Универзитет Сингидунум
Департман за последипломске студије

Докторска дисертација

Једна класа криптографски заштићене аутентификације клијената заснована на опозивој биометрији

Ментор: проф. др Милан М. Милосављевић

Студент: Милош Јовановић
Број индекса: 460075/2015

Београд,
јун 2020. године

Захваљујем се својој породици и ментору проф. др Милану М. Милосављевићу.

Сажетак

У овом раду је представљен један нови приступ криптографски заштићеној биометијској аутентификацији корисника, заснован на криптографији са јавним кључевима, генератору псеудослучајних бројева и опозивој биометрији. Биометријски шаблони су шифровани или опозиви током свих фаза у раду система, изузев у фази издвајања обележја, што резултује системом који је отпоран на велики број напада. Систем није процесорски захтеван, а генерисани биометријски шаблони су прихватљиве величине.

Предложени приступ криптографски заштићеној аутентификацији је имплементиран кроз модуларни биометријски систем за проверу идентитета корисника услуга мобилног банкарства базиране на биометрији дужице људског ока. Саопштени су позитивни резултати анализе перформанси предложеног система на реалистичном скупу података, и испитивања случајности шифрованих опозивих шаблона и података који се преносе преко мреже.

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.

Садржај

Листа слика

Листа табела

Глава 1

Увод

1.1 Општа разматрања

Биометријска аутентификација је процес утврђивања идентитета заснован на физиолошким или понашајним особинама корисника. Биометрија се може посматрати као један условно идеалан начин аутентификације: корисници не морају да памте лозинке или носе уређаје на којима су смештени аутентификациони подаци, док су биометријске карактеристике у основи неопозиве, чиме се обезбеђује и сервис непорецивости. Међутим, као и било који лични подаци, биометријски шаблони могу се пресрести, украсти, репродуковати или изменити, што може довести до крађе идентитета. Имајући то у виду, може се закључити да биометријски системи обрађују осетљиве личне податке, као и да су сигурност и приватност биометријских шаблона важна питања на која треба обратити пажњу приликом пројектовања система за проверу идентитета. Крађа идентитета се спречава технолошким противмерама које пружају јаку сигурност биометријских шаблона и заштиту приватности корисника. Међутим, мере технолошке заштите не смеју да наруше перформансе система до нивоа да употреба система више није практична, нпр. оптерећивањем система додатним процесорски захтевним математичким операцијама или захтевом за додатним простором за складиштење.

Поред криптографске сигурности, очекује се да биометријски систем пружа снажну заштиту приватности, што резултује следећим скупом захтева. Биометријски шаблони треба да остану шифровани или у најгорем случају опозиви током свих фаза употребе (складиштење, пренос и верификација). Ниједан клијент не сме да

приступи приватним кључевима који се налазе на аутентификацијоном серверу, јер се на тај начин може угрозити сигурност биометријских шаблона. Такође, систем би требао бити отпоран на замену шаблона и све нападе ниског нивоа, у систем се не смеју уносити процесорски исувише захтевне операције, а криптографске противмере не смеју умањити укупну тачност (тј. не смеју повећавати степен лажног прихватања или степен лажног одбијања).

1.2 Предмет, циљ и доприноси истраживања

Полазећи од схватања да су биометријски подаци неопозиви у природи, и да компромитовање биометријских шаблона може довести до крађе идентитета корисника, што за последицу може имати различите облике злоупотребе, овај рад разматра следеће хипотезе.

Хипотеза 1. Тренутна решења за заштиту биометријских шаблона не обезбеђују довољно висок ниво сигурности шаблона и приватности корисника.

Хипотеза 2. Развојем сопственог биометријског система у ком биометријски шаблони остају шифровани или у најгорем случају опозиви током свих фаза њихове примене (складиштење, пренос и верификација) обезбеђује се употребљивост предложеног приступа у реалним доменима примене.

Научни циљ овог рада је да се представи један нови начин криптографски заштићене аутентификације клијената помоћу биометријских података који, у поређењу са досадашњим истраживањама и достигнућама у овој области, унапређује сигурност и гарантује аутентичност приликом провере идентитета корисника. Посебна пажња је посвећена анализи постојећих решења за заштиту биометријских система за проверу идентитета са аспекта сигурности и заштите приватности. Намена ове анализе је да се прикаже ефикасност постојећих решења, и да се пружи основа за предлагање новог приступа који би ефикасно одговорио на недостатке постојећих решења.

Технички циљ овог рада је да се предложени начин криптографски заштићене аутентификације клијената имплементира кроз модуларни биометријски систем за проверу идентитета. Систем користи криптографију са јавним кључевима, генератор псеудослучајних бројева и опозиву биометрију. Неинвертибилна трансформација се

извршава помоћу кључа који се налази на сигурном меморијском складишту уређаја. Биометријски шаблони су шифровани или, у најгорем случају, опозиви током свих фаза у раду система, изузев у фази издвајања обележја, што резултује системом који је отпоран на велики број напада. Предложени систем не користи процесорски захтевне операције, а генерисани биометријски шаблони су прихватљиве величине. Систем је процењен у домену провере идентитета корисника услуга мобилног банкарства базиране на биометрији дужице људског ока.

Друштвени циљ овог рада је да допринесе већој друштвеној прихватљивости криптографски заштићене аутентификације клијената помоћу биометријских података.

Основни доприноси овог рада укључују:

1. преглед постојећих система и метода за заштиту биометријских шаблона,
2. критички осврт на опозиву биометрију и хомоморфно шифровање,
3. предлагање новог приступа биометријској аутентификацији помоћу шифрованих опозивих шаблона,
4. примена XOR биометрије дужице у предложеном приступу,
5. увођење новог система за криптографску заштиту клијената који се аутентификују помоћу биометријских података,
6. развој модуларног биометријског система за проверу идентитета корисника на основу биометрији дужице људског ока.

1.3 Структура рада

Рад је структуриран на следећи начин. У глави 2. дат је преглед релевантних истраживања у области, при чеми су посебно обрађена питања биометријске верификације корисника, употребе опозиве биометрије и криптографске заштита биометријских шаблона. Глава 3. уводи теоријске основе истраживања које су релевантне за присутуп предложен у овом раду. Оне укључују криптографију са јавним кључевима, генераторе псеудослучајних бројева, заштитивне кодере, интерливере и неинвертибилне трансформације.

У глави 4. предложен је један нови приступ криптографски заштићеној биометијској аутентификацији, заснован на криптографији са јавним кључевима, генератору псеудослучајних бројева и опозивој биометрији. На основу тога, изложен је и предлог система за проверу идентитета корисника услуга мобилног банкарства базирана на биометрији дужице људског ока, уз дефинисање алгоритама за упис и верификацију корисника.

Систем који имплементира предлог из главе 4., процењен је у глави 5. Прво је размотрен истраживачки проблем издвајања обележја дужице и верификације идентитета особе. Потом су саопштени позитивни резултати анализе перформанси предложеног система на реалистичном скупу података. Коначно, саопштени су позитивни резултати испитивања случајности шифрованих опозивих шаблона и података који се преносе преко мреже.

Закључак и преглед могућих смерова даљег истраживања дати су у глави 6.

Глава 2

Преглед у области истраживања

Биометријски систем за проверу идентитета корисника састоји се од: сензора, модула за издвајање обележја (енгл. *feature extraction module*), модула за поређење биометријских шаблона (енгл. *matching module*), базе података у којој су смештени шаблони генерисани у фази уписа (енгл. *enrollment phase*) и модула за доношење одлуке (енгл. *decision module*).

Приликом регистрације корисника на систем (такозвана фаза уписа), корисник прилаже биометријски узорак сензору. Сензор прослеђује очитане податке модулу за издвајање обележја, који на основу узорка генерише биометријски шаблон који се заједно са корисничким идентитетом (на пример, корисничким именом) смешта у базу података са шаблонима. Провера идентитета корисника након уписа, односно регистрације, може се обавити на два начина: верификацијом и идентификацијом. У случају биометријске верификације, корисник систему прилаже свој идентитет и биометријски узорак. Модул за издвајање обележја генерише нови биометријски шаблон, а модул за поређење након тога рачуна сличност (на пример, Хемингово растојање два низа битова) између шаблона који је генерисан током верификације и шаблона смештеног у бази података након уписа који одговара корисничком идентитету. Након тога модул за доношење одлуке на основу прага поређења одређује да ли се ради о легитимном кориснику или не. У случају да је резултат поређења нижи од прага поређења, корисник се прихвата као легитиман и добија приступ ресурсима сходно правилима ауторизације, а у супротном се одбија. У случају биометријске идентификације од корисника се не захтева да приложи свој идентитет, већ само биометријски узорак, а генерисани шаблон се пореди са свим шаблонима у бази

података. Треба напоменути да је у случају биометријске верификације субјекат кооперативан, док је у случају биометријске идентификације субјекат у одређеном броју случајева некооперативан, као и да процес идентификације може бити процесорски захтеван уколико у бази постоји велики број шаблона (на пример, претрага базе отисака прстију Министарства унутрашњих послова, Федералног бироа за истраге и слично).

Иако су биометријски системи веома погодни за проверу идентитета, зато што не постоји потреба да корисници памте лозике које лако могу заборавити или носе аутентификационе токене (на пример, флеш меморије или паметне картице) које могу изгубити, као и сви остали системи за аутентификацију (на пример, системи засновани на нечему што корисник зна) подложни су нападима. Неки од напада који су изводљиви на ове системе су употреба лажних биометријских узорака, напад понављањем, заобилажење сензора и генерисање лажних шаблона, као и замена биометријских шаблона у бази података. Неки од ових напада за последицу имају прихватање нелегитимног корисника као легитимног, док неки, попут замене шаблона у бази могу резултовати и одбијањем услуга (енгл. *Denial of Service*, DoS) легитимним корисницима.

У обзир треба узети да су ови напади изводљиви искључиво уколико је систем пројектован на принципу сигурности засноване на скривању (енгл. *security by obscurity*), односно уколико пројектант не узима у обзир присуство нападача и скуп акција које може извршити како би извео одређене нападе, већ је заснован на скривању архитектуре и начина рада система. Уколико се приликом пројектовања користи принцип сигурности засноване на дизајну (енгл. *security by design*), где пројектант система у обзир узима и присуство нападача и скупа акција које може обавити, извршење већине напада се може онемогућити.

Као и било који други незаштићени лични подаци, биометријски шаблони се могу пресрести, украсти, репродуковати или изменити у случлају да је је незаштићени биометријски уређај повезан на мрежу или у случају да је вешт нападач стекао физички приступ уређају који не користи анти-форензичке технике којима би се спречио неовлашћен приступ осетљивим подацима (тј. незаштићеним шаблонима). Због неопозивости биометријских података, један од могућих резултата успешног извршења напада на биометријске системе за аутентификацију је крађа идентитета

легитимних корисника. Узевши то у обзир, постаје јасно да биометријски системи обрађују осетљиве личне податке, као и да су сигурност и приватност биометријских шаблона важна питања на која треба обратити пажњу приликом пројектовања система за проверу идентитета заснованих на нечему што корисник јесте (биометрија заснована на физичким карактеристикама) или што корисник може да уради (биометрија заснована на понашајним карактеристикама).

Да би се спречила крађа идентитета, пројектант система не сме се ослањати на откривање злоупотребе након успешног извршења напада, већ се мора ослонити на методе које обезбеђују висок ниво сигурности шаблона и заштиту приватности корисника. Додатно, перформансе биометријског система смеју се смањити искључиво на прихватљив ниво након увођења ових противмера у систем. Другим речима, очекује се да увођење ових противмера у систем неће смањити тачност верификације или идентификације на неприхватљив ниво, односно да се проценат лажно одбијених корисника (енгл. *False Rejection Rate*, FRR) и лажно прихваћених корисника (енгл. *False Acceptance Rate*, FAR) неће значајно повећати. Такође, увођење ових противмера не сме за последицу имати знатно повећање сложености израчунавања и повећање простора потребног за складиштење заштићених биометријских шаблона.

Један од начина заштите биометријских шаблона и очувања приватности је употреба такозване опозиве биометрије (енгл. *cancelable biometrics*), методе заштите која се у наводима извесних аутора може наћи и под називом поништива биометрија. Две основне технике које се користе у опозивој биометрији су намерно изобличавање биометријских шаблона или узорака употребом неинвертибилних, односно једносмерних трансформација [74], попут блок пермутације текстуре дужице (енгл. *iris*), и биометријско сољење (енгл. *biometric salting*).

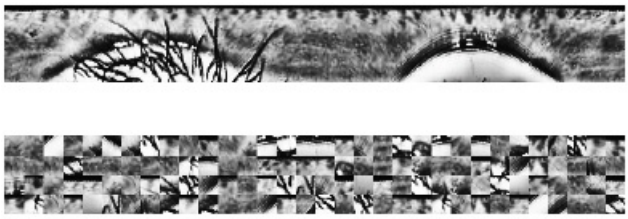
Опозива биометрија која користи неинвертибилне трансформације заснива се на примени исте трансформације на датом биометријском узорку или шаблону у фази уписа и у фази верификације. Примена ових трансформација донекле подсећа на смештање хеш вредности лозинке у базу података приликом креирања корисничког налога и поређење те вредности са хеш вредношћу лозинке генерисаним приликом пријављивања корисника на систем. Постоји велики број неинвертибилних трансформација за различите биометријске модалитете, од којих неке користе и кључ. Узевши то у обзир, сваки компромитовани шаблон може се лако опозвати, а при-

ликом накнадне регистрације корисника може се применити друга трансформација. У случају да неинвертибилна трансформација користи кључ, приликом замене компромитованог шаблона може се заменити само кључ. Примери ових трансформација које се применити на отисак прста и дужицу су описани у [94] и [141], респективно. Међутим, неинвертибилне трансформације могу бити делимично инвертибилне (у литератури се најчешће не наводе концизни математички докази потпуне једносмерности ових трансформација) и у највећем броју случајева смањују тачност верификације, односно повећавају грешке лажног прихватања и одбијања, што значи да не представљају потпуно решење проблема заштите биометријских шаблона. Смањење перформанси узроковано је чињеницом да је над трансформисаним биометријским шаблонима тешко извршити одговарајућа поређења, као и да је количина информације корисне за поређење у неким случајевима смањена [92, 141].

Биометријско сољење односи се на трансформације биометријских шаблона који су одабрани као инвертибилни, при чему се свака трансформација сматра приступом биометријском сољењу чак и ако су шаблони генерисани тако да није могуће реконструисати оригинални биометријски сигнал [99]. Иако биометријско сољење не смањује тачност верификације, неинвертибилне трансформације пружају виши ниво сигурности, што значи да се ни ова техника не може сматрати сигурним решењем проблема.

Приступи опозивој биометрији могу се такође класификовати и на основу домена у којима се примењују трансформације. У домену сигнала, трансформације се примењују на сирове биометријске узорке (на пример, слика лица [92] или на предобрађене биометријске сигнале (на пример, текстура дужице [50]). У случају да се су трансформације примене у домену сигнала, модуле за издвајање обележја и поређење шаблона није потребно мењати. Међутим извесне промене у овим модулима је потребно начинити уколико се трансформације извршавају у домену издвојених обележја (на пример, црте лица [126]).

Други начин заштите и очувања приватности биометријских шаблона је примена хомоморфних шема шифровања [21, 108]. Хомоморфно шифровање односи се на криптографске алгоритме који омогућавају да се одређена израчунавања изврше у шифрованом домену. Иако су постојала извесна очекивања да ће истраживања у области хомоморфног шифровања увести значајна унапређења заштите биометрij-



Слика 2.1: Један пример примене опозиве биометрије дужице: оригинална текстура дужице (горе) и блок пермутација текстуре (доле). Слика преузета из [99].

ских шаблона [44], у релевантној литератури за сада нису пријављени значајнији резултати употребљиви у пракси. Иако је теоријски применљиво — на пример, хомоморфно шифровање је теоријски погодно за примену у системима који користе операцију ексклузивно ИЛИ за израчунавање Хеминговог растојања између два бинарна кода дужице (енгл. *iris code*) — постоје два разлога због којих хомоморфно шифровање није практично: значајно повећање шифрованог шаблона и сложености израчунавања [108].

У наставку овог поглавља укратко су анализурани алгоритми, поступци, методе и резултати пријављени у релевантним научним радовима у којима је описана употреба опозиве биометрије и криптографске заштите биометријских шаблона.

2.1 Употреба опозиве биометрије

Трансформације које се користе у опозивој биометрији дизајнирају се тако да је практично немогуће у разумном временском периоду са ограниченом процесорском снагом регенерисати оригинални биометријски податак. На сл. 2.1 приказана је оригинална текстура дужице и текстура над којом је извршен један тип једносмерне трансформације — блок пермутација. Као што је већ поменуто, постоје две основне технике које се примењују у опозивој биометрији: једносмерне, односно неинвертибилне трансформације и биометријско сољење.

Примена ових трансформација не сме да утиче на индивидуалност биометријских карактеристика, односно, не сме да повећа проценат лажно прихваћених корисника. С друге стране, постоји и ограничење које се односи на грешку лажног прихватања, која такође не сме да се повећа [92]. Међутим, уколико шум није пречишћен пре извршавања саме трансформације (на пример, нису пречишћене шаре дужице од

трепавица), вероватноћа да се ове грешке неће повећати је релативно мала. У случају да трансформисани биометријски подаци постану компромитовани, параметри трансформације се мењају а корисници се поново региструју на систем како би се ажурирао биометријски шаблон. Додатна мера заштите која отежава извршавање напада на биометријске системе који користе опозиву биометрију је употреба различитих трасформација у различитим доменима примене за исте кориснике. У том случају, компромитовање једног шаблона неће за последицу имати компромитовање шаблона за друге домене примене.

Иако у већини предложених приступа поређење опозивих шаблона није једноставно, а примењене трансформације које су изабране као неинвертибилне смањују тачност поређења, постоје радови у којима су описане методе и алгоритми (на пример, [103, 126]), посебно за биометријско сољење, које повећавају перформансе система. На пример, у случају да се приликом уписа и верификације примењују трансформације специфичне за корисника, аутентификација постаје двофакторска, што значи да може повећати сигурност, али да увођење трансформације не утиче на тачност биометријске аутентификације.

2.1.1 Приступи засновани на неинвертибилним трансформацијама

Ratha и др. [92] су међу првима увели концепт неинвертибилних трансформација као једну од метода опозиве биометрије. У фази уписа корисника, на биометријске податке се примењују неинвертибилне трансформације које се бирају на основу конкретног домена примене. У фази аутентификације, биометријски подаци се трансформишу на исти начин, користећи трансформацију за дати домен примене, и врши се поређење трансформисаних шаблона.

Неколико типова трансформација, укључујући и функционалну трансформацију, које се могу користити за конструкцију претходно поменутих система заснованих на отиску прста и биометрији лица представљене су у [92, 93, 94].

Трансформације предложене у [92] успешно су примењене на биометрију дужице, сходно резултатима експеримената представљеним у [50]. Међутим, у истраживању које је описано у [41] показано је да примена обе трансформације на правоугаоне слике дужице значајно смањује тачност верификације. Слично истраживању описаном

у [141], Rathgeb и Uhl [98] предлажу примену блок-пермутација кодова дужице.

Један типичан приступ генерисању опозивих биометријских шаблона заснован је на случајним пермутацијама обележја. У истраживању [141] представљене су четири различите трансформације које су примењене у домену слике дужице и у домену издвојених обележја, при чему, сходно резултатима експеримената, свака трансформација уноси малу деградацију перформанси. Први метод трансформације у домену обележја трансформише Габор-заснована обележја кружним померањем и случајним додавањем редова. Други метод примењује трансформацију засновану на случајном мешању и примењивању операције екслузивно ИЛИ. Сходно наводима аутора, ове методе постепено умањују количину информације доступне за препознавање. Пошто су претходно поменуте методе засноване на примени линеарних трансформација на Габор-заснованим векторима обележја, осетљиве су на шум. Аутори у [89] указују на могуће начине на које се ова ограничења могу заобићи. Један од предложених начина је подела обележја у регионе и случајна пермутација на основу речника, али се указује на чињеницу да је препознавање немогуће уколико је локација обележја у речнику непозната. Сличан приступ је предложен у [50], где је сваки блок циљне текстуре мапиран на блок изворне текстуре. Ова метода користи ремапирање блокова уместо пермутације зато што је ремапирање неинвертибилно. Изворни блокови који нису део мапирања нису садржани у трансформисаној текстури, што значи да је немогуће реконструисати оригиналну текстуру дужице.

Један приступ генерисању опозивих шаблона отиска прста заснован на пермутацијама помоћу кључа представљен је у [40]. У овом приступу пермутује се бинарни вектор издвојен из обележја отиска прста и чува се у бази података. Приликом аутентификације, од корисника се захтева да приложи кључ како би систем извршио пермутацију новог вектора и извршио поређење са шаблоном смештеним у бази. У овој, као и у сличним трансформацијама које зависе од кључа, сигурност кључа је од суштинског значаја за приватност корисника и сигурност шаблона. Предност пермутација са кључем је у томе што оне не уносе суштинске измене у вектор обележја, што значи да нема губитка корисне информације, а самим тим ни умањења тачности препознавања.

У истраживањима описаним у [78, 79, 80] примењене су неинвертибилне трансформације како би се генерисали опозиви шаблони на основу такозваних on-line

потписа. У њиховом присупу, биометријски шаблони, који су представљени као низ временских секвенци, подељени су у непреклапајуће секвенце на основу случајног вектора који обезбеђује опозивост. Након тога, трансформисани шаблон се генерише линеарном конволуцијом претходно поменутог низа. Реконструкција оригиналних продатака из трансформисаног шаблона рачунски је сложена колико и насумично погађање, што овом виду трансформације значајно повећава ниво сигурности.

Boult и др. [14, 15] су у својим радовима представили криптографски сигурне биометријске токене (такозване биотокене, енгл. *biotokens*) које су применили на биометријске модалитете лица и отиска прста. Како би увећали сигурност биометријских система, биотокени су примењени уз постојеће шеме препознавања, као што је анализа главних компоненти (енгл. *Principal Component Analysis*, PCA) која се користи приликом фотометријског препознавања лица. Међутим, иако је на први поглед идеја употребљива, на извесна питања није дат одговор — на пример, како треба дизајнирати помоћну функцију која раздваја биометријске шаблоне на стабилне и нестабилне делове, као и да ли је систем могуће прилагодити за рад са другим биометријским модалитетима. У истраживањима које су аутори наставили и објавили у [16, 17] представљена је нова врста биометријских токена који су успешно примењени на биометрију отиска прста с циљем обезбеђивања сигурне комуникације преко несигурног канала, при чему се криптографски кључеви генеришу на основу успешног поређења биотокена.

Још један тип неинвертибилних трансформација који се често користи за генерисање опозивих биометријских узорака заснован је на употреби случајних пројекција [89, 90]. Ове методе су засноване на пројектовању издвојених обележја из биометријског узорка на случајни потпростор.

Опозива биометрија за препознавање дужице заснована на случајним пројекцијама представљена је у [89]. У случају примене случајне пројекције на необрађену слику дужице перформансе система се умањују из неколико разлога. Пре свега, у реалистичним сликама дужица, упркос добрим алгоритмима за сегментацију, постоји одређени шум који потиче од рефлексија, трепавица и капака. Такође, различити делови дужица имају различит квалитет, односно садрже различиту количину корисне информације. У случају употребе линеарне трансформације целокупног вектора, комбинују се региони доброг квалитета са зашумљеним регионима који на тај начин

оштећују податке. Аутори као решење проблема предлажу секторске случајне пројекције (енгл. *Sectored Random Projections*, SRP) у којима се случајне пројекције примењују одвојено на сваки сектор, а резултујући трансформисани вектори се спајају како би се формирао опозиви шаблон. Последица тога је да зашумљени подаци имају негативан утицај само на део вектора обележја али не и на целокупан вектор. Приликом уписа систем издваја узорак дужице корисника, израчунава Габор-заснована обележја, примењује различите случајне пројекције за сваки домен примене и смешта нови опозиви узорак у базу података. Треба узети у обзир чињеницу да чак и у случају компромитовања опозивог шаблона и кључа (односно матрице пројекције) оригинални узорак дужице не може бити регенерисан због редукције димензионалности коју намеће сама пројекција. Такође, нападач који на нелегалан начин дође у посед узорка дужице са биометријског уређаја или употребом скривеног уређаја за крађу слике дужице, неће бити у могућности да да регенерише шаблон без познавања скривене пројекције. У фази верификације, корисник прилаже слику дужице и матрицу пројекције систему, а систем израчунава трансформисан шаблон и пореди га са шаблоном који је сачуван у бази података.

2.1.2 Приступи засновани на биометријском сољењу

У истраживању које су описали Savvides и др. [107] опозива биометрија лица генерисана је применом такозваних корелационих филтра минималне средње вредности који обезбеђују једносмерност трансформације. Лични идентификациони бројеви корисника користе се као кључ на сличан начин као што је описано у [121].

Техника звана биометријско хешовање (енгл. *BioHashing*) [46], преузета из домена биометријске криптографије, такође се може искористити за генерисање опозивих шаблона уколико се из ње уклони процедура којом се кључ везује за биометријски узорак. Првобитне варијанте алгоритма за биометријско хешовање нису у обзир узимале сценарио украдених токена. У даљим истраживањима показано је да грешка приликом екстракције 180-битног кода отиска прста расте са 0% на 5,31% у сценарију украдених токена [124]. Проблем је накнадно решен увођењем такозване методе вишепросторних случајних пројекција (енгл. *Multispace Random Projections*, MRP) [125, 127]. Сходно наводима аутора, претходно поменутом техником примењеном на модалитете лица и гласа, могуће је спречити пад перформанси препознавања у сце-

нарију украденог токена. Аутори су такође представили метод генерисања опозивих кључева на основу динамичких потписа [139, 67] заснован на *BioPhasor* кораку случајног мешања и кориснички зависне $2N$ дискретизације.

Kim и Toh [66] применили су кориснички-зависне случајне пројекције на обележја лица издвојена методом главних компоненти на које су затим применили трансформацију за минимизацију грешке. Аутори, међутим, нису у обзир узели сценарио украденог токена.

Још један приступ биометријском сољењу представљен је у [144] у коме су обележја лица трансформисана на основу тајног кључа. Једносмерност, односно неинвертибилност, постигнута је употребом квантизације.

Ouda и др. представили су технику за генерисање опозивих кодова дужице [86, 87]. Из неколико шаблона генерисаних у фази уписа формира се вектор конзистентних битова (такозвани *BioCode*) и позиције тих битова. Опозивост је обезбеђена кодовањем формираних вектора на основу случајног унутрашњег кључа.

Још једном треба напоменути да неинвертибилне трансформације пружају виши ниво сигурности у односу на биометријско сољење.

2.1.3 Остали значајнији приступи у опозивој биометрији

Мотивисани успехом примене методе корелације засноване на филтрима у истраживањима која се односе на препознавање облика и рачунарску визију [68], аутори су описали метод случајне конволуције за генерисање опозивих биометријских шаблона у [107]. Основна идеја је шифровање биометријских шаблона употребом случајних кориснички-зависних конволуционих језгара. На сликама које се користе за обуку најпре се обавља конволуција случајним конволуционим језгром (енгл. *kernel*). Кључ који се користи за генерисање случајног конволуционог језгра је лични идентификатор корисника (енгл. *Personal Identification Number*, PIN). Након тога се слике за тренинг користе за генерисање такозваног MACE биометријског филтра (енгл. *Minimum Average Correlation Energy*). Овај шифровани филтар се чува и даље користи за аутентификацију. Током фазе препознавања, корисник систему прилаже PIN и шифровани филтар који се користи за генерисање конволуционог језгра. Систем даље обавља конволуцију језгра са тест сликама које је корисник приложио. Конволуционе тест слике се након тога унакрсно корелишу са шифрованим MACE фил-

тром а резултат конволуције се користи за аутентификацију корисника. Аутори су доказали да коволуција слика коришћених за тренинг са случајним конволуционим језгром пре генерисања MACE филтара коришћених за биометријско препознавање не мења излаз корелације [107], што резултује непромењеном тачношћу препознавања. Осим тога, различити опозиви биометријски шаблони се могу генерисати из истог узорка једноставном променом конволуционог језгра.

Друге методе опозиве биометрије засноване на корелацији укључују CIRF (енгл. *Correlation Invariant Random Filtering*), метод за који је показано да обезбеђује скоро идентичну тачност као конвенционални системи за верификацију отиска прста засновани на жетону [123, 53].

Системи за заштиту опозивих биометријских узорака засновани на Блумовим филтрима су такође описани у релевантној литератури [100, 101, 102]. У основи, Блумов филтар је просторно-ефикасна пробабилистичка структура података која служи за проверу да ли је дати елемент члан скупа. Конкретно, опозиви биометријски шаблони дужице засновани на адаптивним Блумовим филтрима представљени су у [101]; генеричка адаптивна Блумова филтарска трансформација примењује се на бинарне векторе обележја у случају различитих алгоритама препознавања дужице. Показано је да овај метод обезбеђује заштиту шаблона, компресију биометријских података и рачунски ефикасну биометријску идентификацију. Додатно, ротационо-независна Блумова филтарска трансформација обезбеђује висок ниво сигурности без смањења тачности препознавања [101].

Jeong и др. [62] комбиновали су две различите технике издвајања обележја како би обезбедили опозиву биометрију лица. Коефицијенти метода PCA и независне анализе компоненти (енгл. *Independent Component Analysis*, ICA) су издвојени, а потпом оба вектора обележја измешана с циљем генерисања трансформисаног шаблона.

Tulyakov и др. [130, 131] предложили су методу за генерисање опозивих хешева отисака прста. Уместо поравнавања карактеристичних тачака, аутори примењују хеш-функције попут симетричних сложених хеш функција.

Hirata и Takahashi [53] предложили су систем опозиве биометрије применљив за отиске прстију који трансформише слике користећи Фуријеову трансформацију. Резултат се након тога обрађује случајно генерисаним филтром, а корисник чува одговарајући инверзни филтар на токену. Инверзни филтар се користи у фази ау-

тентификације како би се регенерисали одређени подаци преузети у фази уписа и извршило поређење употребом корелације.

Bringer и др. [22] изнели су идеју о креирању временски зависне опозиве биометрије с циљем обезбеђивања немогућности уласка у траг различитим идентитетима током одређених временских интервала.

2.1.4 Кратки осврт на сигурност опозиве биометрије

Иако се у релевантној литератури која се односи на опозиву биометрију наводи делимична анализа сигурности система упоредо са тачношћу препознавања у односу на референтни систем, конкретне анализе које се односе на неинвертибилност опозивог шаблона и неповезаност шаблона истог корисника генерисаних помоћу различитих параметара трансформације ретко су извршене у потпуности.

Анализе које се тичу неинвертибилности, односно могућности да се након примене једносмерне трансформације регенерише оригинални биометијски шаблон, потребно је извршити као детаљно испитивање претходно поменутих трансформација. На пример, уколоко је условно неинвертибилна блок пермутација примењена на биометријски податак (на пример, дужицу [50] или отисак прста [94]) како би се генерисао опозив шаблон, потребно је проценити рачунску сложеност регенерисања оригиналног биометријског узорка или његових делова на основу опозивог шаблона. За неке приступе анализа неинвертибилности је релативно једноставна, док се за друге захтева далеко сложенија и софистицираније анализа. На пример, у неким случајевима сложеност реконструкције оригиналног сигнала може зависити од сложености решавања извесних математичких проблема, попут проблема слепе деконволуције (енгл. *blind deconvolution problem*) [79]. Да би се осигурала обновљивост заштићених биометријских шаблона, примењене трансформације обележја изводе се на основу различитих параметара — другим речима, примењени параметри дефинишу коначан простор кључева, што се ретко пријављује у релевантној литератури. У општем случају, разлика између заштићених шаблона је већа уколико је простор кључева дефинисан параметрима трансформације већи [80].

Да би се задовољило својство неповезаности, различити опозиви шаблони истог корисника генерисани помоћу различитих параметара неинвертибилне трансформације морају се разликовати као и шаблони различитих субјеката. Другим речима,

простор кључева дефинисан параметрима трансформације мора бити довољно велики да обезбеди довољно висок ниво случајности који ће резултовати ниским нивоом могућности повезивања шаблона истих субјеката.

2.2 Криптографска заштита биометријских шаблона

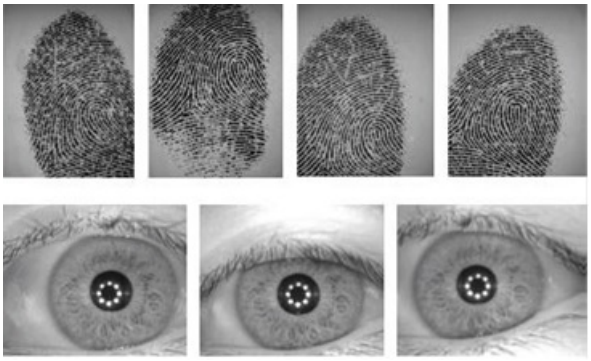
Термин биометријска криптографија, односно биометријски криптосистеми (енгл. *biometric cryptosystems*) најчешће се односи на системе за генерисање криптографских кључева на основу биометријских узорака или на системе који везују кључ генерисан помоћу генератора случајних или псеудослучајних бројева за помоћни податак. Алтернативно, претходно поменути термин може се односити и на криптографску заштиту биометријских шаблона. У овом делу рада укратко ће бити анализирани биометријски криптосистеми док ће посебна пажња бити посвећена криптографској заштити биометријски шаблона.

2.2.1 Биометријски криптосистеми

Биометријски криптосистеми дизајнирају се са намером да на сигуран начин вежу кључ за биометријски шаблон или да на основу биометријског шаблона генеришу криптографски кључ [26] чиме је омогућена репродукција кључа која је зависна од биометријског узорка, као и заштита биометријских шаблона [59, 27]. У односу на репродукцију, односно генерисање криптографског кључа на основу лозинке, предност биометријских криптосистема је значајно отежано фалсификовање, копирање, крађа и дељење биометријских података у односу на лозинке [58].

Због биометријске промељивости (енгл. *biometric variance*), в. сл. 2.2, конвенционални биометријски системи извршавају такозвано расплинуто (енгл. *fuzzy*) поређење за дискриминацију легитимних и нелегитимних корисника. За разлику од њих, биометријски криптосистеми су дизајнирани тако да репродукују идентичне кључеве у фази аутентификације. Другим речима, излаз биометријског криптосистема може бити или кључ или порука о грешци.

Већина биометријских криптосистема захтева постојање ускладиштене јавне ин-



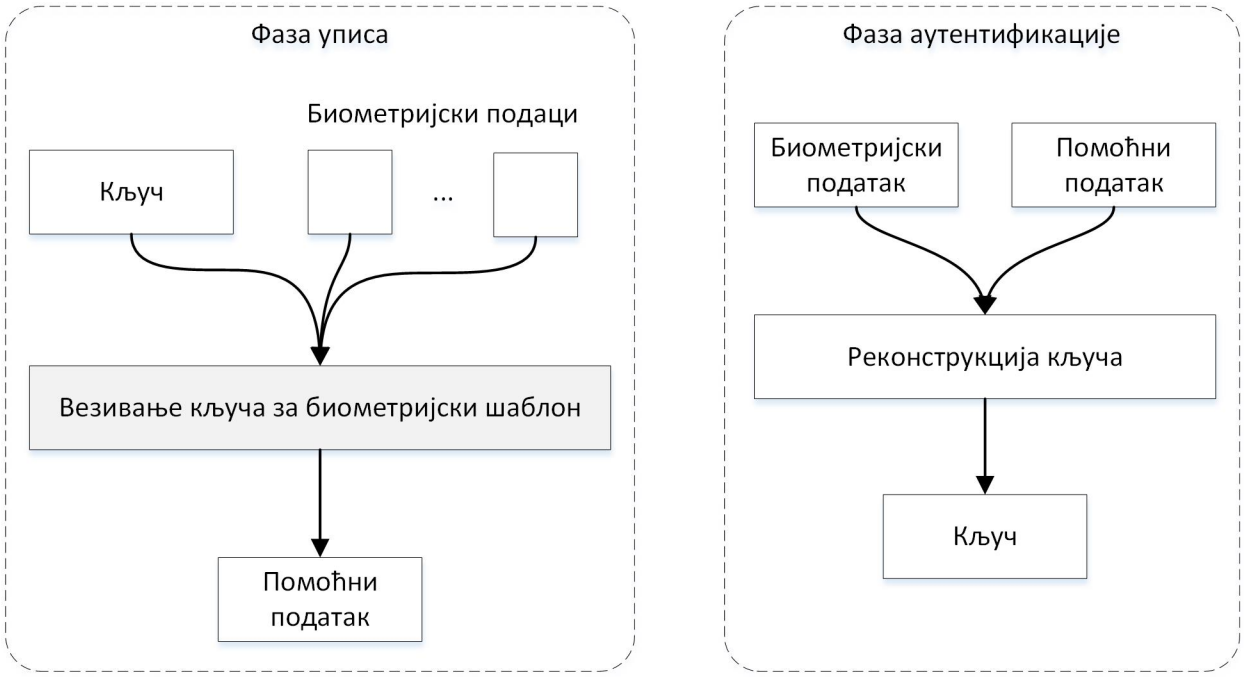
Слика 2.2: Два примера биометријске променљивости која се односе на отисак прста и дужицу. Слика преузета из [76]. Оригинални биометријски узорци су преузети из FCV (http://bias.csr.unibo.it/fvc2004/databases.asp) и CASIA (http://biometrics.idealtest.org/) база података биометријских узорака.

формације која је зависна од биометријског податка како би систем мога да репродукује или генерише кључ. Ова јавна информација, која се назива помоћни податак (енгл. *helper data*) не сме да открије значајнију количину информације о оригиналном биометријском податку или шаблону [60]. Због биометријске променљивости већина система ове класе није у могућности да репродукује или генерише криптографски кључ без помоћног податка. С обзиром да се биометријско поређење врши у шифрованом домену [59], биометријски криптосистеми се могу користити и као метода заштите биометријских шаблона [60].

На основу тога како се помоћни податак користи, биометријски криптосистеми се могу поделити у две класе:

- системи за везивње кључева за биометријски шаблон (енгл. *key binding systems*) и
- системи за генерисање кључева на основу биометријског шаблона (енгл. *key generation systems*).

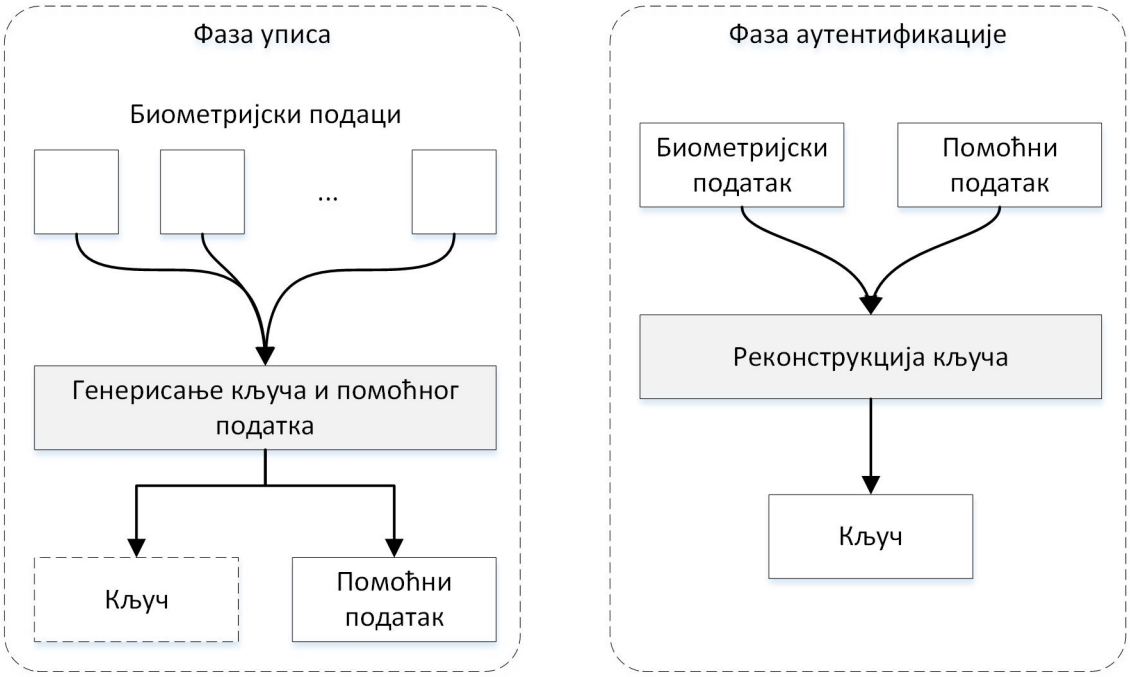
У системима за везивање кључева помоћни податак се генерише чврстим везивањем криптографског кључа за биометријски шаблон. Применом алгоритма за репродукцију, кључ се добија на основу помоћног податка у фази аутентификације [133]. С обзиром да су криптографски кључеви условно независни од биометријских обележја, то значи да је биометрија опозива, док замена кључа захтева фазу поновног уписа како би систем генерисао нови помоћни податак. Генеричка шема система за везивање кључева приказана је на сл. 2.3.



Слика 2.3: Генеричка шема система за везивање кључева.

У системима за генерисање кључева на основу биометријских података помоћни податак се генерише на основу биометријског шаблона, док се кључеви у фази аутентификације генеришу на основу помоћног податка и приложеног биометријског узорка [61]. Иако у овој класи система употреба помоћног податка није обавезна, већина система ове класе користи помоћни податак с циљем смањивања грешака. Осим тога, уколико систем не користи помоћни податак, могућност компромитовања корисника се увећава. Системи за генерисање кључева који користе помоћни податак се у литератури помињу као системи за расплинуто издвајање (енгл. *fuzzy extractors*) и сигурне скице (енгл. *secure sketches*) [36, 143]. Систем за расплинуто издвајање издваја униформно случајни низ из биометријског шаблона при чему се помоћни податак користи при реконструкцији. За разлику од тога, у шеми сигурне скице, помоћни податак се користи за издвајање оригиналног биометријског шаблона. Генеричка шема система за генерисање кључева на основу биометријског шаблона приказана је на сл. 2.4.

Као и конвенционални криптолошки кључеви, кључеви генерисани помоћу биометријских података (који се у литератури помињу и као „биометријски кључеви“) морају да испуне услове попут довољне количине случајности (тј. морају да задовоље статистичке тестове случајности), стабилности и јединствености [5, 6].



Слика 2.4: Генеричка шема система за генерисање кључева на основу биометријског шаблона.

Други начин класификације биометријских криптосистема је начин решавања проблема биометријске променљивости. Неке предложене шеме користе кодове за корекцију грешака (енгл. *Error Correction Codes*, ECC) [63, 64], док друге користе прилагодљиве филтре и корелацију [117] или квантизацију [42, 142].

Приликом мерења перформанси биометријских система у обзир се узимају грешка лажног одбијања, грешка лажног прихватања и једнака стопа грешке (енгл. *Equal Error Rate*, EER) [58, 61] која се дефинише као тачка пресека FRR и FAR кривих. У контексту биометријских криптосистема значење ових метрика се мења зато што системи нису засновани на расплинутом поређењу на основу прага — захтева се генерисање или репродукција идентичног кључа, док конвенционални биометријски системи доносе једноставну бинарну одлуку. Грешка лажног одбијања у биометријским криптосистемима дефинише се као однос кључева које систем није успео да генерише или репродукује за легитимне кориснике и укупан број покушаја легитимних корисника да од система добију кључ (исправан кључ је зависан од корисника и повезан са помоћним податком). По аналогији, грешка лажног прихватања формира се на основу броја исправних кључева који су испоручени нелегитимним корисницима. Имајући претходно поменуто у виду, као и резултате пријављене у релевантној

литератури, може се закључити да биометријски криптосистеми имају већу стопу грешке у односу на конвенционалне биометријске системе за аутентификацију [133]. Један од разлога за повећање стопе грешке је чињеница да биометријски криптосистеми не чувају биометријски шаблон након фазе уписа и самим тим не могу извршити поређење шаблона у бази и шаблона генерисаног у фази аутентификације. Додатно, већина биометријских криптосистема користи виши ниво квантизавије у фази издвајања обележја у односу на конвенционалне биометријске системе.

Један од првих приступа системима за везивање кључева предложили су Soutar и др. [118, 119, 120]. Предложени систем, назван Mytec2, је наследник система Mytec1 [117], првог биометријског криптосистема за који је показано да не задовољава минималне потребне услове који се односе на тачност и сигурност. Основа Mytec2 и Mytec1 алгоритама је механизам корелације.

Juels и Wattenberg [63] су 1999. године употребом техника из области кодова за корекцију грешака и криптографије формирали нову криптографску методу названу шема расплинутог везивања (енгл. *fuzzy commitment scheme*).

Примену шеме расплинутог везивања кодова дужице предложили су Hao и др. [51]. У њиховом предлогу, кодови дужице дужине 2048 бита су употребљени за везивање и репродукцију криптографских кључева дужине 140 бита, који су претходно обрађени Хадамардовим и Рид-Соломоновим кодовима за корекцију грешака. Хадамардови кодови су примењени како би се уклониле грешке које потичу од природне биометријске променљивости узорака, рок су Рид-Соломонови кодови употребљени како би се уклониле грешке настале изобличењем. Систем је тестиран на 700 слика дужице које потичу од 70 субјеката. Резултати експеримената указују на јако високу тачност и ниску стопу грешке која до тада није постигнута, или барем није пријављена у релевантној литератури.

Rathgeb и Uhl [95] представили су систематичан приступ конструкцији шеме расплинутог везивања која је примењена на дужицу. Након анализирања дистрибуције грешке између кодова дужица генерисаних различитим алгоритмима за препознавање, аутори примењују Рид-Соломонов и Хадамардов код за корекцију грешака (на сличан начин као што је описано у [51]). У истраживању описаном у [96] аутори примењују поуздан избор компоненти заснованих на контексту како би извукли кључеве из кодова дужица који су затим везани за Хадамардове кодне речи.

Различите технике за повећање перформанси система заснованих на дужици и шемама расплинутог везивања представљене су у [55, 140]. Бинарни кодови дужица су прикладни за примену у шемама расплинутог везивања, а поравнавање шаблона је изводљиво јер укључује само једнодимензионални кружни померај датог кода дужице.

Осим дужице, шема расплинутог везивања је примењивана и на друге биометријске модалитете уз неопходну бинаризацију издвојеног вектора обележја.

Друга значајна метода која се односи на биометријске криптосистеме, названа расплинути трезор (енгл. fuzzy vault), представљена је у [64], 2002. године. Clancy и др. [30] предложили су прву практичну и најочитију примену методе расплинутог трезора закључавањем карактеристичних тачака отиска прста (енгл. *minutiae points*) у такозваном „трезору отиска прста“.

Nandakumar и др. [85] предлажу да се као помоћни подаци користе тачке велике закривљености изведене из оријентационог поља отиска прста како би се помогао процес поравнања. У њиховом трезору отиска прста, кључеви дужине 128 бита су везивани и реконструисани. Uludag и Jain [134, 135] су предложили линијско представљање карактеристичних тачака отиска прста; перформансе система испитане су на тест скупу који садржи 450 парова отисака прстију. Неколико других присупа за побољшање поравнања у расплинутом трезору отиска прста предложени су у [137, 29, 71].

Иницијална идеја генерисања криптографских кључева директно из биометријских шаблона представљена је у патенту описаном у [13]. Имплементација ове шеме не постоји, а један од разлога који то објашњава је чињеница да већина биометријских модалитета не обезбеђује довољну количину информације за поуздано генерисање довољно дугог и стабилног кључа без употребе помоћних података.

У шеми приватног шаблона (енгл. *private template scheme*) заснованој на биометрији дужице, коју су предложили Davida и др. [34, 35] биометријски шаблон (или хеш вредност биометријског шаблона) користи се као кључ. Складиштење помоћних података, односно битова за исправљање грешака, је неопходно за корекцију неисправних битова датих кодова дужице.

У оквиру групе шема заснованих на квантизацији, помоћни подаци се генеришу тако да служе као помоћ при квантизацији биометријских обележја са циљем

добијања стабилних кључева. Детаљнија анализа шема квантизације дата је у [54]. Примене шема квантизације на биометрију лица, отисак прста и дужицу описане су у [122], [70] и [97], респективно.

2.2.2 Кратки осврт на сигурност биометријских криптосистема

Биометријска криптографија може значајно повећати сигурност биометријског система и приватност података који су ускладиштени у њему. Овакви системи су отпорнији на нападе вишег нивоа попут напада замене, маскирања, варања и надглашавања коначне одлуке на модулу за поређење. Системи засновани на биометријској криптографији могу функционисати у неповерљивој или мање поверљивој околини и мање су зависни од конретног хардвера, процедура и сигурносних полиса у односу на конвенционалне биометријске системе. Такође треба узети у обзир чињеницу да су кључеви знатно дужи у односу на кључеве који су генерисани на основу лозинки, те да корисници не морају да памте дугачке кључеве. Помоћни подаци су опозиви, попут шаблона генерисаних методама опозиве биометрије.

Међутим, у литератури је описан велики број напада који се могу успешно извршити на биометријске криптосистеме, попут расплинутих система издвајања. Један пример је напад на помоћне податке који се изводи помоћу базе података са сликама с циљем остваривања грешке лажног прихватања. Другим речима, неки биометријски криптосистеми могу бити рањиви на нападе ниског нивоа уколико је нападач упознат са алгоритмом и има приступ помоћним подацима (али не и легитимним биометријским узорцима). У том случају, циљ нападача је да дође до кључа (или да смањи простор претраге), да приступи легитимном биометријском шаблону или генерише лажну верзију истог.

2.2.3 Примена криптографије за заштиту биометријских узорака и шаблона

Обрада биометријских сигнала у шифрованом домену је један од начина за отклањање проблема који се односе на сигурност биометријских шаблона и приватност корисника. Међутим, треба узети у обзир да у великом броју конвенционалних

биометријских система за проверу идентитета нису имплементиране криптографске мере заштите. Једно време су извесни истраживачи чак сматрали да је немогуће извршити биометријску проверу идентитета у шифрованом домену због природне променљивости биометријских узорака и криптографске нетолеранције на неисправност једног бита података. Сходно томе, применом класичних метода шифровања, које не подразумевају извршавање операција у шифрованом домену, шифровани биометријски подаци морају бити дешифровани приликом аутентификације, што доводи до проблема који се односе на сигурност и приватност. Такође крађа кључа за дешифровање за последицу има компромитовање свих шаблона у бази.

Међутим, захваљујући могућностима које пружају такозване технике сигурног рачунања које извршава више ентитета (енгл. *Secure Multiparty Computation*, SMPC) могуће је упоредити два биометријска шаблона у шифрованом домену, односно извршити поређење користећи само шифроване податке. Осим тога, могуће је дизајнирати протокол поређења на такав начин да резултат поређења буде познат само ентитету коме је намењен без цурења информација о биометријском шаблону или субјекту на основу чијег узорка је шаблон генерисан. Овакве технике које омогућавају обраду шифрованих сигнала називају се обрада сигнала у шифрованом домену (*Signal Processing in the Encrypted Domain*, SPED).

Као пример, размотрићемо сценарио у којем је потребно да сервер добије информацију да ли је власник биометријског шаблона део листе уписаних субјеката који су легитимни корисници (на пример, корисници који могу приступити одређеном ресурсу) или криминалац чији је идентитет добро познат полицији или Федералном бироу за истраге. На серверу се налази база биометријских шаблона а корисник је заинтересован да искористи услугу без откривања свог идентитета. Алтернативно, потенцијални корисник може желети да сазна да ли његов биометријски сигнал одговара неком од шаблона који су смештени на серверу. Сходно скупу техника за обраду сигнала у шифрованом домену, претходно поменути захтеви су испуњиви, тј. све што је захтевано се може извести уколико се серверу дозволи да упореди приложен шаблон са шаблонима смештеним у бази података у шифрованом домену.

Два основна приступа обради сигнала у шифрованом домену су хомоморфно шифровање (енгл. *homomorphic encryption*) [104] и такозвана техника изопаченог пута (енгл. *garbled circuits*, GC) [138].

Хомоморфно шифровање обезбеђује начин за извршавање линеарних операција над шифрованим подацима. Међутим, када су у питању нелинеарне операције, потребно је прибећи интерактивним и обично сложеним протоколима. У скорије време, предложене су шеме потпуног хомоморфног шифровања (енгл. *Fully Homomorphic Encryption*, FHE) [44] које омогућавају извршавање било које финкције без интеракције укључених ентитета. На жалост, потпуно хомоморфног шифровање је за сада веома неефикасно, што је највећим делом последица величине јавног кључа.

Упркос знатним скорашњим достигнућима и новим ефикаснијим криптографским примитивама, протокол обраде сигнала у шифрованом домену је често исувише сложен како би се употребио у практичним доменима примене. Такође треба узети у чињеницу да је за сада непознато да ли се много бољи резултати могу добити развијањем класе алгоритама за које се изричито верује да олакшавају имплементацију техника обраде сигнала у шифрованом домену (на пример, разматрањем које су најсложеније операције које треба извести на сигуран начин и избегавањем истих).

Да би се сложеност смањила на прихватљив ниво, неопходно је да се приликом пројектовања алгоритама који обрађују биометријске податке и протокола који обрађује податке између два ентитета (енгл. *Secure Two-Party Computation*, STPC) узму у обзир како криптографски аспекти, тако и аспекти обраде сигнала. Међутим, најчешћи приступ до сада је супротан претходно поменутом захтеву: класичан биометријски алгоритам за поређење се једноставно претвара у протокол који ће се извршавати у шифрованом домену.

У основи, неопходно је да биометријски шаблони буду представљени вектором обележја константне дужине и да проста метрика (на пример, Хемингово или Еуклидско растојање) могу бити искоришћени за мерење сличности између два вектора. Уколико су претходна два услова испуњена, протокол за биометријску аутентификацију, односно верификацију корисника може се развити на једноставан начин, при чему ће се састојати од следећих блокова: рачунање растојања, одабир минимума и поређење са прагом [24, 23]. Приликом дизајнирања система такође треба узети у обзир чињеницу да ефикасност не зависи само од прикладног алгоритма за поређење, већ у обзир треба узети и количину информације у биометријском шаблону. Другим речима, сложеност система за обраду сигнала у шифрованом домену зависи од броја обележја које алгоритам за поређење користи као и од броја битова којима

су обележја представљена. Употребом мањег броја обележја или краћих обележја сложеност протокола се смањује, али се истовремено смањује и тачност препознавања због умањене количине информације која се пореди. То значи да је неопходно наћи компромис или обезбедити исправан дизајн система како се не би повећавала сложеност или деградирала ефикасност.

Криптографски систем се сматра хомоморфним [43] уколико су одређене операције над шифрованим подацима изводљиве и уколико одговарају операцијама изведеним над отвореним текстовима датих шифрата. Већина хомоморфних шифарских система се у основи ослања на криптографију са јавним кључем, при чему својство хомоморфности обезбеђује јавни кључ једног од ентитета који је део протокола. Другим речима, уколико другачије није назначено, претпоставља се да је приватни кључ познат једино клијенту, док сервер може да приступи само јавном кључу.

Најчешћи хомоморфини криптосистеми су адитивно хомоморфни (на пример, системи представљени у [88, 31]). Адитивно хомоморфни криптосистем дозвољава ентитету који је у поседу кључа за дешифровање да изврши шифровање суме две вредности које су једино њему доступне у шифрованом облику. Сложеније операције се могу извести уколико се прибегне интерактивном протоколу између сервера и клијента.

Упркос очигледној употребној вредности, коришћење хомоморфног шифровања је веома захтевно по питању рачунске сложености и простора потребног за складиштење. На пример, у Paillier-овом криптосистему, једноставне вредности представљене са неколико бита производе шифрат дужине 2.048 бита, што значи да се суме малих вредности мапирају на производе, односно да резултују веома дугачким шифратом. Нелинеарне операције, попут множења шифрованих вредности или поређења су још сложеније и захтевају интеракцију између ентитета. Због тога, комуникациона захтевност протокола заснованог на хомоморфном шифровању зависи од броја пренешених шифрата, као и од броја порука послатих у комуникацији, док рачунска сложеност зависи од броја рачунања експоненцијалних функција (које представљају рачунски најзахтевније операције) у протоколу.

Мултипликативни хомоморфни системи [104, 39] дозвољавају израчунавање производа две шифроване вредности, међутим, имају мању употребну вредност у односу на адитивне системе.

Један од првих радова у коме се помиње протокол за биометријску аутентификацију који штити приватност је [19]. Протокол није заснован на конкретном биометријском модалитету, већ на генералном биометријском представљању узорака помоћу бинарних низова. Након тога, у раду је представљена сигурна имплементација рачунања Хемингового растојања.

Имплементација биометријских идентификационих протокола који чувају приватност шаблона заснована на ејген-лицима [132] достиже тачност класификације 96% у случају промене осветљења, тачност класификације 85% уколико се у обзир узму и измене оријентације лица и 64% уколико се мења и величина лица. За разлику од већине биометријских протокола за препознавање заснованих на обради сигнала у шифрованом домену, у овом приступу се издвајање обележја такође изводи у шифрованом домену ослањајући се на својства Paillier-овог криптосистема [88]. Рачунање квадрата Еуклидовог растојања имплементирано је такође употребом Paillier-овог криптосистема, док је протокол за поређење имплементиран сходно приступу који су представили Damgard и др. [31]. Међутим, просечно време потребно за препознавање лица износи око 40 секунди. Аутори наводе да је могуће смањити рачунску сложеност и комуникациону захтевност под претпоставком да су параметри који се користе у протоколу за издвајање обележја јавни. Ова претпоставка је усвојена у већини радова у којима су описана истраживања из дате области.

Истраживања везана за хомоморфно шифровање и препознавање дужице спровели су Luo и др. [72] тако што су имплементирали протокол за биометријску аутентификацију заснован на коду дужице [33] и верификовали резултате на CASIA Iris бази података биометријских узорака — конкретно на 100 шаблона величине 9.600 бирова. Резултујућем протоколу је потребно око 27 минута у просеку да обради захтев на рачунару са процесором чији је радни такт 2,4 GHz. Ову комплексност аутори оправдавају величином кодова дужице који су шифровани Paillier-овим криптосистемом.

Bringer и др. [21, 20], Schoenmakers и Tuyls [108], и Upmanyu и др. [136] такође су предложили употребу хомоморфног шифровања у биометријским системима за аутентификацију у којима је очувана приватност корисника. Аутори су размотрили следеће хомоморфне криптосистеме: Goldwasser-Micali, Paillier, ElGamal и RSA. Аутори су такође установили да су криптографски алгоритми који поседују својство

хомоморфности најпогоднији за поређење шаблона уколико се у шифрованом домену извршавају једноставне операције (на пример, операција ексклузивно ИЛИ над два бинарна низа). У том смислу, аутори сматрају да је ова врста заштите шаблона погодна у системима за препознавање дужице који користе бинарни шаблон дужине 2048 bita.

Другачији приступ је представљен у [10]. Аутори су користили хибридни приступ за биометријску идентификацију (хомоморфно шифровање и технику изопаченог пута) за биометријску идентификацију који је оптипизован and optimize it by пред-рачунањем већине операција. Даља унапређења се своде на оптимизацију протокола за множење и употребом Damgard-Geisler-Kroigard методе [31] за израчунавање сличности. Имплементација протокола је тестирана, а остварени резлтати указују на 25% повећања у брзини у односу на идентичан протокол који користи само хомоморфно шифровање. Сходно наводима аутора, поређење два шифрована кода дужице дужине 2.048 bita траје само 0,15 секунди.

Протокол описан у истраживању објављеном у [73] извршен на процесору са радним тактом од 3GHz употребљен је за поређење кодова дужице генерисаних на основу CASIA Iris базе података дужине 9.600 и 2.048 битова. Захваљујући пред-обради, односно унапред обављеним израчунавањима, поређење два кода дужице дужине 2.048 битова траје 0,56 секунди уз пренос 571 килобајта података, док поређење кодова величине 9.600 битова траје 2,5 секунди и захтева пренос 2,655 килобајта података.

Узевши у обзир чињеницу да претходно поменути протоколи користе векторе фиксне дужине, већина шема предложених за поређење отисака прста засноване су на такозваним кодовима прстију (енгл. fingercodes) [56]. На пример, у истраживањима која су спровели Barni и др. [7, 8] имплементиран је идентификациони протокол заснован на Paillier-овом криптосистему. Извршавање протокола над базом која садржи 64 идентитета траје око 16 секунди на рачунару са процесором чији је радни такт 2,4 GHz.

Истраживања у области препознавања отисака прстију, у којима су употребљени слични протоколи који су коришћени за препознавање дужице, описана су у [10]. Сходно [7], имплементација заснована на кодовима прстију је 35 пута бржа (извршавање на клијенту траје око 0,35 секунди, док на серверу траје око 0,45 секунди).

Протокол је такође прилагођен за рад са карактеристичним тачкама отисака прстију [81] (резултати пријављени у [56] указују на чињеницу да је FAR мањи од 1%), али је време извршавања знатно увећано.

Повећањем популарности шема потпуног хомоморфног шифровања за последицу има и дизајн неколико потпуно неинтерактивних решења за очување приватности у биометријским системима за аутентификацију. Први неинтерактивни протокол за биометријску аутентификацију [129] заснован је на проширењу решења представљеног у [45]. Сва израчунавања, осим шифровања улаза и дешифровања резултата, обављају се на серверу.

Рачунска сложеност се значајно смањује у односу на Pailler-ов криптосистем. На пример, имплементација представљена у [129] захтева 59 секунди за верификацију лица, док је 420 секунди потребно за верификацију на еквивалентној имплементацији заснованој на Paillier-овом криптосистему. Додатна предност је елиминисање интеракције између ентитета. Негативна последица употребе проширења решења представљеног у [45] је повећање комуникационе захтевности: имплементација представљена у [129] захтева пренос 393 MB података, док је само 16,4 MB потребно за верзију засновану на Paillier-овом криптосистему.

Иако су истраживања која се односе на ефикасност, односно смањивање сложености привукло пажњу истраживача, већина истраживања је усмерена на ефикасније примитиве протокола који обрађује податке између два ентитета и њихову примену у конвенционалним биометријским системима за поређење у оквиру радног оквира за обраду сигнала у шифрованом домену. Постоје извесне претпоставке да се значајна унапређења могу остварити истраживањима на нивоу обраде сигнала, као и на заједничком разматрању криптографских аспеката и аспеката обраде сигнала.

Глава 3

Теоријске основе истраживања

3.1 Криптографија са јавним кључевима

Криптографија са јавним кључевима подразумева коришћење два кључа (K_e, K_d) [114]. Кључ K_e је јавни, и користи се за шифровање, а кључ K_d је тајни, и користи се за дешифровање. Примена криптографије са јавним кључевима се може описати на следећи начин. Нека субјекат B поседује пар кључева (K_e^B, K_d^B). Свако може да пошаље поруку M субјекту B тако што ће је шифровати јавним кључем K_e^B:

$$C = E(M, K_e^B) \ , \tag{3.1}$$

при чему само B може да дешифрује C, користећи тајни кључ K_d^B:

$$M = D(C, K_d^B) \ . \tag{3.2}$$

Осим тога, субјекат B може дигитално да потпише поруку тако што ће је шифровати својим тајним кључем K_d^B. Тада свако може да верификује овај дигитални потпис дешифровањем поруке помоћу јавног кључа K_e^B. Коначно, трећа примена се односи на размену симетричних кључева. У наставку је описан алгоритам RSA за криптографију са јавним кључевима.

3.1.1 Алгоритам RSA

Најпознатији алгоритам за криптографију са јавним кључевима, RSA [104, 114], базира се на следећој једносмерној функцији са замком[1] (енгл. trapdoor function).

[1] Једносмерне функције са замком су дефинисане у секцији 3.4.1.

Нека су p и q два изабрана велика проста броја, на основу којих се одређују следеће вредности: (а) модул n, као производ:

$$n = pq \ , \tag{3.3}$$

(б) експонент за шифровање e, као изабрани цели број из опсега $[1, (p-1)(q-1)-1]$ који је узајамно прост са $(p-1)(q-1)$, што ћемо обележавати:

$$(e, (p-1)(q-1)) = 1 \ , \tag{3.4}$$

и (в) експонент за дешифровање d, тако да важи:

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

Уређени пар (n, e) представља јавни кључ, а број d приватни кључ. Пре шифровања, порука M се дели на секвенцу блокова $M_1, M_2, \ldots, M_b$, од којих је сваки представљен целим бројем из опсега $[0, n-1]$. Поступак шифровања блока M_i, за $1 \leq i \leq b$ је:

$$C_i = M_i^e \pmod{n} \ , \tag{3.6}$$

а дешифровања:

$$M_i = C_i^d \pmod{n} \ . \tag{3.7}$$

Да бисмо објаснили ове поступке, искористићемо Ојлерову функцију, Ојлерову теорему, и њен слецијални случај — Фермаову теорему [47, 52, 114].

Дефиниција 1. Ојлерова функција: Вредност Ојлерове функције $\varphi : \mathbb{N} \to \mathbb{N}$ за дати број n једнака је броју позитивних целих бројева који су мањи од n и узајамно прости са n:

$$\varphi(n) = |\{e | e \in \{1, 2, \ldots, n-1\} \wedge (e, n) = 1\}| \ . \tag{3.8}$$

Лема 1. *Нека је p прост број. Тад важи:*

$$\varphi(p) = p - 1 \ . \tag{3.9}$$

Доказ. По дефиницији Ојлерове функције, није могуће да важи $\varphi(p) > p-1$. Ако би важило $\varphi(p) < p-1$, то би значило да постоји број $1 < x < p$ такав да је p дељив са x, што је немогуће, јер је p прост број. Закључујемо да је $\varphi(p) = p-1$. □

Ојлерова функција је мултипликативна, тј., за узајамно просте бројеве m и n важи:

$$\varphi(mn) = \varphi(m)\varphi(n) \ . \tag{3.10}$$

За потребе овог излагања биће довољно да покажемо да једнакост (3.10) важи кад су m и n прости бројеви.

Лема 2. *Нека су бројеви p и q прости бројеви, и $p \neq q$. Тад важи:*

$$\varphi(pq) = (p-1)(q-1) \ . \tag{3.11}$$

Доказ. Полазећи од поставке да су p и q прости бројеви, скуп целих бројева из опсега $[1, pq-1]$ који нису узајамно прости са pq једнак је

$$S = S_p \cup S_q \ , \tag{3.12}$$

где су:

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

при чему се лако показује да $S_p \cap S_q = \emptyset$, односно $|S| = |S_p| + |S_q| = p+q-2$. Одатле следи:

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

□

Теорема 3. *Ојлерова теорема: Нека су n и a узајамно прости природни бројеви. Тада важи:*

$$a^{\varphi(n)} = 1 \pmod{n} \ . \tag{3.15}$$

Доказ. За дато n, нека скуп $X = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$ садржи све различите природне бројеве мање од n који су узајамно прости са n:

$$(\forall \ 1 \leq i \leq \varphi(n)) \ (ax_i, n) = 1 \ . \tag{3.16}$$

Пошто су a и $x_i \in X$ узајамно прости са n, тада и производ ax_i мора бити узајамно прост са n. У супротном, када би важило да ax_i и n нису узајамно прости, то би значило да један од бројева a и x_i није узајамно прост са n, што је контрадикција.

Такође, важи и:

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

Кад би важило $ax_i = ax_j \pmod{n}$, тада би разлика $ax_i - ax_j$ морала бити дељива са n, што је контрадикција.

Имајући у виду (3.16) и (3.17), лако се показује да је скуп остатака бројева $\{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$ при дељењу са n једнак скупу X. Даље имамо:

$$\begin{aligned} &\prod_{i=1}^{\varphi(n)} ax_i = \prod_{i=1}^{\varphi(n)} x_i \pmod{n} \\ \Leftrightarrow\; &a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i = \prod_{i=1}^{\varphi(n)} x_i \pmod{n} \\ \Leftrightarrow\; &a^{\varphi(n)} = 1 \pmod{n}\,. \end{aligned} \tag{3.18}$$

Тиме је доказ Ојлерове теореме завршен. □

Теорема 4. *Фермаова теорема: Нека су p прост број, и a цели број. Тада важи:*

$$a^p = a \pmod{p}\,. \tag{3.19}$$

Доказ. По Ојлеровој теореми (теорема 3) важи:

$$a^{\varphi(p)} = 1 \pmod{p}\,, \tag{3.20}$$

а по леми 1:

$$\varphi(p) = p - 1\,. \tag{3.21}$$

Даље следи:

$$\begin{aligned} &a^{\varphi(p)} = 1 \pmod{p} \\ \Leftrightarrow\; &a^{p-1} = 1 \pmod{p} \\ \Leftrightarrow\; &a^p = a \pmod{p}\,. \end{aligned} \tag{3.22}$$

Овим је доказ теореме завршен, а у наставку излагања ћемо се позвати на једнакост $a^{p-1} = 1 \pmod{p}$. □

Теорема 5. *Под условима дефинисам ставкама (3.3), (3.4), (3.5) и (3.6), важи:*

$$M_i = C_i^d \pmod{n} . \tag{3.23}$$

Доказ.

$$\begin{aligned}
& M_i = C_i^d \pmod{n} \\
\Leftrightarrow\ & M_i = M_i^{ed} \pmod{n}, && \leftarrow \text{(в. једнакост (3.6))} \\
\Leftrightarrow\ & M_i = M_i \cdot M_i^{ed-1} \pmod{n} \\
\Leftrightarrow\ & M_i = M_i \cdot M_i^{k\varphi(n)} \pmod{n}, && \leftarrow \text{(в. једнакост (3.5))} \\
\Leftrightarrow\ & M_i = M_i \cdot M_i^{k\varphi(pq)}, && \leftarrow \text{(в. једнакост (3.3))} \\
\Leftrightarrow\ & M_i = M_i \cdot M_i^{k(p-1)(q-1)}, && \leftarrow \text{(в. лему 2)} \\
\Leftrightarrow\ & M_i = M_i \cdot 1^k \pmod{n}, && \leftarrow \text{(в. теорему 4)} \\
\Leftrightarrow\ & \top .
\end{aligned}$$

□

Једносмерна функција са замком која се примењује у алгоритму RSA је:

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

где важи $(l, \varphi(n)) = 1$. Ваља приметити да се тајност алгоритма RSA базира на тежини факторисања броја $n = pq$. Због тога се фактори p и q (из једнакости (3.3)) заменарују након израчунавања вредности n [47, 52, 114].

3.1.2 Бинарно потенцирање

Као пример извршавања алгоритма RSA, узмимо да су $p = 5$ $q = 11$. Тада је модул $n = pq = 55$. Експонент за шифровање се бира тако да буде узајамно прост са $(p-1)(q-1) = 40$, а експонент за дешифровање се бира тако да важи $ed = 1 \pmod{40}$. Нека су $e = 3$ и $d = 27$. Јавни кључ је $(55, 3)$, а приватни 27. Шифровањем поруке $M = 4$ добија се шифрат $C = M^e \pmod{n} = 4^3 \pmod{55} = 9$, а његовим дешифровањем почетна порука $M = C^d \pmod{n} = 9^{27} \pmod{55} = 4$.

У горњем примеру, јавља се вредност $9^{27} \pmod{55}$. Њено израчунавање простим степеновањем пре дељења по модулу није практично, јер даје непотребно велики број ($\approx 5.8149737 \cdot 10^{25}$). Овај проблем је још израженији у реалним применама, у којима

модул n заузима не мање од 1024 бита. Због тога, примењује се метода бинарног потенцирања.

Ову методу ћемо приказати на примеру израчунавања вредности $7^{18} \pmod{33}$. Вредност експонента 18 у бинарном запису је 10010. Ако бисмо овај бинарни број генерисали бит по бит, почевши од најзначајнијег бита, секвенца бинарних вредности би гласила:

$$0, 1, 10, 100, 1001, 10010 \; . \tag{3.25}$$

а секвенца одговарајућих декадних вредности:

$$0, 1, 2, 4, 9, 18 \; . \tag{3.26}$$

Из последње секвенце се може утврдити следећи начин за генерисање експонента 18:

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

Поступак израчунавања вредности $7^{18} \pmod{33}$ се изводи на следећи начин:

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

У општем сличају, вредности које се израчунавају у овом постуку нису веће од n^3, чиме је избегнуто израчунавање непрактично великих вредности.

3.2 Генератори псеудослучајних бројева

Генератори псеудослучајних бројева су детерминистички програми који као улазни параметар прихватају кратку секвенцу битова x и генеришу дугачку секвенцу

Табела 3.1: Изабрани генератори псеудослучајних бројева (табела прилагођена из [47]).

Име	Једносмерна функција са замком f	Комплексност израчунавања:	
		f	j-тог бита
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]	$exp(p, q, x)$	k^3	jk^3
Blum/Blum/Shub [11]	$x_{k+1} = x_k^2$	k^2	$max(k^2 \log j, k^3)$

битова y, која изгледа као да је случајно генерисана. Улазни параметар називамо кључем, а резултат генерисања псеудослучајном секвенцом битова. Генерисана секвенца y је псеудослучајна, јер скуп секвенци које је могуће генерисати не обухвата све могуће секвенце, тј., број секвенци које је могуће генерисати је мањи од или једнак броју могућих кључева x [47].

Да би се постигао задовољавајући ниво сигурности, секвенца y мора да буде таква да ако је нападачу познат део секвенце, он не може да предвиди остале делове секвенце, ни почетни кључ x. Генератор псеудослучајних бројева се сматра сигурним ако вероватноћа предвиђања следећег бита на основу префиксне секвенце битова није већа од вероватноће случајног погађања [12]. Овакви генератори су перфектни у смислу да вероватноћа да ће алгоритам који се извршава у полиномном времену погодити да ли је секвенца дужине k случајно изабрана из скупа $\{0,1\}^k$ или генерисана није значајно већа од 0.5 [**?**], тј. задовољава све статистичке тестове који се извршавају у полиномном времену.

Изабрани генератори псеудослучајних бројева дати су у табели 3.1.

3.2.1 Основни појмови

У наставку ћемо формално дефинисати релевантне појмове [47].

Дефиниција 2. Нека су X_n и Y_n расподеле вероватноће над скупом $\{0,1\}^n$. Кажемо да се $\{X_n\}$ не може разликовати у полиномном времену од $\{Y_n\}$ ако за сваки алгоритам са полиномним временом извршавања A, и сваки полином Q, постоји n_0 такво да за свако $n > n_0$ важи:

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

Дефиниција 3. Расподела $\{X_n\}$ је псеудослучајна ако се не може разликовати у полиномном времену од униформне расподеле $\{U_n\}$, тј., ако за сваки алгоритам са полиномним временом извршавања A, и сваки полином Q, постоји n_0 такво да за свако $n > n_0$ важи:

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

Дефиниција 4. Детерминистички програм $G : \{0,1\}^k \to \{0,1\}^{\hat{k}}$ са полиномним временом извршавања је генератор псеудослучајних бројева ако важи:

- $\hat{k} > k$,
- $\{G_{\hat{k}}\}_{\hat{k}}$ је псеудослучајна расподела, где је $G_{\hat{k}}$ расподела над скупом $\{0,1\}^{\hat{k}}$ добијена на следећи начин:
  - изабере се $x \in U_k$, где је U_k униформна расподела над скупом $\{0,1\}^k$,
  - додели се вредност $t = G(x)$.

тј., ако за сваки алгоритам са полиномним временом извршавања A, сваки полином Q, и за свако довољно велико k важи:

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

Алгоритам са полиномним временом извршавања A, који се спомиње у горњим дефиницијама, назива се статистичким тестом. Један од статистичких тестова је тест следећег бита.

Дефиниција 5. Генератор псеудослучајних бројева задовољава тест следећег бита A ако за сваки полином Q постоји k_0 такво да за свако $\hat{k} > k_0$ и $p < \hat{k}$ важи:

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

Овде наводимо следећу теорему без доказа (доказ је дат у [47]).

Теорема 6. *G задовољава све тестове следећег бита ако и само ако G задовољава све статистичке тестове.*

Табела 3.2: NIST тестови за проверу случајности произвољно дугачких бинарних секвенци [106].

Бр.	Тест
1.	Испитивање учесталости у низу
2.	Испитивање учесталости у блоку
3.	Испитивање узастопног понављања истих битова у низу
4.	Испитивање најдужег узастопног понављања јединица у n-битним блоковима
5.	Испитивање стања бинарне матрице
6.	Тест заснован на дискретној Фуријеовој трансформацији
7.	Испитивање непреклапајућих узорака
8.	Испитивање преклапајућих узорака
9.	Мауреров универзални статистички тест
10.	Испитивање линеарне сложености
11.	Испитивање учесталости свих могућих преклапања n-битних поднизова
12.	Испитивање приближне ентропије
13.	Испитивање кумулативних збирова
14.	Испитивање случајне дигресије
15.	Испитивање случајне променљиве дигресије

3.2.2 Испитивање приближне ентропије

Преглед NIST тестова за проверу случајности произвољно дугачких бинарних секвенци [106] дат је у табели 3.2, а овде ће се детаљније размотрити један од њих: испитивање приближне ентропије.

Једна од претпоставки за тестирање генератора псеудослучајних бројева је да две случајне променљиве које имају исту расподелу вероватноће, имају и исту меру неодређености [128]. Као мера неодређености користи се појам ентропије [110]. Ентропија случајне променљиве $X = \{x_1, x_2, \ldots, x_n\}$ се дефинише:

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

Основна идеја испитивања приближне ентропије је следећа [105]. Нека је $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ секвенца независних и једнако расподељених случајних вредности. Узмимо да су:

$$Y_i(m) = (\epsilon_i, \ldots, \epsilon_{i+m-1}) \ \text{ за } \ 1 \leq i \leq n - m + 1 \ , \tag{3.34}$$

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

и

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

Приближна ентропија $ApEn$ реда m дефинисана је са:

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

при чему је:

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

Мале вредности $ApEn(m)$ имплицирају снажну правилност у секвенци, док велике вредности $ApEn(m)$ имплицирају флуктуацију у секвенци. Може се показати да важи:

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

и

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

где је s број различитих вредности које ϵ_i може да узме. Због особине исказане у једнакости (3.40), аналитички докази асимптотског понашања и процењених варијанси приближне ентропије су екстремно тешки [105]. Због тога се уводи нова дефиниција за $\Phi^{(m)}$:

$$\tilde{\Phi}^{(m)} = \sum_{i_1 \ldots i_m} \nu_{i_1 \ldots i_m} \log v_{\nu_{i_1 \ldots i_m}} \ , \tag{3.41}$$

У овој дефиницији, $\nu_{i_1 \cdots i_m}$ представља релативну учесталост узорка $i_1 \ldots i_m$ у циркуларном стрингу:

$$(\epsilon_1, \ldots, \epsilon_n, \epsilon_1, \ldots, \epsilon_{m-1}) \ , \tag{3.42}$$

тј.:

$$\nu_{i_1 \ldots i_m} = \frac{\omega_{i_1 \ldots i_m}}{n} \ , \tag{3.43}$$

и важи:

$$\sum_{i_1 \ldots i_m} \nu_{i_1 \ldots i_m} = n \ . \tag{3.44}$$

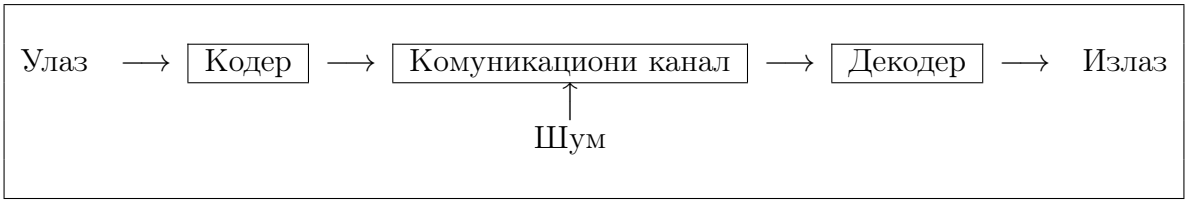
Сада је приближна ентропија дефинисана са:

$$Ap\widetilde{En}(m) = \tilde{\Phi}^{(m)} - \tilde{\Phi}^{(m+1)} \ . \tag{3.45}$$

Предност $Ap\widetilde{En}(m)$ у односу на $ApEn(m)$ је што за $Ap\widetilde{En}(m)$ важи:

$$(\forall m) \ \log s \geq Ap\widetilde{En}(m) \ , \tag{3.46}$$

што није случај за $ApEn(m)$. Са порастом n, разлика између $Ap\widetilde{En}(m)$ и $ApEn(m)$ постаје мања. У [105] је показано да приближне ентропије $Ap\widetilde{En}(m)$ и $ApEn(m)$



Слика 3.1: Илустрација модела комуникационог канала са заштитним кодерима.

конвергирају у расподели ка случајној променљивој χ^2 када је m фиксно или тежи бесконачности. То омогућава да се концепт приближне ентропије примени на статистички тест случајности секвенце. За дато $ApEn(m)$, $\chi^2(obs)$ се дефинише као:

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

а P-вредност се израчунава у складу са:

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

где $\mathbb{P}$ означава некомплетну гама-функцију [105].

Ако је P-вредност мања од $0,01$, сматра се да секвенца није случајна. У супротном, сматра се да је секвенца случајна. За практичне примене овог теста, саветује се да избор параметара n и m буде такав да важи $m < \lfloor \log n \rfloor - 5$ (в. [106]).

3.3 Кодери и интерливери

3.3.1 Заштитни кодери

Деловање шума у каналу за пренос података утиче на поузданост преноса (модел комуникационог канала са шумом илустрован је на сл. 3.1). Заштитни кодери су намењени исправљању грешака насталих услед шума, тј., свођењу вероватноће грешке на произвољно малу вредност [84].

Уведимо основне појмове који су значајни за даље излагање [84]:

- Разлика између две бинарне кодне речи исте дужине се може дефинисати помоћу операције екслузивне дисјункције, $x_i \veebar x_j$, што одговара аритметици по модулу 2.

- Хемингово растојање између две бинарне кодне речи исте дужине, $d(x_i, x_j)$ се дефинише као број позиција у којима се речи разликују.

- Тежина бинарне кодне речи, $w(x_i)$, се дефинише као број јединица у речи.

Лако се показује да за две бинарне кодне речи исте дужине, x_i и x_j, важи:

$$d(x_i, x_j) = w(x_i \veebar x_j) \ . \tag{3.49}$$

Нека је x реч која је саопштена каналу, и $\hat{x}$ испоручена реч. Број грешака насталих током преноса речи x једнак је тежини разлике речи x и $\hat{x}$, а тиме и Хеминговом растојању између ове две речи. Проблем исправљање грешака насталих у преносу, у условима када кодна реч x није позната, може се свести на минимизовање тежине $w(x_i \veebar x_j)$, односно Хеминговог растојања $d(x_i, x_j)$. За дати код C, декодована реч $D(\hat{x})$ се одређује као реч која је најближа, у смислу Хеминговог растојања, речи $\hat{x}$:

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

Са друге стране, декодована реч $D(\hat{x})$ се може одредити као реч која максимизује вероватноћу $P(x|\hat{x})$. У бајесовском контексту, то све своди на [84]:

$$D(\hat{x}) = \underset{x \in C}{\operatorname{argmax}}\, P(x|\hat{x}) \tag{3.51}$$

$$\underset{x \in C}{\operatorname{argmax}}\, \frac{P(\hat{x}|x)P(x)}{P(\hat{x})} \tag{3.52}$$

$$\underset{x \in C}{\operatorname{argmax}}\, P(\hat{x}|x)P(x) \ . \tag{3.53}$$

Под претпоставком да је вероватноћа $P(x)$ константна, имамо:

$$D(\hat{x}) = \underset{x \in C}{\operatorname{argmax}}\, P(\hat{x}|x)P(x) \tag{3.54}$$

$$= \underset{x \in C}{\operatorname{argmax}}\, P(\hat{x}|x) \ . \tag{3.55}$$

Ако претпоставимо и да сви битови имају исту вероватноћу грешке, једнаку p, добија се:

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

Заштитни кодери се могу поделити у две групе: линеарни кодери и конволуциони кодери. Размотрићемо примере из обе групе.

3.3.1.1 Пример линеарног заштитног кодера

Пример из прве групе је бинарни Хемингов код $(2^k-1, 2^k-k-1)$, који је намењен исправљању вектора који садрже само једну грешку. Верификациона матрица за овај код је [84]:

$$H_{k\times 2^k-1}(k) = \begin{bmatrix} b(1,k)^T & b(2,k)^T & \dots & b(2^k-1,k)^T \end{bmatrix}, \tag{3.57}$$

где $b(i,k)$ представља бинарни запис броја i, дужине k.

Хемингов код ћемо илустовати за случај $k=3$. Верификациона матрица је:

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

Генераторску матрицу $G_{4\times 7}$ налазимо тако да задовољава:

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

Једно од решења је:

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

Нека порука која треба да се пренесе преко комуникационог канала има вредност:

$$l_{1\times 4} = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}. \tag{3.61}$$

Њеним множењем са генераторском матрицом $G_{4\times 7}(3)$ добија се кодна реч:

$$x_{1\times 7} = l_{1\times 4} \times G_{4\times 7}(3) = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \tag{3.62}$$

Претпоставимо да се током преноса поруке десила грешка на четвртом биту, тј., да је испоручена порука:

$$\hat{x}_{1\times 7} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{3.63}$$

Да би се ова грешка открила, испоручена порука се множи са $H_{3\times 7}(3)^T$, а резултат индикује позицију бита на коме се десила грешка. У посматраном примеру имамо:

$$\hat{x}_{1\times 7} \times H_{3\times 7}(3)^T = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}, \tag{3.64}$$

тј., детектована је грешка на четвртој ($100_2 = 4_{10}$) позицији испоручене поруке.

3.3.1.2 Пример конволуционог заштитног кодера

Нека је:

$$l = l_1, l_2, \ldots, l_n \tag{3.65}$$

вредност поруке која треба да се пренесе преко комуникационог канала. Конволуциони кодер кодује ову поруку у (в. [84]):

$$x = x_1, x_2, x_3, x_4, \ldots, x_{2n-1}, x_{2n} \ , \tag{3.66}$$

где важи:

$$x_{2i-1} = l_i + l_{i-2} \ , \tag{3.67}$$

$$x_{2i} = l_i + l_{i-1} + l_{i-2} \ , \tag{3.68}$$

$$l_0 = 0 \ , \tag{3.69}$$

$$l_{-1} = 0 \ . \tag{3.70}$$

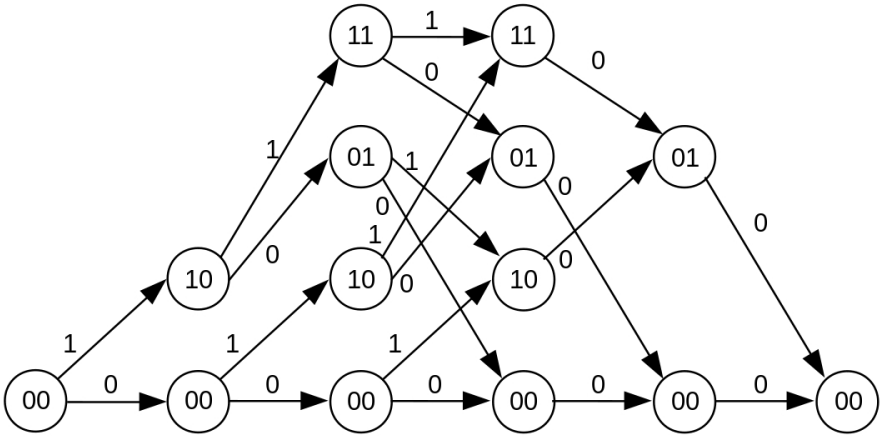
За поруку дужине три бита, генераторска мартрица је:

$$G_{3\times 10}(3) = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \ . \tag{3.71}$$

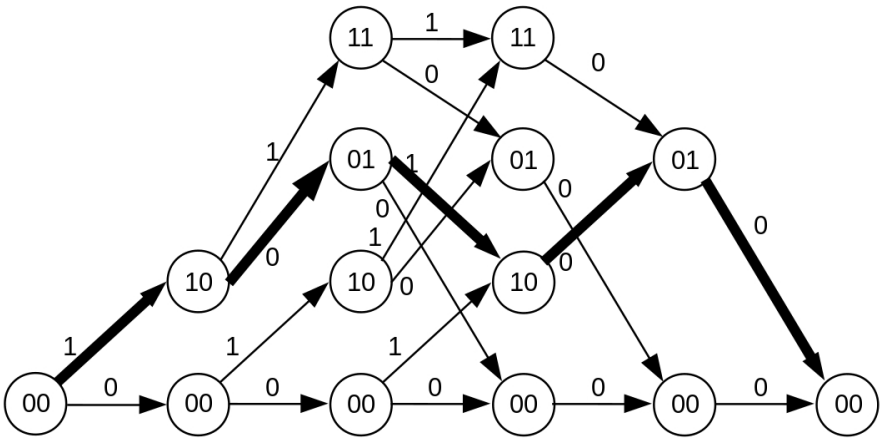
Међутим, рад оваквог кодера се може представити Марковљевим ланцем, у коме су стања дефинисана скупом:

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

што значи да кодовање сваке поруке представља путању кроз Витербијев трелис [65]. За посматрани пример поруке дужине три бита, на коју додајемо две нуле (због (3.69) и (3.70)), Витербијев трелис је дат на сл. 3.2. Број колона у трелису је одређен дужином поруке, а у две колоне које претходе последњем чвору, излазне гране се односе само на додате нуле. Путања кроз Витербијев трелис која одговара почетној поруци 101, на коју се додају још две нуле (10100), дата је на сл. 3.3. Декодовање почетне поруке се своди на одређивање највероватније путање кроз трелис, што се може извршити применом Витербијевог алгоритма [65].



Слика 3.2: Илустрација Витербијевог трелиса (слика прилагођена из [84]).



Слика 3.3: Илустрација декодовања почетне поруке на основу Витербијевог трелиса (слика прилагођена из [84]).

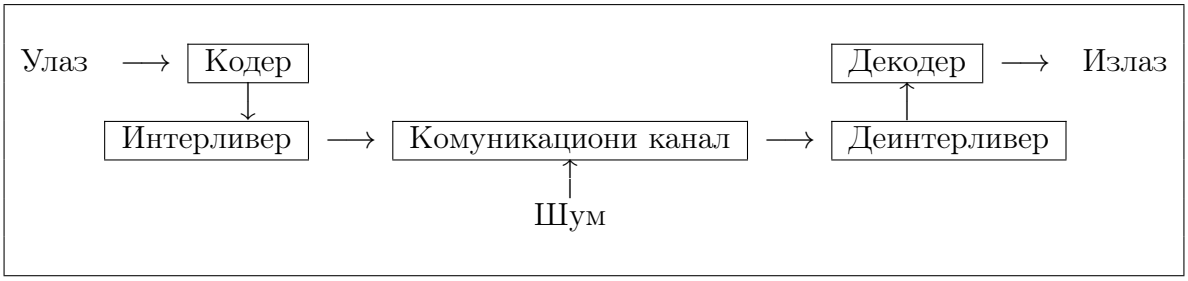
3.3.2 Интерливери

Горе смо размотрили пример бинарног Хемингговог кода који може да коригује векторе који садрже само једну грешку. Међутим, у комуникационом каналу се могу генерисати и пакетске грешке. Њихова корекција се врши применом интерливера, а модел комуникационог канала је илустрован на сл. 3.4 (в. [84]).

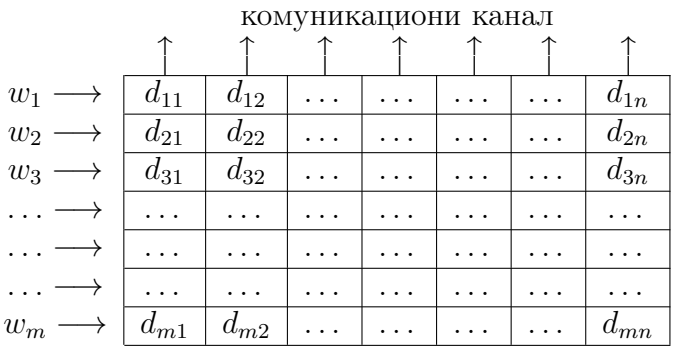
Две главне групе интерливера су: блоковски интерливери и конволуциони интерливери. Размотрићемо примере из обе групе.

3.3.2.1 Пример блоковског интерливера

Блоковски интерливер подразумева генерисање блока података димензија $m \times n$. У овај блок се учитава m кодних речи, $w_1, w_2, \ldots, w_m$, по врстама, при чему свака



Слика 3.4: Илустрација модела комуникационог канала са заштитним кодерима и интерливерима.



Слика 3.5: Илустрација блоковског интерливера.

реч има дужину n. Учитани блок података се затим по колонама шаље кроз комуникациони канал са шумом, као што је илустровано на сл. 3.5. Пренесени подаци се инверзно преузимају кроз блок података, пре него што се декодују [113].

Ако се у комуникационом каналу генеришу пакетске грешке, блоковски интерливер ће их распоредити по коднм речима. Да бисмо илустровали ову технику, претпоставимо да важи $m = 3$ и $n = 4$, и посматрајмо секвенцу битова дужине $mn = 12$, која је преузета са излаза кодера:

$$\underbrace{w_1[1], w_1[2], w_1[3], w_1[4]}_{\text{реч } w_1}, \underbrace{w_2[1], w_2[2], w_2[3], w_2[4]}_{\text{реч } w_2}, \underbrace{w_3[1], w_3[2], w_3[3], w_3[4]}_{\text{реч } w_3} ,$$

Блок података је представљен са три кодне речи, од којих свака садржи по четири бита:

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

Након примене блоковског интерливера, битови који се шаљу кроз комуникациони

канал реорганизовани су на следећи начин:

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

Претпоставимо да је током транспорта кроз комуникациони канал дошло до пакетске грешке, и да су битови који припадају пакету означени са $\textcircled{w}_i[j]$:

$$w_1[1], w_2[1], w_3[1], w_1[2], \underbrace{\textcircled{w}_2[2], \textcircled{w}_3[2], \textcircled{w}_1[3]}_{\text{пакет}}, w_2[3], w_3[3], w_1[4], w_2[4], w_3[4] \ .$$

Након преноса, подаци пролазе кроз инверзни блок података, чиме се пакетска грешка распоређује по кодним речима, пре декодовања:

$$\underbrace{w_1[1], w_1[2], \textcircled{w}_1[3], w_1[4]}_{\text{реч } \hat{w}_1}, \underbrace{w_2[1], \textcircled{w}_2[2], w_2[3], w_2[4]}_{\text{реч } \hat{w}_2}, \underbrace{w_3[1], \textcircled{w}_3[2], w_3[3], w_3[4]}_{\text{реч } \hat{w}_3} \ .$$

3.3.2.2 Пример конволуционог интерливера

Основна верзија конволуционог интерливера састоји се од низа померачких регистара, као што је приказано на сл. 3.6 (в. [113]). Нулти регистар не смешта битове, већ их одмах преноси. Сваки наредни регистар може да смеси J битова више од претходног, чиме се имплементирају временски помераји појединачних регистара. Са доласком сваког новог бита, комутатор се пребацује на следећи регистар у низу (померање је циклично, тј. после регистра $(N-1)J$, комутатор прелази на нулти регистар). Тада се нови бит додаје у текући регистар, док се најстарији бит у регистру шаље ка модулатору. Деинтерливер спроводи инверзно пресликавање, које следи из обрнутог редоследа регистара, уз услов да комутатори интерливера и деинтерливера морају да буду синхронизовани [113].

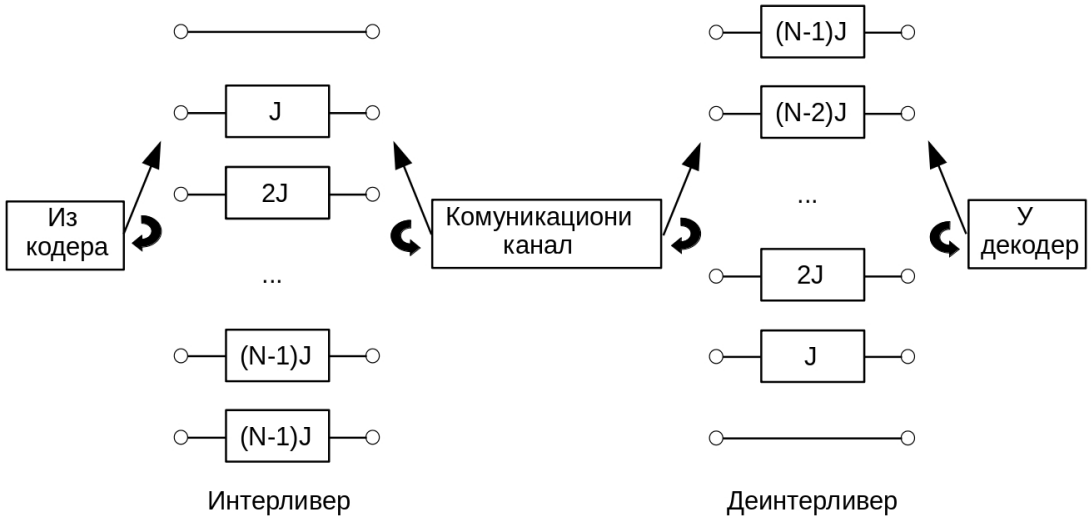
Као илустрација, на сл. 3.7 су приказана четири стања конволуционог интерливера кад му се саопшти улаз:

$$\underbrace{1, 2, 3, 4}_{\text{стање А}}, \underbrace{5, 6, 7, 8}_{\text{стање Б}}, \underbrace{9, 10, 11, 12}_{\text{стање В}}, \underbrace{13, 14, 15, 16}_{\text{стање Г}} \ . \tag{3.73}$$

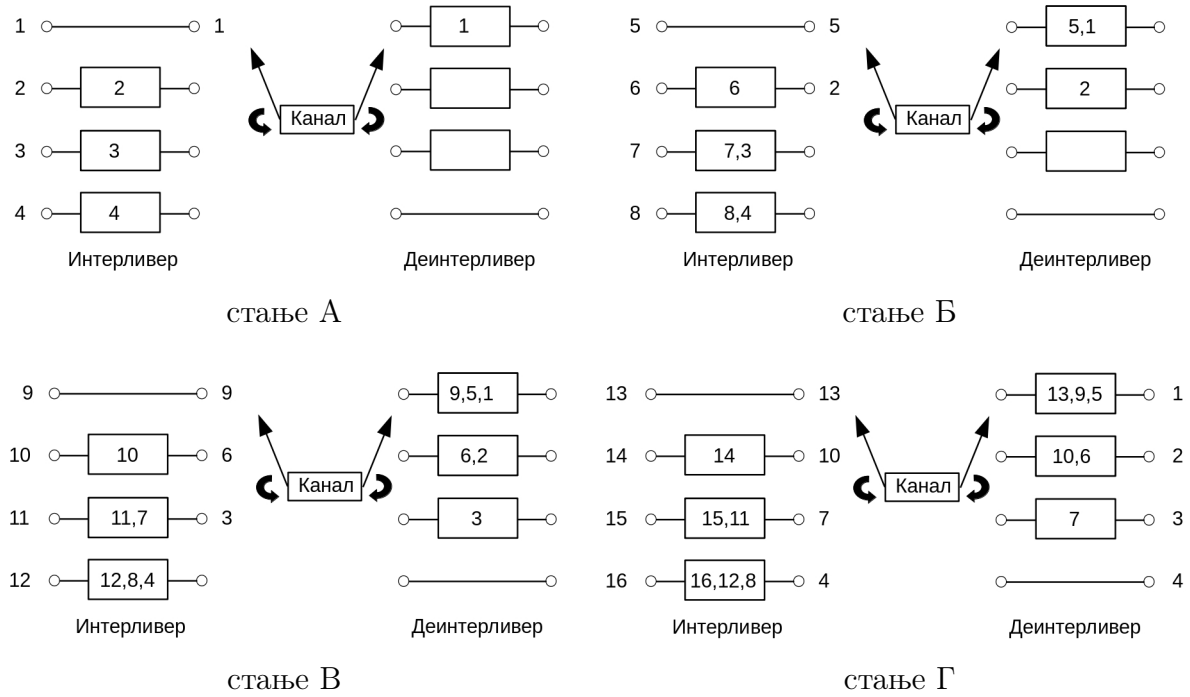
3.4 Неинвертибилне трансформације

3.4.1 Једносмерне функције са замком

Основна идеја криптографије са јавним кључевима базирана је на једносмерним функцијама са замком, тј., функцијама чије се вредности за произвољни елемент



Слика 3.6: Конволуциони интерливер (слика прилагођена из [113]).



Слика 3.7: Четири стања конволуционог интерливера за улаз (3.73), (слике прилагођене из [113]).

из домена могу израчунати у полиномном времену, док је вероватноћа инвертовања једносмерне функције било којим алгоритмом са полиномним временом извршавања „занемарљива" [47].

Дефиниција 6. Функција $\nu : \mathbb{N} \to \mathbb{R}$ је занемарљива ако за сваку константну вредност $c \geq 0$ постоји цели број k_c такав да важи:

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

Дефиниција 7. Функција $f : \{0,1\}^* \to \{0,1\}^*$ је једносмерна ако су задовољени следећи услови:

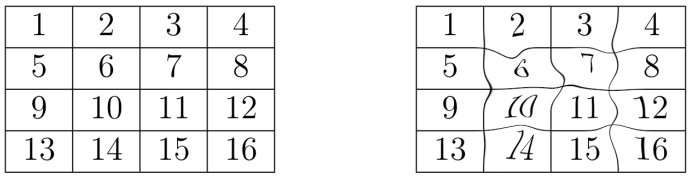
- постоји алгоритам са полиномним временом извршавања који за дату вредност x израчунава вредност $f(x)$,
- за било који алгоритам са полиномним временом извршавања A постоји занемарљива функција ν_A, таква да за довољно велику вредност k важи:

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

Једносмерна функција са замком f је једносмерна функција за коју постоји тајна инверзна функција која се извршава у полиномном времену.

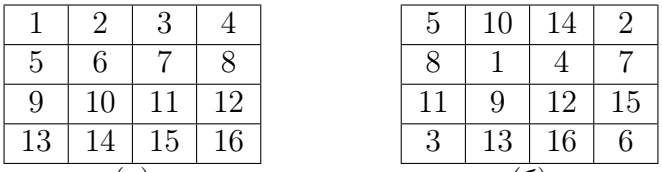
Дефиниција 8. Једносмерна функција са замком је једносмерна функција $f : \{0,1\}^* \to \{0,1\}^*$ за коју постоје полином p и алгоритам са полиномним временом извршавања I такви да за свако k постоји $t_k \in \{0,1\}^*$ за које важи $|t_k| \leq p(k)$, и за свако $x \in \{0,1\}^*$ постоји $I(f(x), t_k) = y$ такво да важи $f(y) = f(x)$.

Међутим, без познавања тајне инверзне функције, вероватноћа инвертовања једносмерне функције са замком у полиномном времену је и даље занемарљива. Један пример једносмерне функције са замком је $f(x,n) = x^2 \pmod{n}$, где је $n = pq$ производ два проста броја, и $x \in \mathbb{Z}_n^*$. Инвертовање ове функције је лако ако и само ако је факторисање броја n лако [91]. Познатији пример је једносмерна функција са замком већ размотрена у секцији 3.1.1, која се користи у алгоритму RSA за криптографију са јавним кључевима.



(а) (б)

Слика 3.8: Илустрација изобличења мреже слике: (а) пре и (б) после трансформације.



(а) (б)

Слика 3.9: Илустрација пермутација блокова слике: (а) пре и (б) после трансформације.

3.4.2 Трансформације дигиталних слика

У секцији 3.4.1 смо размотрили појам једносмерних функција са замком, који пружа основ за опозив биометријских шаблона. Овде ћемо размотрити изабране трансформације дигиталних слика.

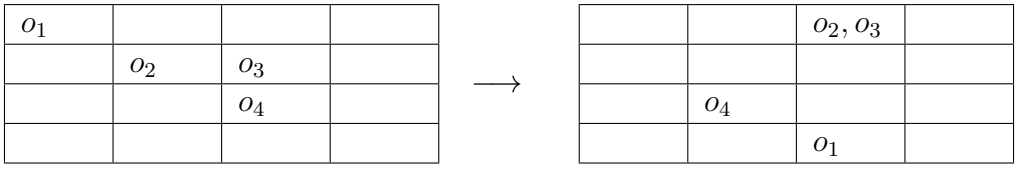
Трансформације слике могу се спроводити у домену сигнала (одмах после аквизиције), или у домену издвојених обележја (након обраде слике). Две трансформације у домену сигнала су изобличење мреже слике (илустровано на сл. 3.8) и пермутација блокова слике (илустровано на сл. 3.9). У обе трансформације, слика се подели на блокове, чији су положаји и димензије одређени детектованим обележјима ентитета на слици [92].

Трансформација у домену издвојених обележја се базира на случајном и вишеструком пресликавању издвојених обележја [92]. Без губитка општости, нека је дат скуп биометријских обележја издвојених са слике:

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

За дати скуп обележја F, неивертибилна трансформација $f : F \to F'$ генерише нови скуп обележја

$$F' = \{(X_1, Y_1, \Theta_1), (X_2, Y_2, \Theta_2), \ldots, (X_n, Y_n, \Theta_n)\} \, , \tag{3.77}$$



Слика 3.10: Илустрација неинвертибилног пресликавања издвојених обележја (прилагођено из [92]).

такав да се из њега не може реконструисати почетни скуп F. Функција $f : F \to F'$ се може дефинисати тако да се на сваку класу параметара у обележју примењује засебна неинвертибилна функција, на пример, полином вишег реда (в. [92]):

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

где су:

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

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

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

Неинвертибилност овакве трансформације заснива се на чињеници да је могуће да више обележја која припадају различитим блоковима изворне слике буду пресликана у исти блок трансформисане слике, као што је илустровано на слици 3.10.

Глава 4

Предлог радног оквира и једне имплементације

Ово поглавље засновано је на решењу предложеном у раду [77], који је проширена верзија истраживања описаног у [75].

Као што је речено у 2. глави, биометријски системи пројектовани на принципу сигурности засноване на дизајну су подложни нападима. Осам различитих типова напада идентификовано је у [9, 57]. Да би се спречило успешно извршавање ових напада, цео систем је подељен на три модула високог нивоа, који се налазе на најмање два уређаја. Осим тога, систем је занован на опозивој биометрији (неинвертибилним трансформацијама) и јакој криптографској заштити, која укључује генераторе псеудослучајних бројева, једносмерне хеш функције и криптографију са јавним кључем.

Предложени модуларни систем се састоји од следећих компоненти:

- једног или више клијената, односно уређаја који преузимају биометријске податке корисника, управљају помоћним подацима и генеришу шифроване биометријске шаблоне;
- сервера за проверу идентитета, који генерише парове кључева, односно управља кључевима и пореди опозиве биометријске шаблоне и
- складишта података од поверења (енгл. *trusted storage*) у коме се чувају шифровани опозиви шаблони.

Сходно томе да ли се у складиште од поверења налази на клијенту или је реализовано као засебни уређај, односно база података на издвојеном серверу, могу се

издвојити две врсте система за проверу идентитета:

- системи са дистрибуираним складиштењем и
- системи са централизованим складиштењем.

У случају да у систему постоји више клијената, и да постоји потреба да корисник који је уписан на једном клијенту има могућност да провери свој идентитет на другом клијенту који је повезан на исти сервер, складиште података од поверења мора бити централизовано. У супротном корисник се мора уписати на сваком клијенту.

Осим криптографске заштите шаблона, систем треба да обезбеди и висок ниво заштите приватости, што значи да мора да задовољи и следеће захтеве:

- биометријски шаблони морају бити шифровани, или у најгорем случају опозиви, и то док су ускладиштени, док се преносе и док се верификују (на пример, сервер за проверу идентитета не сме имати приступ незаштићеном биометријском шаблону);
- ни један клијент не сме имати приступ привантим кључевима који се налазе на серверу за проверу идентитета, јер се, у случају да клијент оствари приступ приватним кључевима могу компромитовати шаблони;
- систем мора бити отпоран на напад замене биометријског шаблона (енгл. *template substitution attack*) и све нападе ниског нивоа;
- увођење опозиве биометрије и криптографских мера заштите не сме значајно да повећа рачунску сложеност и простор потребан за складиштење шаблона;
- тачност верификације не сме да се смањи, односно не смеју да се повећају грешке лажног прихватања и лажног одбијања.

Другим речима, од система се захтева да обезбеди захтеве које испуњава идеални биометијски систем [116].

Радни оквир модуларног система за проверу идентитета представљен у овом делу рада заснован је на конвенционалној биометрији која користи операцију ексклузивно ИЛИ, односно Хемингово растојање као меру сличности два вектора обележја која су представљена као низови битова приликом верификације корисника. Хемингово

растојање је одабрано као метрика за верификацију зато што је погодно за примену у неинвертибилној трансформацији зановане на једнократним бележницама (енгл. *one-time-pad*). Другим речима, неинвертибилна трансформација која се користи у предложеном решењу је једноставно рачунање операције ексклузивно ИЛИ над шаблоном и кључем за трансформацију исте дужине као и оригинални шаблон. Овај начин заштите биометријских шаблона штити корисника од крађе идентитета и поједностављује фазу поновног уписа (енгл. *re-enrollment*) у случају да постоји сумња о компромитовању шаблона или кључа за трансформацију, зато што не постоји потреба да корисник поново приложи свој биометријски податак.

Две значајне карактеристике предложеног радног оквира јесу да испуњава услове о чувању и преносу шаблона у шифрованом облику и верификацији у домену опозивих шаблона, као и да увођење мера заштите не повећава значајно рачунску сложеност, док се величина простора за складиштење не мења, зато што су опозиви шаблони исте величине као и оригинални. Осим тога, радни оквир не намеће употребу конретних криптографских алгоритама (гереатора псеудослучајних низова, хеш функција и асиметричних алгоритама), док модуларност система омогућава кориснику регистрованом на једном клијенту провери свој идентитет на другом који је повезан на исти сервер (што је значајно лакше извести у системима са централизованим складиштем).

4.1 Модуларни системи за биометријску проверу идентитета са дистрибуираним складиштењем шифрованих опозивих шаблона

У системима са дистрибуираним складиштењем шифровани шаблони се чувају на клијентима. Потребно је напоменути да је у овој класи система неопходно да на клијенту постоји складиште од поверења отпорно на форензичке технике.

У овом случају, током фазе уписа систем функционише на следећи начин:

- Корисник прилаже свој нумерички кориснички идентитет и кључ за неинвертибилну трансформацију K_t клијенту.

- Нека је $H(x)$ једносмерна хеш функција (као што је већ речено, пројектант система може одабрати ону коју сматра најсигурнијом), ID идентитет корсника а K_{priv} и K_{pub} приватни и јавни кључ корисника, респективно. Клијент рачуна хеш вредност корисничког идентитета и шаље ту вредност серверу за проверу идентитета.

- Сервер генерише пар кључева (K_{priv}, K_{pub}), чува приватни кључ и хеш корисничког идентитета $(H(ID), K_{priv})$ и шаље јавни кључ клијенту.

- Нека је $\oplus$ операција ексклузивно ИЛИ. Корисник прилаже биометријски узорак клијенту. Клијент генерише бинарни шаблон b_0, а затим и опозиви бинарни шаблон на следећи начин: $b = K_t \oplus b_0$.

- Нека је E операција шифровања. За шифровање се може искористити било који алгоритам са јавним кључем који задовољава принципе теорије информација и јаке криптографске заштите. Клијент на основу извора случајности генерише унутрашњи кључ s_0 за генератор псеудослучајних бројева и шифрује га јавним кључем: $s_E = E(s_0, K_{pub})$.

- Нека је $PRNG$ ознака за употребу генератора псеудослучајних бројева који задовољава статистичке тестове случајности, односно обезбеђује довољно ентропије у генерисаном низу. Клијент генерише псеудослучајни низ битова $s = PRNG(s_0)$ помоћу генератора и датог кључа.

- Клијент рачуна $s \oplus b$, чува $(H(ID), s_E, s \oplus b)$ у складишту од поверења и брише све остале податке.

У фази верификације корисника, систем функционише на следећи начин:

- Корисник прилаже свој идентитет (ID) и кључ за једносмерну трансформацију K_t клијенту.

- Клијент преузима биометријски податак корисника, генерише шаблон b'_0 а затим и опозиви шаблон $b' = K_t \oplus b'_0$.

- Клијент рачуна $H(ID)$ и преузима вредносхти s_E и $(s \oplus b)$ из одговарајућег сачуваног записа $(H(ID), s_E, s \oplus b)$.

- Клијент рачуна $s \oplus b \oplus b'$ и шаље серверу заједно са шифрованим унутрашњим кључем s_E.

- Клијент шаље хеш вредност корисничког идентитета серверу за проверу идентитета. Сервер преузима приватни кључ из одговарајућег записа $(H(ID), K_{priv})$.

- Нека је D операција дешифровања у шифарском систему са јавним кључем. Сервер за проверу идентитета дешифрује вредност s_E како би остварио приступ унутрашњем кључу s_0 извршавајући операцију $s_0 = D(s_E, K_{priv})$.

- Сервер након тога генерише низ битова $s' = PRNG(s_0)$.

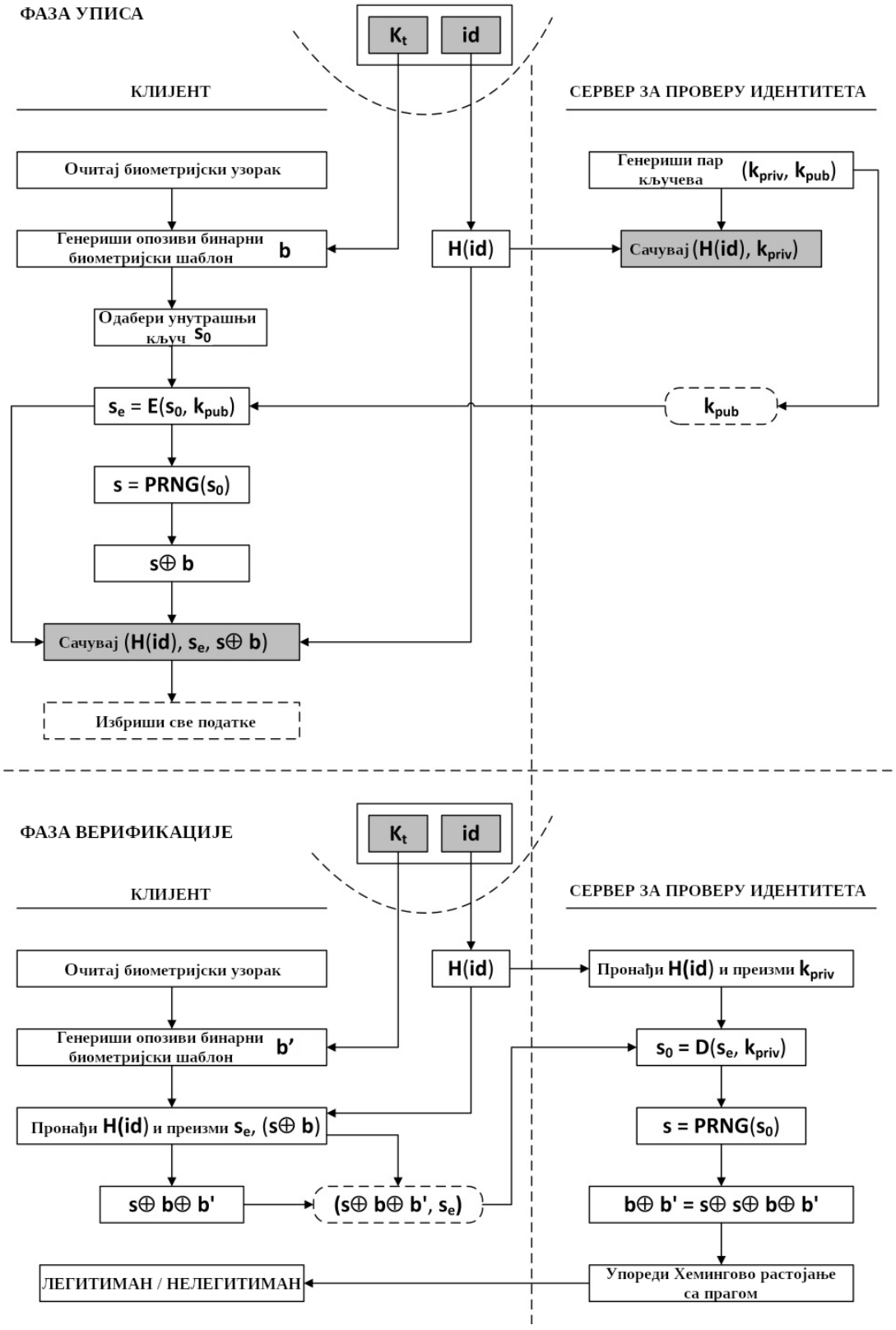
- Пошто је генератор псеудослучајних бројева детерминистички и пошто се исти унутрашњи кључ користи за генерисање низова у фази уписа и у фази верификације, генерисани низови s и s' су идентични, тј. важи $s = s'$. Осим тога, идентични кључ за неинвертибилну трансформацију K_t се користи у обе фазе. Имајући то у виду сервер рачуна $s \oplus b \oplus s' \oplus b' = K_t \oplus b_0 \oplus K_t \oplus b'_0 = b_0 \oplus b'_0$ и пореди Хемингово растојање шаблона b_0 и b'_0 са прагом поређења. На основу тога, сервер доноси одлуку да ли је корисник легитиман или не и шаље је клијенту.

Фазе уписа и верификације корисника приказане су на сл. 4.1.

Треба нагласити да, иако је резултат поређења заправо Хемингово растојање између оригиналних шаблона, сервер израчунава то растојање на основу опозивих шаблона генерисаних помоћу кључа за једносмерну трансформацију.

4.1.1 Осврт на сигурност и ограничења предложеног решења

Следећи закључци се могу изнести о сигурности предложеног решења. Као што је захтевано, шаблони су шифровани у свим фазама (пренос и складиштење) док се приликом верификације пореде опозиви шаблони. Осим тога, клијент не може да приступи приватним кључевима на серверу. Систем је занован на дво-факторској провери идентитета, што значи да нелигитиман корисник који је дошао у посед кључа за трансформацију или помоћног података (у овом случају, шифровани шаблон) не може да се представи као легитиман корисник. Уколико су шаблони који се чувају на клијенту компромитовани, поновни упис се може извршити помоћу другог кључа



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

за трансформацију и другог пара кључева за шифарски систем са јавним кључем. Напади замене шаблона се не могу извршити зато што се јавни кључ брише након фазе уписа. Иако је јавни кључ јавни информација, као додатна мера сигурности може се увести размена јавног кључа употребом Дифи-Хелмановог протокола, што спречава нападача да пресретне комуникацију и покуша да изврши накнадно напад замене шаблона. Пошто нападач не може да регенерише низ битова s на основу шифрованог низа sE и јавног кључа (уколико престретне оба податка), систем је такође отпоран и на све нападе на биометријске криптосистеме.

То значи да предложено решење испуњава све услове које мора да испуни идеални биометријски систем описане у [116], с изузетком другог услова — уместо шифрованих, пореде се опозиви шаблони (услови идеалног биометријског криптосистема преузети су из [116]):

1. биометријски шаблони се чувају и преносе искључиво у шифрованом облику;
2. приликом аутентификације биометријски шаблони се не дешифрују;
3. шифровани шаблони за различите примене се не могу повезати;
4. сервер никада не добија шаблоне који нису шифровани;
5. клијент нема приступ приватним кључевима;
6. шифровани шаблон се може заменити новим без поновног узимања биометријског податка;
7. систем је отпоран на напад заменом шаблона;
8. шифровани шаблон је отпоран на све нападе ниског нивоа;
9. систем није рачунски исувише захтеван и задржава прихватљив ниво тачности.

Следећи закључци се могу изнести о употребљивости система и извесним ограничењима. Систем је употребљив у сценарију један клијент — један сервер. Систем је такође употребљив и у сценарију где постоји више клијената повезаних на један сервер уколико се од корисника који је уписан на једном клијенту не захтева да провери своји идентитет на другом. Уколико се то ипак захтева, потребно је да се на серверу са кључем корисника и корисничким идентитетом чува и идентитет клијента. Осим

тога, корисник би морао да обави поновну фазу уписа на сваком клијенту у случају да је кључ за неинвертивилну трансформацију компромитован или изгубљен.

Друго ограничење које се односи на употребљивост система је употреба биометрије засноване на операцији екслузивно ИЛИ која за сада није применљива на све биометријске модалитете (за неке модалитете нису пријављени алгоритми за издвајање биометријских шаблона у виду бинарних низова у релевантној литератури). Међутим, треба узети у обзир да се свет кога ми перципирамо као стварност може представити као бесконачни број нула и јединица.

4.2 Модуларни системи за биометријску проверу идентитета са централизованим складиштењем шифрованих опозивих шаблона

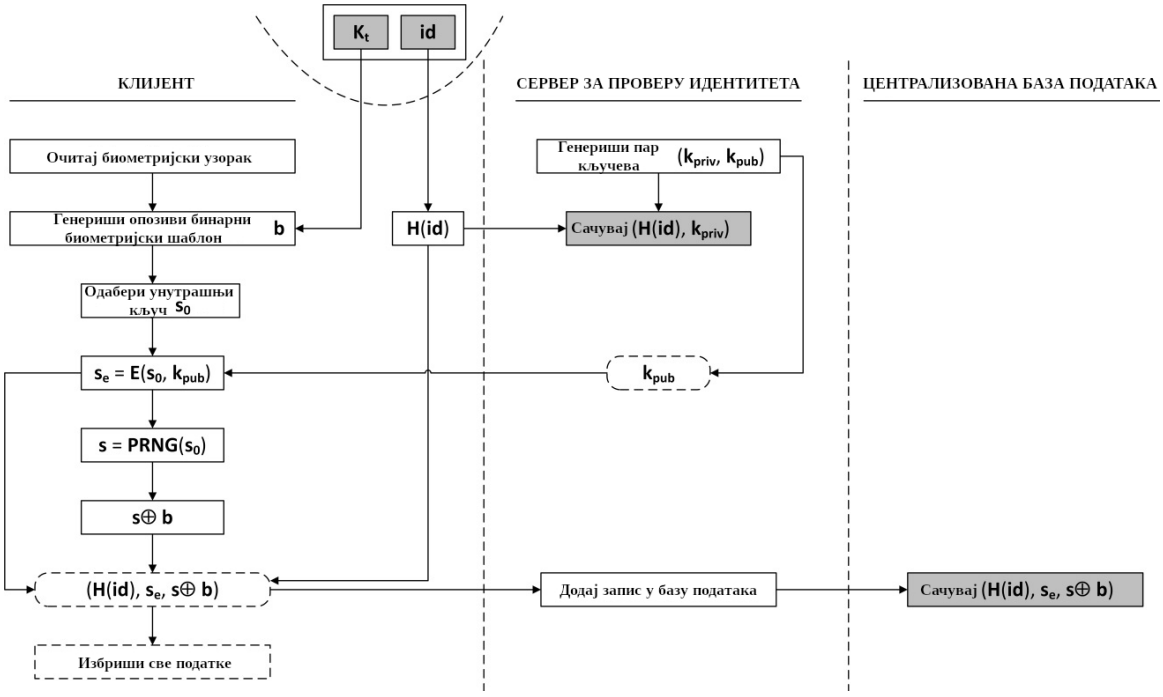
У системима са централизованим складиштењем шифровани шаблони се не чувају на клијентима. Ова класа система представља проширење система система са дистрибуираним складиштењем које уклања извесна ограничења везана за сценарио у коме је више клијената повезано на један сервер за проверу идентитета.

У фази уписа корисника, систем функционише слично системима са дистрибуираним складиштењем, уз две битне разлике (в. сл. 4.2):

- Вредности $(H(ID), s_E, s \oplus b)$ се не чувају на клијенту. Након рачунања тих вредности, клијент шаље захтев серверу за проверу идентитета да дода запис који садржи те вреднисти у централизовано складиште.

- Клијент у овом случају након успешно извршене фазе уписа не брише само јавни кључ, нешифровани унутрашњи кључ и оригинални шаблон, већ брише све податке. То значи да се на клијенту не чува ни један податак.

Веома битна чињеница је да се шифровани унутрашњи кључ генератора псеудослучајних бројева не сме чувати на серверу зато што се на серверу налази одговарајући приватни кључ којим би нападач могао извршити дешифровање унутрашњег кључа уколико оствари приступ серверу. Другим речима, централизовано складиште се мора реализовати у виду базе података на посебном серверу који ће комуници-

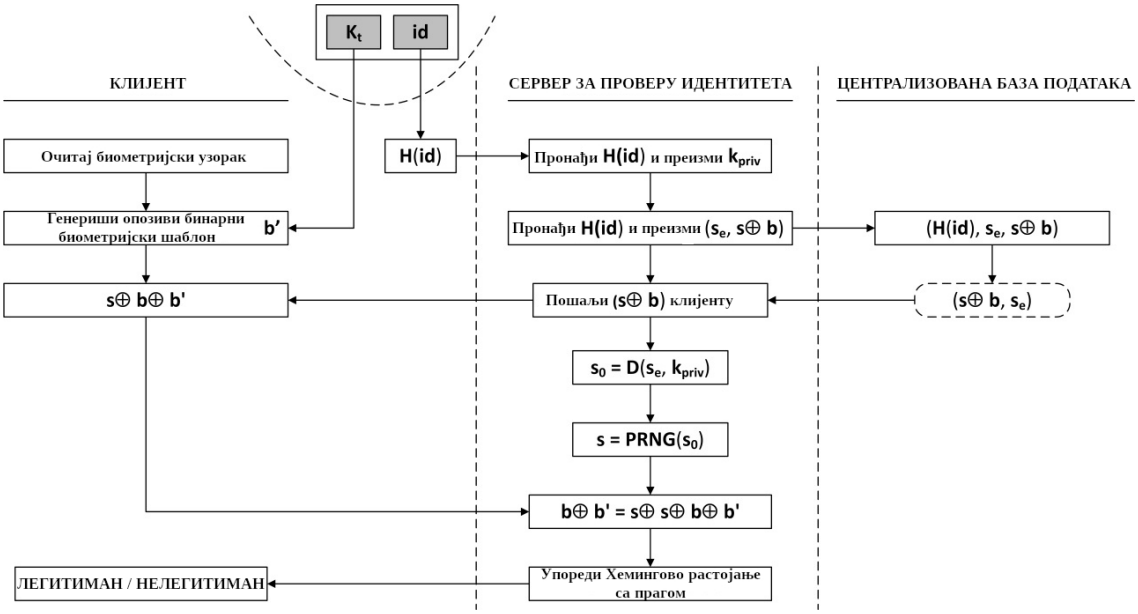


Слика 4.2: Фаза уписа корисника у модуларном систему са централизованим складиштењем. Изворни облик слике може се наћи у [75].

рати са сервером за проверу идентитета путем шифрованог канала. Конструкција шифрованог канала између ова два уређаја и управљање кључевима нису предмет овог истраживања.

У фази верификације корисника, систем функционише на следећи начин:

- Корисник се идентификије на клијентској страни и прилаже кључ K_t.
- Корисник прилаже свој биометријски узорак клијенту, клијент генерише шаблон b'_0 и опозиви шаблон $b' = K_t \oplus b'_0$'.
- Клијент рачуна хеш вредност $H(ID)$ и шаље је серверу за проверу идентитета.
- Сервер за проверу идентитета шаље упит централизованом складишту и преузима вредности s_E и $(s \oplus b)$ на основу записа који садржи вредности $(H(ID), s_E, s \oplus b)$ које су сачуване.
- Сервер шаље вредност $s \oplus b$ клијенту.
- Клијент израчунава $s \oplus b \oplus b'$ и шаље израчунату вредност серверу.
- Сервер за проверу идентитета преузима јавни кључ из записа одговарајућег пара $(H(ID), K_{priv})$.



Слика 4.3: Фаза верификације корисника у модуларном систему са централизованим складиштењем. Изворни облик слике може се наћи у [75].

- Сервер дешифрује унутрашњи кључ генератора псеудослучајних бројева $s_0 = D(s_E, K_{priv})$ и генерише низ битова: $s = PRNG(s_0)$. Поново се напомиње да су због детерминистичке природе генератора и употребе истог унутрашњег кључа генерисани низови у фази уписа и у фази верификације идентични.

- Сервер пореди Хемингово растојање између два опозива шаблона, односно између низа битова b и b' са прагом поређења. На основу резултата поређења, одлука о томе да ли је корисник легитиман или не се шаље клијенту.

Фаза верификације корисника приказана је на слици 4.3.

4.2.1 Осврт на сигурност и ограничења предложеног решења

Закључци о сигурности предложеног решења са централизованим складиштењем су веома слични као и закључци о сигурности система са дистрибуираним складиштењем. Међутим, потребно је нагласити да је у овом случају неопходно увести додатне мере заштите комуникационог канала између сервера за проверу идентитета и централизованог складишта у ком је смештен унуташњи кључ генератора и шифровани опозив шаблон.

Основна разлика између система са дистрибуираним и централизованим складиштењем односи се на ограничења примене. У овом случају, од корисника се не

захтева да обаве фазу уписа на свим клијентима на којима желе да се верификују зато што се биометријски шаблони чувају у централизованом складишту. Другим речима, корисник који је регистрован на једном клијенту може верификовати свој идентитет на свим клијентима који су повезани на исти аутентификациони сервер. Овакви системи су применљиви у великом броју домена примене, почев од контроле присупа одређеним просторијама (за улаз у сваку просторију потребан је један клијент) до криптографске заштите пријављивања корисника на услуге мобилног банкарства помоћу биометријских података (што је изводљиво и помоћу система са дистрибуираним складиштењем у случају да корисник услуга користи само један мобилни уређај).

4.3 Једна примена система са дистрибуираним складиштењем за проверу идентитета корисника услуга мобилног банкарства која је заснована на биометрији дужице

Мобилно банкарство је услуга коју клијентима пружа финансијска институција која пружа услугу обављања финансијских трансакција помоћу мобилног уређаја (паметног телефона или таблета) и пратећег софтвера, који најчешће обезбеђује иста институција. Узевши то у обзир, може се закључити да је мобилно банкарство једна од најосетљивијих употреба у контексту сигурности који обавља типичан корисник паметних мобилних уређаја [82]. Иако многе финансијске институције нуде своје услуге мобилног банкарства по принципу „будите без бриге“ [69], за сада не постоји решење које корисницима обезбеђује потпуну сигурност.

Постоји неколико безбедносних аспеката у вези са финансијским трансакцијама које се врше путем мобилних уређаја на које треба обратити пажњу:

- физичка сигурност мобилног уређаја,
- сигурност апликације која се извршава на уређају,
- верификација идентитета корисика и уређаја на серверу који пружа услуге мобилног банкарства и

- шифровање података који су пренети преко мреже, као и података који су сачувани на самом уређају које корисник жели касније да анализира.

У овом делу рада биће укратко описан сценарио који се односи на проверу идентитета корисника и мобилног уређаја даваоцу услуга. Данас се у мобилном банкарству примењују различите методе провере идентитета, а све имају своје предности и мане. На пример, аутентификацију засновану на лозинкама је најлакше имплементирати, али су корисници услуга мобилног банкарства у том случају изложени ризику од превара или крађа идентитета. Већина произвођача мобилних уређаја уочило је потребу за јаким сигурносним противмерама и сходно томе производе нове уређаје са уграђеним биометријским скенерима. Сходно истраживању које је извршио Gartner,преко 30% мобилних уређаја произведених 2014. године тренутно користи биометрију као начин провере идентитета. Данас је тај број знатно већи. Финансијске институције би ово требале да прихвате као јако добру могућност да својим клијентима обезбеде виши ниво сигурности приликом извршавања трансакција са мобилних уређаја, а не као препреку прихватању биометријских метода заштите [115].

У овом делу поглавља описан је један начин примене предложеног модуларног система за биометријску проверу идентитета са дистрибуираним складиштењем шифрованих опозивих шаблона у мобилном банкарству.

Сервер за проверу идентитета се налази у финансијској институцији (другим речима, банка). На серверу се налауе кључеви за дешифровање, што значи да се шифровани биометријски шаблони налазе на клијенту. На овај начин се спречава да нападач који је остварио нелегитиман приступ серверу за проверу идентитета дешифрује шаблоне. Клијент је мобилни уређај (паметни телефон или таблет) опремљен скенером дужице или предњом камером високог квалитета (већина уређаја средње класе испуњава један од претходно поменута два захтева). Додатно, на клијенту мора постојати софтвер који ће извршити издвајање обележја и неопходне криптографске операције – овај проблем се може решити у виду апликације коју ће обезбедити финансијска установа. Кључ за неинвертибилну трансформацију се смешта на сам уређај – корисник преузима кључ као излаз генератора случајних или псеудослучајних бројева од финансијске установе. Треба напоменути да кључ мора бити исте дужине као и код дужице како би клијент могао извршити операцију ексклузивно ИЛИ одмах након издвајања обележја. Кориснику треба дозволити да

са другог упареног уређаја избрише кључ и остале релевантне податке у случају да је уређај украден или у случају да постоји сумња да су подаци компромитовани. Такође, финансијској институцији треба омогућити да обрише податке са свих или одабраних клијената у сличају компромитовања сервера за проверу идентитета.

Током фазе уписа, предложени систем за проверу идентитета функционише на следећи начин:

- Софтвер на клијенској страни рачуна хеш вредност $IMEI$ (*International Mobile Equipment Identity*) и шаље је серверу за проверу идентитета. Уместо самог $IMEI$ броја, шаље се хеш вредност како би се заштитио идентитет корисника — израчунавање хеш вредности спречава слање отвореног текста са клијента ка серверу, као и чување осетљивих приватних података корисника на серверу.

- Сервер генерише пар кључева — приватни и јавни кључ — (K_{priv}, K_{pub}), чува приватни кључ у својој бази податак упарен са хеш вредношћу $IMEI$ $(H(IMEI), K_{priv})$ и шаље јавни кључ мобилном уређају.

- Корисник прилаже биометрију дужице мобилном уређају. Софтвер на клијентској страни генерише бинарни шаблон дужице b_0 (на начин који је описан у секцији 5.1) и генерише опозиви биометријски шаблон $b = K_t \oplus b_0$ користећи кључ за једносмерну трансформацију који се налази на самом уређају.

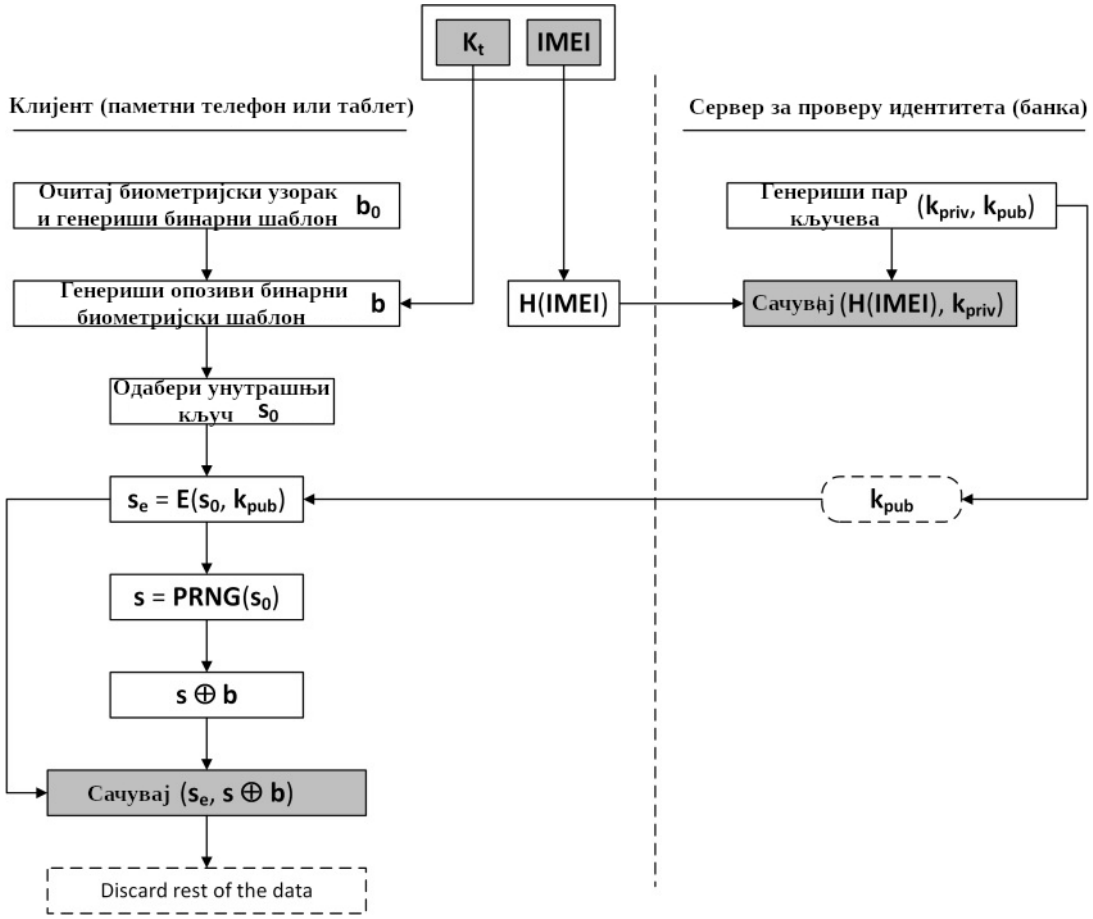
- Клијентски софтвер на основу извора случајности генерише унутрашњи кључ s_0 и шифрује га помоћу јавног кључа: $s_E = E(s_0, K_{pub})$.

- Софтвер затим генерише низ битова $s = PRNG(s_0)$ користећи генератор псеудослучајних бројева и унуташњи кључ, рачуна вредност $s \oplus b$, чува уређени пар $(s_E, s \oplus b)$ у складишту од поверења на уређају и брише остале податке.

Фаза уписа је приказана на сл. 4.4.

Током фазе верификације корисника, систем обавља следеће операције (в. сл. 4.5):

- На клијентској страни, апликација рачуна хеш вредност $IMEI$ броја и шаље је серверу за проверу идентитета.



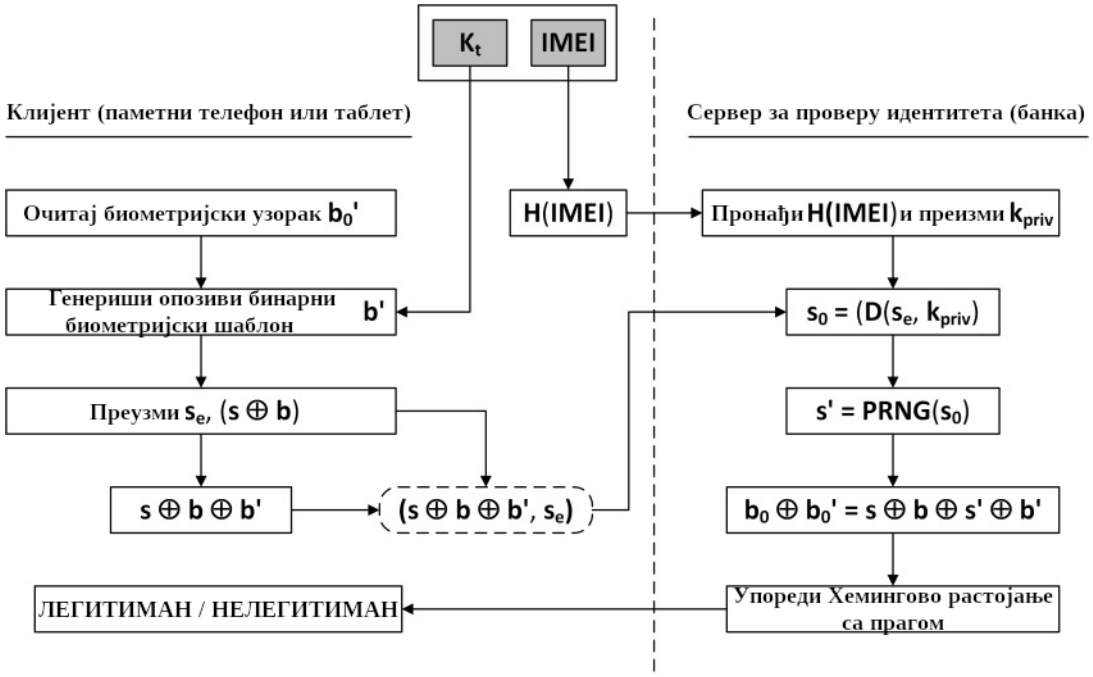
Слика 4.4: Фаза уписа корисника у систему за проверу идентитета корисника услуга мобилног банкарства. Изворни облик слике може се наћи у [77].

- Корисник прилаже биометријски узорак сензору на мобилном уређају. Софтвер на паметном мобилном уређају генерише бинарни шаблон дужице b'_0 а потом и опозиви шаблон $b' = K_t \oplus b'_0$.

- Софтвер преузима вредности s_E и $(s \oplus b)$ са складишта од поверења на уређају, рачуна $s \oplus b \oplus b'$ и шаље са унуташњим кључем генератора s_E и хеш вредношћу $IMEI$ броја серверу за проверу идентитета.

- Сервер преузима из базе података сачуван запис $(H(IMEI), K_{priv})$ који одговара хеш вредности $IMEI$ уређаја, дешифрује унутрашњи кључ генератора помоћу приватног кључа $s_0 = D(s_E, K_{priv})$ и генерише низ битова: $s' = PRNG(s_0)$.

- Као што је речено у секцији 4.1, због детерминистичке природе генератора псеудослучајних бројева, на основу идентичних унутрашњих кључева s и s', и



Слика 4.5: Фаза верификације корисника у систему за проверу идентитета корисника услуга мобилног банкарства. Изворни облик слике може се наћи у [77].

идентричног кључа K_t за једносмерну трансформацију који се користи приликом уписа и аутентификације, сервер за проверу идентитета рачуна вредност $s \oplus b \oplus s' \oplus b' = b \oplus b' = K_t \oplus b_0 \oplus K_t \oplus b'_0 = b_0 \oplus b'_0$.

- Као и у случају радног оквира, разултат поређења је Хемингово растојање (специјалан случај Левенштајновог растојања за низове исте дужине) оригиналних, неизмењених шаблона, међутим сервер израчунава ово растојање на основу опозивих шаблона (другим речима, нема приступ оригиналним шаблонима или кључу за једносмерну трансформацију).

Псеудокодови алгоритама за фазе уписа и верификације су наведени на сл. 4.6 и 4.7.

4.3.1 Осврт на сигурност предложене имплементације

Што се тиче сигурности предложеног имплементације радног оквира са дистрибуираним складиштењем у мобилном банкарству, закључци који се могу извући су идентични закључцима наведеним о сигурности радног оквира на коме је решење предложено. Другим речима, шаблони си шифровани или, у најгорем случају опозиви, током свих фаза, а мобилни уређај нема приступ приватним кључевима на

Алгоритам за упис корисника		
УЛАЗ:	b	— биометријски шаблон,
	K_t	— кључ за трансформацију
ИЗЛАЗ:	$s \oplus b$	— шифровани опозиви биометријски шаблон,
	s_E	— шифровани унутрашњи кључ
Клијент:		
	1.	пошаљи $(H(IMEI))$
	2.	$b = K_t \oplus b_0$
	3.	одабери случајно (s_0); $s = PRNG(s_0)$
	4.	преузми (K_{pub}); $s_E = E(s_0, K_{pub})$
	5.	сачувај $(s_E, s \oplus b)$
Сервер:		
	1.	преузми $(H(IMEI))$
	2.	генериши (K_{priv}, K_{pub})
	3.	пошаљи (K_{pub}); сачувај $(H(IMEI), K_{priv})$

Слика 4.6: Алгоритам за упис корисника.

Алгоритам за верификацију корисника		
УЛАЗ:	b'	— биометријски шаблон,
	K_t	— кључ за трансформацију
	t	— праг поређења
ИЗЛАЗ:	одлука	
Клијент:		
	1.	пошаљи $(H(IMEI))$
	2.	$b' = K_t \oplus b'_0$
	3.	пошаљи $(s \oplus b \oplus b', s_E)$
	4.	преузми (одлука)
Сервер:		
	1.	преузми $(H(IMEI, s \oplus b \oplus b', s_E))$
	2.	$s_0 = D(s_E, K_{priv})$; $s' = PRNG(s_0)$
	3.	$b_0 \oplus b'_0 = s \oplus b \oplus s \oplus b'$
	4.	ако је $(b_0 \oplus b'_0) < t$ онда је одлука = „легитиман“, иначе одлука = „нелегитиман“
	5.	пошаљи (одлука)

Слика 4.7: Алгоритам за верификацију корисника.

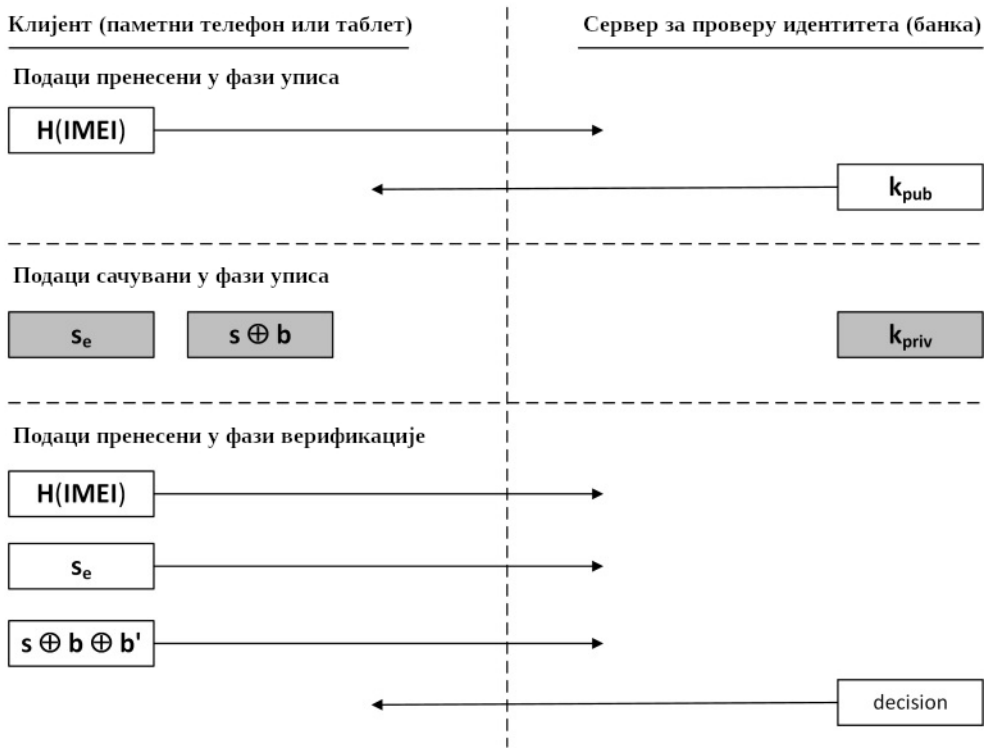
серверу финансијске установе. Сервер за проверу идентитета нема приступ кључевима који се користе за генерисање опозивих биометријских шаблона и шифрованим шаблонима генерисаним у фази уписа.

У случају да је мобилни уређај украден или изгубљен, нападач се не може представити као легитиман корисник, зато што је систем отпоран на нападе пописане у [57] као и на нападе успоном (енгл. *hill-climbing attack* [3]), нападе засноване на недовољној количини случајности (енгл. *non-randomness attack* [28]), нападе поновном употребом (енгл. *re-usability attack* [18]), нападе слепом заменом [109] и нападе повезивањем (енгл. *linkage attack*) [27].

Иако се у систем могу додати изабрани протоколи за размену кључева, најсигурнији начин за дистрибуцију кључа за једносмерну трансформацију директно преузимање кључа из банке. На овај начин се укида могућност лажирања идентитета, које за последицу може имати успешно извршење напада заснованих на техникама друштвеног инжењеринга. И кориснику и финансијској институцији је дозвољено удаљено брисање података (укључујући и кључева) уколико је уређај украден или изгубљен.

У случају да се кориснику врати изгубљени уређај, корисник може преузети други кључ за неинвертибилну трансформацију од финансијске институције и извршити процедуру поновног уписа. Прилагање биометријског узорка у фази поновног уписа је непотребно — резултат извршавања операције ексклузивно ИЛИ над опозивим шаблоном и кључем за трансформацију је оригинални шаблон. Међутим, због повећања нивоа сигурности, предложену фазу поновног уписа треба извршити на следећи начин: корисник прилаже биометријски узорак, клијент генерише унутрашњи кључ генератора, а сервер нови пар кључева који ће се даље користити за шифровање унутрашњег кључа.

Такође потребно је нагласити да физички приступ уређају не омогућава нападачу да преузме кључ за једносмерну трансформацију. У новијим моделима паметних телефона са биометријским сензорима за више модалитета (на пример, отисак прста, лице и дужица) на којима се извршава оперативни систем Android (верзија 6 или новија) уграђене су против-форензичке технике које спречавају очитавање осетљивих података, чак и са најновијим форензичким алатима и уређајума. Ова чињенца која потиче из домена дигиталне форензике омогућава да се са високим нивоом си-



Слика 4.8: Подаци који се чувају и подаци који се преносе. Изворни облик слике може се наћи у [77].

гурности на уређају чувају осетљиве информације, попут кључа за трансформацију.

Подаци који се шаљу преко мреже и подаци који се чувају на мобилном уређају и серверу за проверу идентитета приказани су на сл. 4.8. Са слике се може видети да се следећи подаци преносе преко мреже: јавни кључ корисника се преноси само једном, у фази уписа, док се у фази уписа и приликом сваке верификације преносе хеш вредност IMEI броја и вредност добијена применом операције ексклузивно ИЛИ над опозивим шаблонима и генерисаним псеудослучајним низом: $s \oplus b \oplus b'$. На основу сл. 4.8 је немогуће идентификовати слабости предложеног решења које би омогућиле нападачу да из података који се преносе преузме било какву корисну информацију која би омогућила успешно извршење напада.

Једну ствар је, међутим, јако битно напоменути — избор лошег генератора псеудослучајних низова може довести до извесног цурења информација када се податак $s \oplus b \oplus b'$ преноси са клијента ка серверу. Сходно томе, неопходно је користити криптографски генератор псеудослучајних бројева који генерише низове битова високе ентропије.

Такође је потребно нагласити да сигурност система зависи и од сигурности под-

система за верификацију дужице. Иако је тешко извршити напад лажним представљањем, односно натерати систем да лажног корисника прихвати као легитимног, група етичких хакера је успела то да изведе са скенером дужице на паметном телефону Samsung Galaxy S8. Интересанта чињеница је да је цена хардвера који је коришћен за напад мања од цене паметног уређаја [48].

До сличних сценарија може доћи у случају да у уређају нису имплементирани алгоритми за откривање лажних дужица. На пример, подаци који су преузети са слика снимљених паметним телефонима са камерама високог квалитета могу се искористити за генерисање лажних слика дужице.

У литератури је пријављено неколико приступа за откривање лажних дужица. Један приступ откривању контактних сочива са лажном шаром ириса заснован на конволуционим неуронским мрежама описан је у [111]. Приступ који дискриминише дужицу корисника од слике (енгл. *liveness detection*) [112] заснован на детекцији покрета у оку пре издвајања обележја и поређења са ускладиштеним кодом дужице значајно повећава сигурност и поузданост система. Решење које је погодно за имплементацију у мобилним уређајима предложили су Gragnaniello и др. [49]. Ова брза и поуздана метода за детекцију лажних шара дужице заснована је на техници описивача локалних бинарних узорака (енгл. *local binary pattern descriptor*) и класификацији помоћу методе вектора ослонца са линеарним језгром. Сходно наводима аутора, тачност детекције лажних дужица предложеном методом је висока, иако је метода заснована на алгоритмима који нису претерано сложени.

Глава 5

Анализа експерименталних резултата са реалистичним подацима

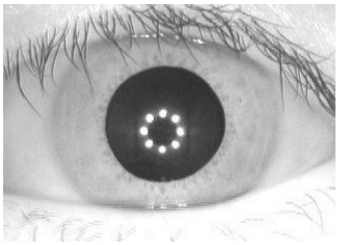
Ово поглавље је делом засновано на резултатима објављеним у [77]. Конкретно, из рада су преузети резултати који се односе на тачност верификације особе помоћу снимака дужице генерисаних паметним телефоном.

Поглавље је организовано на следећи начин: најпре је укратко описана Daugman-ова метода за издвајање обележја дужице и верификацију идентитета особе. Након тога су пријављени резултати поређења на реалистичном скупу података, а потом су обављене анализе које се односе на шифроване опозиве биометријске шаблоне и податке који се преносе преко мреже $s \oplus b \oplus b'$ (в. секцију 4.3).

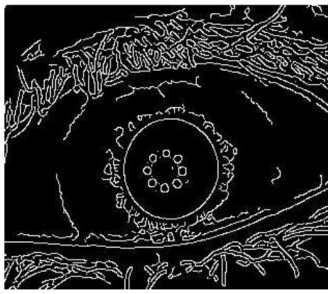
5.1 Препознавање дужице

Дужица (в. сл. 5.1) је део људског ока који се налази између рожњаче и сочива, и окружује зеницу. Једна од њених функција је да регулише количину светла које пролази кроз зеницу, ширењем и скупљањем два мишића: *sphincter pupillae* и *dilator pupillae* [4].

За процес аутентификације, најважнији аспект дужице представља њен шаблон, тј. шаре које су јединствене за сваког човека (ове шаре се разликују чак и на два ока исте особе). Препознавање особе на основу дужице се врши кроз низ корака. На слици ока је потребно детектовати дужицу, и издвојити одговарајући сегмент уз уклањање шумова. Издвојена дужица се нормализује, тј. преводи у формат који је



Слика 5.1: Слика ока, преузето из CASIA (http://biometrics.idealtest.org/) базе података биометријских узорака.



Слика 5.2: Илустрација резултата примене Canny edge детектора на сл. 5.1, преузето из CASIA (http://biometrics.idealtest.org/) базе података биометријских узорака.

прикладан за даљу обраду и представљање јединственим кодом. Кодовање дужице се врши помоћу филтера, при чему се издвајају обележја која ће се користити за поређење у поступку аутентификације. У наставку ћемо детаљније размотрити овај процес [74].

5.1.1 Сегментација, нормализација и кодовање дужице

Сегментација дужице представља поступак издвајања сегмента слике људског ока који садржи дужицу, тј. простор између унутрашње и спољашње ивице дужице. Очни капци и трепавице који на слици делимично покривају дужицу представљају шум који је потребно уклонити.

Сегментација почиње детектовањем ивица и контура на слици ока, за шта се уобичајено користи Canny edge детектор [25]. Илустрација резултата примене овог детектора дата је на сл. 5.2. Да би се уклонио шум, прво се примењују Гаусови филтери:

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

где су x и y растојања од центра. Након уклањања шума, израчунавају се интензи-

тети и смерови градијената у појединачним пикселима:

$$G = \sqrt{G_x^2 + G_y^2}\,, \tag{5.2}$$

и

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

где G_x и G_y представљају прве изводе у хоризонталном и вертикалном смеру израчунате применом Собелових филтера [32]:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \quad \text{и} \quad \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}, \tag{5.4}$$

а угао Θ се заокружује на вредности из редукованог скупа (на пример, умношци угла $\frac{\pi}{4}$). Ивице детектоване у досадашњем поступку су широке и неправилне, па се на њих примењује техника немаксималног сузбијања ивица, којом се детектоване ивице сужавају до јасног облика.

Овако обрађена слика и даље садржи шум који није уклоњен применом Гаусовог филтера. Зато се прво примењују два прага прихватљивости, тј. горњи и доњи прагови пропустљивости, да би се уклониле ивице које се налазе ван задатог опсега.

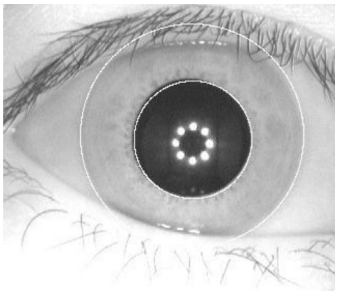
Поред тога, додатни шумови се уклањају праћењем повезаности ивица. Ивице које су слабије повезане са осталима се уклањају. Повезаност ивица се процењује тако што се за сваки пиксел посматра његова непосредна околина. Ако у њој постоји јака ивица, посматрани пиксел јој се придружује, а у супротном се одбацује.

Да би се детектовале ивице дужице, зенице и капка, примењује се Hough трансформација [38]:

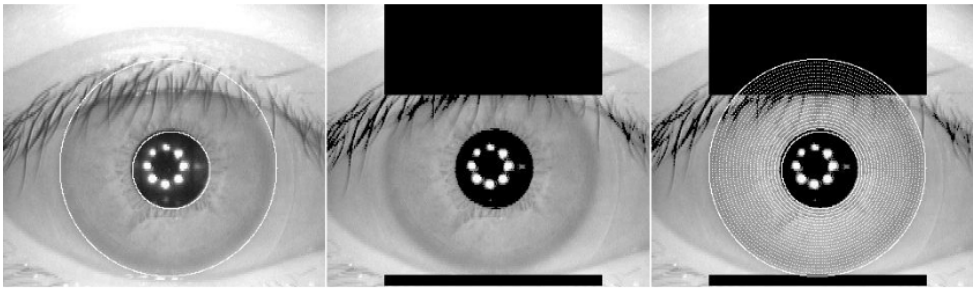
$$[-(x - h_i)\sin\theta_j + (y - k_j)\cos\theta_j]^2 = a_j[(x - h_i)\sin\theta_j + (y - k_j)\cos\theta_j]\,, \tag{5.5}$$

где a_j контролише закривљеност, (k_j, h_j) су врхови парабола, и θ представља угао у односу на x-осу.

Да би се детектовале спољне ивице зенице и дужице, примењује се кружна трансформација на слици на којој је претходно примењен Canny edge детектор за издвајање вертикалних ивица. За детекцију и уклањање капака примењује се линијска трансформација на слици на којој је примењен Canny edge детектор за издвајање



Слика 5.3: Пример детектовања кружница зенице и дужице на сл. 5.1, преузето из CASIA (http://biometrics.idealtest.org/) базе података биометријских узорака.



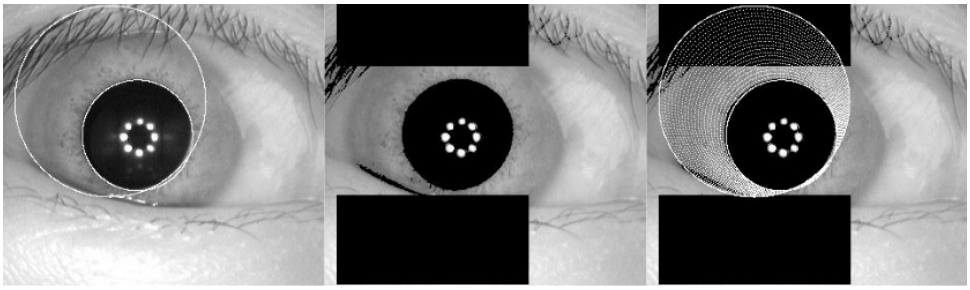
Слика 5.4: Примери успешне сегментације дужице, преузето из CASIA (http://biometrics.idealtest.org/) базе података биометријских узорака.

хоризонталних ивица. Пример детектовања кружница зенице и дужице дат је на сл. 5.3, а детектована кружница је представљена једначином:

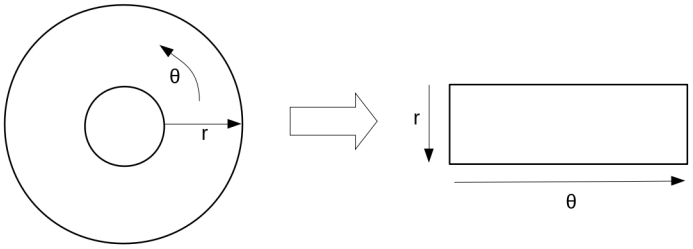
$$x^2 + y^2 - r^2 = 0 \, . \tag{5.6}$$

Практични проблеми ове трансформације су што је релативно спора, и што захтева ручно постављање прагова пропустљивости, што може довести до ефеката уклањања важних ивица или задржавања шума. Такође, ова трансформација је доста спора јер испитује пиксел по пиксел сваке ивице како би нашла одговарајуће облике. Приликом сегментације дужице, прво се детектује њена спољна ивица, па спољна ивица зенице. Након тога се детектују линије капака, да би се уклонио шум који они узрокују. Шум који узрокују трепавице се уклања на основу прага пропустљивости. Примери успешне и неуспешне сегментације дужице дате су на сл. 5.4 и 5.5, респективно.

Да би се упоредиле дужице различитих величина, потебно је извршити њихову нормализацију, што се врши применом Daugman-овог модела Rubber Sheet [33]. Овај модел трансформише слику дужице из кружне у правоугаону форму, превођењем



Слика 5.5: Примери неуспешне сегментације дужице, , преузето из CASIA (http://biometrics.idealtest.org/) базе података биометријских узорака.



Слика 5.6: Уобичајено илустровање поступка нормализације применом Daugman-овог модела Rubber Sheet.

из Декартовог координатног система у поларни:

$$I(x(r,\theta), y(r,\theta)) = I(r,\theta) \ , \tag{5.7}$$

где су:

$$x(r,\theta) = (1-r)x_p(\theta) + rx_i(\theta) \ , \tag{5.8}$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_i(\theta) \ , \tag{5.9}$$

$I(x,y)$ је почетна слика, а (x_p, y_p) и (x_i, y_i) координате центра кружница које одговарају спољним ивицама зенице и дужице. Уобичајена илустрација поступка нормализације дата је на сл. 5.6.

Центри кружнице које спољне ивице дужице и зенице се у општем случају не полкапају. Зато се посматрају центар зенице и вектор помераја између центра зенице и центра дужице:

$$r' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha - r_i^2} \ , \tag{5.10}$$

где су:

$$\alpha = o_x^2 + o_y^2 \ , \tag{5.11}$$

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

Слика 5.7: Нормализација дужице дате на сл. 5.1.

r_i је пречник дужице, o_x и o_y одређују верктор помераја, а r' је растојање између спољних ивица дужице и зенице.

У поступку нормализације дужице генерише се и маска нормализације, која садржи елементе који представљају шум (на пример капци и трепавице) и служи за редуковање шума приликом поређења. Сл. 5.7 садржи пример нормализоване дужице.

Један од захтева за поређење дужица је да шаблони дужица исте особе буду слични, без обзира на потенцијално различито осветљење током снимања које утиче на димензије зенице. Зато се у поступку кодовања из дужице издвајају кључна обележја која су јединствена за особу, применом 1Д логаритамског Габоровог филтера:

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

Нормализована дужица се декомпонује у више једнодимензионалних сигнала, од којих се сваки кодује применом Daugman-ове методе кодовања помоћу 2Д Габорових филтера:

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

где важи:

- $h_{Re,Im}$ је комплексни бит чије реалне и имагинарне компоненте узимају вредности 0 или 1.
- sgn је знак 2Д интеграла,
- $I(rho,\phi)$ је слика дужице у поларном координатном систему,
- α и β су величине 2Д таласа,
- ω је таласна фреквенција,

Слика 5.8: Кодовање дужице дате на сл. 5.1.

Слика 5.9: Маска шума за дужицу дату на сл. 5.1.

- (r_0, θ_0) су поларне координате региона дужица за које је израчунато $h_{Re,Im}$.

Применом овог филтера генеришу се по два бита за сваки фазор.

Резултат процеса кодовања је бинарни шаблон дужице. Сл. 5.8 садржи пример кодоване дужице, а сл. 5.9 пример маске шума. Код дужице и одговарајућа маска шума се заједно примењују у поступку поређења.

5.1.2 Класификација на основу дужице

За потребе поређења шаблона дужице може се применити Хемингово растојање, већ разматрано у глави 3. У основној форми, Хемингово растојање једнако је броју позиција у којима се кодови разликују:

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

Међутим, због присуства маски шума, адекватније је применити модификовано Хемингово растојање:

$$H(X_j, Y_j) = \frac{1}{N - \sum_{k=1}^{N} X_{n_k} \vee Y_{n_k}} \sum_{j=1}^{N} X_j \oplus Y_j \wedge X_{n_j} \wedge Y_{n_j} \ , \tag{5.16}$$

где важи:

- X_j и Y_j су два кодована шаблона дужице,
- X_n и Y_n су одговарајуће маске шума,
- N је сума битова која одговара сваком шаблону дужице.

У пракси се дешава да је слика дужице ротирана услед положаја главе. Ротација дужице може знатно да повећа растојање између кодова дужице, чак и кад се ради о истој особи. Да би се овај проблем превазишао, примењује се метода померања

шаблона дужице на једну и другу страну, коју је предложио Daugman. Помераји шаблона одговарају ротацији дужице. У поступку поређења шаблона X и Y, шаблон Y се помера неколико пута, симулирајући ротације дужице, и генеришући скуп шаблона

$$\mathbb{Y}(Y) = \{Y, Y_1, \ldots, Y_l\} \ . \tag{5.17}$$

Сваки шаблон из скупа $\mathbb{Y}$ се пореди са шаблоном X, а растојање између X и Y се рачуна као:

$$H(X, Y) = \underset{Y_i \in \mathbb{Y}(Y)}{\operatorname{argmin}} H(X, Y_i) \ . \tag{5.18}$$

Одлука о аутентификацији дужице се доноси поређењем вредности (5.18) са задатим прагом прихватљивости.

5.2 Перформансе предложеног система

Перформансе предложеног система зависе од неколико параметара попут квалитета саме камере или скенера дужице, осветљења, као и од параметара које користи алгоритам за издвајање вектора обележја. Јако је битно нагласити да у сценарију који се односи на мобилно банкарство, криптографска заштита или опозива биометрија немају никакав негативан утицај на тачност система – другим речима, примењене мере заштите не повећавају грешку која се односи на број лажно прихваћених или лажно одбијених корисника.

Већина експерименталих резултата пријављених у релевантној литератури заснована је на употреби CASIA-Iris базе података дужица. Међутим, како би се извели прави закључци о тачности верификације дужице на основу паметних телефона, односно мобилних уређаја, за прикупљање биометријских узорака и генерисање скупова података употребљена је предња камера Huawei P10 Lite телефона (телефон је релативно јефтин, што значи да сама камера није толико квалитетна попут оних које су уграђене у новијим и скупљим уређајима — другим речима, грешке могу само да се умање у случају употребе квалитетнијих уређаја).

Слике дужица обрађене су у софтверском пакету MATLAB (верзија R2016a). Скуп слика дужица коришћен у експерименту састоји се од 210 узорака преузетих од 10 субјеката, при чему су слике генерисане на дневној светлости (споља) и са различитим нивоима осветљења (унутра). Свака слика дужице је предобрађена и

Табела 5.1: Испитивање перформанси система (слике дужице су генерисане предњом камером мобилног телефона). Табела преузета из [77].

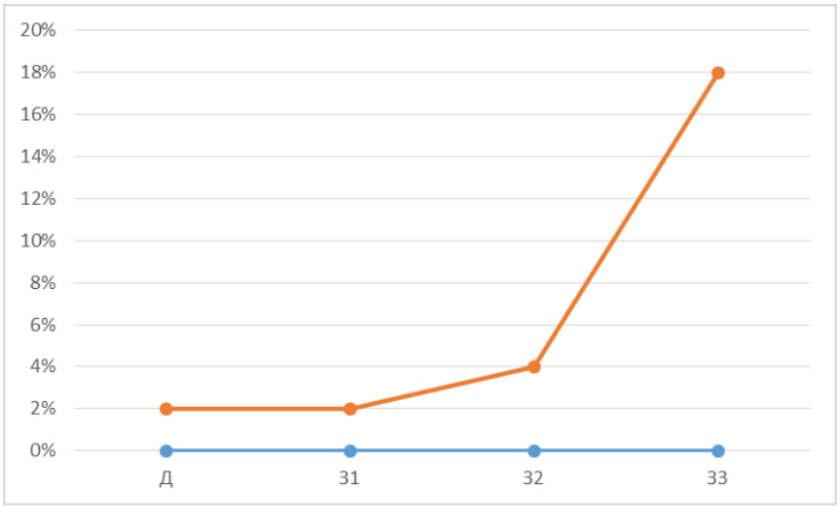
Праг поређења	Ознака за осветљење	FAR	FRR
Низак праг поређења (умањује грешку лажног прихватања, тј. FAR)	Д	0%	2%
	$З_1$	0%	2%
	$З_2$	0%	4%
	$З_3$	0%	18%
Висок праг поређења (умањује грешку лажног одбијања, тј. FRR)	Д	0%	0%
	$З_1$	0%	0%
	$З_2$	2%	2%
	$З_3$	6%	4%

нормализована у слику резолуције 240×20 пиксела, а након тога је примењен једнодимензионални логаритамски Габоров филтер са параметром $\sigma = 0,5$ и централном дужином од 12 пиксела, што генерише узорак од 9600 бита. Ови параметри су одабрани зато што је у истраживањима пријављеним у [1, 2] наглашено да обезбеђују висок ниво локалне ентропије и оптимално кодовање. Једна насумично изабрана слика преузета споља коришћена је за упис корисника, док су остале коришћене за верификацију.

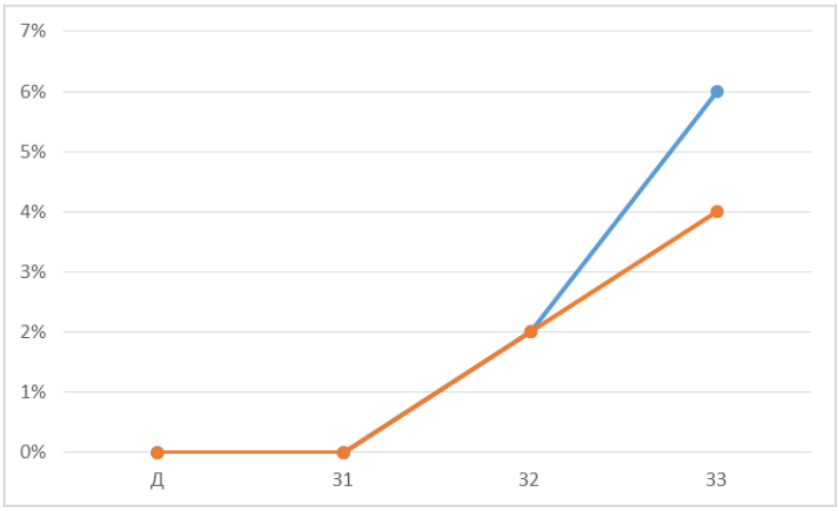
Резултати експеримента су представљени табелом 5.1 и приказани графиконима на сл. 5.10 и 5.11. Ознаке за осветљење на графиконима приказаним на сл. 5.10 и 5.11 су следеће:

- Д — снимак дужуце на дневној светлости,
- $З_1$ — снимак дужуце у затвореној застакљеној просторији (осветљење нормалног нивоа),
- $З_2$ — снимак дужуце у затвореној застакљеној просторији (осветљење средњег нивоа) и
- $З_3$ — снимак дужуце у затвореној застакљеној просторији (осветљење релативно ниског нивоа).

Иако верификација корисника са ниским прагом поређења за последицу има високу учесталост лажно одбијених корисника, ово не треба сматрати лошом особином решења зато што је кориснику дозвољено да покуша поново да се верификује. Проблем настаје у случају да је праг поређења висок, зато што се нелегитимни корисник



Слика 5.10: Перформансе система са ниским прагом поређења (плавом бојом је означен FAR, црвеном FRR).



Слика 5.11: Перформансе система са високим прагом поређења (плавом бојом је означен FAR, црвеном FRR).

може пријавити на систем као да је легитиман ако је Хемингово растојање између два низа битова веће.

Ово за последицу има појаву већег броја лажно прихваћених корисника у случају снимања у затвореној просторији са осветљењем осредњег нивоа (мање од 450 лумена, што одговара једној компактној флуоресцентној сијалици снаге од 9 до 11 вати која осветљава собу величине 25 квадратних метара) или слабим осветљењем (мање од 200 лумена, што одговара сијалици снаге од 3 до 5 вати која осветљава просторију исте величине).

Другим речима, ако је праг поређења висок, а осветљење неприкладно, систем је

подложан неприкладним одлукама, које нису прихватљиве у систему мобилног банкарства. Ван скупа неприкладних одлука, систем је стабилан и захтева евентуално поновно пријављивање корисника на систем. Другим речима, потребно је да праг поређења буде што нижи како би се избегле грешке лажног прихватања.

Праг поређења зависи од уређаја и камере који се користе за снимање слике дужице, и треба да се поставити на клијентској софтверској страни (уколико унапред израчунати оптимални праг за конкретни клијентски уређај постоји у записима који се односе на уређаје претходно коришћене у ту сврху). Алтернативно, овлашћени службеник финансијске институције, приликом првог уписа може поставити претходно поменути параметар (ако унапред израчунати подаци не постоје за конкретни модел уређаја).

У оквиру фазе накнадног уписа требало би узети у обзир неколико дужица корисника, скуп дужица различитих субјеката и могућност одређивања прага прећења који узима у обзир средње и стандардне девијације унутар класне и међукласне дистрибуције.

Крајња одлука препознавања дужице одређује се расподелом поређења Хемингових растојања истих у односу на на различите дужице [33]. Корисницима се не сме дозволити да самостално постављају вредност прага на мобилним уређајима.

Још једно питање на које треба дати одговор је присуство контактних сочива. Контактна сочива, нарочито сочива ошарана текстуром дужице, могу се употребити као лажна дужица, што представља додатни изазов системима за верификацију. Истраживања која се односе на утицај контактних сочива приликом верификације дужице описана су у [37, 145]. Yada и др. [145] објавили су у свом истраживању алгоритам за смањивање утицаја сочива, и доказали да њихов приступ значајно повећава перформансе верификације корисника.

5.3 Испитивање случајности

У овом делу рада испитаћемо случајност шифрованог биометријског шаблона и података који се преносе преко мреже. Случајност шаблона је битна зато што се на основу ње може проценити да ли постоји било каква корелација шаблона. Случајност података који се преносе је од значаја како нападач не би могао да дискриминише

шифрат шаблона од случајног низа.

Приликом испитивања случајности наилазимо на два проблема. Математички доказ да су низови заиста случајни не постоји, а такође не постоји ни универзални тест којим би се измерио квалитет низа битова. Другим речима, случајност се испитује низом тестова од којих сваки служи за мерење неке од карактеристика низа. Дефинишу се вредности на основу којих се одређује да ли је дати резултат задовољавајући и на основу серије тестова утврђује да ли низ поседује својство случајности.

Постоји неколико скупова тестова, од којих су неки застарели, попут FIPS 140-1 стандарда који садржи:

- монобитни тест,
- покер тест,
- тест секвенци различитих дужина и
- тест дугачких секвенци.

Због тога се овде примењује серија тестова коју је дефинисао је NIST [106] која се данас сматра *de-facto* стандардом за испитивање случајности. У овој серији тестова налазе се измењени тестови из FIPS 140-1 стандарда као и неки нови, попут:

- Мауеровог универзалног статистичког теста,
- испитивања приближне ентропије и
- теста заснованог на дискретног Фуријеовој трансформацији.

Детаљи о начинима тестирања, рачунању вредности P у тестовима и другим параметрима описани су у [83, 106].

Подаци који се испитују у овом делу рада генерисани су употребом RSA генератора псеудослучајних низова, SHA-3 хеш функције која генерише отисак дужине 256 бита и RSA алгоритма са јавним кључем дужине 2048 бита.

Најпре је извршена анализа случајности шифрованог опозивог шаблона дужине 9600 бита. Претпоставља се да шаблон поседује особине случајности зато што је настао као резултат извршавања операције екслузивно ИЛИ над оригиналним шаблоном, кључем за трансформацију који је случајни низ и генерисаним псеудослучајним низом.

Резултати тестова су дати у попису који следи (в. табелу 3.2 у 3. глави) и сумирани у табели 5.2.

1. Испитивање учесталости у низу (енгл. *test for examining the frequency in the series*). Резултат овог теста је $P = 0,817215$. Пошто је $P \geq 0,01$ сматра се да је основу овог теста шаблон показује особине случајности.

2. Испитивање учесталости у блоку (*the test for examining the frequency in the block*). Резултат овог теста је $P = 0,962751$. И на основу овог теста шаблон се може сматрати случајним низом зато што је $P \geq 0,01$.

3. Испитивање узастопног понављања истих битова у низу (енгл. *the test for examining the successive repetition of the same bits in the series*). Као резултат овог теста добијена је вредност $P = 0,029180$, што указује на случајност зато што је $P \geq 0,01$.

4. Испитивање најдужег узастопног понављања јединица у n-битним блоковима (енгл. *the test for examining the longest consecutive repetition of units in n-bit blocks*). Добијена вредност $P = 0,297120$ упућује на то да је шаблон на основу овог теста случајан зато што је $P \geq 0,01$.

5. Испитивање стања бинарне матрице (енгл. *the test for examining the state of the binary matrix*). Резултат теста је $P = 0,689410$ — другим речима, низ је случајан зато што је $P \geq 0,01$.

6. Тест заснован на дискретној Фуријеовој трансформацији (енгл. *the test for examining the discrete Fourier transform*). Вредност P једнака је 1, што указује на чињеницу да је сходно резултатима овог теста шаблон случајан.

7. Испитивање непреклапајућих узорака (енгл. *the test for examining the non-overlapping samples*). Као резултат теста, добијено је $P = 0,981392$, што значи да је низ случајан и на основу овог теста.

8. Испитивање преклапајућих узорака (енгл. *the test for examining the overlapping samples*). Овај тест не враћа као резултат конктетну P вредност, већ само бинарну одлуку — низ је задовољио (SUCCESS) или није задовољио (FAILURE)

Табела 5.2: Сумарни резултати испитивања случајности шифрованог опозивог шаблона. Редни бројеви тестова су усклађени са редним бројевима у опису.

Тест бр.	P-вредност(и)	Исход
1.	$P = 0,817215$	Успех
2.	$P = 0,962751$	Успех
3.	$P = 0,029180$	Успех
4.	$P = 0,297120$	Успех
5.	$P = 0,689410$	Успех
6.	$P = 1$	Успех
7.	$P = 0,981392$	Успех
8.	—	Успех
9.	$P = 0,921749$	Успех
10.	$P_1 = 0,012001,\ P_2 = 0,937112$	Успех
11.	$P = 0,839057$	Успех
12.	$P_1 = 0,991329,\ P_2 = 0,932901$	Успех

критеријуме теста. Пошто је као резултат теста добијена одлука SUCCESS, сматра се да је шифровани шаблон успешно прошао и овај тест.

9. Испитивање линеарне сложености (енгл. *the test for examining the linear complexity*). Резултат теста је $P0,921749$. Пошто је $P \geq 0,01$, шаблон је задовољио услове задате овим тестом.

10. Испитивање учесталости свих могућих преклапања n-битних поднизова у целом низу (енгл. *the serial test*). Резултати теста су вредности $P_1 = 0,012001$ и $P_2 = 0,937112$. Шаблон се на основу резултата може сматрати случајним, пошто су $P_1 \geq 0,01$ и $P_2 \geq 0,01$.

11. Испитивање приближне ентропије (енгл. *the test for examining the approximate entropy*). као резултат у овом случају враћа вредност $P = 0,839057$ што значи да је низ на основу добијене P вредности случајан.

12. Испитивање збирова случајних поднизова (енгл. *the test for examining the random summations*). Као резултат добија се $P_1 = 0,991329$ и $P_2 = 0,932901$. Узевши у обзир да је $P_1 \geq 0,01$ и $P_2 \geq 0,01$, низ је задовољио критеријуме овог теста.

Пошто је низ задовољио критеријуме свих наметнутих тестова, можемо сматрати да поседује довољно висок ниво случајности, чиме је претпоставка потврђена.

Као и за испитивање случајности шаблона, случајност података који се преносе преко мреже испитује се NIST скупом тестова. Неопходно је испитати случајност

Табела 5.3: Сумарни резултати испитивања случајности података који се преносе преко мреже. Редни бројеви тестова су усклађени са редним бројевима у табели 5.2.

Тест бр.	P-вредност(и)	Исход
1.	$P = 0,836312$	Успех
2.	$P = 0,971007$	Успех
3.	$P = 0,031070$	Успех
4.	$P = 0,312240$	Успех
5.	$P = 0,691870$	Успех
6.	$P = 1$	Успех
7.	$P = 0,990124$	Успех
8.	—	Успех
9.	$P = 0,930273$	Успех
10.	$P_1 = 0,013105,\ P_2 = 0,939076$	Успех
11.	$P = 0,841131$	Успех
12.	$P_1 = 0,992517\ P_2 = 0,954713$	Успех

ових података како би се онемогућио напад разликовањем. Податак који се шаље генерисан је извршавањем операције ексклузивно ИЛИ над псеудослучајним низом и два опозива шаблона који припадају истом кориснику. Треба напоменути да случајност ових података зависи од ентропије генерисаног случајног низа и кључева за једносмерну трансформацију. Пошто је употребљен јак криптографски генератор, а кључеви за трансформацију су генерисани као случајни низови, може се претпоставити да ће и ови подаци задовољити критеријуме који намећу тестови случајности.

Резултати испитивања случајности података који се преносе преко мреже дати су у табели 5.3. Пошто су задовољени критеријуми свих наметнутих тестова, може се сматрати је ниво случајности висока чиме је претходно поменута претпоставка потврђена.

Овим је показано да осетљиви подаци који су смештени на телефону (конкретно, шифровани шаблони) и подаци које нападач може пресрести поседују довољну количину случајности, у случају да се користе јаке криптографске мере заштите, што значи да је нападачу онемогућено да изврши корелацију шаблона или да изврши напад разликовањем податка од случајног низа.

Глава 6

Критичка анализа и закључак

У односу на велики број модела и начина примене криптографске заштите биометријских система за проверу идентитета пријављених у литератури, модел предложен у овом раду не умањује тачност класификације субјеката и не захтева додатне процесорске ресурсе, као ни простор за складиштење.

Недостатак модела пријављених у релевантној литератури је повећање учесталости лажно прихваћених и лажно одбијених корисника која потиче од система заштите заснованих на шифарским системима — било да су у питању системи са симетричним или јавним кључем или хомоморфни шифарски системи — као и од алгоритама употребљених у неинвертибилним трансформацијама.

Предложеним модуларним приступом криптографској заштити биометријских шаблона успешно су решени проблеми који се односе на процесорску захтевност и умањење тачности верификације корисника, као и услови које треба да задовољи идеални биометријски систем. У односу на предложена решења објављена у релевантној литератури, предложени систем за проверу идентитета корисника је независтан од криптографских мера заштите које су примењене, а осим тога и од подсистема за издвајање обележја која морају бити бинаризована. Независност предложеног решења од конкретних криптографских алгоритама, као и од алгоритама за издвајање бинарних неопозивих биометријских шаблона може се сматрати изазовом за пројектанте нових криптографских решења или алгоритама за издвајање бинаризованих обележја.

Недостатак предложеног модела је зависност од биометријских шаблона генерисаних на основу извршења операције екслузивно ИЛИ. За сада је у релевантној

литератури пријављено неколико модалитета који могу бити бинаризовани — почев од кода дужице — а накнадно су пријављене шеме за генерисање бинарних биометријских шаблона отисака прстију, и условно речено, други модалитети за које је пријављена тачност верификације неупотребљива у предложеном моделу. Модалитети попут гласа и сличних понашајних биометријских узорака за сада нису бинаризовани.

Предложена имплементација модела која користи јаке криптографске алгоритме постиже јако високу тачност провере идентитета корисника, као и ниску учесталост лажно прихваћених и одбијених корисника.

На основу експеримената извршених на реалистичном скупу података, може се закључити да је систем употребљив у већини доменима примене, попут мобилног банкарства.

6.1 Закључак и резиме доприноса

Истраживање представљено у овом раду потврдило је постављене истраживачке хипотезе:

Хипотеза 3. Тренутна решења за заштиту биометријских шаблона не обезбеђују довољно висок ниво сигурности шаблона и приватности корисника.

Хипотеза 4. Развојем сопственог биометријског система у ком биометријски шаблони остају шифровани или у најгорем случају опозиви током свих фаза њихове примене (складиштење, пренос и верификација) обезбеђује се употребљивост предложеног приступа у реалним доменима примене.

Поред тога, показано је да опозива биометрија не мора да наруши тачност верификације корисника, што је условно неизводљиво за модалитете који нису засновани на XOR биометрији.

Важно је истаћи да примењена метода криптографске заштите није умањила тачност верификације корисника, што до сада није пријављено у релевантној литератури. У условима нормалног осветљења при аквизицији слике, грешка лажног прихватања конвергира нули.

Циљ је постигнут кроз емпиријско истраживање, које је потврдило да се употребом предложеног решења значајно смањује број лажно одбијених корисника, док се уз употребу исправно одабраног прага може смањити и број лажно прихваћених корисника.

Потврђени доприноси овог рада су следећи:

- предложена је нова метода за проверу идентитета корисника помоћу шифрованих опозивих биометријских шаблона;
- предложено решење је модуларно у погледу примењених криптографских механизама, и независно од тога да ли се примењују шифарски алгоритми са симетричним или јавним кључем;
- предложена је измењена шема за верификацију дужице у систему — шема не користи кодове за корекцију грешака, а верификација корисника се не заснива на поређењу хеш кодних речи које носе минималну количину информације о биометријском узорку;
- предложени систем за проверу идентитета је погодан за примену у сценарију мобилног банкарства, зато што је грешка лажног прихватања занемарљива, а величина биометријског узорка је прикладна за смештање на мобилним уређајима (за разлику од биометријских узорака добијених хомоморфним шифровањем, који су знатно већи);
- предложено решење је применљиво у технологији облака због релативно ниске процесорске захтевности, за разлику од других шифарских алгоритама који су знатно захтевнији по питању процесорских ресурса.

6.2 Смернице за даља истраживања

Потенцијална даља истраживања у овој области укључују:

- истраживања везана за бинаризовање других биометријских модалитета, попут лица или гласа;
- формирање система за верификацију која није заснована на употреби операције ексклузивно ИЛИ.

Библиографија

[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. Boult: 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. Boult, 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. Boult, W. Scheirer: Bio-cryptographic protocols with bipartite biotokens. Proc of the IEEE Biometric Symposium, BSYM '08, pp. 9–16. 150, 2008.

[17] T. Boult, 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 identication 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. Pschernig, 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 commitment 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: Sectored 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. Breitinger, 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. Breitinger, 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. Boult: 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, 1984.

[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.

Индекс