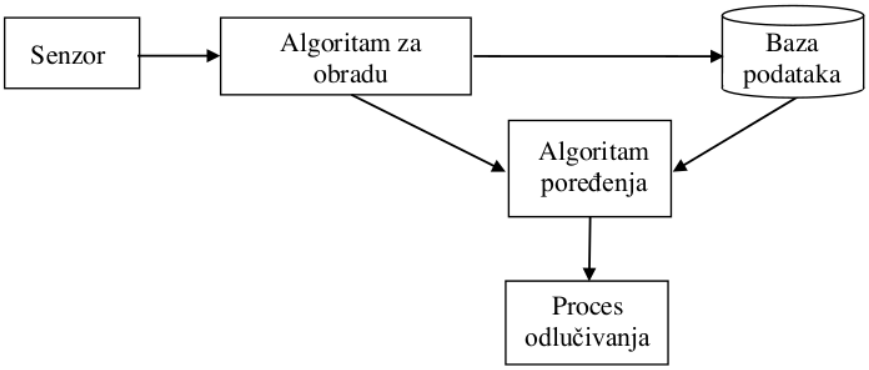
Autentifikacija zasnovana na objektima predstavlja viši nivo bezbednosti, usled značajno veće kompleksnosti objekta u odnosu na lozinku i činjenice da korisnik nema uticaja na odabir tajne jednoznačnosti. U praksi, najčešće se koristi u kombinaciji sa prvom metodom, kako bi se dodatno osigurao proces autentifikacije od neovlašćene upotrebe ili krađe objekta. Nedostaci ovog pristupa su potreba za dodatnim hardverom i problemi vezani za eventualni gubitak, krađu ili oštećenje objekta. Ipak, bez obzira na navedene nedostatke, pristup sistemima od velike važnosti često se oslanja na ovaj metod autentifikacije.

Generalizacijom, biometrijski sistemi za autentifikaciju mogu se posmatrati kao potklasa autentifikacionih sistema zasnovanih na objektima, gde objekat predstavlja neka biometrijska fizička osobina ili karakterističnost ponašanja. Biometrijski „objekat“ se ne može izgubiti, ali potrebe za posebnim dodatnim hardverom postoje. Prethodne dve metode autentifikacije bazirane na znanju i objektu omogućavaju samo pozitivnu autentifikaciju, pa se kao dodatna prednost primene biometrije ogleda u njenoj mogućnosti za uspostavljanje negativne autentifikacije.

Sve je češća primena slojevite autentifikacije. Slojevitost se ogleda u nivou potrebne bezbednosti za određeni servis ili sistem. Naravno, prvi sloj čine lozinke za autentifikaciju na servise nižeg značaja, a najviši sloj uključuje upotrebu biometrije. Kako raste potreba za najvišim nivoom sigurnosti, raste i unapređenje biometrijskih sistema koji se sve više primenjuju u svim segmentima društva kada je potrebno nedvosmisleno pronaći ili verifikovati nečiji identitet. Od šire primene biometrijskih sistema, deli nas kompleksnost ove tehnologije, određeni stepen odbojnosti ljudi prema upotrebi njihovih ličnih karakteristika, kao i samo pitanje privatnosti podataka i korisnika.

2.3. Biometrijske karakteristike

Biometrijski sistem za autentifikaciju zasniva se na komparaciji specifičnih fizičkih osobina ili karakterističnosti ponašanja, sa onima koje se čuvaju u bazi podataka sistema. Apstrakcija jednog takvog sistema prikazana je na slici 1.



Slika 1 – Opšti model biometrijskog autentifikacionog sistema

Uopšteni model biometrijskog sistema za autentifikaciju može se predstaviti svojim osnovnim gradivnim modulima:

- senzor za akviziciju biometrijskih karakteristika i njihovu digitalnu reprezentaciju,
- algoritam za obradu obeležja – poboljšanje kvaliteta ulaznih podataka i formiranje šablona,
- baza podataka za čuvanje biometrijskih šablona,
- algoritam za poređenje šablona i
- modul odlučivanja – proces donošenja odluke o podudarnosti.

Postupak unošenja šablona u biometrijsku bazu podataka naziva se faza upisa. Tom prilikom se jednom ili više puta uzima uzorak na osnovu kojeg se formira šablon, koji se zatim verifikuje i skladišti. Korišćenje sistema za autentifikaciju naziva se faza prepoznavanja tj. poređenja. Biometrijski sistem za verifikaciju donosi odluku o nečijem identitetu, tako što ga potvrđuje ili ne, odnosno prihvata ili odbija, respektivno. To se može predstaviti teorijom odlučivanja i testiranjem hipoteze. Ako je T neki biometrijski šablon sačuvan u bazi podataka, a I neki biometrijski uzorak koji treba da uporedimo sa šablonom T, tada se sistem bazira na prostoj hipotezi:

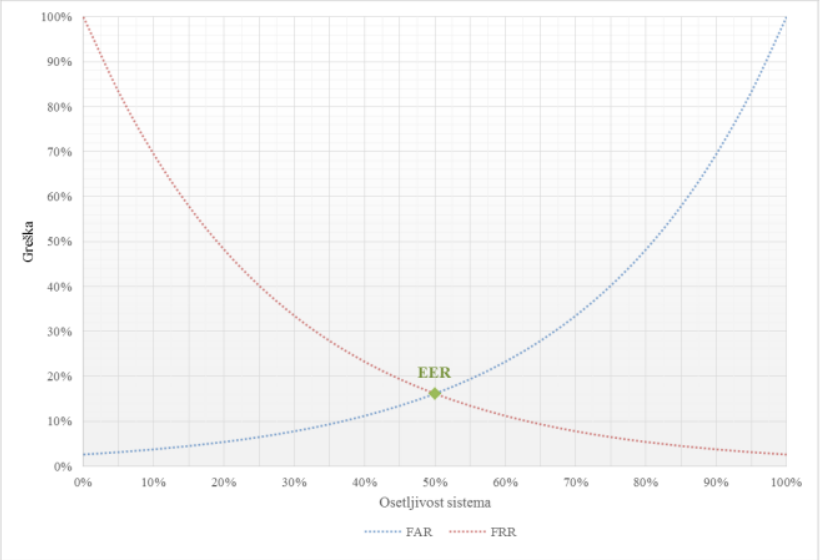
$$H_0 : \ I = T , \tag{1}$$

odnosno da šablon T odgovara uzorku I. Postupak verifikacije poredi T i I, utvrđuje njihovu sličnost i na osnovu definisane granične vrednosti donosi odluku o prihvatanju ili odbijanju hipoteze. U slučaju donošenja pogrešne odluke, javljaju se dve vrste grešaka:

- **greška I vrste** – kada hipotezu H_0 odbijemo a ona je tačna, što se predstavlja grešku odbijanja (engl. *False Rejection Rate* – FRR) i
- **greška II vrste** – kada hipotezu H_0 prihvatimo a ona nije tačna, što predstavlja grešku prihvatanja (engl. *False Acceptance Rate* – FAR).

Kod autentifikacionih sistema zasnovanih na znanju ili objektu, ispravan unos kredencijala, odnosno očitavanje pravog tokena, garantuje pozitivan ishod autentifikacije. Kod biometrijskih autentifikacionih sistema primena istog biometrijskog izvora podataka ne mora nužno imati kao ishod uspešnu autentifikaciju. Na rezultat poređenja utiče više faktora. Pre svega, biometrijske karakteristike su varijabilne, svaki senzor dodaje šum prilikom uzorkovanja, različiti senzori daju drugačija očitavanja itd. Zbog toga je potrebno definisati neku graničnu vrednost, na osnovu koje se donosi odluka o prihvatanju ili odbacivanju autentifikacije. Iz postojanja ove granične vrednosti proističu FRR i FAR greške. Za sisteme visoke sigurnosti margina greške mora biti minimalna, što znači da greška prilikom koje bi se izvršila pogrešna autentifikacija – FAR, mora biti minimalna. Međutim, sa previše malom marginom greške, usled pomenutih faktora nesavršenosti ovih

sistema, doći će do povećanja greške usled koje će sistem odbiti autentifikaciju legitimnog korisnika – FRR. Zavisnost ove dve vrste grešaka prikazana je na slici 2.



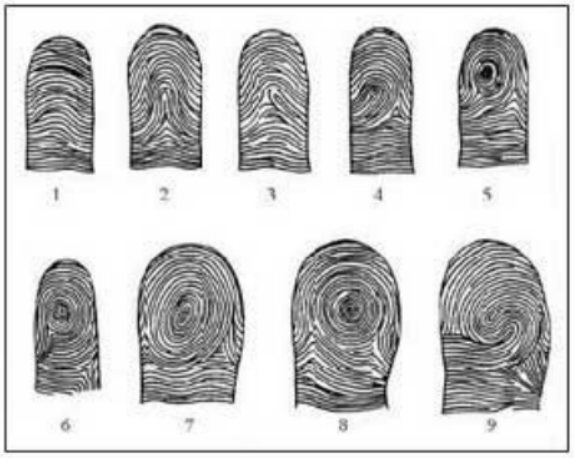
Slika 2 – Međusobna zavisnost FRR i FAR grešaka

Tačka preseka dve krive na dijagramu, naziva se greška jednakosti (engl. *Equal Error Rate* – EER), s obzirom na to da su greške FRR i FAR jednake pri toj graničnoj vrednosti. EER služi za komparaciju različitih biometrijskih sistema, gde manja vrednost greške označava bolje ukupne performanse. Prilikom iskazivanja performansi biometrijskih sistema, u literaturi se još koriste parametri: FMR (engl. *False match rate*) i FNMR (engl. *False non-match rate*), koji su respektivno ekvivalentni FAR i FRR, kao i GAR (engl. *Genuine acceptance rate*) kao mera tačnosti sistema prilikom verifikacije, gde je *GAR=1-FRR*.

2.3.1. Otisak prsta

Sa fiziološkog aspekta otisak prsta predstavljaju udubljenja i ispupčenja, odnosno doline i brazde kojima se formiraju papilarne linije. Otisak prsta je jedinstven za svakog čoveka, ne menja se vremenom i samim tim zadovoljava osnovne kriterijume za njegovu primenu u autentifikaciji. Papilarne linije formiraju izvesne složene strukture koje se mogu klasifikovati u više grupa. Prvu takvu klasifikaciju uradio je češki patolog i fiziolog Jan Purkinje (*Jan Evangelista Purkyně*) 1823. godine, podelom otisaka u 9 grupa, kao na slici 3. Henri Folds je 1886. godine napravio svoju klasifikaciju koristeći slogove. U njegovom sistemu svaka ruka je predstavljena sa pet slogova, po jedan za svaki prst. Slogovi se prave od suglasnika i samoglasnika, čije je značenje dato u odgovarajućoj listi, a predstavlja određene karakteristike otiska. Ovaj sistem je teoretski mogao da napravi $17 \cdot 10^{12}$ različitih

klasifikacija [8]. Frensis Galton je 1892. godine u [2] predložio svoju klasifikaciju na tri vrste otisaka: luk, petlja i spirala. Dve godine kasnije Skotland Jard je pridodao ovu klasifikaciju Bertiljonovom sistemu koji su koristili. Ivan Vučetić proširio je Glatonovu klasifikaciju na četiri vrste: luk, unutrašnja petlja, spoljašnja petlja i spirala. Ovoj osnovnoj klasifikaciji je pridodao i dodatnu klasifikaciju koja je dodatno opisivala svaku od osnovnih vrsta iskazano brojevima od 5 do 10, formirajući tako podtipove. Takođe, na osnovu Galtonovih radova, 1899. godine Edvard Henri (*Sir Edward Henry*) razvio je svoju klasifikaciju otisaka prstiju. Prvo se otisci predstavljaju numeričkom reprezentacijom svakog prsta i podelom na 1024 grupa u zavisnosti od broja spiralnih petlji na svakom prstu, a zatim se radi podela prema strukturi otiska na: luk, visoki luk, leva petlja, desna petlja i spirala [1] [10]. Henrijev sistem je dao odlične rezultate u Indiji, nakon čega je prihvaćen i u Velikoj Britaniji. Danas, klasifikacije otisaka prstiju koje se koriste u svetu u osnovi su bazirane na Galtonovoj, Vučetićevoj i Henrijevoj klasifikaciji ili njihovim kombinacijama uz određene modifikacije i unapređenja. Na primer FBI koristi klasifikaciju koja se bazira na tri glavna tipa koje je definisao Galton i podtipovima svake od njih [9]. U Tabeli 1. data je zastupljenost svakog tipa otiska prstiju po Henrijevoj kategorizaciji [10].



Slika 3 – Purkinjeova klasifikacija otisaka prstiju (preuzeto iz [7])

Tabela 1 – Zastupljenost tipova otiska prstiju po Henrijevoj kategorizaciji

Kategorija	Zastupljenost
Luk	3,70%
Visoki luk	2,90%
Leva petlja	33,80%
Desna petlja	31,70%
Spirala	27,90%

Postupak upoređivanja otisaka prstiju se može podeliti na sledeće faze:

- skeniranje prsta,
- obrada rezultata skeniranja,
  - poboljšanje kvaliteta – redukcija šuma,
  - segmentacija otiska od pozadine,
  - određivanje polja orijentacije,
  - binarizacija, istanjivanje i izdvajanje papilarnih linija i
  - izdvajanje obeležja (karakteristični detalji, klasifikacija otiska i uklanjanje lažnih detalja);
- poređenje izdvojenih obeležja.

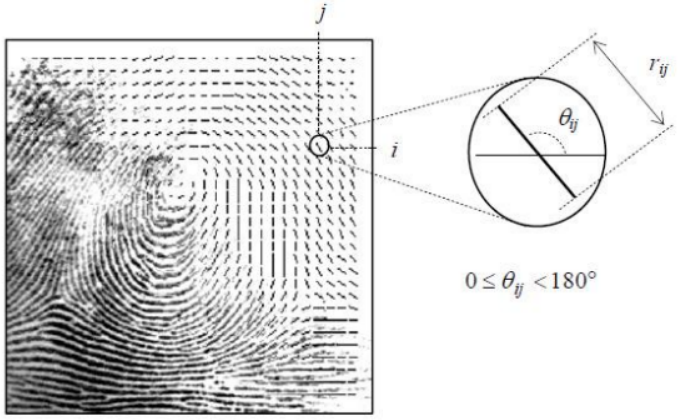
Prve kolekcije otisaka prstiju pravljene su uz pomoć crnog mastila i papira. Napretkom informacionih tehnologija, slika je sa papirnog zapisa digitalizovana i tako upisivana u baze podataka. Prvi specijalizovani čitači otisaka prstiju pojavili su se sredinom osamdesetih godina prošlog veka i u njima su korišćeni senzori bazirani na optičkoj tehnologiji. Senzori su se razvijali i danas ih prema principu rada možemo podeliti na [11]: optičke, ultrazvučne i poluprovodničke.

Optički senzori su najstariji i najčešće korišćeni. Baziraju se na principu totalne unutrašnje refleksije (engl. *Total Internal Reflection*). Pritiskom prsta na staklenu prizmu, ispupčenja ostvaruju direktan kontakt sa površinom, dok se udubljenja nalaze na izvesnoj distanci. Jedna strana prizme se osvetljava difuznim svetlom, koje se odbija od udubljenja, a apsorbuje u ispupčenjima. Sa druge strane prizme reflektovana svetlost izlazi i sistemom sočiva se fokusira na CCD (engl. *Charge Coupled Device*) ili CMOS (engl. *Complementary Metal–Oxide–Semiconductor*) senzor. Ultrazvučni senzori se retko koriste, a princip rada je zasnovan na osobini zvučnih talasa da prodiru u materijale i različitog odbijanja od prelaznih površina. Na taj način se dobijaju informacije o površini prsta. Ovi senzori su otporni na smetnje usled masnih ili zaprljanih prstiju, koje predstavljaju problem kod optičkih i poluprovodničkih senzora. Međutim, njihova cena je dosta velika i nisu u masovnoj upotrebi. Poluprovodnički senzori ostvaruju direktan kontakt sa prstom i, u zavisnosti od načina rada, detektuju ispupčenja i udubljenja na prstu. Po načinu prevođenja fizičkih veličina u električne signale mogu se podeliti u četiri glavne grupe: kapacitivne, temperaturne, elektromagnetne i piezoelektrične.

Kvalitet uzorkovane slike otiska prsta ima značajan uticaj na performanse kasnije obrade. Ključni faktori, u tom smislu, su: rezolucija slike, obuhvaćena površina i jasnoća papilarnih linija. U većini primena, rezolucija slike potrebna za uspešnu obradu je 500ppi, dok se u poslednje vreme u forenzičkoj primeni sve više upotrebljava 1000ppi. U civilnoj upotrebi se mogu naći senzori manje rezolucije od 500ppi, zbog niske cene ili fizičkih ograničenja uređaja u koje se ugrađuju. Pri rezoluciji od 500ppi, razmak između susednih ispupčenja je oko 9 piksela [10]. Obuhvaćena površina otiska zavisi od senzora i načina akvizicije. Razlikujemo otiske gde se koristi samo površina koju dobijemo prislanjanjem ili

prevlačenjem prsta preko senzora i one gde je prst potrebno valjati po senzoru. Prvi slučaj ima manju obuhvaćenu površinu, pa je samim tim siromašniji sa karakterističnim detaljima koji se mogu izdvojiti. U zavisnosti od primene, bira se odgovarajući senzor i metodologija uzimanja otisaka. Jasnoća dobijene slike zavisi od kvaliteta senzora, stanja kože i uslova prilikom skeniranja. Stanje kože prstiju kod ljudi koji se bave fizičkim poslom i kod starijih ljudi je dosta lošije. Takođe, čistoća i vlažnost prstiju imaju dodatni uticaj na jasnoću papilarnih linija.

Prilikom obrade slike otiska radi se: segmentacija, izračunavanje polja orijentacije, binarizacija slike, istanjivanje i izdvajanje papilarnih linija, kako bi se u poslednjem koraku pronašlo što više specifičnih obeležja. Segmentacija se sastoji od izdvajanja regiona otiska od pozadinskog dela slike, koje nema informacije od značaja za dalju obradu. Na taj način se sprečava slučajno izvlačenje obeležja iz šuma koji je obično prisutan na periferiji slike otiska. Postoji više pristupa ovom procesu, od prostih rešenja koji se baziraju na činjenici da je neiskorišćena pozadina uniformna i svetlija od dela slike koji sadrži otisak, pa se uz određivanje praga intenziteta odstranjuju takve površine, do veoma robusnih algoritama koji utvrđuju u nekom diskretnom regionu postojanje papilarnih linija i njihove orijentacije. U zavisnosti od pristupa segmentaciji, ona se radi pre ili nakon određivanja polja orijentacije papilarnih linija. Orijentisanost brazdi predstavlja jednu od najvažnijih osobina slike otiska prsta i zapravo predstavlja ugao θ_{xy} kojim se brazda prostire duž slike u tački (x,y). Zbog optimizacije opterećenja računarskih resursa, ne radi se proračun ugla svakog piksela. S obzirom na to da brazde nemaju oštre promene uglova, radi se njihova aproksimacija. Jedna od metoda je da se slika predstavi kvadratnom matricom gde svaki element θ_{ij}, odgovara čvoru $[i,j]$ mreže, koji se nalazi u pikselu $[x_i,y_j]$ i određuje prosečnu orijentaciju ispupčenja u okolini tog piksela. Dodatna vrednost r_{ij} se povezuje sa svakim elementom θ_{ij} i označava pouzdanost orijentacije. Vrednost r_{ij} je mala za regione sa izraženijim šumom ili ozbiljno oštećene regione, a velika za visokokvalitetne regione u otisku prsta. Princip je prikazan na slici 4.



Slika 4 – Određivanje polja orijentacije (preuzeto iz **[10]**)

Izdvajanje i istanjivanje papilarnih linija je sledeći korak obrade slike otiska. Kada se posmatra jedan mali region slike, ispupčenja i udubljenja formiraju sinusoidu. U takvom malom regionu imaju izraženu frekvenciju i lokalnu orijentaciju, što olakšava izdvajanje piksela koji predstavljaju brazde. Izdvajanje brazdi se vrši primenom Gaborovog filtra, koji ima sledeći oblik:

$$G(x,y) = e^{\left[-\frac{1}{2}\left(\frac{x^2}{\partial_x^2}+\frac{y^2}{\partial_y^2}\right)\right]}\cos(2\pi x u_0), \qquad (2)$$

gde je u_0 učestanost sinusoide uzduž x ose, dok ∂_x i ∂_y predstavljaju standardnu devijaciju Gausove anvelope uzduž x i y ose, respektivno. Pomoću ovih Gaborovih filtara izdvajamo papilarne linije zahvaljujući njihovoj osobini da primenom određenog ugla θ izdvajaju se sve linije koje se prostiru u pravcu $(\theta+\pi/2)$ [8]. Sliku otiska delimo u pojedinačne male regione – blokove, određujemo frekvenciju i lokalnu orijentaciju brazdi u bloku, koji zatim filtriramo. Nakon izdvajanja papilarnih linija, sledi njihovo istanjivanje i binarizacija, što za rezultat ima sliku otiska sa papilarnim linijama širine jednog piksela. Neki algoritmi poređenja ne koriste metodu binarizacije i istanjivanje brazdi, zato što se ovom aproksimacijom gubi deo informacija.

Specifična obeležja otisaka prstiju mogu se hijerarhijski rasporediti u tri nivoa [3]:

- I nivo – singularni regioni i orijentacija papilarnih linija,
- II nivo – minucije i
- III nivo – najsitnija obeležja, kao što su pore, oblik ivica linija itd.

Prvi i drugi nivo specifičnih obeležja koriste se u aktuelnim tehnikama poređenja otisaka prstiju, dok se treći nivo primenjuje uglavnom samo za potrebe kriminalističke forenzike, u slučajevima latentnih ili parcijalnih otisaka kad se ne raspolaže sa dovoljno specifičnih obeležja prethodnih nivoa. Prvi nivo specifičnih obeležja otisaka prstiju se uglavnom koristi za kategorizaciju otisaka. Papilarne linije u određenim regionima obrazuju specifične oblike, a takvi delovi otiska zovu se singularni regioni, odnosno singulariteti. Singulariteti se mogu kategorizovati u tri osnovne tipologije: petlja, delta i spirala, što je prikazano na slici 5. U praksi, centar jezgra odgovara centru severnog singularnog regiona sa najvećim brojem singularnosti tipa petlje. Za otiske koji ne sadrže singularitete tipa petlja ili spirala (npr. tipa luk), teško je definisati jezgro. U ovim slučajevima, centar jezgra se obično povezuje sa tačkom maksimalne zakrivljenosti papilarne linije. Nažalost, zbog velike varijabilnosti strukture prstiju, automatizovana detekcija centralne tačke nije uvek moguća u svim otiscima prstiju.



Slika 5 – Jezgro i delta u otiscima prstiju (leva petlja, desna petlja i spirala)

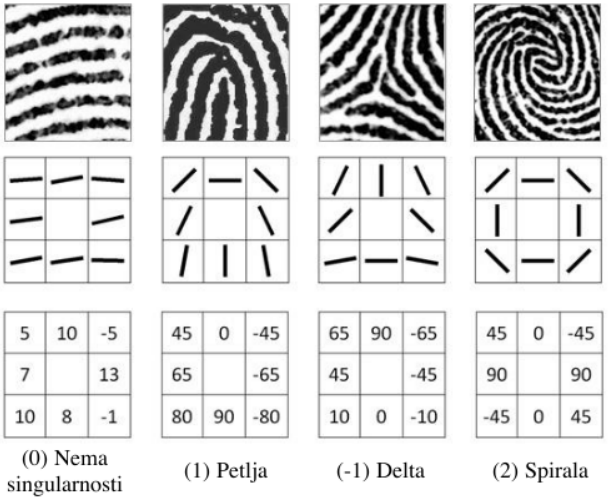
Singularni regioni mogu se izdvojiti iz polja orijentacije upotrebom Poenkareove (*Poincaré*) metode indeksiranja. Poenkareov indeks (PI) se odnosi na kumulativnu promenu orijentacije duž zatvorene putanje polja. Da bi se odredila tačna lokacija i vrsta singularnosti, PI se određuje na osnovu osam susednih piksela, formulom:

$$PI = \frac{1}{\pi}\sum_{i=0}^{7}\delta\left(O\left[(i+1)_{\mathrm{mod}8}\right]-O_i\right), \tag{3}$$

gde je $O_i \in [0,\pi)$ orijentacija osam susednih piksela u smeru suprotnom od kazaljke, i je redni broj piksela, a $\delta(\theta)$ je definisana:

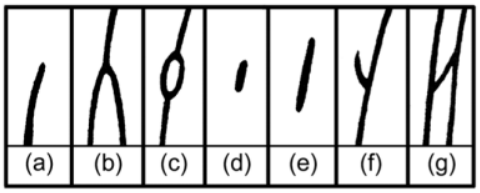
$$\delta(\theta)=\begin{cases}\theta-\pi, & \theta>\dfrac{\pi}{2}\\ \theta, & -\dfrac{\pi}{2}\le\theta\le\dfrac{\pi}{2}\\ \theta+\pi, & \theta<-\dfrac{\pi}{2}\end{cases}. \tag{4}$$

PI jednog piksela može imati jednu od četiri moguće vrednosti: 0 – nema singularnosti, -1 – delta, 1 – petlja i 2 – spirala, što je prikazano na slici 6. U okolini centralne tačke singularnosti detektuje se više singularnih tačaka. Zato se koristi algoritam za grupisanje, koji objedinjuje sve pronađene bliske singularne tačke istog tipa. Pomoću određenih singularnih regiona radi se kategorizacija otiska.



Slika 6 – Poenkareov indeks

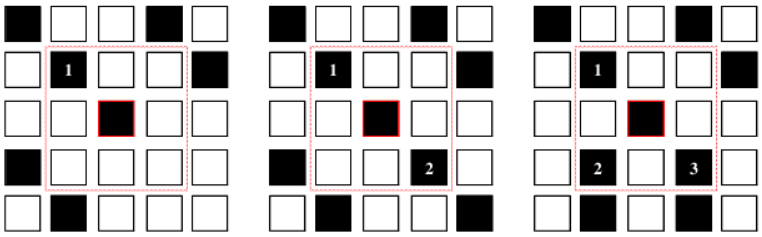
U drugom nivou, specifična obeležja predstavljaju tačke u kojima se javljaju promene kod papilarnih linija, kao što su: prekid, ukrštanje linija, formiranje ostrva, račvanje itd. Ovakve singularne tačke nazivaju se minucije. Na slici 7. prikazane su neke od najznačajnijih minucija. Do sada je prepoznato oko 150 različitih singularnih tačaka, međutim zbog najlakše i najpreciznije detekcije, u većini razvijenih sistema za autentifikaciju najčešće se primenjuju samo dva tipa: prekid i račvanje linije. Kvalitetan otisak, uzorkovan valjanjem prsta po senzoru, poseduje oko 100 ovakvih singularnih tačaka [10], dok se iz dela otiska koji je obuhvaćen skenerima u komercijalnoj upotrebi (na principu prislanjanja ili prevlačenja prsta) može izdvojiti između 30 i 40 minucija.



a) prekid linije; b) račvanje; c) jezero; d) ostrvo;
e) kratka nezavisna linija; f) kuka; g) ukrštanje

Slika 7 – Najznačajnije vrste minucija

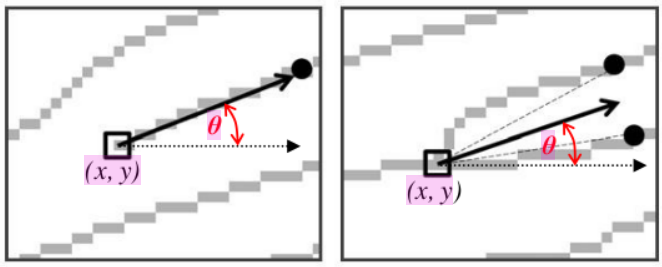
Na osnovu istanjene slike otiska, gde je svaka papilarna linija debljine jedan piksel, pristupa se detekciji prekida linije i račvanja. To je moguće postići brojanjem susednih piksela koji predstavljaju deo papilarne linije. Princip je prikazan na slici 8. Ukoliko jedan piksel u svom okruženju ima samo jedan susedni piksel, koji predstavlja papilarnu liniju, to je tačka u kojoj je kraj papilarne linije. Ukoliko je u okruženju tri piksela, onda je u pitanju račvanje. Kada je broj piksela dva, tada je reč o pikselu koji se nalazi unutar papilarne linije, dok vrednost veća od tri predstavlja neki kompleksni oblik.



a) 1 susedni piksel b) 2 susedna piksela c) 3 susedna piksela

Slika 8 – Princip detekcije prekida i račvanja papilarnih linija

Svaka minucija predstavlja se kodom, u kojem je navedena vrsta singulariteta, njene koordinate i ugao. Kako bi se odredio ugao minucije tipa kraj linije, određuje se pravac papilarne linije, a na osnovu njega računa se ugao koji zaklapa, što je ilustrovano na slici 9. a). U slučaju minucije račvanja, pravac se određuje sredinom ugla koji zaklapaju dve grane u odnosu na poziciju minucije, pa se na osnovu određenog pravca utvrđuje ugao minucije, kao na slici 9. b).[2]



a) kraj linije b) račvanje

Slika 9 – Određivanje pravca papilarne linije i ugla minucije

U praksi, neke detektovane minucije mogu biti lažne zbog artefakata koji se javljaju pri obradi slike i šuma prilikom uzimanja otiska prsta. Da bi se uklonile ove lažne minucije, koristi se algoritam za filtriranje, koji se obično sastoji od više heurističkih pravila. Na primer, minucije koje ispunjavaju neki od sledećih uslova smatraju se lažnim i odbacuju se:

- minucije na papilarnim linijama koje nemaju susednu liniju sa obe strane (nepouzdani periferni regioni slike otiska prsta);
- minucijama koje su blizu jedna drugoj, a suprotnog su smera (greške nastale prilikom binarizacije gde dolazi do lažnog prekida papilarne linije);
- previše minucija u istom malom segmentu (šum).

[2] Ovo je jedan od načina određivanja ugla minucije, a postoji više standarda koji se značajno razlikuju [10].

Upoređivanjem otisaka samo na osnovu njihove slike, bez primene neke tehnike za izdvajanje specifičnih obeležja ili karakteristika, računski je zahtevno i nije moguće ostvariti tačne rezultate u značajnoj meri zbog varijabilnosti uzoraka usled nelinearnih izobličenja, različitog pozicioniranja i rotacije. Autentifikacioni sistemi se prema pristupu poređenju otisaka dele na one bazirane na:

- korelaciji,
- minucijama,
- globalnim i lokalnim informacijama o teksturi i
- ostalim osobinama otisaka prstiju.

Poređenje metodom korelacije radi po principu direktnog poređenja odgovarajućih piksela ili malih regiona dva otiska. Ova tehnika je veoma osetljiva na nelinearna izobličenja, stanje kože i pritisak prsta prilikom skeniranja, a takođe je računarski veoma zahtevna.

Najzastupljenije su metode poređenja otisaka prstiju koje su zasnovane na primeni minucija [11]. Izdvojene minucije se predstavljaju u vidu skupa tačaka u dvodimenzionalnoj ravni, gde je svaka singularna tačka m reprezentovana sa tri parametra: $\{x, y, \theta\}$, odnosno njenim koordinatama i uglom minucije. Pre početka upoređivanja otiska, neophodno je sprovesti njihovo poravnanje pomoću detektovanih singulariteta: delte i jezgra otiska. Poređenje otisaka se zatim sprovodi jednostavnim upoređivanjem skupova izdvojenih minucija i utvrđivanjem broja zajedničkih elemenata.

Informacije o teksturi otisaka najčešće se koriste kao pomoćne tehnike koje imaju za cilj da ubrzaju poređenje drugim metodama u režimu identifikacije. Na osnovu teksture otisci se klasifikuju u predefinisane klase. Prilikom identifikacije, uzorak se upoređuje samo sa šablonima koji pripadaju istoj klasi, čime se značajno smanjuje broj potrebnih poređenja. Ipak, u teksturi otiska sadržane su informacije o različitim prostornim frekvencijama, orijentaciji i fazi, pa je dekompozicijom u više prostornih frekvencija i orijentacija, moguće ostvariti neophodnu diskriminativnost prilikom poređenja ovih svojevrsnih obeležja.

Ostale metode poređenja otisaka se koriste kao dopuna metodama baziranim na minucijama zarad povećanja tačnosti i robusnosti sistema, a ne kao zasebne metode. Koriste se kod loših uzoraka (npr. latentni otisci) ili tamo gde su u primeni senzori loših karakteristika, pa nije moguće odrediti dovoljan broj ispravnih minucija. Neki od primera ovih metoda su: veličina i oblik spoljnog otiska prsta – silueta, broj, tip i položaj singulariteta, geometrijski atributi i prostorni odnos papilarnih linija i karakteristični detalji trećeg nivoa (pore, oblik ivica brazdi itd.).

2.3.2. Dužica oka

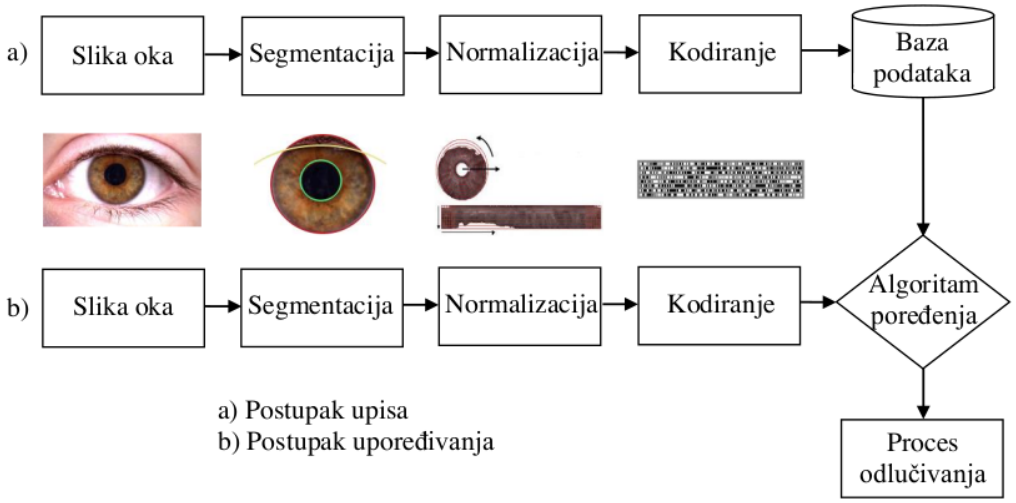
Dužica oka (engl. *iris*) je obojeno tkivo koje okružuje zenicu, a nalazi se između rožnjače i sočiva. Uloga dužice je regulacija količine svetlosti koja se propušta u oko. Sastoji se od nekoliko slojeva: sloj epitelnih ćelija visoke pigmentacije koji je neprobojan za svetlost, mišićni sloj koji je zadužen za skupljanje i širenje zenice, stromalni sloj koji se sastoji od vezivnog tkiva i krvnih sudova i spoljnog graničnog sloja koji sadrži veliki broj hromatofora, ćelija koje sadrže pigment. U zavisnosti od količine pigmenta u ovim ćelijama, zavisi boja dužice i to: veliko prisustvo pigmenta kao rezultat ima crnu i smeđu boju, malo prisustvo pigmenta zelenu, a odsustvo pigmenta plavu boju. Boja dužice nema značaj u biometrijskim sistemima, već je od značaja njena šara koja je rezultat specifične višeslojne strukture. Dužica prosečno poseduje oko 200 detalja koji se mogu upotrebiti za upoređivanje [12]. Zbog njene slučajne morfogeneze, veruje se da šara dužice poseduje dovoljnu jedinstvenost za primenu u biometrijskim sistemima. Zbog nepostojanja teorijskog modela za kvantifikaciju njene jedinstvenosti, nije prihvatljiva u sudskim postupcima kao dokaz[3]. Ipak, upotreba dužice oka je našla svoju primenu u civilnim sistemima, ali i državnim projektima za kontrolu granica. Statistička analiza i empirijska provera na osnovu baza velikog broja uzoraka u [13], potvrdila je jedinstvenost dužice oka u biometrijskim sistemima za autentifikaciju sa 249 stepena slobode i entropijom od 3,2 bita po mm^2. Kasnije eksperimentalne studije [14] su ukazale na problem postojanosti ove biometrijske karakteristike tokom starenja, usled čega dolazi do povećanja greške odbijanja kada postoji duži vremenski period između uzorkovanog šablona i uzorka za verifikaciju.

Ideju korišćenja dužice oka, kao prepoznatljivog ljudskog identifikatora, prvi je predložio Bertiljon [15] opisujući njenu boju i šaru. Britanski oftalmolog Džejms Dogart (*James Doggart*) 1949. godine u svom radu [16] razmatra kompleksnost šare dužice i predlaže da bi ona mogla da ima istu ulogu kao i otisci prstiju, u pogledu jedinstvenosti i trajnosti. Na osnovu istraživanja Dogarta, 1987. godine američki oftalmolozi Lenord Flom (*Leonard Flom*) i Eron Safir (*Aran Safir*) patentirali su ovaj koncept, a na osnovu njihovog koncepta Džon Dougman (*John Daugman*) napravio je i patentirao prvi algoritam za prepoznavanje dužice oka [17]. Dougmanov algoritam nije jedini, ali je najprihvaćeniji i predstavlja polaznu osnovu drugih inovativnih biometrijskih sistema, npr. [18] i [19].

[3] Ovaj podatak se odnosi na SAD i Kanadu, gde se primenjuje Dobertov (*Daubert*) standard o prihvatljivosti dokaza, koji se zasniva na empirijski dokazivom modelu [20].

Biometrijski sistem za autentifikaciju zasnovan na dužici oka može se podeliti u sledeće celine, u skladu sa slikom 10:

- akvizicija (snimanje dužice),
- segmentacija,
- normalizacija,
- kodiranje
- skladištenje ili poređenje.



Slika 10 – Blok dijagram sistema za prepoznavanje dužice oka

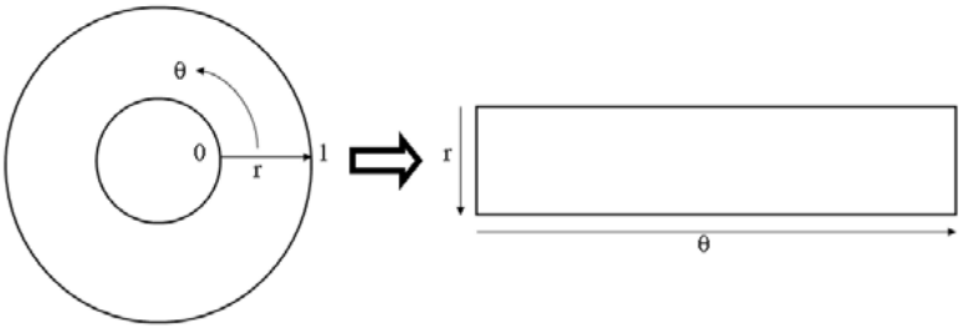
Snimanje oka je prva faza ovog sistema, a cilj je dobijanje 2D slike visoke rezolucije oka. S obzirom na relativno malu veličinu dužice i osetljivost oka na nadražaje, kao što je na primer neophodno osvetljenje, realizacija ove faze je kompleksna. Za kvalitetnu sliku potrebno je kvalitetno osvetljenje, ali takvo da ono ne smeta korisniku. Zato se koristi opseg bliskog infracrvenog zračenja (700nm – 900nm) nevidljivog za ljudsko oko i odgovarajući senzor (CCD) koji radi u istom opsegu. Takođe, ovaj deo spektra se pokazao veoma dobar za tamne dužice oka, kod kojih je teško dobiti jasnu strukturu šare vidljivim spektrom svetlosti, dok se usled bolje penetracije kroz slojeve dužice infracrvenim spektrom dobija jasnija i bogata šara dužice [20]. Upotreba vidljive svetlosti prilikom snimanja izaziva širenje zenice i na taj način dodatno otežava ovaj postupak. Ovaj efekat kontrakcije zenice se koristi samo kao sredstvo zaštite, kako bi se proverila reakcija oka i potvrdilo da se ispred senzora zaista nalazi oko, a ne npr. fotografija. Kompletan postupak zahteva kooperativnost korisnika u smislu pozicioniranja oka, mirovanja i sl. Sistemi često prave više uzastopnih snimaka, a zatim procenjuju njihov kvalitet i biraju najbolji uzorak.

U fazi segmentacije se iz slike izdvaja dužica oka a uklanjaju se ostali nepoželjni elementi oka: beonjača, zenica, kapci i trepavice. Uglavnom, segmentacija se postiže određivanjem unutrašnjih i spoljašnjih granica dužice, kao i konture kapaka i trepavica koji zaklanjaju dužicu. Ova faza je ključna u ovom biometrijskom sistemu, zato što svaka nepreciznost pri segmentaciji dužice u velikoj meri utiče na tačnost komparacije dva šablona dužice. Postoji nekoliko algoritama u upotrebi za segmentaciju, kao što su: kružna Hafova transformacija, Geodezijske aktivne konture [20] i najpoznatiji Dougmanov integralno-diferencijalni operator [17] koji je dat u sledećoj formulaciji:

$$\max_{(r,x,y)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2r\pi} ds \right| . \qquad (5)$$

$I(x,y)$ je intenzitet piksela na lokaciji (x,y) slike oka I, koji konvoluira sa radijalnim Gausovim filterom $G_\sigma(r)$ razmere σ i poluprečnika r. Kontura kruga s je definisana sa (r,x_0,y_0). Operator određuje u slici maksimum u parcijalnom izvodu po rastućem poluprečniku, konturnog integrala. Dakle, operator je kružni detektor ivice sa finoćom koja se podešava Gausovom funkcijom. Ovim postupkom se prvo određuje granična kontura između dužice i zenice. Slična procedura se koristi i za određivanje spoljne granice zenice i kapaka, s tim što se za kapke kružna putanja konture menja na lučnu [17].

Normalizacija sledi nakon što se uspešno izdvoji region dužice i ima za cilj transformaciju tog regiona u region fiksnih dimenzija, nezavisnih od veličine, pozicije i orijentacije dužice u nekom konkretnom uzorkovanju. Na taj način se postiže da dva različita snimka iste dužice, rezultuju istim karakteristikama. Za normalizaciju najčešće se koristi Dougmanov model gumene trake, koji je dobio ime po svom principu rada. Ovim modelom radi se konverzija teksture dužice iz kartezijanskog koordinatnog sistema u pseudo-polarni koordinatni sistem. Princip konverzije je prikazan na slici 11.



Slika 11 – Princip konverzije dužice Dougmanovim modelom (preuzeto iz [20])

Model transformiše radijalne nizove dužice u odgovarajuće redove u pravougaoniku, odnosno dodeljuje svakoj tački segmentirane dužice par realnih koordinata (r,θ), gde je r predstavljeno jediničnim intervalom $[0,1]$, a ugao θ intervalom $[0,2\pi]$. Transformacija se može predstaviti sledećom jednačinom:

$$I(x(r,\theta),y(r,\theta)) \rightarrow I(r,\theta) \tag{6}$$

gde je $I(x,y)$ oblast dužice u kartezijanskom koordinatnom sistemu, a $I(r,\theta)$ u normalizovanom polarnom sistemu. Takođe, $x(r,\theta)$ i $y(r,\theta)$ definišemo kao linearnu kombinaciju unutrašnjih graničnih tačaka dužice $(x_u(\theta),y_u(\theta))$ i spoljašnjih graničnih tačaka dužice $(x_s(\theta),y_s(\theta))$, pa je:

$$x(r,\theta) = (1-r)x_u(\theta) + rx_s(\theta) \tag{7}$$

$$y(r,\theta) = (1-r)y_u(\theta) + ry_s(\theta) \tag{8}$$

Kôd dužice se dobija primenom dvodimenzionalnih Gaborovih vejvleta. Ovim procesom se struktura dužice predstavlja kao niz fazora, čiji fazni uglovi određuju vrednosti bita koda dužice. Funkcija Gabor filtera je kompleksna i sastoji se od realne i imaginarne komponente:

$$G(x,y) = e^{-\pi\left[\frac{(x-x_0)^2}{\alpha^2}+\frac{(y-y_0)^2}{\beta^2}\right]} e^{-2\pi i\left[u_0(x-x_0)+v_0(y-y_0)\right]}, \tag{9}$$

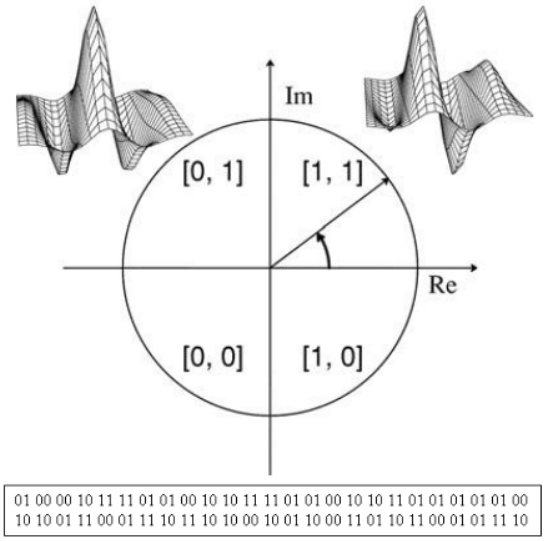
i te dve komponente možemo razdvojiti u dve jednačine:

$$\Re\{G(x,y)\} = e^{-\pi\left[\frac{(x-x_0)^2}{\alpha^2}+\frac{(y-y_0)^2}{\beta^2}\right]} \cos(-2\pi\left[u_0(x-x_0)+v_0(y-y_0)\right]) \text{ i} \tag{10}$$

$$\Im\{G(x,y)\} = e^{-\pi\left[\frac{(x-x_0)^2}{\alpha^2}+\frac{(y-y_0)^2}{\beta^2}\right]} \sin(-2\pi\left[u_0(x-x_0)+v_0(y-y_0)\right]), \tag{11}$$

gde (x_0,y_0) označavaju poziciju slike, (α,β) efektivnu visinu i širinu, a (u_0,v_0) određuju pravac talasa prostorne frekvencije $\omega_o = \sqrt{u_0^2+v_0^2}$.

Fazni uglovi su kvantizovani na jedan od četiri kvadranta, od kojih svaki nosi dva bita informacije o bazi. Princip je prikazan na slici 12.



Slika 12 – Dobijanje koda dužice faznom demodulacijom (preuzeto iz [17])

S obzirom na to da je dužica normalizovana u prethodnom koraku, ovaj proces se odvija u dvostruko bezdimenzionom polarnom koordinatnom sistemu koji je invarijantan na veličinu irisa, samim tim invarijantan na udaljenost oka od skenera i faktora uvećanja optičkog sistema, što istovremeno znači da je invarijantan na dilataciju zenice unutar dužice [17]. Kako se koristi samo fazna informacija teksture dužice, a amplitudna je zanemarena, ovaj metod je nezavistan od kontrasta i osvetljaja slike. Primenom 2D Gaborovog vejvleta, svaka pojedinačna šara dužice se demodulira i izdvaja se njena fazna informacija. Projekcijom diskretne oblasti na kompleksne 2D Gaborove vejvlete utvrđuje se u kom kvadrantu kompleksne ravni se nalazi svaki rezultanti fazor. Demodulacija i fazna kvantizacija se može matematički predstaviti:

$$h_{\{\mathrm{Re,Im}\}} = \operatorname{sgn}_{\{\mathrm{Re,Im}\}} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi , \qquad (12)$$

$$h_{\{\mathrm{Re}\}} = \begin{cases} 1 & \Re\left\{\int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi\right\} \geq 0 \\ 0 & \Re\left\{\int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi\right\} < 0 \end{cases}, \qquad (13)$$

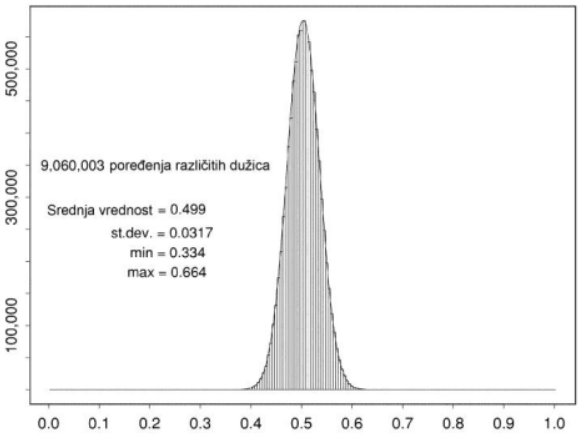
$$h_{\{\mathrm{Im}\}} = \begin{cases} 1 & \Im\left\{\int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi\right\} \geq 0 \\ 0 & \Im\left\{\int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} \rho d\rho d\phi\right\} < 0 \end{cases}, \qquad (14)$$

gde se $h_{\{\mathrm{Re,Im}\}}$ posmatra kao bit kompleksne vrednosti čija realna i imaginarna vrednost može biti 0 ili 1 u zavisnosti od znaka integrala, $I(\rho,\phi)$ je normalizovana slika dužice u bezdimenzionalnom polarnom koordinatnom sistemu, ω je frekvencija vejvleta, α i β njegovi parametri, a (ρ_o,ϕ_o) su polarne koordinate svakog regiona dužice za koji se računaju koordinate fazora $h_{\{\mathrm{Re,Im}\}}$. Rezultat faze kodiranja je kôd dužine 2048 bita, od svake dužice oka.

Poređenje dve dužice se zasniva na testu statističke nezavisnosti. Ovaj test ima toliko mnogo stepeni slobode da će garantovano proći kada se porede fazni kodovi dve različite dužice, odnosno da neće proći kada se fazni kodovi dužice porede sa bilo kojim uzorkom iste dužice [17]. Test se implementira pomoću ekskluzivnog ILI (XOR) operatora Bulove algebre nad bitovima faznih vektora dve dužice koje se porede. Kako bi se iz poređenja isključili regioni u kojima se nalaze trepavice, kapci ili neke druge smetnje, primenjuju se odgovarajuće maske obe dužice sa I operatorom.

$$HD = \frac{\left\|(codeA \oplus codeB) \cap maskA \cap maskB\right\|}{\left\|maskA \cap maskB\right\|} \qquad (15)$$

Hemingovo rastojanje (engl. *Hamming Distance* - HD) se često primenjuje u obradi signala za procenu greške nastale prilikom prenosa signala, dok se u biometriji dužice oka koristi za utvrđivanje poklapanja dva biometrijska binarna koda. Domen vrednosti rezultujućeg Hemingovog rastojanja nalazi u opsegu od nule do jedan, gde nula predstavlja idealno poklapanje dva koda, dok u slučaju kodova različitih dužica očekivana vrednost poređenja iznosi *0,5*, s obzirom na to da je podjednaka verovatnoća da je neki bit koda svake dužice *0* ili *1*. Histogram na slici 13. prikazuje raspodelu HD poređenja više od devet miliona različitih dužica oka prikazanih u [17]. Na osnovu prezentovanih podataka, predložena je granična vrednost Hemingovog rastojanja od 0,26, gde se za svaki rezultat poređenja manji od granične vrednosti smatra da pripada istoj dužici, u suprotnom različitim dužicama oka. Verovatnoća greške, u zavisnosti od različitih vrednosti HD uzete za graničnu vrednost prilikom poređenja dužica, data je u tabeli 2.



Slika 13 – Raspodela HD poređenja više od devet miliona različitih dužica oka (prilagođeno iz [17])

Tabela 2 – Verovatnoća greške u zavisnosti od različitih vrednosti HD (prilagođeno iz [17])

HD	Verovatnoća greške
0,26	$1 : 10^{13}$
0,27	$1 : 10^{12}$
0,28	$1 : 84 \cdot 10^{9}$
0,29	$1 : 8{,}6 \cdot 10^{9}$
0,30	$1 : 10^{9}$
0,31	$1 : 127 \cdot 10^{6}$
0,32	$1 : 18 \cdot 10^{6}$
0,33	$1 : 2{,}9 \cdot 10^{6}$
0,34	$1 : 527 \cdot 10^{3}$
0,35	$1 : 105 \cdot 10^{3}$

Korišćenje dužice oka u svrhe autentifikacije i autorizacije je oblast koja privlači pažnju istraživačima. Iako sistemi postoje već neko vreme i uspešno se primenjuju, usavršavanje i unapređenje su predmet trenutnih istraživanja. Trenutni pravci istraživanja usmereni su na dobijanje koda dužice od ljudi u pokretu iz daljine.

2.3.3. Karakteristike lica

Može se reći da su karakteristike lica najčešće korišćena biometrija kod ljudi, imajući u vidu da ljudi svakog dana međusobno prepoznaju na osnovu nje. Zbog toga je uobičajeno da sve značajne legitimacije sadrže fotografiju lica (npr. lična karta, pasoš, vozačka dozvola itd.). Zbog toga što lice sadrži dodatne informacije, kao što su: pol, starost, etnička pripadnost i trenutno emocionalno stanje, ova biometrijska karakteristika je od velikog značaja bezbednosnim službama. Prepoznavanje lica može se definisati kao proces utvrđivanja identiteta neke osobe, na osnovu njenih specifičnih obeležja lica.

Međutim, automatizovan mašinski postupak poređenja slika lica suočen je sa brojnim varijabilnostima nastalih usled varijacije poze, starosti, osvetljenja i izraza lica, kao i promene izgleda usled promene frizure, šminkanja, nošenja naočara i sl. Dodatni problem predstavljaju genetske sličnosti (blizanci, braća, roditelj – dete itd.). Međutim, ova biometrijska karakteristika ima određene prednosti nad drugim, što je čini veoma poželjnom za primenu u nekim sistemima. Za sliku lica se koriste beskontaktni senzori, nije neophodna mala udaljenost od objekta slikanja, što kao posledicu ima da nije potrebna velika kooperativnost kao kod nekih drugih karakteristika. Zbog dozvoljene udaljenosti i sve boljih karakteristika senzora i sočiva, ova biometrijska karakteristika je našla veliku primenu u sistemima video nadzora. Veoma značajnu prednost u odnosu na druge biometrijske karakteristike, u pogledu društvene prihvatljivosti i privatnosti, predstavlja činjenica da su ljudi naviknuti na primenu ove biometrije i uglavnom nisu rezervisani u pogledu prikupljanja, obrade i skladištenja slika lica.

Lice čoveka se može podeliti na njegove elemente: čelo, obrve, oči, nos, usta, obrazi i brada. Antropometrijom se određuju mere lica na osnovu niza anatomski značajnih obeležja. Ova obeležja se koriste u forenzici, ali ne i u sistemima za automatsko prepoznavanje lica zbog njihove teže detekcije. Karakteristična obeležja lica možemo hijerarhijski predstaviti sa tri nivoa:

- I nivo – lako uočljiva obeležja (pol, boja kože, etnička pripadnost, geometrija glave i dr.),
- II nivo – geometrijska obeležja (struktura i odnos između elemenata lica, precizna geometrija glave i sl.) i
- III nivo – mikroobeležja, kao što su ožiljci, mladeži i sl.

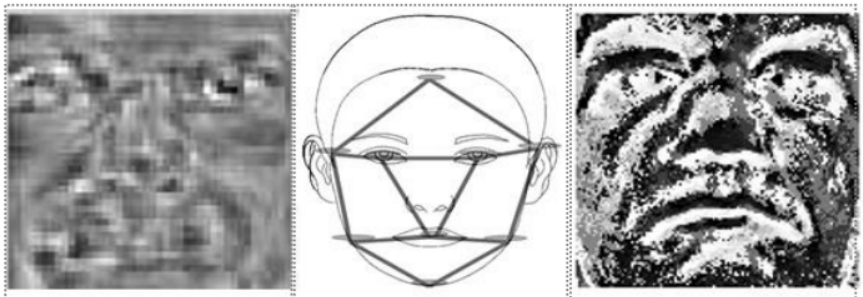
Različiti principi rada sistema baziranih na karakteristikama lica, zahtevaju različite senzore za prikupljanje slika i možemo ih podeliti prema korišćenom spektru (vidljivi, infracrveni - NIR i termalni - MIR)[4] i prema tehnici renderovanja (2D, 3D i video snimak). Većina konvencionalnih sistema za automatsko prepoznavanje lica koristi 2D slike prikupljene vidljivim svetlom [20]. Međutim, kao i kod senzora za dužicu oka, kvalitet dobijene slike je podložna velikim varijacijama usled lošeg osvetljenja i rezolucije. Rezolucija slike se u ovim sistemima iskazuje jedinicom *ipd* (engl. *Inter-Pupilary Distance*). Za izdvajanje detalja prvog nivoa dovoljna je slika rezolucije 30 idp, dok je za drugi nivo detalja potrebna slika rezolucije 75 idp. Da bi se prevazišli pomenuti problemi, koriste se PTZ (engl. *Pan Tilt Zoom*) kamere sa senzorima visoke rezolucije, u kombinaciji sa infracrvenim spektrom osvetljenja. U dinamičnom okruženju, koriste se i kombinacije statičkih i pokretnih kamera, gde statička kamera detektuje lice od interesa, koje se zatim

[4] Vidljivi deo spektra obuhvata talasne dužine od 0,4μm do 0,7μm, deo bliskog infracrvenog spektra koji se koristi obuhvata talasne dužine od 0,7μm do 0,9μm, a termalni spektar je deo srednjeg infracrvenog spektra i obuhvata talasne dužine od 8μm do 14μm.

zumira i slika PTZ kamerom. U početku je fokus pri razvijanju algoritama za detekciju lica bio tradicionalno usmeren na otkrivanje frontalnog ljudskog lica, dok noviji algoritmi pokušavaju da reše težak problem detekcije lica snimljenih iz različitih uglova. Pionirski algoritam Viola-Džons (*Viola-Jones*) [21], zasnovan je na primeni binarnog šablona klasifikacija. Sadržaj dela slike se pretvara u obeležja prvog nivoa, nakon čega algoritam, na osnovu uskladištenih obeležja, odlučuje da li je taj region slika lica ili ne. Koristi se tehnika „kliznih prozora" različitih veličina, koji obuhvataju deo površine slike i za svaki prozor se određuje da li se u njemu nalazi lice ili ne. U svakom prozoru o postojanju lica se odlučuje primenom klasifikatora na pronađena obeležja pomoću pravougaonih filtera. Ovi 2D filtri mogu se grupisati u dva, tri ili četiri pravougaonika i slični su jednodimenzionalnim Hârovim vejvlet (engl. *Haar wavelet*) filtrima koji se koriste u domenu obrade signala. Vrednosti obeležja dobijaju se izračunavanjem razlike između zbira intenziteta piksela u svetlim i tamnim pravougaonim regionima. Na primer, filtar sastavljen od tri pravougaonika može da se koristi za otkrivanje dva oka i nosa, na osnovu toga što oči obično imaju veliki intenzitet tamnih vrednosti u odnosu na nos između. Korišćenje regiona i obeležja, umesto vrednosti piksela, omogućava bržu detekciju lica i poboljšava otpornost sistema na promene u osvetljenju i perspektivi.

Tehnike izdvajanja i poređenja obeležja segmentiranih regija lica mogu se podeliti na osnovu klase primenjenih algoritama i to baziranih na: izgledu, modelu i teksturi [20] (slika 14). **Tehnike bazirane na izgledu** rade kompaktnu reprezentaciju čitavog regiona lica mapiranjem slike u potprostor, koji je definisan skupom reprezentativnih baznih vektora. Način mapiranja može biti linearan ili nelinearan, dok najčešće korišćeni algoritmi poput: analize glavnih komponenti (engl. *Principal Component Analysis* - PCA) [22], linearne diskriminantne analize (engl. *Linear Discriminant Analysis* - LDA) [23] i analize nezavisnih komponenti (engl. *Independent Component Analysis* - ICA) [24] koriste linearne projekcije. Projekcioni koeficijenti se koriste za predstavljanje slike lica. Šeme na bazi izgleda su zasnovane na predstavljanju slike lica kao funkcije drugih slika lica dostupnih u obučavajućem skupu slika ili kao funkciju samo nekoliko baznih lica. Na primer, vrednost piksela na lokaciji *(x,y)* na slici lica može biti izražen kao težinska suma vrednost piksela svih slika iz obučavajućeg skupa slika na lokaciji *(x,y)*. Skup obučavajućih ili baznih slika formira potprostor i kad se data slika lica linearno projektuje na ovaj potprostor, ona se referencira kao linearna potprostorna analiza. Izazov je da se pronađe odgovarajući potprostor u kojem će se sačuvati diskriminatorne informacije koje su sadržane u slici lica. Drugim rečima, cilj je da se pronađe mali skup najreprezentativnijih baznih lica. Svaka nova slika lica može biti predstavljena kao težinska suma baznih lica i dve slike lica se mogu upariti direktnim poređenjem njihovog vektora. **Tehnike na bazi modela** prave 2D ili 3D modele lica koje olakšavaju poređenje slika lica u prisustvu različitih poza. Grupa grafova lica (engl. *Face Bunch Graphs* - FBG) [25] i Aktivni model pojavljivanja (engl. *Active Appearance Model* - AAM) [26] su primeri 2D modela lica, a Morfološki model (engl. *Morphable Model* - MM) [27] je 3D

model. Ove tehnike postižu reprezentaciju nezavisnu od poze lica na slici i mogu omogućiti upoređivanje slika lica različitih poza. Ove šeme obično zahtevaju otkrivanje nekoliko karakterističnih tačaka na licu, kao što su npr. uglovi očiju, vrh nosa, uglovi usana i brada, što dovodi do povećanja složenosti u odnosu na tehnike bazirane na izgledu. Neke od ovih tehnika mogu da se koriste za prepoznavanje lica, kao i za generisanje animacije realnog lica. **Tehnike bazirane na teksturi** pokušavaju da pronađu robusna lokalna obeležja koja su invarijantna na pozu i osvetljenje. Tehnike bazirane na izgledu obično koriste izvorne vrednosti intenziteta piksela, koji su prilično osetljivi na promene u osvetljenju i izrazu lica. Alternativa je da se koriste složenije reprezentacije obeležja koje definišu teksturu slike pomoću raspodele vrednosti lokalnih piksela. Primeri ovih tehnika su: SIFT (engl. *Scale Invariant Feature Transform*) [28] i LBP (engl. *Local Binary Patterns*) [29].



a) Tehnika bazirana na izgledu – PCA (Eigen vrednost)

b) Tehnika bazirana na modelu – FBG

c) Tehnika bazirana na teksturi – LBP

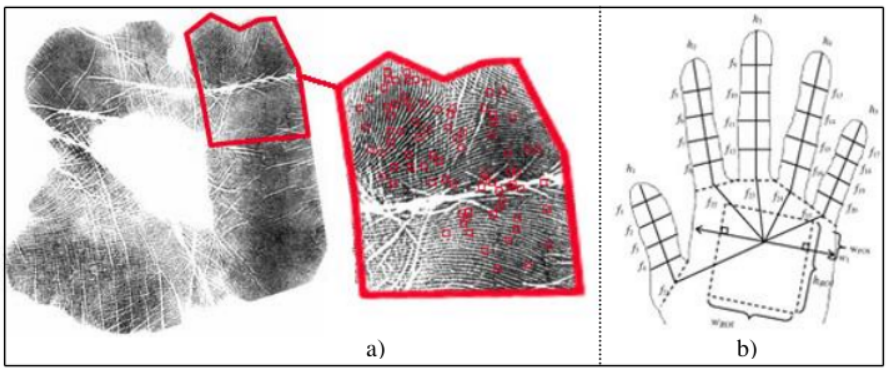
Slika 14 – Pristup izdvajanja obeležja kod različitih tehnika (prilagođeno iz [20])

Tehnologije za prepoznavanje karakteristika lica su u stalnom napretku, ali je još uvek izražen problem poze lica, uticaja različitog osvetljenja i izraza lica prilikom upoređivanja. Tehnološki napredak u sistemima video nadzora uslovili su razvoj 3D sistema za prepoznavanje karakteristika lica, koji mogu da rade sa video sekvencama u realnom vremenu, a uticaj osvetljenja i poze lica je mnogo manji na ove sisteme. Uvođenjem dubokih konvolucionih neuronskih mreža u tehnike prepoznavanja lica, koju karakteriše hijerarhijska arhitektura za spajanje piksela u nepromenljivu sliku lica, značajno su poboljšane performanse najsavremenijih sistema, što je rezultiralo primenom ovih metoda u realnim aplikacijama [30][31]. Usled lakoće akvizicije i dostupnosti kamere na većini modernih prenosnih uređaja, ova biometrijska karakteristika se sama nametnula da zameni ili unapredi postojeće sisteme za autentifikaciju, pre svega onih baziranih na korisničkom imenu i lozinci. Sigurnost postojećih protokola za autentifikaciju, kao što je na primer *WebID*, unapređuju se dodavanjem biometrijskih karakteristika [30][32].

2.3.4. Pregled ostalih značajnijih biometrijskih karakteristika

Otisak dlana je sličan otisku prsta, koji se već decenijama koristi za autentifikaciju ljudi. Površina dlana je mnogo veća od jednog otiska i zbog toga se od dlanova očekuje da sadrže više različitosti od otisaka. Upravo zbog veće površine, senzori za dlanove su mnogo robusniji i skuplji od onih za otiske prstiju, što je jedan od razloga zašto se oni ređe koriste za autentifikaciju. Tekstura dlanova se, takođe, sastoji od ispupčenja i udubljenja kože, odnosno minucija i singularnih regiona, kao što se može videti na slici 15 a). Broj specifičnih obeležja koji se nalaze na jednom dlanu je deset puta veći od detalja koji se nalaze na jednom kompletnom otisku prsta. Obeležja se mogu podeliti u ista tri nivoa kao kod otisaka prstiju, a tehnike njihovog izdvajanja i poređenja zasnovane su na istim principima [33].

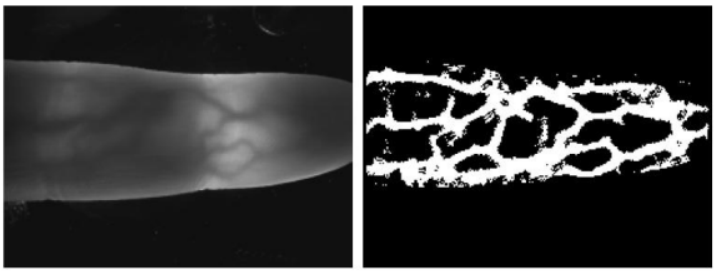
Geometrija šake pripada grupi biometrijskih fizičkih karakteristika gde se primenjuju geometrijske osobine ruku. Zasniva se na velikom broju merenja karakteristika šake, kao što su dužina i širina prstiju i dlana, što je ilustrovano na slici 15 b). Prednosti ove karakteristike su njena jednostavnost i neosetljivost na oštećenja ili promene na koži, kojima su podložne karakteristike otisaka prstiju i dlanova. Međutim, geometrija šake ima dosta slabosti: promenljivost u vremenu (period rasta i starenja), smetnje usled nošenja nakita i nedovoljne osobine jedinstvenosti, koju ova karakteristika ne zadovoljava pri upotrebi na velikoj populaciji. Zbog toga ona najčešće ima komercijalnu primenu za verifikaciju identiteta pri malom broju korisnika ili se koristi u multimodalnim biometrijskim sistemima, najčešće kombinujući istovremeno karakteristiku vaskularnih obrazaca šake ili otisak dlana. Njena primena na maloj populaciji može dati odlične rezultate u pogledu tačnosti, čak su razvijene tehnike koje ne zahtevaju primenu namenske opreme [34].



Slika 15 – Otisak dlana i geometrija šake

Biometrija vaskularnih obrazaca oslanja se na strukturu krvnih sudova, koja zbog slučajne morfogeneze predstavlja nasumičnu mrežu u telu čoveka, što je ilustrovano na

slici 16. Vaskularni obrasci su jedinstveni za svaku osobu, nepromenljivi su tokom života izuzev u slučaju nekih bolesti ili povreda. Upravo na činjenicu da se krvni sudovi nalaze unutar tela, oslanja se i sigurnost ove karakteristike, jer bi za njihovo dupliranje bila potrebna veoma precizna operacija sa neizvesnim ishodom. Najčešće se koriste vaskularni obrasci prsta i dlana. Pri izloženosti vidljivom spektru svetlosti može se videti raspored vena, dok se korišćenjem infracrvenog spektra vidljivost povećava, na principu sličnom onom koji se koristi kod dužice oka. Velika prednost ove biometrije je da se ona u poslednje vreme primenjuje beskontaktno, što kao rezultat ima veću prihvatljivost od strane korisnika. Pored toga, ova biometrijska karakteristika ima veoma nisku vrednost EER od 0,0009% do 0,1% u zavisnosti od primenjenog algoritma [35]. U Japanu se biometrijska karakteristika vaskularnih obrazaca odavno uspešno koristi u bankarskom sektoru za verifikaciju identiteta prilikom podizanja novca na bankomatima, što je zakonski regulisano. Zbog velikog uspeha, ovu tehniku su kasnije primenile centralne banke Poljske, Turske i Brazila [36].



Slika 16 – Vaskularni obrasci prsta (preuzeto iz [35])

Termografija lica predstavlja svojevrsnu sintezu biometrija vaskularnih obrazaca i karakteristika lica. Različiti objekti emituju različite vrste infracrvene energije, shodno njihovoj temperaturi i osobinama. Spektralna raspodela energije koju emituje neki objekat, određuje se pomoću Plankove raspodele za datu temperaturu. Opseg temperature ljudskog lica i tela je dosta ujednačen i varira od 35,5°C do 37,5°C, obezbeđujući dosledan termalni potpis. Plankova raspodela za tu temperaturu postiže maksimum na talasnoj dužini od oko 9μm, pa se za termografiju koristi opseg dugotalasnog infracrvenog spektra. Termalni šabloni lica izvedeni su prvenstveno iz šablona površinskih krvnih sudova ispod kože. Vene i struktura tkiva lica su jedinstvene za svaku osobu, pa iz toga sledi da su i njihove termalne slike jedinstvene [37][38]. Infracrvena termografija, odnosno termalno snimanje ima značajnu ulogu u vojnoj i civilnoj primeni. Primeri vojne primene su otkrivanje objekata u mraku i njihovo praćenje, navođenje meta na projektilima itd. Pored primene u biometriji, u civilne svrhe se koristi za proučavanje stepena termičkog iskorišćenja objekata, daljinsko merenje temperature itd. Termografija lica nije osetljiva na osvetljenje, različita je kod jednojajčanih blizanaca i sigurnija je u odnosu na klasičnu biometriju crta lica.

Mrežnjača oka poseduje unikatnu mrežu krvnih žila i zahvaljujući njihovoj slučajnoj genezi može se upotrebiti za biometrijsku autentifikaciju. Veruje se da je struktura jedinstvena za svakog čoveka, a isto važi za svako oko ponaosob. Za mrežnjaču se tvrdi da je najsigurnija biometrijska karakteristika, s obzirom na trenutno uverenje da je nemoguće menjati ili kopirati pomenutu strukturu. Dobijanje odgovarajuće slike strukture krvnih žila mrežnjače zahteva veliku kooperativnost korisnika, fizički kontakt sa okularom, postupanje po uputstvima, pa se ova karakteristika ujedno smatra najneprijatnijom, što je razlog njene neprihvatljivosti kod ljudi i izuzetno retke primene u praksi. Dodatni razlog je i povreda privatnosti, jer se neke bolesti mogu uočiti prilikom analiziranja mrežnjače. Zbog svega navedenog, primena ove karakteristike uglavnom je ograničena samo na kontrolu pristupa najvišeg nivoa.

DNK je skraćenica od dezoksiribonukleinske kiseline, koja je nosilac genetskih informacija neophodnih za razvoj i funkcionisanje živih bića. Te informacije se predstavljaju jednodimenzionim kodom, jedinstvenim za svaki živi organizam, izuzev kod jednojajčanih blizanaca. Njena primena je ograničena na polje forenzike, gde trenutno predstavlja glavnu biometrijsku karakteristiku. Pored identifikacije i verifikacije osumnjičenih ili žrtava, njena svojstva omogućavaju otkrivanje krvnog srodstva među subjektima. Međutim, njena primena za komercijalne ili lične potrebe autorizacije je izuzetno retka. DNK uzorak je lako ukrasti, pa samim tim i zloupotrebiti. Zatim, tu je pitanje privatnosti, s obzirom na to da genetske informacije otkrivaju privatne podatke o nekoj osobi, kao što su npr. potencijalne bolesti, slabosti i sl. Takođe, proces dobijanja DNK koda zahteva komplikovane hemijske procese, za koje je potrebna vrhunska oprema i sudelovanje eksperata. Osim visoke cene takve opreme, proces nije moguće izvesti u realnom vremenu.

Telesni miris se formira spojem više različitih izlučevina i zahvaljujući njihovim različitim kombinacijama i intenzitetima, u velikoj meri poseduje odlike jedinstvenosti za svaku osobu. Do sada je izdvojeno oko 300 specifičnih mirisnih sastojaka koje oslobađa ljudsko telo, a da ih je moguće detektovati i diferencirati. Psi imaju veoma razvijen njuh koji se već decenijama koristi kao izvesna metoda identifikacije u kriminalistici. Kad je reč o egzaktnijim metodama, danas se pomoću masene spektometrije može odrediti oko 130 specifičnih sastojaka telesnog mirisa. Većina mirisa se luči sa površine tela, odnosno kože i potkožnog tkiva, ali znatan deo potiče iz pluća i gastrointestinalnog trakta. Složenost takvog traga doprinosi njegovoj individualnosti. Prema dosadašnjim istraživanjima nepobitno je utvrđena individualnost i nepromenljivost temeljnih karakteristika mirisa čoveka. Smetnje se javljaju prilikom upotrebe različitih hemijskih sredstava za ličnu higijenu i promenljive hemijske kompozicije mirisa u okruženju. Ova biometrijska fizička karakteristika koristi se u forenzičke svrhe, dok je njena primena za potrebe autentifikacije predmet istraživanja.

Biometrija govora kombinuje fizičke osobine i karakterističnosti ponašanja. Prepoznavanje govora koristi se za autentifikaciju korisnika na osnovu njihovih jedinstvenih glasovnih obeležja. Govor pojedinca zavisi od fizičkih osobina koje se koriste u sintezi zvuka, kao što su: vokalni trakt, nosne šupljine, usta, usne itd. Ove fizičke osobine ljudskog govora su u velikoj meri invarijante za odraslog pojedinca, dok se aspekti govora vremenom menjaju usled starosti, zdravstvenog stanja, emotivnog stanja itd. Postoje dve različite tehnike ove karakteristike: zavisne i nezavisne od teksta. Da bi se izvršila autentifikacija, kod tehnika zavisnih od teksta korisnik mora ponoviti neki tekst koji je prethodno izgovorio prilikom faze upisa i koji je sačuvan u bazi podataka kao šablon. Tu se javlja jedinstvenost s obzirom na to da različiti ljudi uglavnom drugačije izgovaraju iste rečenice u pogledu tonaliteta, brzine, prekida i sl. Tehnike koje su nezavisne od teksta se zasnivaju samo na izdvajanju vokalnih karakteristika korisnika i zahtevaju duže govorne sekvence za upis i poređenje šablona. Biometrija govora nije dovoljno diskriminativna i može se primenjivati samo u autentifikacionim sistemima koji obuhvataju malu populaciju. Ipak, lakoća akvizicije, bez dodatnog hardvera, zaslužna je za to da se ova biometrija primenjuje za verifikaciju identiteta na personalnim uređajima, u slučajevima kada je populacija nad kojom se primenjuje malobrojna, kao i u fuziji sa drugim biometrijskim karakteristikama.

Biometrija potpisivanja pripada kategoriji karakterističnosti ponašanja, gde se analiziranjem dinamike potpisivanja izdvajaju i kvantifikuju obeležja, kao što su: brzina, pritisak i ugao pisanja. Različiti potpisi se međusobno značajno razlikuju. Čak ni, vizuelno posmatrano, uspešno falsifikovanje nečijeg potpisa, neće rezultovati uspešnom autentifikacijom zbog različitih osobina načina potpisivanja. Ipak, veruje se da profesionalni falsifikatori mogu savladati i imitirati celokupan način nečijeg potpisivanja, pa se ova karakteristika ne smatra sigurnom. Iako je potrebna velika kooperativnost, ova biometrijska karakteristika je veoma prihvatljiva za korisnike, imajući u vidu da se potpis tradicionalno već dugo koristi za svakodnevne potrebe. S obzirom na to da je u pitanju karakteristika ponašanja, ona se menja vremenom i zavisna je od fizičkog i emocionalnog stanja korisnika.

Dinamika kucanja na tastaturi predstavlja biometriju zasnovanu na hipotezi da se specifičnost načina kucanja na tastaturi može kvantifikovati pomoću: brzine, prekida, vremenskog razmaka između određenih slova i sl., formirajući tako obeležja ove karakteristike ponašanja. Kao u slučaju potpisivanja, dinamika kucanja se menja vremenom, a fizičko i emocionalno stanje korisnika utiče na dinamiku koja se izdvaja. Ova biometrija ima velike margine greške, kako bi obuhvatila veliku varijabilnost obeležja. Usled toga, ne smatra se mnogo pouzdanom. Ipak, u dužem periodu analize može se obezbediti dovoljno diskriminatornih informacija za verifikaciju nečijeg identiteta u primeni nad malom populacijom, zatim kao dodatna kontrola uz neke druge biometrijske tehnike autentifikacije ili za sigurnosne provere. Na primer, kada se korisnik uspešno

autentifikuje pomoću drugih sistema, njegov rad za računarom se može konstantno koristiti za verifikaciju prethodno utvrđenog identiteta. Na sličnom principu, kao kod potpisa ili kucanja na tastaturi, zasniva se još biometrijskih karakteristika ponašanja (npr. način hoda), koje dele iste prednosti i mane s obzirom na prirodu ljudskog ponašanja.

2.4. Multibiometrija

Autentifikacioni sistemi zasnovani na biometriji nisu još uvek ispunili maksimalna očekivanja, ali su postali nezamenljivi, pre svega na polju forenzike i u državnim projektima za identifikaciju stanovništva, kontrole granica i sl., ali i u svakodnevnim potrebama za autentifikacijom na pametnim uređajima, za mobilno bankarstvo, na bankomatima, za kontrolu pristupa itd. Primenom unimodalnih biometrijskih sistema za autentifikaciju primetni su potencijalni problemi koji se mogu javiti. Oštećenjem implementirane biometrije sistema, kao što je npr. povreda oka, nije moguće izvršiti biometrijsku autentifikaciju. Paralelna upotreba više biometrijskih karakteristika (npr. otisak prsta i dužica oka ili otisci više različitih prstiju), predstavlja efikasan način prevazilaženja ovakvih izazova. Biometrijski sistemi koji istovremeno koriste različite izvore biometrijskih podataka nazivaju se multibiometrijski sistemi. Na taj način moguće je značajno uvećati funkcionalnost, pouzdanost i tačnost, u poređenju sa klasičnim unimodalnim biometrijskim sistemima. Upotreba višestrukih biometrijskih izvora direktno utiče na povećanje faktora univerzalnosti, što je od velikog značaja u slučajevima primene nad velikom populacijom, kao što je to slučaj u nacionalnim projektima koji uključuju biometriju, kao npr. kontrola granica. Osim povećanja tačnosti i univerzalnosti biometrijskog sistema, kao primarnih razloga za upotrebu višestruke biometrije, postoji još korisnih efekata, kao što je npr. povećanje otpornosti na obmane korišćenjem falsifikovanih biometrija. Otpornost se povećava na osnovu činjenice da je mnogo teže obezbediti više lažnih biometrijskih karakteristika. Takođe, prilikom postupka identifikacije radi se pretraga velikih baza biometrijskih podataka. Ukoliko se koristi više različitih biometrija, tada se pretraga može raditi na osnovu one biometrijske karakteristike koja je računski najlakša za poređenje, bez obzira na njenu tačnost, jer će se konačna verifikacija identiteta izvršiti poređenjem najpreciznije ili poređenjem svih karakteristika koje su na raspolaganju. Upotreba multibiometrijskih sistema obezbeđuje mnogo prednosti, međutim, ovakvi sistemi su višestruko skuplji zbog dodatnog hardvera i softvera, a od korisnika zahtevaju veću kooperativnost. Multibiometrijske sisteme možemo podeliti na osnovu načina na koji se [4]:

- sprovodi odabir biometrijskih podataka,
- prikupljaju i obrađuju podaci i
- sjedinjavanju biometrijski podaci.

2.4.1. Odabir biometrijskih podataka

Kombinovanjem višestrukih biometrijskih izvora podataka postiže se veća jedinstvenost u odnosu na klasične biometrijske sisteme. Šum ili oštećenja jedne od izabranih biometrija mogu biti kompenzovane ostalim, u zavisnosti od izvedbe sistema. U zavisnosti od odabira biometrijskih podataka, primenjuje se standardizovana klasifikacija[5] multibiometrijskih sistema na one koji primenjuju:

- višestruke senzore (engl. *multi-sensor*) gde se primenom različitih senzora radi akvizicija istih biometrijskih podataka (npr. upotreba kapacitivnih i poluprovodničkih senzora za isti otisak);
- višestruko uzorkovanje (engl. *multi-sample*) iste biometrije u cilju formiranja što kvalitetnije reprezentacije uzorka;
- višestruke izvore podataka iste biometrijske osobine (engl. *multi-instance*), kao na primer akvizicijom geometrije obe šake ili obe dužice;
- višestruke načine obrade biometrijskih podataka (engl. *multi-algorithm*), gde se paralelno koriste različiti algoritmi za analizu podataka;
- multimodalnost (engl. *multimodal*), princip istovremene upotrebe višestrukih različitih biometrijskih osobina, kao npr. otisak prsta i dužica oka.

Više različitih senzora u multibiometrijskim sistemima koriste se kako bi izdvojili različite informacije iz istog izvora, odnosno iste biometrijske karakteristike. Na taj način postiže se veća tačnost poređenja karakteristika i ukupnih performansi sistema. Međutim, u slučajevima invaliditeta ili oštećenja biometrijske karakteristike, ovakav sistem ima iste slabosti, kao i sistem sa jednim senzorom. Takođe, između ovako dobijena dva uzorka iste karakteristike izražena je korelacija, pa se na ovaj način ne postiže mnogo veća jedinstvenost uzorka. Primeri ovakvih sistema su: optički i kapacitivni senzor za otiske prstiju [39], kamere koje rade u vidljivom i termalnom spektru za prepoznavanje lica i sl.

Isti senzor može se upotrebiti za prikupljanje više uzoraka istog biometrijskog izvora podataka, kako bi se dobila što bolja reprezentacija. Različiti uzorci se analiziraju i izdvajaju se sve varijacije, čime se dobija više informacija o istoj prezentovanoj biometriji. Na primer, višestrukim uzorkovanjem jednog istog prsta, može se prikupiti mnogo veći broj minucija, nego što je to slučaj kada se koristi jedan uzorak. Veća jedinstvenost se postiže, ali u mnogo manjoj meri nego kod drugih multibiometrijskih sistema.

[5] Podela prema ISO/IEC JTC1 SC37 – ISO 24722:2007 *„Technical Report on MultiModal and other Biometric Fusion“*

Jednim senzorom ili sa više senzora istovremeno može se prikupiti više različitih uzoraka iste biometrijske karakteristike (npr. otisci svih prstiju ili obe dužice oka). Ukoliko se koristi samo jedan senzor, ovaj metod se može implementirati u postojećim klasičnim biometrijskim sistemima bez dodatnih troškova. S obzirom na to da su dva različita uzorka od iste osobe međusobno nezavisni, odnosno među njima nije izražena korelacija, ovim pristupom se postiže veća jedinstvenost objedinjenog šablona. Većina današnjih nacionalnih baza biometrijskih podataka koriste otiske svih prstiju, što predstavlja upravo ovaj model multibiometrije.

Primenom više različitih algoritama za obradu istih ulaznih biometrijskih podataka, dobijaju se višestruki skupovi izdvojenih obeležja, čime se mogu povećati performanse sistema. Na primer, iz jednog otiska prsta se mogu izvući obeležja u vidu minucija primenom jednog algoritma, dok se primenom drugog mogu obraditi obeležja teksture [40]. Ovakav sistem zahteva implementaciju više algoritama za obradu, ali nisu potrebni dodatni senzori pa se smatra pristupačnim za proširenje klasičnog biometrijskog sistema. Nedostaci ovakvog sistema su izražena korelacija između skupova izdvojenih karakteristika, s obzirom na to da proizilaze iz istih ulaznih podataka.

Multimodalnost podrazumeva korišćenje dve ili više različitih biometrijskih karakteristika (npr. otisak prsta i dužica oka). S obzirom na to da se različite biometrijske karakteristike smatraju međusobno nezavisnim, među njima ne postoji korelacija. Zbog toga, multimodalni biometrijski sistemi značajno unapređuju performanse i tačnost autentifikacije u odnosu na klasične biometrijske sisteme i ostale multibiometrijske sisteme. Povećanjem primenjenih biometrijskih karakteristika, povećava se i primenljivost sistema, tj. pokrivenost obuhvaćene populacije. Troškovi implementacije ovog sistema predstavljaju njegovu najveću manu, zbog upotrebe dodatnih senzora, algoritama obrade, računskih resursa i prostora za skladištenje. Takođe, multimodalni biometrijski sistemi zahtevaju veću kooperativnost korisnika i često pokreću pitanja privatnosti zbog prikupljanja višestrukih biometrijskih karakteristika.

Pored navedenih vrsta multibiometrijskih sistema, moguće su i njihove međusobne kombinacije, što se naziva hibridnim multibiometrijskim sistemima. Tako je, na primer najveći nacionalni biometrijski sistem za identifikaciju stanovništva u Indiji (UIDAI), spoj više instanci iste biometrijske karakteristike i multimodalne biometrije, s obzirom na to da se prikupljaju otisci svih deset prstiju i obe dužice oka. Upravo ove dve vrste multibiometrije su najpopularnije, najbolje pokrivaju veliku populaciju i smatraju se najtačnijima. Pored svih navedenih ulaznih biometrijskih podataka i njihovih kombinacija, moguće je uključiti i neke nebiometrijske faktore u proces autentifikacije (npr. lozinke, PIN i sl.). Takav postupak autentifikacije se naziva višefaktorska autentifikacija (engl. *multi-factor authentication*).

2.4.2. Prikupljanje i obrada podataka

Akvizicija biometrijskih podataka može se sprovoditi: serijski ili paralelno, dok se njihova obrada može izvršavati: serijski, paralelno i hijerarhijski. Kada multibiometrijski sistem koristi samo jedan senzor, tada je moguće samo serijsko prikupljanje podataka. Prilikom serijskog prikupljanja, svaki ulazni podatak se nezavisno dobija, sa kratkim vremenskim intervalom između dva uzorkovanja. Kod paralelnog prikupljanja preduslov je postojanje više senzora sa kojih će se simultano prikupiti ulazni podaci. Postojanje više senzora ne mora nužno značiti da će se oni koristiti istovremeno. Upotreba serijskog prikupljanja podataka obično predstavlja jednostavnije, samim tim jeftinije rešenje, dok paralelni pristup skraćuje vreme potrebno za upis podataka i autentifikaciju, čime se povećava efikasnost biometrijskog sistema.

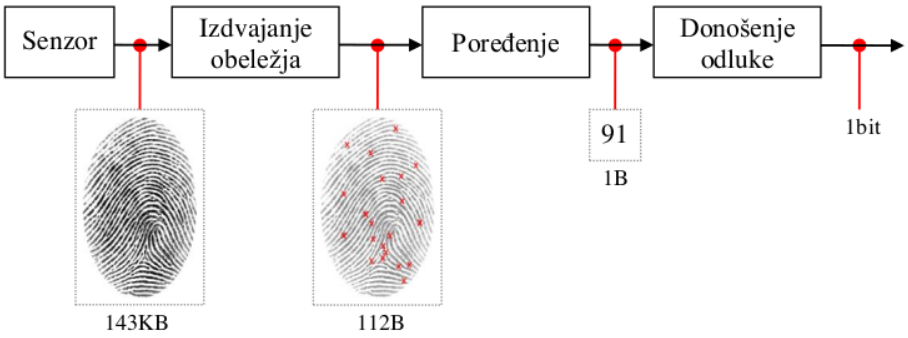
Način obrade biometrijskih podataka je nezavisan od načina prikupljanja podataka, što znači da se podaci mogu prikupljati paralelno, a obrađivati serijski i obrnuto. U režimu verifikacije identiteta, serijska obrada podataka podrazumeva da se sprovede upoređivanje primarne biometrijske karakteristike, pa ukoliko na osnovu nje nije uspešno izvršena autentifikacija, postupak se ponavlja sekundarnom biometrijom. Paralelni režim obrade podataka obuhvata istovremeno sve ulazne biometrijske podatke i primenjuje se kada je neophodna maksimalna sigurnost autentifikacije. Biometrijski podaci se nezavisno obrađuju, a sjedinjavanje informacija se obavlja u skladu sa utvrđenim načinom i nivoom. Primer hijerarhijske obrade podataka može se prikazati u režimu identifikacije, kada se na osnovu jedne biometrijske karakteristike iz baze podataka izdvaja podskup mogućih identiteta, da bi se u narednim iteracijama primenom drugih biometrijskih karakteristika odredio pravi. U scenariju identifikacije iz velikih baza podataka, primarno se koristi računski najbrža karakteristika u funkciji filtriranja, kako bi se najpreciznija i računski zahtevnija poređenja sprovela na malom skupu izdvojenih kandidata. Rezultujući identitet na kraju zadovoljava poređenje svih biometrija u hijerarhijskom nizu.

2.4.3. Sjedinjavanje biometrijskih podataka

U postupku razvijanja nekog multibiometrijskog sistema od ključnog značaja je odabir načina i nivoa na kom će doći do sjedinjavanja biometrijskih podataka. Sjedinjavanje je moguće na nivou svakog modula biometrijskog sistema, pa se na osnovu toga može izvršiti podela prema sjedinjavanju biometrijskih podataka tokom:

- akvizicije na senzoru,
- izdvajanja obeležja,
- upoređivanja obeležja i
- postupka odlučivanja.

Na osnovu kompleksnosti, sjedinjavanje podataka često se deli na dve kategorije: sjedinjavanje pre poređenja i sjedinjavanje nakon poređenja biometrijskih podataka. Sjedinjavanje pre poređenja podrazumeva objedinjavanje veće količine podataka, imajući u vidu da svaki modul nakon obrade generiše manji set podataka u odnosu na svoj ulaz, što je ilustrovano u šemi na slici 17. Izvorni oblik biometrije prilikom akvizicije poseduje najveću količinu podataka, ali istovremeno sadrži najveću količinu šuma. Modul za izdvajanje obeležja formira biometrijski šablon koji se sastoji od ključnih reprezentativnih detalja sa uklonjenim šumom i eliminisanim podacima koji nisu od značaja, što predstavlja idealno mesto za sjedinjavanje podataka. Međutim, sjedinjavanje pre poređenja u određenim slučajevima, kao što je multimodalnost, zahteva modifikaciju modula za poređenje novih vrsta obeležja, što predstavlja veliki izazov. Sjedinjavanje podataka na nivou poređenja i donošenja odluke ne zahteva dodatnu kompleksnost već se svodi na jednostavno kombinovanje pojedinačnih rezultata i odluka, pa se najčešće primenjuje.



Slika 17 – Prikaz veličine podataka jednog otiska prsta nakon svakog modula

2.4.3.1. Sjedinjavanje na nivou senzora

Sjedinjavanje na nivou senzora je primenljivo samo za podatke koji pripadaju istoj biometrijskoj karakteristici. Istovremeno, potrebna je potpuna međusobna kompatibilnost upotrebljenih senzora. Zbog toga se sjedinjavanje podataka na ovom nivou retko koristi i uglavnom se primenjuje u specifičnim slučajevima. Kao primer, može se navesti upotreba kompaktnih senzora za otiske prstiju koji rade na principu prevlačenja prsta preko senzora. Ovi senzori generišu kompletnu sliku jednog otiska sjedinjavanjem više manjih delova slike koje senzor detektuje prilikom prevlačenja prsta. Takođe, sjedinjavanje na nivou senzora može se primeniti za poboljšanje kvaliteta uzorkovanja, gde se od više uzoraka formira jedan koji ih objedinjuje. Ovaj proces se naziva mozaikovanje [41] i prikazan je na slici 18. Sličan primer se može naći prilikom prepoznavanja lica, gde se od više snimaka lica u različitim pozama, sjedinjavanjem tih podataka dobija kompletnija slika lica ili 3D model.



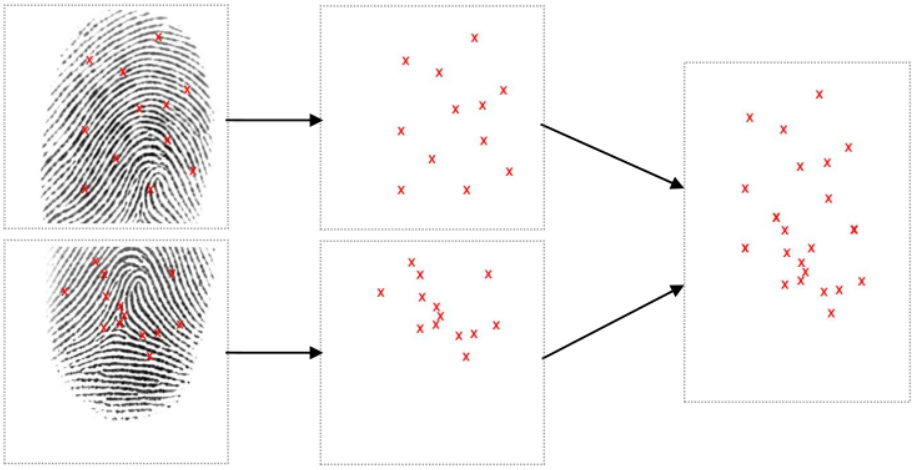
Slika 18 – Primer sjedinjavanja na nivou senzora dva parcijalna otiska

2.4.3.2. Sjedinjavanje na nivou izdvajanja obeležja

Sjedinjavanje podataka na ovom nivou obuhvata dva skupa izdvojenih obeležja biometrijske karakteristike, koji potiču od istog korisnika. Ukoliko je reč o istoj biometrijskoj karakteristici i primeni istog algoritma za izdvajanje obeležja u oba skupa, onda je u pitanju homogeno sjedinjavanje. U suprotnom, ukoliko se koriste različite biometrijske karakteristike (npr. otisak prsta i dužica oka), različiti algoritmi za izdvajanje karakteristika ili različiti izvori (instance) iste biometrijske karakteristike (npr. dužice oba oka), tada je reč o heterogenom sjedinjavanju.

U slučaju homogenog sjedinjavanja, princip je sličan sjedinjavanju na nivou senzora, samo što se umesto slike, sjedinjavaju izdvojena obeležja. Obeležja sa dva različita senzora ili dva nezavisna uzorka istog biometrijskog izvora, sjedinjavaju se tako što se uzorci poziciono usklade na osnovu zajedničkih karakterističnih detalja, dupla obeležja se uklone i podaci se spoje u jedan biometrijski šablon, što je ilustrovano na slici 19. Rezultujući šablon se na taj način poboljšava, sadržeći veći broj specifičnih obeležja biometrijskog izvora [41].

Heterogeno sjedinjavanje karakteristika je teško postići kada su u pitanju različite biometrijske karakteristike ili različiti algoritmi za izdvajanje obeležja, zbog međusobne nekompatibilnosti njihovih reprezentacija. Na primer, minucije otisaka prstiju predstavljaju se vektorima i njihova reprezentacija je promenljive dužine, dok su *Eigen* koeficijenti kod karakteristike lica skalarne vrednosti i fiksne dužine reprezentacije.



Slika 19 – Primer homogenog sjedinjavanja dva parcijalna otiska

2.4.3.3. Sjedinjavanje na nivou poređenja

Sjedinjavanje na nivou poređenja je najčešće korišćeni pristup u multibiometrijskim sistemima, zbog jednostavnosti kombinovanja rezultata dobijenih sa različitih modula poređenja. Izazovi se javljaju kada su rezultati pojedinačnih modula poređenja nehomogeni, što je slučaj kada su: pojedinačni rezultati u različitom opsegu, rezultati imaju različitu raspodelu verovatnoće ili jednostavno imaju različit način poređenja (merenje podudarnosti i merenje nepodudarnosti). Kvalitet biometrijskih uzoraka ima značajan uticaj na tačnost poređenja. Loš kvalitet biometrijskog uzorka često ima za posledicu pogrešne rezultate, jer izdvojena obeležja iz takvih uzoraka nisu pouzdana. Na osnovu kvaliteta uzoraka na ulazu može se dinamički dodeljivati težinski koeficijent izlazima pojedinačnih modula poređenja i tako mogu da se poboljšaju ukupne performanse multibiometrijskog sistema [42]. U zavisnosti od korišćenog modela za klasifikaciju, tehnike sjedinjavanja na ovom nivou se mogu podeliti u tri kategorije: sjedinjavanje na osnovu odnosa verovatnoća, sjedinjavanje na osnovu transformacije i klasifikacioni pristupi bazirani na neuronskim mrežama, drvu odlučivanja, genetskim algoritmima, *Support Vector Machines* i dr.

Sjedinjavanje na osnovu odnosa verovatnoća (engl. *Likelihood ratio*) [43] najčešće se bazira na Bajesovoj teoriji odlučivanja (engl. *Bayesian decision theory*) i *Neyman-Person* statističkom testiranju hipoteza. Osnovni cilj je da se donese odluka kojoj kategoriji klasa posmatrani uzorak pripada. U biometrijskim sistemima to su dve klase: ω_0 - uljez ili ω_1 - legitiman korisnik, a $P(\omega_0)$ i $P(\omega_1)$ su njihove apriorne verovatnoće dobijene na osnovu opservacija ovih klasa. Opservacijom rezultata poređenja uspostavlja se vektor merenja s. Ovaj vektor predstavlja ulazne parametre pravila za odlučivanje, na osnovu kojeg se dodeljuje nekoj od postojećih klasa. Aposteriorna uslovna funkcija gustine verovatnoće za

uljeza je $p(s|\omega_0)$ a za legitimnog korisnika $p(s|\omega_1)$. Uz pretpostavku da je vektor s slučajan i da njegova uslovna funkcija gustine verovatnoće zavisi od klase, ako su ove uslovne funkcije gustina verovatnoće poznate, onda se ovaj problem svodi na statističko testiranje hipoteza.

U modelu sjedinjavanja na osnovu transformacije, rezultati poređenja se prethodno normalizuju u zajednički domen, a zatim se kombinuju. Izbor normalizacione šeme zavisi od podataka. U [44] razvijena je teorijska osnova za sjedinjavanje različitih klasifikatora koristeći pravila kombinovanja: zbira, proizvoda, minimalne i maksimalne vrednosti, medijane i većinskog izbora (engl. *majority voting*). Za razvoj ovih šema potrebno je rezultate poređenja konvertovati u aposteriorne verovatnoće koje odgovaraju legitimnom korisniku i uljezu [45]. Od predloženih pravila kombinovanja, šema zbira je nadmašila preostale u [44].

2.4.3.4. Sjedinjavanje na nivou odlučivanja

Kada biometrijski sistem radi u režimu identifikacije, izlaz sistema može se predstaviti kao skup potencijalnih identiteta u vidu rang liste sortirane na osnovu poverenja. Multibiometrijski sistem se sastoji od dva ili više pojedinačna biometrijska sistema koji imaju zasebne rezultujuće rang liste, pa je potrebno izvršiti njihovu konsolidaciju u jedinstvenu rang listu. Ovaj postupak se naziva sjedinjavanje na nivou rangiranja, a s obzirom na to da se na osnovu rang liste donosi odluka, može se svrstati u podgrupu sjedinjavanja na nivou odlučivanja. Za razliku od rezultata poređenja, u ovom pristupu nije potrebna nikakva normalizacija podataka, već se rangiranje može direktno porediti. Rangiranje svakog pojedinačnog biometrijskog sistema može se predstaviti matricom $R=[r_{nm}]$, gde je r_{nm} rang dodeljen identitetu n od strane modula poređenja pojedinačnog biometrijskog sistema m. Računa se statistika $\hat{r}_n$ za svaki identitet n, takva da najmanja vrednost predstavlja najbolji rang nove zajedničke liste. Osnovne tri metode za računanje statistike $\hat{r}_n$ [46]:

- **Metoda najvećeg ranga** - svakom identitetu se dodeljuje najveći rang od svih m pojedinačnih sistema:

$$\hat{r}_n = \min_{m=1}^{M} r_{nm}. \qquad (16)$$

  Prednost ovog modela je što je dovoljno da samo jedan od biometrijskih podsistema dodeli najbolji rang i taj identitet će biti visoko rangiran u zajedničkoj listi, čime dolazi do izražaja snaga svakog pojedinačnog sistema.
- ***„Borda count"* metoda** je poznata tehnika obračuna izbornih glasova, koju je osmislio francuski matematičar Borda (*Jean-Charles de Borda*). Izborni princip je

primenjen nad izlazima više pojedinačnih biometrijskih sistema, tako što se rangovi svakog od njih sabiraju:

$$\hat{r}_n = \sum_{m=1}^{M} r_{nm} \ . \tag{17}$$

Na taj način se izračunava stepen saglasnosti više pojedinačnih biometrijskih sistema oko rezultujućeg identiteta. Ova metoda podrazumeva da je rangiranje pojedinačnih biometrijskih sistema međusobno statistički nezavisno i podjednako tačno, analogno tome da svaki glas ima podjednaku vrednost, što često nije slučaj u multibiometrijskim sistemima.

- **Metoda logističke regresije** predstavlja unapređenje prethodne metode uvođenjem težinskih koeficijenata w_m za svaki od m pojedinačnih biometrijskih sistema:

$$\hat{r}_n = \sum_{m=1}^{M} w_m r_{nm} \ . \tag{18}$$

Zahvaljujući težinskim koeficijentima, ovom metodom se izračunava stepen saglasnosti više pojedinačnih biometrijskih sistema oko rezultujućeg identiteta, uzimajući u obzir preciznost svakog od korišćenih sistema i biometrijskih karakteristika. Težinski koeficijenti se određuju logističkom regresijom, po čemu je ova metoda dobila ime.

U tabeli 3, dat je primer dva pojedinačna biometrijska sistema i uporedni pregled rezultujućeg rangiranja za sve tri metode. Izabrani biometrijski sistemi su različite tačnosti, pa je prikazan uticaj različitih težinskih koeficijenata na konačni rang, iz čega se može zaključiti da tačnost metode logističke regresije zavisi od pravilno određenih koeficijenata.

Tabela 3 – Uporedni pregled rezultata različitih metoda sjedinjavanja na nivou rangiranja

Identitet	Rang biometrijskog sistema		Metoda najvećeg ranga		*Borda count* metoda		Logistička regresija [w_1=0,8; w_2=0,2]		Logistička regresija [w_1=0,7; w_2=0,3]	
	Otisak prsta	Crte lica	Sjedinjeni rezultati	Novi rang	Sjedinjeni rezultati	Novi rang	Sjedinjeni rezultati	Novi rang	Sjedinjeni rezultati	Novi rang
A	3	1	1	1	4	2	2,6	3	2,4	2
B	4	3	3	4	7	4	3,8	4	3,7	4
C	1	2	1	2	3	1	1,2	1	1,3	1
D	2	4	2	3	6	3	2,4	2	2,6	3

Kada na izlazu pojedinačnih biometrijskih sistema, koji zajedno formiraju multibiometrijski sistem, nemamo rang liste već pojedinačne odluke, kao što je to slučaj u režimu verifikacije, potrebno je odrediti konačnu odluku multibiometrijskog sistema. Tada

se odluke pojedinačnih biometrijskih sistema sjedinjavaju u konačnu odluku multibiometrijskog sistema i to nazivamo sjedinjavanjem na nivou odlučivanja. U praksi, ovo je najčešći slučaj realizacije komercijalnih multibiometrijskih sistema iz praktičnih razloga. Neke od metoda za sjedinjavanje podataka na nivou odlučivanja su:

- **Metoda I i ILI pravila** predstavlja najjednostavniji način objedinjavanja odluka pojedinačnih biometrijskih sistema. Rezultujuća odluka multibiometrijskog sistema upotrebom I pravila je pozitivna (verifikovanje identiteta) samo ukoliko su sve odluke pojedinačnih sistema pozitivne. Kada se koristi ILI pravilo, tada je dovoljno da samo jedan od pojedinačnih biometrijskih sistema potvrdi da priloženi uzorak odgovara odgovarajućem uskladištenom šablonu. Međutim, metode I i ILI pravila retko se koriste zbog rezultujućih ekstremnih FAR i FRR vrednosti. Primenom I pravila FAR je veoma mala, dok je FRR veoma velika, što je uglavnom neprihvatljivo. Korišćenjem ILI pravila, efekti su suprotni: velika vrednost FAR, uz malu vrednost FRR, što je takođe neprihvatljivo u praksi.

- **Izbor većine** (engl. *majority voting*) je jedna od jednostavnih metoda za sjedinjavanje podataka na nivou odlučivanja, koja se primenjuje kada se koristi više od dve nezavisne biometrijske karakteristike za autentifikaciju [47]. Bilo da je reč o verifikaciji ili identifikaciji, rezultujuća odluka multibiometrijskog sistema odgovara većini odluka pojedinačnih podsistema. U ovoj metodi tačnost svakog pojedinačnog sistema nije od značaja, već svaki od njih ima isti značaj.

- **Težinski izbor većine** (engl. *weighted majority voting*) predstavlja unapređenje prethodne metode, tako što se svakom od pojedinačnih sistema dodeljuju težinski koeficijenti u zavisnosti od tačnosti tog sistema [48].

2.4.4. Prednosti upotrebe multibiometrijskih sistema

Korišćenje više nezavisnih biometrijskih izvora podataka ima pozitivan uticaj na sveobuhvatne performanse i faktore biometrijskog sistema. Postiže se veća tačnost usled povećanja ulaznih podataka, zahvaljujući kojima se postiže bolja diskriminativnosti. Izabrane biometrije međusobno kompenzuju nedostatke koje poseduju, što rezultuje manjim vrednostima FAR i FRR grešaka. Poboljšanje sigurnosti postiže se povećanjem otpornosti na obmane korišćenjem falsifikovanih biometrija, iz prostog razloga što je mnogo teže izvršiti obmanu više biometrijskih karakteristika istovremeno. Primenom multimodalnosti ostvaruje se bolja univerzalnost sistema, samim tim i prihvatljivost njegove primene od strane korisnika. Univerzalnost biometrijskog sistema se ogleda u tome da svi korisnici poseduju neku od karakteristika primenjenu u multibiometrijskom sistemu. Prilikom oštećenja jedne biometrijske karakteristike (npr. posekotina prsta),

autentifikacija se može izvršiti pomoću drugih karakteristika koje sistem podržava. Prilagodljivost sistema individualnim pitanjima privatnosti korisnika, može se rešiti fleksibilnim pravilima, tako da korisnik može za autentifikaciju koristiti one karakteristike za koje smatra da su manje invazivne i njemu lično prihvatljive. Na taj način korisnici bolje prihvataju biometrijski sistem i stiču poverenje u njega. Prilikom postupka identifikacije, često se radi pretraga velikih baza biometrijskih podataka. Ukoliko se koristi više različitih biometrijskih izvora podataka, tada se pretraga može raditi na osnovu one biometrijske karakteristike koja je računski najlakša za poređenje, bez obzira na njenu tačnost, jer će se konačna potvrda identiteta izvršiti poređenjem najpreciznije ili poređenjem svih karakteristika. Multibiometrijski sistemi imaju mnogo prednosti nad klasičnim biometrijskim sistemima, međutim višestruko su skuplji zbog dodatnog hardvera i softvera, a od korisnika zahtevaju veću kooperativnost. Dodatna kompleksnost sistema, osim skuplje implementacije, ima i veće troškove održavanja sistema i obuke zaposlenih, pa odluka o upotrebi multibiometrijskog sistema predstavlja kompromis između realnih potreba organizacije za određenim nivoom bezbednosti i raspoloživim novčanim sredstvima.

3. Sigurnost biometrijskih sistema

Savremeni sistemi kontrole pristupa u velikoj meri koriste biometriju kao sredstvo autentifikacije. Na primer, biometrija je integrisana kao mehanizam za autentifikaciju na većini komercijalnih prenosnih uređaja, kao što su pametni telefoni i prenosni računari. Biometrijski sistemi koriste se za sprečavanje i otkrivanje kriminala, kontrolu granica, autentifikaciju bankarskih transakcija, evidenciju radnog vremena itd. Sledi da od sigurnosti biometrijskih sistema zavisi celokupna sigurnost svih drugih sistema, koji se na njega oslanjaju. Povreda integriteta jedne pojedinačne finansijske transakcije prenosi se lančano na bankarski ili neki drugi povezan korporativni sistem. Usled kompromitovane autentifikacije prilikom granične kontrole, može doći do ugrožavanja bezbednosti cele države. Zbog toga se sigurnost biometrijskog sistema mora ozbiljno razmatrati prilikom izbora biometrijske karakteristike, projektovanja sistema i same implementacije. Izbor biometrije zavisi od više faktora, kao što su: prihvatljivost od strane korisnika, ekonomski faktor, tehničke mogućnosti i ograničenja, sama svojstva biometrijske karakteristike itd. Sa aspekta sigurnosti, najbolja je ona biometrija koja ima najmanju verovatnoću otkaza, koja vodi ka narušavanju bezbednosti. Bezbednost podataka i informacionih sistema, što se primenjuje i na biometrijske sisteme, počiva na osnovim načelima:

- integriteta,
- poverljivosti i
- dostupnosti.

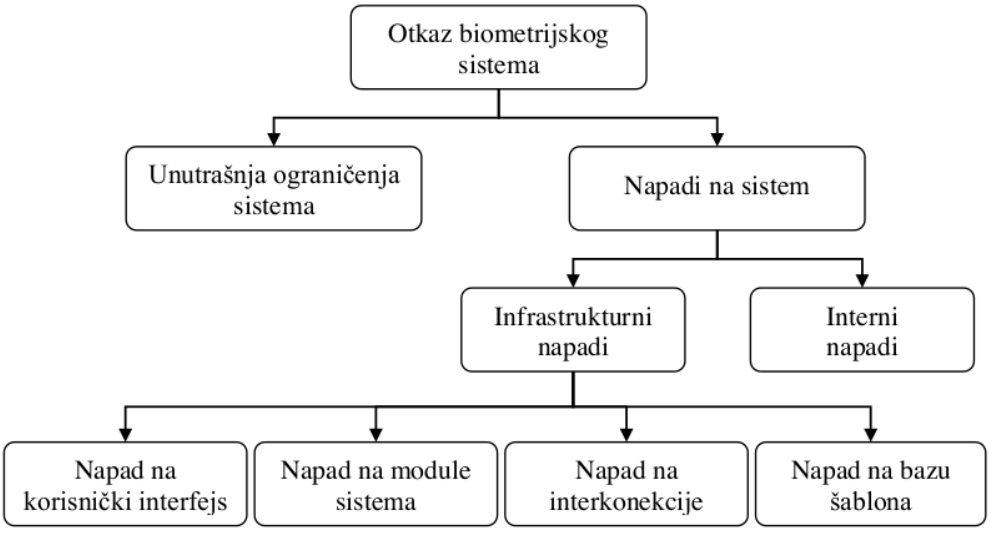
Integritet jednog biometrijskog sistema određen njegovom sposobnošću da garantuje neporecivost autentifikacije. Autentifikacija podrazumeva da se na osnovu nje legitimnim korisnicima autorizuje pristup nekim resursima, koji su u ovom slučaju zaštićeni biometrijskim sistemom, dok se drugima na osnovu autentifikacije to pravo uskraćuje. Neporecivost osigurava da korisnik koji je pristupio nekim resursima kasnije ne može da poriče svoj pristup i postupke. Integritet biometrijskog sistema je u direktnoj vezi sa mogućnošću njegove obmane, odnosno dobijanja nelegitimnog pristupa resursima, što predstavlja najveće narušavanje bezbednosti sistema. Ukoliko je dobijanje nelegitimnog pristupa moguće, tada legitimni korisnik može da poriče svoje postupke i pristup, pozivajući se na otkaz sigurnosti biometrijskog sistema.

Poverljivost kod biometrijskih sistema odnosi se na biometrijske podatke koji su uskladišteni u bazi podataka. Ovi podaci namenjeni su isključivo za funkcionisanje konkretnog sistema, pa u skladu sa ovim načelom nije dozvoljeno da se oni čuvaju u izvornom nezaštićenom obliku. Povredom poverljivosti, odnosno nelegitimnim pristupom izvornim podacima može doći do trajne kompromitacije biometrijske karakteristike i svih

sistema koji se oslanjaju na nju. Neki biometrijski podaci, kao što je slika lica, sadrže dodatne privatne podatke koji mogu biti zloupotrebljeni. Zbog toga je zaštita biometrijskih podataka ključni segment razvoja svakog biometrijskog sistema i uvek aktuelni predmet istraživanja.

Dostupnost biometrijskog sistema podrazumeva mogućnost korisnika da se uspešno autentifikuju i na osnovu toga raspolažu resursima na koja imaju pravo. Odbijanje usluge (engl. *Denial of Service* - DoS), krši princip dostupnosti sistema legitimnim korisnicima, što istima izaziva neprijatnost, a česta pojava ovog problema ima za posledicu nepoverenje u sistem, korišćenje alternativnih manje sigurnih tehnika autentifikacije ili kontrole pristupa, pa čak i obustavu upotrebe biometrijskog sistema.

Svaki sistem je zaštićen na neki način, u protivnom ne bi bio pouzdan i funkcionalan. Od njegove važnosti zavisi i stepen zaštite sistema. Međutim, ni jedan sistem nije apsolutno bezbedan i otporan na obmane ili upade. Pod određenim okolnostima, uz dovoljno resursa i raspoloživog vremena, svaki sigurnosni sistem se može savladati. Isto važi i za sigurnost biometrijskih sistema. Zbog toga je neophodno sprovesti detaljnu analizu sigurnosti, s ciljem da se identifikuju sve ranjivosti i potencijalne slabosti. Na osnovu formiranog modela pretnji, neophodno je definisanje i preduzimanje protivmera. Pretnje se mogu podeliti u dve grupe prema vrsti potencijalnog otkaza usled: unutrašnjih (tehničkih) ograničenja sistema i napada na sistem. Napadi na sistem mogu se podeliti na: interne i eksterne napade, odnosno insajderske i napade na infrastrukturu, respektivno [49]. Hijerarhijski, napadi na biometrijske sisteme se mogu klasifikovati kao na slici 20.



Slika 20 – Hijerarhijska klasifikacija potencijalnih napada na biometrijski sistem

Usled unutrašnjih ograničenja sistema može doći do otkaza, odnosno neispravnog funkcionisanja biometrijskog sistema. Ovi otkazi povezani su sa greškama poređenja izdvojenih biometrijskih obeležja – FAR i FRR, kao i odgovarajućim greškama prilikom upisa korisnika u biometrijski sistem. Greške su posledica unutrašnjih ograničenja koja se javljaju u različitim procesima biometrijskog sistema prilikom prikupljanja podataka, segmentacije, izdvajanja obeležja, formiranja šablona, poređenja, donošenja konačne odluke i sl. Iako uzrok nije namerni napad na sistem, posledica grešaka nastalih usled unutrašnjih ograničenja je proboj ili otkaz sigurnosti, što se naziva „napad bez truda“ (engl. *zero-effort attack*) [49]. FAR greške dovode do proboja sigurnosti, dok FRR greške izazivaju neprijatnost legitimnim korisnicima i doprinose nepoverenju u biometrijski sistem. Greške prilikom upisa i česte FRR greške krše princip dostupnosti sistema legitimnim korisnicima, što za posledicu ima korišćenje alternativnih tehnika autentifikacije, obično nižeg stepena bezbednosti. Takođe, greške usled unutrašnjih ograničenja sistema direktno utiču na princip neporecivosti. Stalnim tehnološkim razvojem novih senzora i naučno-istraživačkim radom na algoritmima za reprezentaciju obeležja i njihovo poređenje, povećava se stepen sigurnosti biometrijskih sistema, a ujedno smanjuje pojava grešaka ove vrste. Sve to doprinosi sve većem poverenju ljudi u biometrijske sisteme i društvenoj prihvatljivosti.

3.1. Interni napadi na biometrijske sisteme

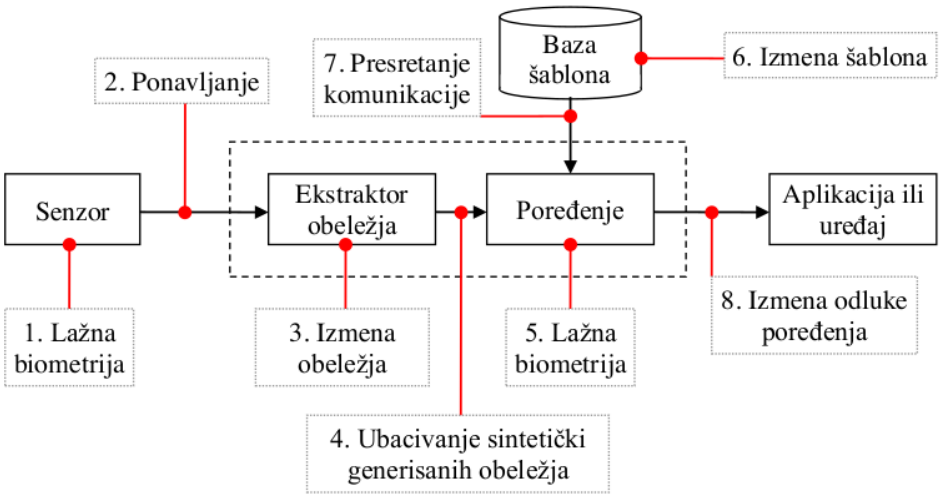
Pokušaj da se iskoristi neka ranjivost infrastrukture biometrijskog sistema ili ljudskog faktora, s ciljem dobijanja pristupa nekim resursima koji pripadaju samo legitimnim korisnicima, predstavlja napad na biometrijski sistem. Za primenu, administraciju i održavanje biometrijskog sistema potrebna je njegova interakcija sa ljudima. Ova interakcija se može iskoristiti za proboj sigurnosti sistema, s obzirom na to da na sigurnost celokupnog sistema direktno utiču ljudski postupci. Napadi na biometrijski sistem u kome direktno ili indirektno učestvuje neko od korisnika ili administratora, smatra se internim napadom. Napad može biti izveden u dosluhu sa nekim (engl. *collusion attack*), pod nečijom prisilom (engl. *coercion attack*) i usled nemara nekog korisnika (engl. *negligence attack*) [20][50]. Na svaki od ova tri načina, spoljni napadač ostvaruje legitimni pristup nekom resursu. Na primer, pristup nekom računarskom sistemu, koji je zaštićen biometrijom, legitimni korisnik može da omogući napadaču koristeći svoje biometrijske podatke, zarad neke materijalne nadoknade, pod prisilom ili svojim nemarom kada zaboravi da se odjavi sa računara. Nažalost, ovde nije moguće povećati bezbednost biometrijskog sistema upotrebom nekih tehničkih protivmera, već obukom, proverom i konstantnim nadzorom korisnika i njihovih akcija.

Većina sistema za autentifikaciju poseduje pomoćni način autentifikacije, koji se koristi u specifičnim slučajevima kada biometrijski sistem zakaže usled nemogućnosti

očitavanja biometrije (npr. oštećenje kože kod biometrije otiska prsta) ili kvara sistema. Pomoćni sistem je obično dosta nižeg stepena sigurnosti i baziran na identifikacionim karticama, RFID ili lozinkama. Znajući ove procedure napadač može namerno izazvati (npr. namernim oštećenjem kože prsta) upotrebu pomoćne procedure autentifikacije (engl. *exception abuse attack*) i tako zaobići biometrijski sigurnosni sistem. Slična vrsta obmane biometrijskog sistema može se izvršiti prilikom faze upisa šablona (engl. *enrollment fraud*), kada se biometrijski podaci napadača unesu u sistem na osnovu lažnih identifikacionih dokumenata, kao što su lična karta ili pasoš [20]. Zajedničko za obe navedene vrste obmane je da se sigurnost sistema u tom trenutku zasniva na identifikaciji nižeg stepena bezbednosti od samog primenjenog biometrijskog sistema. Razlog zašto se ove obmane smatraju internim napadima je to što se oslanjanje na druge sisteme autentifikacije smatra slabom tačkom dizajna biometrijskog sistema.

3.2. Napadi na infrastrukturu biometrijskog sistema

Opšti model biometrijskog sistema sastoji se od više funkcionalnih modula: senzor za akviziciju podataka, modul za obradu podataka i izdvajanje obeležja, baza šablona, modul poređenja šablona i modul donošenja odluke. Svi ovi moduli se sastoje od hardverskih i softverskih komponenti, međusobno povezanih putem komunikacionih kanala, što sve zajedno čini infrastrukturu biometrijskog sistema. U [51] sprovedena je detaljna analiza slabosti, dat je opšti model infrastrukturnih pretnji, gde je izdvojeno osam ključnih pozicija prikazanih na slici 21.



Slika 21 – Ranjivost infrastrukture biometrijskog sistema (prilagođeno iz [51])

Napadom na infrastrukturu, smatra se svaki napad koji dolazi izvan sistema i usmeren je na fizičke ili logičke slabosti neke njegove komponente. Prema delu infrastrukture koja se napada, možemo napraviti klasifikaciju napada na:

- korisnički interfejs,
- module obrade biometrijskih podataka,
- komunikacione kanale između modula i
- napade na bazu šablona.

Napad na korisnički interfejs predstavlja napad na interfejs između korisnika i sistema, odnosno na ulazni modul za akviziciju podataka biometrijskog sistema. Ovi napadi se nazivaju direktni napadi, s obzirom na to da imaju za cilj da već na ulaznom nivou prevare biometrijski sistem oponašajući biometrijsku karakteristiku. Takođe, za ove vrste napada ne zahteva se nikakvo poznavanje načina rada biometrijskog sistema, u smislu načina njegove implementacije, upotrebljenih algoritama za obradu podataka, načina komunikacije modula i čuvanja šablona. Kada je reč o sistemima zasnovanim na fizičkoj osobini, tada se za obmanu (engl. *spoofing attack*) koriste falsifikovane biometrije u vidu gumenih prstiju, slika dužice oka ili lica i sl. Kod sistema zasnovanih na biometrijskoj karakteristici ponašanja, obmana se vrši imitiranjem osobina ponašanja (engl. *mimicry attack*), npr. falsifikovanjem potpisa, imitiranjem glasa, kucanja na tastaturi i sl. Ovi napadi se pretežno zasnivaju na slabostima obrade podataka biometrijskog sistema i pokušavaju da iskoriste njegovu FAR grešku. Kod biometrijskih sistema negativne verifikacije, postoji još i napad prikrivanja svoje biometrijske karakteristike (engl. *obfuscation attack*), kako bi se izbegla verifikacija. Napad se izvodi oštećenjem ili izmenama svoje fizičke karakteristike, a kod karakteristika ponašanja namernom promenom ponašanja, slično kao kod napada imitacije.

Opšte protivmere za ovu vrstu napada na korisnički interfejs biometrijskog sistema baziraju se na poboljšanju ulaznog modula i povećanju robusnosti algoritama za obradu podataka i njihovo poređenje, kako bi se smanjila FAR greška. Za razliku od biometrijskih sistema zasnovanih na karakteristikama ponašanja gde je moguće primeti samo opšte protivmere, kod fizičkih osobina moguće je uvesti dodatnu zaštitu od obmane, koja se realizuju kroz testove fizičkih reakcija subjekta na određene pobude, kako bi se napravila razlika između ljudskog tela i veštačkih materijala. Kod biometrije otiska prsta koriste se metode detektovanja pulsa, krvnog pritiska, znojenja, merenja električne provodljivosti, odnosno otpornosti kože itd. Kod biometrije oka primenjuju se metode detektovanja reakcije oka na svetlosnu pobudu u vidu kontrakcije zenice, dok se kod drugih biometrijskih karakteristika koristi princip apsorpcije i refleksije svetlosti različitih talasnih dužina. Najbolji rezultati mogu se postići upotrebom multimodalnih biometrijskih sistema, koji paralelno koriste dve ili više biometrijskih karakteristika u svom radu. Dobrim izborom biometrija koje će se upotrebiti za neki specifičan sistem, korišćenjem prednosti

svake od njih tako da se njihova sigurnost međusobno dopunjuje i primenom inteligentnog interaktivnog procesiranja, može se podići stepen sigurnosti biometrijskog sistema na visok nivo, koji je izuzetno teško prevariti.

Indirektne napade predstavljaju napadi na module i njihove međusobne veze, čime napadač može manipulisati radom nekog modula, očitavati ili menjati međurezultate prilikom komunikacije, a može napasti i samu bazu biometrijskih šablona. Napadi na module se obično izvode uz pomoć nekog malicioznog softvera, koji na neki način utiče na rad algoritma za obradu ulaznih podataka, na poređenje ili donošenje odluke. Drugi način je pronalaženje i iskorišćavanje propusta u samom dizajnu biometrijskog sistema. Na svaki od ovih načina, napadač može da preuzme kontrolu nad nekim od modula i da generiše željenu izlaznu vrednost, umesto legitimne. Na taj način može da omogući uspešnu lažnu autentifikaciju ili odbijanje autentifikacije (DoS) legitimnim korisnicima [52]. Zaštita od ovih napada se svodi na tradicionalne metode zaštite informacionog sistema od malicioznog softvera, primenu kriptografskih tehnika zaštite podataka i veza.

Napadom na komunikaciju između modula, napadač može očitavati ili menjati međurezultate. Na taj način, on može doći u posed izdvojenih obeležja legitimnog korisnika, može menjati ili ubacivati svoje podatke i takve ih poslati na dalju obradu. Dva napada koja važe za svaki komunikacioni kanal su: „Čovek u sredini“ (engl. *Man in the middle attack*) i „Napad ponavljanja“ (engl. *Replay attack*). U kriptografiji, napad „Čovek u sredini“ je poznat kao jednostavan način za prevazilaženje kompleksnog Difi-Helman algoritma za razmenu ključeva, gde napadač presreće poruke učesnika u komunikaciji, predstavlja se kao onaj drugi učesnik i kao posrednik između njih sa svakim od učesnika formira svoj tajni ključ, a učesnici nisu u mogućnosti da otkriju da je njihov komunikacioni kanal kompromitovan. Slično tome, u biometrijskom sistemu napadač presreće komunikaciju između dva modula i postiže isti efekat, kao i kod napada kada preuzme kontrolu nad modulom nekim malicioznim softverom. Ovaj napad se može prevazići međusobnom autentifikacijom između modula. Napad ponavljanja se zasniva na presretanju komunikacije između modula u trenutku kada se šalju podaci nekog legitimnog korisnika i njihovim ponovnim slanjem u nekom željenom trenutku. Ovaj napad je moguće primeniti i na kriptografski šifrovanim podacima, ukoliko se koriste isti ključevi, pa je protivmera korišćenje ključa sesije za šifrovanje ili neka specifična implementacija vremenskih oznaka (engl. *timestamp*) na podatke prilikom razmene.

Napad grubom silom (engl. *brute-force attack*) se oslanja na neki od prethodno opisanih napada na komunikaciju između modula, čime napadač stiče mogućnost da ubacuje ulazne biometrijske podatke ili obeležja direktno u neki od odgovarajućih modula sistema. Isprobavanjem velikog broja biometrijskih uzoraka, koji mogu biti sintetički generisani, napadač će u nekom trenutku uspeti da pronađe uzorak koji rezultuje pozitivnim ishodom poređenja usled FAR greške sistema. Ovaj napad je ekvivalentan

napadu pomoću rečnika (engl. *dictionary attack*) u sistemima autentifikacije pomoću lozinki.

Hilov napad (engl. *Hill climbing attack*) [53] je specifičan napad razvijen za biometrijske sisteme, a predstavlja unapređenje napada grubom silom. Za ovaj napad je napadaču, pored ostvarivanja mogućnosti da ubacuje ulazne biometrijske podatke ili izdvojena biometrijska obeležja direktno u neki od odgovarajućih modula sistema, potreban pristup izlaznom rezultatu poređenja uzorka i šablona. Cilj napada je da se odredi biometrijski uzorak ili šablon, koji prilikom poređenja odgovara ciljanom šablonu sačuvanom u bazi. Umesto korišćenja velikog broja nasumičnih biometrijskih uzoraka iz napadačeve biometrijske baze, ovde se koriste veštački generisani biometrijski uzorci tzv. sintetički biometrijski uzorci. Tako generisan uzorak se inicijalno dâ biometrijskom sistemu na obradu i poređenje. Rezultat poređenja se beleži, inicijalni sintetički uzorak se modifikuje i ponovo šalje sistemu na obradu i poređenje. Ukoliko je novi rezultat poređenja bolji od prethodnog, modifikacija se zadržava, a u suprotnom se poništava. Sledi nova modifikacija i analiza dobijenog rezultata poređenja. Postupak se iterativno ponavlja, dok se ne dobije dovoljno dobar sintetički uzorak, koji ima pozitivan ishod poređenja. Ovaj napad, osim što izaziva proboj sigurnosti biometrijskog sistema u pogledu autentifikacije, ostvaruje mnogo veću povredu sigurnosti u vidu trajne kompromitacije biometrijskog izvora. S obzirom na to da napadač pomoću ovog napada dolazi u posed sintetički generisane biometrije nekog subjekta, koja predstavlja dovoljno dobru aproksimaciju originala, kompromitovan je svaki drugi biometrijski sistem u kome je korišćena ista biometrijska karakteristika tog subjekta. Neke od mera zaštite od ovog napada mogu biti: unapređenje protivmera koje se odnose na napade na komunikaciju, imajući u vidu da je za Hilov napad preduslov prethodno uspešan napad na komunikaciju između modula, zatim kontrola i ograničavanje broja odbijenih poređenja jednog subjekta u određenom vremenskom periodu i gruba kvantizacija izlaznog rezultata poređenja tj. povećanje njegove granularnosti, čime se napadaču umanjuje povratna informacija o uspešnosti modifikacije uzorka između dve iteracije.

Napadi na bazu šablona. Postoji mnogo različitih načina implementacije biometrijskih sistema. Na primer, svi funkcionalni moduli mogu se smestiti na jednu pametnu karticu, gde biometrijski podaci ni u jednom trenutku ne napuštaju karticu, već je izlaz samo konačni rezultat poređenja – podudaranje ili ne. Nasuprot tome, nacionalne baze biometrijskih karakteristika stanovništva nalaze se na nekoj centralnoj lokaciji, dok su ostali moduli raspoređeni na više različitih udaljenih lokacija sa kojih im se pristupa. Napad na bazu šablona može biti usmeren u dva pravca: dobijanje pristupa sistemu napadaču ili odbijanje pristupa legitimnim korisnicima i krađa biometrijskih podataka. Dobijanje pristupa sistemu napadom na bazu podataka podrazumeva nelegalni pristup bazi podataka i unošenje novog ili modifikovanje postojećeg biometrijskog zapisa, čime se omogućava proboj sigurnosti biometrijskog sistema. Odbijanje pristupa legitimnim

korisnicima se postiže modifikovanjem ili brisanjem njihovog biometrijskog zapisa. Sa aspekta načela biometrije mnogo ozbiljniji napad predstavlja krađa biometrijskih podataka. Za razliku od drugih sistema zaštite, gde se koriste metode bazirane na znanju ili nekom objektu koje se mogu povući ili promeniti, kod biometrijskih sistema se koriste biometrijske karakteristike koje se ne mogu promeniti. Biometrijska obeležja trajno su povezana sa nekom osobom i njihova kompromitacija se prenosi na sve sisteme koji koriste tu karakteristiku. Upravo je to razlog zašto se u bazama biometrijskih podataka ne čuvaju izvorni podaci (slika otiska, dužice lica itd.), već njihovi šabloni koji predstavljaju digitalnu reprezentaciju specifičnih obeležja biometrijske karakteristike. Funkcija kreiranja šablona teži da bude jednosmerna funkcija, slično kao heš funkcija u kriptografiji, s ciljem da se na osnovu šablona ne mogu dobiti sva obeležja neke biometrijske karakteristike. Međutim, mogućnost rekonstrukcije izvorne biometrije na osnovu izdvojenih obeležja je moguća, što je prikazano u pionirskim radovima na ovu temu u [54] i [55]. Krađa biometrijskih podataka krši osnovni princip poverljivosti biometrijskog sistema i zato zaštita biometrijskih šablona predstavlja veoma bitan segment u sigurnosti celokupnog biometrijskog sistema.

3.3. Zaštita biometrijskih šablona

Biometrijski šablon je digitalna reprezentacija izdvojenih specifičnih obeležja nekog biometrijskog uzorka. Kao odgovor na sigurnosne izazove, potrebno je primeniti sigurnosne mehanizme za formiranje zaštićenih biometrijskih šablona. Da bi zaštićeni šabloni zadovoljili bezbednosne kriterijume, a da istovremeno nemaju negativan uticaj na rad biometrijskog sistema, neophodno je da prilikom generisanja i upotrebe zaštićenih šablona budu zadovoljeni kriterijumi [10][56]:

- jednosmerna transformacija izdvojenih obeležja,
- nepostojanje degradacije performansi,
- mogućnost opozivosti šablona i
- međusobna nepovezivost generisanih šablona u različitim sistemima.

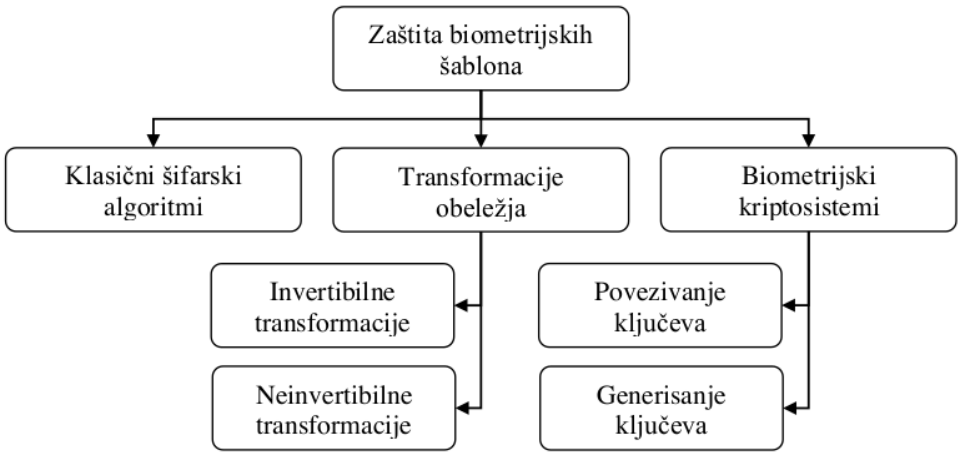
Funkcije kojima se generišu zaštićeni šabloni spadaju u klasu jednosmernih matematičkih transformacija, koje na osnovu skupa izdvojenih biometrijskih obeležja formiraju šablon, ali tako da postupak ne sme biti reverzibilan. Generisanje šablona mora biti veoma brzo, jednostavno i jednoznačno, što znači da primena iste funkcije na istom skupu odabranih biometrijskih obeležja, mora da rezultira istim šablonom. Istovremeno, ne sme da dođe do postojanja kolizije (engl. *collision free*), odnosno da dva različita ulaza rezultuju istim izlaznim šablonom. Zavisnost izlaza od ulaza funkcije ne sme biti ni na koji način predvidiva, a najmanja promena ulaznih podataka neophodno je da izazove efekat

lavinske promene na izlazu. Funkcije kojima se generišu zaštićeni šabloni analogne su heš funkcijama koje se koriste u kriptografiji.

Primena zaštite biometrijskih šablona ne sme imati uticaja na performanse biometrijskog sistema. Prvenstveno, uticaja ne sme biti na FAR i FRR greške biometrijskog sistema, a zatim ni u brzini rada i odzivu sistema.

Opozivost šablona podrazumeva mogućnost generisanja više različitih zaštićenih šablona na osnovu istog biometrijskog uzorka. Takvi šabloni moraju biti međusobno značajno različiti, tako da se prilikom njihovog poređenja ili analize ne može odrediti da potiču od istog biometrijskog uzorka. Opozivost šablona omogućava da se u slučaju kompromitacije biometrijskog zaštićenog šablona isti može otkazati, a da se na osnovu iste biometrijske karakteristike može generisati novi zaštićeni šablon koji se razlikuje od prethodnog. Time se poboljšava privatnost korisnika, imajući u vidu da se u dva zasebna biometrijska sistema zaštićeni šabloni istog korisnika razlikuju iako su generisani na osnovu istih biometrijskih ulaznih podataka. Na ovaj način nije moguće njihovo međusobno poređenje, niti prikupljanje podataka o korisniku unakrsnim referenciranjem.

Na slici 22. šematski je prikazana klasifikacija načina generisanja zaštićenog biometrijskog šablona prema modalitetu rada u tri osnovne klase: klasični šifarski algoritmi, transformacije obeležja i biometrijski kriptosistemi [56].

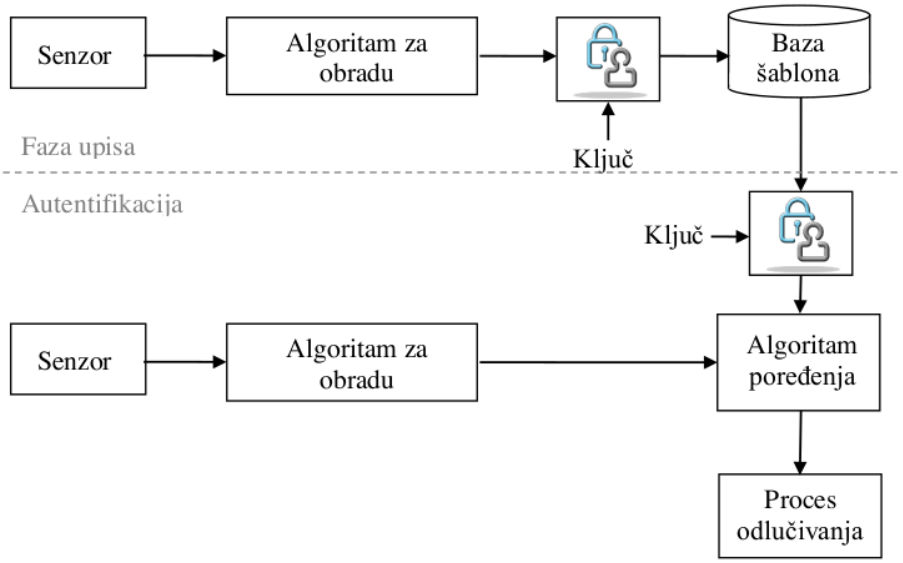


Slika 22 – Različiti pristupi načinu zaštite biometrijskog šablona

3.3.1. Klasični šifarski algoritmi za zaštitu biometrijskog šablona

Standardno šifrovanje digitalne reprezentacije biometrijskih podataka oslanja se na klasične kriptografske šifarske algoritme (npr. DES, AES, RSA i dr.), koji se uobičajeno

koriste za zaštitu podataka. Ovaj način zaštite je najzastupljeniji u komercijalnoj upotrebi, s obzirom na to da nisu potrebne nikakve dodatne modifikacije modula obrade i poređenja biometrijskog sistema. Zaštićeni šablon se čuva u šifrovanom obliku, a prilikom poređenja se prvo dešifruje. Izuzetak od ovog uobičajenog postupka su primene homomorfnog i asimetričnog šifrovanja, koji ne zahtevaju dešifrovanje zaštićenog šablona [57]. Poređenje dva šifrovana šablona nije moguće, zato što najmanja razlika izdvojenih obeležja iz uzorka i onih sačuvanih u šablonu, rezultuje velikim razlikama između dva zaštićena šablona. Zbog toga, šabloni se mogu porediti samo u izvornom obliku, a čuvaju se u šifrovanom, što je šematski predstavljeno na slici 23. Upravo to je i najveća slabost ovog pristupa, zato što je šablon u trenutku poređenja dešifrovan i dostupan napadaču u njegovom izvornom nezaštićenom obliku. Ujedno, sigurnost šablona počiva na tajnosti ključa, što otvara druga sigurnosna pitanja. Opozivost zaštićenog šablona se postiže promenom tajnog ključa.

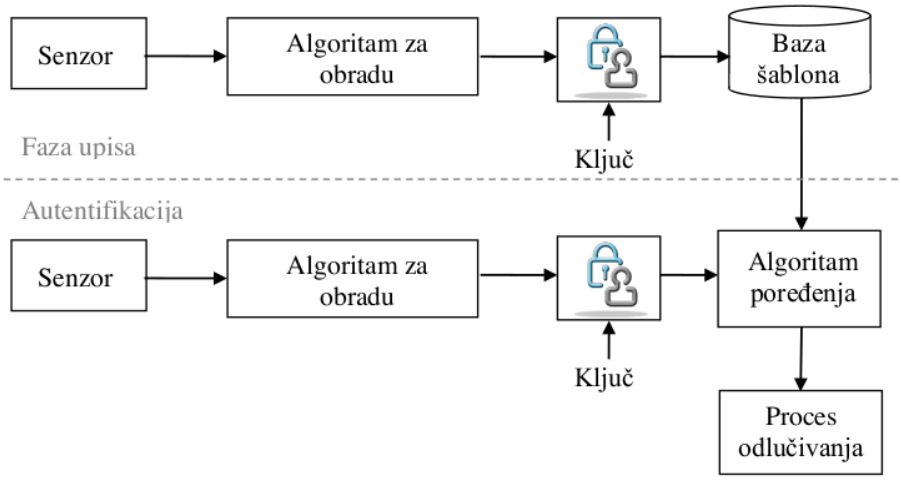


Slika 23 – Primena klasičnih šifarskih algoritama za zaštitu biometrijskog šablona

3.3.2. Transformacije obeležja u šablonu

Transformisanje izdvojenih obeležja u šablonu se u literaturi naziva još „Otkaziva/opoziva biometrija“ (engl. *Cancelable/revocable biometry*). Pristup transformacije specifičnih obeležja u šablonu, u osnovi je sličan pristupu šifrovanja klasičnim kriptografskim algoritmima. Na izvorni šablon se primenjuje funkcija koja ga menja i u izmenjenom obliku se čuva u bazi šablona. Kod kriptografskih sistema se koriste šifarski algoritmi za izmenu šablona, dok se u ovom pristupu koristi specifična transformaciona funkcija. Parametri funkcije se izvode iz nekog slučajnog ključa, tajnog ključa ili lozinke. Prednost

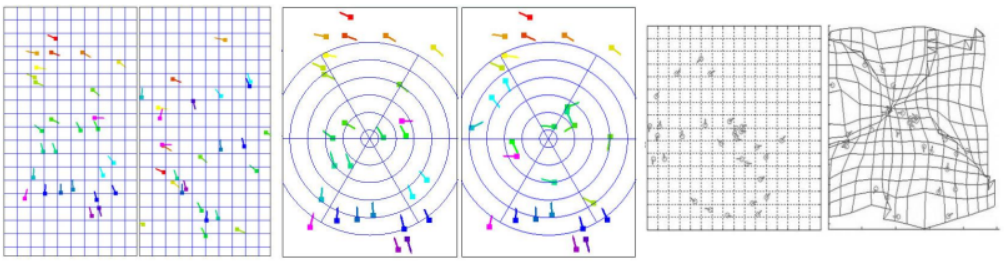
ovog pristupa je što se poređenje šablona radi u zaštićenom obliku, tako da tokom tog postupka šablon nije dostupan napadaču u njegovom izvornom obliku, što se može videti na slici 24. Međutim, ovakav način rada zahteva izmene u modulu poređenja, kako bi se omogućilo da se poređenje sprovodi u transformisanom domenu. Na osnovu vrste transformacione funkcije, ovaj pristup možemo podeliti u dve grupe [56]: invertibilne (u literaturi poznate još kao *Biometric salting*) i neinvertibilne transformacije.



Slika 24 – Pristup transformacije obeležja u šablonu

Invertibilne transformacije su reverzibilne, a sigurnost zaštićenog šablona svodi se na tajnost upotrebljenog ključa, pa ukoliko napadač dođe u posed tajnog ključa može da na osnovu zaštićenog šablona dobije izvorni oblik biometrijskih podataka. Neinvertibilne transformacije koriste jednosmerne funkcije, zbog čega je računski teško odrediti izvorni šablon na osnovu zaštićenog šablona, čak i ako su svi parametri transformacione funkcije poznati. Ako bi se transformacione funkcije poredile sa kriptografskim algoritmima, onda se može reći da su invertibilne transformacione funkcije slične šifarskim sistemima, a neinvertibilne funkcije slične heš funkcijama, s tim da ključ predstavlja parametar i utiče na rezultat funkcije sažimanja. Kao i kod primene klasičnih šifarskih sistema za zaštitu biometrijskog šablona i kod pristupa transformacije odabranih obeležja u šablonu, opozivost zaštićenog šablona se postiže promenom ključa. Sa aspekta bezbednosti biometrijske karakteristike i odgovarajućeg izvornog šablona, neinvertibilne transformacije obezbeđuju veću sigurnost, dok obe vrste transformacija obezbeđuju opozivost šablona. Međutim, performanse poređenja šablona neinvertibilne transformacije, obrnuto su srazmerne neinvertibilnosti njene funkcije transformacije. Zbog toga je teško napraviti neinvertibilnu funkciju koja istovremeno zadovoljava performanse biometrijskog sistema i sigurnost šablona.

Neinvertibilne transformacione funkcije se razlikuju u zavisnosti od biometrijske karakteristike i vrste obeležja koja se izdvajaju. Zajedničko za sve karakteristike je da transformacija mora biti otporna na varijabilnost biometrijske karakteristike. Kod otisaka prstiju koncept neinvertibilnih transformacija pozicije i ugla minucija otiska prsta je uveden u [58], a kasnije unapređen u [59], gde su predložene tri vrste transformacija: kartezijanska, polarna i funkcionalna (poznata i kao - savijanje površine). Kartezijanska transformacija se zasniva na predstavljanju otiska prsta i njegovih obeležja, u pravougaonom prostoru podeljenom na sektore - ćelije. Na osnovu ključa, transformaciona funkcija radi permutaciju ćelija, čime se dobija potpuno izmenjen raspored minucija. Sličan princip se primenjuje u polarnoj transformaciji, gde se otisak predstavlja u kružnom prostoru, podeljenom na više koncentričnih slojeva podeljenih u više sektora. Funkcionalna transformacija u [59] koristi prostornu raspodelu za premeštanje minucija, na osnovu vektorske funkcije polja električnog potencijala primenom parametara sa slučajnom raspodelom naelektrisanja i 2D modela Gausovih filtara gde se smer translacije izvodi iz gradijenta, a magnituda predstavlja stepen translacije. Efekat koji se postiže liči na površinu koja je presavijana, po čemu je ova funkcija dobila ime. Ilustracija sve tri transformacione tehnike data je na slici 25.



a) Kartezijanska transformacija b) Polarna transformacija c) Funkcionalna transformacija

Slika 25 – Neinvertibilne transformacione funkcije otiska prsta (preuzeto iz: a i b [56]; c [59])

3.3.3. Biometrijski kriptosistemi

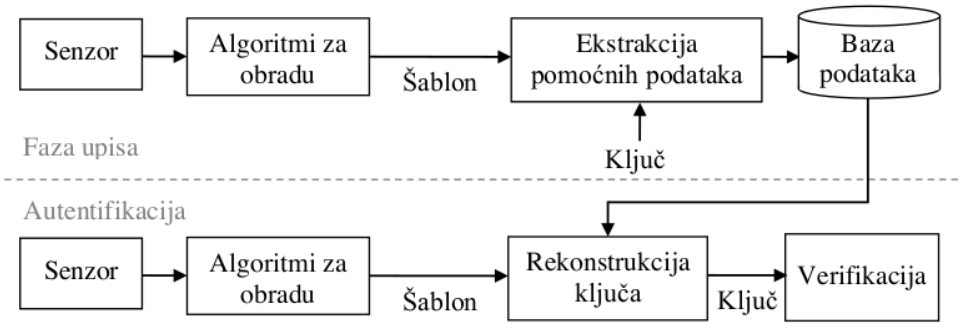
Kriptologija je nauka o razvoju, analizi i otkrivanju tajnih kodova i tehnika zaštite podataka, na osnovu matematičkih načela i implementacijom kriptografskih metoda. Kriptografija je oblast kriptologije koja izučava metode transformacija podataka za njihovo šifrovanje i dešifrovanje. Šifrovanje predstavlja postupak transformacije ulaznog podatka (otvoreni tekst), na osnovu niza funkcija i tajnog ključa, u zaštićeni oblik – šifrat. Sigurnost i tajnost sistema šifrovanja ne oslanja se na tajnovitost svog načina rada, već se bazira na tajnosti kriptografskog ključa. Iz tog razloga, generisanje i čuvanje kriptografskih ključeva je primarni sigurnosni izazov kriptografskih sistema. Razvojem biometrije i njenom

uspešnom primenom u funkciji autentifikacije, ona se nameće kao prirodno rešenje problema skladištenja i čuvanja tajni u kriptografskim sistemima – kriptografskih ključeva. Upravljanje ključevima smatra se najslabijim segmentom nekog kriptosistema, jer se sigurnost ključa obično oslanja na niži nivo bezbednosti, kao što su lozinke koje mogu biti zaboravljene ili ukradene i sl. Biometrijski generisan kriptografski ključ zavisi od biometrije korisnika, koja ujedno predstavlja izvor slučajnosti ključa i njegovo mesto čuvanja, što čini ceo sistem sigurnijim. U zavisnosti od načina ostvarivanja veze između biometrije i kriptografskih ključeva, biometrijski kriptosistemi se mogu podeliti na dva osnovna koncepta:

- povezivanje ključeva (engl. *key binding*) i
- generisanje ključeva (engl. *key generation*).

Zajednički problem svih biometrijskih kriptosistema je varijabilnost biometrijskih podataka, koja unosi grešku u kriptografski sistem. Problem varijabilnosti biometrijskih podataka je moguće prevazići mehanizmima rekonstrukcije i pomoćnim podacima (engl. *helper data*) u biometrijskim kriptosistemima. Prilikom faze upisa pomoćni podaci se generišu i čuvaju u bazi podataka, dok se pomoću njih prilikom autentifikacije radi rekonstrukcija ključa na osnovu uzorkovanih biometrijskih podataka. Pomoćni podaci nisu tajni i ne smeju otkrivati informacije o izvornom biometrijskom šablonu i kriptografskom ključu. Mnogo predloženih rešenja u literaturi mehanizam rekonstrukcije ključa bazira na kodovima za korekciju grešaka (engl. *error correction code* - ECC), poznate tehnike ispravljanja grešaka koje se javljaju prilikom prenosa podataka u telekomunikacijama. Pored ove tehnike, koriste se još i podesive funkcije filtra, korelacije ili kvantizacije [61].

Kod sistema povezivanja ključa, fuzijom biometrijskog šablona sa kriptografskim ključem, koji je nezavistan od biometrijskih podataka, dobijaju se pomoćni podaci i čuvaju se u bazi podataka ili u nekom drugom bezbednom okruženju. Ovi podaci ne otkrivaju informacije o povezanom ključu i biometrijskom šablonu, a računski je teško odrediti ključ ili šablon bez posedovanja odgovarajućih biometrijskih podataka. Prilikom autentifikacije, primenjuje se algoritam za rekonstrukciju ključa, koji na osnovu biometrijskog šablona i pomoćnih podataka rezultuje tajnim ključem, koji se zatim verifikuje. Koncept ovog sistema prikazan je na slici 26. Kako su kriptografski ključevi nezavisni od biometrijskih podataka, oni su opozivi. Međutim, prilikom promene ključa potrebno je ponovo izvršiti fazu upisa kako bi se generisali novi pomoćni podaci. U biometrijskim kriptosistemima povezivanja ključeva dominantna su dva pristupa: fazi povezanost (engl. *Fuzzy commitment scheme* - FCS) [62] i fazi trezor (engl. *Fuzzy vault* - FV) [63].



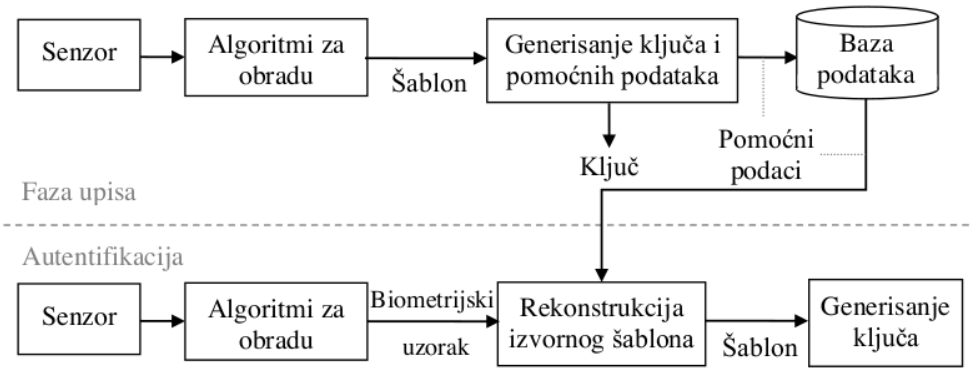
Slika 26 – Koncept povezivanja ključa u biometrijskim kriptosistemima

Fazi povezanost se koristi kada se šabloni mogu predstaviti sa binarnim nizom fiksne dužine. Tada se koristi kôd za korekciju grešaka iste dužine kao binarni zapis šablona, koji prethodno može biti generisan na osnovu tajnog ključa. XOR operacijom nad šablonom i kodom za korekciju grešaka dobija se vrednost koja se zove vektor razlike i istovremeno predstavlja zaštićeni biometrijski šablon. Vektor razlike i heš vrednost koda za korekciju grešaka se čuvaju u bazi podataka i predstavljaju pomoćne podatke. Prilikom autentifikacije, pseudo-kôd za korekciju grešaka se dobija XOR operacijom uzorkovanog šablona sa sačuvanim vektorom razlike. Ukoliko su uzorkovani šablon i izvorni šablon bliski, odnosno potiču od istih biometrijskih podataka, tada se dobija pseudo-kôd koji je dovoljno blizak izvornom kodu za korekciju grešaka i svojim algoritmom korekcije može da se obnovi u izvorni oblik. Heš funkcijom nad tako dobijenim kodom i poređenjem sa heš vrednošću koda iz pomoćnih podataka, utvrđuje se poklapanje. Ukoliko je u kôd za korekciju grešaka ugrađen tajni ključ, on se dekodovanjem uspešno rekonstruiše.

Fazi trezor ima sličan pristup problemu, kao kod šeme fazi povezanosti. Šablon korisnika se povezuje sa tajnim ključem, formirajući tako neuređen skup – fazi trezor, primenom polinomijalnog kodiranja i koda za korekciju grešaka. U formirani trezor se unose dodatni slučajni podaci, kako bi se prikrili oni pravi. Za generisanje kodnih reči koristi se Rid-Solomonov (engl. *Reed-Solomon*) algoritam, a sigurnost ovog pristupa leži u polinomijalnoj složenosti. Prilikom autentifikacije, ako je odgovarajući šablon dovoljno sličan izvornom, na osnovu njega i kodova za korekciju grešaka se može rekonstruisati ključ.

Postoji mnogo kriptografskih sistema koji omogućavaju sigurnost, ukoliko na svom ulazu imaju neki tajni niz sa ravnomernom raspodelom, koji se može pouzdano reprodukovati po potrebi. Kada bi se na osnovu biometrijskih karakteristika mogao generisati jedan takav niz, biometrija bi mogla da se primeni na čitav niz postojećih kriptografskih rešenja. Prvi biometrijski kriptosistemi za generisanje ključeva su bili bazirani na korisnički specifičnim šemama kvantizacije, gde su pomoćni podaci bili

granične vrednosti intervala kvantizacije [64]. Za generisanje kriptografskih ključeva iz podataka sa izraženim prisustvom šuma, kakvi su biometrijski podaci, u [65] je predloženo da se za generisanje ključeva koristi fazi ekstraktor (engl. *fuzzy extractors*). Izvorni biometrijski podaci nemaju ravnomernu raspodelu potrebnu za kriptografski ključ, pa se primenom fazi ekstraktora dobija ravnomerni slučajni niz na osnovu biometrijskog ulaza. Pomoćni podaci su u funkciji ekstraktora u vidu sigurnih skica (engl. *secure sketches*) i zaduženi su za stabilnost ključa prilikom svake njegove rekonstrukcije. Fazi ekstraktor je zadužen za generisanje kvalitetnog ključa na osnovu biometrijskog ulaza, a uskladišteni pomoćni podaci pomažu da se prilikom autentifikacije rekonstruiše niz istovetan onom koji je dobijen prilikom faze upisa. Koncept ovog sistema prikazan je na slici 27. U drugim pristupima, pomoćni podaci rešavanju problem promenljivosti šablona, pa se koriste za rekonstrukciju izvornog biometrijskog šablona, a na osnovu kog se onda generiše istovetni ravnomerni slučajni niz.



Slika 27 – Koncept generisanja ključa u biometrijskim kriptosistemima

Da bi biometrijski kriptografski ključ ispunio zahteve kriptosistema, mora da zadovolji odgovarajuće kriterijume: entropije, jedinstvenosti i stabilnosti. Entropija ključa je mera njegove snage i predstavlja količinu neodređenosti samog ključa iz ugla napadača. Statistički i računski ključ mora biti nepredvidiv, odnosno ne sme se razlikovati od slučajnog niza. Kada se ključ generiše na osnovu nekog skupa vrednosti, tada se entropija može lako izračunati kao binarni logaritam veličine tog skupa. Međutim, ukoliko se o skupu na osnovu kojeg se generiše neki slučajan niz znaju neke zakonitosti ili statističke informacije, to utiče na smanjenje entropije generisanog slučajnog niza, odnosno ključa. Biometrijski generatori ključeva koriste slučajnost iz biometrijske karakteristike za generisanje ključeva. U slučaju nekih biometrijskih karakteristika, njihova statistika u populaciji može umanjiti entropiju biometrije nekog korisnika, što za posledicu ima smanjenje entropije dobijenog ključa. Jedinstvenost ključa se oslanja na jedinstvenost same biometrijske karakteristike i odgovarajućeg biometrijskog šablona, a odnosi se na

nepostojanje kolizije. Jedan ključ mora odgovarati samo jednom korisniku, odnosno njegovoj biometrijskoj karakteristici koja je upotrebljena prilikom generisanja. Stabilnost ključa predstavlja njegovu nepromenljivost u odnosu na varijabilnost biometrijskog izvora podataka.

3.4. Multimodalni biometrijski kriptosistemi

Multimodalni biometrijski autentifikacioni sistemi značajno unapređuju performanse i tačnost autentifikacije, u odnosu na klasične biometrijske sisteme i ostale multibiometrijske sisteme, pa se od primene multimodalnosti u biometrijskim kriptosistemima očekuju slični pozitivni efekti. U biometrijskim autentifikacionim sistemima sjedinjavanje podataka moguće je postići na nivou svakog njegovog modula. Na osnovu kompleksnosti, sjedinjavanje podataka se često deli na dve kategorije: sjedinjavanje pre poređenja i sjedinjavanje nakon poređenja biometrijskih podataka. Sjedinjavanje podataka na nivou poređenja i donošenja odluke ne zahteva dodatnu kompleksnost već se svodi na jednostavno kombinovanje pojedinačnih rezultata i odluka. U takvim slučajevima se biometrijski šabloni nezavisno štite i čuvaju odvojeno u bazi podataka. Ukoliko baza podataka postane kompromitovana, napadač može doći u posed više biometrijskih karakteristika istog korisnika. Mnogo veća kompleksnost se može postići ujedinjavanjem dve karakteristike u jednu složenu, nego kada svaka nezavisno čini deo sistema. Zbog toga se predlaže primena multimodalnih biometrijskih kriptosistema, gde se sjedinjavanje biometrijskih karakteristika može izvršiti na nivou senzora u slučajevima homogenih biometrijskih karakteristika, ali se u većini predloženih rešenja to radi na nivou izdvajanja obeležja. Više modaliteta tada formira jedan šablon, koji se štiti već opisanim tehnikama.

Heterogeno sjedinjavanje karakteristika je teško postići kada su u pitanju različite biometrijske karakteristike ili različiti algoritmi za izdvajanje karakteristika, zbog nekompatibilnosti reprezentacije njihovih karakteristika. U fazi povezivanju koristi se binarna reprezentacija, gde se poređenje dva šablona radi merenjem Hemingovog rastojanja. U biometrijskim kriptosistemima baziranim na šemi fazi trezora koristi se skup elemenata predstavljenih polinomijalnom funkcijom i određuje se skup različitih elemenata kao mera različitosti. Da bi više modaliteta formiralo jedan integrisani biometrijski šablon, potrebno je da se primene algoritmi za konverziju različitih biometrijskih reprezentacija u jednu zajedničku. Među prvim pionirskim pokušajima da se napravi multimodalni biometrijski kriptosistem, u [66] je izvršeno sjedinjavanje na nivou obeležja biometrije lica i otisaka prstiju. Primenom geometrijskih transformacija minucije su transformisane u vektore fiksnih dužina, dok je ista reprezentacija postignuta za predstavljanje karakteristika lica pomoću SVD metode (engl. *Singular Value Decomposition*). U [67] predložen je multibiometrijski kriptosistem u kojem su biometrijski šabloni reprezentovani binarnim

nizom i skupom elementa, za dužicu oka i otisak prsta, respektivno. Ove dve nekompatibilne biometrijske reprezentacije su objedinjene tako što je binarni niz podeljen u veliki broj segmenata, koji su svaki ponaosob obezbeđeni pomoću šeme fazi povezivanja. Ključevi korišćeni za svaki segment, predstavljeni su kao dodatni elementi skupa koji formira fazi trezor na osnovu otisaka prstiju. U [68] predložen je opšti okvir za formiranje multibiometrijskih kriptosistema sa heterogenim karakteristikama. Takođe, razmatrani su problemi pri praktičnoj implementaciji u slučajevima reprezentacija u binarnom i skupovnom obliku. Predložena su tri algoritma za transformaciju reprezentacije: skalarnih vektora u binarni niz, elemente skupa u binarni niz i za transformaciju binarnog niza u elemente skupa. Usaglašavanjem reprezentacija biometrijskih šablona, razmatraju se njihove implementacije u postojećim rešenjima za biometrijske sisteme za povezivanje ključa: fazi povezivanju i fazi trezoru.

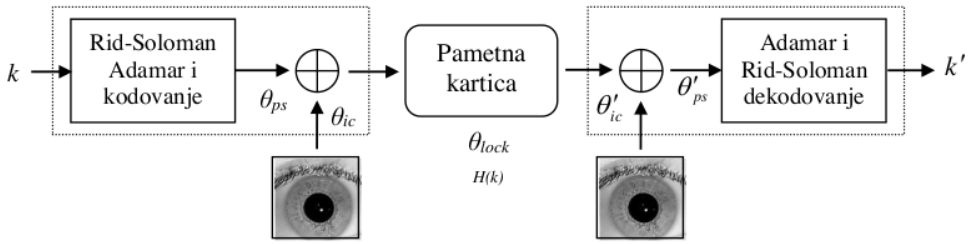
4. Jedna klasa biometrijskih kriptosistema zasnovana na konvolucionim neuronskim mrežama

4.1. Prethodni radovi

Prvi sofisticirani pristup, koji objedinjuje biometriju i kriptografiju, predložen je u [69] i [70]. Šema je bazirana na otiscima prstiju, koji su se tada smatrali najpouzdanijom biometrijskom karakteristikom. Takođe, ovaj pristup je prvi koji je potpuno realizovan i postao komercijalno dostupan pod zaštićenim nazivom *Bioscrypt* (kasnije poznati kao *Mytec 1* i *Mytec 2*). Za izdvajanje biometrijskih obeležja koristi se Furijeova transformacija, a za dobijanje koda metoda izbora većine. Tako dobijen kôd koristi se za zaštitu predefinisanog kriptografskog ključa, čime se uspostavlja veza između ključa i biometrije. Među prvim pristupima baziranim na karakteristikama ponašanja je hibridni sistem za povećanje sigurnosti lozinki, predstavljen u [71]. Na osnovu dinamike kucanja na tastaturi, merenjem brzine kucanja i vremenskog perioda između dva tastera, ovaj sistem generiše kratak binarni kôd, koji se zatim kombinuje sa lozinkom, čime se povećava njena entropija, a ukupan broj svih mogućnosti uvećava se i do 2^{15} puta. Sličnu metodologiju isti autor je primenio za biometrijsku karakteristiku govora [72], gde je uspešno generisan ključ dužine 46 bita, uz FRR od oko 12%. U [73] definisane su 43 karakteristike potpisivanja, koje su kvantizovane i njihovim spajanjem je generisan binarni niz. Prosečna entropija ključa koja je ostvarena iznosi 40 bita, uz 28% FRR.

Pristup predložen u [74] koristi dužicu oka za koju se navodi da poseduje najveću entropiju od svih do sada istraženih biometrijskih karakteristika. U radu je predstavljen način formiranja kriptografskog ključa pomoću koda dužice oka i koda za ispravljanje grešaka metodom izbora većine. Dobijeni kôd za ispravljanje grešaka i heš vrednost biometrijskog šablona, skladište se u zaštićenom obliku i služe za rekonstrukciju ključa. Na izraženu korelaciju između biometrijskih podataka i koda za ispravljanje grešaka, usled upotrebe metode izbora većine, ukazano je u [18]. Primena fazi logike u biometriji prvi put je predstavljena u [62], gde je razvijena šema fazi povezivanja, koristeći osnove kriptografije i tehnika za korekciju grešaka. Ovaj rad predstavlja generalizaciju i unapređenje pristupa koji je predložen u [74], sa unapređenom sigurnošću i kraćim kodovima za korekciju greške. U [18] je prezentovan praktičan i siguran način za primenu biometrije dužice oka u kriptografskim sistemima, baziran na fazi povezivanju. Koncept predloženog pristupa je prikazan na slici 28. Kôd dužice oka (engl. *iris code*) je dužine 2048 bita i formira se demodulacijom slike dužice oka sa kompleksnim 2D Gabor vejvletima. Razlika koja se javlja prilikom poređenja dva uzorka iste dužice, predstavlja grešku sistema. Ove greške se mogu podeliti u dve grupe: slučajne greške nastale usled šuma senzora, izobličenja dužice i sl., i greške u nizu (engl. *burst errors*) nastale usled

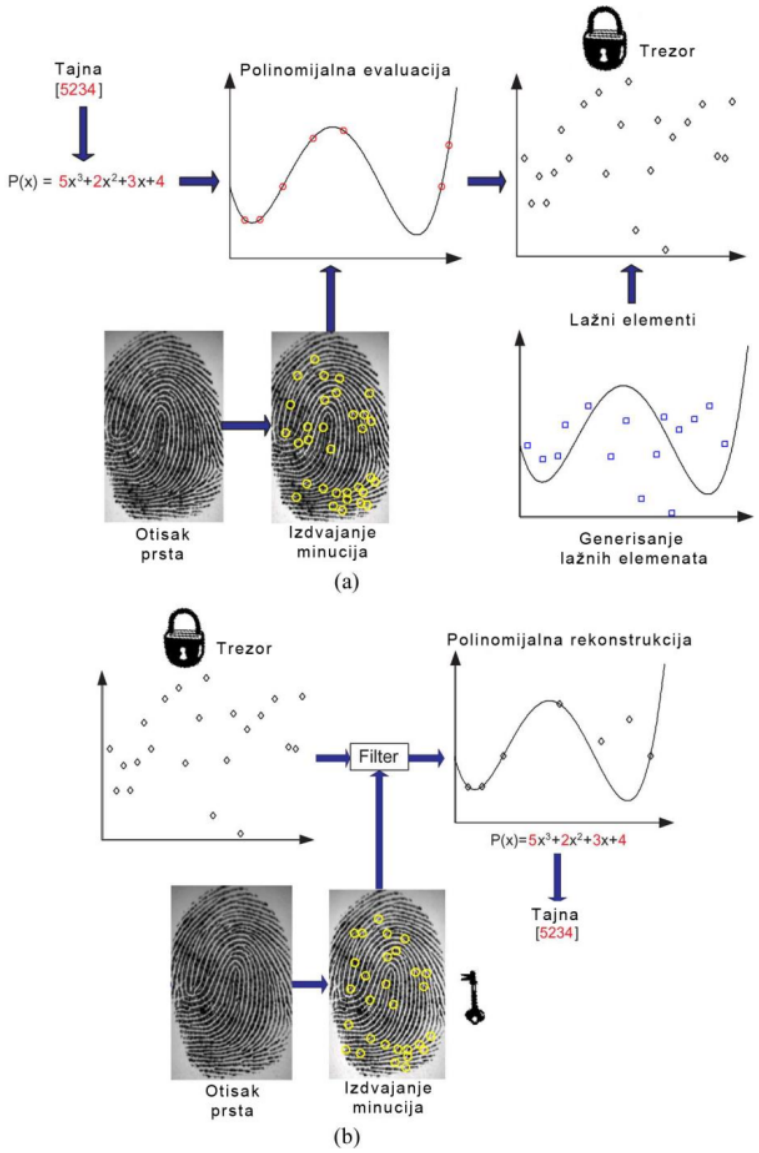
nedetektovanih trepavica i odsjaja. Algoritam za dobijanje koda dužice ima mehanizme za detekciju kapaka i trepavica, koji generišu masku nad odgovarajućim bitima, ali nije apsolutno tačan. Na uzorku od 70 dužica oka utvrđeno je da prosečno 13,69% bita koda dužice oka sadrži grešku usled odsjaja ili trepavica. Višestrukim uzorkovanjem i primenom metode izbora većine, grešku je moguće smanjiti na 9,36% (5 uzoraka). Za prevazilaženje ovog problema, osnovu predloženog sistema čini primena dve tehnike za ispravljanje grešaka. Na pojedinačne greške na nivou bita, primenjuju se Adamarovi (fr. *Hadamard*) kodovi, a usnopljene greške u sekvencijalnom nizu bita koriguju se Rid-Solomonovim kodovima. Kôd dužice istog oka prilikom dva nezavisna uzorkovanja razlikuje se od 10% do 20%, dok je ta razlika između dva različita oka između 40% i 60%. Primenjeni kodovi za korekciju grešaka moraju izvršiti korekciju razlike u kodu dužice koja se javlja između dva ista oka, dok to ne sme biti u mogućnosti da uradi za kodove dužica različitih očiju. Eksperimentalno je dokazana stabilnost ključa od 99,5%, a generisan je ključ dužine do 140 bita, što omogućava njegovu primenu za AES algoritam sa 128-bitnim ključem.



Slika 28 – Fazi povezivanje dvoslojnom metodom kodova za korekciju grešaka

Primena polinomijalnog kodiranja i Rid-Solomonovog koda za korekciju grešaka predložena je u [63], čime se ostvaruje povezivanje šablona korisnika sa tajnim ključem i formira neuređen skup – fazi trezor. Sigurnost ovog pristupa zasnovan je na polinomijalnoj složenosti, odnosno nemogućnosti polinomijalne rekonstrukcije koja je specijalan slučaj Rid-Solomonovog koda za korekciju grešaka. Neuređeni skup A (npr. minucije otiska prsta) koristi se za zaštitu tajnog ključa k. Primenom polinomijalnog kodiranja, generiše se polinom P koji implementira tajni ključ u vidu koeficijenata $(P \leftarrow k)$. Zatim se svi elementi skupa A izračunavaju sa polinomom $P(A)$, čime se projektuju na polinomijalnu krivu. Na kraju se dodaje veliki broj lažnih elemenata (engl. *chaff points*), kako bi se prikrili oni pravi, formirajući tako trezor V_A. Na slici 29. a) ilustrovan je princip formiranja fazi trezora, a na slici 29. b) postupak rekonstrukcije ključa. Ukoliko se neki drugi skup B preklapa u značajnoj meri sa skupom A, određuju se zajednički elementi i pomoću koda za korekciju grešaka moguće je odrediti P i rekonstruisati tajni ključ k, odnosno otključati trezor V_A. U slučaju da skupovi A i B imaju mali broj zajedničkih elemenata, nije moguće odrediti P i k. Sigurnost fazi trezora zavisi od broja lažnih elemenata u V_A. Što je veći njihov broj, to je veća sigurnost P, jer lažni elementi zajedno sa pravim formiraju veliki broj lažnih polinomijalnih funkcija, sličnih P. Iz toga sledi da je broj lažnih elemenata

mnogo veći od broja pravih. Dužina tajnog ključa *k* nema uticaja na sigurnost predloženog sistema. Prednost ove metode povezivanja tajnog ključa sa biometrijom, u odnosu na fazi povezivanje, je u njenoj nezavisnosti od redosleda prikupljenih obeležja, što je u slučaju minucija od presudne važnosti.



Slika 29 – Fazi trezor šema za otiske prstiju (modifikovano iz [67])

Na osnovu opisanog koncepta u [75] predložen je sistem zaštite pametnih kartica pomoću biometrije otisaka prstiju, gde je u idealnim uslovima moguće zaštititi ključ dužine do 265 bita, uz EER od 30%. Empirijski je dokazano da je 2^{69} puta napadaču teže da

otkrije ključ od legitimnog korisnika. Sistem baziran na fazi trezoru i otiscima prstiju za zaštitu ključeva dužine od 128 bita uz GAR do 96%, opisan je u [76], dok su u [77] i [78] predloženi sistemi bazirani na dužici oka i otisku dlana uz ostvarene ključeve dužine 256 i 292 bita, respektivno.

Najpopularnije i najčešće korišćene tehnike za poređenje otisaka prstiju koriste minucije, dok se informacije o teksturi otiska u literaturi najčešće primenjuju samo za klasifikaciju otisaka prstiju. Informacije o teksturi otisaka prstiju sadrže podatke o specifičnim prostornim učestanostima, orijentaciji i fazi, pa je njihovom dekompozicijom moguće ostvariti neophodnu diskriminativnost. Za svaki piksel slike moguće je ustanoviti korelaciju u odnosu na dominantnu lokalnu orijentaciju i koherenciju lokalne teksture. Specifična obeležja za poređenje otisaka predstavljaju ove kvantitativne mere, koje obezbeđuju potrebnu diskriminativnost, što je ujedno prva postavljena hipoteza ovog rada da se informacije o teksturi otisaka prstiju mogu upotrebiti za formiranje biometrijskog kriptosistema. Pionirska šema za ekstrakciju obeležja iz teksture otisaka predložena je u [79] i poslužila je kao inspiracija za razvoj predloženog biometrijskog kriptosistema u ovom radu. U šemi se određuje region od interesa u odnosu na referentnu tačku uzorkovanog otiska prsta. Region od interesa se deli na i sektora, gde je ukupan broj određen jednačinom $i=B\cdot k$, gde B predstavlja ukupan broj staza, a k broj sektora jedne staze. Sektor S_i određuje se na osnovu parametara (r,θ):

$$S_i = \{(x,y) | b(T_i+1) \le r < b(T_i+2), \theta_i \le \theta < \theta_{i+1}, 1 \le x \le N, 1 \le y \le M\} \quad (19)$$

$$T_i = i \; div \; k \quad (20)$$

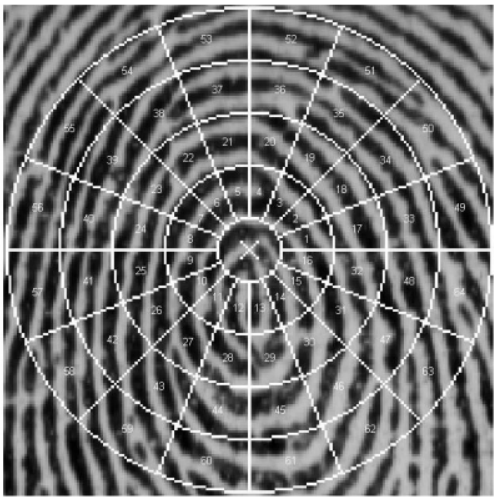
$$\theta_i = (i \bmod k) \times (2\pi / k) \quad (21)$$

$$r = \sqrt{(x-x_c)^2 + (y-y_c)^2} \quad (22)$$

$$\theta = \tan^{-1}((y-y_c)/(x-x_c)) \quad (23)$$

gde su: (x,y) koordinate piksela slike otiska prsta, (x_c,y_c) koordinate za prethodno utvrđenu referentnu tačku, M x N dimenzije ulazne slike, a b označava širinu svake staze izraženu brojem piksela. Princip izdvajanja regiona od interesa i formiranje sektora prikazan je na slici 30. Parametri B, k i b zavisni su od rezolucije i veličine uzorkovanih slika otisaka prstiju. Širinu staze potrebno je odrediti tako da prosečno obuhvata jedan par papilarnih linija, što u slučaju slike rezolucije 500dpi iznosi 20px. Na taj način ostvaruje se da svaki sektor poseduje lokalnu informaciju o promeni u toku šare, kao što je minucija. Veća širina staze postiže negativan efekat da globalne informacije modulišu lokalne, čime se

specifična obeležja gube. Zbog pomenutog efekta, sve staze neophodno je segmentirati u 16 sektora. Tekstura unutrašnje površine kruga, u odnosu na referentnu tačku, poseduje lošu koherentnost i ne primenjuje se prilikom izdvajanja obeležja. Od tako izdvojene 4 staze, gde svaka sadrži po 16 sektora, uspostavlja se niz od 64 sektora na osnovu kojeg se formira vektor obeležja.



Slika 30 – ROI podeljen na sektore

Vektor obeležja formira se od skupa karakterističnosti izdvojenih iz lokalnih informacija svakog sektora. Time se postiže da svaki sektor ponaosob sadrži lokalne informacije, dok se zbog određenog redosleda sektora mogu izdvojiti nepromenljive globalne veze između lokalnih tekstura. Lokalne diskriminatorne informacije svakog sektora potrebno je dekomponovati u odvojene komponente. Banka Gabor filtra je dobro poznata tehnika za izdvajanje korisnih informacija u kanalima specifičnih propusnih opsega, kao i za razlaganje ovih informacija u biortogonalne komponente, u smislu prostornih frekvencija. Pomoću Gaborovih filtara eliminiše se šum i izdvaja struktura papilarnih linija određene orijentacije. Gaborov simetrični filtar u prostornom domenu može se predstaviti opštim oblikom:

$$G(x,y;f,\theta) = e^{\left[-\frac{1}{2}\left(\frac{x'^2}{\delta_x^2}+\frac{y'^2}{\delta_y^2}\right)\right]}\cos(2\pi x' f) \tag{24}$$

$$x' = x\sin\theta + y\cos\theta \tag{25}$$

$$y' = x\cos\theta - y\sin\theta \tag{26}$$

gde f predstavlja prosečnu učestanost papilarnih linija izračunatu na osnovu R – prosečnog rastojanja između dve linije ($f=1/R$), θ je primenjeni ugao u filtru, a $\delta_{x'}$ i $\delta_{y'}$ su prostorne konstante Gausove krive uzduž x' i y' ose koje približno iznose $R/2$. Na normalizovanom regionu od interesa sprovodi se konvolucija Gaborovim filtrima za osam različitih vrednosti ugla θ od 0° do 157,5° u koracima od 22,5°. Iz slike otiska prsta koja konvoluira sa filtrom ugla $\theta=0°$, izdvajaju se sve brazde paralelne sa x osom, dok se primenom različitih uglova u filtru izdvajaju brazde odgovarajućeg radijalnog pomeraja, što se može videti na slici 31. Na taj način, svakim od osam filtara moguće je izdvojiti deo lokalnih obeležja, dok skup svih osam konvoluiranih slika sadrži globalne informacije o teksturi otiska prsta.



Slika 31 – Region od interesa konvoluiran sa Gaborovim filtrom u osam uglova: 0°, 22,5°, 45°, 67,5°, 90°, 112,5°, 135° i 157,5° (preuzeto iz [79])

Vektor obeležja jednog otiska prsta, koji su autori nazvali *FingerCode*, skup je obeležja dobijenih od svakog sektora ponaosob. Ova obeležja sadrže kako globalne informacije o ispupčenjima i udubljenjima otiska, tako i lokalne karakteristike. Na osnovu apsolutne prosečne devijacije svakog sektora za sve filtrirane slike u osam uglova, utvrđuju se elementi vektora obeležja. Za svaki sektor, nivo sive ima specifičnu vrednost, odnosno predstavlja obeležje tog sektora. Vektor obeležja $V_{i\theta}$ jednog otiska prsta predstavlja skup obeležja dobijenih iz svih osam filtriranih slika, odnosno apsolutnu prosečnu devijaciju, što se može predstaviti jednačinom:

$$V_{i\theta} = \frac{1}{n_i}\left(\sum_{n_i}\left|F_{i\theta}(x,y) - P_{i\theta}\right|\right) \tag{27}$$

gde je: $i \in \{1,2,...,64\}$ redni broj sektora; n_i je broj piksela sektora S_i; $F_{i\theta}(x,y)$ referiše na filtriranu sliku uglom θ za sektor S_i, gde je $\theta \in \{0°, 22,5°, 45°, 67,5°, 90°, 112,5°, 135° \text{ i } 157,5°\}$; $P_{i\theta}$ predstavlja prosečnu vrednost svih piksela filtrirane slike $F_{i\theta}$ sektora S_i.

Pored varijabilnosti obeležja, koje su posledica elastičnih osobina prsta, veliki izazov predstavlja poravnanje otisaka prilikom poređenja. Kako bi se izvršilo poravnanje otisaka, odnosno izdvojenih obeležja, neophodno je pronaći rešenje za problem translacije i različite rotacije prilikom akvizicije. Primenom referentne tačke kao centralnog orijentira, u odnosu na koju se segmentira region od interesa i deli na sektore iz kojih se izdvajaju obeležja, rešava se problem translacije otisaka. Neosetljivost sistema na različitu rotaciju otisaka postignuta je primenom tehnike cikličnih rotacija obeležja u vektoru. Na taj način se prilikom poređenja sprovodi simulacija rotiranja otiska prsta radijalnim pomerajem obeležja u koracima od 22,5° u odnosu na referentnu tačku. Kako bi se obezbedila dodatna neosetljivost na rotaciju, u predloženom rešenju prilikom faze upisa identiteta formiraju se dva šablona na osnovu izdvojenih obeležja otiska prsta, s tim da se drugi šablon formira na osnovu izdvojenih obeležja otiska zarotiranog za 11,25° u odnosu na referentnu tačku. Prilikom faze autentifikacije, priloženi uzorak se upoređuje sa svakom cikličnom permutacijom obeležja u oba sačuvana šablona. U ovom biometrijskom sistemu poređenje otisaka sprovodi se postupkom utvrđivanja najmanjeg Euklidovog rastojanja svih permutacija obeležja oba šablona sa priloženim uzorkom i donošenjem odluke na osnovu definisane granične vrednosti. U tabeli 4. prikazani su ostvareni rezultati. Baza otisaka prstiju je formirana na Univerzitetu „Mičigen stejt“ u čemu je učestvovalo 167 dobrovoljaca koji su dali otiske 4 prsta na optičkom skeneru. Iako su otisci pažljivo uzorkovani sa što manjom rotacijom i translacijom prsta, oko 4% otisaka je kasnije uklonjeno iz baze, zato što nisu zadovoljavali zadate kriterijume u pogledu kvaliteta uzorka ili je referentna tačka bila previše blizu ivice slike.

Tabela 4 – FAR i FRR vrednosti ostvarene u [79]

Granična vrednost	FAR [%]	FRR [%]
30	0,10	19,32
35	1,07	7,87
40	4,59	2,83

Biometrijski kriptosistemi na osnovu šeme fazi povezivanja primenjuju jednostavne principe kodova za ispravljanje grešaka u kombinaciji sa logičkom operacijom XOR, ali je njihova primena ograničena na binarne nizove fiksne dužine, što nije slučaj u postojećim algoritmima za poređenje otisaka prstiju. Kod sistema koji koriste minucije, broj detektovanih obeležja varira prilikom svakog uzorkovanja. Princip formiranja vektora obeležja *FingerCode* na osnovu segmentacije ROI u fiksni broj sektora, obezbeđuje prvi preduslov u vidu neophodne fiksne dužine obeležja. Drugi preduslov, koji se odnosi na

binarnu reprezentaciju obeležja, moguće je ostvariti njihovom kvantizacijom na osnovu nekih graničnih vrednosti. U [80], [81] i [82] predloženi su načini formiranja XOR biometrije otisaka prstiju i demonstrirane su kvantizacije svakog elementa vektora obeležja kodovanjem pomoću jednog bita. Imajući u vidu da su elementi vektora obeležja $V_i \in \{0,1,...,255\}$, za kvantizaciju pomoću jednog bita važi:

$$B_i = \begin{cases} 1, & ako\ je\ V_i > T \\ 0, & ako\ je\ V_i \leq T \end{cases} \tag{28}$$

gde B_i predstavlja binarnu reprezentaciju obeležja, dok je T izabrana granična vrednost kvantizacije. Ovim pristupom, uz ostale nepromenjene parametre formiranja vektora obeležja, moguće je ostvariti biometrijske šablone dužine 512 bita.

U [80] je koncipirano izdvajanje obeležja pomoću dva nezavisna algoritma na osnovu direkcionih polja i primene Gaborovih filtara na osnovu algoritma iz [79], koji rezultuju sa obeležjima od po 512 i 1024 elemenata. Prostom konkatenacijom vektori se spajaju i kvantizuju na osnovu dinamički određene srednje vrednosti svakog bloka koja se koristi kao granična vrednost. Od tako dobijenog niza izvaja se 511 bita najveće pouzdanosti, koji formiraju šemu fazi povezivanja. Prezentovani rezultati u tabeli 5. ostvareni su na osnovu baze otisaka prstiju FVC2000 DB2 [10] formirane 2000. godine za takmičenje dobavljača opreme (engl. *Fingerprint Vendor Competition*). Bazu sačinjava 800 otisaka prikupljenih kapacitivnim senzorom, a svaki identitet je reprezentovan sa osam otisaka. Dimenzije slika su 256x364px, dok je rezolucija svake 500dpi. Šest otisaka svakog identiteta je korišćeno prilikom faze upisa, a dva prilikom verifikacije. Rezultati su ostvareni na kompletnoj bazi otisaka, a autori su ukazali na problem određenog broja otisaka koji nisu adekvatni za tehnike koje su bazirane na karakteristikama teksture otisaka prstiju.

Tabela 5 – FAR i FRR vrednosti ostvarene u [80]

Dužina ključa [bita]	**FAR [%]**	**FRR [%]**
85	9,9	2,5
76	5,4	5,2
67	5,2	5,5

Unapređeni koncept šeme fazi povezivanja predložen je u [81], gde su prikazane kvantizacije kodovanjem s jednim i dva bita svakog elementa vektora obeležja, čime su ostvarene dužine šablona od 512 i 1024 bita, respektivno. Vektor obeležja je zasnovan isključivo na primeni Gaborovih filtara na osnovu algoritma iz [79]. U prvoj konfiguraciji predloženog biometrijskog sistema primenjuje se kvantizacija jednim bitom, a granična vrednost se dinamički određuje na nivou svakog uzorka. Nakon uzorkovanja i uspešnog

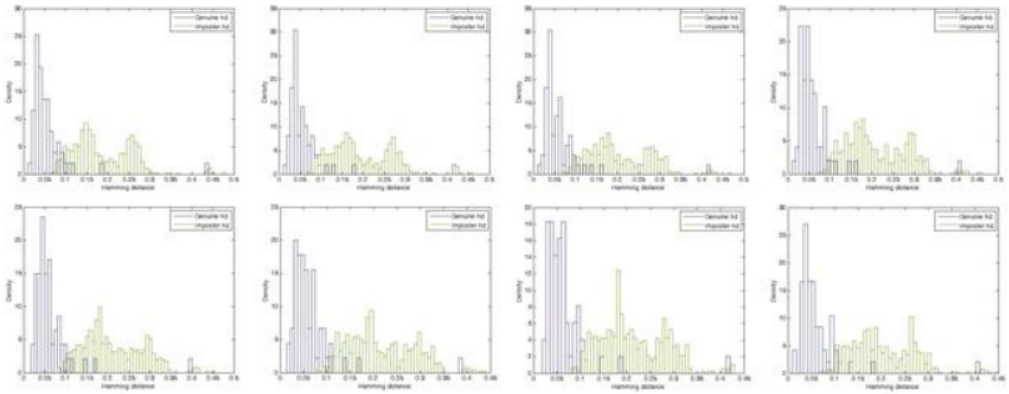
izdvajanja skupa obeležja na osnovu svih sektora, određuje se medijana tog skupa i ona predstavlja graničnu vrednost T za kvantizaciju na osnovu jednačine 28. U odnosu na statičke principe određivanja granične vrednosti, eksperimentalnim testiranjem uočeno je da dinamičko određivanje granične vrednosti rezultira manjim vrednostima FAR i FRR grešaka u ovom konceptu. Iako je sprovedena normalizacija slika, u izvesnoj meri se zadržava interklasna varijabilnost kao posledica različite sile pritiska prsta na senzor, što rezultuje različitim uzorkovanim intenzitetom.

Sprovedenom kvantizacijom s jednim bitom, generisani su binarizovani šabloni iste dužine kao izvorni vektori obeležja. Zbog povećanja diskriminativnosti i dužine šablona, s ciljem da se omogući primena veće dužine kriptografskih ključeva, predložena je unapređena tehnika za kvantizaciju, koja svaki element vektora obeležja koduje sa dva bita. Tehnika se zasniva na tri granične vrednosti, koje definišu četiri kvantizaciona opsega. Prvo je potrebno odrediti graničnu vrednost T_2 pronalaženjem medijane skupa vektora obeležja, kao u tehnici kvantizacije jednim bitom. Podelom skupa vektora obeležja u dva podskupa na osnovu granične vrednosti T_2, postupak se ponavlja nad svakim podskupom kako bi se odredile preostale dve granične vrednosti T_1 i T_3. Na osnovu utvrđenih svih graničnih vrednosti, sprovodi se kvantizacija svakog elementa t vektora obeležja na osnovu:

$$(B_i)_t = \begin{cases} 00, & ako\ je\ (V_i)_t \le (T_1)_t \\ 01, & ako\ je\ (T_1)_t < (V_i)_t \le (T_2)_t \\ 10, & ako\ je\ (T_2)_t < (V_i)_t \le (T_3)_t \\ 11, & ako\ je\ (V_i)_t > (T_3)_t \end{cases}. \qquad (29)$$

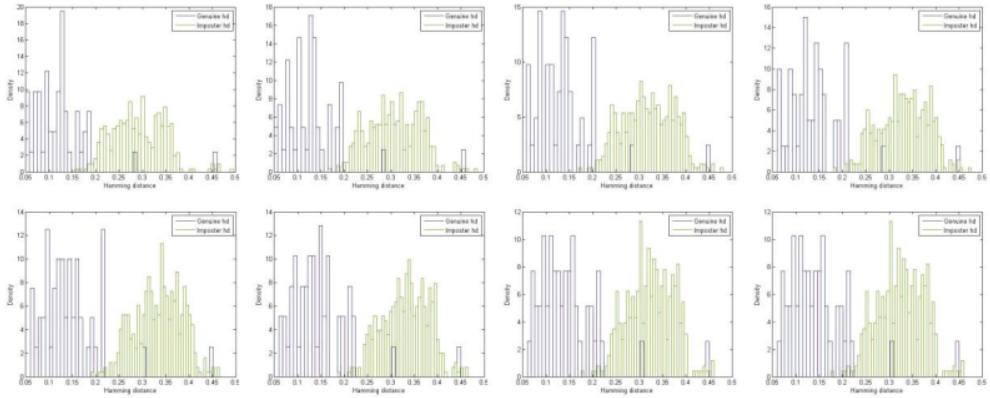
Kodovanje vektora obeležja sa 2 bita daje bolje rezultate, što se može videti poređenjem rezultujućih raspodela na slikama 32 a) i 33 a). Ujedno, primenom kodovanja sa 2 bita postiže se dvostruko veća dužina binarne digitalne reprezentacije otiska prsta, što doprinosi većoj dužini kriptografskog ključa za implementaciju u biometrijskom kriptosistemu. U cilju povećanja diskriminativnosti binarnih biometrijskih šablona, statističkim tehnikama moguće je odrediti stepen pouzdanosti svakog bita u šablonu. Ove tehnike moguće je primeniti zahvaljujući obučavajućem skupu, koji se sastoji od svih otisaka prstiju korišćenih prilikom faze upisa. Prilikom formiranja konačnog šablona isključuju se najnepouzdaniji biti, a njihove pozicije u šablonu se čuvaju kao vid pomoćnih podataka u biometrijskog bazi, kako bi se isti postupak primenio na uzorku prilikom autentifikacije. Pomoćni podaci ove vrste ne otkrivaju nikakve informacije o biometrijskim obeležjima i mogu se bez posebnih mera zaštite čuvati. Predložena je statistička tehnika bazirana na Bajesovoj teoremi utvrđivanja aposteriornih verovatnoća i greške sistema. Testirano je više scenarija u pogledu broja bita koji se odbacuju, a pregled različitih raspodela Hemingovog rastojanja nakon primene tehnike odstranjivanja nepouzdanih bita

na šablonu dužine 512 prikazani su na slici 32, dok je na slici 33 prikazana ista raspodela na šablonu dužine 1024 bita.



a) Početno stanje - 0 bita b) 32 bita c) 64 bita d) 96 bita e) 128 bita f) 160 bita g) 196 bita h) 224 bita

Slika 32 – Raspodela Hemingovog rastojanja sa primenom tehnike odstranjivanja nepouzdanih bita na šablonu dužine 512 bita (preuzeto iz [81])

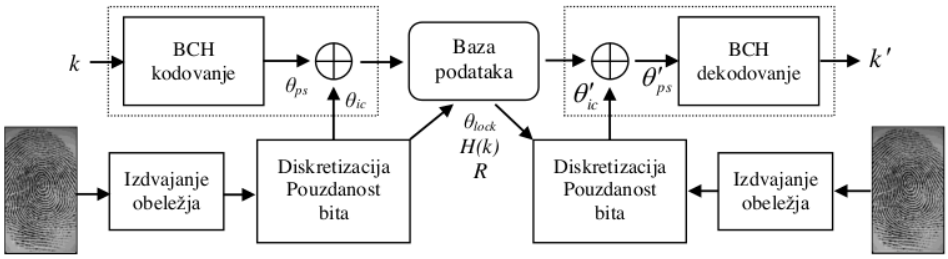


a) Početno stanje - 0 bita b) 64 bita c) 128 bita d) 196 bita e) 256 bita f) 320 bita g) 384 bita h) 512 bita

Slika 33 – Raspodela Hemingovog rastojanja sa primenom tehnike odstranjivanja nepouzdanih bita na šablonu dužine 1024 bita (preuzeto iz [81])

Finalni biometrijski šablon sa izuzetim nepouzdanim bitima, primenjen je za formiranje biometrijskog kriptosistema na osnovama šeme fazi povezanosti i tehnike za korekciju grešaka, gde je kao osnova poslužio sličan kriptosistem [18] koji koristi dužicu oka. Konceptualna šema je prikazana na slici 34. Na kriptografski ključ k primenjuje se izabrana tehnika za ispravljanje grešaka, što rezultuje pseudo-kodom θ_{ps} iste dužine. Tako dobijena dva binarna niza spajaju se logičkom operacijom ekskluzivno ILI i formiraju kôd θ_{lock}, koji predstavlja zaštićeni biometrijski šablon ili kriptografski ključ.

$$\theta_{lock} = \theta_{ps} \oplus \theta_{ic} \tag{30}$$



Slika 34 – Koncept FCS sa otiscima prstiju (preuzeto iz [81])

Podaci koji se čuvaju u bazi podataka biometrijskog sistema za svaki identitet, sastoje se od: zaštićenih šablona θ_{lock}, heš vrednosti ključeva $H(k)$ i pozicija eliminisanih bita R. U postupku faze verifikacije, odnosno rekonstruisanja ključeva, na kôd θ'_{ic} koji predstavlja binarnu reprezentaciju uzorka otiska prsta i zaštićeni kôd θ_{lock} iz baze podataka primenjuje se ista logička operacija kako bi se dobio pseudo-kod θ'_{ps}, na osnovu formule:

$$\theta'_{ps} = \theta_{lock} \oplus \theta'_{ic} = \theta_{ps} \oplus \varepsilon\,. \tag{31}$$

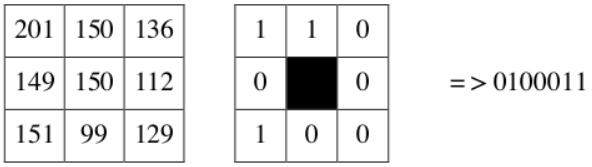
Ukoliko otisci prstiju koji se porede potiču iz istog biometrijskog izvora, tehnike za korekciju grešaka bi trebalo da eliminišu grešku ε koja se javlja usled unutarklasne varijabilnosti podataka. Na taj način moguće je rekonstruisati ključ k, a njegova verifikacija sprovodi se upoređivanjem dobijene heš vrednosti sa onom iz baze podataka. U tabeli 6. navedeni su rezultati predloženog biometrijskog kriptosistema baziranog na teksturi otisaka prstiju. Predloženi koncept testiran je na bazi otisaka prstiju FVC2002 DB2 [10]. Baza sadrži 800 otisaka prstiju prikupljenih optičkim senzorom, od čega je svaki identitet reprezentovan sa osam otisaka, rezolucije 569dpi i dimenzija 296x560px.

Tabela 6 – FAR i FRR vrednosti ostvarene u [81]

Dužina ključa [bita]	**FAR [%]**	**FRR [%]**
123	0	3,33
133	0	20

Hibridni sistem izdvajanja obeležja koncipiran na objedinjavanju dva nezavisna algoritma za izdvajanje iz [80], unapređen je u [82], gde je implementirana fuzija tehnike LBP kodovanja i Gaborovih filtara. LBP definiše teksturu slike pomoću raspodele vrednosti lokalnih piksela, izdvaja obeležja kao što su prekidi linija, ivice i tačke, a važne osobine ove tehnike su da je računski nezahtevna i da je neosetljiva na različite intenzitete

pozadine slike. U osnovnom LBP kodu svaki piksel se predstavlja osmobitnim binarnim kodom koji se formira na osnovu piksela koji ga okružuju, što je ilustrovano na slici 35. Ukoliko je vrednost intenziteta susednog piksela veća ili jednaka centralnom pikselu, susedni piksel se koduje jedinicom, u suprotnom nulom. Ova tehnika je ostvarila veliki uspeh u biometrijskim sistemima autentifikacije zasnovanim na crtama lica, što je navedeno u sekciji 2.3.3.



Slika 35 – LBP kodovanje

Pored osnovnog modela LBP kodovanja, postoje varijacije koje podrazumevaju da se ne koriste susedni pikseli, već određeni broj piksela koji se nalaze na nekoj kružnoj distanci u odnosu na centralni piksel, gde se kao parametri definišu: broj piksela koji formiraju kôd i poluprečnik izražen u pikselima, odnosno udaljenost sa koje se koriste pikseli. Na taj način se u određenoj meri postiže otpornost na rotaciju. Tako dobijen kôd se konkatenacijom spaja sa klasičnim vektorom obeležja dobijenih pomoću Gaborovih filtara i formira se 511 obeležja. Za kvantizaciju je izabrana srednja vrednost celokupnog seta za obučavanje. Šema fazi povezivanja je ostvarena primenom BCH tehnike za ispravljanje grešaka za ključ dužine 76 bita i LDPC (engl. *low-density parity check*) tehnike za ispravljanje grešaka za ključeve dužine: 100, 120 i 140 bita. Ostvareni rezultati su prikazani u tabeli 7. Za eksperimentalno testiranje korišćena je baza otisaka prstiju FVC2000 DB2, gde je pet otisaka svakog identiteta korišćeno prilikom faze upisa, a tri prilikom verifikacije.

Tabela 7 – FAR i FRR vrednosti ostvarene u [82]

Dužina ključa [bita]	**ECC**	**FAR [%]**	**GAR [%]**
76	BCH	0	95,30
100	LDPC	0	92,67
120	LDPC	0	92,00
140	LDPC	0	89,33

Poslednjih godina, napredak u razvoju mašinskog učenja utiče na sve češću primenu neuronskih mreža za klasifikaciju, prepoznavanje i izdvajanje obeležja predmeta sa slika. Konvolucione neuronske mreže razvijene su za klasifikaciju ulaznih podataka, tako da njihov izlaz predstavlja određivanje predefinisane klase nekog ulaznog podatka. Kako se tekstura otisaka prstiju u tradicionalnim biometrijskim sistemima većinski koristi samo za klasifikaciju, prirodno se primena CNN nametnula kao nov metod koji može unaprediti

proces klasifikacije otisaka, pa su istraživanja išla u tom pravcu. Početni rezultati primene CNN-a za poređenje biometrijskih karakteristika ili njihovo izdvajanje daju obećavajuće rezultate. U [83] je primenom prenesenog znanja (engl. *transfer learning*) na dve konvolucione mreže VGG-F i VGG-S [84] postignuta tačnost klasifikacije otisaka od 94,4% i 95,05%, respektivno u odnosu na primenjenu neuronsku mrežu. Klasifikacija otisaka u šest klasa, razvojem nove arhitekture konvolucione mreže *FCTP-Net* [85], dostigla je tačnost od 94,87%, dok je u primeni na NIST bazi otisaka i klasifikaciji u 4 klase ostvarena tačnost od 92,90%. Arhitektura lagane konvolucione mreže predstavljena je u [86], koja za klasifikaciju koristi izdvojene ROI koji sadrže singularne tačke. Ulazne slike otisaka prstiju prolaze kroz procese normalizacije i poboljšanja slike, a eksperimentalni rezultati su potvrdili da je moguće ostvariti tačnost od 93% primenom manje neurona i istovremeno povećati otpornost na šum. U [87] autori su predložili *Res-FingerNet*, duboku konvolucionu neuronsku mrežu za klasifikaciju otisaka. Kako bi se smanjila varijansa unutar klase i povećala međuklasna varijansa otisaka prstiju, iskoristili su centralni gubitak u fazi obuke mreže, tako da su naučene karakteristike diskriminantnije, čime je tačnost klasifikacije povećana za oko 1,5%. Performanse pristupa ocenjene su na bazi podataka NIST-DB4, postižući tačnost klasifikacije od 97,9%. U [88] je predstavljen biometrijski sistem za verifikaciju zasnovan na dva CNN modula, koji paralelno izdvajaju obeležja iz dva otiska prsta koja se porede. Za izdvajanje obeležja je izabrana *AlexNet* neuronska mreža [89]. Konkatenacijom izdvojenih obeležja uspostavlja se ulaz poslednjeg sloja koji izračunava skor njihovog poklapanja. U ovom pristupu se ne koristi ulazna obrada i poboljšanje slike, već se ceo sistem oslanja na mogućnosti CNN-a. Na polju primene konvolucionih mreža za izdvajanja minucija, u [90] je predstavljen koncept izdvajanja minucija kategorizacijom svakog piksela slike u jednu od 36 klasa koje odgovaraju minucijama ili jednoj klasi koja ne predstavlja minuciju, uz čuvanje podataka o orijentaciji i lokaciji tačke.

Princip iz tradicionalnih biometrijskih sistema da se informacije o teksturi otisaka prstiju većinski koriste samo za klasifikaciju, preneo se i na istraživanja koja uključuju formiranje biometrijskih kriptosistema. Da tekstura otisaka prstiju sadrži dovoljno diskriminantnih informacija za primenu u biometrijskim sistemima za autentifikaciju, prvobitno je potvrđeno u [79]. Mogućnost da se izdvojena obeležja iz sveobuhvatnih globalnih i lokalnih informacija o teksturi otisaka prstiju konvertuju u binarni domen, uspešno je sprovedeno u radovima koji su opisani, gde su formirani biometrijski kriptosistemi na šemi fazi povezivanja. Razvojem mašinskog učenja i dubokih konvolucionih mreža, otvorila se mogućnost istraživanja da li su te tehnike dovoljno uznapredovale da izdvoje biometrijska obeležja i tako zamene odgovarajuće module za ekstrakciju u postojećim biometrijskim kriptosistemima. U [91] je primenom prenesenog znanja na konvolucionu neuronsku mrežu *Alexnet*, formiran modul za izdvajanje biometrijskih obeležja iz teksture otisaka prstiju, čime je u potpunosti zamenjen modul baziran na Gaborovim filtrima. Izlazni sloj neuronske mreže je modifikovan da generiše

niz fiksne dužine, koji se tehnikama kvantizacije prevodi u binarni domen i omogućava primenu Hemingove metrike za poređenje ili formiranje biometrijskog kriptosistema fazi povezivanje. U narednim sekcijama ovog poglavlja, biće detaljno prezentovana šema ovog biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama.

4.2. Određivanje referentne tačke i poboljšanje slike

Referentna tačka ima ključnu ulogu u segmentaciji regiona od interesa, na osnovu kojeg se dalje sprovode tehnike izdvajanja i poređenja biometrijskih obeležja. Precizno određivanje referentne tačke u velikoj meri utiče na tačnost biometrijskih sistema zasnovanih na poređenju karakteristika teksture otisaka prstiju. Papilarne linije otisaka prstiju uglavnom su paralelne, dok u određenim regionima obrazuju specifične forme, o čemu je detaljno diskutovano u sekciji 2.3.1. ovog rada. Za referentnu tačku u predloženoj šemi odabrana je centralna tačka jezgra otiska, odnosno piksel u kome jedna linija formira maksimalnu konkavnu zaobljenost u poređenju sa ostalim.

Kako bi se odredila referentna tačka neophodno je definisati polje orijentacije O slike otiska, koje za svaki piksel (i,j) poseduje aproksimaciju lokalne orijentacije papilarne linije $O(i,j)$. Ovaj postupak je računski isuviše kompleksan da bi se sprovodio za svaki piksel, zbog čega se lokalna orijentacija utvrđuje na nivou blokova određenih veličina. Na ulaznu sliku I primenjuje se postupak normalizacije na srednju vrednost 0 uz standardnu devijaciju 1, a zatim se deli u nepreklapajuće blokove dimenzija $w \times w$. Svakom pikselu bloka određuju se gradijenti $\partial_x(i,j)$ i $\partial_y(i,j)$, na osnovu Sobelovog operatora, koji se sastoji od dve konvolucione matrice kao na slici 36.

1	0	-1
2	0	-2
1	0	-1

1	2	1
0	0	0
-1	-2	-1

Slika 36 – Horizontalni i vertikalni Sobelov operator

Lokalna orijentacija svakog bloka određuje se u njegovom centralnom pikselu na osnovu sledećih jednačina:

$$V_x(i,j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} 2\partial_x(u,v)\partial_y(u,v), \tag{32}$$

$$V_y(i,j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} (\partial_x^2(u,v) - \partial_y^2(u,v)), \tag{33}$$

$$O(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_y(i,j)}{V_x(i,j)}\right). \quad (34)$$

Ovako dobijeno polje orijentacije O je reprezentacija ortogonalnog pravca u poređenju sa dominantnim pravcem Furijeovog spektra svakog bloka. Radi ujednačavanja, neophodno je primeniti niskopropusne filtre, a kako bi to bilo moguće, slika orijentacije se prethodno konvertuje u kontinualni vektor polja:

$$\Phi_x(i,j) = \cos(2O(i,j)), \quad (35)$$

$$\Phi_y(i,j) = \sin(2O(i,j)), \quad (36)$$

gde su Φ_x i Φ_y komponente vektora polja, respektivno. Rezultujući vektor se zatim filtrira:

$$\Phi'_x(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2}\sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_x(i-uw, j-vw), \quad (37)$$

$$\Phi'_y(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2}\sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_y(i-uw, j-vw), \quad (38)$$

gde W označava dvodimenzionalni niskopropusni filtar, a w_Φ x w_Φ su njegove dimenzije. Konačna aproksimacija polja orijentacije O' izračunava se na osnovu filtriranih vektora polja:

$$O'(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right). \quad (39)$$

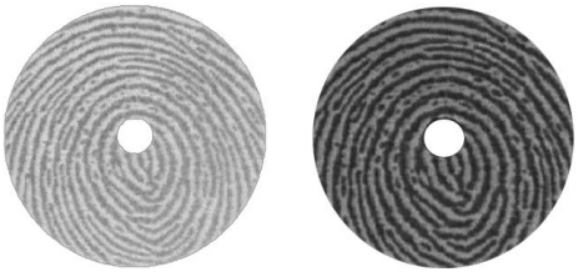
U predloženom biometrijskom kriptosistemu implementirano je dvostepeno određivanje referentne tačke. U prvom koraku primenjen je metod iz [92] modifikovan da se izvršava u više iteracija sa fiksnom varijansom gradijenata 1, ali sa različitom varijansom σ bloka prilikom određivanja polja orijentacije papilarnih linija iz [93] i [94]. U prvoj iteraciji koristi se varijansa $\sigma = 3$, a ukoliko ne dođe do detekcije referentne tačke, onda se primenjuje $\sigma = 5$ koja rezultuje nešto lošijom preciznošću, ali ima veći stepen detekcije. U oba koraka su korišćeni parametri: dužina koraka 7, broj polaznih tačaka uzorkovanih duž x i y ose 2 i prag za zaustavljanje 2. U slučaju da nakon svih zadatih iteracija ne dođe do detekcije jezgra, primenjuju se fiksne referentne vrednosti. Određena tipologija otisaka, kao što su petlja ili spirala, rezultuju sa dve centralne tačke – severnom i

južnom. Prvobitno je predloženi sistem konstruisan tako da u potpunosti bude neosetljiv na rotaciju otiska, pa su se u takvim slučajevima obe detektovane referentne tačke uzorka koristile prilikom poređenja. Međutim, iako je takav pristup smanjivao FRR grešku sistema, značajno je povećavao vreme izvršavanja i istovremeno ostvarivao negativan uticaj na FAR grešku sistema. Usled toga, u slučaju detekcije severne i južne centralne tačke, u predloženom pristupu koristi se samo severna kao referentna tačka. Na taj način napravljen je kompromis u korist performansi sistema, zarad nepotrebne potpune neosetljivosti na rotaciju otiska. Važno je naglasiti da je predloženi biometrijski sistem neosetljiv na uobičajene i nenamerne manje rotacije otiska prilikom uzorkovanja.

U svakom tradicionalnom biometrijskom sistemu neophodno je izvršiti poboljšanje ulazne slike biometrijske karakteristike. Kod otisaka prstiju poboljšanje slike neophodno je radi eliminacije pozadinskog šuma koji se javlja prilikom akvizicije i kako bi se ublažila varijabilnost intenziteta kao posledica razlike u pritisku na površinu senzora. U izvornim šemama [79] i [81] sprovodi se normalizacija svakog piksela u izdvojenom regionu od interesa na prosečnu vrednost i varijansu pripadajućeg sektora. Razlog ovakvog pristupa, umesto normalizacije na nivou celokupne slike, jeste da se na ovaj način kompenzuje neujednačenost intenziteta različitih regiona slike usled osobine elastičnosti prstiju. Vrednost normalizovanog piksela N_i dobija se na osnovu:

$$N_i(x,y) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 \times (I(x,y) - M_i)^2}{V_i}}, & ako\ je\ I(x,y) > M_i \\ M_0 - \sqrt{\dfrac{V_0 \times (I(x,y) - M_i)^2}{V_i}}, & ako\ je\ I(x,y) \le M_i \end{cases} \quad (40)$$

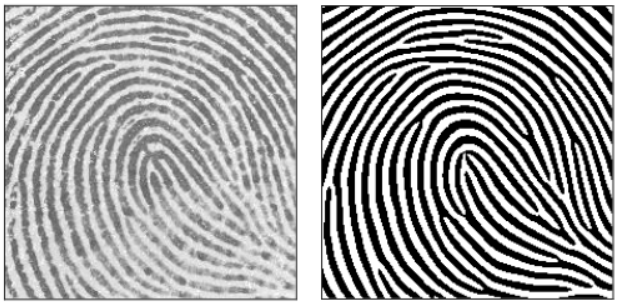
gde su M_0 i V_0 ciljane prosečna vrednost i varijansa, respektivno; I označava ulazni intenzitet piksela, dok su M_i i V_i ulazna prosečna vrednost i varijansa sektora S_i. Rezultat normalizacije jednog ROI prikazan je na slici 37.



a) Ulazni ROI b) Normalizovan ROI

Slika 37 – Normalizacija regiona od interesa

Za potrebe ekstrakcije obeležja konvolucionim neuronskim mrežama eksperimentalno su u velikoj meri potvrđeni poboljšani rezultati primenom konvolucije 2D Gaborovog filtra na prethodno normalizovanu sliku, primenom algoritma iz [94]. Na osnovu praga za binarizaciju, tako dobijena poboljšana slika zatim se konvertuje u monohromatsku, kao na slici 38.



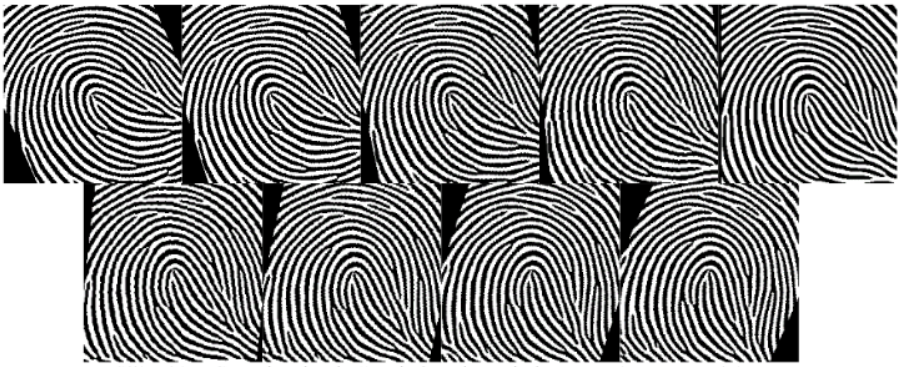
(a) (b)

Slika 38 – Poboljšanje slike otiska prsta - (a) izvorna slika (b) poboljšana slika

4.3. Segmentacija regiona od interesa i formiranje skupa za obučavanje

Na osnovu referentne tačke izdvaja se region od interesa u skladu sa ulaznim parametrima primenjene neuronske mreže. Za neuronsku mrežu *AlexNet* veličina ulazne slike je 227x227px, dok je za *GoogleNet* i *ResNet* potrebna veličina 224x224px, pa se slika svodi na potrebne dimenzije odsecanjem, tako da referentna tačka bude u sredini. Na taj način se iz slike izdvaja deo otiska za koji je u prethodnim radovima utvrđeno da poseduje potrebnu diskriminativnost i koherentnost, a uklanjaju se nekonzistentni delovi čiji detalji mogu negativno uticati na učenje neuronske mreže.

Konvolucione neuronske mreže zahtevaju što veći broj uzoraka u skupu za obučavanje. Njihova najčešća primena je prepoznavanje objekata, gde se za svaku klasu detekcije obezbeđuje više stotina slika za obučavanje. Kod otisaka prstiju to nije moguće ostvariti, već je potrebno izvršiti upis jednog identiteta sa svega nekoliko slika, što negativno utiče na tačnost neuronske mreže i predstavlja izazov za primenu u biometriji. Generisanjem više instanci od jedne ulazne slike, rotacijom u odnosu na referentnu tačku u opsegu ±24° sa korakom od 6°, postižemo veći skup za obučavanje, što je prikazano na slici 39. Na taj način istovremeno se povećava tačnost sistema i njegova neosetljivost na uobičajene male rotacije otiska prilikom uzorkovanja. Sa ovako pripremljenim rotacijama otisaka, za svaku klasu imamo 45 slika koje čine skup za obučavanje konvolucione neuronske mreže. Prilikom formiranja biometrijskih šablona koriste se samo izvorne slike otisaka, bez rotacije, čime se formira 5 nezavisnih šablona koji se čuvaju u bazi šablona.



Slika 39 – Generisanje obučavajućeg skupa jednog uzorkovanog otiska

4.4. Izdvajanje obeležja primenom konvolucione neuronske mreže i diskretizacija

Konvolucione neuronske mreže predstavljaju istraživački atraktivan i aktuelan deo oblasti veštačke inteligencije. Naziv su dobile po konvoluciji, operatoru koji ima čestu primenu pri obradi slika, pomoću kojeg se na slikama radi detekcija ivica objekata, izoštravanje ili zamućenje slika. Po svojoj arhitekturi svrstavaju se u duboke neuronske mreže i predstavljaju evoluciju veštačkih neuronskih mreža poznatih pod nazivom *Multi-Layer Perceptron (MLP)*. U osnovi, neuronsku mrežu čine slojevi sa neuronima koji imaju određene težine za učenje. Svaki neuron prima ulazne podatke, pomnožene sa njihovim težinama i primenjuje nelinearnost putem funkcija aktivacije.

Postoje različiti tipovi arhitekture konvolucionih neuronskih mreža, ali osnovni gradivni slojevi su: konvolucija, sloj sažimanja (engl. *pooling layer*) i potpuno povezani sloj (engl. *Fully Connected Layer – FC layer*). Pomoću konvolucionih filtera iz slike se izdvajaju specifična obeležja, na osnovu kojih se mreža obučava da klasifikuje objekte. Periodično se između slojeva konvolucije radi sažimanje podatka s ciljem da se smanji broj parametara i neophodnih kalkulacija, odnosno pretreniranost mreže (engl. *overfitting*). Potpuno povezani sloj se obično koristi na kraju neuronske mreže i poseduje neurone koji su svi povezani sa izlazom, po čemu je dobio ime.

Implementacija konvolucionih neuronskih mreža u ovom radu ograničena je na modul za izdvajanje biometrijskih obeležja, umesto tradicionalnih metoda izdvajanja minucija ili informacija o globalnim i lokalnim karakteristikama teksture. Kako bi se formirala neuronska mreža i optimizovale njene performanse, potrebno je da mreža prođe kroz proces treniranja sa velikim skupom podataka, što je dugotrajan proces. Zbog toga se često koriste postojeće mreže na koje se primenjuje princip prenosa učenja. Postojeće mreže su formirane i obučene skupovima podataka koji broje na hiljade slika i stotine

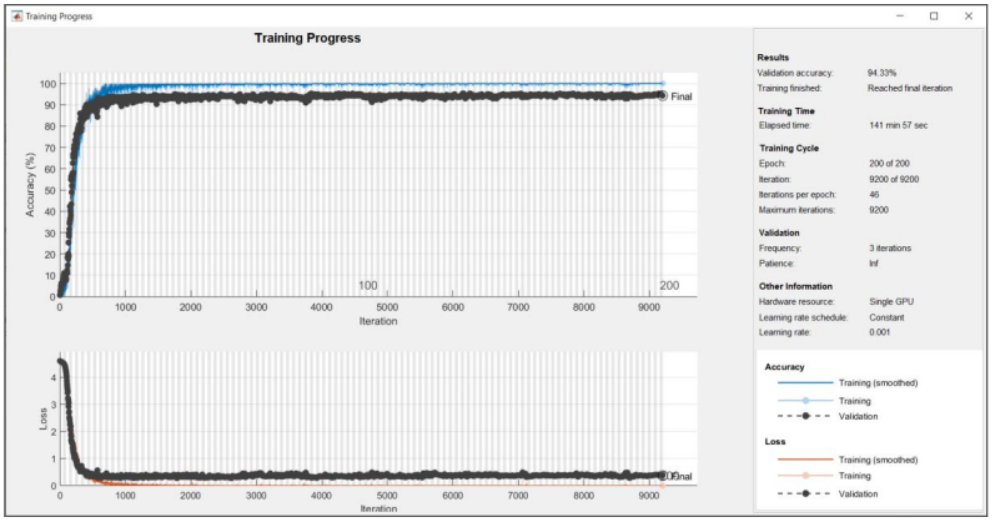
kategorija za klasifikaciju. Prilagođavanjem postojećih slojeva i treniranjem sa mnogo manjim skupom za obučavanje, možemo obučiti mrežu za nove zadatke klasifikacije. U tabeli 8 su date osnovne karakteristike tri konvolucione mreže koje su eksperimentalno testirane i evaluirane u ovom radu.

Tabela 8 – Karakteristike korišćenih konvolucionih neuronskih mreža

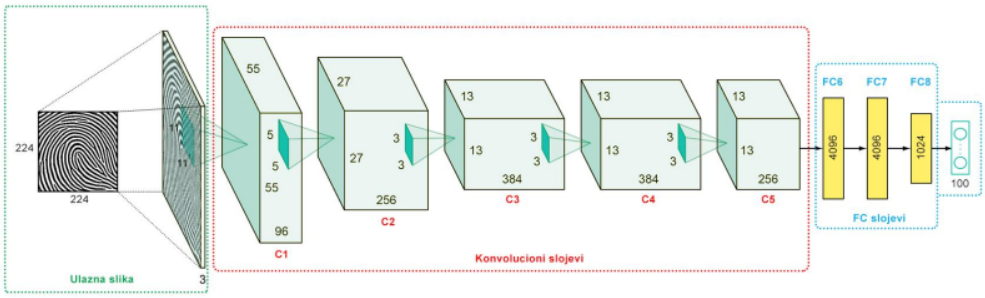
CNN	Veličina ulazne slike	Ukupan broj slojeva	Godina
AlexNet	227x227x3	25	2012.
GoogLeNet	224x224x3	144	2014.
ResNet	224x224x3	50/101*/152	2015.

* koristi se u ovom radu

Bazična *AlexNet* neuronska mreža se sastoji od 5 konvolucionih slojeva i 3 potpuno povezana sloja. Ova mreža poseduje 60 miliona parametara i 650 hiljada neurona. Poslednji potpuno povezani sloj je prilagođen da generiše 1024 obeležja, na osnovu kojih se formira biometrijski šablon, odnosno digitalna reprezentacija ulazne slike otiska prsta. Za potrebe praćenja obučavanja mreže i postignute tačnosti pri klasifikaciji, dodat je još jedan sloj za klasifikaciju 100 otisaka u skladu sa brojem različitih identiteta korišćenih baza otisaka prstiju. Nakon obimnih testiranja, primenom različitih ulaznih parametara, rezultati predstavljeni u radu su postignuti obučavanjem mreže u 200 epoha, s inicijalnom stopom učenja 0,001 u serijama veličine 96. Na slici 40. dat je prikaz postignutih performansi mreže nakon procesa obuke. Ostvareni rezultati prikazani su u poslednjoj sekciji ovog poglavlja, a arhitektura modifikovane neuronske mreže data je na slici 41.

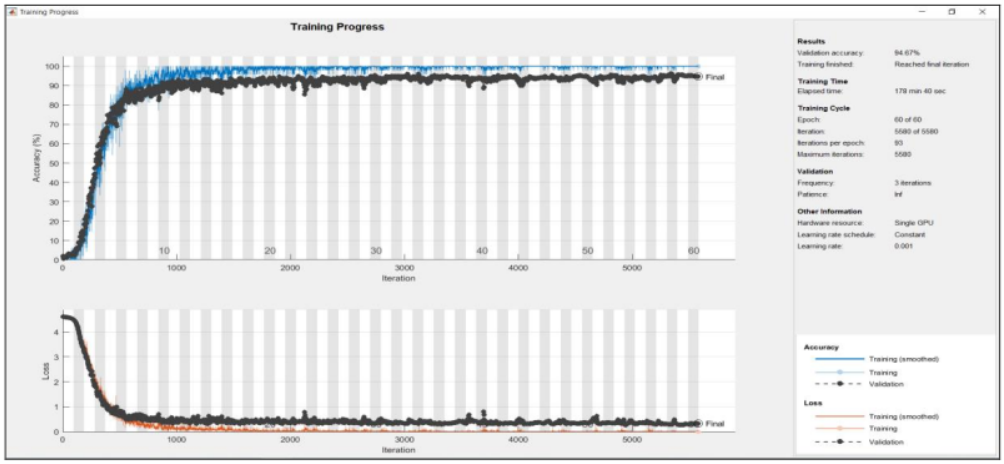


Slika 40 – Obuka *AlexNet* neuronske mreže

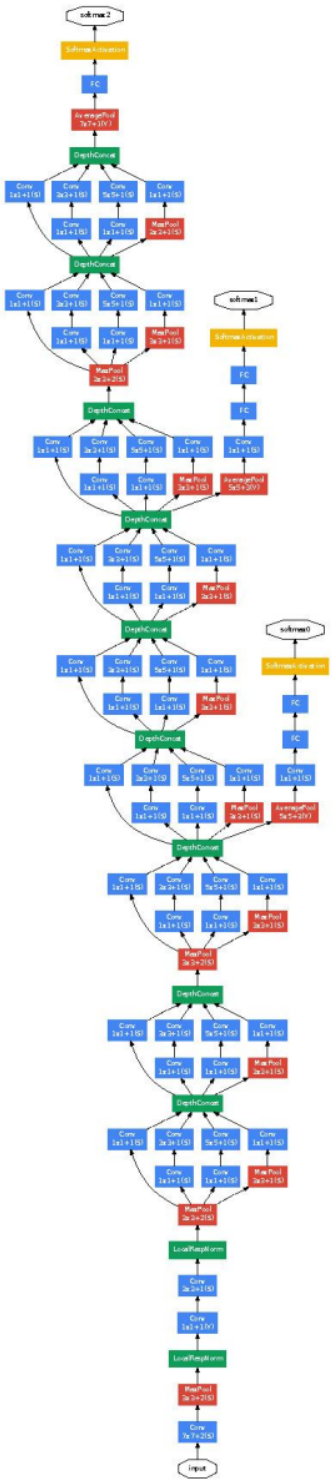


Slika 41 – Arhitektura modifikovane *AlexNet* neuronske mreže

GoogLeNet [95] je konvoluciona neuronska mreža razvijena 2014. godine i sastoji se od 22 sloja koji sadrže parametre za funkcije i 5 slojeva za sažimanje, dok ukupan broj slojeva iznosi 144. *GoogLeNet* je bazirana na malim konvolucijama, kako bi se značajno smanjio broj parametara. U poređenju sa *AlexNet* mrežom, koja ima 60 miliona parametara, ova mreža ih sadrži svega 7 miliona. To je postignuto uvođenjem tehnike multidimenzionalnih konvolucija koje su grupisane u jedan sloj. Unapređenje koje se postiže paralelnom primenom različitih dimenzija konvolucionih filtera je da se na taj način nezavisno izdvajaju globalne (5x5) i lokalne (3x3) karakteristike. Modifikacija ove mreže za izdvajanje obeležja otisaka prstiju podrazumevala je da poslednji potpuno povezani sloj bude izmenjen da izdvaja 1024 obeležja, a da se doda još jedan potpuno povezani sloj koji će predstavljati izlaz za 100 klasa. Rezultat tačnosti klasifikacije otisaka prstiju, predstavljen u radu, ostvaren je obučavanjem mreže u 60 epoha, s inicijalnom stopom učenja 0,001 u serijama veličine 48. Za izdvajanje obeležja primenjeni su drugi parametri za obučavanje, što je navedeno u sledećoj sekciji ovog poglavlja. Na slici 42. dat je prikaz postignutih performansi mreže nakon procesa obuke, a na slici 43. prikazana je arhitektura ove mreže. Postignuti rezultati za izdvajanje obeležja prikazani su u poslednjoj sekciji ovog poglavlja.

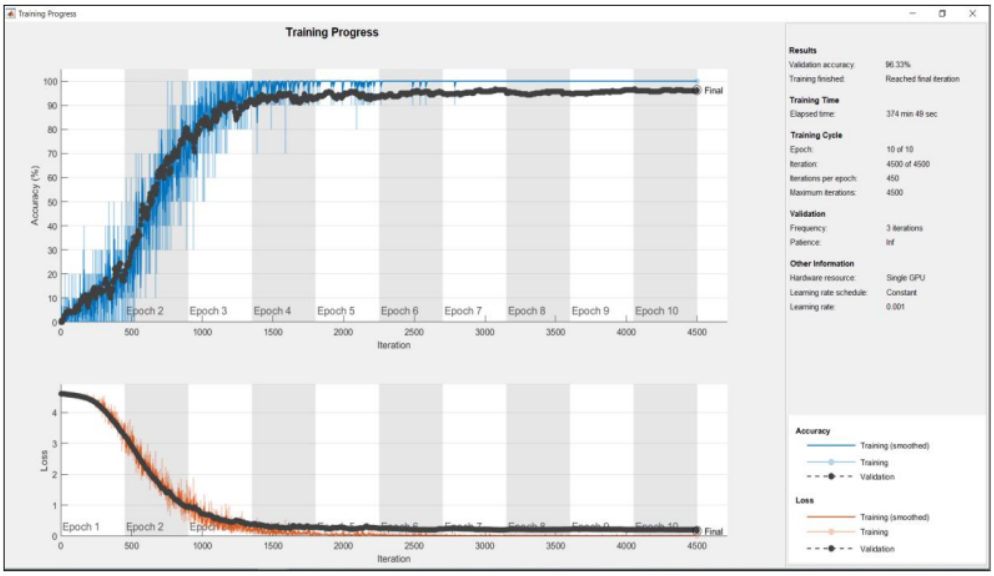


Slika 42 – Obuka *GoogLeNet* neuronske mreže

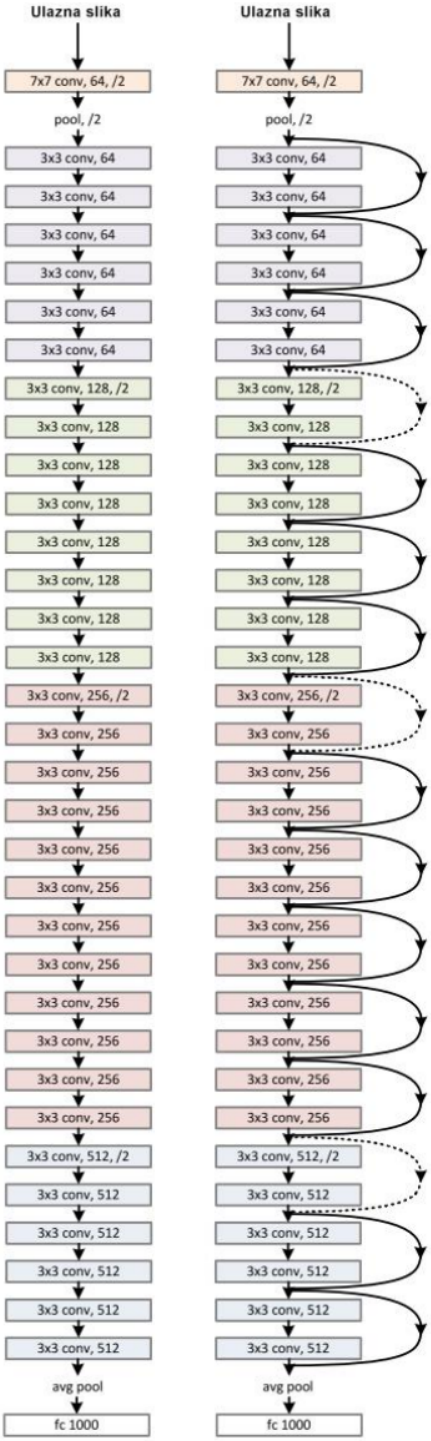


Slika 43 – Arhitektura *GoogLeNet* neuronske mreže (preuzeto iz [95])

ResNet (*Residual Network*) [96] je razvijena u tri različita modela koji se razlikuju u broju slojeva. U ovom radu je eksperimentalno korišćena verzija sa 101 slojem i oko 43 miliona parametara. Po arhitekturi se značajno razlikuje od međusobno sličnih *AlexNet* i *GoogLeNet* mreža, po principu sažimanja. Razvoj ove mreže praćen je istraživanjem zašto se performanse neuronske mreže ne poboljšavaju povećavanjem broja slojeva, naprotiv zašto dolazi do degradacije. Kako bi rešili ovaj problem, autori su predložili uvođenje blokova u kojima srednji slojevi bloka uče funkciju ostatka u odnosu na ulaz bloka, u poređenju sa klasičnom mrežom u kojoj je očekivano da svaki sloj nauči samo nove i različite mape karakteristika. Uporedni prikaz klasične i rezidualne arhitekture neuronske mreže, dat je na slici 45. U slučaju da nije potrebno preciziranje, srednji slojevi mogu naučiti da postepeno prilagođavaju svoje težine prema nuli, tako da blok ostatka predstavlja funkciju identiteta. Prilikom prilagođavanja ove mreže, sloj za klasifikaciju je u skladu sa odabranom bazom otisaka za testiranje modifikovan za rad sa 100 klasa, a poslednji potpuno povezani sloj izmenjen da izdvaja 1024 obeležja. Rezultati predstavljeni u radu su postignuti obučavanjem mreže u 10 epoha, s inicijalnom stopom učenja 0,001 u serijama veličine 10. Na slici 44. dat je prikaz postignutih performansi mreže nakon procesa obuke. Postignuti rezultati su prikazani u poslednjoj sekciji ovog poglavlja.



Slika 44 – Obuka *ResNet* neuronske mreže



Slika 45 – Uporedni prikaz klasične i rezidualne arhitekture neuronske mreže (modifikovano iz [96])

Radi poređenja tačnosti konvolucionih neuronskih mreža u režimu klasifikacije identiteta, sve tri mreže su prošle kroz postupak obuke nad istim skupom za obučavanje u potrebnom broju epoha, dok tačnost obuke ne postigne 100%. U tabeli 9. dat je uporedni pregled ostvarene tačnosti i utrošenog vremena za obuku mreže. Veća tačnost klasifikacije može se ostvariti povećanjem broja epoha, ali određivanje ovih maksimalnih vrednosti izlazi iz okvira ovog rada. Eksperimentalno je utvrđeno da ostvarena tačnost u režimu klasifikacije nije u potpunoj korelaciji sa kvalitetom izdvojenih obeležja iz biometrijskih karakteristika. Dodatnim brojem epoha moguće je uvećati tačnost klasifikacije, ali se javlja negativan uticaj na kvalitet izdvajanja obeležja i tačnost biometrijskog kriptosistema u kom se ta obeležja koriste. Usled toga, obimnim testiranjem su isprobane mreže različitog intenziteta treniranja i za izdvajanje obeležja su primenjene one koje su dale najbolje rezultate pri implementaciji u biometrijskom kriptosistemu.

Tabela 9 – Uporedni pregled tačnosti klasifikacije

CNN	Ostvarena tačnost [%]	Vreme obuke [min]	Broj epoha
AlexNet	94,33	142	200
GoogLeNet	94,67	179	60
ResNet	96,33	225	6

Preduslovi za uspostavljanje šeme fazi povezanosti su da izdvojena biometrijska obeležja imaju fiksnu dužinu i da budu transformisana u binarni domen. Izlaz modula za izdvajanje obeležja daje skup realnih brojeva fiksnog broja elemenata, pa je za ispunjenje drugog preduslova neophodno sprovesti njihovu diskretizaciju. Primenjen je princip kvantizacije na osnovu tri granične vrednosti, koja formira četiri opsega za kvantizaciju, gde se svaki element vektora obeležja koduje sa dva bita, na osnovu izabranih graničnih vrednosti. Princip kodovanja je modifikovan iz [81] u odnosu na formulu 29, tako što se kôd susednih opsega razlikuje samo u jednom bitu, čime se ostvaruje pozitivan uticaj na ukupnu tačnost kvantizacije onih vrednosti izdvojenih obeležja, koje su bliske graničnim vrednostima opsega. Modifikovana formula glasi:

$$(B_i)_t = \begin{cases} 00, & ako\ je\ (V_i)_t \le (T_1)_t \\ 01, & ako\ je\ (T_1)_t < (V_i)_t < (T_2)_t \\ 11, & ako\ je\ (T_2)_t \le (V_i)_t < (T_3)_t \\ 10, & ako\ je\ (V_i)_t \ge (T_3)_t \end{cases} \tag{41}$$

gde je B_i diskretizovan binarni šablon, a T_1, T_2 i T_3 su granične vrednosti. Na ovaj način, formirana je binarna reprezentacija vektora obeležja dužine 2048 bita.

Granične vrednosti za kvantizaciju mogu biti statičke i dinamičke. Statičke granične vrednosti su zajedničke za sve otiske prstiju u sistemu, a iste se određuju empirijski ili

eksperimentalno na osnovu skupa za obučavanje ili prilikom registracije. Kombinovani model podrazumeva da se prilikom registracije svake klase identiteta odrede granične vrednosti koje su fiksne prilikom njihove kvantizacije. U oba slučaja se iste fiksne vrednosti koriste za kvantizaciju uzorka prilikom registracije i autentifikacije, a one se čuvaju u bazi podataka kao vid pomoćnih podataka ili su deo algoritma. Dinamičke granične vrednosti se određuju na nivou svakog otiska i omogućavaju bolju diskriminativnost, s obzirom na to uzorkovana slika otiska prsta poseduje varijabilnost i pored sprovedene normalizacije. Dinamičku graničnu vrednost T_2 možemo odrediti kao medijanu ili srednju vrednost skupa elemenata vektora obeležja svakog pojedinačnog biometrijskog uzorka. Tako dobijena granična vrednost T_2 formira dva podskupa i na svakom od njih se sprovodi isti proces dinamičkog određivanja graničnih vrednosti T_1 i T_3 određivanjem srednje vrednosti ili medijane svakog podskupa obeležja, respektivno.

Oba pristupa imaju svoje prednosti i mane. Dinamičko određivanje granične vrednosti daje bolje rezultate u pogledu sigurnosti biometrijskog sistema. Eksperimentalno je utvrđeno da ovako određene granične vrednosti u predloženom rešenju marginalizuju FAR grešku, koja teži nuli. Međutim, istovremeno greška odbijanja postaje neprihvatljiva. Korišćenjem isključivo medijane prilikom dinamičke kvantizacije, četiri rezultujuća koda za binarizaciju su ravnopravno zastupljeni u šablonu, čime se unosi izvesna zakonitost prilikom njegovog formiranja, što je u suprotnosti sa kriptografskim načelima slučajnog niza i entropije. S druge strane, statičko određivanje graničnih vrednosti omogućava fino podešavanje sistema radi pronalaženja optimalnog balansa FAR i FRR grešaka i najmanje vrednosti EER.

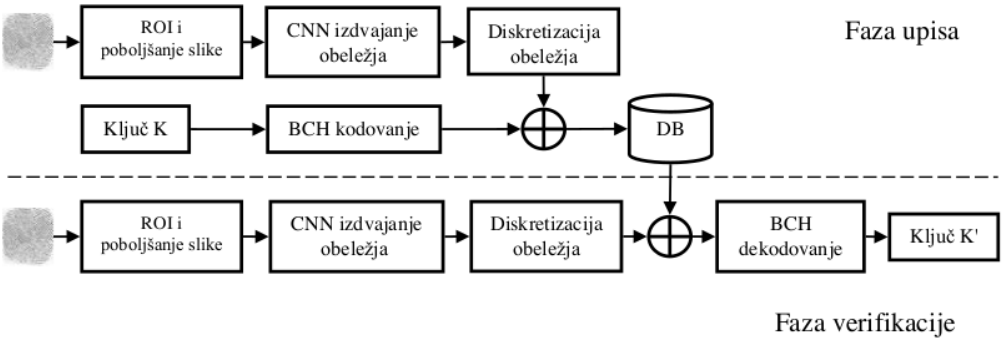
U predloženoj šemi primenjene su statičke granične vrednosti koje se eksperimentalno određuju u zavisnosti od izabrane konvolucione mreže i željene primene biometrijskog sistema. Granična vrednost T_2 je fiksna i iznosi 0, dok su T_1 i T_3 negativna i pozitivna granična vrednost koje imaju istu apsolutnu vrednost. Izbor graničnih vrednosti T_1 i T_3 su u direktnoj korelaciji sa tačnošću biometrijskog sistema, odnosno sa vrednostima FAR i FRR greške, što je prikazano u poslednjoj sekciji ovog poglavlja na dijagramima za svaku primenjenu neuronsku mrežu i izabranu dužinu ključa. Povećanjem apsolutne granične vrednosti FAR greška se uvećava, dok se FRR greška smanjuje, pa odabirom željene granične vrednosti moguće je podešavati rad sistema u skladu sa potrebama.

4.5. Formiranje biometrijskog kriptosistema

Teorijski model šeme fazi povezanosti detaljno je predstavljen u sekciji 3.3.3. ovog rada. Fazi povezanost moguće je ostvariti samo ukoliko se biometrijski šabloni uvek mogu predstaviti binarnim nizom fiksne dužine. Problem varijabilnost biometrijskih podataka rešava se mehanizmima rekonstrukcije i pomoćnim podacima. U većini predloženih

rešenja to se postiže upotrebom kodova za korekciju grešaka i tom prilikom neophodno je koristiti kôd iste dužine kao binarni zapis šablona. Fazi povezanost se ostvaruje primenom logičke XOR operacije nad šablonom i kodom za korekciju greške. Radi validacije moguća je izvedba gde se koriste pomoćni podaci u vidu primene jednosmerne heš funkcije na kôd za korekciju greške ili tajni ključ, čiji se rezultat čuva u bazi podataka zajedno sa zaštićenim biometrijskim šablonom. Ovaj pomoćni podatak ne odaje nikakve informacije o izvornom kodu. Upoređivanjem heš vrednosti rekonstruisanog koda ili ključa sa odgovarajućom iz pomoćnih podataka, obavlja se finalni proces autentifikacije.

U predloženom biometrijskom kriptosistemu uspostavljena je šema fazi povezanosti otisaka prstiju i tajnog ključa, a polaznu osnovu čini sličan kriptosistem zasnovan na dužici oka, koji je predložen u [18]. Blok šema predloženog pristupa data je na slici 46.



Slika 46 – Blok šema predloženog biometrijskog kriptosistema

U prethodnim sekcijama ovog poglavlja opisan je način na koji se ulazna slika otiska prsta poboljšava, nakon što joj se odredi referentna tačka i na osnovu nje izdvoji region od interesa. Primenom konvolucione neuronske mreže iz regiona od interesa se formira vektor izdvojenih obeležja, koji se prevodi u binarni domen i rezultira binarnim kodom fiksne dužine θ_{ic}. Istovremeno, na kriptografskom ključu K sprovodi se kodovanje izabranom tehnikom za ispravljanje grešaka, što rezultuje pseudo-kodom θ_{ps} iste dužine. Tako dobijena dva binarna niza spajaju se logičkom operacijom ekskluzivno ILI, kao što je navedeno u jednačini 30. Na taj način formira se kôd θ_{lock}, koji predstavlja zaštićeni biometrijski šablon i kriptografski ključ. U postupku faze verifikacije, odnosno rekonstruisanja ključeva, na kôd θ'_{ic} koji predstavlja binarnu reprezentaciju uzorka otiska prsta i zaštićeni kôd θ_{lock} iz baze podataka primenjuje se ista logička operacija kako bi se dobio pseudo-kod θ'_{ps}, na osnovu jednačine 31. Ukoliko binarni kodovi otiska prsta korišćenog prilikom faze upisa θ_{ic} i uzorkovanog u fazi verifikacije θ'_{ic} potiču iz istog biometrijskog izvora, tehnike za korekciju grešaka bi trebalo da eliminišu grešku koja se javlja usled unutarklasne varijabilnosti podataka. Na taj način moguće je rekonstruisati

ključ K. U suprotnom, ukoliko biometrijski kodovi ne potiču iz istog izvora, nije moguće rekonstruisati ispravan ključ K. Mogućnost rekonstrukcije ključa zavisi od kapaciteta primenjene tehnike za korekciju grešaka i izabranih parametara, gde je potrebno voditi računa da se nađe optimalan odnos FAR i FRR grešaka, u skladu sa aplikacijom sistema.

Greška ili otkaz biometrijskog sistema predstavlja ozbiljnu sigurnosnu pretnju sistemima koji se na njega oslanjaju. Detaljna analiza ranjivosti i mogućih napada na autentifikacione sisteme izlazi iz okvira ovog rada. Ipak, u trećem poglavlju su analizirane najznačajnije ranjivosti koje su specifične za biometrijske sisteme. Za razliku od drugih sistema za autentifikaciju, gde se konačna odluka o verifikaciji donosi na osnovu jednostavnog poređenja ulaznog i sačuvanog podatka, biometrijski autentifikacioni sistemi konačnu odluku donose na osnovu rezultata i postavljenih margina greške, što omogućava specifične napade u ovoj fazi rada. S druge strane, biometrijski kriptosistemi objedinjavaju oba pristupa, imajući u vidu da je, za razliku od klasičnih biometrijskih sistema, izlazni podatak ispravan tajni ključ ili poruka o odbijanju. Zahvaljujući tome, biometrijski kriptosistemi su inherentno zaštićeni od napada na fazu donošenja odluke. Ipak, postoje ranjivosti u drugim fazama rada, pa je potrebno obratiti pažnju na postojeće poznate napade. Usled mogućnosti da napadač ostvari pristup internoj komunikaciji modula i tako dobije pristup međurezultatima, neophodno je razmotriti sigurnosne analize posvećene poznatim napadima koji su zasnovani na statističkim podacima. Iz svega navedenog, može se zaključiti da sigurnost biometrijskih kriptosistema u značajnoj meri zavisi od odabira kodova za ispravku grešaka.

U nekom komunikacionom kanalu prilikom prenosa podataka moguća je pojava grešaka koje delimo na: vezane (greške na nivou niza bita) i pojedinačne (greške na nivou bita). Za ispravljanje ovih grešaka često se u literaturi može naći predlog istovremene primene dve tehnike za ispravljanje grešaka. Za pojedinačne greške primenjuju se Adamarovi kodovi, dok se vezane greške u sekvencijalnom nizu bita ispravljaju Rid-Solomonovim kodovima. Kriptografski ključevi, heš ključeva ili lozinki i ostali tajni kodovi smatraju se statistički nezavisnim i slučajnim, dok to nije slučaj sa kodovima za korekciju grešaka. Kada se ovi kodovi primenjuju na način kao u predloženoj šemi, moguće je iskoristiti statističke podatke kodova za korekciju grešaka za izvođenje napada na biometrijski kriptosistem. Detaljna analiza ranjivosti tehnika za korekciju grešaka na napade zasnovane na statističkim podacima data je u [97], gde su autori ukazali na mnoge vrste poznatih napada. Za sve prikazane ranjivosti zajednički činilac je pristup da se prilikom kodovanja podaci dele u male segmente. Opšti zaključak je da su svi kodovi koji rade na ovom principu, u koje spadaju Adamarovi i Rid-Solomonovi kodovi, osetljivi na napade zloupotrebom izlaznih statističkih podataka. Imajući u vidu iznete argumente, u predloženom biometrijskom kriptosistemu implementiran je BCH kôd, tehnika ispravljanja grešaka iteracionog blokovskog tipa. U pogledu otpornosti na poznate napade na izlazni modul biometrijskog kriptosistema diskutovano je u sekciji 3.3.3. ovog rada. Ukoliko je

kapacitet ispravljanja grešaka primenjenog BCH koda značajno manji od polovine dužine bloka (n/2), teško je izvodljivo da napadač prevaziđe veliki korak kvantizacije.

Bose-Chaudhuri-Hocquenghem kodovi su ciklične tehnike za korekciju grešaka. Binarni BCH kôd [98] definisan je sa tri parametra *(n,k,t)*, gde *n* predstavlja dužinu rezultujućeg bloka za korekciju, čija je dužina definisana formulom $n=2^m-1$, što se u predloženom sistemu podudara sa dužinom biometrijskog šablona. Parametar *k* predstavlja dužinu poruke koja se koduje, što u konkretnom sistemu predstavlja dužinu kriptografskog ključa, dok *t* predstavlja kapacitet koda u pogledu broja bita koje može ispraviti. Zbog parametra *n* veličina bloka mora biti 2047 bita, pa se u predloženoj šemi poslednji bit biometrijskog binarnog koda otiska prsta odbacuje. Cilj predložene šeme je da se mogu implementirati ključevi dužine 128 i 256 bita, koji bi zatim mogli da se primene u nekim drugim simetričnim kriptosistemima. U slučaju primene BCH koda ne postoji dužina poruke *k* koja se koduje od 128 bita, pa je izabrana prva sledeća vrednost – 133 bita, dok je u slučaju dužine ključa od 256 bita korišćen ključ od 265 bita. U tabeli 10. dat je prikaz mogućih parametara *k* i *t* za dužinu bloka od 2047 bita. U praktičnoj primeni, višak bita u ovako formiranom ključu je moguće lako odstraniti.

Broj bita koje je BCH kôd u mogućnosti da ispravi za dužinu ključa od 133 bita je 365 bita. Primenom BCH dekodovanja na pseudo-kod θ'_{ps} odstranjuje se greška razlike dve uzorkovane biometrije istog identiteta. Zbog neravnomernog odnosa dužine ključa i broja bita koji se mogu ispraviti, rezultati u radu su približno isti i za ključ dužine 199 bita, gde je moguće ispraviti 341 bit. Za dužinu ključa od 265 bita, moguće je ispraviti 247 bita. Povećavanjem dužine ključa, smanjujemo kapacitet koda za ispravljanje grešaka, što rezultuje smanjivanje FAR greške, ali povećanje FRR greške.

Tabela 10 – Prikaz odnosa dužine ključa i mogućnosti korekcije grešaka za BCH kôd dužine 2047 bita

BCH kôd za n=2047					
k	t	k	t	k	t
2036	1	1354	69	672	167
2025	2	1343	70	661	169
2014	3	1332	71	650	170
2003	4	1321	73	639	171
1992	5	1310	74	628	173
1981	6	1299	75	617	174
1970	7	1288	76	606	175
1959	8	1277	77	595	179
1948	9	1266	78	584	181
1937	10	1255	79	573	182
1926	11	1244	81	562	183
1915	12	1233	82	551	185
1904	13	1222	83	540	186
1893	14	1211	84	529	187
1882	15	1200	85	518	189

1871	16	1189	86	507	190
1860	17	1178	87	496	191
1849	18	1167	89	485	205
1838	19	1156	90	474	206
1827	20	1145	91	463	207
1816	21	1134	92	452	211
1805	22	1123	93	441	213
1794	23	1112	94	430	214
1783	24	1101	95	419	215
1772	25	1090	99	408	218
1761	26	1079	100	397	219
1750	27	1068	101	386	221
1739	28	1057	102	375	222
1728	29	1046	103	364	223
1717	30	1035	105	353	231
1706	31	1024	106	342	234
1695	33	1013	107	331	235
1684	34	1002	108	320	237
1673	35	991	109	309	238
1662	36	980	110	298	239
1651	37	969	111	287	245
1640	38	958	114	276	246
1629	39	947	115	**265**	**247**
1618	40	936	116	254	250
1607	41	925	117	243	251
1596	42	914	118	232	253
1585	43	903	119	221	254
1574	44	892	121	210	255
1563	45	881	122	**199**	**341**
1552	46	870	123	188	343
1541	47	859	124	177	347
1530	49	848	125	166	349
1519	50	837	126	155	351
1508	51	826	127	144	363
1497	52	815	146	**133**	**365**
1486	53	804	147	122	367
1475	54	793	149	111	375
1464	55	782	150	100	379
1453	56	771	151	89	381
1442	57	760	153	78	383
1431	58	749	154	67	439
1420	59	738	155	56	443
1409	60	727	157	45	447
1398	61	716	158	34	479
1387	62	705	159	23	495
1376	63	694	165	12	511
1365	68	683	166		

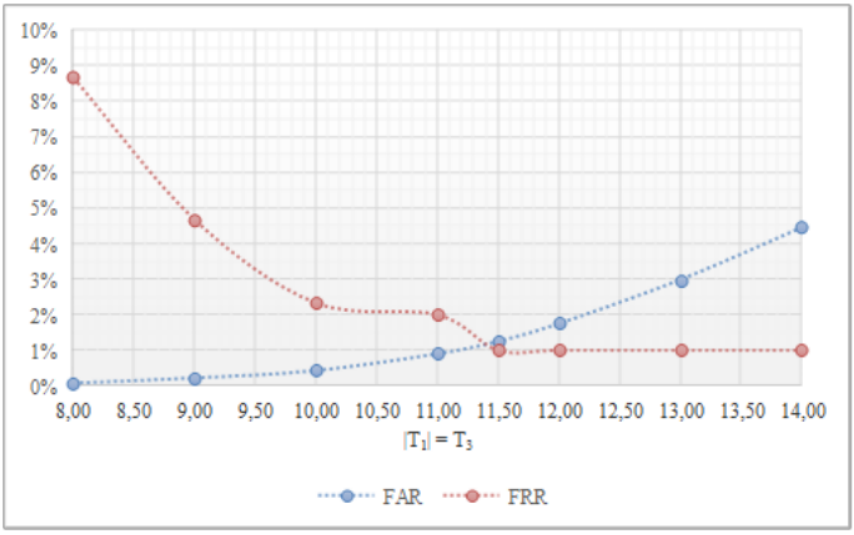
4.6. Eksperimentalni rezultati

Za eksperimentalno testiranje predloženog biometrijskog kriptosistema korišćena je baza otisaka prstiju FVC2000 DB2, radi efektivnog poređenja s drugim konkurentnim konceptima. Iz navedene baze otisaka korišćeni su svi otisci, bez obzira na njihov kvalitet, odnosno nisu uklonjeni oni koji ne ispunjavaju osnovne kriterijume u pogledu celovitosti uzorka, posedovanja referentne tačke ili njene pozicije. Za trening i upis identiteta upotrebljeno je prvih 5 otisaka svake klase, dok su poslednja 3 iskorišćena za verifikaciju. Prilikom faze upisa identiteta, formira se 5 biometrijskih šablona. Pre formiranja zaštićenih šablona, odnosno pre njihovog ujedinjavanja sa pseudo-kodom ključa i skladištenja, šabloni se međusobno upoređuju Hemingovom metrikom, kako bi se proverio kvalitet uzorkovanja. Ukoliko se neki od šablona ne poklapa ni sa jednim od preostalih šablona iste klase, takav šablon se odbacuje kao nepouzdan. Poređenje uzoraka za verifikaciju radi se sa svim generisanim šablonima, što zbirno iznosi poređenje 1500 otisaka prstiju koji odgovaraju istom identitetu (engl. *genuine*), s tim da je efektivan maksimalan rezultat 300 mogućih poklapanja, imajući u vidu da svaki od šablona iste klase može da rezultuje ispravnim rekonstruisanim ključem. Istovremeno, sprovodi se 148500 poređenja sa uzorcima pogrešnog identiteta, koje tretiramo kao napadače na sistem (engl. *imposter*), a koji mogu teoretski da postignu maksimalno 29700 neispravnih poklapanja, što bi predstavljalo 100% grešku prihvatanja. Ukupno se u eksperimentalnoj proveri biometrijskog sistema izvrši poređenje 150 hiljada otisaka. Eksperiment je sproveden u programu Matlab 2018a, na prenosnom računaru sledećih osnovnih karakteristika: procesor *Intel i7-8750H*, kapacitet radne memorije 16GB i grafička kartica *Nvidia GeForce GTX1050*.

Primena *AlexNet* neuronske mreže za izdvajanje obeležja postigla je značajne rezultate za dužine ključeva 133 i 199 bita. Postignuti rezultati u [91] nadmašili su konkurentne biometrijske kriptosisteme bazirane na fazi povezivanju i izdvajanju obeležja iz teksture otisaka prstiju u pogledu dužine ključa i ostvarenom EER. Ostvareni rezultati prikazani su u tabelama 11. i 12, a grafički prikaz odnosa FAR i FRR greške na slikama 47. i 48, za ključeve dužine 133 i 199 bita, respektivno.

Tabela 11 – Rezultati FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita [91]

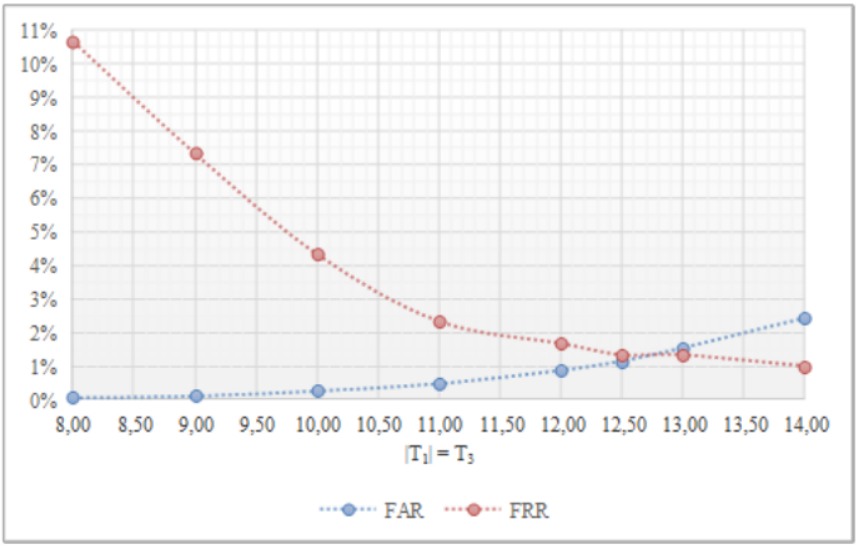
Granica $\|T_1\| = T_3$	**8,00**	**9,00**	**10,00**	**11,00**	**11,50**	**12,00**	**13,00**	**14,00**
FAR	0,08%	0,22%	0,43%	0,90%	**1,25%**	1,75%	2,98%	4,45%
FRR	8,67%	4,67%	2,33%	2,00%	**1,00%**	1,00%	1,00%	1,00%
GAR	91,33%	95,33%	97,67%	98,00%	**99,00%**	99,00%	99,00%	99,00%



Slika 47 – Odnos FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita

Tabela 12 – Rezultati FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita [91]

Granica $\lvert T_1 \rvert = T_3$	**8,00**	**9,00**	**10,00**	**11,00**	**12,00**	**12,50**	**13,00**	**14,00**
FAR	0,05%	0,10%	0,25%	0,47%	0,87%	**1,15%**	1,54%	2,43%
FRR	10,67%	7,33%	4,33%	2,33%	1,67%	**1,33%**	1,33%	1,00%
GAR	89,33%	92,67%	95,67%	97,67%	98,33%	**98,67%**	98,67%	99,00%

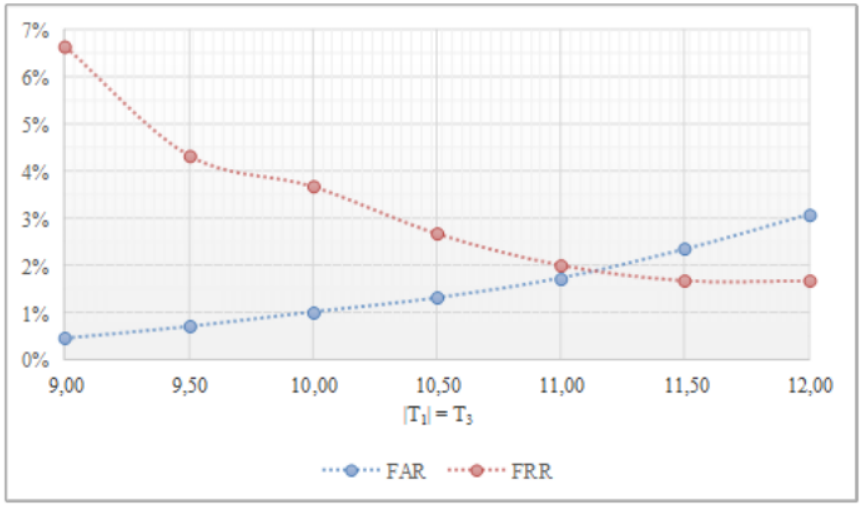


Slika 48 – Odnos FAR i FRR primenom *AlexNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita

Iako je postigla impresivne rezultate na takmičenjima za klasifikaciju objekata, *GoogLeNet* neuronska mreža nije nadmašila prethodno testiranu mrežu u pogledu izdvajanja obeležja iz otisaka prstiju. U tabeli 13. prikazani su rezultati ostvareni za dužinu ključa od 133 bita a na slici 49. grafički prikaz odnosa FAR i FRR greške u zavisnosti od odabranih graničnih vrednosti kvantizacije. Prikazani rezultati su postignuti obučavanjem mreže u 80 epoha, s inicijalnom stopom učenja 0,001 u serijama veličine 48. S obzirom na ostvarene lošije rezultate u odnosu na *AlexNet* mrežu, veće dužine ključeva nisu bile predmet daljih testiranja.

Tabela 13 – Rezultati FAR i FRR primenom *GoogLeNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita

Granica $\lvert T_1 \rvert = T_3$	**9,00**	**9,50**	**10,00**	**10,50**	**11,00**	**11,50**	**12,00**
FAR	0,45%	0,70%	1,01%	1,31%	**1,73%**	2,34%	3,08%
FRR	6,65%	4,33%	3,67%	2,67%	**2,00%**	1,67%	1,67%
GAR	93,35%	95,67%	96,33%	97,33%	**98,00%**	98,33%	98,33%



Slika 49 – Odnos FAR i FRR primenom *GoogLeNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita

Rezidualna mreža *ResNet* je zahvaljujući inovativnoj arhitekturi ostvarila najbolje rezultate izdvajanja obeležja iz otisaka prstiju. Pored ostvarene najbolje tačnosti izražene greškama FAR, FRR i EER, ostvarena je najveća dužina ključa. Primenom ove neuronske mreže u modulu za izdvajanje obeležja, eksperimentalno su testirani biometrijski kriptosistemi sa dužinama ključeva od: 133, 199 i 265 bita. Obučavanje mreže je sprovedeno u 10 epoha, s inicijalnom stopom učenja 0,001 u serijama veličine 10. U tabelama i dijagramskim prikazima koji slede, prikazani su ostvareni rezultati FAR i FRR greške u zavisnosti od odabranih graničnih vrednosti kvantizacije T_1 i T_3.

Tabela 14 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita

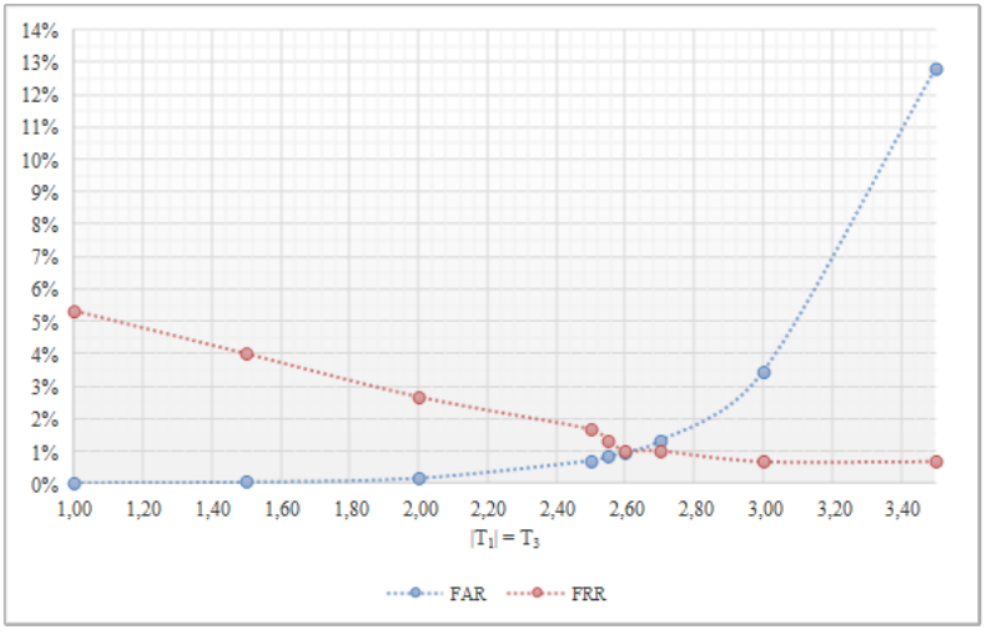
Granica $\|T_1\| = T_3$	**1,00**	**1,50**	**2,00**	**2,50**	**2,55**	**2,60**	**2,70**	**3,00**	**3,50**
FAR	0,01%	0,04%	0,16%	0,70%	0,83%	**0,97%**	1,31%	3,46%	12,81%
FRR	5,33%	4,00%	2,67%	1,67%	1,33%	**1,00%**	1,00%	0,67%	0,67%
GAR	94,67%	96,00%	97,33%	98,33%	98,67%	**99,00%**	99,00%	99,33%	99,33%

Tabela 15 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita

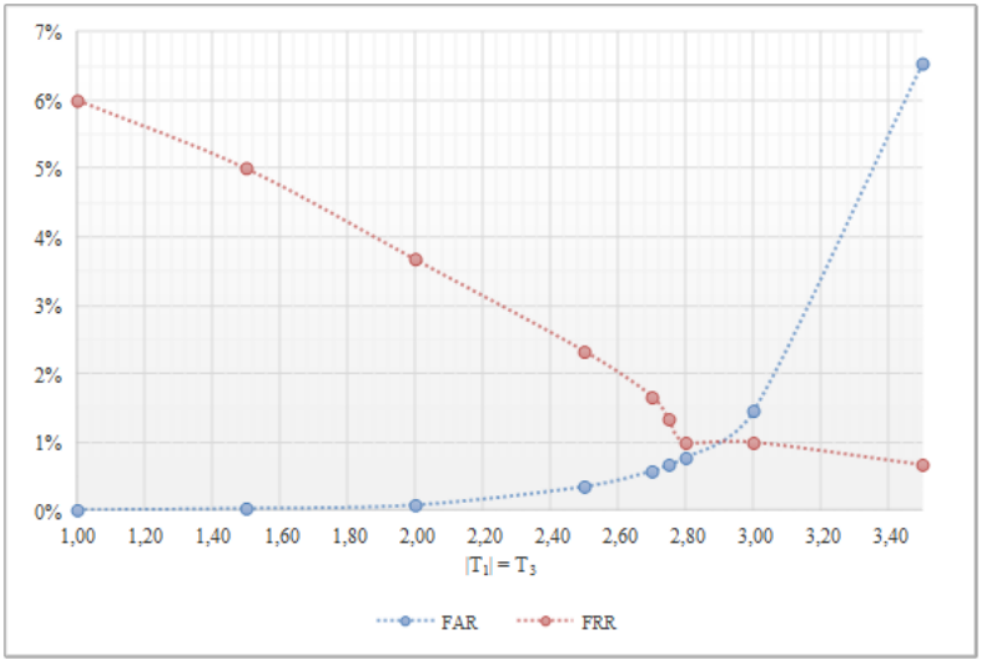
Granica $\|T_1\| = T_3$	**1,00**	**1,50**	**2,00**	**2,50**	**2,70**	**2,75**	**2,80**	**3,00**	**3,50**
FAR	0,01%	0,03%	0,08%	0,35%	0,58%	0,67%	**0,78%**	1,45%	6,53%
FRR	6,00%	5,00%	3,67%	2,33%	1,67%	1,33%	**1,00%**	1,00%	0,67%
GAR	94,00%	95,00%	96,33%	97,67%	98,33%	98,67%	**99,00%**	99,00%	99,33%

Tabela 16 – Rezultati FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 265 bita

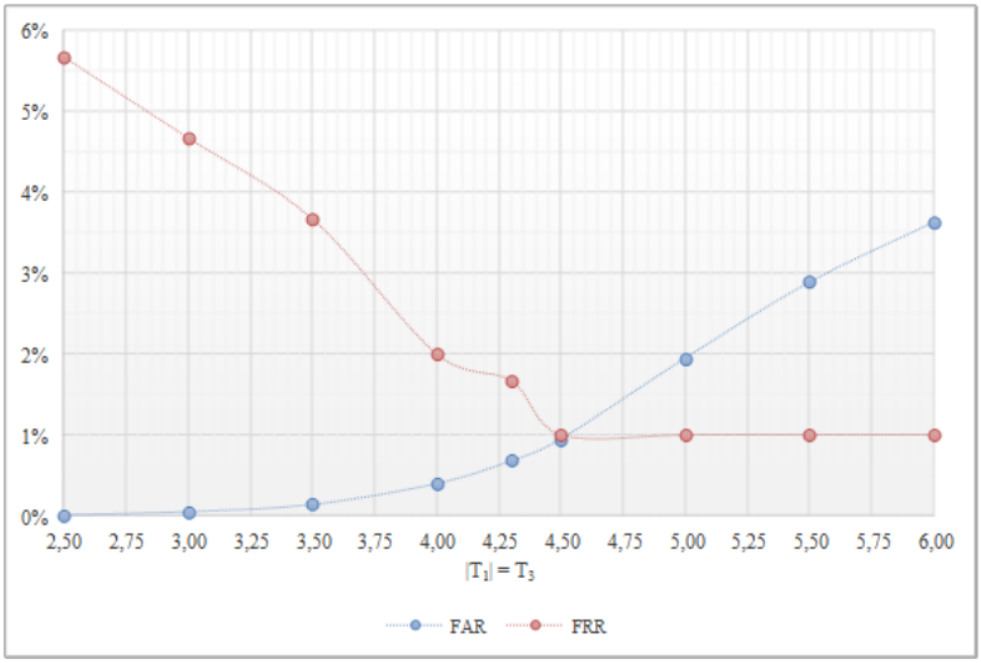
Granica $\|T_1\| = T_3$	**2,50**	**3,00**	**3,50**	**4,00**	**4,30**	**4,50**	**5,00**	**5,50**	**6,00**
FAR	0,01%	0,05%	0,14%	0,40%	0,68%	**0,95%**	1,95%	2,89%	3,63%
FRR	5,67%	4,67%	3,67%	2,00%	1,67%	**1,00%**	1,00%	1,00%	1,00%
GAR	94,33%	95,33%	96,33%	98,00%	98,33%	**99,00%**	99,00%	99,00%	99,00%



Slika 50 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 133 bita

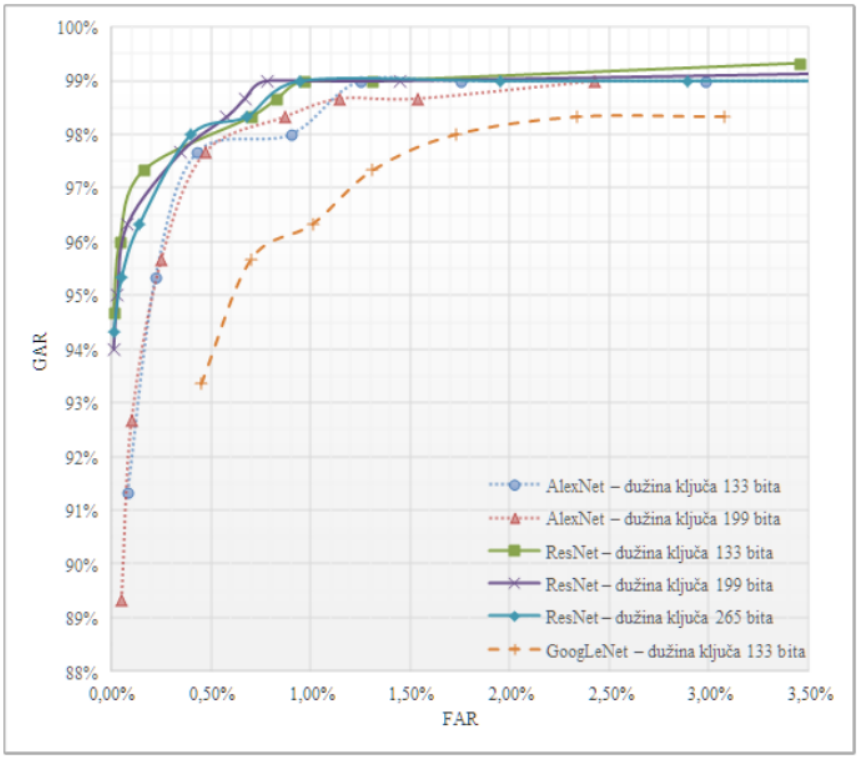


Slika 51 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 199 bita



Slika 52 – Odnos FAR i FRR primenom *ResNet* neuronske mreže za izdvajanje obeležja u zavisnosti od apsolutne granične vrednosti za dužinu ključa 265 bita

Odabir granične vrednosti za konkretnu primenu u nekom biometrijskom sistemu za autentifikaciju, zavisi od potrebe i namene tog sistema, odnosno predstavlja balans između neophodnog stepena sigurnosti i upotrebljivosti. Za sisteme visokog stepena sigurnosti margina greške prihvatanja mora biti minimalna, što posledično dovodi do povećanja greške usled koje će sistem odbiti legitimnog korisnika, dok se u sistemima koji zahtevaju maksimalnu funkcionalnost, može podesiti minimalna margina greške odbijanja uz proračunat rizik od mogućih obmana. Na slici 53. dat je ROC dijagram (engl. *Receiver Operating Characteristic* – ROC) svih predloženih šema za izdvajanje obeležja pomoću konvolucionih neuronskih mreža u ovom radu, na osnovu kojeg se može videti ova zavisnost i izvršiti njihovo međusobno poređenje.



Slika 53 – ROC dijagram predloženih šema

Iz prezentovanih rezultata i dijagrama može se primetiti da u većini predloženih šema greška FRR, bez obzira na povećanje granične vrednosti, ne može da bude niža od 1%, što u konkretnoj bazi otisaka predstavlja 3 slučaja greške odbijanja. Razlog za ovakav rezultat su otisci koji ne zadovoljavaju bazične kriterijume ovakve šeme, odnosno parcijalni su, ne sadrže referentnu tačku ili je ista uz samu ivicu uzorkovane slike. Na osnovu uspostavljenih kriterijuma, ovakvi otisci ne bi ni smeli da budu detektovani kao

legitimni, a neretko se u literaturi isključuju iz konačnih rezultata. Primeri ovakvih otisaka iz baze upotrebljene za eksperimentalno testiranje prikazani su na slici 54.



a) b) c)

Slika 54 – Uporedni prikaz dva uzorka istog identiteta: a) parcijalni, b) bez referentne tačke i c) referentna tačka na ivici slike

EER služi za poređenje različitih biometrijskih sistema, pa su u tabelama koje prethode obeležene vrednosti u kojima FAR i FRR teže jednakosti. Ove vrednosti i aproksimacija odgovarajuće EER upotrebljene su za komparativni pregled ostvarenih rezultata u svim predloženim šemama (primenom različitih neuronskih mreža za izdvajanje obeležja) i prethodno opisanih konkurentnih šema, a koji je dat u tabeli 17.

Tabela 17 – Komparativni pregled rezultata

Metod	FAR	FRR	EER	Dužina ključa	Baza otisaka
Fingercode [79]	4,59%	2,83%	/	/	[79]
Bakhishi-Veisi [88]	/	/	17,50%	/	FVC2002
Tuyls i dr. [80]	5,2%	5,4%	5,3%	76	FVC2000
Imamverdiyev i dr. [82]	0%	4,7%	/	76	FVC2000
Imamverdiyev i dr. [82]	0%	10,67%	/	140	FVC2000
Predložena šema (*AlexNet*) [91]	**1,25%**	**1,00%**	**1,13%**	**133**	**FVC2000**
Predložena šema (*AlexNet*) [91]	**1,15%**	**1,33%**	**1,23%**	**199**	**FVC2000**
Predložena šema (*ResNet*)	**0,97%**	**1,00%**	**0,99%**	**133**	**FVC2000**
Predložena šema (*ResNet*)	**0,78%**	**1,00%**	**0,97%**	**199**	**FVC2000**
Predložena šema (*ResNet*)	**0,95%**	**1,00%**	**1,00%**	**265**	**FVC2000**

U poređenju sa tradicionalnim pristupima za izdvajanje obeležja iz teksture otisaka prstiju zasnovanih na osnovu direkcionih polja, Gaborovim filtrima i LBP kodovanju, konvolucione neuronske mreže postigle su zavidne rezultate i nadmašile su sve do sada ostvarene rezultate u biometrijskim kriptosistemima baziranim na sličnim osnovama šeme fazi povezivanja. Osim manjih EER vrednosti, postignute su značajno veće dužine ključeva, koji se mogu dalje iskoristiti u svim savremenim kriptografskim sistemima. Takođe, predložena šema je postigla značajno bolje rezultate od druge tehnike za poređenje pomoću konvolucionih neuronskih mreža, koja je u potpunosti bazirana na mašinskom učenju. Na osnovu toga se može zaključiti da je od velikog značaja primenjena obrada slike u vidu normalizacije, segmentacije i izdvajanja regiona od interesa, pre uključivanja konvolucionih neuronskih mreža u proces izdvajanja biometrijskih obeležja.

U radu je predloženo izdvajanje biometrijskih obeležja otisaka prstiju konvolucionim neuronskim mrežama, pri čemu su testirane tri najzastupljenije neuronske mreže. Na osnovu dobijenih rezultata, može se zaključiti da je najbolja diskriminativnost izdvojenih obeležja ostvarena primenom rezidualne *ResNet* neuronske mreže, što je omogućilo da se formira šema sa dužinom ključeva od 265 bita. *AlexNet* mreža je ostvarila nešto lošije rezultate u domenu izdvajanja obeležja, ali je računski najmanje zahtevna i vreme potrebno za prenos znanja je najkraće. *GoogLeNet* neuronska mreža je inferiorna pri izdvajanju biometrijskih obeležja u odnosu na preostale dve mreže. Predloženom kvantizacijom kodovanjem sa dva bita, kako bi se obeležja prevela u binarni domen i omogućila primena XOR biometrije, ostvareno je generisanje binarnih šablona fiksne dužine 2048 bita i tako je ispunjen preduslov za formiranje šeme fazi povezivanja. BCH kodovi za korekciju grešaka izabrani su na osnovu sigurnosne analize ovih tehnika u odnosu na statističke pretnje i poznate napade na biometrijske autentifikacione sisteme. Eksperimentalna evaluacija predloženog rešenja i prezentovani rezultati potvrđuju efektivnost predloženog pristupa i unapređenje zaštite biometrijskih šablona i upravljanja kriptografskim ključevima uz pomoć biometrije otisaka prstiju.

5. Zaključak

5.1. Sumarni pregled istraživanja

Biometrija nudi niz prednosti nad konvencionalnim tehnikama autentifikacije baziranim na znanju ili objektu: smanjuje se mogućnost obmane čime se povećava sigurnost, ne može se zaboraviti ili izgubiti, teže se krade ili falsifikuje itd. Usled svega navedenog, kao i zbog brzine i lakoće njene primene, povećava se društvena prihvatljivost biometrije, poverenje korisnika u sisteme zaštite bazirane na njoj, pa sve više menja tradicionalne tehnike autentifikacije u svakodnevnom životu. Savremeno mobilno poslovanje skoro u potpunosti je primenilo biometrijske sisteme za autentifikaciju ugrađene u prenosne uređaje. Ipak, biometrijski sistemi poseduju svoje nedostatke, prvenstveno izazvane usled varijabilnosti biometrijskih karakteristika i greškama koje se usled toga javljaju prilikom poređenja. Zatim, otvaraju se pitanja privatnosti, sigurnosti podataka i društvene prihvatljivosti, s obzirom na to da se radi o ličnim fizičkim osobinama ili karakteristikama ponašanja koje se prikupljaju, obrađuju i skladište. Za razliku od drugih sistema autentifikacije gde se koriste metode zasnovane na znanju ili objektu, koji se mogu povući ili promeniti, kod biometrijskih sistema za autentifikaciju koriste se biometrijske karakteristike koje se ne mogu promeniti. Upravo je to razlog zašto se u bazama biometrijskih podataka ne čuvaju izvorni podaci, već njihovi šabloni koji predstavljaju digitalnu reprezentaciju specifičnih obeležja neke biometrijske karakteristike. One su trajno povezane sa nekom osobom i njihova kompromitacija se prenosi na sve sisteme koji koriste tu karakteristiku, zbog čega je njihova zaštita najznačajniji segment sigurnosti celokupnog biometrijskog sistema. Primena različitih modela za zaštitu biometrijskih šablona dovela je do formiranja biometrijskih kriptosistema, koji su objedinili biometriju i kriptografiju, čime je došlo do značajnog unapređenja obe oblasti, s obzirom na to da je pored uspešne zaštite biometrijskih obeležja, ponuđen efikasan sistem upravljanja, odnosno zavisnog oslobađanja kriptoloških ključeva pomoću biometrije. Sve navedeno, ističe značaj ovog rada i aktuelnost istraživanja koja se bave zaštitom biometrijskih podataka.

S ciljem da se utvrdi teorijski okvir predmetne teme i ustanove načela primene biometrije u kriptografiji, u skladu sa opštom hipotezom rada analizirana su brojna istraživanja sprovedena u ovoj oblasti, koja su upotrebljena kao polazna osnova. Kako bi se stekao kompletan uvid u probleme i izazove koji se javljaju u spoju biometrije i kriptografije, sprovedena je temeljna analiza i evaluacija najistaknutijih istraživanja iz oblasti biometrije, sistema za autentifikaciju, prepoznavanje obrazaca (engl. *pattern recognition*), računarskog vida (engl. *computer vision*), zaštite biometrijskih podataka, biometrijskih kriptosistema, mašinskog učenja i veštačke inteligencije u segmentu dubokih

konvolucionih neuronskih mreža. U prvom delu teze prezentovani su osnovni postulati na kojima počiva biometrija, rezultati istraživanja o poznatim tehnikama i različitim pristupima automatizovane autentifikacije na osnovu biometrijskih podataka, kao i potencijalnim pretnjama i sigurnosnim izazovima. Na osnovu obavljenog istraživanja, izdvojena su zapažanja na osnovu kojih su potvrđene pojedinačne hipoteze ovog rada. Vrhunski biometrijski sistemi su u najvećem broju slučajeva bazirani na otiscima prstiju i dužici oka. Ove fizičke karakteristike su već dugo u primeni, pa je stepen poverenja i društvene prihvatljivosti nametnuo da ovo istraživanje ide u pravcu onih karakteristika koje se efektivno i svakodnevno koriste. Otisci prstiju se izdvajaju po svojoj širokoj primeni, a u hardverskom pogledu čitači su zastupljeni u mnogim uređajima, te je praktičnu primenu moguće brzo i lako ostvariti. Biometrijski sistemi bazirani na dužici oka poređenje mahom izvršavaju u binarnom domenu, dok kod otisaka prstiju to nije slučaj i postoje skromna istraživanja koja su prihvatila ovaj izazov. Razlog leži u tome što je velika većina biometrijskih sistema zasnovana na minucijama, čija detekcija je promenljiva u pogledu njihovog broja i reprezentacije. Informacije o teksturi otiska se u literaturi najčešće primenjuju samo za klasifikaciju otisaka prstiju. Dekompozicijom informacija o različitim prostornim frekvencijama, različitoj orijentaciji ili fazi u više prostornih frekvencija i orijentacija, može se dobiti vektor obeležja fiksne dužine, a konverzijom podataka u binarni domen otvara se mogućnost za primenu Hemingove metrike pri poređenju i formiranje biometrijskog kriptosistema za zaštitu biometrijskih šablona i kriptoloških ključeva. Razvoj mašinskog učenja i dubokih konvolucionih mreža, doveo je do sve češće primene neuronskih mreža za prepoznavanje i klasifikaciju objekata sa slika. Primarno, one su razvijene za klasifikaciju ulaznih podataka, tako da njihov izlaz predstavlja određivanje predefinisane klase nekog ulaznog podatka. Kako se tekstura otisaka prstiju u tradicionalnim biometrijskim sistemima većinski koristi samo za klasifikaciju, CNN su se prirodno nametnule kao nova generacija klasifikatora i otvorila se mogućnost istraživanja da li su te tehnike dovoljno uznapredovale da izdvoje biometrijska obeležja dovoljne diskriminativnosti da zamene odgovarajuće module za ekstrakciju u postojećim biometrijskim kriptosistemima.

Izdvajanje obeležja iz teksture otiska je u dosadašnjim šemama realizovana primenom banke Gaborovih filtara različitih prostornih radijalnih uglova. Glavni doprinos ove disertacije je predlog novog pristupa automatskom izdvajanju obeležja iz otiska prsta zasnovanom na konvolucionim neuronskim mrežama, koji je nadmašio prethodno ostvarene rezultate sistema baziranih na izdvajanju obeležja iz teksture otisaka prstiju. Tom prilikom testirane su tri najpoznatije konvolucione mreže, kako bi se procenila opšta primenljivost predloženog koncepta. Predložena šema je formirana da generiše obeležja fiksne dužine, što je prvi preduslov za formiranje biometrijskog kriptosistema na osnovu fazi povezivanja. Predložena je kvantizacija kodovanjem sa dva bita, kako bi se obeležja prevela u binarni domen i omogućila primena XOR biometrije, čime je ispunjen drugi preduslov. Problem varijabilnosti biometrijskih podataka rešava se mehanizmima

rekonstrukcije upotrebom kodova za korekciju grešaka. Detaljna analiza pokazala je ranjivost segmentnih tehnika za korekciju grešaka na napade zasnovane na statističkim podacima, pa je u skladu sa tim predložena BCH tehnika za korekciju grešaka, koja radi na nivou celog bloka dužine biometrijskog šablona. Kapacitet ispravljanja grešaka značajno je manji od polovine bloka koda, odnosno dužine šablona, pa je računski teško izvodljivo da se prevaziđe veliki korak kvantizacije u poznatim statističkim napadima na ovaj modul biometrijskog sistema. U skladu sa svim navedenim, formirana je šema fazi povezivanja sa maksimalnom dužinom kriptološkog ključa od 265 bita, uz prihvatljive margine greške, koji se može dalje koristiti u drugim savremenim kriptografskim sistemima. Istovremeno, na taj način je izvedena zaštita biometrijskog šablona, koji nije moguće rekonstruisati bez tajnog ključa. Evaluacija eksperimentalnih rezultata potvrđuje efektivnost predloženog pristupa, čime je ostvaren značajan napredak u polju biometrije i kriptografije.

5.2. Pregled naučnih doprinosa

U disertaciji je iznet predlog jedne klase biometrijskog kriptosistema za autentifikaciju sa zaštitom šablona i biometrijski zavisnim oslobađanjem kriptografskog ključa. Glavni naučni doprinos predstavlja nov pristup automatskom izdvajanju obeležja iz teksture otiska prsta, u potpunosti zasnovanom na dubokim konvolucionim neuronskim mrežama. Pored toga, ističu se sledeći doprinosi prikazani u radu:

1. Izvršena je sveobuhvatna analiza postojećih biometrijskih sistema, s posebnim osvrtom na pitanja privatnosti i sigurnosti biometrijskih podataka, koja je prethodila sintezi predloženog biometrijskog kriptosistema.

2. Unapređeni su postojeći pionirski sistemi za autentifikaciju bazirani na teksturi otisaka prstiju, primenom novih metoda za određivanje referentne tačke i tehnike određivanja pouzdanosti bita primenom Bajesove teoreme za određivanje aposteriorne verovatnoće i greške sistema.

3. Predložena je kvantizacija izdvojenih obeležja kodovanjem sa dva bita, čime su biometrijski šabloni prevedeni u binarni domen, što je omogućilo primenu Hemingove metrike za poređenje otisaka prstiju.

4. Generisanjem binarnih šablona otisaka prstiju fiksne dužine, postavljeni su okviri za formiranje biometrijskog kriptosistema fazi povezivanjem izdvojenih obeležja i kriptografskog ključa, uz primenu kodova za korekciju grešaka.

5. Analizom postojećih statističkih napada na biometrijske sisteme i sigurnosnih analiza šablona, potvrđena je neophodnost primene kodova za korekciju grešaka koji rade na nivou bloka, pa je umesto uobičajenih Adamarovih i Rid-Solomonovih kodova implementiran BCH kôd.

6. Predložena je primena tehnika za poboljšanje slike i segmentaciju regiona od interesa u odnosu na referentnu tačku, pre izdvajanja obeležja u CNN modulu. Izdvajanjem regiona od interesa sprečava se slučajno izdvajanje obeležja iz šuma koji je obično prisutan na periferiji slike otiska, čime je značajno povećana međuklasna diskriminativnost i smanjena je greška prihvatanja sistema.

7. Problem kratkih obučavajućih skupova, inherentan biometriji, rešen je generisanjem dodatnih instanci svake klase rotacijom izvornog otiska prsta, čime je povećana tačnost i neosetljivost sistema na uobičajene rotacije koje se javljaju prilikom uzorkovanja, što je eksperimentalno potvrđeno.

8. Predloženi biometrijski kriptosistem može upravljati ključevima dužine 265 bita, uz prihvatljivu marginu EER greške od 1%, što je značajno bolje u poređenju sa drugim sistemima baziranim na teksturi otisaka prstiju i zadovoljava potrebe savremenih kriptografskih sistema.

5.3. Predlog budućih istraživanja

S obzirom na važnost zaštite biometrijskih podataka, budući rad može biti usmeren na dalja unapređenja ovih tehnika zaštite i sistema upravljanja kriptografskim ključevima, pre svega fuzijom multibiometrije i kriptografije. Objedinjavanjem multimodalnih izdvojenih obeležja ili obeležja više instanci iste biometrijske karakteristike prostom konkatenacijom, mogle bi se ostvariti veće dužine ključeva. Pored automatskog izdvajanja obeležja konvolucionim neuronskim mrežama, predloženoj šemi bi mogle da se pridruže obeležja izdvojena nekom drugom tehnikom, ali uz preduslov da tako dobijena obeležja nisu u korelaciji, kako bi se izbegao negativan uticaj na sigurnost usled statističke povezanosti. Objedinjavanjem oba pomenuta pristupa, moguće je formirati hibridni biometrijski kriptosistem, primenom multimodalnih biometrijskih karakteristika i različitih algoritama u modulima za izdvajanje obeležja. Multibiometrija nudi mnogo novih mogućnosti za unapređenje postojećih rešenja.

Očekuje se da će prezentovana analiza mnogobrojnih biometrijskih sistema, kao i inovativni doprinos ove disertacije, poslužiti kao polazna osnova za dalja istraživanja, unapređenje postojećih rešenja i kao inspiracija za nove inovacije.

Literatura

[1] A. Bertillon, *Signaletic Instructions including the Theory and Practice of Anthropometrical Identification*, R. W. McClaughry Translation, The Werner Company, 1896.

[2] F. Galton, *Finger prints*, McMillan & Co., London and New York, 1892.

[3] S. Barzut, „Internet i elektronsko poslovanje“, ATSSB, 2020. [Online]. Available: https://www.tehnikum.edu.rs/predmeti/internet/ [Accessed: 17.02.2020]

[4] S. Barzut, M. Milosavljević, „Pregled savremenih sistema za biometrijsku autentifikaciju“, IV Naučni skup Mreža 2013. – Internet u edukacionom i poslovnom okruženju, Poslovni fakultet Valjevo, Univerzitet Singidunum, 2013, str. 18–23. [Online]. Available: http://poslovnifakultetvaljevo.edu.rs/konferencija-mreza-2013/ [Accessed: 19.02.2020]

[5] A. K. Jain, R. Bolle, S. Pankanti, “Introduction to Biometrics,” *Biometrics: Personal Identificationin Networked Society*, A. K. Jain, R. Bolle, S. Pankanti Eds. Kluwer Academic Publishers, pp. 1–41, 1996, doi:10.1007/0-306-47044-6_1.

[6] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, P. Van Oorschot, “The Future of Authentication,” IEEE Security & Privacy, vol.10, no. 1, pp. 22–27, 2012, doi:10.1109/MSP.2012.24.

[7] H. Cummins, C. Midlo, *Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics*, Blakiston Company, New Orleans, 1943.

[8] Scientific Working Group on Friction Ridge Analysis, Study and Technology, *The fingerprint sourcebook*, A. McRoberts Ed. National Institute of Justice, Washington, 2011.

[9] Federal bureau of investigation, *The Science of Fingerprints, Classification and Uses*, The Project Gutenberg EBook, 2006.

[10] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *Handbook of fingerprint recognition*, 2nd ed., London, England: Springer, 2009, doi:10.1007/978-1-84882-254-2.

[11] D. Maltoni, R. Cappelli, “Fingerprint recognition,” *Handbook of Biometrics*, A. K. Jain, F. Patrick, A. A. Ross, Eds. New York, NY: Springer Science+Business Media, pp. 23–42, 2008, doi:10.1007/978-0-387-71041-9_2.

[12] J. Daugman, “Iris recognition,” *Handbook of Biometrics*, A. K. Jain, F. Patrick, A. A. Ross, Eds. New York, NY: Springer Science+Business Media, pp. 71–90, 2008, doi:10.1007/978-0-387-71041-9_4.

[13] J. Daugman, “The importance of being random: statistical principles of iris recognition,” Pattern Recognition, vol. 36, no. 2, pp. 279–291, 2003, doi:10.1016/S0031-3203(02)00030-4.

[14] S. P. Fenker, E. Ortiz, K. W. Bowyer, “Template Aging Phenomenon in Iris Recognition,” in IEEE Access, vol. 1, pp. 266–274, 2013, doi:10.1109/ACCESS.2013.2262916.

[15] A. Bertillon, *La couleur de l’iris*, Revue Scientifique, 1885.

[16] J. H. Doggart, *Ocular Signs in Slit-lamp Microscopy*, Kimpton, London, 1949.

[17] J. Daugman, "How Iris Recognition Works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, 2004, doi:10.1109/tcsvt.2003.818350.

[18] F. Hao, R. Anderson, J. Daugman, "Combining cryptography with biometrics effectively," Technical Report 640, University of Cambridge, 2005.

[19] S. Adamović, V. Miškovic, N. Maček, M. Milosavljević, M. Šarac, M. Saračević, M. Gnjatović, "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," Future Generation Computer Systems, vol. 107, pp. 144–157, 2020, doi:10.1016/j.future.2020.01.056.

[20] A. K. Jain, A. Ross, K. Nandakumar, *Introduction to Biometrics*, Springer Science + Business Media, New York, 2011, doi:10.1007/978-0-387-77326-1.

[21] P. Viola, M. J. Jones, "Robust Real-Time Face Detection," International Journal of Computer Vision, vol. 57, no. 2, pp. 137–154, 2004, doi:10.1023/B:VISI.0000013087.49260.fb.

[22] M. Turk, A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991, doi:10.1162/jocn.1991.3.1.71.

[23] P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 711–720, 1997, doi:10.1109/34.598228.

[24] M. S. Bartlett, J. R. Movellan, T. J. Sejnowski, "Face recognition by independent component analysis," IEEE Transactions on Neural Networks, vol. 13, no. 6, pp. 1450–1464, 2002, doi:10.1109/tnn.2002.804287.

[25] L. Wiskott, J.-M. Fellous, N. Kuiger, C. von der Malsburg, "Face recognition by elastic bunch graph matching," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 775–779, 1997, doi:10.1109/34.598235.

[26] T. F. Cootes, K. Walker, C. J. Taylor, "View-based active appearance models," Proceedings Fourth IEEE International Conference on Automatic Face and Gesture Recognition (Cat. No. PR00580), France, pp. 227–232, 2000, doi:10.1109/afgr.2000.840639.

[27] V. Blanz, T. Vetter, "Face recognition based on fitting a 3D morphable model," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp. 1063–1074, 2003, doi:10.1109/tpami.2003.1227983.

[28] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," International Journal of Computer Vision, vol. 60, no. 2, pp. 91–110, 2004, doi:10.1023/b:visi.0000029664.99615.94.

[29] T. Ojala, M. Pietikainen, T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 7, pp. 971–987, 2002, doi:10.1109/tpami.2002.1017623.

[30] M. Wang, W. Deng, "Deep face recognition: A survey," Neurocomputing, vol. 429, pp. 215–244, 2021, doi:10.1016/j.neucom.2020.10.081.

[31] T. Martin, Y. Eady, J. Zhang, C. Sabol, A. Esterline, J. Mason, "The WebID Protocol Enhanced with Biometrics and a Federated Enrollment Protocol," 2019 SoutheastCon, 2019, doi:10.1109/southeastcon42311.2019.9020618.

[32] S. Bashbaghi, E. Granger, R. Sabourin, M. Parchami, "Deep Learning Architectures for Face Recognition in Video Surveillance," *Deep Learning in Object Detection and Recognition*, X. Jiang, A. Hadid, Y. Pang, E. Granger, X. Feng Eds, Springer, pp. 133–154, Singapur, 2019, doi:10.1007/978-981-10-5152-4_6.

[33] D. Zhong, X. Du, K. Zhong, "Decade progress of palmprint recognition: A brief survey," Neurocomputing, vol. 328, pp. 16–28, 2019, doi:10.1016/j.neucom.2018.03.081.

[34] M. Klonowski, M. Plata, P. Syga, "User authorization based on hand geometry without special equipment," Pattern Recognition, vol. 73, pp. 189–201, 2018, doi:10.1016/j.patcog.2017.08.017.

[35] N. Miura, A. Nagasaka, T. Miyatake, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles," IEICE Transactions on Information and Systems, vol. E90-D, no. 8, pp. 1185–1194, 2007, doi:10.1093/ietisy/e90-d.8.1185.

[36] A. Uhl, "State of the Art in Vascular Biometrics,", *Handbook of Vascular Biometrics*, A. Uhl, C. Busch, S. Marcel, R. Veldhuis Eds, Advances in Computer Vision and Pattern Recognition, Springer, Cham, pp. 3–61, 2020, doi:10.1007/978-3-030-27731-4_1.

[37] S. G. Kong, J. Heo, B. R. Abidi, J. Paik, M. A. Abidi, "Recent advances in visual and infrared face recognition—a review," Computer Vision and Image Understanding, vol. 97, no. 1, pp. 103–135, 2005, doi:10.1016/j.cviu.2004.04.001.

[38] M. K. Bhowmik, K. Saha, S. Majumder, G. Majumder, A. Saha, A. N. Sarma, D. Bhattacharjee, D. K. Basu, M. Nasipuri, "Thermal Infrared Face Recognition – A Biometric Identification Technique for Robust Security system," Reviews, Refinements and New Ideas in Face Recognition, 2011, doi:10.5772/18986.

[39] G. L. Marcialis, F. Roli, "Fingerprint verification by fusion of optical and capacitive sensors," Pattern Recognition Letters, vol. 25, no. 11, pp. 1315–1322, 2004, doi:10.1016/j.patrec.2004.05.011.

[40] A. Ross, A. Jain, J. Reisman, "A hybrid fingerprint matcher," Pattern Recognition, vol. 36, no. 7, pp. 1661–1673, 2003, doi:10.1016/s0031-3203(02)00349-7.

[41] Y. S. Moon, H. W. Yeung, K. C. Chan, S. O. Chan, "Template synthesis and image mosaicking for fingerprint registration: an experimental study," 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 409–412, Montreal, 2004, doi:10.1109/icassp.2004.1327134

[42] K. Nandakumar, Yi Chen, A. K. Jain, S. C. Dass, "Quality-based Score Level Fusion in Multibiometric Systems," 18th International Conference on Pattern Recognition (ICPR'06), pp. 473–476, 2006, doi:10.1109/icpr.2006.951.

[43] K. Nandakumar, Yi Chen, S. C. Dass, A. K. Jain, "Likelihood Ratio-Based Biometric Score Fusion," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, no. 2, pp. 342–347, Feb. 2008, doi:10.1109/tpami.2007.70796.

[44] J. Kittler, M. Hatef, R. P. W. Duin, J. Matas, "On combining classifiers," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226–239, Mar. 1998, doi:10.1109/34.667881.

[45] Y. Makihara, D. Muramatsu, Y. Yagi, M. A. Hossain, "Score-level fusion based on the direct estimation of the Bayes error gradient distribution," 2011 International Joint Conference on Biometrics (IJCB), pp. 1–8, 2011, doi:10.1109/ijcb.2011.6117532.

[46] T. K. Ho, J. J. Hull, S. N. Srihari, "Decision combination in multiple classifier systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 16, no. 1, pp. 66–75, 1994, doi:10.1109/34.273716.

[47] L. Lam, S. Y. Suen, "Application of majority voting to pattern recognition: an analysis of its behavior and performance," IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 27, no. 5, pp. 553–568, 1997, doi:10.1109/3468.618255.

[48] L. Kuncheva, *Combining Pattern Classifiers – Methods and Algorithms*, 2nd ed., John Wiley & Sons, 2014, doi:10.1002/9781118914564.

[49] A. K. Jain, A. Ross, S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006, doi:10.1109/tifs.2006.873653.

[50] A. Adler, "Biometric System Security," *Handbook of Biometrics*, A. K. Jain, F. Patrick, A. A. Ross, Eds. New York, NY: Springer Science+Business Media, pp. 381–402, 2008, doi:10.1007/978-0-387-71041-9_19.

[51] N. K. Ratha, J. H. Connell, R. M. Bolle, "An Analysis of Minutiae Matching Strength," Proceedings of Third International Conference on Audio and Video Based Biometric Person Authentication (AVBPA), pp. 223–228, 2001, doi:10.1007/3-540-45344-x_32.

[52] A. K. Jain, A. Ross, U. Uludag, "Biometric Template Security: Challenges and Solutions," Proceedings of the 13th European Signal Processing Conference, 2005.

[53] C. Hill, "Risk of masquerade arising from the storage of biometrics," Bachelor's thesis, Australian National University, Australia, 2001.

[54] A. Ross, J. Shah, A. K. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 544–560, 2007, doi:10.1109/tpami.2007.1018.

[55] R. Cappelli, D. Maio, A. Lumini, D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489–1503, Sep. 2007, doi:10.1109/tpami.2007.1087.

[56] A. K. Jain, K. Nandakumar, A. Nagar, "Biometric Template Security," EURASIP Journal on Advances in Signal Processing, vol. 2008, no. 1, 2008, doi:10.1155/2008/579416.

[57] Y. Luo, S. S. Cheung, S. Ye, "Anonymous Biometric Access Control based on homomorphic encryption," 2009 IEEE International Conference on Multimedia and Expo, 2009, doi:10.1109/icme.2009.5202677.

[58] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, pp. 614–634, 2001, doi:10.1147/sj.403.0614.

[59] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle, "Generating Cancelable Fingerprint Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007, doi:10.1109/tpami.2007.100.

[60] M. Upmanyu, A. M. Namboodiri, K. Srinathan, C. V. Jawahar, "Efficient Biometric Verification in Encrypted Domain," ICB '09: Proceedings of Third International Conference on Biometrics, pp. 899–908, 2009, doi:10.1007/978-3-642-01793-3_91.

[61] C. Rathgeb, A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP Journal on Information Security, vol. 2011, no. 1, 2011, doi:10.1186/1687-417x-2011-3.

[62] A. Juels, M. Wattenberg, "A fuzzy commitment scheme," Proceedings of the 6th ACM conference on Computer and communications security – CCS '99, 1999, doi:10.1145/319709.319714.

[63] A. Juels, M. Sudan, "A fuzzy vault scheme," Proceedings IEEE International Symposium on Information Theory, 2002, doi:10.1109/isit.2002.1023680.

[64] Y. J. Chang, W. Zhang, T. Chen, "Biometrics-based cryptographic key generation," 2004 IEEE International Conference on Multimedia and Expo (ICME), pp. 2203–2206, 2004, doi:10.1109/icme.2004.1394707.

[65] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," SIAM Journal on Computing, vol. 38, no. 1, pp. 97–139, 2008, doi:10.1137/060651380.

[66] Y. Sutcu, Q. Li, N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," 2007 IEEE Conference on Computer Vision and Pattern Recognition, 2007, doi:10.1109/cvpr.2007.383385.

[67] K. Nandakumar, A. K. Jain, "Multibiometric Template Security Using Fuzzy Vault," 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, Sep. 2008, doi:10.1109/btas.2008.4699352.

[68] A. Nagar, K. Nandakumar, A. K. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 255–268, 2012, doi:10.1109/tifs.2011.2166545.

[69] C. Soutar, G. J. Tomco, "Secure private key generation using a fingerprint," Cardtech/Securetech Conference Proceedings, Atlanta, pp. 245–252, 1996.

[70] Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar B. V., "Biometric encryption," *ICSA Guide to Cryptography*, R. K. Nichols Ed. McGrow-Hill, 1999.

[71] F. Monrose, M. K. Reiter, S. Wetzel, "Password hardening based on keystroke dynamics," Proceedings of the 6th ACM conference on Computer and communications security – CCS '99, pp. 73–82, 1999, doi:10.1145/319709.319720.

[72] F. Monrose, M. K. Reiter, Qi Li, S. Wetzel, "Cryptographic key generation from voice," Proceedings 2001 IEEE Symposium on Security and Privacy, pp. 202-213, 2001, doi:10.1109/secpri.2001.924299.

[73] H. Feng, C. C. Wah, "Private key generation from on-line handwritten signatures," Information Management & Computer Security, vol. 10, no. 4, pp. 159–164, 2002, doi:10.1108/09685220210436949.

[74] G. I. Davida, Y. Frankel, B. J. Matt, "On enabling secure applications through off-line biometric identification," Proceedings of The IEEE Symposium on Security and Privacy, pp. 148–157, 1998, doi:10.1109/secpri.1998.674831.

[75] T. C. Clancy, N. Kiyavash, D. J. Lin, "Secure smartcardbased fingerprint authentication," Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pp. 45–52, 2003, doi:10.1145/982507.982516.

[76] K. Nandakumar, A. K. Jain, S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744–757, 2007, doi:10.1109/tifs.2007.908165.

[77] X. Wu, N. Qi, K. Wang, D. Zhang, "A Novel Cryptosystem Based on Iris Key Generation," 2008 Fourth International Conference on Natural Computation, pp. 53–56, 2008, doi:10.1109/icnc.2008.808.

[78] X. Wu, K. Wang, D. Zhang, "A cryptosystem based on palmprint feature," 19th International Conference on Pattern Recognition, pp. 1–4, 2008, doi:10.1109/icpr.2008.4761117.

[79] A. K. Jain, S. Prabhakar, L. Hong, S. Pankanti, "Filterbank-based fingerprint matching," IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846–859, 2000, doi:10.1109/83.841531.

[80] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical Biometric Authentication with Template Protection," Audio- and Video-Based Biometric Person Authentication, pp. 436–446, 2005, doi:10.1007/11527923_45.

[81] S. Barzut, M. Milosavljević, "A method of forming an XOR biometrics from fingerprints by using Gabor filtration," Sinteza 2014 – Impact of the Internet on Business Activities in Serbia and Worldwide, Belgrade, Singidunum University, Serbia, pp. 610–615, 2014, doi:10.15308/sinteza-2014-610-615.

[82] Y. Imamverdiyev, A. B. J. Teoh, J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," Expert Systems with Applications, vol. 40, no. 5, pp. 1888–1901, 2013, doi:10.1016/j.eswa.2012.10.009.

[83] D. Michelsanti, A.-D. Ene, Y. Guichi, R. Stef, K. Nasrollahi, T. B. Moeslund, "Fast Fingerprint Classification with Deep Neural Networks," Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, pp. 202–209, 2017, doi:10.5220/0006116502020209.

[84] K. Chatfield, K. Simonyan, A. Vedaldi, A. Zisserman, "Return of the Devil in the Details: Delving Deep into Convolutional Nets," Proceedings of the British Machine Vision Conference 2014, pp. 1–11, 2014, doi:10.5244/c.28.6.

[85] F. Wu, J. Zhu, X. Guo, "Fingerprint pattern identification and classification approach based on convolutional neural networks," Neural Computing and Applications, vol. 32, no. 10, pp. 5725–5734, 2020, doi:10.1007/s00521-019-04499-w.

[86] W. Jian, Y. Zhou, H. Liu, "Lightweight Convolutional Neural Network Based on Singularity ROI for Fingerprint Classification," IEEE Access, vol. 8, pp. 54554–54563, 2020, doi:10.1109/access.2020.2981515.

[87] S. Ge, C. Bai, Y. Liu, Y. Liu, T. Zhao, "Deep and discriminative feature learning for fingerprint classification," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, doi:10.1109/compcomm.2017.8322877.

[88] B. Bakhshi, H. Veisi, "End to End Fingerprint Verification Based on Convolutional Neural Network," 2019 27th Iranian Conference on Electrical Engineering (ICEE), pp. 1994–1998, 2019, doi:10.1109/iraniancee.2019.8786720.

[89] A. Krizhevsky, I. Sutskever, G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Communications of the ACM, vol. 60, no. 6, pp. 84–90, 2017, doi:10.1145/3065386.

[90] V. H. Nguyen, J. Liu, T. H. B. Nguyen, H. Kim, "Universal fingerprint minutiae extractor using convolutional neural networks," IET Biometrics, vol. 9, no. 2, pp. 47–57, 2019, doi:10.1049/iet-bmt.2019.0017.

[91] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, M. Gnjatović, "A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks," Mathematics, vol. 9, no. 7, p. 730, 2021, doi:10.3390/math9070730.

[92] E. Zhu, X. Guo, J. Yin, "Walking to singular points of fingerprints," Pattern Recognition, vol. 56, pp. 116–128, 2016, doi:10.1016/j.patcog.2016.02.015.

[93] P. Kovesi, "MATLAB and Octave functions for computer vision and image processing". [Online]. Available: https://www.peterkovesi.com/matlabfns [Accessed: 28.10.2019]

[94] R. Thai, "Fingerprint image enhancement and minutiae extraction," The University of Western Australia, 2003.

[95] C. Szegedy, Wei Liu, Yangqing Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, A. Rabinovich, "Going deeper with convolutions," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1–9, 2015, doi:10.1109/cvpr.2015.7298594.

[96] K. He, X. Zhang, S. Ren, J. Sun, "Deep Residual Learning for Image Recognition," 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016, doi:10.1109/cvpr.2016.90.

[97] A. Stoianov, T. Kevenaar, M. van der Veen, "Security issues of Biometric Encryption," 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH), 2009, doi:10.1109/tic-sth.2009.5444478.

[98] R. C. Bose, D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," Information and Control, vol. 3, no. 1, pp. 68–79, 1960, doi:10.1016/s0019-9958(60)90287-4.

Jedna klasa biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama

ORIGINALITY REPORT

7%
SIMILARITY INDEX

PRIMARY SOURCES

1	singipedia.singidunum.ac.rs Internet	1097 words — 3%
2	eprints.ugd.edu.mk Internet	204 words — 1%
3	Srđan Barzut, Milan Milosavljević, Saša Adamović, Muzafer Saračević, Nemanja Maček, Milan Gnjatović. "A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks", Mathematics, 2021 Crossref	128 words — < 1%
4	poslovnifakultetvaljevo.edu.rs Internet	106 words — < 1%
5	www.mdpi.com Internet	99 words — < 1%
6	www.tehnikum.edu.rs Internet	80 words — < 1%
7	www.singipedia.singidunum.ac.rs Internet	61 words — < 1%
8	www.ito.umnw.ethz.ch Internet	53 words — < 1%

9	Srđan Barzut, Milan Milosavljević. "Jedan metod formiranja XOR biometrije otisaka prstiju Gaborovom filtracijom", Proceedings of the 1st International Scientific Conference - Sinteza 2014, 2014 Crossref	52 words	< 1%
10	link.springer.com Internet	38 words	< 1%
11	nardus.mpn.gov.rs Internet	36 words	< 1%
12	hrsltd.com Internet	31 words	< 1%
13	2009.telfor.rs Internet	28 words	< 1%
14	uvidok.rcub.bg.ac.rs Internet	25 words	< 1%
15	www.scribd.com Internet	25 words	< 1%
16	repozitorij.unizg.hr Internet	22 words	< 1%
17	www.bond.hr Internet	19 words	< 1%
18	citeseerx.ist.psu.edu Internet	17 words	< 1%
19	John Daugman, Cathryn Downing. "Epigenetic randomness, complexity and singularity of	15 words	< 1%

human iris patterns", Proceedings of The Royal Society B Biological Sciences, 08/22/2001
Crossref

20	core.ac.uk Internet	15 words — < 1%
21	repozitorij.unidu.hr Internet	14 words — < 1%
22	hdl.handle.net Internet	12 words — < 1%
23	idoc.pub Internet	12 words — < 1%
24	repozitorij.etfos.hr Internet	12 words — < 1%
25	repozitorij.mefos.hr Internet	12 words — < 1%
26	file.allitebooks.com Internet	11 words — < 1%
27	repozitorij.foi.unizg.hr Internet	11 words — < 1%
28	www.freshpatents.com Internet	11 words — < 1%
29	archive.org Internet	10 words — < 1%
30	biometrics.cse.msu.edu Internet	10 words — < 1%

31	www.coursehero.com Internet	10 words — < 1%
32	Lecture Notes in Computer Science, 2005. Crossref	9 words — < 1%
33	istocar.bg.ac.rs Internet	9 words — < 1%
34	minerva.usc.es Internet	9 words — < 1%
35	poincare.matf.bg.ac.rs Internet	9 words — < 1%
36	www.cris.uns.ac.rs Internet	9 words — < 1%
37	www.slideshare.net Internet	9 words — < 1%
38	zir.nsk.hr Internet	9 words — < 1%
39	M. S. AlTarawneh, W.L. Woo, S.S. Dlay. "Fuzzy Vault Crypto Biometric Key Based on Fingerprint Vector Features", 2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008 Crossref	8 words — < 1%
40	M.U. Munir, M.Y. Javed. "Fingerprint Matching using Ridge Patterns", 2005 International Conference on Information and Communication Technologies, 2005 Crossref	8 words — < 1%

41	bib.irb.hr Internet	8 words — < 1%
42	fr.scribd.com Internet	8 words — < 1%
43	kupdf.net Internet	8 words — < 1%
44	repozitorij.svkst.unist.hr Internet	8 words — < 1%
45	rik.mrizp.rs Internet	8 words — < 1%
46	symopis.vggs.rs Internet	8 words — < 1%
47	tel.archives-ouvertes.fr Internet	8 words — < 1%
48	www.sersc.org Internet	8 words — < 1%
49	www.sremturizam.org Internet	8 words — < 1%
50	Kai Cao, Anil K. Jain. "Learning Fingerprint Reconstruction: From Minutiae to Image", IEEE Transactions on Information Forensics and Security, 2015 Crossref	7 words — < 1%
51	eteze.bg.ac.rs Internet	7 words — < 1%
52	Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. "Handbook of Fingerprint Recognition",	6 words — < 1%

Springer Nature, 2009
Crossref

53 blog.b92.rs
Internet

6 words — < 1%

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON
EXCLUDE MATCHES OFF