

# Jedna klasa kriptografski zaštićene autentifikacije klijenata zasnovana na opozivoj biometriji

*By* Miloš Jovanović

Univerzitet Singidunum  
Departman za poslediplomske studije

Doktorska disertacija

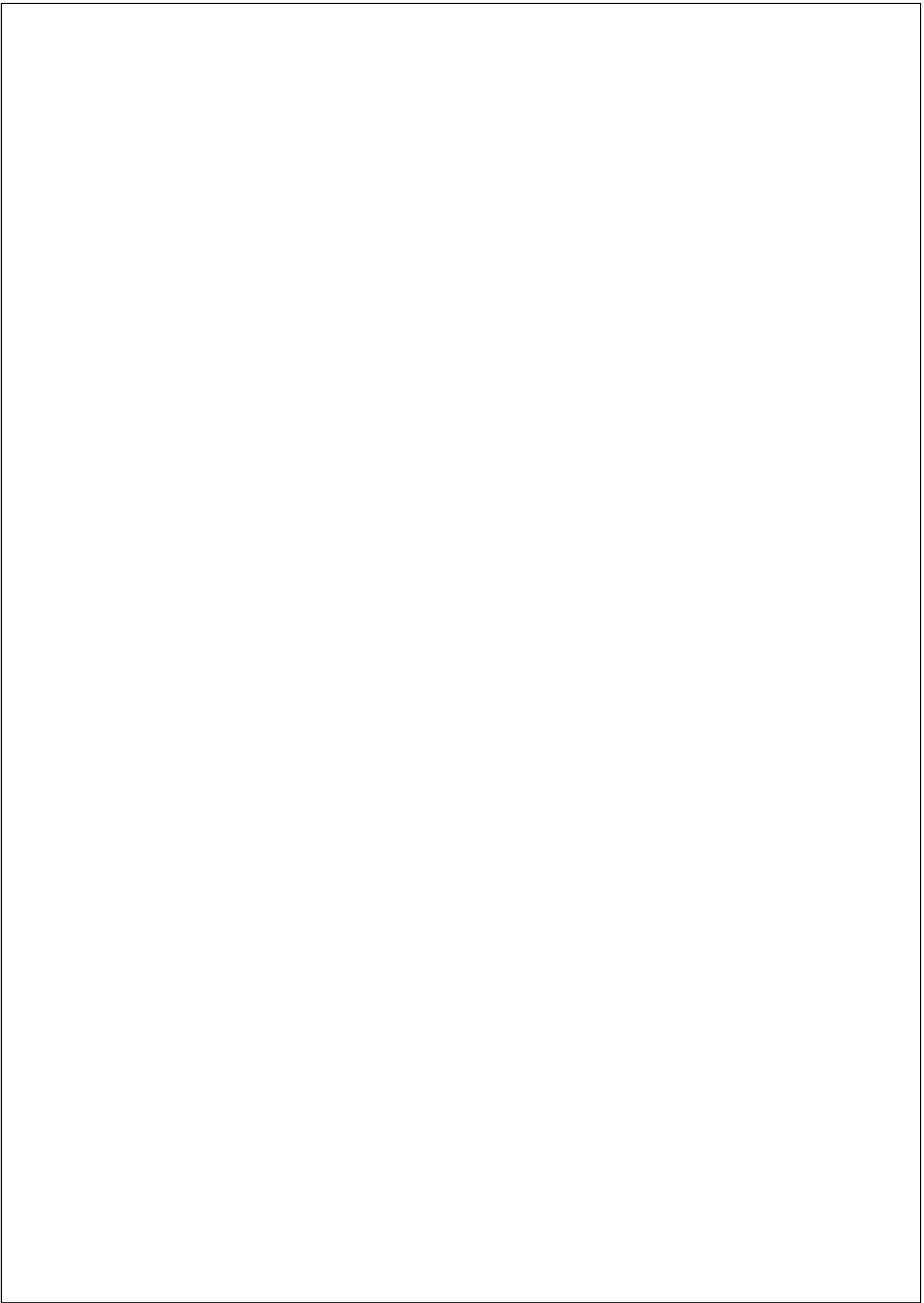
# Jedna klasa kriptografski zaštićene autentifikacije klijenata zasnovana na opozivoj biometriji

Mentor: prof. dr Milan M. Milosavljević Student: Miloš

Jovanović

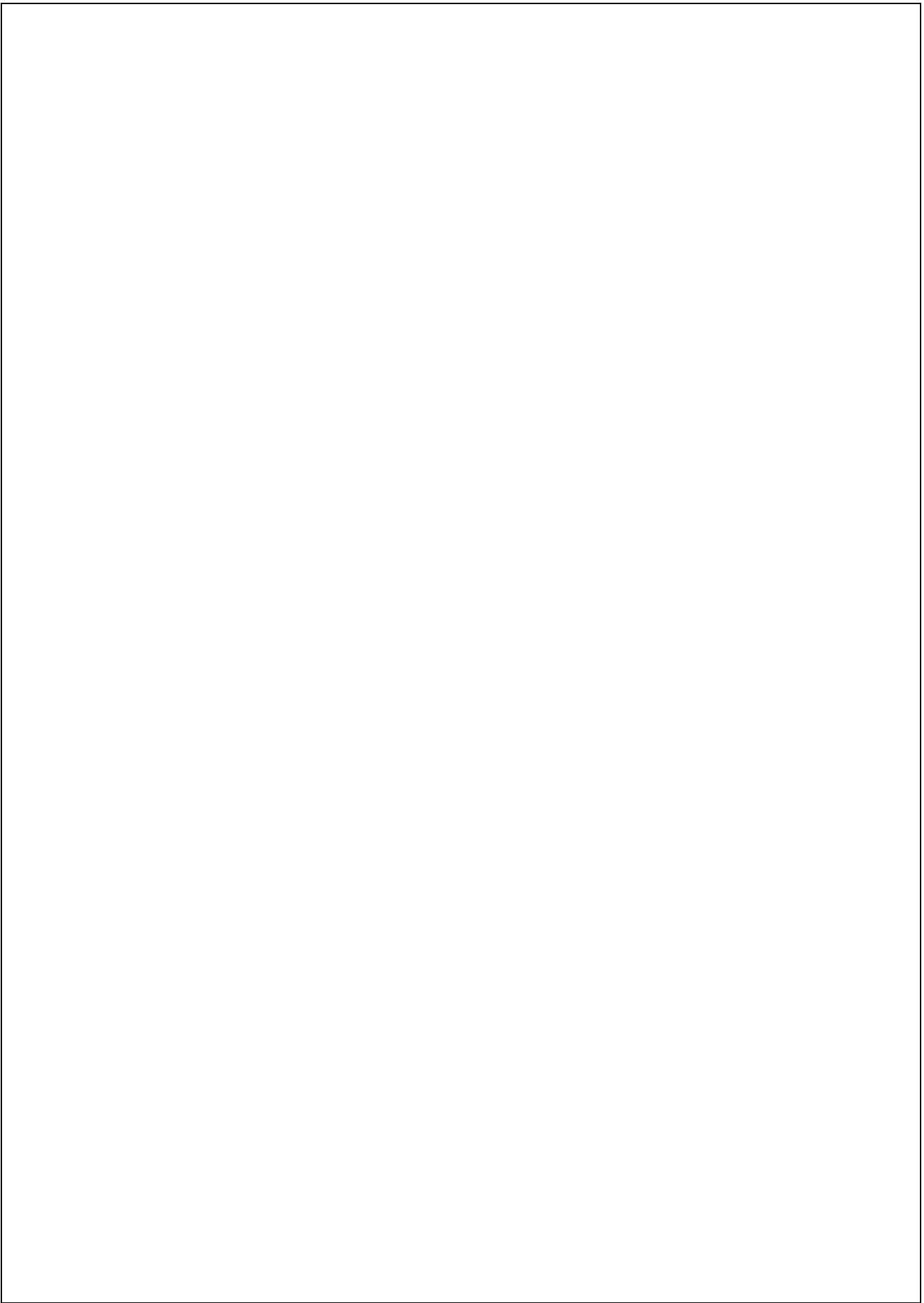
Broj indeksa: 460075/2015

Beograd,  
jun 2020. godine



Zahvaljujem se svojoj porodici i mentoru prof. dr Milanu M. Milosavljeviću.

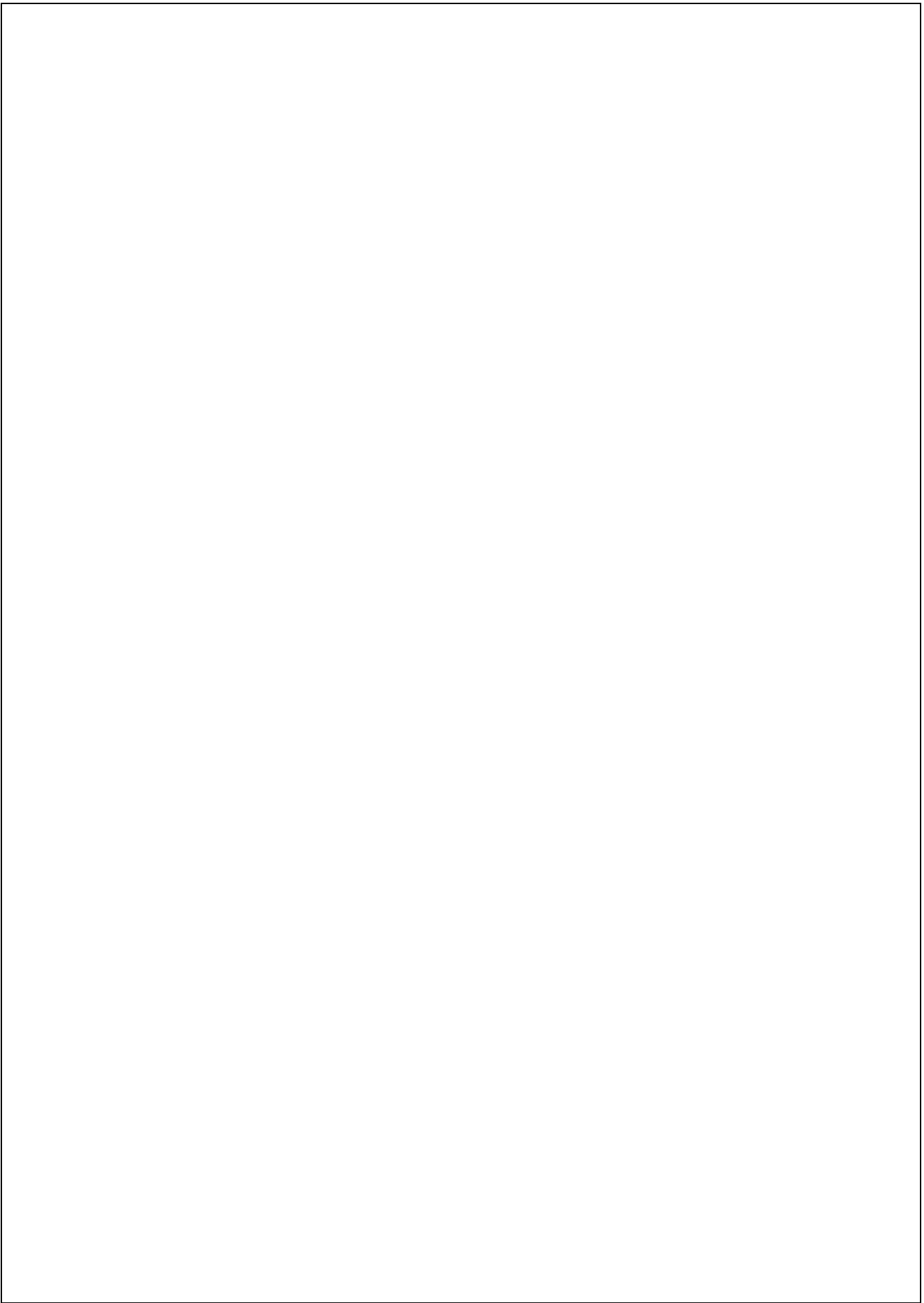




## Sažetak

U ovom radu je predstavljen jedan novi pristup kriptografski zaštićenoj bio- metrijskoj autentifikaciji korisnika, zasnovan na kriptografiji sa javnim ključevima, generatoru pseudoslučajnih brojeva i opozivoj biometriji. Biometrijski šabloni su šifrovani ili opozivi tokom svih faza u radu sistema, izuzev u fazi izdvajanja obeležja, što rezultuje sistemom koji je otporan na veliki broj napada. Sistem nije procesorski zahtevan, a generisani biometrijski šabloni su prihvatljive veličine.

Predloženi pristup kriptografski zaštićenoj autentifikaciji je implementiran kroz modularni biometrijski sistem za proveru identiteta korisnika usluga mobilnog bankarstva bazirane na biometriji dužice ljudskog oka. Saopšteni su pozitivni rezultati analize performansi predloženog sistema na realističnom skupu podataka, i ispitivanja slučajnosti šifrovanih opozivih šablona i podataka koji se prenose preko mreže.



# Abstract

This work proposes a novel approach to cryptographically secure biometric authentication based on cryptography with public keys, pseudo-random number generator and cancelable biometrics. The biometric templates are encrypted or cancelable during all the stages of the system's use except the feature extraction stage, which makes the approach secure against a number of attacks. In addition, the system is not computationally demanding, and the size of biometric templates is acceptable.

The proposed approach to cryptographically secure authentication is implemented through a modular biometric system for mobile banking user verification, based on the human eye iris biometrics. Both the system performance and the randomness of the biometric templates and the data transferred over the network in this use scenario are positively evaluated on realistic data.

v



# Sadržaj

|                                                                             |            |
|-----------------------------------------------------------------------------|------------|
|                                                                             | i          |
| <b>Sažetak</b>                                                              | <b>iii</b> |
| <b>Abstract</b>                                                             | <b>v</b>   |
| <b>Lista slika</b>                                                          | <b>xi</b>  |
| <b>Lista tabela</b>                                                         | <b>xv</b>  |
| <b>1 Uvod</b>                                                               | <b>1</b>   |
| 1.1 Opštarazmatranja . . . . .                                              | 1          |
| 1.2 Predmet, cilj i doprinosi istraživanja . . . . .                        | 2          |
| 1.3 Struktura rada . . . . .                                                | 3          |
| <b>2 Pregled u oblasti istraživanja</b>                                     | <b>5</b>   |
| 2.1 Upotreba opozive biometrije . . . . .                                   | 9          |
| 2.1.1 pristupi zasnovani na neinvertibilnim transformacijama .              | 10         |
| 2.1.2 pristupi zasnovani na biometrijskom soljenju.....                     | 13         |
| 2.1.3 Ostali značajniji pristupi u opozivoj biometriji.....                 | 14         |
| 2.1.4 Kratki osvrt na sigurnost opozive biometrije.....                     | 16         |
| 2.2 Kriptografska zaštita biometrijskih šablona .....                       | 17         |
| 2.2.1 Biometrijski kriptosistemi.....                                       | 17         |
| 2.2.2 Kratki osvrt na sigurnost biometrijskih kriptosistema.....            | 23         |
| 2.2.3 Primena kriptografije za zaštitu biometrijskih uzoraka i šablona..... | 23         |
| <b>3 Teorijske osnove istraživanja</b>                                      | <b>31</b>  |

|          |                                                                                                                                                                    |           |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 3.1      | Kriptografija sa javnim ključevima . . . . .                                                                                                                       | 31        |
| 3.1.1    | Algoritam RSA . . . . .                                                                                                                                            | 31        |
| 3.1.2    | Binarno potenciranje . . . . .                                                                                                                                     | 35        |
| 3.2      | Generatori pseudoslučajnih brojeva . . . . .                                                                                                                       | 36        |
| 3.2.1    | Osnovni pojmovi . . . . .                                                                                                                                          | 37        |
| 3.2.2    | Ispitivanje približne entropije . . . . .                                                                                                                          | 39        |
| 3.3      | Koderi i interliveri . . . . .                                                                                                                                     | 41        |
| 3.3.1    | Zaštitni koderi . . . . .                                                                                                                                          | 41        |
| 3.3.1.1  | Primer linearnog zaštitnog koda . . . . .                                                                                                                          | 43        |
| 3.3.1.2  | Primer konvolucionog zaštitnog koda . . . . .                                                                                                                      | 44        |
| 3.3.2    | Interliveri . . . . .                                                                                                                                              | 45        |
| 3.3.2.1  | Primer blokovskog interlivera . . . . .                                                                                                                            | 45        |
| 3.3.2.2  | Primer konvolucionog interlivera . . . . .                                                                                                                         | 47        |
| 3.4      | Neinvertibilne transformacije . . . . .                                                                                                                            | 47        |
| 3.4.1    | Jednosmerne funkcije sa zamkom . . . . .                                                                                                                           | 47        |
| 3.4.2    | Transformacije digitalnih slika . . . . .                                                                                                                          | 50        |
| <b>4</b> | <b>Predlog radnog okvira i jedne implementacije</b>                                                                                                                | <b>53</b> |
| 4.1      | Modularni sistemi za biometrijsku proveru identiteta sa distribu-<br>iranim skladištenjem šifrovanih opozivih šablona.....                                         | 55        |
| 4.1.1    | Osvrt na sigurnost i ograničenja predloženog rešenja.....                                                                                                          | 57        |
| 4.2      | Modularni sistemi za biometrijsku proveru identiteta sa centrali-<br>zovanim skladištenjem šifrovanih opozivih šablona.....                                        | 60        |
| 4.2.1    | Osvrt na sigurnost i ograničenja predloženog rešenja.....                                                                                                          | 62        |
| 4.3      | Jedna primena sistema sa distribuiranim skladištenjem za proveru<br>identiteta korisnika usluga mobilnog bankarstva koja je zasnovana<br>na biometriji dužice..... | 63        |
| 4.3.1    | Osvrt na sigurnost predložene implementacije.....                                                                                                                  | 67        |
| <b>5</b> | <b>Analiza eksperimentalnih rezultata sa realističnim podacima</b>                                                                                                 | <b>73</b> |
| 5.1      | Prepoznavanje dužice.....                                                                                                                                          | 73        |
| 5.1.1    | Segmentacija, normalizacija i kodovanje dužice.....                                                                                                                | 74        |
| 5.1.2    | Klasifikacija na osnovu dužice.....                                                                                                                                | 79        |

|                                          |            |
|------------------------------------------|------------|
|                                          | ix         |
| 5.2 Performanse predloženog sistema..... | 80         |
| 5.3 Ispitivanje slučajnosti.....         | 83         |
| <b>6 Kritička analiza i zaključak</b>    | <b>89</b>  |
| 6.1 Zaključak i rezime doprinosa.....    | 90         |
| 6.2 Smernice zadalja istraživanja.....   | 91         |
| <b>Bibliografija</b>                     | <b>93</b>  |
| <b>Indeks</b>                            | <b>107</b> |



# Lista slika

|      |                                                                                                                                                                                                                                                                                                                                                                                                             |    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 2.1  | Jedan primer primene opozive biometrije dužice: originalna tekstura dužice (gore) i blok permutacija tekstone (dole). Slika preuzeta iz [99].                                                                                                                                                                                                                                                               | 9  |
| 2.2  | Dva primera biometrijske promenljivosti koja se odnose na otisak prsta i dužicu. Slika preuzeta iz [76]. Originalni biometrijski uzorci su preuzeti iz FCV ( <a href="http://bias.csr.unibo.it/fvc2004/databases.asp">http://bias.csr.unibo.it/fvc2004/databases.asp</a> ) i CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baza podataka biometrijskih uzoraka. | 18 |
| 2.3  | Generička šema sistema za vezivanje ključeva.                                                                                                                                                                                                                                                                                                                                                               | 19 |
| 2.4  | Generička šema sistema za generisanje ključeva na osnovu biometrijskog šablona.                                                                                                                                                                                                                                                                                                                             | 20 |
| 3.1  | Ilustracija modela komunikacionog kanala sa zaštitnim koderima.                                                                                                                                                                                                                                                                                                                                             | 41 |
| 3.2  | Ilustracija Viterbijevog trelisa (slika prilagođena iz [84]).                                                                                                                                                                                                                                                                                                                                               | 45 |
| 3.3  | Ilustracija dekodovanja početne poruke na osnovu Viterbijevog trelisa (slika prilagođena iz [84]).                                                                                                                                                                                                                                                                                                          | 45 |
| 3.4  | Ilustracija modela komunikacionog kanala sa zaštitnim koderima i interliverima.                                                                                                                                                                                                                                                                                                                             | 46 |
| 3.5  | Ilustracija blokovskog interlivera.                                                                                                                                                                                                                                                                                                                                                                         | 46 |
| 3.6  | Konvolucioni interliver (slika prilagođena iz [113]).                                                                                                                                                                                                                                                                                                                                                       | 48 |
| 3.7  | Četiri stanja konvolucionog interlivera za ulaz (3.73), (slike prilagođene iz [113]).                                                                                                                                                                                                                                                                                                                       | 48 |
| 3.8  | Ilustracija izobličenja mreže slike: (a) pre i (b) posle transformacije.                                                                                                                                                                                                                                                                                                                                    | 50 |
| 3.9  | Ilustracija permutacija blokova slike: (a) pre i (b) posle transformacije.                                                                                                                                                                                                                                                                                                                                  | 50 |
| 3.10 | Ilustracija neinvertibilnog preslikavanja izdvojenih obeležja (prilagođeno iz [92]).                                                                                                                                                                                                                                                                                                                        | 51 |

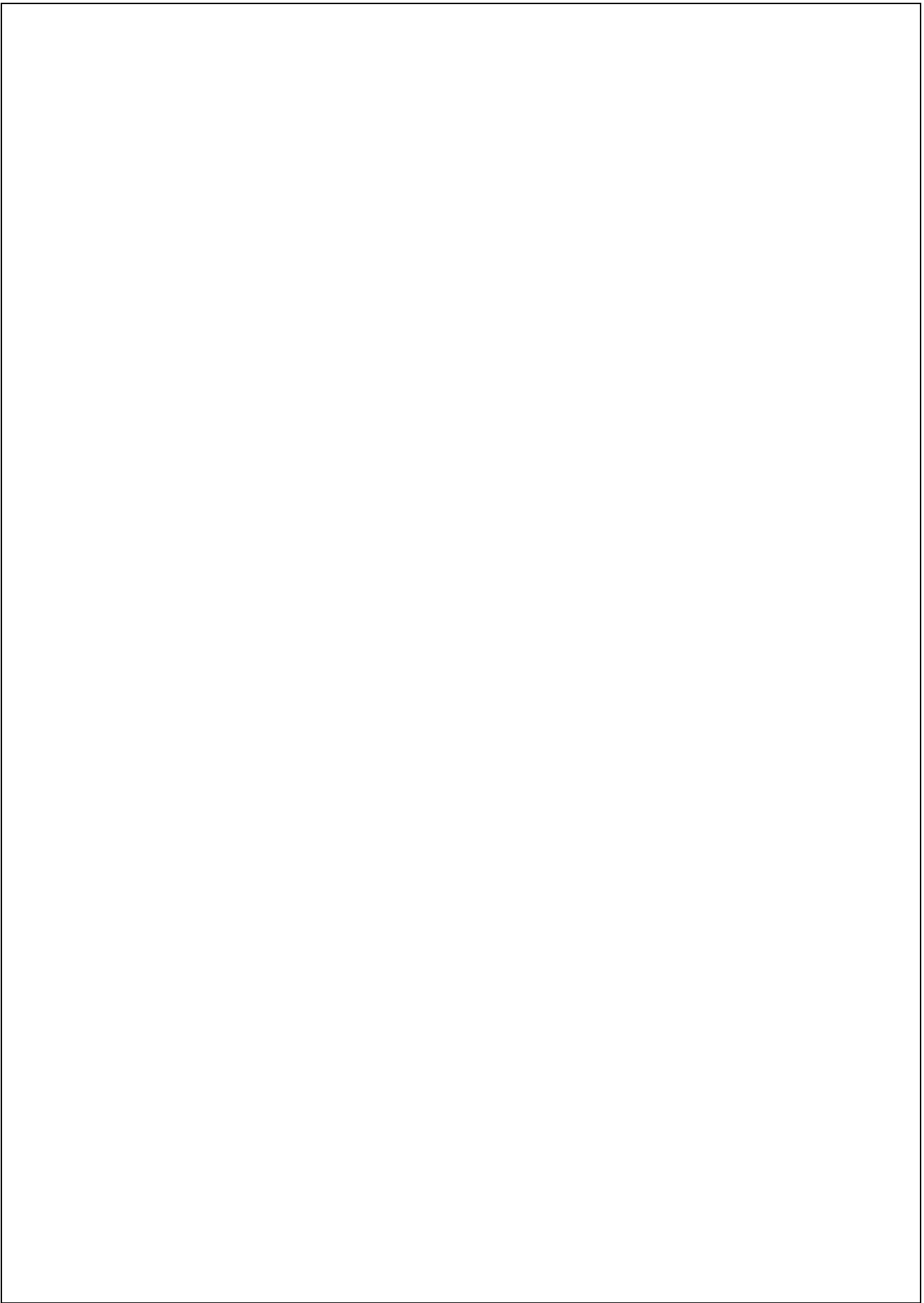
|     |                                                                                                                                                                                                                |    |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.1 | Faza upisa i verifikacije korisnika u modularnom sistemu sa distri- buiranim skladištenjem. Izvorni oblik slike može se naći u [75]. .....                                                                     | 58 |
| 4.2 | Faza upisa korisnika u modularnom sistemu sa centralizovanim skla- dištenjem. Izvorni oblik slike može se naći u [75]. .....                                                                                   | 61 |
| 4.3 | Faza verifikacije korisnika u modularnom sistemu sa centralizovanim skladištenjem. Izvorni oblik slike može se naći u [75]. .....                                                                              | 62 |
| 4.4 | Faza upisa korisnika u sistemu za proveru identiteta korisnika usluga mobilnog bankarstva. Izvorni oblik slike može se naći u [77]. .....                                                                      | 66 |
| 4.5 | Faza verifikacije korisnika u sistemu za proveru identiteta korisnika usluga mobilnog bankarstva. Izvorni oblik slike može se naći u [77]. .....                                                               | 67 |
| 4.6 | Algoritam za upis korisnika. ....                                                                                                                                                                              | 68 |
| 4.7 | Algoritam za verifikaciju korisnika. ....                                                                                                                                                                      | 68 |
| 4.8 | Podaci koji se čuvaju i podaci koji se prenose. Izvorni oblik slike može se naći u [77]. .....                                                                                                                 | 70 |
| 5.1 | Slika oka, preuzeto iz CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baze poda- taka biometrijskih uzoraka. ....                                                   | 74 |
| 5.2 | Ilustracija rezultata primene Canny edge detektora na sl. 5.1, preuzeto iz CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baze podataka biometrijskih uzoraka. .... | 74 |
| 5.3 | Primer detektovanja kružnica zenice i dužice na sl. 5.1, preuzeto iz CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baze podataka biometrijskih uzo- raka. ....     | 76 |
| 5.4 | Primeri uspešne segmentacije dužice, preuzeto iz CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baze podataka biometrijskih uzoraka. ....                           | 76 |
| 5.5 | Primeri neuspešne segmentacije dužice, , preuzeto iz CASIA ( <a href="http://biometrics.idealtest.org/">http://biometrics.idealtest.org/</a> ) baze podataka biometrijskih uzoraka. ....                       | 77 |
| 5.6 | Uobičajeno ilustrovanje postupka normalizacije primenom Daugman-ovog modela Rubber Sheet. ....                                                                                                                 | 77 |
| 5.7 | Normalizacija dužice date na sl. 5.1. ....                                                                                                                                                                     | 78 |
| 5.8 | Kodovanje dužice date na sl. 5.1. ....                                                                                                                                                                         | 79 |
| 5.9 | Maska šuma za dužicu datu na sl. 5.1. ....                                                                                                                                                                     | 79 |

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| 5.10 Performanse sistema sa niskim pragom poređenja (plavom bojom je ozna-<br>čen FAR, crvenom FRR). .....  | 82 |
| 5.11 Performanse sistema sa visokim pragom poređenja (plavom bojom je ozna-<br>čen FAR, crvenom FRR). ..... | 82 |



## Lista tabela

|     |                                                                                                                                                      |    |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.1 | Izabrani generatori pseudoslučajnih brojeva (tabela prilagođena iz [47]).                                                                            | 37 |
| 3.2 | NIST testovi za proveru slučajnosti proizvoljno dugačkih binarnih sekvenci [106].                                                                    | 39 |
| 5.1 | Ispitivanje performansi sistema (slike dužice su generisane prednjom kamerom mobilnog telefona). Tabela preuzeta iz [77].                            | 81 |
| 5.2 | Sumarni rezultati ispitivanja slučajnosti šifrovanog opozivog šablona. Redni brojevi testova su usklađeni sa rednim brojevima u opisu.               | 86 |
| 5.3 | Sumarni rezultati ispitivanja slučajnosti podataka koji se prenose preko mreže. Redni brojevi testova su usklađeni sa rednim brojevima u tabeli 5.2. | 87 |



# Glava 1

## Uvod

### 1.1 Opšta razmatranja

Biometrijska autentifikacija je proces utvrđivanja identiteta zasnovan na fiziološkim ili ponašajnim osobinama korisnika. Biometrija se može posmatrati kao jedan uslovno idealan način autentifikacije: korisnici ne moraju da pamte lozinke ili nose uređaje na kojima su smešteni autentifikacioni podaci, dok su biometrijske karakteristike u osnovi neopozive, čime se obezbeđuje i servis neposrednosti. Međutim, kao i bilo koji lični podaci, biometrijski šabloni mogu se presresti, ukrasti, reprodukovati ili izmeniti, što može dovesti do krađe identiteta. Imajući to u vidu, može se zaključiti da biometrijski sistemi obrađuju osetljive lične podatke, kao i da su sigurnost i privatnost biometrijskih šablona važna pitanja na koja treba obratiti pažnju prilikom projektovanja sistema za proveru identiteta. Krađa identiteta se sprečava tehnološkim protivmerama koje pružaju jaku sigurnost biometrijskih šablona i zaštitu privatnosti korisnika. Međutim, mere tehnološke zaštite ne smeju da naruše performanse sistema do nivoa da upotreba sistema više nije praktična, npr. opterećivanjem sistema dodatnim procesorski zahtevnim matematičkim operacijama ili zahtevom za dodatnim prostorom za skladištenje.

Pored kriptografske sigurnosti, očekuje se da biometrijski sistem pruža snažnu zaštitu privatnosti, što rezultuje sledećim skupom zahteva. Biometrijski šabloni treba da ostanu šifrovani ili u najgorem slučaju opozivi tokom svih faza upotrebe (skladištenje, prenos i verifikacija). Nijedan klijent ne sme da

pristupi privatnim ključevima koji se nalaze na autentifikacionom serveru, jer se na taj način može ugroziti sigurnost biometrijskih šablona. Takođe, sistem bi trebao biti otporan na zamenu šablona i sve napade niskog nivoa, u sistem se ne smeju unositi procesorski isuviše zahtevne operacije, a kriptografske protokole ne smeju umanjiti ukupnu tačnost (tj. ne smeju povećavati stepen lažnog prihvatanja ili stepen lažnog odbijanja).

## 1.2 Predmet, cilj i doprinosi istraživanja

Polazeći od shvatanja da su biometrijski podaci neopozivi u prirodi, i da kompromitovanje biometrijskih šablona može dovesti do krađe identiteta korisnika, što za posledicu može imati različite oblike zloupotrebe, ovaj rad razmatra sledeće hipoteze.

**Hipoteza 1.** Trenutna rešenja za zaštitu biometrijskih šablona ne obezbeđuju dovoljno visok nivo sigurnosti šablona i privatnosti korisnika.

**Hipoteza 2.** Razvojem sopstvenog biometrijskog sistema u kom biometrijski šabloni ostaju šifrovani ili u najgorem slučaju opozivi tokom svih faza njihove primene (skladištenje, prenos i verifikacija) obezbeđuje se upotrebljivost predložene pristupa u realnim domenima primene.

Naučni cilj ovog rada je da se predstavi jedan novi način kriptografski zaštićene autentifikacije klijenata pomoću biometrijskih podataka koji, u poređenju sa dosadašnjim istraživanjima i dostignućima u ovoj oblasti, unapređuje sigurnost i garantuje autentičnost prilikom provere identiteta korisnika. Posebna pažnja je posvećena analizi postojećih rešenja za zaštitu biometrijskih sistema za proveru identiteta sa aspekta sigurnosti i zaštite privatnosti. Namena ove analize je da se prikaže efikasnost postojećih rešenja, i da se pruži osnova za predlaganje novog pristupa koji bi efikasno odgovorio na nedostatke postojećih rešenja.

Tehnički cilj ovog rada je da se predloženi način kriptografski zaštićene autentifikacije klijenata implementira kroz modularni biometrijski sistem za proveru identiteta. Sistem koristi kriptografiju sa javnim ključevima, generator pseudoslučajnih brojeva i opozivu biometriju. Neinvertibilna transformacija se

izvršava pomoću ključa koji se nalazi na sigurnom memorijskom skladištu uređaja. Biometrijski šabloni su šifrovani ili, u najgorem slučaju, opozivi tokom svih faza u radu sistema, izuzev u fazi izdvajanja obeležja, što rezultuje sistemom koji je otporan na veliki broj napada. Predloženi sistem ne koristi procesorski zahtevne operacije, a generisani biometrijski šabloni su prihvatljive veličine. Sistem je procenjen u domenu provere identiteta korisnika usluga mobilnog ban- karstva bazirane na biometriji dužice ljudskog oka.

Društveni cilj ovog rada je da doprinese većoj društvenoj prihvatljivosti kriptografski zaštićene autentifikacije klijenata pomoću biometrijskih podataka.

Osnovni doprinosi ovog rada uključuju:

1. pregled postojećih sistema i metoda za zaštitu biometrijskih šablona,
2. kritički osvrt na opozivu biometriju i homomorfno šifrovanje,
3. predlaganje novog pristupa biometrijskoj autentifikaciji pomoću šifrovanih opozivih šablona,
4. primena XOR biometrije dužice u predloženom pristupu,
5. uvođenje novog sistema za kriptografsku zaštitu klijenata koji se autentifikuju pomoću biometrijskih podataka,
6. razvoj modularnog biometrijskog sistema za proveru identiteta korisnika na osnovu biometriji dužice ljudskog oka.

### 1.3 Struktura rada

Rad je strukturiran na sledeći način. U glavi 2. dat je pregled relevantnih istraživanja u oblasti, pri čemu su posebno obrađena pitanja biometrijske verifikacije korisnika, upotrebe opozive biometrije i kriptografske zaštita biometrijskih šablona. Glava 3. uvodi teorijske osnove istraživanja koje su relevantne za pristup predložen u ovom radu. One uključuju kriptografiju sa javnim ključevima, generatore pseudoslučajnih brojeva, zaštitivne kodere, interlivere i neinvertibilne transformacije.

U glavi 4. predložen je jedan novi pristup kriptografski zaštićenoj biometrijskoj autentifikaciji, zasnovan na kriptografiji sa javnim ključevima, generatoru pseudoslučajnih brojeva i opozivoj biometriji. Na osnovu toga, izložen je i predlog sistema za proveru identiteta korisnika usluga mobilnog bankarstva bazirana na biometriji dužice ljudskog oka, uz definisanje algoritama za upis i verifikaciju korisnika.

Sistem koji implementira predlog iz glave 4., procenjen je u glavi 5. Prvo je razmotren istraživački problem izdvajanja obeležja dužice i verifikacije identiteta osobe. Potom su saopšteni pozitivni rezultati analize performansi predloženog sistema na realističnom skupu podataka. Konačno, saopšteni su pozitivni rezultati ispitivanja slučajnosti šifrovanih opozivih šablona i podataka koji se prenose preko mreže.

Zaključak i pregled mogućih smerova daljeg istraživanja dati su u glavi 6.

## Glava 2

### Pregled u oblasti istraživanja

Biometrijski sistem za proveru identiteta korisnika sastoji se od: senzora, modula za izdvajanje obeležja (engl. *feature extraction module*), modula za poređenje biometrijskih šablona (engl. *matching module*), baze podataka u kojoj su smešteni šabloni generisani u fazi upisa (engl. *enrollment phase*) i modula za donošenje odluke (engl. *decision module*).

Prilikom registracije korisnika na sistem (takozvana faza upisa), korisnik prilaže biometrijski uzorak senzoru. Senzor prosleđuje očitane podatke modulu za izdvajanje obeležja, koji na osnovu uzorka generiše biometrijski šablon koji se zajedno sa korisničkim identitetom (na primer, korisničkim imenom) smešta u bazu podataka sa šablonima. Provera identiteta korisnika nakon upisa, odnosno registracije, može se obaviti na dva načina: verifikacijom i identifikacijom. U slučaju biometrijske verifikacije, korisnik sistemu prilaže svoj identitet i biometrijski uzorak. Modul za izdvajanje obeležja generiše novi biometrijski šablon, a modul za poređenje nakon toga računa sličnost (na primer, Hemingovo rastojanje dva niza bitova) između šablona koji je generisan tokom verifikacije i šablona smeštenog u bazi podataka nakon upisa koji odgovara korisničkom identitetu. Nakon toga modul za donošenje odluke na osnovu praga poređenja određuje da li se radi o legitimnom korisniku ili ne. U slučaju da je rezultat poređenja niži od praga poređenja, korisnik se prihvata kao legitiman i dobija pristup resursima shodno pravilima autorizacije, a u suprotnom se odbija. U slučaju biometrijske identifikacije od korisnika se ne zahteva da priloži svoj identitet, već samo biometrijski uzorak, a generisani šablon se poredi sa svim šablonima u bazi

podataka. Treba napomenuti da je u slučaju biometrijske verifikacije subjekat kooperativan, dok je u slučaju biometrijske identifikacije subjekat u određenom broju slučajeva nekooperativan, kao i da proces identifikacije može biti procesorski zahtevan ukoliko u bazi postoji veliki broj šablona (na primer, pretraga baze otisaka prstiju Ministarstva unutrašnjih poslova, Federalnog biroa za istrage i slično).

Iako su biometrijski sistemi veoma pogodni za proveru identiteta, zato što ne postoji potreba da korisnici pamte lozike koje lako mogu zaboraviti ili no- se autentifikacione tokene (na primer, fleš memorije ili pametne kartice) koje mogu izgubiti, kao i svi ostali sistemi za autentifikaciju (na primer, sistemi zasnovani na nečemu što korisnik zna) podložni su napadima. Neki od napada koji su izvodljivi na ove sisteme su upotreba lažnih biometrijskih uzoraka, na- pad ponavljanjem, zaobilaženje senzora i generisanje lažnih šablona, kao i zamena biometrijskih šablona u bazi podataka. Neki od ovih napada za posledicu imaju prihvatanje nelegitimnog korisnika kao legitimnog, dok neki, poput zamene ša- blona u bazi mogu rezultovati i odbijanjem usluga (engl. *Denial of Service*, DoS) legitimnim korisnicima.

U obzir treba uzeti da su ovi napadi izvodljivi isključivo ukoliko je si- stem projektovan na principu sigurnosti zasnovane na skrivanju (engl. *security by obscurity*), odnosno ukoliko projektant ne uzima u obzir prisustvo napadača i skup akcija koje može izvršiti kako bi izveo određene napade, već je zasnovan na skriva- nju arhitekture i načina rada sistema. Ukoliko se prilikom projektovanja koristi princip sigurnosti zasnovane na dizajnu (engl. *security by design*), gde projektant sistema u obzir uzima i prisustvo napadača i skupa akcija koje može obaviti, izvršenje većine napada se može onemogućiti.

Kao i bilo koji drugi nezaštićeni lični podaci, biometrijski šabloni se mo- gu presresti, ukrasti, reprodukovati ili izmeniti u slučaju da je je nezaštićeni biometrijski uređaj povezan na mrežu ili u slučaju da je vešt napadač stekao fizički pristup uređaju koji ne koristi anti-forenzičke tehnike kojima bi se sprečio neovlašćen pristup osetljivim podacima (tj. nezaštićenim šablonima). Zbog neopozivosti biometrijskih podataka, jedan od mogućih rezultata uspešnog izvršenja napada na biometrijske sisteme za autentifikaciju je krađa identiteta

legitimnih korisnika. Uzevši to u obzir, postaje jasno da biometrijski sistemi obrađuju osetljive lične podatke, kao i da su sigurnost i privatnost biometrijskih šablona važna pitanja na koja treba obratiti pažnju prilikom projektovanja sistema za proveru identiteta zasnovanih na nečemu što korisnik jeste (biometrija zasnovana na fizičkim karakteristikama) ili što korisnik može da uradi (biometrija zasnovana na ponašajnim karakteristikama).

Da bi se sprečila krađa identiteta, projektant sistema ne sme se oslanjati na otkrivanje zloupotrebe nakon uspešnog izvršenja napada, već se mora osloniti na metode koje obezbeđuju visok nivo sigurnosti šablona i zaštitu privatnosti korisnika. Dodatno, performanse biometrijskog sistema smeju se smanjiti isključivo na prihvatljiv nivo nakon uvođenja ovih protivmera u sistem. Drugim rečima, očekuje se da uvođenje ovih protivmera u sistem neće smanjiti tačnost verifikacije ili identifikacije na neprihvatljiv nivo, odnosno da se procenat lažno odbijenih korisnika (engl. *False Rejection Rate*, FRR) i lažno prihvaćenih korisnika (engl. *False Acceptance Rate*, FAR) neće značajno povećati. Takođe, uvođenje ovih protivmera ne sme za posledicu imati znatno povećanje složenosti izračunavanja i povećanje prostora potrebnog za skladištenje zaštićenih biometrijskih šablona.

Jedan od načina zaštite biometrijskih šablona i očuvanja privatnosti je upotreba takozvane opozive biometrije (engl. *cancelable biometrics*), metode zaštite koja se u navodima izvesnih autora može naći i pod nazivom poništiva biometrija. Dve osnovne tehnike koje se koriste u opozivoj biometriji su namerno izobličavanje biometrijskih šablona ili uzoraka upotrebom neinvertibilnih, odnosno jednosmernih transformacija [74], poput blok permutacije teksture dužice (engl. *iris*), i biometrijsko soljenje (engl. *biometric salting*).

Opoziva biometrija koja koristi neinvertibilne transformacije zasniva se na primeni iste transformacije na datom biometrijskom uzorku ili šablonu u fazi upisa i u fazi verifikacije. Primena ovih transformacija donekle podseća na smeštanje heš vrednosti lozinke u bazu podataka prilikom kreiranja korisničkog naloga i poređenje te vrednosti sa heš vrednošću lozinke generisanim prilikom prijavljivanja korisnika na sistem. Postoji veliki broj neinvertibilnih transformacija za različite biometrijske modalitete, od kojih neke koriste i ključ. Uzevši to u obzir, svaki kompromitovani šablon može se lako opozvati, a pri-

likom naknadne registracije korisnika može se primeniti druga transformacija. U slučaju da neinvertibilna transformacija koristi ključ, prilikom zamene kompromitovanog šablona može se zameniti samo ključ. Primeri ovih transformacija koje se primeniti na otisak prsta i dužicu su opisani u [94] i [141], respektivno. Međutim, neinvertibilne transformacije mogu biti delimično invertibilne (u literaturi se najčešće ne navode koncizni matematički dokazi potpune jednosmernosti ovih transformacija) i u najvećem broju slučajeva smanjuju tačnost verifikacije, odnosno povećavaju greške lažnog prihvatanja i odbijanja, što znači da ne predstavljaju potpuno rešenje problema zaštite biometrijskih šablona. Smanjenje performansi uzrokovano je činjenicom da je nad transformisanim biometrijskim šablonima teško izvršiti odgovarajuća poređenja, kao i da je količina informacije korisne za poređenje u nekim slučajevima smanjena [92, 141].

Biometrijsko soljenje odnosi se na transformacije biometrijskih šablona koji su odabrani kao invertibilni, pri čemu se svaka transformacija smatra pristupom biometrijskom soljenju čak i ako su šabloni generisani tako da nije moguće rekonstruisati originalni biometrijski signal [99]. Iako biometrijsko soljenje ne smanjuje tačnost verifikacije, neinvertibilne transformacije pružaju viši nivo sigurnosti, što znači da se ni ova tehnika ne može smatrati sigurnim rešenjem problema.

Pristupi opozivoj biometriji mogu se takođe klasifikovati i na osnovu domena u kojima se primenjuju transformacije. U domenu signala, transformacije se primenjuju na sirove biometrijske uzorke (na primer, slika lica [92] ili na predobrađene biometrijske signale (na primer, tekstura dužice [50]). U slučaju da se su transformacije primene u domenu signala, module za izdvajanje obeležja i poređenje šablona nije potrebno menjati. Međutim izvesne promene u ovim modulima je potrebno načiniti ukoliko se transformacije izvršavaju u domenu izdvojenih obeležja (na primer, crte lica [126]).

Drugi način zaštite i očuvanja privatnosti biometrijskih šablona je primena homomorfni šema šifrovanja [21, 108]. Homomorfno šifrovanje odnosi se na kriptografske algoritme koji omogućavaju da se određena izračunavanja izvrše u šifrovanom domenu. Iako su postojala izvesna očekivanja da će istraživanja u oblasti homomornog šifrovanja uvesti značajna unapređenja zaštite biometrije-



Slika 2.1: Jedan primer primene opozive biometrije dužice: originalna tekstura dužice (gore) i blok permutacija tekstone (dole). Slika preuzeta iz [99].

skih šablona [44], u relevantnoj literaturi za sada nisu prijavljeni značajniji rezultati upotrebljivi u praksi. Iako je teorijski primenljivo – na primer, homomorfno šifrovanje je teorijski pogodno za primenu u sistemima koji koriste operaciju ekskluzivno ILI za izračunavanje Hemingovog rastojanja između dva binarna koda dužice (engl. *iris code*) – postoje dva razloga zbog kojih homomorfno šifrovanje nije praktično: značajno povećanje šifrovanog šablona i složenosti izračunavanja [108].

U nastavku ovog poglavlja ukratko su analizurani algoritmi, postupci, metode i rezultati prijavljeni u relevantnim naučnim radovima u kojima je opisana upotreba opozive biometrije i kriptografske zaštite biometrijskih šablona.

## 2.1 Upotreba opozive biometrije

Transformacije koje se koriste u opozivoj biometriji dizajniraju se tako da je praktično nemoguće u razumnom vremenskom periodu sa ograničenom procesorskom snagom regenerisati originalni biometrijski podatak. Na sl. 2.1 prikazana je originalna tekstura dužice i tekstura nad kojom je izvršen jedan tip jednosmerne transformacije – blok permutacija. Kao što je već pomenuto, postoje dve osnovne tehnike koje se primenjuju u opozivoj biometriji: jednosmerne, odnosno neinvertibilne transformacije i biometrijsko soljenje.

Primena ovih transformacija ne sme da utiče na individualnost biometrijskih karakteristika, odnosno, ne sme da poveća procenat lažno prihvaćenih korisnika. S druge strane, postoji i ograničenje koje se odnosi na grešku lažnog prihvatanja, koja takođe ne sme da se poveća [92]. Međutim, ukoliko šum nije prečišćen pre izvršavanja same transformacije (na primer, nisu prečišćene šare dužice od

trepavica), verovatnoća da se ove greške neće povećati je relativno mala. U slučaju da transformisani biometrijski podaci postanu kompromitovani, parametri transformacije se menjaju a korisnici se ponovo registruju na sistem kako bi se ažurirao biometrijski šablon. Dodatna mera zaštite koja otežava izvršavanje napada na biometrijske sisteme koji koriste opozivu biometriju je upotreba različitih transformacija u različitim domenima primene za iste korisnike. U tom slučaju, kompromitovanje jednog šablona neće za posledicu imati kompromitovanje šablona za druge domene primene.

Iako u većini predloženih pristupa poređenje opozivih šablona nije jednostavno, a primenjene transformacije koje su izabrane kao neinvertibilne smanjuju tačnost poređenja, postoje radovi u kojima su opisane metode i algoritmi (na primer, [103, 126]), posebno za biometrijsko soljenje, koje povećavaju performanse sistema. Na primer, u slučaju da se prilikom upisa i verifikacije primenjuju transformacije specifične za korisnika, autentifikacija postaje dvofaktorska, što znači da može povećati sigurnost, ali da uvođenje transformacije ne utiče na tačnost biometrijske autentifikacije.

### **2.1.1 Pristupi zasnovani na neinvertibilnim transformacijama**

Ratha i dr. [92] su među prvima uveli koncept neinvertibilnih transformacija kao jednu od metoda opozive biometrije. U fazi upisa korisnika, na biometrijske podatke se primenjuju neinvertibilne transformacije koje se biraju na osnovu konkretnog domena primene. U fazi autentifikacije, biometrijski podaci se transformišu na isti način, koristeći transformaciju za dati domen primene, i vrši se poređenje transformisanih šablona.

Nekoliko tipova transformacija, uključujući i funkcionalnu transformaciju, koje se mogu koristiti za konstrukciju prethodno pomenutih sistema zasnovanih na otisku prsta i biometriji lica predstavljene su u [92, 93, 94].

Transformacije predložene u [92] uspešno su primenjene na biometriju dužice, shodno rezultatima eksperimenata predstavljenim u [50]. Međutim, u istraživanju koje je opisano u [41] pokazano je da primena obe transformacije na pravougaone slike dužice značajno smanjuje tačnost verifikacije. Slično istraživanju opisanom

u [141], Rathgeb i Uhl [98] predlažu primenu blok-permutacija kodova dužice.

Jedan tipičan pristup generisanju opozivih biometrijskih šablona zasnovan je na slučajnim permutacijama obeležja. U istraživanju [141] predstavljene su četiri različite transformacije koje su primenjene u domenu slike dužice i u domenu izdvojenih obeležja, pri čemu, shodno rezultatima eksperimenata, svaka transformacija unosi malu degradaciju performansi. Prvi metod transformacije u domenu obeležja transformiše Gabor-zasnovana obeležja kružnim pomeranjem i slučajnim dodavanjem redova. Drugi metod primenjuje transformaciju zasnovanu na slučajnom mešanju i primenjivanju operacije ekskluzivno ILI. Shodno navodima autora, ove metode postepeno umanjuju količinu informacije dostupne za prepoznavanje. Pošto su prethodno pomenute metode zasnovane na primeni linearnih transformacija na Gabor-zasnovanim vektorima obeležja, osetljive su na šum. Autori u [89] ukazuju na moguće načine na koje se ova ograničenja mogu zaobići. Jedan od predloženih načina je podela obeležja u regione i slučajna permutacija na osnovu rečnika, ali se ukazuje na činjenicu da je prepoznavanje nemoguće ukoliko je lokacija obeležja u rečniku nepoznata. Sličan pristup je predložen u [50], gde je svaki blok ciljne teksture mapiran na blok izvorne teksture. Ova metoda koristi remapiranje blokova umesto permutacije zato što je remapiranje neinvertibilno. Izvorni blokovi koji nisu deo mapiranja nisu sadržani u transformisanoj teksturi, što znači da je nemoguće rekonstruisati originalnu teksturu dužice.

Jedan pristup generisanju opozivih šablona otiska prsta zasnovan na permutacijama pomoću ključa predstavljen je u [40]. U ovom pristupu permutuje se binarni vektor izdvojen iz obeležja otiska prsta i čuva se u bazi podataka. Prilikom autentifikacije, od korisnika se zahteva da priloži ključ kako bi sistem izvršio permutaciju novog vektora i izvršio poređenje sa šablonom smeštenim u bazi. U ovoj, kao i u sličnim transformacijama koje zavise od ključa, sigurnost ključa je od suštinskog značaja za privatnost korisnika i sigurnost šablona. Prednost permutacija sa ključem je u tome što one ne unose suštinske izmene u vektor obeležja, što znači da nema gubitka korisne informacije, a samim tim ni umanjenja tačnosti prepoznavanja.

U istraživanjima opisanim u [78, 79, 80] primenjene su neinvertibilne transformacije kako bi se generisali opozivi šabloni na osnovu takozvanih on-line

potpisa. U njihovom prisupu, biometrijski šabloni, koji su predstavljeni kao niz vremenskih sekvenci, podeljeni su u nepreklapajuće sekvence na osnovu slučajnog vektora koji obezbeđuje opozivost. Nakon toga, transformisani šablon se generiše linearnom konvolucijom prethodno pomenutog niza. Rekonstrukcija originalnih prodataka iz transformisanog šablona računski je složena koliko i nasumično pogađanje, što ovom vidu transformacije značajno povećava nivo sigurnosti.

Boult i dr. [14, 15] su u svojim radovima predstavili kriptografski sigurne biometrijske tokene (takozvane biotokene, engl. *biotokens*) koje su primenili na biometrijske modalitete lica i otiska prsta. Kako bi uvećali sigurnost biometrijskih sistema, biotokeni su primenjeni uz postojeće šeme prepoznavanja, kao što je analiza glavnih komponenti (engl. *Principal Component Analysis*, PCA) koja se koristi prilikom fotometrijskog prepoznavanja lica. Međutim, iako je na prvi pogled ideja upotrebljiva, na izvesna pitanja nije dat odgovor – na primer, kako treba dizajnirati pomoćnu funkciju koja razdvaja biometrijske šablone na stabilne i nestabilne delove, kao i da li je sistem moguće prilagoditi za rad sa drugim biometrijskim modalitetima. U istraživanjima koje su autori nastavili i objavili u [16, 17] predstavljena je nova vrsta biometrijskih tokena koji su uspešno primenjeni na biometriju otiska prsta s ciljem obezbeđivanja sigurne komunikacije preko nesigurnog kanala, pri čemu se kriptografski ključevi generišu na osnovu uspešnog poređenja biotokena.

Još jedan tip neinvertibilnih transformacija koji se često koristi za generisanje opozivih biometrijskih uzoraka zasnovan je na upotrebi slučajnih projekcija [89, 90]. Ove metode su zasnovane na projektovanju izdvojenih obeležja iz biometrijskog uzorka na slučajni potprostor.

Opoziva biometrija za prepoznavanje dužice zasnovana na slučajnim projekcijama predstavljena je u [89]. U slučaju primene slučajne projekcije na neobrađenu sliku dužice performanse sistema se umanjuju iz nekoliko razloga. Pre svega, u realističnim slikama dužica, uprkos dobrim algoritmima za segmentaciju, postoji određeni šum koji potiče od refleksija, trepavica i kapaka. Takođe, različiti delovi dužica imaju različit kvalitet, odnosno sadrže različitu količinu korisne informacije. U slučaju upotrebe linearne transformacije celokupnog vektora, kombinuju se regioni dobrog kvaliteta sa zašumljenim regionima koji na taj način

oštećuju podatke. Autori kao rešenje problema predlažu sektorske slučajne projekcije (engl. *Sectored Random Projections*, SRP) u kojima se slučajne projekcije primenjuju odvojeno na svaki sektor, a rezultujući transformisani vektori se spajaju kako bi se formirao opozivi šablon. Posledica toga je da zašumljeni podaci imaju negativan uticaj samo na deo vektora obeležja ali ne i na celokupan vektor. Prilikom upisa sistem izdvaja uzorak dužice korisnika, izračunava Gabor-zasnovana obeležja, primenjuje različite slučajne projekcije za svaki domen primene i smešta novi opozivi uzorak u bazu podataka. Treba uzeti u obzir činjenicu da čak i u slučaju kompromitovanja opozivog šablona i ključa (odnosno matrice projekcije) originalni uzorak dužice ne može biti regenerisan zbog redukcije dimenzionalnosti koju nameće sama projekcija. Takođe, napadač koji na nelegalan način dođe u posed uzorka dužice sa biometrijskog uređaja ili upotrebom skrivenog uređaja za krađu slike dužice, neće biti u mogućnosti da regeneriše šablon bez poznavanja skrivene projekcije. U fazi verifikacije, korisnik prilaže sliku dužice i matricu projekcije sistemu, a sistem izračunava transformisan šablon i poredi ga sa šablonom koji je sačuvan u bazi podataka.

### 2.1.2 pristupi zasnovani na biometrijskom soljenju

U istraživanju koje su opisali Savvides i dr. [107] opoziva biometrija lica generisana je primenom takozvanih korelacionih filtra minimalne srednje vrednosti koji obezbeđuju jednosmernost transformacije. Lični identifikacioni brojevi korisnika koriste se kao ključ na sličan način kao što je opisano u [121].

Tehnika zvana biometrijsko hešovanje (engl. *BioHashing*) [46], preuzeta iz domena biometrijske kriptografije, takođe se može iskoristiti za generisanje opozivih šablona ukoliko se iz nje ukloni procedura kojom se ključ vezuje za biometrijski uzorak. Prvobitne varijante algoritma za biometrijsko hešovanje nisu u obzir uzimale scenario ukradenih tokena. U daljim istraživanjima pokazano je da greška prilikom ekstrakcije 180-bitnog koda otiska prsta raste sa 0% na 5,31% u scenariju ukradenih tokena [124]. Problem je naknadno rešen uvođenjem takozvane metode višeprostorinih slučajnih projekcija (engl. *Multispace Random Projections*, MRP) [125, 127]. Shodno navodima autora, prethodno pomenutom tehnikom primenjenom na modalitete lica i glasa, moguće je sprečiti pad performansi prepoznavanja u sce-

nariju ukradenog tokena. Autori su takođe predstavili metod generisanja opozivih ključeva na osnovu dinamičkih potpisa [139, 67] zasnovan na *BioPhasor* koraku slučajnog mešanja i korisnički zavisne  $2N$  diskretizacije.

Kim i Toh [66] primenili su korisnički-zavisne slučajne projekcije na obeležja lica izdvojena metodom glavnih komponenti na koje su zatim primenili transformaciju za minimizaciju greške. Autori, međutim, nisu u obzir uzeli scenario ukradenog tokena.

Još jedan pristup biometrijskom soljenju predstavljen je u [144] u kome su obeležja lica transformisana na osnovu tajnog ključa. Jednosmernost, odnosno neinvertibilnost, postignuta je upotrebom kvantizacije.

Ouda i dr. predstavili su tehniku za generisanje opozivih kodova dužice [86, 87]. Iz nekoliko šablona generisanih u fazi upisa formira se vektor konzistentnih bitova (takozvani *BioCode*) i pozicije tih bitova. Opozivost je obezbeđena kodovanjem formiranih vektora na osnovu slučajnog unutrašnjeg ključa.

Još jednom treba napomenuti da neinvertibilne transformacije pružaju viši nivo sigurnosti u odnosu na biometrijsko soljenje.

### **2.1.3 Ostali značajniji pristupi u opozivoj biometriji**

Motivisani uspehom primene metode korelacije zasnovane na filtrima u istraživanjima koja se odnose na prepoznavanje oblika i računarsku viziju [68], autori su opisali metod slučajne konvolucije za generisanje opozivih biometrijskih šablona u [107]. Osnovna ideja je šifrovanje biometrijskih šablona upotrebom slučajnih korisnički-zavisnih konvolucionih jezgara. Na slikama koje se koriste za obuku najpre se obavlja konvolucija slučajnim konvolucionim jezgrom (engl. *kernel*). Ključ koji se koristi za generisanje slučajnog konvolucionog jezgra je lični identifikator korisnika (engl. *Personal Identification Number*, PIN). Nakon toga se slike za trening koriste za generisanje takozvanog MACE biometrijskog filtra (engl. *Minimum Average Correlation Energy*). Ovaj šifrovani filter se čuva i dalje koristi za autentifikaciju. Tokom faze prepoznavanja, korisnik sistemu prilaže PIN i šifrovani filter koji se koristi za generisanje konvolucionog jezgra. Sistem dalje obavlja konvoluciju jezgra sa test slikama koje je korisnik priložio. Konvolucionu test slike se nakon toga unakrsno korelišu sa šifrovanim MACE fil-

trom a rezultat konvolucije se koristi za autentifikaciju korisnika. Autori su dokazali da konvolucija slika korišćenih za trening sa slučajnim konvolucionim jezgrom pre generisanja MACE filtara korišćenih za biometrijsko prepoznavanje ne menja izlaz korelacije [107], što rezultuje nepromenjenom tačnošću prepoznavanja. Osim toga, različiti opozivi biometrijski šabloni se mogu generisati iz istog uzorka jednostavnim promenom konvolucionog jezgra.

Druge metode opozive biometrije zasnovane na korelaciji uključuju CIRF (engl. *Correlation Invariant Random Filtering*), metod za koji je pokazano da obezbeđuje skoro identičnu tačnost kao konvencionalni sistemi za verifikaciju otiska prsta zasnovani na žetonu [123, 53].

Sistemi za zaštitu opozivih biometrijskih uzoraka zasnovani na Blumovim filtrima su takođe opisani u relevantnoj literaturi [100, 101, 102]. U osnovi, Blumov filter je prostorno-efikasna probabilistička struktura podataka koja služi za proveru da li je dati element član skupa. Konkretno, opozivi biometrijski šabloni dužice zasnovani na adaptivnim Blumovim filtrima predstavljeni su u [101]; generička adaptivna Blumova filtarska transformacija primenjuje se na binarne vektore obeležja u slučaju različitih algoritama prepoznavanja dužice. Pokazano je da ovaj metod obezbeđuje zaštitu šablona, kompresiju biometrijskih podataka i računski efikasnu biometrijsku identifikaciju. Dodatno, rotaciono-nezavisna Blumova filtarska transformacija obezbeđuje visok nivo sigurnosti bez smanjenja tačnosti prepoznavanja [101].

Jeong i dr. [62] kombinovali su dve različite tehnike izdvajanja obeležja kako bi obezbedili opozivu biometriju lica. Koeficijenti metoda PCA i nezavisne analize komponenti (engl. *Independent Component Analysis*, ICA) su izdvojeni, a potpuno oba vektora obeležja izmešana s ciljem generisanja transformisanog šablona.

Tulyakov i dr. [130, 131] predložili su metodu za generisanje opozivih heševa otisaka prsta. Umesto poravnavanja karakterističnih tačaka, autori primenjuju heš-funkcije poput simetričnih složenih heš funkcija.

Hirata i Takahashi [53] predložili su sistem opozive biometrije primenljiv za otiske prstiju koji transformiše slike koristeći Furijeovu transformaciju. Rezultat se nakon toga obrađuje slučajno generisanim filtrom, a korisnik čuva odgovarajući inverzni filter na tokenu. Inverzni filter se koristi u fazi au-

tentifikacije kako bi se regenerisali određeni podaci preuzeti u fazi upisa i izvršilo poređenje upotrebom korelacije.

Bringer i dr. [22] izneli su ideju o kreiranju vremenski zavisne opozive biometrije s ciljem obezbeđivanja nemogućnosti ulaska u trag različitim identitetima tokom određenih vremenskih intervala.

#### **2.1.4 Kratki osvrt na sigurnost opozive biometrije**

Iako se u relevantnoj literaturi koja se odnosi na opozivu biometriju navodi delimična analiza sigurnosti sistema uporedo sa tačnošću prepoznavanja u odnosu na referentni sistem, konkretne analize koje se odnose na neinvertibilnost opozivog šablona i nepovezanost šablona istog korisnika generisanih pomoću različitih parametara transformacije retko su izvršene u potpunosti.

Analize koje se tiču neinvertibilnosti, odnosno mogućnosti da se nakon primene jednosmerne transformacije regeneriše originalni biometrijski šablon, potrebno je izvršiti kao detaljno ispitivanje prethodno pomenutih transformacija. Na primer, ukoliko je uslovno neinvertibilna blok permutacija primenjena na biometrijski podatak (na primer, dužicu [50] ili otisak prsta [94]) kako bi se generisao opoziv šablon, potrebno je proceniti računsku složenost regenerisanja originalnog biometrijskog uzorka ili njegovih delova na osnovu opozivog šablona. Za neke pristupe analiza neinvertibilnosti je relativno jednostavna, dok se za druge zahteva daleko složenija i sofisticiranija analiza. Na primer, u nekim slučajevima složenost rekonstrukcije originalnog signala može zavisi od složenosti rešavanja izvesnih matematičkih problema, poput problema slepe dekonvolucije (engl. *blind deconvolution problem*) [79]. Da bi se osigurala obnovljivost zaštićenih biometrijskih šablona, primenjene transformacije obeležja izvode se na osnovu različitih parametara - drugim rečima, primenjeni parametri definišu konačan prostor ključeva, što se retko prijavljuje u relevantnoj literaturi. U opštem slučaju, razlika između zaštićenih šablona je veća ukoliko je prostor ključeva definisan parametrima transformacije veći [80].

Da bi se zadovoljilo svojstvo nepovezanosti, različiti opozivi šabloni istog korisnika generisani pomoću različitih parametara neinvertibilne transformacije moraju se razlikovati kao i šabloni različitih subjekata. Drugim rečima,

prostor ključeva definisan parametrima transformacije mora biti dovoljno veliki da obezbedi dovoljno visok nivo slučajnosti koji će rezultovati niskim nivoom mogućnosti povezivanja šablona istih subjekata.

## 2.2 Kriptografska zaštita biometrijskih šablona

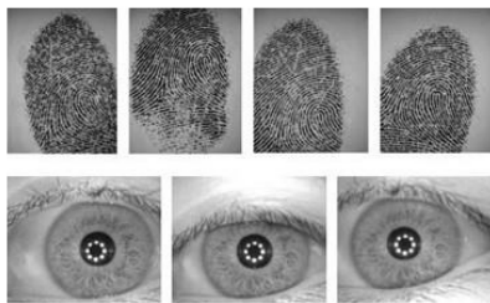
Termin biometrijska kriptografija, odnosno biometrijski kriptosistemi (engl. *biometric cryptosystems*) najčešće se odnosi na sisteme za generisanje kriptografskih ključeva na osnovu biometrijskih uzoraka ili na sisteme koji vezuju ključ generisan pomoću generatora slučajnih ili pseudoslučajnih brojeva za pomoćni podatak. Alternativno, prethodno pomenuti termin može se odnositi i na kriptografsku zaštitu biometrijskih šablona. U ovom delu rada ukratko će biti analizirani biometrijski kriptosistemi dok će posebna pažnja biti posvećena kriptografskoj zaštiti biometrijski šablona.

### 2.2.1 Biometrijski kriptosistemi

Biometrijski kriptosistemi dizajniraju se sa namerom da na siguran način vežu ključ za biometrijski šablon ili da na osnovu biometrijskog šablona generišu kriptografski ključ [26] čime je omogućena reprodukcija ključa koja je zavisna od biometrijskog uzorka, kao i zaštita biometrijskih šablona [59, 27]. U odnosu na reprodukciju, odnosno generisanje kriptografskog ključa na osnovu lozinke, prednost biometrijskih kriptosistema je značajno otežano falsifikovanje, kopiranje, krađa i deljenje biometrijskih podataka u odnosu na lozinke [58].

Zbog biometrijske promeljivosti (engl. *biometric variance*), v. sl. 2.2, konvencionalni biometrijski sistemi izvršavaju takozvano rasplinuto (engl. *fuzzy*) poređenje za diskriminaciju legitimnih i nelegitimnih korisnika. Za razliku od njih, biometrijski kriptosistemi su dizajnirani tako da reprodukuju identične ključeve u fazi autentifikacije. Drugim rečima, izlaz biometrijskog kriptosistema može biti ili ključ ili poruka o grešci.

Većina biometrijskih kriptosistema zahteva postojanje uskladištene javne in-



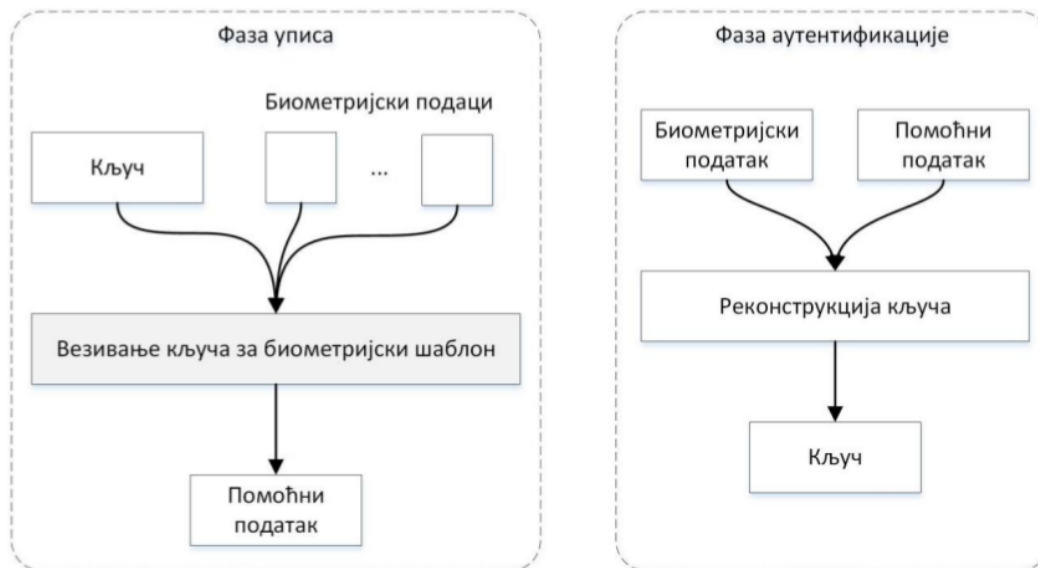
Slika 2.2: Dva primera biometrijske promenljivosti koja se odnose na otisak prsta i dužicu. Slika preuzeta iz [76]. Originalni biometrijski uzorci su preuzeti iz FCV (<http://bias.csr.unibo.it/fvc2004/databases.asp>) i CASIA (<http://biometrics.idealtest.org/>) baza podataka biometrijskih uzoraka.

formacije koja je zavisna od biometrijskog podatka kako bi sistem mogao da reprodukuje ili generiše ključ. Ova javna informacija, koja se naziva pomoćni podatak (engl. *helper data*) ne sme da otkrije značajniju količinu informacije o originalnom biometrijskom podatku ili šablonu [60]. Zbog biometrijske promenljivosti većina sistema ove klase nije u mogućnosti da reprodukuje ili generiše kriptografski ključ bez pomoćnog podatka. S obzirom da se biometrijsko poređenje vrši u šifrovanom domenu [59], biometrijski kriptosistemi se mogu koristiti i kao metoda zaštite biometrijskih šablona [60].

Na osnovu toga kako se pomoćni podatak koristi, biometrijski kriptosistemi se mogu podeliti u dve klase:

- sistemi za vezivanje ključeva za biometrijski šablon (engl. *key binding systems*) i
- sistemi za generisanje ključeva na osnovu biometrijskog šablona (engl. *key generation systems*).

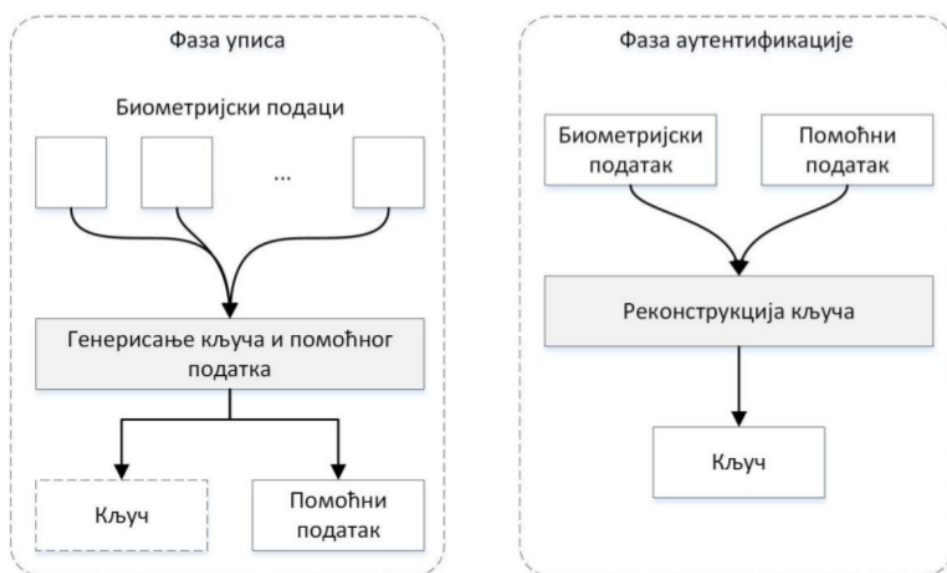
U sistemima za vezivanje ključeva pomoćni podatak se generiše čvrstim vezivanjem kriptografskog ključa za biometrijski šablon. Primenom algoritma za reprodukciju, ključ se dobija na osnovu pomoćnog podatka u fazi autentifikacije [133]. S obzirom da su kriptografski ključevi uslovno nezavisni od biometrijskih obeležja, to znači da je biometrija opoziva, dok zamena ključa zahteva fazu ponovnog upisa kako bi sistem generisao novi pomoćni podatak. Generička šema sistema za vezivanje ključeva prikazana je na sl. 2.3.



Slika 2.3: Generička šema sistema za vezivanje ključeva.

U sistemima za generisanje ključeva na osnovu biometrijskih podataka pomoćni podatak se generiše na osnovu biometrijskog šablona, dok se ključevi u fazi autentifikacije generišu na osnovu pomoćnog podatka i priloženog biometrijskog uzorka [61]. Iako u ovoj klasi sistema upotreba pomoćnog podatka nije obavezna, većina sistema ove klase koristi pomoćni podatak s ciljem smanjivanja grešaka. Osim toga, ukoliko sistem ne koristi pomoćni podatak, mogućnost kompromitovanja korisnika se uvećava. Sistemi za generisanje ključeva koji koriste pomoćni podatak se u literaturi pominju kao sistemi za rasplinuto izdvajanje (engl. *fuzzy extractors*) i sigurne skice (engl. *secure sketches*) [36, 143]. Sistem za rasplinuto izdvajanje izdvaja uniformno slučajni niz iz biometrijskog šablona pri čemu se pomoćni podatak koristi pri rekonstrukciji. Za razliku od toga, u šemi sigurne skice, pomoćni podatak se koristi za izdvajanje originalnog biometrijskog šablona. Generička šema sistema za generisanje ključeva na osnovu biometrijskog šablona prikazana je na sl. 2.4.

Kao i konvencionalni kriptološki ključevi, ključevi generisani pomoću biometrijskih podataka (koji se u literaturi pominju i kao „biometrijski ključevi“) moraju da ispune uslove poput dovoljne količine slučajnosti (tj. moraju da zadovolje statističke testove slučajnosti), stabilnosti i jedinstvenosti [5, 6].



Slika 2.4: Generička šema sistema za generisanje ključeva na osnovu biometrijskog šablona.

Drugi način klasifikacije biometrijskih kriptosistema je način rešavanja problema biometrijske promenljivosti. Neke predložene šeme koriste kodove za korekciju grešaka (engl. *Error Correction Codes*, ECC) [63, 64], dok druge koriste prilagodljive filtre i korelaciju [117] ili kvantizaciju [42, 142].

Prilikom merenja performansi biometrijskih sistema u obzir se uzimaju greška lažnog odbijanja, greška lažnog prihvatanja i jednaka stopa greške (engl. *Equal Error Rate*, EER) [58, 61] koja se definiše kao tačka preseka FRR i FAR kriptosistema. U kontekstu biometrijskih kriptosistema značenje ovih metrika se menja zato što sistemi nisu zasnovani na rasplinutom poređenju na osnovu praga - zahteva se generisanje ili reprodukcija identičnog ključa, dok konvencionalni biometrijski sistemi donose jednostavnu binarnu odluku. Greška lažnog odbijanja u biometrijskim kriptosistemima definiše se kao odnos ključeva koje sistem nije uspeo da generiše ili reprodukuje za legitimne korisnike i ukupan broj pokušaja legitimnih korisnika da od sistema dobiju ključ (ispravan ključ je zavistan od korisnika i povezan sa pomoćnim podatkom). Po analogiji, greška lažnog prihvatanja formira se na osnovu broja ispravnih ključeva koji su isporučeni nelegitimnim korisnicima. Imajući prethodno pomenuto u vidu, kao i rezultate prijavljene u relevantnoj

literaturi, može se zaključiti da biometrijski kriptosistemi imaju veću stopu greške u odnosu na konvencionalne biometrijske sisteme za autentifikaciju [133]. Jedan od razloga za povećanje stope greške je činjenica da biometrijski kripto- sistemi ne čuvaju biometrijski šablon nakon faze upisa i samim tim ne mogu izvršiti poređenje šablona u bazi i šablona generisanog u fazi autentifikaci- je. Dodatno, većina biometrijskih kriptosistema koristi viši nivo kvantizacije u fazi izdvajanja obeležja u odnosu na konvencionalne biometrijske sisteme.

Jedan od prvih pristupa sistemima za vezivanje ključeva predložili su Soutar i dr. [118, 119, 120]. Predloženi sistem, nazvan Mytec2, je naslednik sistema Mytec1 [117], prvog biometrijskog kriptosistema za koji je pokazano da ne zadovoljava minimalne potrebne uslove koji se odnose na tačnost i sigurnost. Osnova Mytec2 i Mytec1 algoritama je mehanizam korelacije.

Juels i Wattenberg [63] su 1999. godine upotrebom tehnika iz oblasti kodova za korekciju grešaka i kriptografije formirali novu kriptografsku metodu nazvanu šema rasplinutog vezivanja (engl. *fuzzy commitment scheme*).

Primenu šeme rasplinutog vezivanja kodova dužice predložili su Hao i dr. [51]. U njihovom predlogu, kodovi dužice dužine 2048 bita su upotrebljeni za vezivanje i reprodukciju kriptografskih ključeva dužine 140 bita, koji su prethodno obrađeni Hadamardovim i Rid-Solomonovim kodovima za korekciju grešaka. Hadamardovi kodovi su primenjeni kako bi se uklonile greške koje potiču od prirodne biometrijske promenljivosti uzoraka, dok su Rid-Solomonovi kodovi upotrebljeni kako bi se uklonile greške nastale izobličenjem. Sistem je testiran na 700 slika dužice koje potiču od 70 subjekata. Rezultati eksperimenata ukazuju na jako visoku tačnost i nisku stopu greške koja do tada nije postignuta, ili barem nije prijavljena u relevantnoj literaturi.

Rathgeb i Uhl [95] predstavili su sistematičan pristup konstrukciji šeme rasplinutog vezivanja koja je primenjena na dužicu. Nakon analiziranja distribucije greške između kodova dužica generisanih različitim algoritmima za prepoznavanje, autori primenjuju Rid-Solomonov i Hadamardov kod za korekciju grešaka (na sličan način kao što je opisano u [51]). U istraživanju opisanom u [96] autori primenjuju pouzdan izbor komponenti zasnovanih na kontekstu kako bi izvukli ključeve iz kodova dužica koji su zatim vezani za Hadamardove kodne reči.

Različite tehnike za povećanje performansi sistema zasnovanih na dužici i šemama rasplnutog vezivanja predstavljene su u [55, 140]. Binarni kodovi dužica su prikladni za primenu u šemama rasplnutog vezivanja, a poravnavanje šablona je izvodljivo jer uključuje samo jednodimenzionalni kružni pomeraj datog koda dužice.

Osim dužice, šema rasplnutog vezivanja je primenjivana i na druge biometrijske modalitete uz neophodnu binarizaciju izdvojenog vektora obeležja.

Druga značajna metoda koja se odnosi na biometrijske kriptosisteme, nazvana rasplnuti trezor (engl. *fuzzy vault*), predstavljena je u [64], 2002. godine. Clancy i dr. [30] predložili su prvu praktičnu i najočitiju primenu metode rasplnutog trezora zaključavanjem karakterističnih tačaka otiska prsta (engl. *minutiae points*) u takozvanom „trezoru otiska prsta“.

Nandakumar i dr. [85] predlažu da se kao pomoćni podaci koriste tačke velike zakrivljenosti izvedene iz orijentacionog polja otiska prsta kako bi se pomogao proces poravnanja. U njihovom trezoru otiska prsta, ključevi dužine 128 bita su vezivani i rekonstruisani. Uludag i Jain [134, 135] su predložili linijsko predstavljanje karakterističnih tačaka otiska prsta; performanse sistema ispitane su na test skupu koji sadrži 450 parova otisaka prstiju. Nekoliko drugih prisupa za poboljšanje poravnanja u rasplnutom trezoru otiska prsta predloženi su u [137, 29, 71].

Iničijalna ideja generisanja kriptografskih ključeva direktno iz biometrijskih šablona predstavljena je u patentu opisanom u [13]. Implementacija ove šeme ne postoji, a jedan od razloga koji to objašnjava je činjenica da većina biometrijskih modaliteta ne obezbeđuje dovoljnu količinu informacije za pouzdano generisanje dovoljno dugog i stabilnog ključa bez upotrebe pomoćnih podataka.

U šemi privatnog šablona (engl. *private template scheme*) zasnovanoj na biometrijskoj dužici, koju su predložili Davida i dr. [34, 35] biometrijski šablon (ili heš vrednost biometrijskog šablona) koristi se kao ključ. Skladištenje pomoćnih podataka, odnosno bitova za ispravljanje grešaka, je neophodno za korekciju neispravnih bitova datih kodova dužice.

U okviru grupe šema zasnovanih na kvantizaciji, pomoćni podaci se generišu tako da služe kao pomoć pri kvantizaciji biometrijskih obeležja sa ciljem

dobijanja stabilnih ključeva. Detaljnija analiza šema kvantizacije data je u [54]. Primene šema kvantizacije na biometriju lica, otisak prsta i dužicu opisane su u [122], [70] i [97], respektivno.

### **2.2.2 Kratki osvrt na sigurnost biometrijskih kriptosistema**

Biometrijska kriptografija može značajno povećati sigurnost biometrijskog sistema i privatnost podataka koji su uskladišteni u njemu. Ovakvi sistemi su otporniji na napade višeg nivoa poput napada zamene, maskiranja, varanja i nadglašavanja konačne odluke na modulu za poređenje. Sistemi zasnovani na biometrijskoj kriptografiji mogu funkcionisati u nepoverljivoj ili manje poverljivoj okolini i manje su zavisni od konkretnog hardvera, procedura i sigurnosnih politika u odnosu na konvencionalne biometrijske sisteme. Takođe treba uzeti u obzir činjenicu da su ključevi znatno duži u odnosu na ključeve koji su generisani na osnovu lozinki, te da korisnici ne moraju da pamte dugačke ključeve. Pomoćni podaci su opozivi, poput šablona generisanih metodama opozive biometrije.

Međutim, u literaturi je opisan veliki broj napada koji se mogu uspešno izvršiti na biometrijske kriptosisteme, poput rasplnutih sistema izdvajanja. Jedan primer je napad na pomoćne podatke koji se izvodi pomoću baze podataka sa slikama s ciljem ostvarivanja greške lažnog prihvatanja. Drugim rečima, neki biometrijski kriptosistemi mogu biti ranjivi na napade niskog nivoa ukoliko je napadač upoznat sa algoritmom i ima pristup pomoćnim podacima (ali ne i legitimnim biometrijskim uzorcima). U tom slučaju, cilj napadača je da dođe do ključa (ili da smanji prostor pretrage), da pristupi legitimnom biometrijskom šablonu ili generiše lažnu verziju istog.

### **2.2.3 Primena kriptografije za zaštitu biometrijskih uzoraka i šablona**

Obrada biometrijskih signala u šifrovanom domenu je jedan od načina za otklanjanje problema koji se odnose na sigurnost biometrijskih šablona i privatnost korisnika. Međutim, treba uzeti u obzir da u velikom broju konvencionalnih

biometrijskih sistema za proveru identiteta nisu implementirane kriptografske mere zaštite. Jedno vreme su izvesni istraživači čak smatrali da je nemoguće izvršiti biometrijsku proveru identiteta u šifrovanom domenu zbog prirodne promenljivosti biometrijskih uzoraka i kriptografske netolerancije na neispravnost jednog bita podataka. Shodno tome, primenom klasičnih metoda šifrovanja, koje ne podrazumevaju izvršavanje operacija u šifrovanom domenu, šifrovani biometrijski podaci moraju biti dešifrovani prilikom autentifikacije, što dovodi do problema koji se odnose na sigurnost i privatnost. Takođe krađa ključa za dešifrovanje za posledicu ima kompromitovanje svih šablona u bazi.

Međutim, zahvaljujući mogućnostima koje pružaju takozvane tehnike sigurnog računanja koje izvršava više entiteta (engl. *Secure Multiparty Computation*, SMPC) moguće je uporediti dva biometrijska šablona u šifrovanom domenu, odnosno izvršiti poređenje koristeći samo šifrovane podatke. Osim toga, moguće je dizajnirati protokol poređenja na takav način da rezultat poređenja bude poznat samo entitetu kome je namenjen bez curenja informacija o biometrijskom šablonu ili subjektu na osnovu čijeg uzorka je šablon generisan. Ovakve tehnike koje omogućavaju obradu šifrovanih signala nazivaju se obrada signala u šifrovanom domenu (*Signal Processing in the Encrypted Domain*, SPED).

Kao primer, razmotrićemo scenario u kojem je potrebno da server dobije informaciju da li je vlasnik biometrijskog šablona deo liste upisanih subjekata koji su legitimni korisnici (na primer, korisnici koji mogu pristupiti određenom resursu) ili kriminalac čiji je identitet dobro poznat policiji ili Federalnom birou za istrage. Na serveru se nalazi baza biometrijskih šablona a korisnik je zainteresovan da iskoristi uslugu bez otkrivanja svog identiteta. Alternativno, potencijalni korisnik može želeći da sazna da li njegov biometrijski signal odgovara nekom od šablona koji su smešteni na serveru. Shodno skupu tehnika za obradu signala u šifrovanom domenu, prethodno pomenuti zahtevi su ispunjivi, tj. sve što je zahtevano se može izvesti ukoliko se serveru dozvoli da uporedi priložen šablon sa šablonima smeštenim u bazi podataka u šifrovanom domenu.

Dva osnovna pristupa obradi signala u šifrovanom domenu su homomorfno šifrovanje (engl. *homomorphic encryption*) [104] i takozvana tehnika izopačenog puta (engl. *garbled circuits*, GC) [138].

Homomorfno šifrovanje obezbeđuje način za izvršavanje linearnih operacija nad šifrovanim podacima. Međutim, kada su u pitanju nelinearne operacije, potrebno je pribеći interaktivnim i obično složenim protokolima. U skorije vreme, predložene su šeme potpunog homomorfnog šifrovanja (engl. *Fully Homomorphic Encryption*, FHE) [44] koje omogućavaju izvršavanje bilo koje funkcije bez interakcije uključenih entiteta. Na žalost, potpuno homomorfno šifrovanje je za sada veoma neefikasno, što je najvećim delom posledica veličine javnog ključa.

Uprkos znatnim skorašnjim dostignućima i novim efikasnijim kriptografskim primitivama, protokol obrade signala u šifrovanom domenu je često isuviše složen kako bi se upotrebio u praktičnim domenima primene. Takođe treba uzeti u činjenicu da je za sada nepoznato da li se mnogo bolji rezultati mogu dobiti razvijanjem klase algoritama za koje se izričito veruje da olakšavaju implementaciju tehnika obrade signala u šifrovanom domenu (na primer, razmatranjem koje su najsloženije operacije koje treba izvesti na siguran način i izbegavanjem istih).

Da bi se složenost smanjila na prihvatljiv nivo, neophodno je da se prilikom projektovanja algoritama koji obrađuju biometrijske podatke i protokola koji obrađuje podatke između dva entiteta (engl. *Secure Two-Party Computation*, STPC) uzmu u obzir kako kriptografski aspekti, tako i aspekti obrade signala. Međutim, najčešći pristup do sada je suprotan prethodno pomenutom zahtevu: klasičan biometrijski algoritam za poređenje se jednostavno pretvara u protokol koji će se izvršavati u šifrovanom domenu.

U osnovi, neophodno je da biometrijski šabloni budu predstavljeni vektorom obeležja konstantne dužine i da prosta metrika (na primer, Hemingovo ili Euklidsko rastojanje) mogu biti iskorišćeni za merenje sličnosti između dva vektora. Ukoliko su prethodna dva uslova ispunjena, protokol za biometrijsku autentifikaciju, odnosno verifikaciju korisnika može se razviti na jednostavan način, pri čemu će se sastojati od sledećih blokova: računanje rastojanja, odabir minimuma i poređenje sa pragom [24, 23]. Prilikom dizajniranja sistema takođe treba uzeti u obzir činjenicu da efikasnost ne zavisi samo od prikladnog algoritma za poređenje, već u obzir treba uzeti i količinu informacije u biometrijskom šablonu. Drugim rečima, složenost sistema za obradu signala u šifrovanom domenu zavisi od broja obeležja koje algoritam za poređenje koristi kao i od broja bitova kojima

su obeležja predstavljena. Upotrebom manjeg broja obeležja ili kraćih obeležja složenost protokola se smanjuje, ali se istovremeno smanjuje i tačnost prepoznavanja zbog umanjene količine informacije koja se poredi. To znači da je neophodno naći kompromis ili obezbediti ispravan dizajn sistema kako se ne bi povećavala složenost ili degradirala efikasnost.

Kriptografski sistem se smatra homomorfni [43] ukoliko su određene operacije nad šifrovanim podacima izvodljive i ukoliko odgovaraju operacijama izvedenim nad otvorenim tekstovima datih šifrata. Većina homomorfni šifarskih sistema se u osnovi oslanja na kriptografiju sa javnim ključem, pri čemu svojstvo homomorfni obezbeđuje javni ključ jednog od entiteta koji je deo protokola. Drugim rečima, ukoliko drugačije nije naznačeno, pretpostavlja se da je privatni ključ poznat jedino klijentu, dok server može da pristupi samo javnom ključu.

Najčešći homomorfni kriptosistemi su aditivno homomorfni (na primer, sistemi predstavljeni u [88, 31]). Aditivno homomorfni kriptosistem dozvoljava entitetu koji je u posedu ključa za dešifrovanje da izvrši šifrovanje sume dve vrednosti koje su jedino njemu dostupne u šifrovanom obliku. Složenije operacije se mogu izvesti ukoliko se pribegne interaktivnom protokolu između servera i klijenta.

Uprkos očiglednoj upotrebnoj vrednosti, korišćenje homomorfni šifrovanja je veoma zahtevno po pitanju računске složenosti i prostora potrebnog za skladištenje. Na primer, u Paillier-ovom kriptosistemu, jednostavne vrednosti predstavljene sa nekoliko bita proizvode šifrat dužine 2.048 bita, što znači da se sume malih vrednosti mapiraju na proizvode, odnosno da rezultuju veoma dugačkim šifratom. Nelinearne operacije, poput množenja šifrovanih vrednosti ili poređenja su još složenije i zahtevaju interakciju između entiteta. Zbog toga, komunikaciona zahtevnost protokola zasnovanog na homomorfni šifrovanju zavisi od broja prenešenih šifrata, kao i od broja poruka poslatih u komunikaciji, dok računska složenost zavisi od broja računanja eksponencijalnih funkcija (koje predstavljaju računski najzahtevnije operacije) u protokolu.

Multiplikativni homomorfni sistemi [104, 39] dozvoljavaju izračunavanje proizvoda dve šifrovane vrednosti, međutim, imaju manju upotrebnu vrednost u odnosu na aditivne sisteme.

Jedan od prvih radova u kome se pominje protokol za biometrijsku autentifikaciju koji štiti privatnost je [19]. Protokol nije zasnovan na konkretnom biometrijskom modalitetu, već na generalnom biometrijskom predstavljanju uzoraka pomoću binarnih nizova. Nakon toga, u radu je predstavljena sigurna implementacija računanja Hemingovog rastojanja.

Implementacija biometrijskih identifikacionih protokola koji čuvaju privatnost šablona zasnovana na eigen-licima [132] dostiže tačnost klasifikacije 96% u slučaju promene osvetljenja, tačnost klasifikacije 85% ukoliko se u obzir uzmu i izmene orijentacije lica i 64% ukoliko se menja i veličina lica. Za razliku od većine biometrijskih protokola za prepoznavanje zasnovanih na obradi signala u šifrovanom domenu, u ovom pristupu se izdvajanje obeležja takođe izvodi u šifrovanom domenu oslanjajući se na svojstva Paillier-ovog kriptosistema [88]. Računanje kvadrata Euklidovog rastojanja implementirano je takođe upotrebom Paillier-ovog kriptosistema, dok je protokol za poređenje implementiran shodno pristupu koji su predstavili Damgard i dr. [31]. Međutim, prosečno vreme potrebno za prepoznavanje lica iznosi oko 40 sekundi. Autori navode da je moguće smanjiti računsku složenost i komunikacionu zahtevnost pod pretpostavkom da su parametri koji se koriste u protokolu za izdvajanje obeležja javni. Ova pretpostavka je usvojena u većini radova u kojima su opisana istraživanja iz date oblasti.

Istraživanja vezana za homomorfno šifrovanje i prepoznavanje dužice sprovedli su Luo i dr. [72] tako što su implementirali protokol za biometrijsku autentifikaciju zasnovan na kodu dužice [33] i verifikovali rezultate na CASIA Iris bazi podataka biometrijskih uzoraka – konkretno na 100 šablona veličine 9.600 bitova. Rezultujućem protokolu je potrebno oko 27 minuta u proseku da obradi zahtev na računaru sa procesorom čiji je radni takt 2,4 GHz. Ovu kompleksnost autori opravdavaju veličinom kodova dužice koji su šifrovani Paillier-ovim kriptosistemom.

Bringer i dr. [21, 20], Schoenmakers i Tuyls [108], i Upmanyu i dr. [136] takođe su predložili upotrebu homomornog šifrovanja u biometrijskim sistemima za autentifikaciju u kojima je očuvana privatnost korisnika. Autori su razmotrili sledeće homomorfne kriptosisteme: Goldwasser-Micali, Paillier, ElGamal i RSA. Autori su takođe ustanovili da su kriptografski algoritmi koji poseduju svojstvo

homomorfnosti najpogodniji za poređenje šablona ukoliko se u šifrovanom dome- nu izvršavaju jednostavne operacije (na primer, operacija ekskluzivno ILI nad dva binarna niza). U tom smislu, autori smatraju da je ova vrsta zaštite šablona pogodna u sistemima za prepoznavanje dužice koji koriste binarni šablon dužine 2048 bita.

Drugačiji pristup je predstavljen u [10]. Autori su koristili hibridni pri- stup za biometrijsku identifikaciju (homomorfno šifrovanje i tehniku izopa- čenog puta) za biometrijsku identifikaciju koji je optipizovan and optimize it by pred-računanjem većine operacija. Dalja unapređenja se svode na optimizaciju protokola za množenje i upotrebom Damgard-Geisler-Kroigard metode [31] za izraču- navanje sličnosti. Implementacija protokola je testirana, a ostvareni rezultati ukazuju na 25% povećanja u brzini u odnosu na identičan protokol koji koristi samo homomorfno šifrovanje. Shodno navodima autora, poređenje dva šifrovana koda dužice dužine 2.048 bita traje samo 0,15 sekundi.

Protokol opisan u istraživanju objavljenom u [73] izvršen na procesoru sa rad- nim taktom od 3GHz upotrebljen je za poređenje kodova dužice generisanih na osno- vu CASIA Iris baze podataka dužine 9.600 i 2.048 bitova. Zahvaljujući pred-obradi, odnosno unapred obavljenim izračunavanjima, poređenje dva koda dužice dužine 2.048 bitova traje 0,56 sekundi uz prenos 571 kilobajta podataka, dok poređenje kodova veličine 9.600 bitova traje 2,5 sekundi i zahteva prenos 2,655 kilobajta podataka.

Uzevši u obzir činjenicu da prethodno pomenuti protokoli koriste vektore fiksne dužine, većina šema predloženih za poređenje otisaka prsta zasnovane su na takozvanim kodovima prstiju (engl. fingercodes) [56]. Na primer, u istraživanji- ma koja su sproveli Barni i dr. [7, 8] implementiran je identifikacioni protokol zasnovan na Paillier-ovom kriptosistemu. Izvršavanje protokola nad bazom koja sa- drži 64 identiteta traje oko 16 sekundi na računaru sa procesorom čiji je radni takt 2,4 GHz.

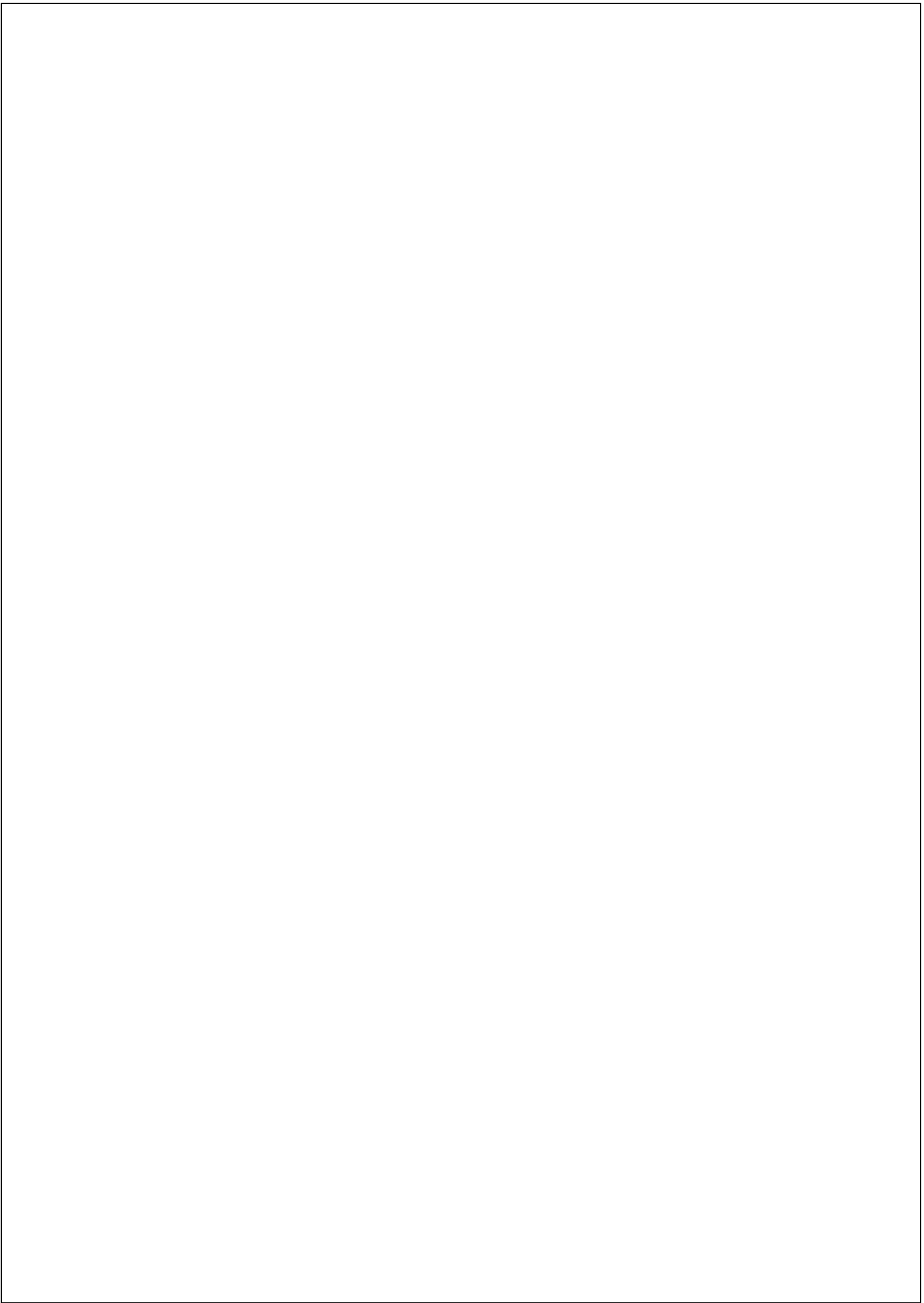
Istraživanja u oblasti prepoznavanja otisaka prstiju, u kojima su upotrebljeni slični protokoli koji su korišćeni za prepoznavanje dužice, opisana su u [10]. Shodno [7], implementacija zasnovana na kodovima prstiju je 35 puta brža (izvr- šavanje na klijentu traje oko 0,35 sekundi, dok na serveru traje oko 0,45 sekundi).

Protokol je takođe prilagođen za rad sa karakterističnim tačkama otisaka prstiju [81] (rezultati prijavljeni u [56] ukazuju na činjenicu da je FAR manji od 1 %), ali je vreme izvršavanja znatno uvećano.

Povećanjem popularnosti šema potpunog homomornog šifrovanja za posledicu ima i dizajn nekoliko potpuno neinteraktivnih rešenja za očuvanje privatnosti u biometrijskim sistemima za autentifikaciju. Prvi neinteraktivni protokol za biometrijsku autentifikaciju [129] zasnovan je na proširenju rešenja predstavljeno u [45]. Sva izračunavanja, osim šifrovanja ulaza i dešifrovanja rezultata, obavljaju se na serveru.

Računska složenost se značajno smanjuje u odnosu na Pailler-ov kriptosistem. Na primer, implementacija predstavljena u [129] zahteva 59 sekundi za verifikaciju lica, dok je 420 sekundi potrebno za verifikaciju na ekvivalentnoj implementaciji zasnovanoj na Paillier-ovom kriptosistemu. Dodatna prednost je eliminisanje interakcije između entiteta. Negativna posledica upotrebe proširenja rešenja predstavljenog u [45] je povećanje komunikacione zahtevnosti: implementacija predstavljena u [129] zahteva prenos 393 MB podataka, dok je samo 16,4 MB potrebno za verziju zasnovanu na Paillier-ovom kriptosistemu.

Iako su istraživanja koja se odnose na efikasnost, odnosno smanjivanje složenosti privuklo pažnju istraživača, većina istraživanja je usmerena na efikasnije primitive protokola koji obrađuje podatke između dva entiteta i njihovu primenu u konvencionalnim biometrijskim sistemima za poređenje u okviru radnog okvira za obradu signala u šifrovanom domenu. Postoje izvesne pretpostavke da se značajna unapređenja mogu ostvariti istraživanjima na nivou obrade signala, kao i na zajedničkom razmatranju kriptografskih aspekata i aspekata obrade signala.



## Glava 3

# Teorijske osnove istraživanja

### 3.1 Kriptografija sa javnim ključevima

Kriptografija sa javnim ključevima podrazumeva korišćenje dva ključa  $(K_e, K_d)$  [114]. Ključ  $K_e$  je javni, i koristi se za šifrovanje, a ključ  $K_d$  je tajni, i koristi se za dešifrovanje. Primena kriptografije sa javnim ključevima se može opisati na sledeći način. Neka subjekat  $B$  poseduje par ključeva  $(K^B, K^B)$ . Svako može da pošalje poruku  $M$  subjektu  $B$  tako što će je šifrovati javnim ključem  $K^B$ :

$$C = E(M, K_e^B) , \quad (3.1)$$

pri čemu samo  $B$  može da dešifruje  $C$ , koristeći tajni ključ  $K^B$ :

$$M = D(C, K_d^B) . \quad (3.2)$$

Osim toga, subjekat  $B$  može digitalno da potpiše poruku tako što će je šifrovati svojim tajnim ključem  $K^B$ . Tada svako može da verifikuje ovaj digitalni potpis dešifrovanjem poruke pomoću javnog ključa  $K^B$ . Konačno, treća primena se odnosi na razmenu simetričnih ključeva. U nastavku je opisan algoritam RSA za kriptografiju sa javnim ključevima.

#### 3.1.1 Algoritam RSA

Najpoznatiji algoritam za kriptografiju sa javnim ključevima, RSA [104, 114], bazira se na sledećoj jednosmernoj funkciji sa zamkom<sup>1</sup> (engl. trapdoor function).

<sup>1</sup>Jednosmerne funkcije sa zamkom su definisane u sekciji 3.4.1.

Neka su  $p$  i  $q$  dva izabrana velika prosta broja, na osnovu kojih se određuju sledeće vrednosti: (a) modul  $n$ , kao proizvod:

$$n = pq , \quad (3.3)$$

(b) eksponent za šifrovanje  $e$ , kao izabrani celi broj iz opsega  $[1, (p-1)(q-1)-1]$  koji je uzajamno prost sa  $(p-1)(q-1)$ , što ćemo obeležavati:

$$(e, (p-1)(q-1)) = 1 , \quad (3.4)$$

i (v) eksponent za dešifrovanje  $d$ , tako da važi:

$$ed = 1 \pmod{(p-1)(q-1)} . \quad (3.5)$$

Uređeni par  $(n, e)$  predstavlja javni ključ, a broj  $d$  privatni ključ. Pre šifrovanja, poruka  $M$  se deli na sekvencu blokova  $M_1, M_2, \dots, M_b$ , od kojih je svaki predstavljen celim brojem iz opsega  $[0, n-1]$ . Postupak šifrovanja bloka  $M_i$ , za  $1 \leq i \leq b$  je:

$$C_i = M_i^e \pmod{n} , \quad (3.6)$$

a dešifrovanja:

$$M_i = C_i^d \pmod{n} . \quad (3.7)$$

Da bismo objasnili ove postupke, iskoristićemo Ojlerovu funkciju, Ojlerovu teoremu, i njen slecijalni slučaj – Fermaovu teoremu [47, 52, 114].

**Definicija 1.** Ojlerova funkcija: Vrednost Ojlerove funkcije  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  za dati broj  $n$  jednaka je broju pozitivnih celih brojeva koji su manji od  $n$  i uzajamno prosti sa  $n$ :

$$\phi(n) = |\{e \mid e \in \{1, 2, \dots, n-1\} \wedge (e, n) = 1\}| . \quad (3.8)$$

**Lema 1.** Neka je  $p$  prost broj. Tad važi:

$$\phi(p) = p - 1 . \quad (3.9)$$

*Dokaz.* Po definiciji Ojlerove funkcije, nije moguće da važi  $\phi(p) > p - 1$ . Ako bi važilo  $\phi(p) < p - 1$ , to bi značilo da postoji broj  $1 < x < p$  takav da je  $p$  deljiv sa  $x$ , što je nemoguće, jer je  $p$  prost broj. Zaključujemo da je  $\phi(p) = p - 1$ .  $\square$

Ojlerova funkcija je multiplikativna, tj., za uzajamno proste brojeve  $m$  i  $n$  važi:

$$\phi(mn) = \phi(m)\phi(n) . \quad (3.10)$$

Za potrebe ovog izlaganja biće dovoljno da pokažemo da jednakost (3.10) važi kad su  $m$  i  $n$  prosti brojevi.

**Lema 2.** *Neka su brojevi  $p$  i  $q$  prosti brojevi, i  $p \neq q$ . Tad važi:*

$$\phi(pq) = (p - 1)(q - 1) . \quad (3.11)$$

*Dokaz.* Polazeći od postavke da su  $p$  i  $q$  prosti brojevi, skup celih brojeva iz opsega  $[1, pq - 1]$  koji nisu uzajamno prosti sa  $pq$  jednak je

$$S = S_p \cup S_q , \quad (3.12)$$

gde  
su:

$$\begin{aligned} S_p &= \{ip | 1 \leq i \leq q - 1\} , \\ S_q &= \{jq | 1 \leq j \leq p - 1\} , \end{aligned} \quad (3.13)$$

pri čemu se lako pokazuje da  $S_p \cap S_q = \emptyset$ , odnosno  $|S| = |S_p| + |S_q| = p + q - 2$ . Odatle sledi:

$$\begin{aligned} \phi(pq) &= |\{1, 2, \dots, pq - 1\}| - |S| \\ &= (pq - 1) - |S| \\ &= (pq - 1) - (|S_p| + |S_q|) \\ &= (pq - 1) - (p + q - 2) \\ &= (p - 1)(q - 1) . \end{aligned} \quad (3.14)$$

=

**Teorema 3.** *Ojlerova teorema: Neka su  $n$  i  $a$  uzajamno prosti prirodni brojevi. Tada važi:*

$$a^{\phi(n)} \equiv 1 \pmod{n} . \quad (3.15)$$

*Dokaz.* Za dato  $n$ , neka skup  $X = \{x_1, x_2, \dots, x_{\phi(n)}\}$  sadrži sve različite prirodne brojeve manje od  $n$  koji su uzajamno prosti sa  $n$ :

$$(\forall 1 \leq i \leq \phi(n)) (ax_i, n) = 1 . \quad (3.16)$$

Pošto su  $a$  i  $x_i \in X$  uzajamno prosti sa  $n$ , tada i proizvod  $ax_i$  mora biti uzajamno prost sa  $n$ . U suprotnom, kada bi važiolo da  $ax_i$  i  $n$  nisu uzajamno prosti, to bi značilo da jedan od brojeva  $a$  i  $x_i$  nije uzajamno prost sa  $n$ , što je kontradikcija.

Takođe, važi i:

$$(\forall 1 \leq i, j \leq \phi(n)) i \neq j \Rightarrow ax_i \neq ax_j \pmod{n} . \quad (3.17)$$

Kad bi važiolo  $ax_i = ax_j \pmod{n}$ , tada bi razlika  $ax_i - ax_j$  morala biti deljiva sa  $n$ , što je kontradikcija.

Imajući u vidu (3.16) i (3.17), lako se pokazuje da je skup ostataka brojeva  $\{ax_1, ax_2, \dots, ax_{\phi(n)}\}$  pri deljenju sa  $n$  jednak skupu  $X$ . Dalje imamo:

$$\begin{aligned} ax_i &= x_i \pmod{n} \\ \Leftrightarrow a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i &= \prod_{i=1}^{\phi(n)} x_i \pmod{n} \\ \Leftrightarrow a^{\phi(n)} &= 1 \pmod{n} . \end{aligned} \quad (3.18)$$

Time je dokaz Ojlerove teoreme završen. =

**Teorema 4. Fermaova teorema:** Neka su  $p$  prost broj, i  $a$  celi broj. Tada važi:

$$a^p = a \pmod{p} . \quad (3.19)$$

*Dokaz.* Po Ojlerovoj teoremi (teorema 3) važi:

$$a^{\phi(p)} = 1 \pmod{p} , \quad (3.20)$$

a po lemi 1:

$$\phi(p) = p - 1 . \quad (3.21)$$

Dalje sledi:

$$\begin{aligned} a^{\phi(p)} &= 1 \pmod{p} \\ \Leftrightarrow a^{p-1} &= 1 \pmod{p} \\ \Leftrightarrow a^p &= a \pmod{p} . \end{aligned} \quad (3.22)$$

Ovim je dokaz teoreme završen, a u nastavku izlaganja ćemo se pozvati na jednakost  $a^{p-1} = 1 \pmod{p}$ . =

**Teorema 5.** Pod uslovima definisanih stavkama (3.3), (3.4), (3.5) i (3.6), važi:

$$M_i = C_i^d \pmod{n} . \quad (3.23)$$

*Dokaz.*

$$\begin{aligned} M_i &= C_i^d \pmod{n} \\ \Leftrightarrow M_i &= M_i^{ed} \pmod{n}, & \leftarrow \text{(v. jednakost (3.6))} \\ \Leftrightarrow M_i &= M_i \cdot M_i^{ed-1} \pmod{n} \\ \Leftrightarrow M_i &= M_i \cdot M_i^{k\phi(n)} \pmod{n}, & \leftarrow \text{(v. jednakost (3.5))} \\ \Leftrightarrow M_i &= M_i \cdot M_i^{k\phi(pq)}, & \leftarrow \text{(v. jednakost (3.3))} \\ \Leftrightarrow M_i &= M_i \cdot M_i^{k(p-1)(q-1)}, & \leftarrow \text{(v. lemu 2)} \\ \Leftrightarrow M_i &= M_i \cdot 1^k \pmod{n}, & \leftarrow \text{(v. teoremu 4)} \\ \Leftrightarrow & . \end{aligned}$$

=

Jednosmerna funkcija sa zamkom koja se primenjuje u algoritmu RSA je:

$$f(x, n, l) = x^l \pmod{n} , \quad (3.24)$$

gde važi  $(l, \phi(n)) = 1$ . Valja primetiti da se tajnost algoritma RSA bazira na težini faktorisanja broja  $n = pq$ . Zbog toga se faktori  $p$  i  $q$  (iz jednakosti (3.3)) zamenaraju nakon izračunavanja vrednosti  $n$  [47, 52, 114].

### 3.1.2 Binarno potenciranje

Kao primer izvršavanja algoritma RSA, uzmimo da su  $p = 5$  i  $q = 11$ . Tada je modul  $n = pq = 55$ . Eksponent za šifrovanje se bira tako da bude uzajamno prost sa  $(p - 1)(q - 1) = 40$ , a eksponent za dešifrovanje se bira tako da važi  $ed = 1 \pmod{40}$ . Neka su  $e = 3$  i  $d = 27$ . Javni ključ je  $(55, 3)$ , a privatni 27. Šifrovanjem poruke  $M = 4$  dobija se šifrat  $C = M^e \pmod{n} = 4^3 \pmod{55} = 9$ , a njegovim dešifrovanjem početna poruka  $M = C^d \pmod{n} = 9^{27} \pmod{55} = 4$ .

U gornjem primeru, javlja se vrednost  $9^{27} \pmod{55}$ . Njeno izračunavanje prostim stepenovanjem pre deljenja po modulu nije praktično, jer daje nepotrebno veliki broj ( $\approx 5.8149737 \cdot 10^{25}$ ). Ovaj problem je još izraženiji u realnim primenama, u kojima

modul  $n$  zauzima ne manje od 1024 bita. Zbog toga, primenjuje se metoda binarnog potenciranja.

Ovu metodu ćemo prikazati na primeru izračunavanja vrednosti  $7^{18} \pmod{33}$ . Vrednost eksponenta 18 u binarnom zapisu je 10010. Ako bismo ovaj binarni broj generisali bit po bit, počevši od najznačajnijeg bita, sekvenca binarnih vrednosti bi glasila:

$$0, 1, 10, 100, 1001, 10010 . \quad (3.25)$$

a sekvenca odgovarajućih dekadnih vrednosti:

$$0, 1, 2, 4, 9, 18 . \quad (3.26)$$

Iz poslednje sekvence se može utvrditi sledeći način za generisanje eksponenta 18:

$$\begin{aligned} 1 &= 0 \cdot 2 + 1 , \\ 2 &= 1 \cdot 2 , \\ 4 &= 2 \cdot 2 , \\ 9 &= 4 \cdot 2 + 1 , \\ 18 &= 9 \cdot 2 . \end{aligned} \quad (3.27)$$

Postupak izračunavanja vrednosti  $7^{18} \pmod{33}$  se izvodi na sledeći način:

$$\begin{aligned} 7^1 &= (7^0)^2 \cdot 7^1 = 7 \pmod{33} , \\ 7^2 &= (7^1)^2 = 16 \pmod{33} , \\ 7^4 &= (7^2)^2 = 25 \pmod{33} , \\ 7^9 &= (7^4)^2 \cdot 7^1 = 19 \pmod{33} , \\ 7^{18} &= (7^9)^2 \pmod{33} = 31 . \end{aligned} \quad (3.28)$$

U opštem sličaju, vrednosti koje se izračunavaju u ovom postuku nisu veće od  $n^3$ , čime je izbegnuto izračunavanje nepraktično velikih vrednosti.

## 3.2 Generatori pseudoslučajnih brojeva

Generatori pseudoslučajnih brojeva su deterministički programi koji kao ulazni parametar prihvataju kratku sekvencu bitova  $x$  i generišu dugačku sekvencu

Tabela 3.1: Izabrani generatori pseudoslučajnih brojeva (tabela prilagođena iz [47]).

| Ime                         | Jednosmerna funkcija sa zamkom $f$ | Kompleksnost izračunavanja: |                         |
|-----------------------------|------------------------------------|-----------------------------|-------------------------|
|                             |                                    | $f$                         | $j$ -tog bita           |
| Rivest/Shamir/Adleman [104] | $x^e \pmod{n}, n = pq$             | $k^3$                       | $jk^3$                  |
| Rabin [91]                  | $x^e \pmod{n}, n = pq$             | $k^2$                       | $jk^2$                  |
| Blum/Micali [12]            | $\text{exp}(p, q, x)$              | $k^3$                       | $jk^3$                  |
| Blum/Blum/Shub [11]         | $x_{k+1} = x_k^2$                  | $k^2$                       | $\max(k^2 \log j, k^3)$ |

bitova  $y$ , koja izgleda kao da je slučajno generisana. Ulazni parametar nazivamo ključem, a rezultat generisanja pseudoslučajnom sekvencom bitova. Generisana sekvencija je pseudoslučajna, jer skup sekvenci koje je moguće generisati neobuhvata sve moguće sekvence, tj., broj sekvenci koje je moguće generisati je manji od ili jednak broju mogućih ključeva  $x$  [47].

Da bi se postigao zadovoljavajući nivo sigurnosti, sekvenca  $y$  mora da bude takva da ako je napadaču poznat deo sekvence, on ne može da predvidi ostale delove sekvence, ni početni ključ  $x$ . Generator pseudoslučajnih brojeva se smatra sigurnim ako verovatnoća predviđanja sledećeg bita na osnovu prefiksne sekvence bitova nije veća od verovatnoće slučajnog pogađanja [12]. Ovakvi generatori su perfektni u smislu da verovatnoća da će algoritam koji se izvršava u polinomnom vremenu pogoditi da li je sekvenca dužine  $k$  slučajno izabrana iz skupa  $\{0, 1\}^k$  ili generisana nije značajno veća od 0.5 [?], tj. zadovoljava sve statističke testove koji se izvršavaju u polinomnom vremenu.

Izabrani generatori pseudoslučajnih brojeva dati su u tabeli 3.1.

### 3.2.1 Osnovni pojmovi

U nastavku ćemo formalno definisati relevantne pojmove [47].

**Definicija 2.** Neka su  $X_n$  i  $Y_n$  raspodele verovatnoće nad skupom  $\{0, 1\}^n$ . Kažemo da se  $\{X_n\}$  ne može razlikovati u polinomnom vremenu od  $\{Y_n\}$  ako za svaki algoritam sa polinomnim vremenom izvršavanja  $A$ , i svaki polinom  $Q$ , postoji  $n_0$  takvo da za svako  $n > n_0$  važi:

$$|P_{t \in X_n}(A(t) = 1) - P_{t \in Y_n}(A(t) = 1)| < \frac{1}{Q(n)}. \quad (3.29)$$

**Definicija 3.** Raspodela  $\{X_n\}$  je pseudoslučajna ako se ne može razlikovati u polinomnom vremenu od uniformne raspodele  $\{U_n\}$ , tj., ako za svaki algoritam sa polinomnim vremenom izvršavanja  $A$ , i svaki polinom  $Q$ , postoji  $n_0$  takvo da za svako  $n > n_0$  važi:

$$|P_{t \in X_n}(A(t) = 1) - P_{t \in U_n}(A(t) = 1)| < \frac{1}{Q(n)} . \quad (3.30)$$

**Definicija 4.** Deterministički program  $G : \{0, 1\}^k \rightarrow \{0, 1\}^{\hat{k}}$  sa polinomnim vremenom izvršavanja je generator pseudoslučajnih brojeva ako važi:

- $\hat{k} > k$ ,
- $\{G_k\}_k$  je pseudoslučajna raspodela, gde je  $G_k$  raspodela nad skupom  $\{0, 1\}^{\hat{k}}$  dobijena na sledeći način:
  - izabere se  $x \in U_k$ , gde je  $U_k$  uniformna raspodela nad skupom  $\{0, 1\}^k$ ,
  - dodeli se vrednost  $t = G(x)$ .

tj., ako za svaki algoritam sa polinomnim vremenom izvršavanja  $A$ , svaki polinom  $Q$ , i za svako dovoljno veliko  $k$  važi:

$$|P_{t \in G_k}(A(t) = 1) - P_{t \in U_k}(A(t) = 1)| < \frac{1}{Q(\hat{k})} . \quad (3.31)$$

Algoritam sa polinomnim vremenom izvršavanja  $A$ , koji se spominje u gornjim definicijama, naziva se statističkim testom. Jedan od statističkih testova je test sledećeg bita.

**Definicija 5.** Generator pseudoslučajnih brojeva zadovoljava test sledećeg bita  $A$  ako za svaki polinom  $Q$  postoji  $k_0$  takvo da za svako  $\hat{k} > k_0$  i  $p < \hat{k}$  važi:

$$P_{t \in G_k}(A(t_1, t_2, \dots, t_p) = t_{p+1}) < \frac{1}{2} + \frac{1}{Q(k)} . \quad (3.32)$$

Ovde navodimo sledeću teoremu bez dokaza (dokaz je dat u [47]).

**Teorema 6.**  $G$  zadovoljava sve testove sledećeg bita ako i samo ako  $G$  zadovoljava sve statističke testove.

Tabela 3.2: NIST testovi za proveru slučajnosti proizvoljno dugačkih binarnih sekvenci [106].

| Br. | Test                                                                         |
|-----|------------------------------------------------------------------------------|
| 1.  | Ispitivanje učestalosti u nizu                                               |
| 2.  | Ispitivanje učestalosti u bloku                                              |
| 3.  | Ispitivanje uzastopnog ponavljanja istih bitova u nizu                       |
| 4.  | Ispitivanje najdužeg uzastopnog ponavljanja jedinica u $n$ -bitnim blokovima |
| 5.  | Ispitivanje stanja binarne matrice                                           |
| 6.  | Test zasnovan na diskretnoj Furijeovoj transformaciji                        |
| 7.  | Ispitivanje nepreklapajućih uzoraka                                          |
| 8.  | Ispitivanje preklapajućih uzoraka                                            |
| 9.  | Maurerov univerzalni statistički test                                        |
| 10. | Ispitivanje linearne složenosti                                              |
| 11. | Ispitivanje učestalosti svih mogućih preklapanja $n$ -bitnih podnizova       |
| 12. | Ispitivanje približne entropije                                              |
| 13. | Ispitivanje kumulativnih zbirova                                             |
| 14. | Ispitivanje slučajne digresije                                               |
| 15. | Ispitivanje slučajne promenljive digresije                                   |

### 3.2.2 Ispitivanje približne entropije

Pregled NIST testova za proveru slučajnosti proizvoljno dugačkih binarnih sekvenci [106] dat je u tabeli 3.2, a ovde će se detaljnije razmotriti jedan od njih: ispitivanje približne entropije.

Jedna od pretpostavki za testiranje generatora pseudoslučajnih brojeva je da dve slučajne promenljive koje imaju istu raspodelu verovatnoće, imaju i istu me- ru neodređenosti [128]. Kao mera neodređenosti koristi se pojam entropije [110]. Entropija slučajne promenljive  $X = \{x_1, x_2, \dots, x_n\}$  se definiše:

$$H(X) = - \sum_{x \in X} p(x) \log p(x). \quad (3.33)$$

Osnovna ideja ispitivanja približne entropije je sledeća [105]. Neka je  $E_1, E_2, \dots, E_n$  sekvenca nezavisnih i jednako raspodeljenih slučajnih vrednosti. Uzmimo da su:

$$Y_i(m) = (E_i, \dots, E_{i+m-1}) \text{ za } 1 \leq i \leq n - m + 1, \quad (3.34)$$

$$C_i^m = \frac{1}{n - m + 1} \# \{j : 1 \leq j \leq n - m + 1, Y_j(m) = Y_i(m)\}, \quad (3.35)$$

$$\Phi^{(m)} = \frac{1}{n - m + 1} \sum_{i=1}^{n-m+1} \log C_i^m. \quad (3.36)$$

Približna entropija  $ApEn$  reda  $m$  definisana je sa:

$$ApEn(m) = \Phi^{(m)} - \Phi^{(m+1)} , \quad (3.37)$$

pri čemu je:

$$ApEn(0) = -\Phi^{(1)} . \quad (3.38)$$

Male vrednosti  $ApEn(m)$  impliciraju snažnu pravilnost u sekvenci, dok velike vrednosti  $ApEn(m)$  impliciraju fluktuaciju u sekvenci. Može se pokazati da važi:

$$\Phi^{(m)} \sim -m \log s , \quad (3.39)$$

i

$$ApEn(m) = \Phi^{(m)} - \Phi^{(m+1)} \rightarrow \log s , \quad (3.40)$$

gde je  $s$  broj različitih vrednosti koje  $E_i$  može da uzme. Zbog osobine iskazane u jednakosti (3.40), analitički dokazi asimptotskog ponašanja i procenjenih varijansi približne entropije su ekstremno teški [105]. Zbog toga se uvodi nova definicija za  $\Phi^{(m)}$ :

$$\tilde{\Phi}^{(m)} = \sum_{i_1 \dots i_m} v_{i_1 \dots i_m} \log v_{i_1 \dots i_m} , \quad (3.41)$$

U ovoj definiciji,  $v_{i_1 \dots i_m}$  predstavlja relativnu učestalost uzorka  $i_1 \dots i_m$  u cirkularnom stringu:

$$(E_1, \dots, E_n, E_1, \dots, E_{m-1}) , \quad (3.42)$$

tj.:

$$v_{i_1 \dots i_m} = \frac{\omega_{i_1 \dots i_m}}{n} , \quad (3.43)$$

i važi:

$$\sum_{i_1 \dots i_m} v_{i_1 \dots i_m} = n . \quad (3.44)$$

Sada je približna entropija definisana sa:

$$ApEn(m) = \tilde{\Phi}^{(m)} - \tilde{\Phi}^{(m+1)} . \quad (3.45)$$

Prednost  $ApEn(m)$  u odnosu na  $ApEn(m)$  je što za  $ApEn(m)$  važi:

$$(\forall m) \log s \geq ApEn(m) , \quad (3.46)$$

što nije slučaj za  $ApEn(m)$ . Sa porastom  $n$ , razlika između  $ApEn(m)$  i  $ApEn(m)$  postaje manja. U [105] je pokazano da približne entropije  $ApEn(m)$  i  $ApEn(m)$



Slika 3.1: Ilustracija modela komunikacionog kanala sa zaštitnim koderima.

konvergiraju u raspodeli ka slučajnoj promenljivoj  $\chi^2$  kada je  $m$  fiksno ili teži beskonačnosti. To omogućava da se koncept približne entropije primeni na statistički test slučajnosti sekvence. Za dato  $ApEn(m)$ ,  $\chi^2(obs)$  se definiše kao:

$$\chi^2(obs) = 2n | \log s - ApEn(m) | , \quad (3.47)$$

a  $P$ -vrednost se izračunava u skladu sa:

$$P_n(m) = 1 - P(2^{m-1}, \frac{\chi^2(obs)}{2}) , \quad (3.48)$$

gde  $P$  označava nekompletnu gama-funkciju [105].

Ako je  $P$ -vrednost manja od 0,01, smatra se da sekvenca nije slučajna. U suprotnom, smatra se da je sekvenca slučajna. Za praktične primene ovog testa, savetuje se da izbor parametara  $n$  i  $m$  bude takav da važi  $m < \log nj - 5$  (v. [106]).

### 3.3 Koderi i interliveri

#### 3.3.1 Zaštitni koderi

Delovanje šuma u kanalu za prenos podataka utiče na pouzdanost prenosa (model komunikacionog kanala sa šumom ilustrovan je na sl. 3.1). Zaštitni koderi su namenjeni ispravljanju grešaka nastalih usled šuma, tj., svođenju verovatnoće greške na proizvoljno malu vrednost [84].

Uvedimo osnovne pojmove koji su značajni za dalje izlaganje [84]:

- Razlika između dve binarne kodne reči iste dužine se može definisati pomoću operacije ekskluzivne disjunkcije,  $x_i \oplus x_j$ , što odgovara aritmetici po modulu 2.
- Hemingovo rastojanje između dve binarne kodne reči iste dužine,  $d(x_i, x_j)$  se definiše kao broj pozicija u kojima se reči razlikuju.

- Težina binarne kodne reči,  $w(x_i)$ , se definiše kao broj jedinica u reči.

Lako se pokazuje da za dve binarne kodne reči iste dužine,  $x_i$  i  $x_j$ , važi:

$$d(x_i, x_j) = w(x_i \oplus x_j) . \quad (3.49)$$

Neka je  $x$  reč koja je saopštena kanalu, i  $\hat{x}$  isporučena reč. Broj grešaka nastalih tokom prenosa reči  $x$  jednak je težini razlike reči  $x$  i  $\hat{x}$ , a time i Hemingovom rastojanju između ove dve reči. Problem ispravljanje grešaka nastalih u prenosu, u uslovima kada kodna reč  $x$  nije poznata, može se svesti na minimizovanje težine  $w(x_i \oplus x_j)$ , odnosno Hemingovog rastojanja  $d(x_i, x_j)$ . Za dati kod  $C$ , dekodovana reč  $D(\hat{x})$  se određuje kao reč koja je najbliža, u smislu Hemingovog rastojanja, reči  $\hat{x}$ :

$$D(\hat{x}) = \operatorname{argmin}_{x \in C} d(x, \hat{x}) . \quad (3.50)$$

Sa druge strane, dekodovana reč  $D(\hat{x})$  se može odrediti kao reč koja maksimizuje verovatnoću  $P(x|\hat{x})$ . U bajesovskom kontekstu, to sve svodi na [84]:

$$D(\hat{x}) = \operatorname{argmax}_{x \in C} P(x|\hat{x}) \quad (3.51)$$

$$\operatorname{argmax}_{x \in C} \frac{P(\hat{x}|x)P(x)}{P(\hat{x})} \quad (3.52)$$

$$\operatorname{argmax}_{x \in C} P(\hat{x}|x)P(x) . \quad (3.53)$$

Pod pretpostavkom da je verovatnoća  $P(x)$  konstantna, imamo:

$$D(\hat{x}) = \operatorname{argmax}_{x \in C} P(\hat{x}|x)P(x) \quad (3.54)$$

$$= \operatorname{argmax}_{x \in C} P(\hat{x}|x) . \quad (3.55)$$

Ako pretpostavimo i da svi bitovi imaju istu verovatnoću greške, jednaku  $p$ , dobija se:

$$D(\hat{x}) = \operatorname{argmax}_{x \in C} p^{d(x, \hat{x})} (1 - p)^{n - d(x, \hat{x})} . \quad (3.56)$$

Zaštitni koderi se mogu podeliti u dve grupe: linearni koderi i konvolucionni koderi. Razmotrićemo primere iz obe grupe.

### 3.3.1.1 Primer linearnog zaštitnog kodera

Primer iz prve grupe je binarni Hemingov kod  $(2^k - 1, 2^k - k - 1)$ , koji je namenjen ispravljanju vektora koji sadrže samo jednu grešku. Verifikaciona matrica za ovaj kod je [84]:

$$H_{k \times 2^k - 1}(k) = b(1, k)^T \ b(2, k)^T \ \dots \ b(2^k - 1, k)^T, \quad (3.57)$$

gde  $b(i, k)$  predstavlja binarni zapis broja  $i$ , dužine  $k$ .

Hemingov kod ćemo ilustrovati za slučaj  $k = 3$ . Verifikaciona matrica je:

$$H_{3 \times 7}(3) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \quad (3.58)$$

Generatorsku matricu  $G_{4 \times 7}$  nalazimo tako da zadovoljava:

$$G_{4 \times 7}(3) \times H_{3 \times 7}(3)^T = 0. \quad (3.59)$$

Jedno od rešenja je:

$$G_{4 \times 7}(3) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}. \quad (3.60)$$

Neka poruka koja treba da se prenese preko komunikacionog kanala ima vrednost:

$$l_{1 \times 4} = 0 \ 1 \ 1 \ 1. \quad (3.61)$$

Njenim množenjem sa generatorskom matricom  $G_{4 \times 7}(3)$  dobija se kodna reč:

$$x_{1 \times 7} = l_{1 \times 4} \times G_{4 \times 7}(3) = 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0. \quad (3.62)$$

Pretpostavimo da se tokom prenosa poruke desila greška na četvrtom bitu, tj., da je isporučena poruka:

$$\hat{x}_{1 \times 7} = 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0. \quad (3.63)$$

Da bi se ova greška otkrila, isporučena poruka se množi sa  $H_{3 \times 7}(3)^T$ , a rezultat indikuje poziciju bita na kome se desila greška. U posmatranom primeru imamo:

$$\hat{x}_{1 \times 7} \times H_{3 \times 7}(3)^T = 1 \ 0 \ 0, \quad (3.64)$$

tj., detektovana je greška na četvrtoj ( $100_2 = 4_{10}$ ) poziciji isporučene poruke.

### 3.3.1.2 Primer konvolucionog zaštitnog kodera

Neka je:

$$l = l_1, l_2, \dots, l_n \quad (3.65)$$

vrednost poruke koja treba da se prenese preko komunikacionog kanala. Konvolucionni koder koduje ovu poruku u (v. [84]):

$$x = x_1, x_2, x_3, x_4, \dots, x_{2n-1}, x_{2n}, \quad (3.66)$$

gde važi:

$$x_{2i-1} = l_i + l_{i-2}, \quad (3.67)$$

$$x_{2i} = l_i + l_{i-1} + l_{i-2}, \quad (3.68)$$

$$l_0 = 0, \quad (3.69)$$

$$l_{-1} = 0. \quad (3.70)$$

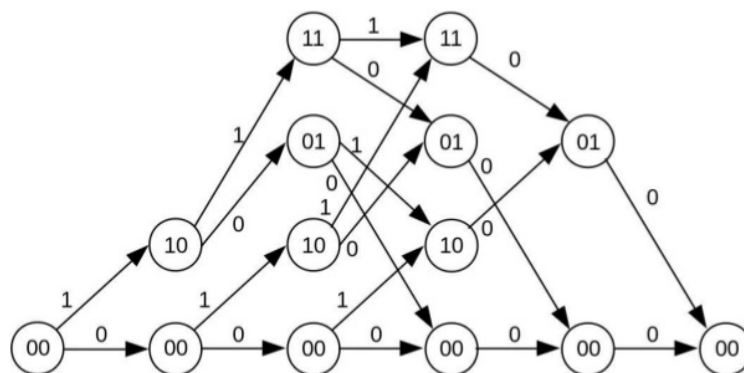
Za poruku dužine tri bita, generatorska martrica je:

$$G_{3 \times 10}^{(3)} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \quad (3.71)$$

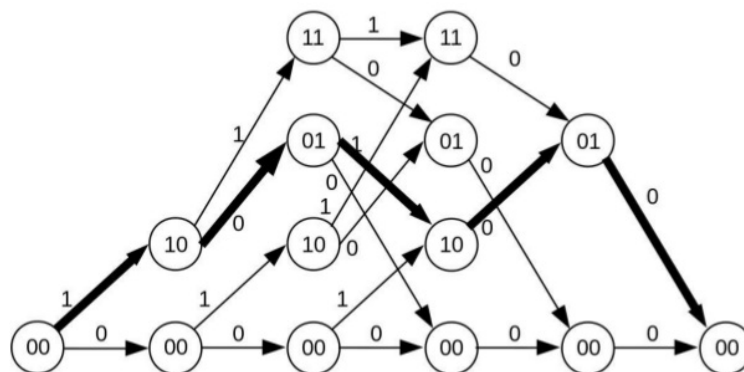
Međutim, rad ovakvog kodera se može predstaviti Markovljevim lancem, u kome su stanja definisana skupom:

$$\{(0, 0), (0, 1), (1, 0), (1, 1)\}, \quad (3.72)$$

što znači da kodovanje svake poruke predstavlja putanju kroz Viterbijev trellis [65]. Za posmatrani primer poruke dužine tri bita, na koju dodajemo dve nule (zbog (3.69) i (3.70)), Viterbijev trellis je dat na sl. 3.2. Broj kolona u trellisu je određen dužinom poruke, a u dve kolone koje prethode poslednjem čvoru, izlazne grane se odnose samo na dodate nule. Putanja kroz Viterbijev trellis koja odgovara početnoj poruci 101, na koju se dodaju još dve nule (10100), data je na sl. 3.3. Dekodovanje početne poruke se svodi na određivanje najverovatnije putanje kroz trellis, što se može izvršiti primenom Viterbijevog algoritma [65].



Slika 3.2: Ilustracija Viterbijevog trelisa (slika prilagođena iz [84]).



Slika 3.3: Ilustracija dekodovanja početne poruke na osnovu Viterbijevog trelisa (slika prilagođena iz [84]).

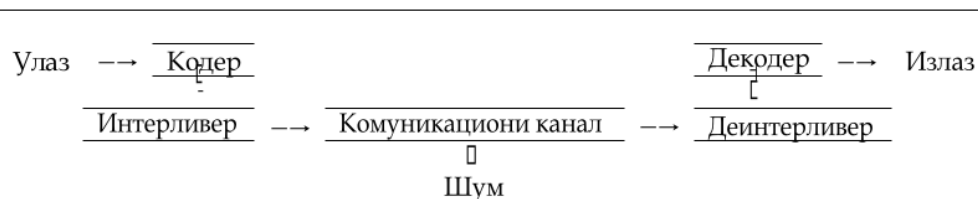
### 3.3.2 Interliveri

Gore smo razmotrili primer binarnog Hemingovog koda koji može da koriguje vektore koji sadrže samo jednu grešku. Međutim, u komunikacionom kanalu se mogu generisati i paketske greške. Njihova korekcija se vrši primenom interlivera, a model komunikacionog kanala je ilustrovan na sl. 3.4 (v. [84]).

Dve glavne grupe interlivera su: blokovski interliveri i konvolucioni interliveri. Razmotrićemo primere iz obe grupe.

#### 3.3.2.1 Primer blokovskog interlivera

Blokovski interliver podrazumeva generisanje bloka podataka dimenzija  $m \times n$ . U ovaj blok se učitava  $m$  kodnih reči,  $w_1, w_2, \dots, w_m$ , po vrstama, pri čemu svaka



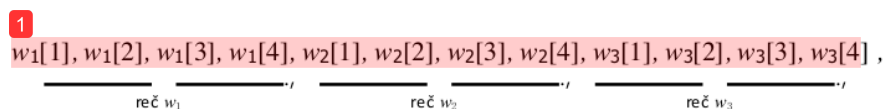
Slika 3.4: Ilustracija modela komunikacionog kanala sa zaštitnim koderima i interliverima.



Slika 3.5: Ilustracija blokovskog interlivera.

reč ima dužinu  $n$ . Učitani blok podataka se zatim po kolonama šalje kroz komunikacioni kanal sa šumom, kao što je ilustrovano na sl. 3.5. Preneseni podaci se inverzno preuzimaju kroz blok podataka, pre nego što se dekoduju [113].

Ako se u komunikacionom kanalu generišu paketske greške, blokovski interli- ver će ih rasporediti po kodnim rečima. Da bismo ilustrovali ovu tehniku, pre- postavimo da važi  $m = 3$  i  $n = 4$ , i posmatrajmo sekvencu bitova dužine  $mn = 12$ , koja je preuzeta sa izlaza koda:



Blok podataka je predstavljen sa tri kodne reči, od kojih svaka sadrži po četiri bita:

$$\begin{aligned} &w_1[1], w_1[2], w_1[3], w_1[4], \\ &w_2[1], w_2[2], w_2[3], w_2[4], \\ &w_3[1], w_3[2], w_3[3], w_3[4]. \end{aligned}$$

Nakon primene blokovskog interlivera, bitovi koji se šalju kroz komunikacioni

kanal reorganizovani su na sledeći način:

$$w_1[1], w_2[1], w_3[1], w_1[2], w_2[2], w_3[2], w_1[3], w_2[3], w_3[3], w_1[4], w_2[4], w_3[4] .$$

Pretpostavimo da je tokom transporta kroz komunikacioni kanal došlo do paketske greške, i da su bitovi koji pripadaju paketu označeni sa  $\mathbf{0}_i[j]$ :

$$w_1[1], w_2[1], w_3[1], w_1[2], \mathbf{0}_2[2], \mathbf{0}_3[2], \mathbf{0}_1[3], w_2[3], w_3[3], w_1[4], w_2[4], w_3[4] .$$

Nakon prenosa, podaci prolaze kroz inverzni blok podataka, čime se paketska greška raspoređuje po kodnim rečima, pre dekodovanja:

$$w_1[1], w_1[2], \mathbf{0}_1[3], w_1[4], w_2[1], \mathbf{0}_2[2], w_2[3], w_2[4], w_3[1], \mathbf{0}_3[2], w_3[3], w_3[4] .$$

### 3.3.2.2 Primer konvolucionog interlivera

Osnovna verzija konvolucionog interlivera sastoji se od niza pomeračkih registara, kao što je prikazano na sl. 3.6 (v. [113]). Nulti registar ne smešta bitove, već ih odmah prenosi. Svaki naredni registar može da smesi  $J$  bitova više od prethodnog, čime se implementiraju vremenski pomeraji pojedinačnih registara. Sa dolaskom svakog novog bita, komutator se prebacuje na sledeći registar u nizu (pomeranje je ciklično, tj. posle registra  $(N - 1)J$ , komutator prelazi na nulti registar). Tada se novi bit dodaje u tekući registar, dok se najstariji bit u registru šalje ka modulatoru. Deinterliver sprovodi inverzno preslikavanje, koje sledi iz obrnutog redosleda registara, uz uslov da komutatori interlivera i deinterlivera moraju da budu sinhronizovani [113].

Kao ilustracija, na sl. 3.7 su prikazana četiri stanja konvolucionog interlivera kad mu se saopšti ulaz:

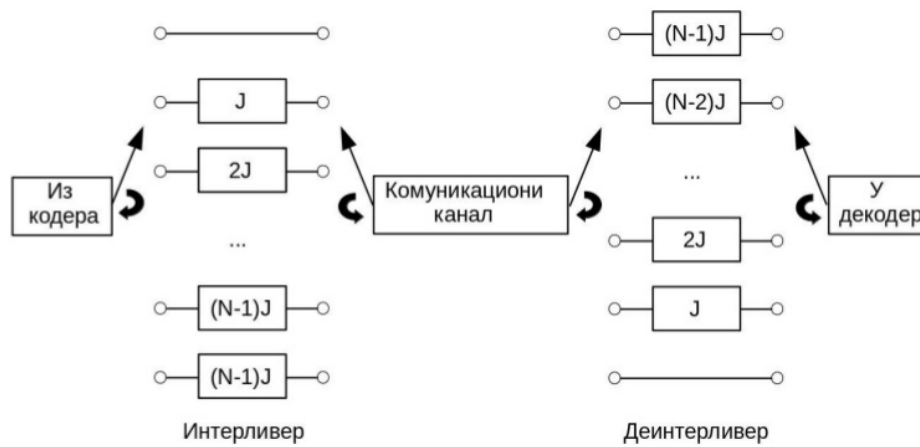
$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 . \quad (3.73)$$

$$\begin{array}{cccc} \text{—} & \text{—} & \text{—} & \text{—} \\ \text{sta rje A} & \text{sta rje B} & \text{sta rje V} & \text{sta rje G} \end{array}$$

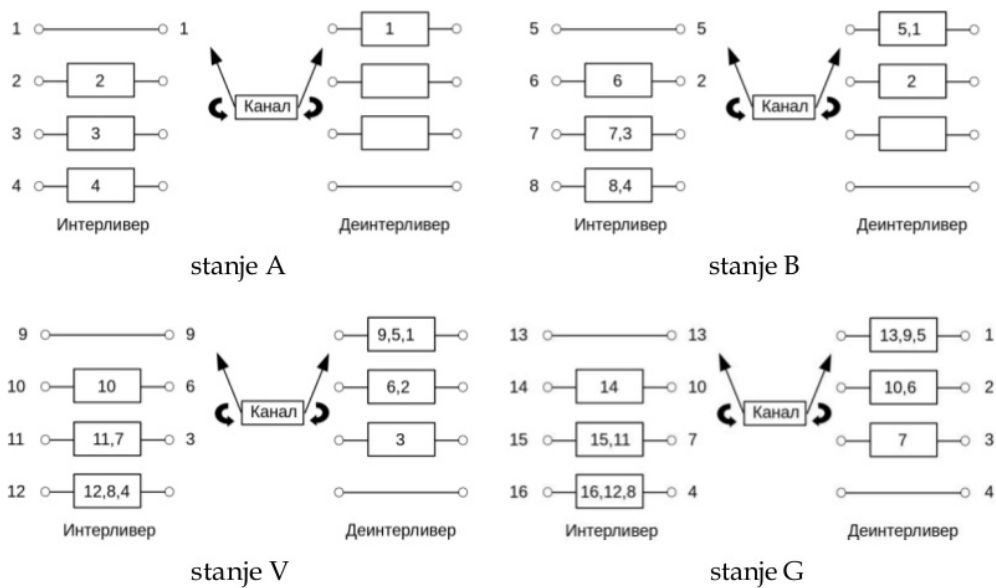
## 3.4 Neinvertibilne transformacije

### 3.4.1 Jednosmerne funkcije sa zamkom

Osnovna ideja kriptografije sa javnim ključevima bazirana je na jednosmernim funkcijama sa zamkom, tj., funkcijama čije se vrednosti za proizvoljni element



Slika 3.6: Konvolucioni interliver (slika prilagođena iz [113]).



Slika 3.7: Četiri stanja konvolucionog interlivera za ulaz (3.73), (slike prilagođene iz [113]).

iz domena mogu izračunati u polinomnom vremenu, dok je verovatnoća invertovanja jednosmerne funkcije bilo kojim algoritmom sa polinomnim vremenom izvršavanja „zanemarljiva” [47].

**Definicija 6.** Funkcija  $v : \mathbb{N} \rightarrow \mathbb{R}$  je zanemarljiva ako za svaku konstantnu vrednost  $c \geq 0$  postoji celi broj  $k_c$  takav da važi:

$$(\forall k \geq k_c) v(k) < k^{-c} . \quad (3.74)$$

**Definicija 7.** Funkcija  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  je jednosmerna ako su zadovoljeni sledeći uslovi:

- postoji algoritam sa polinomnim vremenom izvršavanja koji za datu vrednost  $x$  izračunava vrednost  $f(x)$ ,
- za bilo koji algoritam sa polinomnim vremenom izvršavanja  $A$  postoji zanemarljiva funkcija  $v_A$ , takva da za dovoljno veliku vrednost  $k$  važi:

$$P(f(z) = y : x \leftarrow \{0, 1\}^k; y \leftarrow f(x); z \leftarrow A(1^k, y)) \leq v_A(k) . \quad (3.75)$$

Jednosmerna funkcija sa zamkom  $f$  je jednosmerna funkcija za koju postoji tajna inverzna funkcija koja se izvršava u polinomnom vremenu.

**Definicija 8.** Jednosmerna funkcija sa zamkom je jednosmerna funkcija  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  za koju postoje polinom  $p$  i algoritam sa polinomnim vremenom izvršavanja  $I$  takvi da za svako  $k$  postoji  $t_k \in \{0, 1\}^*$  za koje važi  $|t_k| \leq p(k)$ , i za svako

$x \in \{0, 1\}^*$  postoji  $I(f(x), t_k) = y$  takvo da važi  $f(y) = f(x)$ .

Međutim, bez poznavanja tajne inverzne funkcije, verovatnoća invertovanja jednosmerne funkcije sa zamkom u polinomnom vremenu je i dalje zanemarljiva. Jedan primer jednosmerne funkcije sa zamkom je  $f(x, n) = x^2 \pmod{n}$ , gde je  $n = pq$  proizvod dva prosta broja, i  $x \in \mathbb{Z}_n^*$ . Invertovanje ove funkcije je lako ako i samo ako je faktorisanje broja  $n$  lako [91]. Poznatiji primer je jednosmerna funkcija sa zamkom već razmotrena u sekciji 3.1.1, koja se koristi u algoritmu RSA za kriptografiju sa javnim ključevima.

|    |    |    |    |
|----|----|----|----|
| 1  | 2  | 3  | 4  |
| 5  | 6  | 7  | 8  |
| 9  | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 |

(a)

|    |    |    |    |
|----|----|----|----|
| 1  | 2  | 3  | 4  |
| 5  | 6  | 7  | 8  |
| 9  | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 |

(b)

Slika 3.8: Ilustracija izobličenja mreže slike: (a) pre i (b) posle transformacije.

|    |    |    |    |
|----|----|----|----|
| 1  | 2  | 3  | 4  |
| 5  | 6  | 7  | 8  |
| 9  | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 |

(a)

|    |    |    |    |
|----|----|----|----|
| 5  | 10 | 14 | 2  |
| 8  | 1  | 4  | 7  |
| 11 | 9  | 12 | 15 |
| 3  | 13 | 16 | 6  |

(b)

Slika 3.9: Ilustracija permutacija blokova slike: (a) pre i (b) posle transformacije.

### 3.4.2 Transformacije digitalnih slika

U sekciji 3.4.1 smo razmotrili pojam jednosmernih funkcija sa zamkom, koji pruža osnov za opoziv biometrijskih šablona. Ovde ćemo razmotriti izabrane transformacije digitalnih slika.

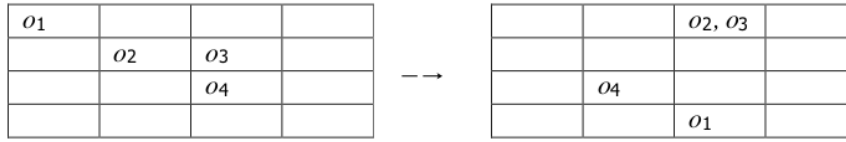
Transformacije slike mogu se sprovoditi u domenu signala (odmah posle akvizicije), ili u domenu izdvojenih obeležja (nakon obrade slike). Dve transformacije u domenu signala su izobličenje mreže slike (ilustrovano na sl. 3.8) i permutacija blokova slike (ilustrovano na sl. 3.9). U obe transformacije, slika se podeli na blokove, čiji su položaji i dimenzije određeni detektovanim obeležjima entiteta na slici [92].

Transformacija u domenu izdvojenih obeležja se bazira na slučajnom i više-strukom preslikavanju izdvojenih obeležja [92]. Bez gubitka opštosti, neka je dat skup biometrijskih obeležja izdvojenih sa slike:

$$F = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), \dots, (x_n, y_n, \theta_n)\} . \quad (3.76)$$

Za dati skup obeležja  $F$ , neinvertibilna transformacija  $f: F \rightarrow F^1$  generiše novi skup obeležja

$$F^1 = \{(X_1, Y_1, \Theta_1), (X_2, Y_2, \Theta_2), \dots, (X_n, Y_n, \Theta_n)\} , \quad (3.77)$$



Slika 3.10: Ilustracija neinvertibilnog preslikavanja izdvojenih obeležja (pri- lagodeno iz [92]).

takav da se iz njega ne može rekonstruisati početni skup  $F$ . Funkcija  $f: F \rightarrow F^I$  se može definisati tako da se na svaky klasu parametara u obeležju primenjuje zasebna neinvertibilna funkcija, na primer, polinom višeg reda (v. [92]):

$$f(\{(x_i, y_i, \theta_i) \mid 1 \leq i \leq n\}) = \{(g_1(x_i), g_2(y_i), g_3(\theta_i)) \mid 1 \leq i \leq n\}, \quad (3.78)$$

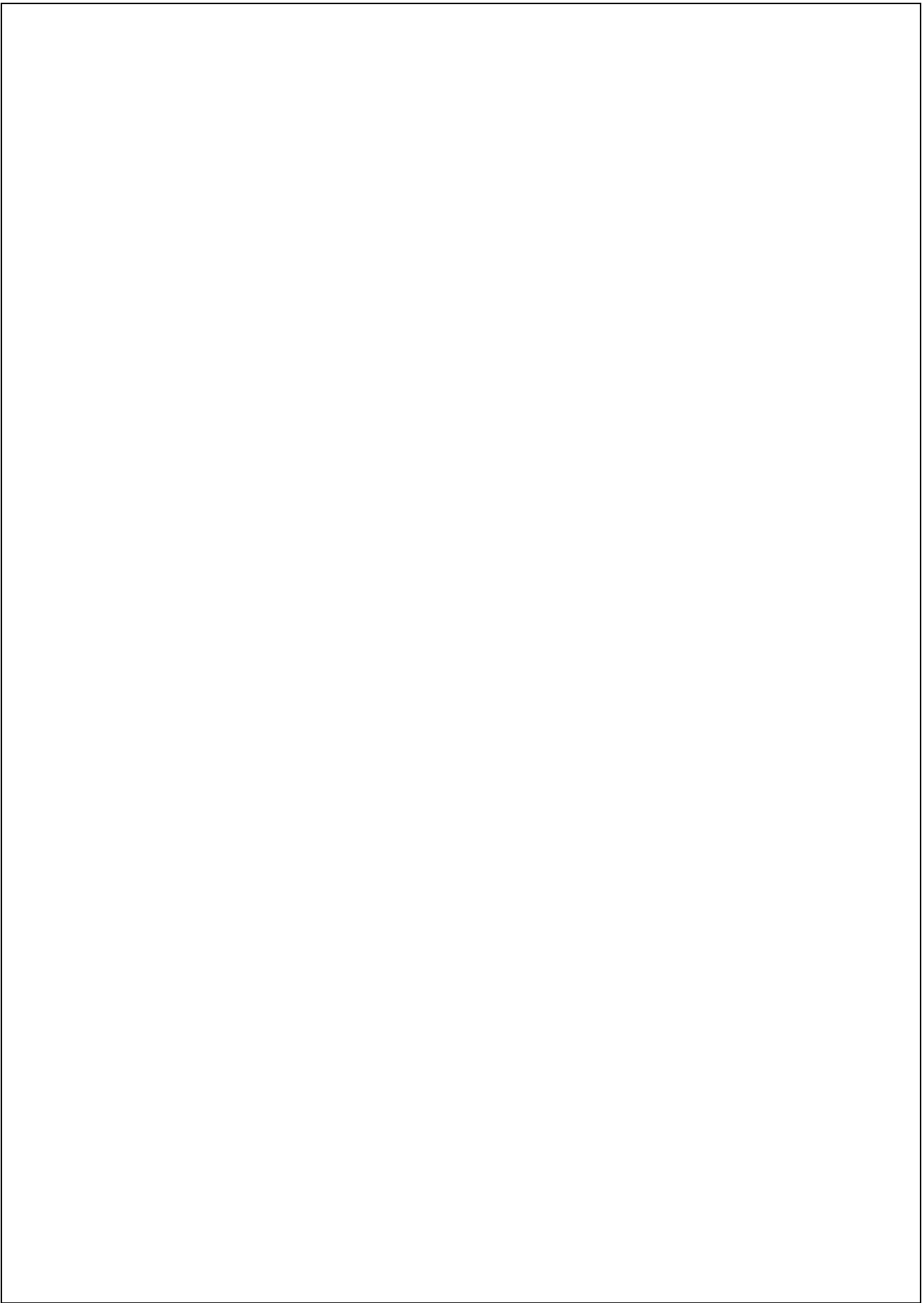
gde su:

$$g_1(x_i) = \sum_{j=0}^n a_j x_i^j = \alpha_1 \prod_{j=1}^n (x_i - b_j), \quad (3.79)$$

$$g_2(y_i) = \sum_{j=0}^n c_j y_i^j = \alpha_2 \prod_{j=1}^n (y_i - d_j), \quad (3.80)$$

$$g_3(\theta_i) = \sum_{j=0}^n e_j \theta_i^j = \alpha_3 \prod_{j=1}^n (\theta_i - h_j). \quad (3.81)$$

Neinvertibilnost ovakve transformacije zasniva se na činjenici da je moguće da više obeležja koja pripadaju različitim blokovima izvorne slike budu preslikana u isti blok transformisane slike, kao što je ilustrovano na slici 3.10.



## Glava 4

# Predlog radnog okvira i jedne implementacije

Ovo poglavlje zasnovano je na rešenju predloženom u radu [77], koji je proširena verzija istraživanja opisanog u [75].

Kao što je rečeno u 2. glavi, biometrijski sistemi projektovani na principu sigurnosti zasnovane na dizajnu su podložni napadima. Osam različitih tipova napada identifikovano je u [9, 57]. Da bi se sprečilo uspešno izvršavanje ovih napada, ceo sistem je podeljen na tri modula visokog nivoa, koji se nalaze na najmanje dva uređaja. Osim toga, sistem je zao van na opozivoj biometriji (neinvertibilnim transformacijama) i jakoj kriptografskoj zaštiti, koja uključuje generatore pseu- doslučajnih brojeva, jednosmerne heš funkcije i kriptografiju sa javnim ključem.

Predloženi modularni sistem se sastoji od sledećih komponenti:

- jednog ili više klijenata, odnosno uređaja koji preuzimaju biometrijske podatke korisnika, upravljaju pomoćnim podacima i generišu šifrovane biometrijske šablone;
- servera za proveru identiteta, koji generiše parove ključeva, odnosno upravlja ključevima i poredi opozive biometrijske šablone i
- skladišta podataka od poverenja (engl. *trusted storage*) u kome se čuvaju šifrovani opozivi šabloni.

Shodno tome da li se u skladište od poverenja nalazi na klijentu ili je reaktivno kao zasebni uređaj, odnosno baza podataka na izdvojenom serveru, mogu se

izdvojiti dve vrste sistema za proveru identiteta:

- sistemi sa distribuiranim skladištenjem i
- sistemi sa centralizovanim skladištenjem.

U slučaju da u sistemu postoji više klijenata, i da postoji potreba da korisnik koji je upisan na jednom klijentu ima mogućnost da proveri svoj identitet na drugom klijentu koji je povezan na isti server, skladište podataka od poverenja mora biti centralizovano. U suprotnom korisnik se mora upisati na svakom klijentu.

Osim kriptografske zaštite šablona, sistem treba da obezbedi i visok nivo zaštite privatosti, što znači da mora da zadovolji i sledeće zahteve:

- biometrijski šabloni moraju biti šifrovani, ili u najgorem slučaju opozivni, i to dok su uskladišteni, dok se prenose i dok se verifikuju (na primer, server za proveru identiteta ne sme imati pristup nezaštićenom biometrijskom šablonu);
- ni jedan klijent ne sme imati pristup privatim ključevima koji se nalaze na serveru za proveru identiteta, jer se, u slučaju da klijent ostvari pristup privatnim ključevima mogu kompromitovati šabloni;
- sistem mora biti otporan na napad zamene biometrijskog šablona (engl. *template substitution attack*) i sve napade niskog nivoa;
- uvođenje opozive biometrije i kriptografskih mera zaštite ne sme značajno da poveća računsku složenost i prostor potreban za skladištenje šablona;
- tačnost verifikacije ne sme da se smanji, odnosno ne smeju da se povećaju greške lažnog prihvatanja i lažnog odbijanja.

Drugim rečima, od sistema se zahteva da obezbedi zahteve koje ispunjava idealni biometrijski sistem [116].

Radni okvir modularnog sistema za proveru identiteta predstavljen u ovom delu rada zasnovan je na konvencionalnoj biometriji koja koristi operaciju ekskluzivno ILI, odnosno Hemingovo rastojanje kao meru sličnosti dva vektora obeležja koja su predstavljena kao nizovi bitova prilikom verifikacije korisnika. Hemingovo

rastojanje je odabrano kao metrika za verifikaciju zato što je pogodno za primenu u neinvertibilnoj transformaciji zvanom na jednokratnim beležnicama (engl. *one-time-pad*). Drugim rečima, neinvertibilna transformacija koja se koristi u predloženom rešenju je jednostavno računanje operacije ekskluzivno ILI nad šablonom i ključem za transformaciju iste dužine kao i originalni šablon. Ovaj način zaštite biometrijskih šablona štiti korisnika od krađe identiteta i pojednostavljuje fazu ponovnog upisa (engl. *re-enrollment*) u slučaju da postoji sumnja o kompromitovanju šablona ili ključa za transformaciju, zato što ne postoji potreba da korisnik ponovo priloži svoj biometrijski podatak.

Dve značajne karakteristike predloženog radnog okvira jesu da ispunjava uslove o čuvanju i prenosu šablona u šifrovanom obliku i verifikaciji u domenu opozivih šablona, kao i da uvođenje mera zaštite ne povećava značajno računsku složenost, dok se veličina prostora za skladištenje ne menja, zato što su opozivi šabloni iste veličine kao i originalni. Osim toga, radni okvir ne nameće potrebu konkretnih kriptografskih algoritama (generatora pseudoslučajnih nizova, heš funkcija i asimetričnih algoritama), dok modularnost sistema omogućava korisniku registrovanom na jednom klijentu proveriti svoj identitet na drugom koji je povezan na isti server (što je značajno lakše izvesti u sistemima sa centralizovanim skladištem).

## **4.1 Modularni sistemi za biometrijsku proveru identiteta sa distribuiranim skladištenjem šifrovanih opozivih šablona**

U sistemima sa distribuiranim skladištenjem šifrovani šabloni se čuvaju na klijentima. Potrebno je napomenuti da je u ovoj klasi sistema neophodno da na klijentu postoji skladište od poverenja otporno na forenzičke tehnike.

U ovom slučaju, tokom faze upisa sistem funkcioniše na sledeći način:

- Korisnik prilaže svoj numerički korisnički identitet i ključ za neinvertibilnu transformaciju  $K_i$  klijentu.

- Neka je  $H(x)$  jednosmerna heš funkcija (kao što je već rečeno, projektant sistema može odabrati onu koju smatra najsigurnijom),  $ID$  identitet korisnika a  $K_{priv}$  i  $K_{pub}$  privatni i javni ključ korisnika, respektivno. Klijent računa heš vrednost korisničkog identiteta i šalje tu vrednost serveru za proveru identiteta.
- Server generiše par ključeva ( $K_{priv}$ ,  $K_{pub}$ ), čuva privatni ključ i heš korisničkog identiteta ( $H(ID)$ ,  $K_{priv}$ ) i šalje javni ključ klijentu.
- Neka je  $\oplus$  operacija ekskluzivno ILI. Korisnik prilaže biometrijski uzorak klijentu. Klijent generiše binarni šablon  $b_0$ , a zatim i opozivi binarni šablon na sledeći način:  $b = K_t \oplus b_0$ .
- Neka je  $E$  operacija šifrovanja. Za šifrovanje se može iskoristiti bilo koji algoritam sa javnim ključem koji zadovoljava principe teorije informacija i jake kriptografske zaštite. Klijent na osnovu izvora slučajnosti generiše unutrašnji ključ  $s_0$  za generator pseudoslučajnih brojeva i šifrue ga javnim ključem:  $s_E = E(s_0, K_{pub})$ .
- Neka je  $PRNG$  oznaka za upotrebu generatora pseudoslučajnih brojeva koji zadovoljava statističke testove slučajnosti, odnosno obezbeđuje dovoljno entropije u generisanom nizu. Klijent generiše pseudoslučajni niz bitova  $s = PRNG(s_0)$  pomoću generatora i datog ključa.
- Klijent računa  $s \oplus b$ , čuva ( $H(ID)$ ,  $s_E$ ,  $s \oplus b$ ) u skladištu od poverenja i briše sve ostale podatke.

U fazi verifikacije korisnika, sistem funkcioniše na sledeći način:

- Korisnik prilaže svoj identitet ( $ID$ ) i ključ za jednosmernu transformaciju  $K_t$  klijentu.
- Klijent preuzima biometrijski podatak korisnika, generiše šablon  $b_0$  a zatim i opozivi šablon  $b^1 = K_t \oplus b_0$ .
- Klijent računa  $H(ID)$  i preuzima vrednosti  $s_E$  i  $(s \oplus b)$  iz odgovarajućeg sačuvanog zapisa ( $H(ID)$ ,  $s_E$ ,  $s \oplus b$ ).

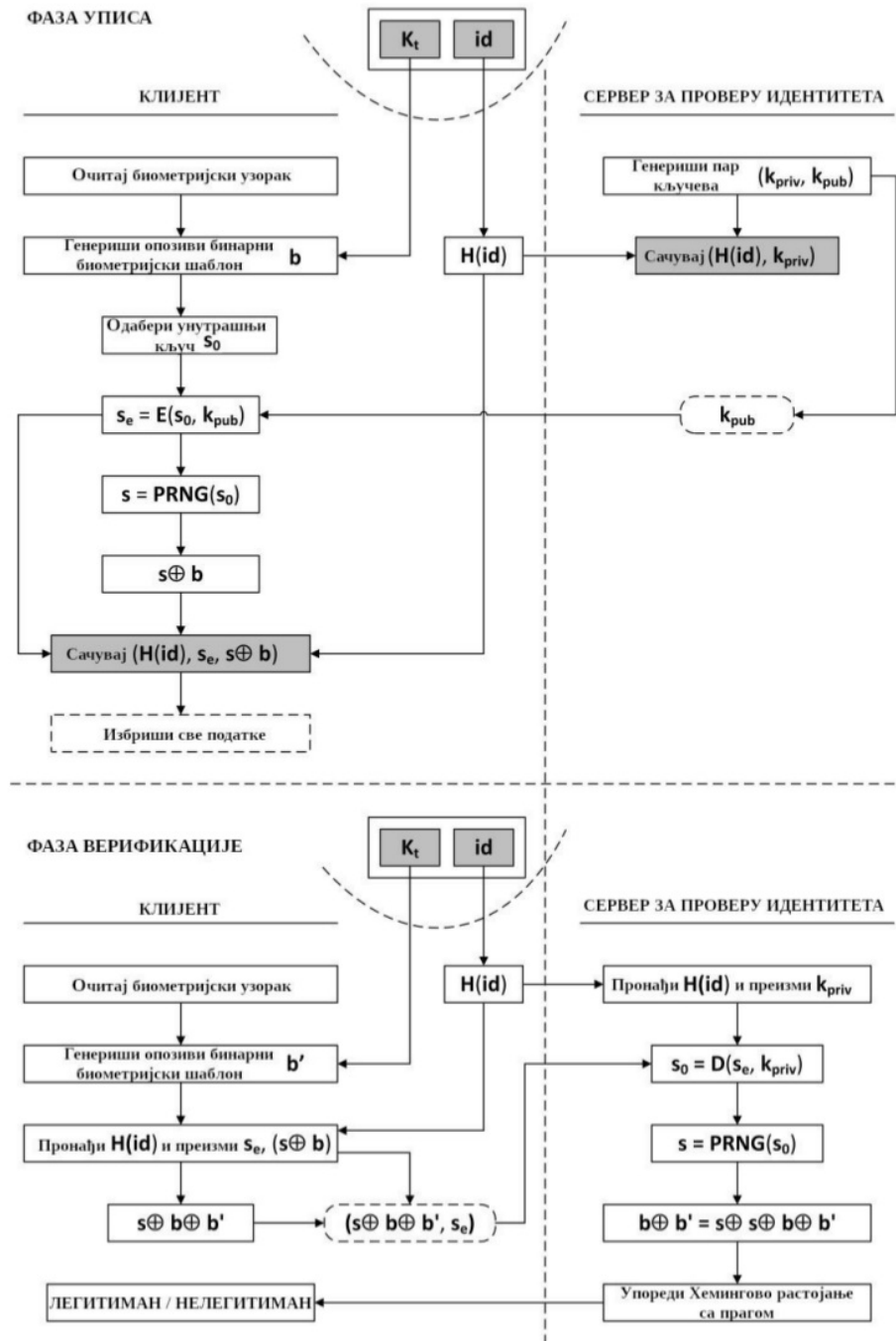
- Klijent računa  $s \oplus b \oplus b^l$  i šalje serveru zajedno sa šifrovanim unutrašnjim ključem  $s_E$ .
- Klijent šalje heš vrednost korisničkog identiteta serveru za proveru identiteta. Server preuzima privatni ključ iz odgovarajućeg zapisa  $(H(ID), K_{priv})$ .
- Neka je  $D$  operacija dešifrovanja u šifarskom sistemu sa javnim ključem. Server za proveru identiteta dešifruje vrednost  $s_E$  kako bi ostvario pristup unutrašnjem ključu  $s_0$  izvršavajući operaciju  $s_0 = D(s_E, K_{priv})$ .
- Server nakon toga generiše niz bitova  $s^l = PRNG(s_0)$ .
- Pošto je generator pseudoslučajnih brojeva deterministički i pošto se isti unutrašnji ključ koristi za generisanje nizova u fazi upisa i u fazi verifikacije, generisani nizovi  $s$  i  $s^l$  su identični, tj. važi  $s = s^l$ . Osim toga, identični ključ za neinvertibilnu transformaciju  $K_t$  se koristi u obe faze. Imajući to u vidu server računa  $s \oplus b \oplus s^l \oplus b^l = K_t \oplus b_0 \oplus K_t \oplus b_0^l = b_0 \oplus b_0^l$  i poredi Hemingovo rastojanje šablona  $b_0$  i  $b_0^l$  sa pragom poređenja. Na osnovu toga, server donosi odluku da li je korisnik legitiman ili ne i šalje je klijentu.

Faze upisa i verifikacije korisnika prikazane su na sl. 4.1.

Treba naglasiti da, iako je rezultat poređenja zapravo Hemingovo rastojanje između originalnih šablona, server izračunava to rastojanje na osnovu opozivih šablona generisanih pomoću ključa za jednosmernu transformaciju.

#### 4.1.1 Osvrt na sigurnost i ograničenja predloženog rešenja

Sledeći zaključci se mogu izneti o sigurnosti predloženog rešenja. Kao što je zahtevano, šabloni su šifrovani u svim fazama (prenos i skladištenje) dok se prilikom verifikacije porede opozivi šabloni. Osim toga, klijent ne može da pristupi privatnim ključevima na serveru. Sistem je zvan na dvo-faktorskoj proveru identiteta, što znači da neligitiman korisnik koji je došao u posed ključa za transformaciju ili pomoćnog podata (u ovom slučaju, šifrovani šablon) ne može da se predstavi kao legitiman korisnik. Ukoliko su šabloni koji se čuvaju na klijentu kompromitovani, ponovni upis se može izvršiti pomoću drugog ključa



Слика 4.1: Фазе уписа и верификације корисника у модуларном систему са дистрибуираним складиштењем. Изворни облик слике може се наћи у [75].

za transformaciju i drugog para ključeva za šifarski sistem sa javnim ključem. Napadi zamene šablona se ne mogu izvršiti zato što se javni ključ briše nakon faze upisa. Iako je javni ključ javni informacija, kao dodatna mera sigurnosti može se uvesti razmena javnog ključa upotrebom Difi-Helmanovog protokola, što sprečava napadača da presretne komunikaciju i pokuša da izvrši naknadno napad zamene šablona. Pošto napadač ne može da regeneriše niz bitova s na osnovu šifrovanog niza sE i javnog ključa (ukoliko prestretne oba podatka), sistem je takođe otporan i na sve napade na biometrijske kriptosisteme.

To znači da predloženo rešenje ispunjava sve uslove koje mora da ispuni idealni biometrijski sistem opisane u [116], s izuzetkom drugog uslova – umesto šifrovanih, porede se opozivi šabloni (uslovi idealnog biometrijskog kriptosistema preuzeti su iz [116]):

1. biometrijski šabloni se čuvaju i prenose isključivo u šifrovanom obliku;
2. prilikom autentifikacije biometrijski šabloni se ne dešifruju;
3. šifrovani šabloni za različite primene se ne mogu povezati;
4. server nikada ne dobija šablone koji nisu šifrovani;
5. klijent nema pristup privatnim ključevima;
6. šifrovani šablon se može zameniti novim bez ponovnog uzimanja biometrijskog podatka;
7. sistem je otporan na napad zamenom šablona;
8. šifrovani šablon je otporan na sve napade niskog nivoa;
9. sistem nije računski isuviše zahtevan i zadržava prihvatljiv nivo tačnosti.

Sledeći zaključci se mogu izneti o upotrebljivosti sistema i izvesnim ograničenjima. Sistem je upotrebljiv u scenariju jedan klijent – jedan server. Sistem je takođe upotrebljiv i u scenariju gde postoji više klijenata povezanih na jedan server ukoliko se od korisnika koji je upisan na jednom klijentu ne zahteva da proveriti svoj identitet na drugom. Ukoliko se to ipak zahteva, potrebno je da se na serveru sa ključem korisnika i korisničkim identitetom čuva i identitet klijenta. Osim

toga, korisnik bi morao da obavi ponovnu fazu upisa na svakom klijentu u slučaju da je ključ za neinvertibilnu transformaciju kompromitovan ili izgubljen.

Drugo ograničenje koje se odnosi na upotrebljivost sistema je upotreba biometrijske zasnovane na operaciji ekskluzivno ILI koja za sada nije primenljiva na sve biometrijske modalitete (za neke modalitete nisu prijavljeni algoritmi za izdavanje biometrijskih šablona u vidu binarnih nizova u relevantnoj literaturi). Međutim, treba uzeti u obzir da se svet koga mi percipiramo kao stvarnost može predstaviti kao beskonačni broj nula i jedinica.

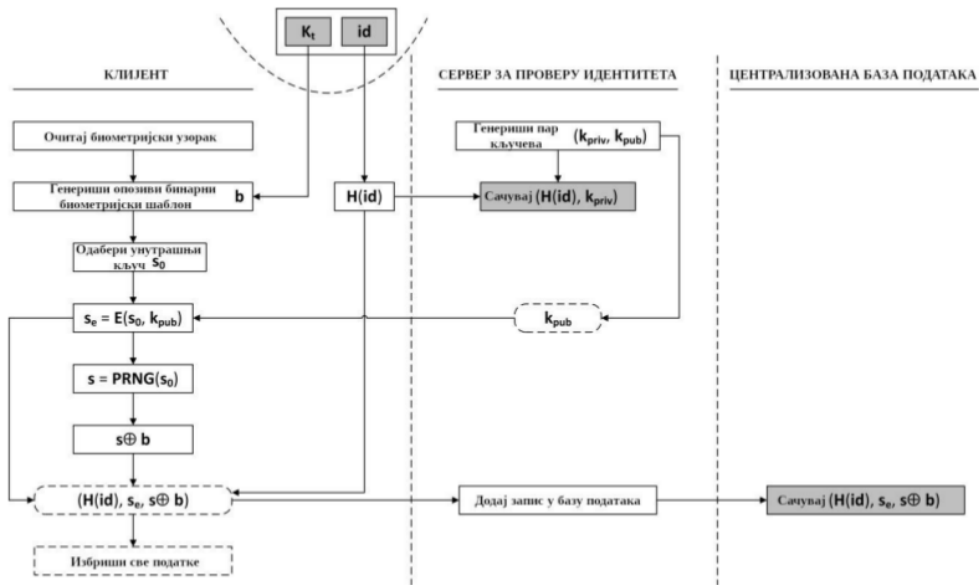
## **4.2 Modularni sistemi za biometrijsku proveru identiteta sa centralizovanim skladištenjem šifrovanih opozivih šablona**

U sistemima sa centralizovanim skladištenjem šifrovani šabloni se ne čuvaju na klijentima. Ova klasa sistema predstavlja proširenje sistema sa distribuiranim skladištenjem koje uklanja izvesna ograničenja vezana za scenario u kome je više klijenata povezano na jedan server za proveru identiteta.

U fazi upisa korisnika, sistem funkcioniše slično sistemima sa distribuiranim skladištenjem, uz dve bitne razlike (v. sl. 4.2):

- Vrednosti  $(H(ID), s_E, s \oplus b)$  se ne čuvaju na klijentu. Nakon računanja tih vrednosti, klijent šalje zahtev serveru za proveru identiteta da doda zapis koji sadrži te vrednosti u centralizovano skladište.
- Klijent u ovom slučaju nakon uspešno izvršene faze upisa ne briše samo javni ključ, nešifrovani unutrašnji ključ i originalni šablon, već briše sve podatke. To znači da se na klijentu ne čuva ni jedan podatak.

Veoma bitna činjenica je da se šifrovani unutrašnji ključ generatora pseudo-slučajnih brojeva nesme čuvati na serveru zato što se na serveru nalazi odgovarajući privatni ključ kojim bi napadač mogao izvršiti dešifrovanje unutrašnjeg ključa ukoliko ostvari pristup serveru. Drugim rečima, centralizovano skladište se mora realizovati u vidu baze podataka na posebnom serveru koji će komunicirati

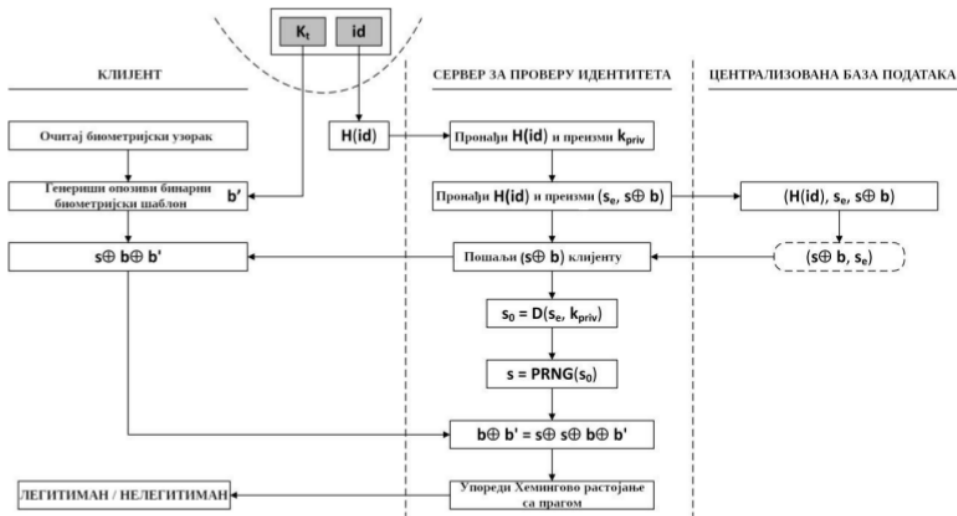


Slika 4.2: Faza upisa korisnika u modularnom sistemu sa centralizovanim skladištenjem. Izvorni oblik slike može se naći u [75].

rati sa serverom za proveru identiteta putem šifrovanog kanala. Konstrukcija šifrovanog kanala između ova dva uređaja i upravljanje ključevima nisu predmet ovog istraživanja.

U fazi verifikacije korisnika, sistem funkcioniše na sledeći način:

- Korisnik se identifikuje na klijentskoj strani i prilaže ključ  $K_t$ .
- Korisnik prilaže svoj biometrijski uzorak klijentu, klijent generiše šablon  $b_0$  i opozivi šablon  $b^l = K_t \oplus b_0^l$ .
- Klijent računa heš vrednost  $H(ID)$  i šalje je serveru za proveru identiteta.
- Server za proveru identiteta šalje upit centralizovanom skladištu i preuzima vrednosti  $s_e$  i  $(s \oplus b)$  na osnovu zapisa koji sadrži vrednosti  $(H(ID), s_e, s \oplus b)$  koje su sačuvane.
- Server šalje vrednost  $s \oplus b$  klijentu.
- Klijent izračunava  $s \oplus b \oplus b^l$  i šalje izračunatu vrednost serveru.
- Server za proveru identiteta preuzima javni ključ iz zapisa odgovarajućeg para  $(H(ID), K_{priv})$ .



Slika 4.3: Faza verifikacije korisnika u modularnom sistemu sa centralizovanim skladištenjem. Izvorni oblik slike može se naći u [75].

- Server dešifruje unutrašnji ključ generatora pseudoslučajnih brojeva  $s_0 = D(s_e, K_{priv})$  i generiše niz bitova:  $s = PRNG(s_0)$ . Ponovo se napominje da su zbog determinističke prirode generatora i upotrebe istog unutrašnjeg ključa generisani nizovi u fazi upisa i u fazi verifikacije identični.
- Server poredi Hemingovo rastojanje između dva opoziva šablona, odnosno iz- među niza bitova  $b$  i  $b'$  sa pragom poređenja. Na osnovu rezultata poređenja, odluka o tome da li je korisnik legitiman ili ne se šalje klijentu.

Faza verifikacije korisnika prikazana je na slici 4.3.

#### 4.2.1 Osvrt na sigurnost i ograničenja predloženog rešenja

Zaključci o sigurnosti predloženog rešenja sa centralizovanim skladištenjem su veoma slični kao i zaključci o sigurnosti sistema sa distribuiranim skladištenjem. Međutim, potrebno je naglasiti da je u ovom slučaju neophodno uvesti dodatne mere zaštite komunikacionog kanala između servera za proveru identiteta i centralizovanog skladišta u kom je smešten unutašnji ključ generatora i šifrovani opoziv šablon.

Osnovna razlika između sistema sa distribuiranim i centralizovanim skladištenjem odnosi se na ograničenja primene. U ovom slučaju, od korisnika se ne

zahteva da obave fazu upisa na svim klijentima na kojima žele da se verifikuju zato što se biometrijski šabloni čuvaju u centralizovanom skladištu. Drugim rečima, korisnik koji je registrovan na jednom klijentu može verifikovati svoj identitet na svim klijentima koji su povezani na isti autentifikacioni server. Ovakvi sistemi su primenljivi u velikom broju domena primene, počev od kontrole pristupa određenim prostorijama (za ulaz u svaku prostoriju potreban je jedan klijent) do kriptografske zaštite prijavljivanja korisnika na usluge mobilnog bankarstva pomoću biometrijskih podataka (što je izvodljivo i pomoću sistema sa distribuiranim skladištenjem u slučaju da korisnik usluga koristi samo jedan mobilni uređaj).

### **4.3 Jedna primena sistema sa distribuiranim skladištenjem za proveru identiteta korisnika usluga mobilnog bankarstva koja je zasnovana na biometriji dužice**

Mobilno bankarstvo je usluga koju klijentima pruža finansijska institucija koja pruža uslugu obavljanja finansijskih transakcija pomoću mobilnog uređaja (pametnog telefona ili tableta) i pratećeg softvera, koji najčešće obezbeđuje ista institucija. Uzevši to u obzir, može se zaključiti da je mobilno bankarstvo jedna od najosetljivijih upotreba u kontekstu sigurnosti koji obavlja tipičan korisnik pametnih mobilnih uređaja [82]. Iako mnoge finansijske institucije nude svoje usluge mobilnog bankarstva po principu „budite bez brige“ [69], za sada ne postoji rešenje koje korisnicima obezbeđuje potpunu sigurnost.

Postoji nekoliko bezbednosnih aspekata u vezi sa finansijskim transakcijama koje se vrše putem mobilnih uređaja na koje treba obratiti pažnju:

- fizička sigurnost mobilnog uređaja,
- sigurnost aplikacije koja se izvršava na uređaju,
- verifikacija identiteta korisnika i uređaja na serveru koji pruža usluge mobilnog bankarstva i

- šifrovanje podataka koji su preneti preko mreže, kao i podataka koji su sačuvani na samom uređaju koje korisnik želi kasnije da analizira.

U ovom delu rada biće ukratko opisan scenario koji se odnosi na proveru identiteta korisnika i mobilnog uređaja davaocu usluga. Danas se u mobilnom bankarstvu primenjuju različite metode provere identiteta, a sve imaju svoje prednosti i mane. Na primer, autentifikaciju zasnovanu na lozinkama je najlakše implementirati, ali su korisnici usluga mobilnog bankarstva u tom slučaju izloženi riziku od prevara ili krađa identiteta. Većina proizvođača mobilnih uređaja uočilo je potrebu za jakim sigurnosnim protivmerama i shodno tome proizvode nove uređaje sa ugrađenim biometrijskim skenerima. Shodno istraživanju koje je izvršio Gartner, preko 30% mobilnih uređaja proizvedenih 2014. godine trenutno koristi biometriju kao način provere identiteta. Danas je taj broj znatno veći. Finansijske institucije bi ovo trebale da prihvate kao jako dobru mogućnost da svojim klijentima obezbede viši nivo sigurnosti prilikom izvršavanja transakcija sa mobilnih uređaja, a ne kao prepreku prihvatanju biometrijskih metoda zaštite [115].

U ovom delu poglavlja opisan je jedan način primene predloženog modularnog sistema za biometrijsku proveru identiteta sa distribuiranim skladištenjem šifrovanih opozivnih šablona u mobilnom bankarstvu.

Server za proveru identiteta se nalazi u finansijskoj instituciji (drugim rečima, banka). Na serveru se nalaze ključevi za dešifrovanje, što znači da se šifrovani biometrijski šabloni nalaze na klijentu. Na ovaj način se sprečava da napadač koji je ostvario nelegitiman pristup serveru za proveru identiteta dešifruje šablone. Klijent je mobilni uređaj (pametni telefon ili tablet) opremljen skenerom dužice ili prednjom kamerom visokog kvaliteta (većina uređaja srednje klase ispunjava jedan od prethodno pomenuta dva zahteva). Dodatno, na klijentu mora postojati softver koji će izvršiti izdvajanje obeležja i neophodne kriptografske operacije – ovaj problem se može rešiti u vidu aplikacije koju će obezbediti finansijska ustanova. Ključ za neinvertibilnu transformaciju se smešta na sam uređaj – korisnik preuzima ključ kao izlaz generatora slučajnih ili pseudoslučajnih brojeva od finansijske ustanove. Treba napomenuti da ključ mora biti iste dužine kao i kod dužice kako bi klijent mogao izvršiti operaciju ekskluzivno ili odmah nakon izdvajanja obeležja. Korisniku treba dozvoliti da

sa drugog uparenog uređaja izbriše ključ i ostale relevantne podatke u slučaju da je uređaj ukraden ili u slučaju da postoji sumnja da su podaci kompromitovani. Takođe, finansijskoj instituciji treba omogućiti da obriše podatke sa svih ili odabranih klijenata u slučaju kompromitovanja servera za proveru identiteta.

Tokom faze upisa, predloženi sistem za proveru identiteta funkcioniše na sledeći način:

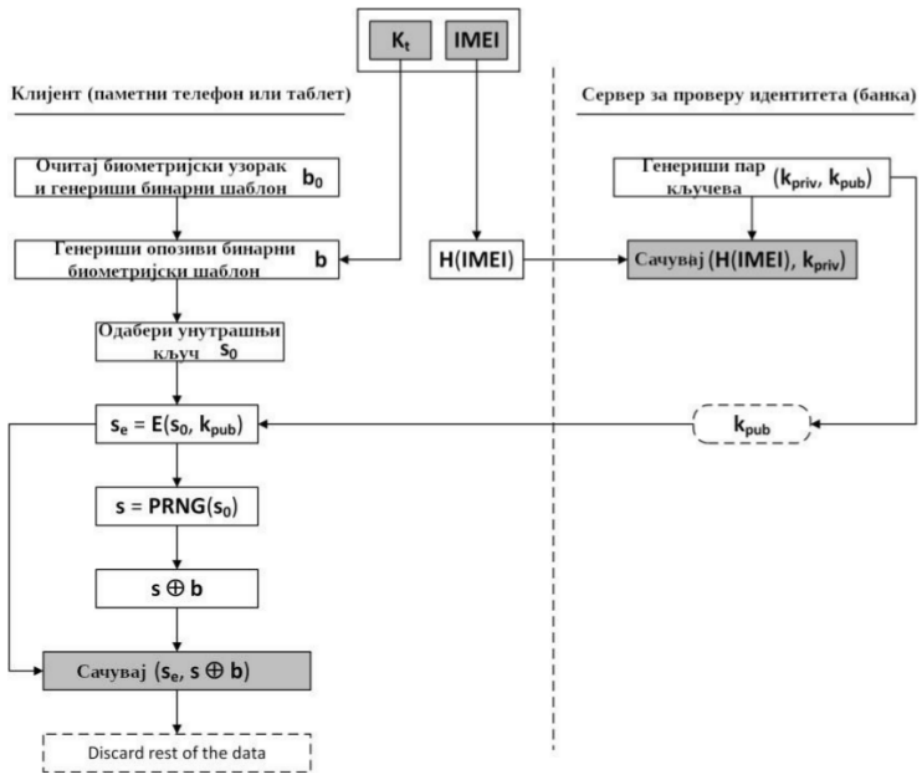
- Softver na klijenskoj strani računa heš vrednost *IMEI* (*International Mobile Equipment Identity*) i šalje je serveru za proveru identiteta. Umesto samog *IMEI* broja, šalje se heš vrednost kako bi se zaštitio identitet korisnika
  - izračunavanje heš vrednosti sprečava slanje otvorenog teksta sa klijenta ka serveru, kao i čuvanje osetljivih privatnih podataka korisnika na serveru.
- Server generiše par ključeva – privatni i javni ključ –  $(K_{priv}, K_{pub})$ , čuva privatni ključ u svojoj bazi podataka uparen sa heš vrednošću  $IMEI(H(IMEI), K_{priv})$  i šalje javni ključ mobilnom uređaju.
- Korisnik prilaže biometriju dužice mobilnom uređaju. Softver na klijentskoj strani generiše binarni šablon dužice  $b_0$  (na način koji je opisan u sekciji 5.1) i generiše opozivi biometrijski šablon  $b = K_i \oplus b_0$  koristeći ključ za jednosmernu transformaciju koji se nalazi na samom uređaju.
- Klijentski softver na osnovu izvora slučajnosti generiše unutrašnji ključ  $s_0$  i šifruje ga pomoću javnog ključa:  $s_E = E(s_0, K_{pub})$ .
- Softver zatim generiše niz bitova  $s = PRNG(s_0)$  koristeći generator pseudoslučajnih brojeva i unutrašnji ključ, računa vrednost  $s \oplus b$ , čuva uređeni par  $(s_E, s \oplus b)$  u skladištu od poverenja na uređaju i briše ostale podatke.

Faza upisa je prikazana na sl. 4.4.

Tokom faze verifikacije korisnika, sistem obavlja sledeće operacije (v. sl.

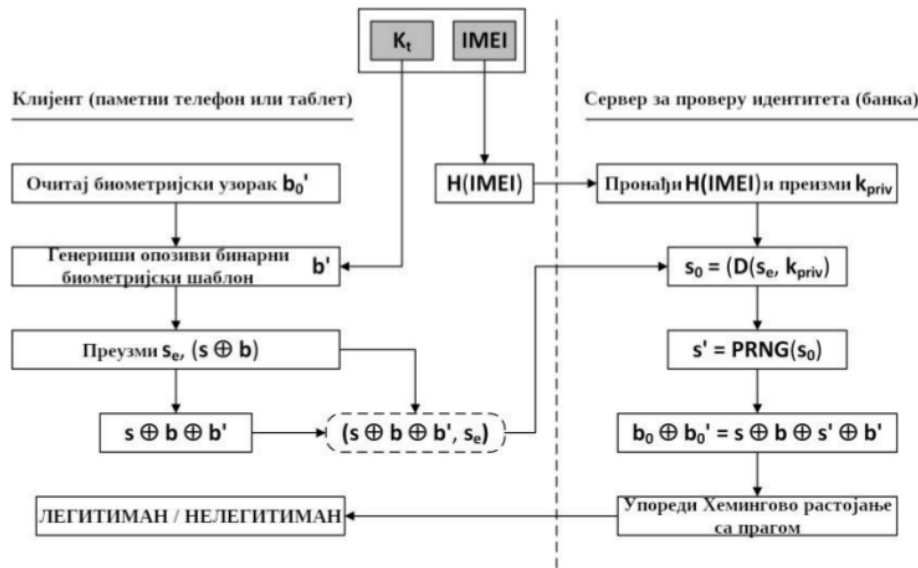
4.5):

- Na klijentskoj strani, aplikacija računa heš vrednost *IMEI* broja i šalje je serveru za proveru identiteta.



Slika 4.4: Faza upisa korisnika u sistemu za proveru identiteta korisnika usluga mobilnog bankarstva. Izvorni oblik slike može se naći u [77].

- Korisnik prilaže biometrijski uzorak senzoru na mobilnom uređaju. Softver na pametnom mobilnom uređaju generiše binarni šablon dužice  $b_0^l$  a potom i opozivi šablon  $b^l = K_t \oplus b_0^l$ .
- Softver preuzima vrednosti  $s_e$  i  $(s \oplus b)$  sa skladišta od poverenja na uređaju, računa  $s \oplus b \oplus b^l$  i šalje sa unutrašnjim ključem generatora  $s_e$  i heš vrednošću  $IMEI$  broja serveru za proveru identiteta.
- Server preuzima iz baze podataka sačuvan zapis  $(H(IMEI), K_{priv})$  koji odgovara heš vrednosti  $IMEI$  uređaja, dešifruje unutrašnji ključ generatora pomoću privatnog ključa  $s_0 = D(s_e, K_{priv})$  i generiše niz bitova:  $s^l = PRNG(s_0)$ .
- Kao što je rečeno u sekciji 4.1, zbog determinističke prirode generatora pseudoslučajnih brojeva, na osnovu identičnih unutrašnjih ključeva  $s$  i  $s^l$ , i



Slika 4.5: Faza verifikacije korisnika u sistemu za proveru identiteta korisnika usluga mobilnog bankarstva. Izvorni oblik slike može se naći u [77].

identričnog ključa  $K_t$  za jednosmernu transformaciju koji se koristi prilikom upisa i autentifikacije, server za proveru identiteta računa vrednost  $s \oplus b \oplus s' \oplus b' = b \oplus b' = K_t \oplus b_0 \oplus K_t \oplus b'_0 = b_0 \oplus b'_0$ .

- Kao i u slučaju radnog okvira, rezultat poređenja je Hemingovo rastojanje (specijalan slučaj Levenštajnovog rastojanja za nizove iste dužine) originalnih, neizmenjenih šablona, međutim server izračunava ovo rastojanje na osnovu opozivih šablona (drugim rečima, nema pristup originalnim šablonima ili ključu za jednosmernu transformaciju).

Pseudokodovi algoritama za faze upisa i verifikacije su navedeni na sl. 4.6 i 4.7.

### 4.3.1 Osvrt na sigurnost predložene implementacije

Što se tiče sigurnosti predloženog implementacije radnog okvira sa distribuiranim skladištenjem u mobilnom bankarstvu, zaključci koji se mogu izvući su identični zaključcima navedenim o sigurnosti radnog okvira na kome je rešenje predloženo. Drugim rečima, šabloni si šifrovani ili, u najgorem slučaju opozivi, tokom svih faza, a mobilni uređaj nema pristup privatnim ključevima na

---

 Algoritam za upis korisnika
 

---

ULAZ:  $b$  – biometrijski šablon,  
 $K_t$  – ključ za transformaciju  
 IZLAZ:  $s \oplus b$  – šifrovani opozivi biometrijski šablon,  
 $s_E$  – šifrovani unutrašnji ključ  
 Klijent:
 

1. pošalji ( $H(IMEI)$ )
2.  $b = K_t \oplus b_0$
3. odaberi slučajno ( $s_0$ );  $s = PRNG(s_0)$
4. preuzmi ( $K_{pub}$ );  $s_E = E(s_0, K_{pub})$
5. sačuvaj ( $s_E, s \oplus b$ )

 Server:
 

1. preuzmi ( $H(IMEI)$ )
2. generiši ( $K_{priv}, K_{pub}$ )
3. pošalji ( $K_{pub}$ ); sačuvaj ( $H(IMEI), K_{priv}$ )

---

Slika 4.6: Algoritam za upis korisnika.

---

 Algoritam za verifikaciju korisnika
 

---

ULAZ:  $b^l$  – biometrijski šablon,  
 $K_t$  – ključ za transformaciju  
 $t$  – prag poređenja  
 IZLAZ: odluka  
 Klijent:
 

1. pošalji ( $H(IMEI)$ )
2.  $b^l = K_t \oplus b_0^l$
3. pošalji ( $s \oplus b \oplus b^l, s_E$ )
4. preuzmi (odluka)

 Server:
 

1. preuzmi ( $H(IMEI), s \oplus b \oplus b^l, s_E$ )
2.  $s_0 = D(s_E, K_{priv})$ ;  $s^l = PRNG(s_0)$
3.  $b_0 \oplus b_0^l = s \oplus b \oplus s \oplus b^l$
4. ako je  $(b_0 \oplus b_0^l) < t$  onda je odluka = „legitiman“,  
inače odluka = „nelegitiman“
5. pošalji (odluka)

---

Slika 4.7: Algoritam za verifikaciju korisnika.

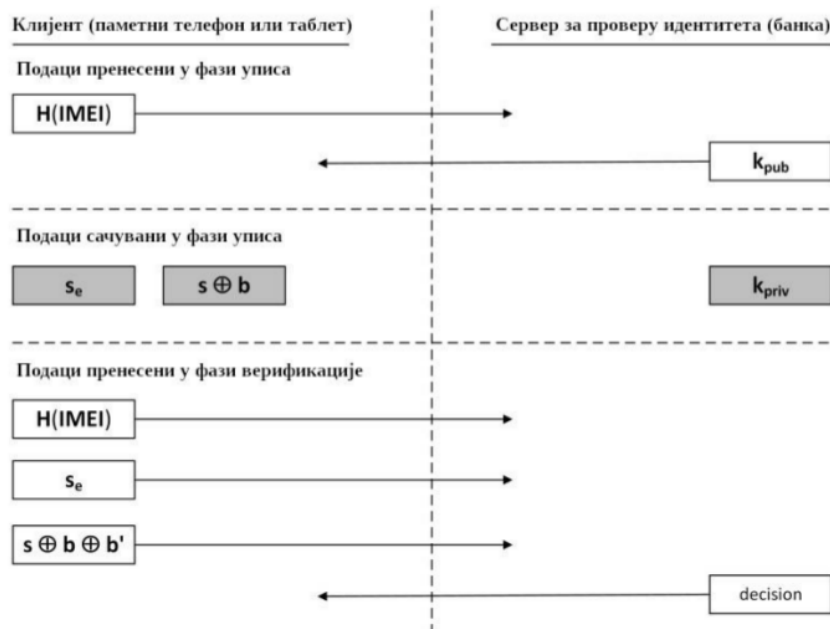
serveru finansijske ustanove. Server za proveru identiteta nema pristup ključevima koji se koriste za generisanje opozivih biometrijskih šablona i šifrovanim šablonima generisanim u fazi upisa.

U slučaju da je mobilni uređaj ukraden ili izgubljen, napadač se ne može predstaviti kao legitiman korisnik, zato što je sistem otporan na napade popisane u [57] kao i na napade usponom (engl. *hill-climbing attack* [3]), napade zasnovane na nedovoljnoj količini slučajnosti (engl. *non-randomness attack* [28]), napade ponovnom upotrebom (engl. *re-usability attack* [18]), napade slepom zamenom [109] i napade povezivanjem (engl. *linkage attack*) [27].

Iako se u sistem mogu dodati izabrani protokoli za razmenu ključeva, najsigurniji način za distribuciju ključa za jednosmernu transformaciju direktno preuzimanje ključa iz banke. Na ovaj način se ukida mogućnost lažiranja identiteta, koje za posledicu može imati uspešno izvršenje napada zasnovanih na tehnikama društvenog inženjeringa. I korisniku i finansijskoj instituciji je dozvoljeno udaljeno brisanje podataka (uključujući i ključeva) ukoliko je uređaj ukraden ili izgubljen.

U slučaju da se korisniku vrati izgubljeni uređaj, korisnik može preuzeti drugi ključ za neinvertibilnu transformaciju od finansijske institucije i izvršiti proceduru ponovnog upisa. Prilaganje biometrijskog uzorka u fazi ponovnog upisa je nepotrebno – rezultat izvršavanja operacije ekskluzivno ILI nad opozivim šablonom i ključem za transformaciju je originalni šablon. Međutim, zbog povećanja nivoa sigurnosti, predloženu fazu ponovnog upisa treba izvršiti na sledeći način: korisnik prilaže biometrijski uzorak, klijent generiše unutrašnji ključ generatora, a server novi par ključeva koji će se dalje koristiti za šifrovanje unutrašnjeg ključa.

Takođe potrebno je naglasiti da fizički pristup uređaju ne omogućava napadaču da preuzme ključ za jednosmernu transformaciju. U novijim modelima pametnih telefona sa biometrijskim senzorima za više modaliteta (na primer, otisak prsta, lice i dužica) na kojima se izvršava operativni sistem Android (verzija 6 ili novija) ugrađene su protiv-forenzičke tehnike koje sprečavaju očitavanje osetljivih podataka, čak i sa najnovijim forenzičkim alatima i uređajuma. Ova činjenica koja potiče iz domena digitalne forenzike omogućava da se sa visokim nivoom si-



Slika 4.8: Podaci koji se čuvaju i podaci koji se prenose. Izvorni oblik slike može se naći u [77].

gurnosti na uređaju čuvaju osetljive informacije, poput ključa za transformaciju.

Podaci koji se šalju preko mreže i podaci koji se čuvaju na mobilnom uređaju i serveru za proveru identiteta prikazani su na sl. 4.8. Sa slike se može videti da se sledeći podaci prenose preko mreže: javni ključ korisnika se prenosi samo jednom, u fazi upisa, dok se u fazi upisa i prilikom svake verifikacije prenose heš vrednost IMEI broja i vrednost dobijena primenom operacije ekskluzivno ILI nad opozivim šablonima i generisanim pseudoslučajnim nizom:  $s \oplus b \oplus b'$ . Na osnovu sl. 4.8 je nemoguće identifikovati slabosti predloženog rešenja koje bi omogućile napadaču da iz podataka koji se prenose preuzme bilo kakvu korisnu informaciju koja bi omogućila uspešno izvršenje napada.

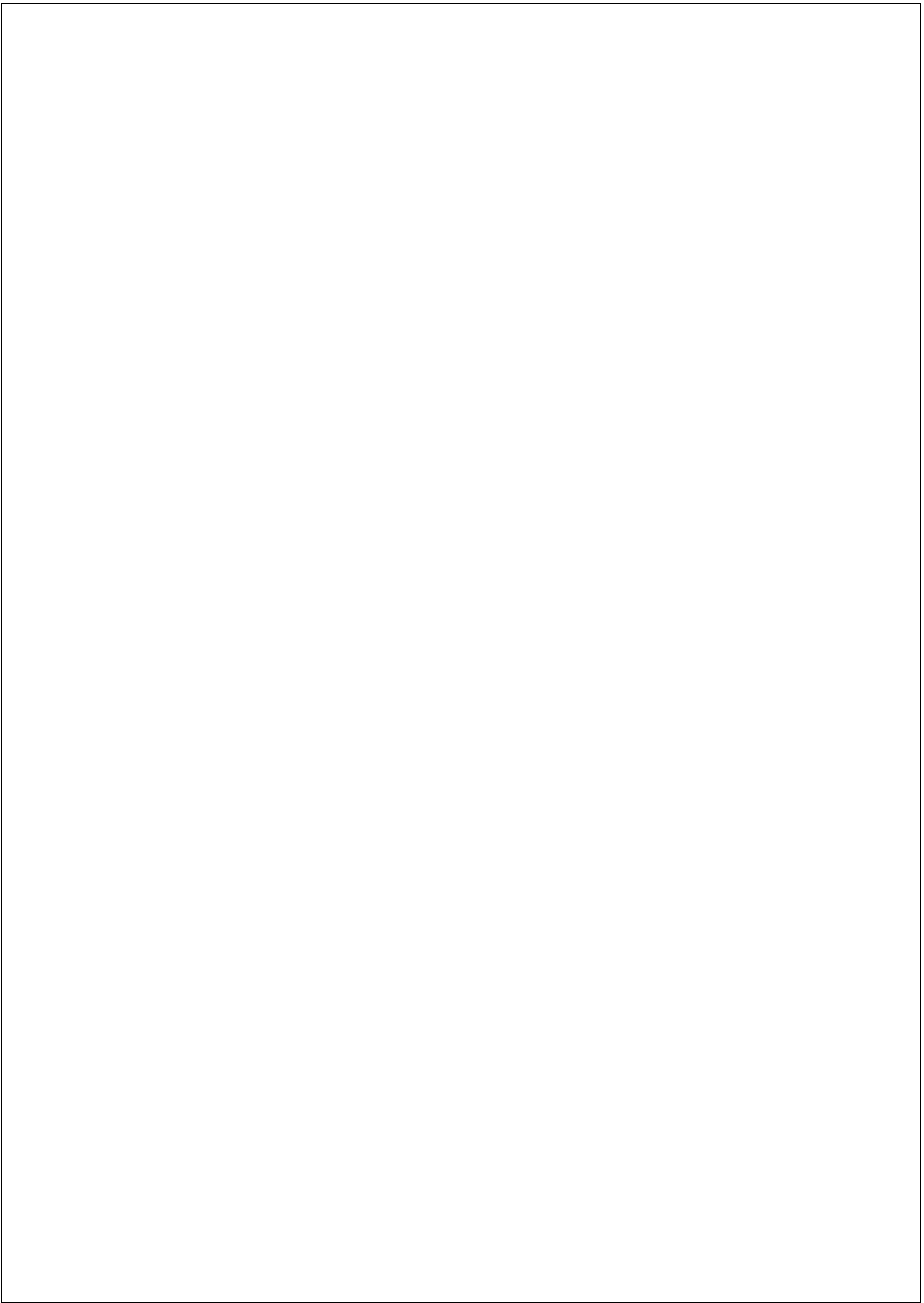
Jednu stvar je, međutim, jako bitno napomenuti – izbor lošeg generatora pseudoslučajnih nizova može dovesti do izvesnog curenja informacija kada se podatak  $s \oplus b \oplus b'$  prenosi sa klijenta ka serveru. Shodno tome, neophodno je koristiti kriptografski generator pseudoslučajnih brojeva koji generiše nizove bitova visoke entropije.

Takođe je potrebno naglasiti da sigurnost sistema zavisi i od sigurnosti pod-

sistema za verifikaciju dužice. Iako je teško izvršiti napad lažnim predstavljanjem, odnosno naterati sistem da lažnog korisnika prihvati kao legitimnog, grupa etičkih hakera je uspela to da izvede sa skenerom dužice na pametnom telefonu Samsung Galaxy S8. Interesanta činjenica je da je cena hardvera koji je korišćen za napad manja od cene pametnog uređaja [48].

Do sličnih scenarija može doći u slučaju da u uređaju nisu implementirani algoritmi za otkrivanje lažnih dužica. Na primer, podaci koji su preuzeti sa slika snimljenih pametnim telefonima sa kamerama visokog kvaliteta mogu se iskoristiti za generisanje lažnih slika dužice.

U literaturi je prijavljeno nekoliko pristupa za otkrivanje lažnih dužica. Jedan pristup otkrivanju kontaktnih sočiva sa lažnom šarom irisa zasnovan na konvolucionim neuronskim mrežama opisan je u [111]. Pristup koji diskriminiše dužicu korisnika od slike (engl. *liveness detection*) [112] zasnovan na detekciji pokreta u oku pre izdvajanja obeležja i poređenja sa uskladištenim kodom dužice značajno povećava sigurnost i pouzdanost sistema. Rešenje koje je pogodno za implementaciju u mobilnim uređajima predložili su Gagnaniello i dr. [49]. Ova brza i pouzdana metoda za detekciju lažnih šara dužice zasnovana je na tehnici opisivača lokalnih binarnih uzoraka (engl. *local binary pattern descriptor*) i klasifikaciji pomoću metode vektora oslonca sa linearnim jezgrom. Shodno navodima autora, tačnost detekcije lažnih dužica predloženom metodom je visoka, iako je metoda zasnovana na algoritmima koji nisu preterano složeni.



## Glava 5

# Analiza eksperimentalnih rezultata sa realističnim podacima

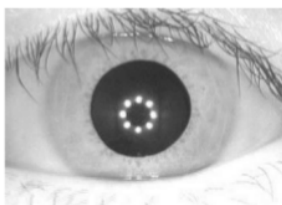
Ovo poglavlje je delom zasnovano na rezultatima objavljenim u [77]. Konkretno, iz rada su preuzeti rezultati koji se odnose na tačnost verifikacije osobe pomoću snimaka dužice generisanih pametnim telefonom.

Poglavlje je organizovano na sledeći način: najpre je ukratko opisana Daugman-ova metoda za izdvajanje obeležja dužice i verifikaciju identiteta osobe. Nakon toga su prijavljeni rezultati poređenja na realističnom skupu podataka, a potom su obavljene analize koje se odnose na šifrovane opozive biometrijske šablone i podatke koji se prenose preko mreže  $s \oplus b \oplus b^l$  (v. sekciju 4.3).

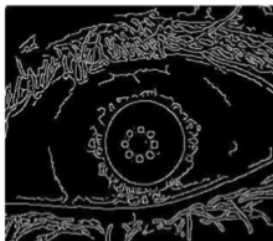
### 5.1 Prepoznavanje dužice

Dužica (v. sl. 5.1) je deo ljudskog oka koji se nalazi između rožnjače i sočiva, i okružuje zenicu. Jedna od njenih funkcija je da reguliše količinu svetla koje prolazi kroz zenicu, širenjem i skupljanjem dva mišića: *sphincter pupillae* i *dilator pupillae* [4].

Za proces autentifikacije, najvažniji aspekt dužice predstavlja njen šablon, tj. šare koje su jedinstvene za svakog čoveka (ove šare se razlikuju čak i na dva oka iste osobe). Prepoznavanje osobe na osnovu dužice se vrši kroz niz koraka. Na slici oka je potrebno detektovati dužicu, i izdvojiti odgovarajući segment uz uklanjanje šumova. Izdvojena dužica se normalizuje, tj. prevodi u format koji je



Slika 5.1: Slika oka, preuzeto iz CASIA (<http://biometrics.idealtest.org/>) baze podataka biometrijskih uzoraka.



Slika 5.2: Ilustracija rezultata primene Canny edge detektora na sl. 5.1, preuzeto iz CASIA (<http://biometrics.idealtest.org/>) baze podataka biometrijskih uzoraka.

prikladan za dalju obradu i predstavljanje jedinstvenim kodom. Kodovanje dužice se vrši pomoću filtera, pri čemu se izdvajaju obeležja koja će se koristiti za poređenje u postupku autentifikacije. U nastavku ćemo detaljnije razmotriti ovaj proces [74].

### 5.1.1 Segmentacija, normalizacija i kodovanje dužice

Segmentacija dužice predstavlja postupak izdvajanja segmenta slike ljudskog oka koji sadrži dužicu, tj. prostor između unutrašnje i spoljašnje ivice dužice. Očni kapci i trepavice koji na slici delimično pokrivaju dužicu predstavljaju šum koji je potrebno ukloniti.

Segmentacija počinje detektovanjem ivica i kontura na slici oka, za šta se uobičajeno koristi Canny edge detektor [25]. Ilustracija rezultata primene ovog detektora data je na sl. 5.2. Da bi se uklonio šum, prvo se primenjuju Gausovi filteri:

$$g(x) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2 + y^2}{2\sigma^2}}, \quad (5.1)$$

gde su  $x$  i  $y$  rastojanja od centra. Nakon uklanjanja šuma, izračunavaju se intenzi-

teti i smerovi gradijenata u pojedinačnim pikselima:

$$G = \sqrt{G_x^2 + G_y^2}, \quad (5.2)$$

i

$$\Theta = \text{atan2}(G_y, G_x), \quad (5.3)$$

gde  $G_x$  i  $G_y$  predstavljaju prve izvode u horizontalnom i vertikalnom smeru izračunate primenom Sobelovih filtera [32]:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \text{ i } \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}, \quad (5.4)$$

a ugao  $\Theta$  se zaokružuje na vrednosti iz redukovano skupa (na primer, umnošci ugla  $\frac{\pi}{4}$ ). Ivice detektovane u dosadašnjem postupku su široke i nepravilne, pa se na njih primenjuje tehnika nemaksimalnog suzbijanja ivica, kojom se detektovane ivice sužavaju do jasnog oblika.

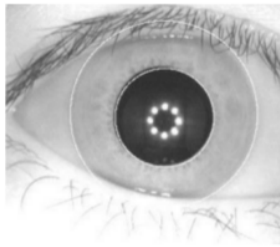
Ovako obrađena slika i dalje sadrži šum koji nije uklonjen primenom Gausovog filtera. Zato se prvo primenjuju dva praga prihvatljivosti, tj. gornji i donji pragovi propustljivosti, da bi se uklonile ivice koje se nalaze van zadatog opsega. Pored toga, dodatni šumovi se uklanjaju praćenjem povezanosti ivica. Ivice koje su slabije povezane sa ostalima se uklanjaju. Povezanost ivica se procenjuje tako što se za svaki piksel posmatra njegova neposredna okolina. Ako u njoj postoji jaka ivica, posmatrani piksel joj se pridružuje, a u suprotnom se odbacuje.

Da bi se detektovale ivice dužice, zenice i kapka, primenjuje se Hough transformacija [38]:

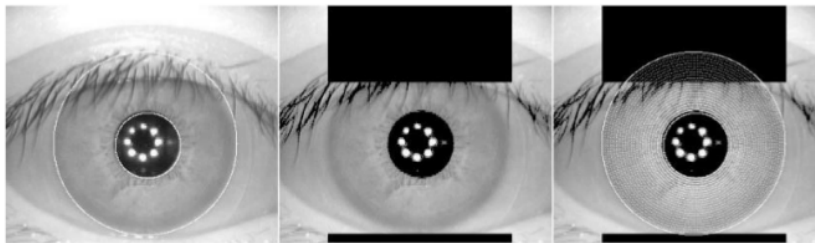
$$[-(x - h_i) \sin \theta_j + (y - k_j) \cos \theta_j]^2 = a_j [(x - h_i) \sin \theta_j + (y - k_j) \cos \theta_j], \quad (5.5)$$

gde  $a_j$  kontroliše zakrivljenost,  $(k_j, h_j)$  su vrhovi parabola, i  $\theta$  predstavlja ugao u odnosu na  $x$ -osu.

Da bi se detektovale spoljne ivice zenice i dužice, primenjuje se kružna transformacija na slici na kojoj je prethodno primenjen Canny edge detektor za izdvajanje vertikalnih ivica. Za detekciju i uklanjanje kapaka primenjuje se linijska transformacija na slici na kojoj je primenjen Canny edge detektor za izdvajanje



Slika 5.3: Primer detektovanja kružnica zenice i dužice na sl. 5.1, preuzeto iz CASIA (<http://biometrics.idealtest.org/>) baze podataka biometrijskih uzoraka.



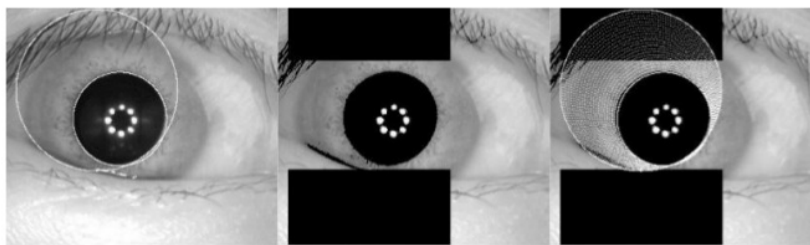
Slika 5.4: Primeri uspešne segmentacije dužice, preuzeto iz CASIA (<http://biometrics.idealtest.org/>) baze podataka biometrijskih uzoraka.

horizontalnih ivica. Primer detektovanja kružnica zenice i dužice dat je na sl. 5.3, a detektovana kružnica je predstavljena jednačinom:

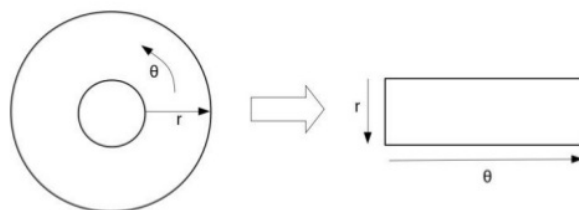
$$x^2 + y^2 - r^2 = 0 . \quad (5.6)$$

Praktični problemi ove transformacije su što je relativno spora, i što zahteva ručno postavljanje pragova propustljivosti, što može dovesti do efekata uklanjanja važnih ivica ili zadržavanja šuma. Takođe, ova transformacija je dosta spora jer ispituje piksel po piksel svake ivice kako bi našla odgovarajuće oblike. Prilikom segmentacije dužice, prvo se detektuje njena spoljna ivica, pa spoljna ivica zenice. Nakon toga se detektuju linije kapaka, da bi se uklonio šum koji oni uzrokuju. Šum koji uzrokuju trepavice se uklanja na osnovu praga propustljivosti. Primeri uspešne i neuspešne segmentacije dužice date su na sl. 5.4 i 5.5, respektivno.

Da bi se uporedile dužice različitih veličina, potrebno je izvršiti njihovu normalizaciju, što se vrši primenom Daugman-ovog modela Rubber Sheet [33]. Ovaj model transformiše sliku dužice iz kružne u pravougaonu formu, prevođenjem



Slika 5.5: Primeri neuspešne segmentacije dužice, , preuzeto iz CASIA (<http://biometrics.idealtest.org/>) baze podataka biometrijskih uzoraka.



Slika 5.6: Uobičajeno ilustriranje postupka normalizacije primenom Daugman-ovog modela Rubber Sheet.

iz Dekartovog koordinatnog sistema u polarni:

$$I(x(r, \theta), y(r, \theta)) = I(r, \theta) , \quad (5.7)$$

gde

su:

$$x(r, \theta) = (1 - r)x_p(\theta) + rx_i(\theta) , \quad (5.8)$$

$$y(r, \theta) = (1 - r)y_p(\theta) + ry_i(\theta) , \quad (5.9)$$

$I(x, y)$  je početna slika, a  $(x_p, y_p)$  i  $(x_i, y_i)$  koordinate centra kružnica koje odgovaraju spoljnim ivicama zenice i dužice. Uobičajena ilustracija postupka normalizacije data je na sl. 5.6.

Centri kružnice koje spoljne ivice dužice i zenice se u opštem slučaju ne polkapaju. Zato se posmatraju centar zenice i vektor pomeraja između centra zenice i centra dužice:

$$r^l = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha - \beta^2} , \quad (5.10)$$

gde

su:

$$\alpha = o_x^2 + o_y^2 , \quad (5.11)$$

$$\beta = \cos(\pi - \arctan(\frac{o_y}{o_x}) - \theta) . \quad (5.12)$$



Slika 5.7: Normalizacija dužice date na sl. 5.1.

$r_i$  je prečnik dužice,  $o_x$  i  $o_y$  određuju vektor pomeraja, a  $r^l$  je rastojanje između spoljnih ivica dužice i zenice.

U postupku normalizacije dužice generiše se i maska normalizacije, koja sadrži elemente koji predstavljaju šum (na primer kapci i trepavice) i služi za redukovanje šuma prilikom poređenja. Sl. 5.7 sadrži primer normalizovane dužice.

Jedan od zahteva za poređenje dužica je da šabloni dužica iste osobe budu slični, bez obzira na potencijalno različito osvetljenje tokom snimanja koje utiče na dimenzije zenice. Zato se u postupku kodovanja iz dužice izdvajaju ključna obeležja koja su jedinstvena za osobu, primenom 1D logaritamskog Gaborovog filtera:

$$G(x) = e^{-\frac{(\log \frac{f}{f_0})^2}{2(\log \frac{\sigma}{f_0})^2}}, \quad (5.13)$$

Normalizovana dužica se dekomponuje u više jednodimenzionalnih signala, od kojih se svaki koduje primenom Daugman-ove metode kodovanja pomoću 2D Gaborovih filtera:

$$h_{Re,Im} = \int_{\rho} \int_{\varphi} I(rho, \varphi) e^{-i\omega(\theta_0 - \varphi)} e^{-\frac{(r_0 - \rho)^2}{\alpha^2}} e^{-\frac{(\theta_0 - \varphi)^2}{\beta^2}} \rho d\rho d\varphi, \quad (5.14)$$

gde važi:

- $h_{Re,Im}$  je kompleksni bit čije realne i imaginarne komponente uzimaju vrednosti 0 ili 1.
- $sgn$  je znak 2D integrala,
- $I(rho, \varphi)$  je slika dužice u polarnom koordinatnom sistemu,
- $\alpha$  i  $\beta$  su veličine 2D talasa,
- $\omega$  je talasna frekvencija,



Slika 5.8: Kodovanje dužice date na sl. 5.1.



Slika 5.9: Maska šuma za dužicu datu na sl. 5.1.

- $(r_0, \theta_0)$  su polarne koordinate regiona dužica za koje je izračunato  $h_{Re,Im}$ .

Primenom ovog filtera generišu se po dva bita za svaki fazor.

Rezultat procesa kodovanja je binarni šablon dužice. Sl. 5.8 sadrži primer kodovane dužice, a sl. 5.9 primer maske šuma. Kod dužice i odgovarajuća maska šuma se zajedno primenjuju u postupku poređenja.

### 5.1.2 Klasifikacija na osnovu dužice

Za potrebe poređenja šablona dužice može se primeniti Hemingovo rastojanje, već razmatrano u glavi 3. U osnovnoj formi, Hemingovo rastojanje jednako je broju pozicija u kojima se kodovi razlikuju:

$$H(x, y) = \sum_{i=1}^n x_i \oplus y_i. \quad (5.15)$$

Međutim, zbog prisustva maski šuma, adekvatnije je primeniti modifikovano Hemingovo rastojanje:

$$H(X, Y) = \frac{1}{N} \sum_{k=1}^N X_{n_k} \oplus Y_{n_k}, \quad (5.16)$$

gde važi:

- $X_j$  i  $Y_j$  su dva kodovana šablona dužice,
- $X_n$  i  $Y_n$  su odgovarajuće maske šuma,
- $N$  je suma bitova koja odgovara svakom šablonu dužice.

U praksi se dešava da je slika dužice rotirana usled položaja glave. Rotacija dužice može znatno da poveća rastojanje između kodova dužice, čak i kad se radi o istoj osobi. Da bi se ovaj problem prevazišao, primenjuje se metoda pomeranja

šablona dužice na jednu i drugu stranu, koju je predložio Daugman. Pomeraji šablona odgovaraju rotaciji dužice. U postupku poređenja šablona  $X$  i  $Y$ , šablon  $Y$  se pomera nekoliko puta, simulirajući rotacije dužice, i generišući skup šablona

$$Y(Y) = \{Y, Y_1, \dots, Y_l\} . \quad (5.17)$$

Svaki šablon iz skupa  $Y$  se poredi sa šablonom  $X$ , a rastojanje između  $X$  i  $Y$  se računa kao:

$$H(X, Y) = \operatorname{argmin}_{Y_i \in Y(Y)} H(X, Y_i) . \quad (5.18)$$

Odluka o autentifikaciji dužice se donosi poređenjem vrednosti (5.18) sa zadatim pragom prihvatljivosti.

## 5.2 Performanse predloženog sistema

Performanse predloženog sistema zavise od nekoliko parametara poput kvaliteta same kamere ili skenera dužice, osvetljenja, kao i od parametara koje koristi algoritam za izdvajanje vektora obeležja. Jako je bitno naglasiti da u scenariju koji se odnosi na mobilno bankarstvo, kriptografska zaštita ili opoziva biometrija nemaju nikakav negativan uticaj na tačnost sistema – drugim rečima, primenjene mere zaštite ne povećavaju grešku koja se odnosi na broj lažno prihvaćenih ili lažno odbijenih korisnika.

Većina eksperimentalnih rezultata prijavljenih u relevantnoj literaturi zasnovana je na upotrebi CASIA-Iris baze podataka dužica. Međutim, kako bi se izveli pravi zaključci o tačnosti verifikacije dužice na osnovu pametnih telefona, odnosno mobilnih uređaja, za prikupljanje biometrijskih uzoraka i generisanje skupa podataka upotrebljena je prednja kamera Huawei P10 Lite telefona (telefon je relativno jeftin, što znači da sama kamera nije toliko kvalitetna poput onih koje su ugrađene u novijim i skupljim uređajima – drugim rečima, greške mogu samo da se umanje u slučaju upotrebe kvalitetnijih uređaja).

Slike dužica obrađene su u softverskom paketu MATLAB (verzija R2016a). Skup slika dužica korišćen u eksperimentu sastoji se od 210 uzoraka preuzetih od 10 subjekata, pri čemu su slike generisane na dnevnoj svetlosti (spolja) i sa različitim nivoima osvetljenja (unutra). Svaka slika dužice je predobrađena i

Tabela 5.1: Ispitivanje performansi sistema (slike dužice su generisane prednjom kamerom mobilnog telefona). Tabela preuzeta iz [77].

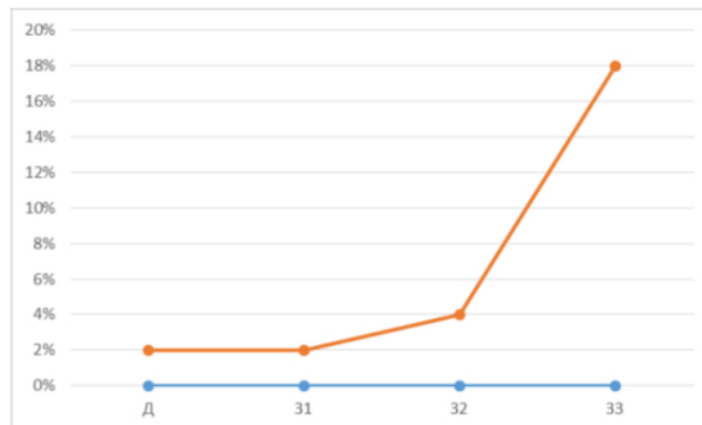
| Prag poređenja                                                     | Oznaka za osvetljenje | FAR | FRR |
|--------------------------------------------------------------------|-----------------------|-----|-----|
| Nizak prag poređenja (umanjuje grešku lažnog prihvatanja, tj. FAR) | D                     | 0%  | 2%  |
|                                                                    | Z <sub>1</sub>        | 0%  | 2%  |
|                                                                    | Z <sub>2</sub>        | 0%  | 4%  |
|                                                                    | Z <sub>3</sub>        | 0%  | 18% |
| Visok prag poređenja (umanjuje grešku lažnog odbijanja, tj. FRR)   | D                     | 0%  | 0%  |
|                                                                    | Z <sub>1</sub>        | 0%  | 0%  |
|                                                                    | Z <sub>2</sub>        | 2%  | 2%  |
|                                                                    | Z <sub>3</sub>        | 6%  | 4%  |

normalizovana u sliku rezolucije  $240 \times 20$  piksela, a nakon toga je primenjen jedno-dimenzionalni logaritamski Gaborov filter sa parametrom  $\sigma = 0,5$  i centralnom dužinom od 12 piksela, što generiše uzorak od 9600 bita. Ovi parametri su odabrani zato što je u istraživanjima prijavljenim u [1, 2] naglašeno da obezbeđuju visok nivo lokalne entropije i optimalno kodovanje. Jedna nasumično izabrana slika preuzeta spolja korišćena je za upis korisnika, dok su ostale korišćene za verifikaciju.

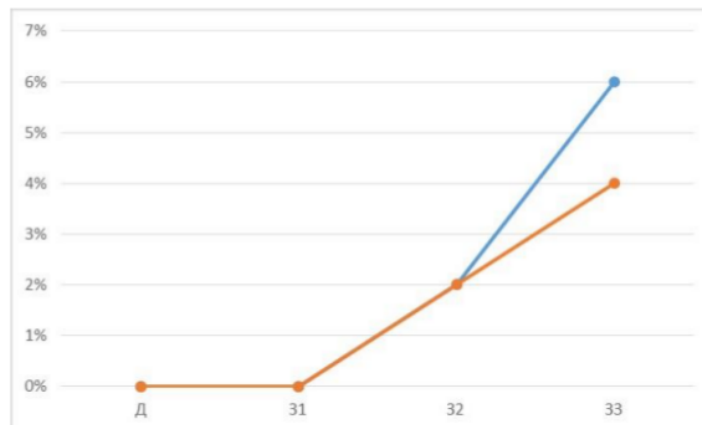
Rezultati eksperimenta su predstavljeni tabelom 5.1 i prikazani grafikonima na sl. 5.10 i 5.11. Oznake za osvetljenje na grafikonima prikazanim na sl. 5.10 i 5.11 su sledeće:

- D – snimak dužice na dnevnoj svetlosti,
- Z<sub>1</sub> - snimak dužice u zatvorenoj zastakljenoj prostoriji (osvetljenje normalnog nivoa),
- Z<sub>2</sub> - snimak dužice u zatvorenoj zastakljenoj prostoriji (osvetljenje srednjeg nivoa) i
- Z<sub>3</sub> - snimak dužice u zatvorenoj zastakljenoj prostoriji (osvetljenje relativno niskog nivoa).

Iako verifikacija korisnika sa niskim pragom poređenja za posledicu ima visoku učestalost lažno odbijenih korisnika, ovo ne treba smatrati lošom osobinom rešenja zato što je korisniku dozvoljeno da pokuša ponovo da se verifikuje. Problem nastaje u slučaju da je prag poređenja visok, zato što se nelegitimni korisnik



Slika 5.10: Performanse sistema sa niskim pragom poređenja (plavom bojom je označen FAR, crvenom FRR).



Slika 5.11: Performanse sistema sa visokim pragom poređenja (plavom bojom je označen FAR, crvenom FRR).

može prijaviti na sistem kao da je legitiman ako je Hemingovo rastojanje između dva niza bitova veće.

Ovo za posledicu ima pojavu većeg broja lažno prihvaćenih korisnika u slučaju snimanja u zatvorenoj prostoriji sa osvetljenjem osrednjeg nivoa (manje od 450 lumena, što odgovara jednoj kompaktnoj fluorescentnoj sijalici snage od 9 do 11 vati koja osvetljava sobu veličine 25 kvadratnih metara) ili slabim osvetljenjem (manje od 200 lumena, što odgovara sijalici snage od 3 do 5 vati koja osvetljava prostoriju iste veličine).

Drugim rečima, ako je prag poređenja visok, a osvetljenje neprikladno, sistem je

podložan neprikladnim odlukama, koje nisu prihvatljive u sistemu mobilnog ban- karstva. Van skupa neprikladnih odluka, sistem je stabilan i zahteva eventualno ponovno prijavljivanje korisnika na sistem. Drugim rečima, potrebno je da prag poređenja bude što niži kako bi se izbegle greške lažnog prihvatanja.

Prag poređenja zavisi od uređaja i kamere koji se koriste za snimanje slike du- žice, i treba da se postaviti na klijentskoj softverskoj strani (ukoliko unapred izračunati optimalni prag za konkretni klijentski uređaj postoji u zapisima ko- ji se odnose na uređaje prethodno korišćene u tu svrhu). Alternativno, ovlašćeni službenik finansijske institucije, prilikom prvog upisa može postaviti pret- hodno pomenuti parametar (ako unapred izračunati podaci ne postoje za konkretni model uređaja).

U okviru faze naknadnog upisa trebalo bi uzeti u obzir nekoliko dužica ko- risnika, skup dužica različitih subjekata i mogućnost određivanja praga pređenja koji uzima u obzir srednje i standardne devijacije unutar klasne i međuklasne distribucije.

Krajnja odluka prepoznavanja dužice određuje se raspodelom poređenja Hemin- govih rastojanja istih u odnosu na različite dužice [33]. Korisnicima se ne sme dozvoliti da samostalno postavljaju vrednost praga na mobilnim uređajima.

Još jedno pitanje na koje treba dati odgovor je prisustvo kontaktnih sočiva. Kontaktna sočiva, naročito sočiva ošarana teksturom dužice, mogu se upotrebiti kao lažna dužica, što predstavlja dodatni izazov sistemima za verifikaciju. Istraživanja koja se odnose na uticaj kontaktnih sočiva prilikom verifikacije dužice opisana su u [37, 145]. Yada i dr. [145] objavili su u svom istraživanju algoritam za smanjivanje uticaja sočiva, i dokazali da njihov pristup značajno povećava performanse verifikacije korisnika.

### 5.3 Ispitivanje slučajnosti

U ovom delu rada ispitaćemo slučajnost šifrovanog biometrijskog šablona i podataka koji se prenose preko mreže. Slučajnost šablona je bitna zato što se na osnovu nje može proceniti da li postoji bilo kakva korelacija šablona. Slučajnost podataka koji se prenose je od značaja kako napadač ne bi mogao da diskriminiše

šifrat šablona od slučajnog niza.

Prilikom ispitivanja slučajnosti nailazimo na dva problema. Matematički dokaz da su nizovi zaista slučajni ne postoji, a takođe ne postoji ni univerzalni test kojim bi se izmerio kvalitet niza bitova. Drugim rečima, slučajnost se ispituje nizom testova od kojih svaki služi za merenje neke od karakteristika niza. Definišu se vrednosti na osnovu kojih se određuje da li je dati rezultat zadovoljavajući i na osnovu serije testova utvrđuje da li niz poseduje svojstvo slučajnosti.

Postoji nekoliko skupova testova, od kojih su neki zastareli, poput FIPS 140-1 standarda koji sadrži:

- monobitni test,
- poker test,
- test sekvenci različitih dužina  $i$
- test dugačkih sekvenci.

Zbog toga se ovde primenjuje serija testova koju je definisao je NIST [106] koja se danas smatra *de-facto* standardom za ispitivanje slučajnosti. U ovoj seriji testova nalaze se izmenjeni testovi iz FIPS 140-1 standarda kao i neki novi, poput:

- Mauerovog univerzalnog statističkog testa,
- ispitivanja približne entropije  $i$
- testa zasnovanog na diskretnog Furijeovoj transformaciji.

Detalji o načinima testiranja, računanju vrednosti  $P$  u testovima i drugim parametrima opisani su u [83, 106].

Podaci koji se ispituju u ovom delu rada generisani su upotrebom RSA generatora pseudoslučajnih nizova, SHA-3 heš funkcije koja generiše otisak dužine 256 bita i RSA algoritma sa javnim ključem dužine 2048 bita.

Najpre je izvršena analiza slučajnosti šifrovanog opozivog šablona dužine 9600 bita. Pretpostavlja se da šablon poseduje osobine slučajnosti zato što je nastao kao rezultat izvršavanja operacije ekskluzivno ILI nad originalnim šablonom, ključem za transformaciju koji je slučajni niz i generisanim pseudoslučajnim nizom.

Rezultati testova su dati u popisu koji sledi (v. tabelu 3.2 u 3. glavi) i sumirani u tabeli 5.2.

1. Ispitivanje učestalosti u nizu (engl. *test for examining the frequency in the series*).  
Rezultat ovog testa je  $P = 0,817215$ . Pošto je  $P \geq 0,01$  smatra se da je osnovu ovog testa šablon pokazuje osobine slučajnosti.
2. Ispitivanje učestalosti u bloku (*the test for examining the frequency in the block*).  
Rezultat ovog testa je  $P = 0,962751$ . I na osnovu ovog testa šablon se može smatrati slučajnim nizom zato što je  $P \geq 0,01$ .
3. Ispitivanje uzastopnog ponavljanja istih bitova u nizu (engl. *the test for examining the successive repetition of the same bits in the series*).  
Kao rezultat ovog testa dobijena je vrednost  $P = 0,029180$ , što ukazuje na slučajnost zato što je  $P \geq 0,01$ .
4. Ispitivanje najdužeg uzastopnog ponavljanja jedinica u  $n$ -bitnim blokovima (engl. *the test for examining the longest consecutive repetition of units in  $n$ -bit blocks*).  
Dobijena vrednost  $P = 0,297120$  upućuje na to da je šablon na osnovu ovog testa slučajan zato što je  $P \geq 0,01$ .
5. Ispitivanje stanja binarne matrice (engl. *the test for examining the state of the binary matrix*). Rezultat testa je  $P = 0,689410$  – drugim rečima, niz je slučajan zato što je  $P \geq 0,01$ .
6. Test zasnovan na diskretnoj Furijeovoj transformaciji (engl. *the test for examining the discrete Fourier transform*). Vrednost  $P$  jednaka je 1, što ukazuje na činjenicu da je shodno rezultatima ovog testa šablon slučajan.
7. Ispitivanje nepreklapajućih uzoraka (engl. *the test for examining the non-overlapping samples*). Kao rezultat testa, dobijeno je  $P = 0,981392$ , što znači da je niz slučajan i na osnovu ovog testa.
8. Ispitivanje preklapajućih uzoraka (engl. *the test for examining the overlapping samples*). Ovaj test ne vraća kao rezultat konketnu  $P$  vrednost, već samo binarnu odluku – niz je zadovoljio (SUCCESS) ili nije zadovoljio (FAILURE)

Tabela 5.2: Sumarni rezultati ispitivanja slučajnosti šifrovanog opozivog šablona. Redni brojevi testova su usklađeni sa rednim brojevima u opisu.

| Test br. | $P$ -vrednost(i)                 | Ishod |
|----------|----------------------------------|-------|
| 1.       | $P = 0,817215$                   | Uspeh |
| 2.       | $P = 0,962751$                   | Uspeh |
| 3.       | $P = 0,029180$                   | Uspeh |
| 4.       | $P = 0,297120$                   | Uspeh |
| 5.       | $P = 0,689410$                   | Uspeh |
| 6.       | $P = 1$                          | Uspeh |
| 7.       | $P = 0,981392$                   | Uspeh |
| 8.       | –                                | Uspeh |
| 9.       | $P = 0,921749$                   | Uspeh |
| 10.      | $P_1 = 0,012001, P_2 = 0,937112$ | Uspeh |
| 11.      | $P = 0,839057$                   | Uspeh |
| 12.      | $P_1 = 0,991329, P_2 = 0,932901$ | Uspeh |

kriterijume testa. Pošto je kao rezultat testa dobijena odluka SUCCESS, smatra se da je šifrovani šablon uspešno prošao i ovaj test.

9. Ispitivanje linearne složenosti (engl. *the test for examining the linear complexity*).

Rezultat testa je  $P = 0,921749$ . Pošto je  $P \geq 0,01$ , šablon je zadovoljio uslove zadate ovim testom.

10. Ispitivanje učestalosti svih mogućih preklapanja  $n$ -bitnih podnizova u celom nizu (engl. *the serial test*). Rezultati testa su vrednosti  $P_1 = 0,012001$  i  $P_2 = 0,937112$ .

Šablon se na osnovu rezultata može smatrati slučajnim, pošto su  $P_1 \geq 0,01$  i  $P_2 \geq 0,01$ .

11. Ispitivanje približne entropije (engl. *the test for examining the approximate entropy*). kao rezultat u ovom slučaju vraća vrednost  $P = 0,839057$  što znači da je niz na osnovu dobijene  $P$  vrednosti slučajan.

12. Ispitivanje zbirova slučajnih podnizova (engl. *the test for examining the random summations*). Kao rezultat dobija se  $P_1 = 0,991329$  i  $P_2 = 0,932901$ . Uzevši u obzir da je  $P_1 \geq 0,01$  i  $P_2 \geq 0,01$ , niz je zadovoljio kriterijume ovog testa.

Pošto je niz zadovoljio kriterijume svih nametnutih testova, možemo smatrati da poseduje dovoljno visok nivo slučajnosti, čime je pretpostavka potvrđena.

Kao i za ispitivanje slučajnosti šablona, slučajnost podataka koji se prenose preko mreže ispituje se NIST skupom testova. Neophodno je ispitati slučajnost

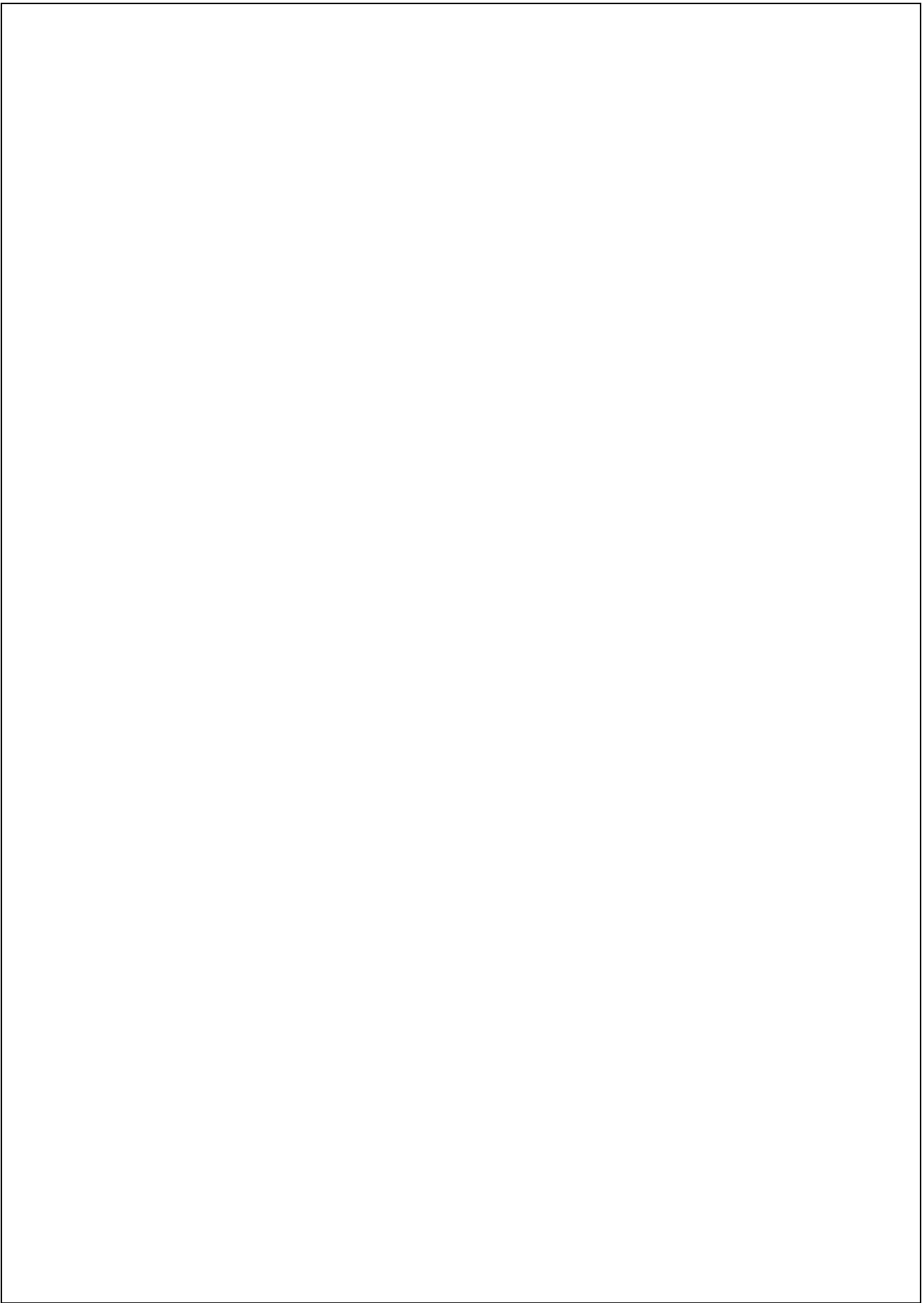
Tabela 5.3: Sumarni rezultati ispitivanja slučajnosti podataka koji se prenose preko mreže. Redni brojevi testova su usklađeni sa rednim brojevima u tabeli 5.2.

| Test br. | $P$ -vrednost(i)                 | Ishod |
|----------|----------------------------------|-------|
| 1.       | $P = 0,836312$                   | Uspeh |
| 2.       | $P = 0,971007$                   | Uspeh |
| 3.       | $P = 0,031070$                   | Uspeh |
| 4.       | $P = 0,312240$                   | Uspeh |
| 5.       | $P = 0,691870$                   | Uspeh |
| 6.       | $P = 1$                          | Uspeh |
| 7.       | $P = 0,990124$                   | Uspeh |
| 8.       | –                                | Uspeh |
| 9.       | $P = 0,930273$                   | Uspeh |
| 10.      | $P_1 = 0,013105, P_2 = 0,939076$ | Uspeh |
| 11.      | $P = 0,841131$                   | Uspeh |
| 12.      | $P_1 = 0,992517 P_2 = 0,954713$  | Uspeh |

ovih podataka kako bi se onemogućio napad razlikovanjem. Podatak koji se šalje generisan je izvršavanjem operacije ekskluzivno ILI nad pseudoslučajnim nizom i dva opoziva šablona koji pripadaju istom korisniku. Treba napomenuti da slučajnost ovih podataka zavisi od entropije generisanog slučajnog niza i ključeva za jednosmernu transformaciju. Pošto je upotrebljen jak kriptografski generator, a ključevi za transformaciju su generisani kao slučajni nizovi, može se pretpostaviti da će i ovi podaci zadovoljiti kriterijume koji nameću testovi slučajnosti.

Rezultati ispitivanja slučajnosti podataka koji se prenose preko mreže dati su u tabeli 5.3. Pošto su zadovoljeni kriterijumi svih nametnutih testova, može se smatrati je nivo slučajnosti visoka čime je prethodno pomenuta pretpostavka potvrđena.

Ovim je pokazano da osetljivi podaci koji su smešteni na telefonu (konkretno, šifrovani šablono) i podaci koje napadač može presresti poseduju dovoljnu količinu slučajnosti, u slučaju da se koriste jake kriptografske mere zaštite, što znači da je napadaču onemogućeno da izvrši korelaciju šablona ili da izvrši napad razlikovanjem podatka od slučajnog niza.



## Glava 6

### Kritička analiza i zaključak

U odnosu na veliki broj modela i načina primene kriptografske zaštite biometrijskih sistema za proveru identiteta prijavljenih u literaturi, model predložen u ovom radu ne umanjuje tačnost klasifikacije subjekata i ne zahteva dodatne procesorske resurse, kao ni prostor za skladištenje.

Nedostatak modela prijavljenih u relevantnoj literaturi je povećanje učestalosti lažno prihvaćenih i lažno odbijenih korisnika koja potiče od sistema zaštite zasnovanih na šifarskim sistemima – bilo da su u pitanju sistemi sa simetričnim ili javnim ključem ili homomorfni šifarski sistemi – kao i od algoritama upotrebljenih u neinvertibilnim transformacijama.

Predloženim modularnim pristupom kriptografskoj zaštiti biometrijskih šablona uspešno su rešeni problemi koji se odnose na procesorsku zahtevnost i umanj enje tačnosti verifikacije korisnika, kao i uslovi koje treba da zadovolji idealni biometrijski sistem. U odnosu na predložena rešenja objavljena u relevantnoj literaturi, predloženi sistem za proveru identiteta korisnika je nezavisan od kriptografskih mera zaštite koje su primenjene, a osim toga i od podsistema za izdvajanje obeležja koja moraju biti binarizovana. Nezavisnost predloženog rešenja od konkretnih kriptografskih algoritama, kao i od algoritama za izdvajanje binarnih neopozivih biometrijskih šablona može se smatrati izazovom za projektante novih kriptografskih rešenja ili algoritama za izdvajanje binarizovanih obeležja.

Nedostatak predloženog modela je zavisnost od biometrijskih šablona generisanih na osnovu izvršenja operacije ekskluzivno ILI. Za sada je u relevantnoj

literaturi prijavljeno nekoliko modaliteta koji mogu biti binarizovani - počev od koda dužice – a naknadno su prijavljene šeme za generisanje binarnih biometrijskih šablona otisaka prstiju, i uslovno rečeno, drugi modaliteti za koje je prijavljena tačnost verifikacije neupotrebljiva u predloženom modelu. Modaliteti poput glasa i sličnih ponašajnih biometrijskih uzoraka za sada nisu binarizovani.

Predložena implementacija modela koja koristi jake kriptografske algoritme postiže jako visoku tačnost provere identiteta korisnika, kao i nisku učestalost lažno prihvaćenih i odbijenih korisnika.

Na osnovu eksperimenata izvršenih na realističnom skupu podataka, može se zaključiti da je sistem upotrebljiv u većini domenima primene, poput mobilnog bankarstva.

## 6.1 Zaključak i rezime doprinosa

Istraživanje predstavljeno u ovom radu potvrdilo je postavljene istraživačke hipoteze:

**Hipoteza 3.** Trenutna rešenja za zaštitu biometrijskih šablona ne obezbeđuju dovoljno visok nivo sigurnosti šablona i privatnosti korisnika.

**Hipoteza 4.** Razvojem sopstvenog biometrijskog sistema u kom biometrijski šabloni ostaju šifrovani ili u najgorem slučaju opozivi tokom svih faza njihove primene (skladištenje, prenos i verifikacija) obezbeđuje se upotrebljivost predloženog pristupa u realnim domenima primene.

Pored toga, pokazano je da opoziva biometrija ne mora da naruši tačnost verifikacije korisnika, što je uslovno neizvodljivo za modalitete koji nisu zasnovani na XOR biometriji.

Važno je istaći da primenjena metoda kriptografske zaštite nije umanjila tačnost verifikacije korisnika, što do sada nije prijavljeno u relevantnoj literaturi. U uslovima normalnog osvetljenja pri akviziciji slike, greška lažnog prihvatanja konvergira nuli.

Cilj je postignut kroz empirijsko istraživanje, koje je potvrdilo da se upotrebom predloženog rešenja značajno smanjuje broj lažno odbijenih korisnika, dok se uz upotrebu ispravno odabranog praga može smanjiti i broj lažno prihvaćenih korisnika.

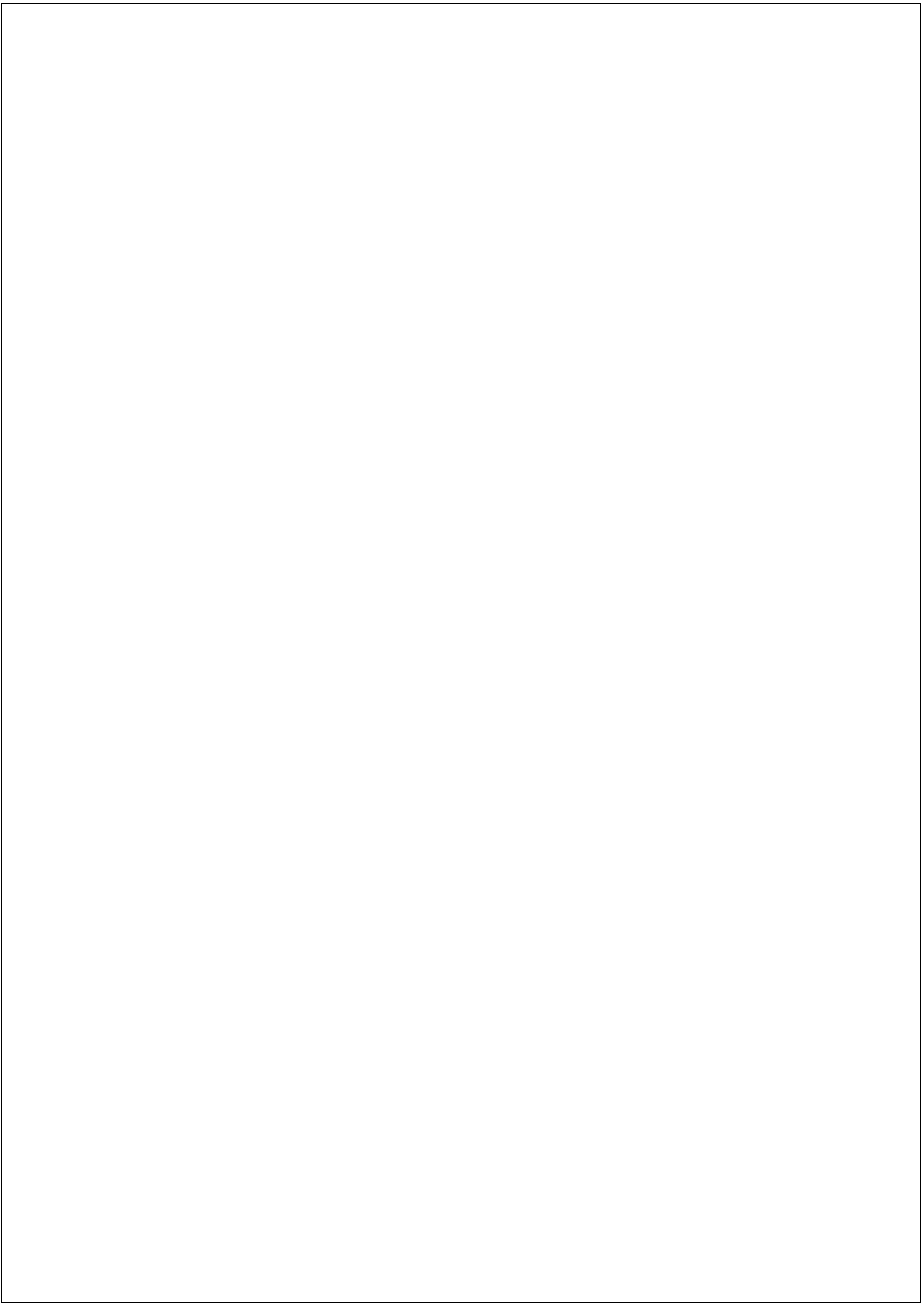
Potvrđeni doprinosi ovog rada su sledeći:

- predložena je nova metoda za proveru identiteta korisnika pomoću šifrovanih opozivih biometrijskih šablona;
- predloženo rešenje je modularno u pogledu primenjenih kriptografskih mehanizama, i nezavisno od toga da li se primenjuju šifarski algoritmi sa simetričnim ili javnim ključem;
- predložena je izmenjena šema za verifikaciju dužice u sistemu – šema ne koristi kodove za korekciju grešaka, a verifikacija korisnika se ne zasniva na poređenju heš kodnih reči koje nose minimalnu količinu informacije o biometrijskom uzorku;
- predloženi sistem za proveru identiteta je pogodan za primenu u scenariju mobilnog bankarstva, zato što je greška lažnog prihvatanja zanemarljiva, a veličina biometrijskog uzorka je prikladna za smeštanje na mobilnim uređajima (za razliku od biometrijskih uzoraka dobijenih homomorfnim šifrovanjem, koji su znatno veći);
- predloženo rešenje je primenljivo u tehnologiji oblaka zbog relativno niske procesorske zahtevnosti, za razliku od drugih šifarskih algoritama koji su znatno zahtevniji po pitanju procesorskih resursa.

## 6.2 Smernice za dalja istraživanja

Potencijalna dalja istraživanja u ovoj oblasti uključuju:

- istraživanja vezana za binarizovanje drugih biometrijskih modaliteta, poput lica ili glasa;
- formiranje sistema za verifikaciju koja nije zasnovana na upotrebi operacije ekskluzivno ILI.



# Bibliografija

- [1] S. Adamović, M. Milosavljević: Information Analysis of Iris Biometrics for the Needs of Cryptology Key Extraction. Serbian Journal of Electrical Engineering, Vol.10, No. 1, pp. 1–12, 2013.
- [2] S. Adamović, M. Milosavljević, M. Veinović, M. Šarac, A. Jevremović: Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. IET Biometrics, Vol. 6, No. 2, pp. 89–96, 2017.
- [3] A. Adler: Vulnerabilities in Biometric Encryption Systems. LNCS, Springer 3546, pp. 1100–1109, 2005.
- [4] M.W. Ansari, A. Nadeem: The Eyeball: Some Basic Concepts. In: Atlas of Ocular Anatomy. Springer, Cham, pp. 11–27, 2016.
- [5] L. Ballard, S. Kamara, F. Monrose, M. Reiter: On the requirements of biometric key generators, Technical Report TR-JHU-SPARBKMR-090707, Submitted and available as JHU Department of Computer Science Technical Report 2007.
- [6] L. Ballard, S. Kamara, M.K. Reiter: The practical subtleties of biometric key generation. SS'08: Proc of the 17th Conf on Security symposium, pp. 61–74, 2008.
- [7] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti et al.: A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates, in Proc. 4th IEEE Int. Conf. Biometrics: Theory Applications and Systems (BTAS), pp. 1–7, 2010.
- [8] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti et al.: Privacy-preserving fingercode authentication, in Proc. 12th ACM Workshop on Multimedia and Security, pp. 231–240 2010.

- [9] B. Biggio: Adversarial Pattern Classification, Doctoral dissertation, University of Cagliari, Cagliari, Italy, 2010.
- [10] M. Blanton, P. Gasti: Secure and efficient protocols for iris and fingerprint identification, in Proc. Computer Security (ESORICS 2011), pp. 190–209, 2011.
- [11] L. Blum, M. Blum, M. Shub: A simple unpredictable pseudo-random number generator, SIAM J. Computing, 15(2), pp. 364–383, 1986.
- [12] M. Blum, S. Micali: How to generate cryptographically strong sequences of pseudo-random bits. SIAM J. Computing, 13(4), pp. 850–863, 1984.
- [13] A. Bodo: Method for producing a digital signature with aid of a biometric feature. German patent DE 4243908 A1, 1994.
- [14] T. Boulton: Robust distance measures for face-recognition supporting revocable biometric tokens. FGR '06: Proc. of the 7th Int Conf on Automatic Face and Gesture Recognition, pp. 560–566, 2006.
- [15] T. Boulton, W. Scheirer, R. Woodworth: Revocable fingerprint biotokens: Accuracy and security analysis. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1, pp. 1–8, 2007.
- [16] T. Boulton, W. Scheirer: Bio-cryptographic protocols with bipartite biotokens. Proc of the IEEE Biometric Symposium, BSYM '08, pp. 9–16. 150, 2008.
- [17] T. Boulton, W. Scheirer: Bipartite biotokens: definition, implementation, and analysis. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09) 5558, pp. 775–785, LNCS: 2009.
- [18] X. Boyen: Reusable cryptographic fuzzy extractors. In Proc. 11th ACM Conf. CCS, Washington, DC, pp. 82–91, 2004.
- [19] J. Bringer, H. Chabanne, D. Pointcheval, Q. Tang: Extended private information retrieval and its application in biometrics authentications, in Proc. Cryptology and Network Security, Singapore, pp. 175–193, 2007.

- [20] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, S. Zimmer: An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication, LNCS 4586, pp. 96–106, 2007.
- [21] J. Bringer, H. Chabanne: An authentication protocol with encrypted biometric data. In International Conference on Cryptology in Africa, pp. 109–124, Springer Berlin Heidelberg, 2008.
- [22] J. Bringer, H. Chabanne, B. Kindarji: Anonymous identification with cancelable biometrics. Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09, pp. 494–499, 2009.
- [23] J. Bringer, H. Chabanne, A. Patey: Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends, IEEE Signal Processing Mag., vol. 30, no. 2, pp. 42–52, 2013.
- [24] P. Campisi: Security and Privacy in Biometrics. New York: Springer, 2013.
- [25] J. Canny: A Computational Approach To Edge Detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, 8(6), pp. 679–698, 1986.
- [26] A. Cavoukian, A. Stoianov: Biometric encryption. Encyclopedia of Biometrics Springer, 2009.
- [27] A. Cavoukian, A. Stoianov: Biometric encryption: the new breed of untraceable biometrics. In N.V Boulgouris et al., eds., Biometrics: fundamentals, theory, and systems, Wiley-IEEE Press, pp. 655–718, 2009.
- [28] E.-C. Chang, R. Shen, F. W. Teo: Finding the Original Point Set Hidden among Chaff. In Proc. ACM Symp. ASIACCS'06, Taipei, Taiwan, pp. 182–188, 2006.
- [29] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, D. Ahn: Automatic alignment of fingerprint features for fuzzy fingerprint vault. Proc of Conf on Information Security and Cryptology, pp. 358–369, 2005.
- [30] T.C. Clancy, N. Kiyavash, D.J. Lin: Secure smartcard-based fingerprint authentication. Proc ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45–52, 2003.

- [31] I. Damgard, M. Geisler, M. Kroigard: Homomorphic encryption and secure comparison, *Int. J. Appl. Cryptogr.*, vol. 1, no. 1, pp. 22–31, 2008.
- [32] P.E. Danielsson, O. Seger: Generalized and Separable Sobel Operators, in *Machine vision for three-dimensional scenes*, H. Freeman (ed), Academic Press, 1990.
- [33] J. Daugman: How iris recognition works. *Circuits and Systems for Video Technology*, IEEE Transactions on, 14(1) pp. 21–30, 2004.
- [34] G. Davida, Y. Frankel, B. Matt: On enabling secure applications through offline biometric identification. *Proc of IEEE, Symp on Security and Privacy*, pp. 148–157, 1998.
- [35] G. Davida, Y. Frankel, B. Matt: On the relation of error correction and cryptography to an off line biometric based identification scheme. *Proc of WCC99, Workshop on Coding and Cryptography*, pp. 129–138, 1999.
- [36] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *Proc Eurocrypt 2004*, pp. 523–540, LNCS: 3027, 2004.
- [37] J. S. Doyle, K. W. Bowyer, P. J. Flynn: Variation in accuracy of textured contact lens detection based on sensor and lens pattern. *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–7, 2013.
- [38] R. O. Duda, P. E. Hart: Use of the Hough Transformation to Detect Lines and Curves in Pictures, *Comm. ACM*, Vol. 15, pp. 11–15, 1972.
- [39] T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithms, in *Proc. Advances in Cryptology*, pp. 10–18, 1985.
- [40] F. Farooq, R. Bolle, T.-Y. Jea, N. Ratha: Anonymous and revocable fingerprint recognition, in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, pp. 1–7, 2007.
- [41] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschermig, A. Uhl: Transforming rectangular and polar iris images to enable cancelable biometrics. In *Proc of the*

- Int Conf on Image Analysis and Recognition (ICIAR'10). Volume 6112. Springer LNCS, pp. 276–386, 2010.
- [42] H. Feng, C.C. Wah: Private key generation from on-line handwritten signatures. *Inf Manag Comput Secur*, 10(18), pp. 159–164, 2002.
  - [43] C. Fontaine, F. Galand: A survey of homomorphic encryption for nonspecialists, *EURASIP J. Inform. Security*, vol. 2007, no. 15, pp. 1–10, 2007.
  - [44] C. Gentry: Fully Homomorphic Encryption Using Ideal Lattices. 41st ACM Symposium on Theory of Computing (STOC), pp. 169–178, 2009.
  - [45] C. Gentry, S. Halevi: Implementing Gentry's fully-homomorphic encryption scheme, in *Proc. Advances in Cryptology (EUROCRYPT)*, pp. 129–148, 2011.
  - [46] A. Goh, D.C.L. Ngo: Computation of cryptographic keys from face biometrics. *Communications and Multimedia Security*, pp. 1–13, LNCS: 2828, 2003.
  - [47] S. Goldwasser, M. Bellare: Lecture Notes on Cryptography, Summer course on cryptography, MIT, 1996–2001, <http://cseweb.ucsd.edu/~mihir/papers/gb.pdf>.
  - [48] D. Goodin: Breaking the iris scanner locking Samsung's Galaxy S8 is laughably easy. *Ars Technica*, May 23, 2017, available online, <https://arstechnica.com/information-technology/2017/05/breaking-the-iris-scanner-locking-samsungs-galaxy-s8-is-laughably-easy/>, visited: May 2020.
  - [49] D. Gragnaniello, C. Sansone, L. Verdoliva: Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters*, Vol. 57, pp. 81–87, 2015.
  - [50] J. Hämmerle-Uhlr, E. Pschernig, A. Uhl: Cancelable iris biometrics using block re-mapping and image warping. *Proc of the Information Security Conf 2009 (ISC'09)* LNCS 2009, 5735, pp. 135–142, 2009.
  - [51] F. Hao, R. Anderson, J. Daugman: Combining cryptography with biometrics effectively. *IEEE Trans Comput* 55(9), pp. 1081–1088, 2006.
  - [52] G.H. Hardy, E.M. Wright: *An Introduction to the Theory of Numbers*, 6th Edition, Oxford University Press, 2008.

- [53] S. Hirata and K. Takahashi: Cancelable biometrics with perfect secrecy for correlation-based matching, in *Advances in Biometrics (Lecture Notes in Computer Science, vol. 5558)*, M. Tistarelli and M. Nixon, Eds. Berlin, Germany: Springer, pp. 868–878, 2009.
- [54] S. Hoque, M. Fairhurst, G. Howells: Evaluating biometric encryption key generation using handwritten signatures. *Proc of the 2008 Bio-inspired, Learning and Intelligent Systems for Security*, pp. 17–22, 2008.
- [55] T. Ignatenko, F. Willems: Achieving secure fuzzy commitment scheme for optical pufs. *Int Conf on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1185–1188, 2009.
- [56] A. K. Jain, L. Hong, S. Pankanti, R. Bolle: An identity-authentication system using fingerprints, *Proc. IEEE*, vol. 85, no. 9, pp. 1365–1388, 1997.
- [57] Jain, C. Kant: Attacks on Biometric Systems - An Overview. *International Journal of Advances in Scientific Research*, 1(07), pp. 283–288, 2015.
- [58] A. K. Jain, A. Ross, S. Prabhakar: An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, pp. 4–20, 2004.
- [59] A. K. Jain, A. Ross, U. Uludag: Biometric template security: Challenges and solutions. *Proc of European Signal Processing Conf (EUSIPCO) 2005*.
- [60] A. K. Jain, K. Nandakumar, A. Nagar: Biometric template security. *EURASIP J Adv Signal Process*, pp. 1–17, 2008.
- [61] A. K. Jain, P.J. Flynn, A.A. Ross: *Handbook of Biometrics*. Springer, 2008.
- [62] M.Y. Jeong, C. Lee, J. Kim, J.Y. Choi, K.A. Toh, J. Kim: Changeable biometrics for appearance based face recognition. *Proc of Biometric Consortium Conf, 2006 Biometrics Symposium*, pp. 1–5, 2006.
- [63] A. Juels, M. Wattenberg: A fuzzy commitments scheme. *6th ACM Conf on Computer and Communications Security*, pp. 28–36, 1999.
- [64] A. Juels, M. Sudan: A fuzzy vault scheme. *Proc 2002 IEEE Int Symp on Information Theory*, 408, 2002.

- [65] D. Jurafsky, J.H. Martin: *Speech and Language Processing: An Introduction to Natural Language Processing, Speech Recognition, and Computational Linguistics*, 2nd edition, Prentice-Hall, 2009.
- [66] Y. Kim, K. Toh: A method to enhance face biometric security. *IEEE Int Conf on Biometrics: Theory, Applications, and Systems, BTAS'07*, pp. 1–6, 2007.
- [67] Y.W. Kuan, A.B.J. Teoh, D.C.L. Ngo: Secure hashing of dynamic hand signatures using wavelet-Fourier compression with biophasor mixing and 2N discretization. *EURASIP J Appl Signal Process* 2007, (1):32, 2007.
- [68] B. V. K. V. Kumar, A. Mahalanobis, R. D. Juday: *Correlation Pattern Recognition*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
- [69] Y.S. Lee, N.H. Kim, H. Lim, H. Jo, H.J. Lee: Online banking authentication system using mobile-OTP with QR-code. In *Proc. 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pp. 644–648, IEEE, 2010.
- [70] Q. Li, M. Guo, E.-C. Chang: Fuzzy extractors for asymmetric biometric representations. *IEEE Workshop on Biometrics (In association with CVPR)*, pp. 1–6, 2008.
- [71] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, J. Tian: An alignment free fingerprint cryptosystem based on fuzzy vault scheme. *J Netw Comput Appl*, 33, pp. 207–220, 2010.
- [72] Y. Luo, S. S. Cheung, S. Ye: Anonymous biometric access control based on homomorphic encryption, in *Proc. IEEE Int. Conf. Multimedia and Expo (ICME)*, pp. 1046–1049, 2009.
- [73] Y. Luo, S.S. Cheung, T. Pignata, R. Lazzeretti, M. Barni: An efficient protocol for private iris-code matching by means of garbled circuits, in *Proc. 19th IEEE Int. Conf. Image Processing (ICIP)*, pp. 2653–2656, 2012.
- [74] N. Maček, B. Đorđević, J. Gavrilović, K. Lalović: An Approach to Robust Biometric Key Generation System Design. *Acta Polytechnica Hungarica*, Vol. 12, No. 8, pp. 43–60, 2015.

- [75] N. Maček, M. Milosavljević, I. Franc, M. Bogdanoski, M. Gnjatović, B. Trenkić. Secure Modular Authentication Systems Based on Conventional XOR Biometrics. In Proc. of the 9th Int. Conf. on Business Information Security (BISEC2017), Belgrade, pp. 27–32, 2017.
- [76] N. Maček, I. Franc, M. Gnjatović, B. Trenkić, M. Bogdanoski, A. Aleksić: Biometric Cryptosystems – Approaches to Biometric Key-binding and Key-generation. In Proceedings of the 10th International Conference on Business Information Security (BISEC 2018), Metropolitan University, Belgrade, pp. 16–19, 2018.
- [77] N. Maček, S. Adamović, M. Milosavljević, M. Jovanović, M. Gnjatović, B. Trenkić: Mobile Banking Authentication Based on Cryptographically Secured Iris Biometrics. Acta Polytechnica Hungarica, Vol. 16, No. 1, pp. 45–62, 2019.
- [78] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri: Template protection for HMM-based on-line signature authentication. Proc Workshop Biometrics CVPR Conference, pp. 1–6, 2008.
- [79] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri: Cancelable biometrics for hmm-based signature recognition. Proc of the 2nd IEEE Int Conf on Biometrics: Theory, applications and systems (BTAS'08), pp. 1–6, 2008.
- [80] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri: Cancelable templates for sequence-based biometrics with application to on-line signature recognition. Trans Syst Man Cybernet A Syst Hum, 40(3), pp. 525–538, 2010.
- [81] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer, 2009.
- [82] M. Mannan, P. C. Van Oorschot: Security and Usability – The Gap in Real-World Online Banking. NSPW'07, North Conway, NH, USA, Sep. 18–21, 2007.
- [83] U. Maurer: A Universal Statistical Test for Random Bit Generators, Journal of Cryptology, vol. 5(2), pp. 89–105, 1992.
- [84] M. Milosavljević, S. Adamović: Osnovi teorije informacije i kodovanja, Univerzitet Singidunum, 2013.

- [85] K. Nandakumar, A.K. Jain, S. Pankanti: Fingerprint-based fuzzy vault implementation and performance. *IEEE Trans Inf Forensic Secur* 2, pp. 744–757, 2007.
- [86] O. Ouda, N. Tsumura, T. Nakaguchi: Bioencoding: a reliable tokenless cancelable biometrics scheme for protecting iris codes. *IEICE Trans Inf Syst*, E93.D, pp. 1878–1888, 2010.
- [87] O. Ouda, N. Tsumura, T. Nakaguchi: Tokenless cancelable biometrics scheme for protecting iris codes. *Proc of the 20th Int. Conf. on Pattern Recognition (ICPR'10)*, pp. 882–885, 2010.
- [88] P. Paillier: Public-key cryptosystems based on composite degree residuosity classes, in *Proc. Advances in Cryptology (EUROCRYPT99)*, pp. 223–238, 1999.
- [89] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha: Sectorized random projections for cancelable iris biometrics, in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, pp. 1838–1841, 2010.
- [90] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha: Secure and robust iris recognition using random projections and sparse representations, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 9, pp. 1877–1893, 2011.
- [91] M. Rabin: Digitalized signatures as intractable as factorization, *Technical Report MIT/LCS/TR-212*, MIT Laboratory for Computer Science, 1979.
- [92] N.K. Ratha, J.H. Connell, R.M. Bolle: Enhancing Security and Privacy in Biometrics-Based Authentication Systems, *IBM Systems Journal*, 40, pp. 614–634, 2001.
- [93] N.K. Ratha, J.H. Connell, R.M. Bolle, S. Chikkerur: Cancelable biometrics: a case study in fingerprints. *ICPR '06: Proc of the 18th Int Conf on Pattern Recognition*, pp. 370–373, 2006.
- [94] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating Cancelable Fingerprint Templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4), pp. 561–572, 2007.

- [95] C. Rathgeb, A. Uhl: Systematic construction of iris-based fuzzy commitment schemes. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), pp. 947–956, LNCS: 5558, 2009.
- [96] C. Rathgeb, A. Uhl: Context-based texture analysis for secure revocable iris-biometric key generation. Proc of the 3rd Int Conf on Imaging for Crime Detection and Prevention, ICDP '09, 2009.
- [97] C. Rathgeb, A. Uhl: An iris-based interval-mapping scheme for biometric key generation. Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09, 2009.
- [98] C. Rathgeb, A. Uhl: Secure iris recognition based on local intensity variations. In Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10). Volume 6112. Springer LNCS, pp. 266–275, 2010.
- [99] C. Rathgeb, A. Uhl: A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security 2011:3, open access, no pagination, 2011.
- [100] C. Rathgeb, F. Breitingner, C. Busch: Alignment-free cancelable iris biometric templates based on adaptive bloom filters, in Proc. IAPR Int. Conf. Biometrics, pp. 1–8, 2013.
- [101] C. Rathgeb, F. Breitingner, C. Busch, H. Baier: On the application of bloom filters to iris biometrics, IET J. Biometrics, vol. 3, no. 4, pp. 207–218, 2014.
- [102] C. Rathgeb, C. Busch: Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters, Comput. Security, vol. 42, pp. 1–12, 2014.
- [103] E. Reddy, I. Babu: Performance of Iris Based Hard Fuzzy Vault. Int J Comput Sci Netw Secur (IJCSNS), 8(1), pp. 297–304, 2008.
- [104] R.L. Rivest, A. Shamir, L. M. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21(2), pp. 120–126, 1978.

- [105] A.L. Rukhin: Approximate Entropy for Testing Randomness, *Journal of Applied Probability* 37(1), pp. 88–100, 2000.
- [106] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standards and Technology Special Publication 800-22, Revision 1a, 131 pages, 2010, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf>.
- [107] M. Savvides, B. Kumar, P. Khosla: Cancelable biometric filters for face recognition. *ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04)* 3, pp. 922–925, 2004.
- [108] B. Schoenmakers, P. Tuyls: Computationally secure authentication with noisy data. Chapter 9 in P. Tuyls, B. Škorić, T. Kevenaar, eds., *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer-Verlag, London, pp. 141–149, 2007.
- [109] W. J. Scheirer, T. E. Boulton: Cracking Fuzzy Vaults And Biometric Encryption. *Biometric Consortium Conference*, Baltimore, 2007.
- [110] C.E. Shannon: A Mathematical Theory of Communication, *Bell System Technical Journal*, pp. 379–423, 1948.
- [111] P. Silva, E. Luz, R. Baeta, H. Pedrini, A. X. Falcao, D. Menotti, D: An approach to iris contact lens detection based on deep image representations. In the *Proc of. 2015 28th SIBGRAPI Conference on Graphics, Patterns and Images*, Salvador, IEEE, pp. 157–164, 2015.
- [112] V. K. Sinha, A. K. Gupta, M. Mahajan: Detecting fake iris in iris bio-metric system. *Digital Investigation*, Vol. 25, pp. 97–104, 2018.
- [113] B. Sklar: *Digital Communication: Fundamentals and Applications*, 2nd Edition, Prentice-Hall, 2001.
- [114] M. Stamp: *Information Security: Principles and Practice*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006.

- [115] C. Stamford: Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016. February 4, 2014, available online, last time visited April 2018.
- [116] A. Stoianov: Cryptographically secure biometrics. In *Biometric Technology for Human Identification VII*, Vol. 7667, p. 76670C. International Society for Optics and Photonics, 2010.
- [117] C. Soutar, G.J. Tomko, G.J. Schmidt: Fingerprint controlled public key cryptographic system. US Patent, 5541994, 1996.
- [118] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V. Kumar: Biometric encryption-enrollment and verification procedures. *Proc SPIE, Optical Pattern Recognition IX*, 3386, pp. 24-35, 1998.
- [119] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V. Kumar: Biometric encryption using image processing. *Proc SPIE, Optical Security and Counterfeit Deterrence Techniques II*, 3314, pp. 178-188, 1998.
- [120] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V. Kumar: Biometric encryption, *ICSA Guide to Cryptography*, 1999.
- [121] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V. Kumar: Method for secure key management using a biometrics. US Patent, 6219794, 2001.
- [122] Y. Sutcu, H.T. Sencar, N. Memon: A secure biometric authentication scheme based on robust hashing. *MMSec '05: Proc of the 7th Workshop on Multimedia and Security*, pp. 111-116, 2005.
- [123] K. Takahashi, S. Hirata: Cancelable biometrics with provable security and its application to fingerprint verification, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 94-A, no. 1, pp. 233-244, 2011.
- [124] A.B.J. Teoh, D.C.L. Ngo: Biophasor: token supplemented cancellable biometrics. *Proc of the Int Conf on Control, Automation, Robotics and Vision (ICARCV'06)*, pp. 1-5, 2006.

- [125] A.B.J. Teoh, C.T. Yuang: Cancellable biometrics realization with multispace random projections. *IEEE Trans SMC B Recent Adv Biomet Syst*, 37(5), pp. 1096–1106, 2007.
- [126] A.B.J. Teoh, Y.W. Kuan, S. Lee: Cancellable biometrics and annotations on biohash. *Pattern Recogn*, 41(6), pp. 2034–2044, 2008.
- [127] A.B.J. Teoh, L.-Y. Chong: Secure speech template protection in speaker verification system. *Speech Commun*, 52(2), pp. 150–163, 2010.
- [128] W. A. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.
- [129] J. Troncoso-Pastoriza, D. Gonzalez-Jimenez, F. Perez-Gonzalez: Fully private noninteractive face verification, *IEEE Trans. Inform. Forensics Security*, vol. 8, no. 7, pp. 1101–1114, 2013.
- [130] S. Tulyakov, F. Farooq, V. Govindaraju: Symmetric hash functions for fingerprint minutiae. *Int Workshop on Pattern Recognition for Crime Prevention (LNCS: 3687), Security and Surveillance*, pp. 30–38, 2005.
- [131] S. Tulyakov, F. Farooq, P. Mansukhani, V. Govindaraju: Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recogn Lett*, 28(16), pp. 2427–2436, 2007.
- [132] M. A. Turk, A. P. Pentland: Face recognition using eigenfaces, in *Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition*, pp. 586–591, 1991.
- [133] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain: Biometric cryptosystems: issues and challenges. *Proc IEEE*, 92(6), pp. 948–960, 2004.
- [134] U. Uludag, A.K. Jain: Fuzzy fingerprint vault. *Proc Workshop: Biometrics: Challenges Arising from Theory to Practice*, pp. 13–16, 2004.
- [135] U. Uludag, A.K. Jain: Securing fingerprint template: fuzzy vault with helper data. *Proc IEEE Workshop on Privacy Research In Vision*, 2006.

- [136] M. Upmanyu, A.M. Namboodiri, K. Srinathan, C.V. Jawahar: Efficient Biometric Verification in Encrypted Domain, ICB 2009, LNCS 5558, pp. 899–908, 2009.
- [137] S. Yang, I. Verbauwhede: Automatic secure fingerprint verification system based on fuzzy vault scheme. Proc of IEEE Int Conf Audio, Speech and Signal Processing (ICASSP'05), 5, pp. 609–612, 2005.
- [138] A.C. Yao: How to generate and exchange secrets, in Proc. 27th Annu. IEEE Symp. Foundations of Computer Science, pp. 162–167, 1986.
- [139] W.K. Yip, A.B.J. Teoh, D.C.L. Ngo: Replaceable and securely hashed keys from online signatures. IEICE Electron Express, 3(18), pp. 410–416, 2006.
- [140] L. Zhang, Z. Sun, T. Tan, S. Hu: Robust biometric key extraction based on iris cryptosystem. Proc of the 3rd Int Conf on Biometrics (ICB'09), pp. 1060–1070, LNCS: 5558, 2009.
- [141] J. Zuo, N. K. Ratha, J. H. Connell: Cancelable iris biometric. 19th International Conference on Pattern Recognition, ICPR 2008, pp. 1–4, IEEE, 2008.
- [142] C. Vielhauer, R. Steinmetz, A. Mayerhöfer: Biometric hash based on statistical features of online signatures. Object recognition supported by user interaction for service robots, Quebec City, Quebec, Canada, vol.1, pp. 123–126, 2002.
- [143] E.A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, B. Škorić: Key extraction from general nondiscrete signals. IEEE Trans Inf Forensic Secur 5(2), pp. 269–279, 2010.
- [144] Y. Wang, K. Plataniotis: Face based biometric authentication with changeable and privacy preservable templates. Proc of the IEEE Biometrics Symposium 2007, pp. 11–13, 2007.
- [145] D. Yada, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, K. W. Bowyer: Unraveling the effect of textured contact lenses on iris recognition. IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, pp. 851–862, 2014.

# Indeks

## N

server za proveru identiteta, 53  
skladište podataka od poverenja, 53  
sistem sa centralizovanim  
    skladištenjem, 54, 60  
sistem sa distribuiranim  
    skladištenjem, 54, 55  
tajni ključ, 31  
test sledećeg bita, 37, 38  
uniformna raspodela, 38  
faza verifikacije, 62  
faza upisa, 57, 65  
faza verifikacije, 65  
homomorfno šifrovanje, 8, 28  
javni ključ, 31, 32, 35, 47, 49  
jednosmerna funkcija sa zamkom, 31,  
    35, 37, 47, 49, 50  
jednokratna beležnica, 55

## S

Viterbijev trelis, 44  
Viterbijev algoritam, 44  
Gaborov filter, 78  
Markovljev lanac, 44  
Ojlerova teorema, 32–34  
Ojlerova funkcija, 32, 33

Sobelov filter, 75  
Fausov filter, 74  
Fermaova teorema, 32, 34  
Hemingov kod, 43, 45  
Hemingovo rastojanje, 41, 42, 79  
algoritam RSA, 31, 35, 49  
blok-permutacija, 11  
blokovski interliver, 45, 46  
binarno potenciranje, 35, 36  
biometrijska verifikacija, 5  
biometrijska kriptografija, 17  
biometrijska identifikacija, 5  
biometrijsko soljenje, 8, 9, 14  
biometrijski šablon, 5 biometrijski  
    modalitet lica, 12 biometrija lica,  
    10, 15  
verifikacija, 57  
generator pseudoslučajnih brojeva, 36–39  
krađa identiteta, 6  
klijent, 53, 55  
konvolucionni koder, 42, 44  
konvolucionni interliver, 45, 47  
kod dužice, 9, 14, 21, 27, 28, 79  
linearni koder, 42, 43

pseudoslučajna raspodela, 38

pametni telefon, 73

neinvertibilna transformacija, 53

neinvertibilna transformacija, 7, 9,  
14, 16, 47, 51

mobilno bankarstvo, 63, 80

otisak prsta, 10, 12, 13, 22

otiska prsta, 15

opoziva biometrija, 16

opoziva biometrija, 10, 53

opozivi šablon, 13, 16, 57, 69 ispitivanje

približne entropije, 39,  
41

dužica, 8–12, 27

idealni biometrijski sistem, 59

idealni biometrijski sistem, 54

# Jedna klasa kriptografski zaštićene autentifikacije klijenata zasnovana na opozivoj biometriji

## ORIGINALITY REPORT

1%

### SIMILARITY INDEX

#### PRIMARY SOURCES

|    |                                                                                |                 |
|----|--------------------------------------------------------------------------------|-----------------|
| 1  | <a href="http://vision.psych.umn.edu">vision.psych.umn.edu</a><br>Internet     | 90 words — < 1% |
| 2  | <a href="http://www.cs.utsa.edu">www.cs.utsa.edu</a><br>Internet               | 39 words — < 1% |
| 3  | <a href="http://www.excode.ru">www.excode.ru</a><br>Internet                   | 29 words — < 1% |
| 4  | <a href="http://uni-obuda.hu">uni-obuda.hu</a><br>Internet                     | 26 words — < 1% |
| 5  | <a href="http://scholarbank.nus.edu.sg">scholarbank.nus.edu.sg</a><br>Internet | 26 words — < 1% |
| 6  | <a href="http://hdl.handle.net">hdl.handle.net</a><br>Internet                 | 25 words — < 1% |
| 7  | <a href="http://www.sce.carleton.ca">www.sce.carleton.ca</a><br>Internet       | 22 words — < 1% |
| 8  | <a href="http://cseweb.ucsd.edu">cseweb.ucsd.edu</a><br>Internet               | 22 words — < 1% |
| 9  | <a href="http://www.scribd.com">www.scribd.com</a><br>Internet                 | 16 words — < 1% |
| 10 | <a href="http://es.scribd.com">es.scribd.com</a><br>Internet                   | 11 words — < 1% |

---

EXCLUDE QUOTES

ON

EXCLUDE MATCHES

< 15 WORDS

EXCLUDE  
BIBLIOGRAPHY

ON