

UNIVERZITET SINGIDUNUM

-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Biometrijski sistemi, njihova bezbednost i generisanje kriptografskih ključeva

- Master rad -

Mentor:
Prof. dr. Mladen Veinović

Student:
Miloš Mitrović
Br. indeksa: 410042/2013

Univerzitet Singidunum

Beograd, 2014

Biometrijski sistemi, njihova bezbednost i generisanje kriptografskih ključeva

Sažetak: U ovom radu predmet razmatranja biće savremeni biometrijski sistemi, njihova bezbednost, kao i korišćenje istih za potrebe generisanja kriptografskih ključeva. U prvom delu razmatraće se biometrija uopšte, biometrijski parametri, biometrijski sistemi, kako oni funkcionišu, gde se primenjuju, koje su im prednosti i mane, a biće obuhvaćeni i multibiometrijski sistemi. Zatim, sagledavaće se bezbednosni aspekti funkcionisanja savremenih biometrijskih sistema, izazovi sa kojima se susreću, kao i moguća rešenja tih bezbednosnih problema. Na kraju, razmatraće se mogućnost njihovog korišćenja za potrebe generisanja kriptografskih ključeva, i biće predstavljeno trenutno stanje u toj oblasti.

Ključne reči: biometrijski parametri, biometrijski sistemi, bezbednost biometrijskih sistema, generisanje kriptografskih ključeva

Biometric systems, their security and cryptographic key generation

Abstract: In this paper, subject of dicussion will be modern biometric systems, their security, and how are they utilized for cryptographic key generation. In the first part, we will discuss about biometrics, biometric parameters, biometric systems, how they work, their applications, advantages and disadvantages, and also, about multibiometric systems. After that, we will review security aspects of modern biometric systems, challenges they face, and possible solutions of their security problems. Lastly, we will discuss about their potential utilization for cryptographic key generation, and we will present the current state in that field.

Keywords: biometric parameters, biometric systems, biometric systems security, cryptographic key generation

SADRŽAJ

1. Uvod 4

2. Metodologija naučnog istraživanja 5

2.1 Uvodne napomene 5

2.2 Predmet istraživanja 5

2.3 Cilj istraživanja 5

2.4 Istraživačke hipoteze 5

2.5 Metodi istraživanja i tok istraživačkog procesa 6

3. Osnovni pojmovi 7

3.1 Identitet u savremenim sistemima 7

3.2 Biometrija i biometrijski parametri 8

3.3 Bitne osobine biometrijskih parametara 9

3.4 Kriptografija 11

3.5 Digitalni potpis 12

3.6 Steganografija, digitalni vodeni žig i vizuelna kriptografija 13

4. Biometrijski sistemi 14

4.1 Biometrijski sistem – pojam i način rada 14

4.2 Osnovni elementi biometrijskog sistema 15

4.3 Pokazatelji performansi biometrijskih sistema 16

4.4 Primena biometrijskih sistema 17

4.5 Klasifikacija biometrijskih sistema 18

4.6 Biometrijski sistemi i privatnost 19

4.7 Prednosti i mane biometrijskih sistema 21

5. Individualni biometrijski sistemi 23

5.1 Otisak prsta 23

5.2 Lice 25

5.3 Iris 27

5.4 Mrežnjača 28
5.5 Geometrija šake 29
5.6 Otisak dlana 30
5.7 Raspored krvnih sudova ruke ili prsta 31
5.8 DNK 32
5.9 Uvo 33
5.10 Glas 34
5.11 Potpis 35
5.12 Dinamika otkucaja na tastaturi 36
5.13 Hod 37
5.14 Biometrijski parametri koji imaju potencijalnu primenu 38
5.15 Meke biometrijske karakteristike 39
6. Multibiometrijski sistemi 40
6.1 Pojam i razlozi nastanka 40
6.2 Komponente multibiometrijskih sistema 40
6.3 Bitni segmenti rada 41
7. Bezbednosni problemi i specifičnosti biometrijskih sistema 44
7.1 Specifične karakteristike i zahtevi kod biometrijskih sistema 44
7.2 Bezbednosni problemi 45
7.3 Napadi na elemente sistema 47
8. Rešenja bezbednosnih problema 49
8.1 Funkcionalni problemi koji utiču na bezbednost 49
8.2 Opšti bezbednosni problemi 49
8.3 Specifični napadi na elemente biometrijskih sistema 49
9. Bezbednost biometrijskih obrazaca 51
9.1 Primena kriptografskih algoritama 51
9.2 Izdvajanje biometrijskih podataka na smart kartice 53
9.3 Steganografija, digitalni vodeni žigovi i vizuelna kriptografija 54
9.4 Primena transformacija podataka i biometrijskih kriptosistema 55
9.4.1 Sistemi bazirani na transformacijama podataka 56

9.4.2 Biometrijski kriptosistemi 58
9.4.3 Kombinovani sistemi 61
10. Generisanje kriptografskih ključeva na osnovu biometrijskih parametara. 63
10.1 Generisanje kriptografskih ključeva 63
10.2 Primena biometrijskih parametara za potrebe generisanja ključeva 64
10.3 Otisak prsta 65
10.4 Lice 67
10.5 Iris 68
10.6 Mrežnjača 69
10.7 Otisak dlana 70
10.8 Raspored krvnih sudova 70
10.9 DNK 71
10.10 Glas 72
10.11 Potpis 73
10.12 Multibiometrijski sistemi 73
11. Zaključak 75
Literatura 77

1. Uvod

Savremeni trendovi i razvoj tehnologija, kao i sve veća integracija Interneta u različite životne i poslovne procese, iznose i zahtev za iznalaženjem adekvatnih rešenja i mehanizama zaštite. Ti procesi podrazumevaju širok spektar aktivnosti, stvaranje, razmenu i čuvanje velikih količina bitnih podataka, kontrolisanje pristupa njima i uspostavljanje kompleksnih linija komunikacija, pri čemu se njihova realizacija i adekvatan nivo bezbednosti postiže kriptografskim ili drugim zaštitnim tehnikama, među kojima je i primena biometrijskih sistema.

Biometrijski sistemi se mogu uopšteno definisati kao tehnički sistemi koji na bazi odgovarajućih, karakterističnih detalja, vrše prepoznavanje ili neku drugu funkciju. Pri razmatranju biometrijskih sistema, treba imati u vidu da su biometrijski parametri, na osnovu kojih ti sistemi funkcionišu, sastavni deo ljudske svesti, jer mi prepoznajemo i razlikujemo jedni druge po licu, glasu, načinu hoda, visini i sl. Sama ta činjenica, govori dosta o značaju i potencijalu biometrije i o mogućnostima koje pruža njeno inkorporiranje u funkcionalne tehničko-tehnološke sisteme.

Zbog navedenog, a i drugih prednosti, biometrijski sistemi imaju zapaženu ulogu, kada se radi o pitanjima bezbednosti, identifikacije ili generisanja kriptografskih ključeva, ali isto tako imaju i čitav niz mana, koje su predmet istraživanja i razvoja, kako bi se one otklonile. Takođe, treba imati u vidu da su i sami biometrijski sistemi, kao faktor zaštite i realizacije određenih ciljeva, izloženi različitim vidovima ugrožavanja njihovog funkcionisanja i narušavanja bezbednosti podataka, i voditi računa o tome, prilikom njihove implementacije u odgovarajuće sisteme.

U prvom delu ovog rada, razmatraće se biometrija i biometrijski parametri, osnovni pojmovi vezani za funkcionisanje i formiranje biometrijskih sistema, prednosti i mane biometrijskih sistema uopšte i njihove primene, kao i individualni biometrijski sistemi. Takođe, sagledavaće se i objedinjavanje tih biometrijskih sistema u multibiometrijske sisteme.

U drugom delu rada, razmatraće se bezbednosni problemi funkcionisanja biometrijskih sistema i zaštite biometrijskih obrazaca. Takođe, sagledavaće se primena kriptografskih, steganografskih i drugih tehnika za rešavanje tih problema.

U poslednjem delu, razmatraće se korišćenje biometrijskih parametara za potrebe generisanja kriptografskih ključeva. Predmet sagledavanja biće primeri korišćenja pojedinih biometrijskih parametara u te svrhe.

2. Metodologija naučnog istraživanja

2.1 Uvodne napomene

U ovom istraživanju obuhvaćeni su biometrijski sistemi, sa razmatranjem njihovih karakteristika, načina realizacije, i različitih primena, u cilju rešavanja različitih bezbednosnih problema, pri čemu se mora uzeti u obzir i njihovo bezbedno funkcionisanje, odnosno, sagledati izazovi sa kojima se susreću i tehnike njihovog rešavanja. Takođe, biće obuhvaćena i problematika generisanja kriptografskih ključeva, sa osvrtom na pojedina rešenja koja su zasnovana na primeni biometrijskih parametara i razmatranjem njihovog potencijala za te svrhe.

2.2 Predmet istraživanja

Predmet ovog istraživanja su biometrijski sistemi, njihova bezbednost i primena za potrebe generisanja kriptografskih ključeva. Obuhvaćeni su pojmovi biometrije, kriptografije, steganografije, metodologije funkcionisanja biometrijskih sistema sa njihovim prednostima i manama, zatim bezbednosni problemi kako biometrijskih sistema, tako i podataka na osnovu kojih oni funkcionišu, kao i moguća rešenja. Takođe, obuhvaćene su metodologije generisanja kriptografskih ključeva, kao i korišćenje biometrijskih parametara u cilju generisanja pomenutih ključeva, sa razmatranjem potencijalnih rešenja.

2.3 Cilj istraživanja

Naučni cilj: Istraživanje, definisanje i analiza funkcionisanja biometrijskih sistema, njihovih bezbednosnih problema i potencijalnih rešenja, kao i njihove primene za potrebe generisanja kriptografskih ključeva.

Društveni ciljevi: Obezbeđivanje adekvatnog informisanja svih koji razmatraju primenu biometrijskih sistema o njihovim karakteristikama, bezbednosnim problemima i rešenjima kao i o mogućnostima njihove primene za generisanje kriptografskih ključeva.

2.4 Istraživačke hipoteze

Opšta hipoteza: Savremeno društvo se suočava sa nizom bezbednosnih izazova, za koje je potrebno naći adekvatna rešenja, a jedno od mogućih rešenja je i primena biometrijskih sistema. Zbog svojih karakteristika, i brojnih prednosti, imaju veliki potencijal za primenu u cilju zaštite, identifikacije ili generisanja kriptografskih ključeva, i shodno tome, predstavljaju oblast istraživanja od velikog značaja. Međutim, kao i drugi sistemi, i oni su sami potencijalna meta napada, i bitno je imati u vidu njihove bezbednosne probleme pri razmatranju njihove implementacije u odgovarajući sistem.

Posebna/radna hipoteza: Biometrijski sistemi predstavljaju potencijalno rešenje za više bezbednosnih problema, među kojima je i generisanje kriptografskih ključeva, ali moraju se imati u vidu i njihove mane, kao i njihova bezbednost.

2.5 Metodi istraživanja i tok istraživačkog procesa

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije.

Metoda deskripcije je korišćenja pri objašnjavanju osnovnih pojmova i sistema funkcionisanja.

U teorijskim segmentima su primenjene metode indukcije, dedukcije i analize, a u izvođenju zaključaka metode sinteze i generalizacije.

3. Osnovni pojmovi

3.1 Identitet u savremenim sistemima

Funkcionisanje savremenog društva i čitav niz segmenata na kojima se ono zasniva, postavlja zahtev za pouzdanim utvrđivanjem ili potvrđivanjem identiteta osobe u velikom broju procesa, i za to se razmatraju i koriste različiti metodi. Njih možemo da grupišemo u sledeće kategorije [1]:

Na osnovu onoga što osoba zna, gde se to postiže korišćenjem neke tajne vrednosti, koju samo ta osoba zna, kao što su lozinke, PIN brojevi, odgovor na neko pitanje...

Na osnovu onoga što osoba poseduje, gde se to postiže korišćenjem neke stvari koja se nalazi u posedu te osobe, kao što su smart kartice, tokeni...

Na osnovu onoga što osoba jeste, gde se to postiže na korišćenjem njenih unikatnih fizioloških karakteristika i obrazaca ponašanja, poput otiska prsta, lica, irisa i sl.

Svaki od predloženih načina ima svoje prednosti i mane. Najednostavniji za primenu su lozinke ili neki drugi parametar koji osoba zna, ali njih je moguće zaboraviti, slučajno otkriti ili podeliti sa nekim.Takođe, mogu da budu i pogođene, primenom adekvatnih tehnika, pri čemu korisnik može da bude nesvestan toga i da nastavi sa korišćenjem iste. Sistemi na osnovu posedovanja predstavljaju sledeći nivo, i nude niz prednosti, jer nema potrebe za pamćenjem nečega, i teže ih je podeliti ili neovlašćeno kopirati. U slučaju krađe ili gubitka, korisnik je uglavnom svestan toga i može da preduzme odgovarajuće mere. Biometrijski parametri takođe imaju niz prednosti jer ne zahtevaju pamćenje ili posedovanje nečega, ne mogu se podeliti, niti mogu biti ukradeni. Postoji mogućnost njihovog neovlašćenog prikupljanja i falsifikovanja, pri čemu je takav vid napada na ove sisteme relativno kompleksan za realizaciju, a javlja se i pitanje njihove preciznosti, zbog difuzne prirode biometrijskih parametara.

Kako bi se te mane otklonile, pri formiranju funkcionalnih sistema, mogu se implementirati različite kombinacije navedenih sistema. Multifaktorska autentifikacija predstavlja kombinovanje više načina rada, u nekim slučajevima i svih, u šta spada npr. smart kartica sa biometrijskim obrascem i korišćenjem i PIN broja, ili korišćenje kartice, lozinke i nekog biometrijskog parametra (otisak prsta, lice, iris, glas...) za potrebe potvrđivanja identiteta. Pored navedenog, još se koristi i izraz dvofaktorska autentifikacija, kojim se označava kombinovanje dva načina rada, npr. znanja i posedovanja (bankovna kartica i PIN broj) ili posedovanja i biometrijskih parametara (biometrijski lični dokumenti), u cilju pouzdane realizacije potvrde identiteta. Imajući u vidu savremene tehnike i tehnologije, kao i veliki broj mogućnosti ugrožavanja bezbednosti kod individualnih načina rada, kombinovanjem dva ili više načina rada značajno se podiže bezbednost funkcionisanja celog sistema i povećava otpornost na zloupotrebe, a pri tom se otklanjaju i funkcionalni nedostaci individualnih sistema.

3.2 Biometrija i biometrijski parametri

Reč biometrija je nastala od grčkih reči bios (*život*) i metron (*mera*) i koristi se da označi neku merljivu fiziološku karakteristiku ili obrazac ponašanja, koja se može iskoristiti za prepoznavanje osobe, ali i automatizovan metod prepoznavanja neke osobe na bazi pomenutih karakteristika, koje nazivamo biometrijskim parametrima.

Biometrijske parametre delimo na fiziološke karakteristike i obrasce ponašanja.

Fiziološke karakteristike koje imaju primenu sa aspekta biometrijskih sistema su:

- otisak prsta
- lice
- iris
- mrežnjača
- geometrija šake
- otisak dlana
- raspored krvnih sudova ruke ili prsta
- DNK
- uvo

Obrasci ponašanja koji imaju primenu sa aspekta biometrijskih sistema su:

- glas
- potpis
- dinamika otkucaja na tastaturi
- hod

Biometrijski parameteri koji imaju potencijal za korišćenje za potrebe biometrijskih sistema i koji su predmet razmatranja i istraživanja:

- miris
- rukopis
- pokreti usana
- elektrokardiogram
- elektroencefalogram
- nokat
- stisak šake
- dinamika pokreta miša i dr.

3.3 Bitne osobine biometrijskih parametara

Bitne osobine, kojima se određuje primenljivost biometrijskih parametara za integraciju u neki biometrijski sistem su [2]:

Univerzalnost, koja se odnosi na to da bi svaka osoba trebala da ima tu karakteristiku ili obrazac ponašanja.

Jedinstvenost, koja se odnosi na to da dve osobe ne bi smele da imaju istu tu karakteristiku ili obrazac ponašanja.

Trajnost, koja se odnosi na to da se karakteristika ili obrazac ponašanja ne bi smela menjati sa starenjem.

Prikupljivost , koja se odnosi na to da se karakteristika ili obrazac ponašanja mogu kvantitativno izmeriti.

Performanse, koja se odnosi na postignutu preciznost, resurse koji su potrebni da bi se postigla ta preciznost, kao i faktore koji utiču na preciznost, kod karakteristike ili obrasca ponašanja.

Prihvatljivost, koja se odnosi na to koliki je stepen prihvatanja biometrijskog sistema zasnovanog na toj karakteristici od strane ljudi.

Zaobilaženje, koja se odnosi na to koliko je lako zavarati sistem tehnikama obmane.

Otisak prsta ima visoku jedinstvenost i razlikuje se i kod identičnih blizanaca, ne menja se sa protokom vremena, ali postoji mogućnost da bude oštećen i uništen usled povrede, zbog same svoje prirode, tako da univerzalnost može da bude dovedena u pitanje. Relativno je lak je za prikupljanje, prirodan je i prihvaćen od strane korisnika, mada ima i negativne konotacije. Sistemi imaju zadovoljavajuće performanse, međutim, postoji veliki broj napada i samim tim, postoji i mogućnost da sistem bude zavaran lažnom biometrijom.

Lice odlikuje manja jedinstvenost, jer postoje manje ili veće sličnosti i razlike, ali je neodvojiv i univerzalan biometrijski parametar. Postoji mogućnost promena, usled starenja ili povreda, ali je lak za prikupljanje, pri čemu se to može učiniti i neprimetno, pa je zbog toga izuzetno prihvaćen. Sistemi su kompleksniji, zbog difuzne strukture lica kao biometrijskog parametra, ali su performanse na zadovoljavajućem nivou. Međutim, lako ga je i neovlašćeno prikupiti i zavarati, tako da to umanjuje upotrebljivost.

Iris ima visoku jedinstvenost, razlikuje se i kod identičnih blizanaca, promene na njemu, usled starenja, su suptilne i ne utiču na funkcionisanje, a i više je zaštićen, tako da mu je univerzalnost na višem nivou, iako i kod njega može da dođe do povrede i onemogućavanja korišćenja. Relativno je lak za prikupljanje i u određenoj meri je prihvaćen od strane korisnika, iako nije toliko prirodan. Sistemi su komplikovaniji i to utiče na performanse, ali ga je zato dosta teže neovlašćeno prikupiti i prezentovati, mada nije nemoguće, tako da je sa aspekta zavaravanja na višem nivou funkcionisanja.

Mrežnjaču isto odlikuje visoka jedinstvenost, razlikuje se čak i između očiju, pri tom je zaštićena i ne menja se usled bolesti ili protoka vremena, tako da sa aspekta univerzalnosti i trajnosti zauzima viši nivo. Međutim, ovaj sistem je teži za realizaciju sa stanovišta prikupljanja podataka, i kompleksniji, pa to utiče na performanse i izuzetno je invazivan, tako da izaziva nelagodnost i značajno umanjuje prihvatljivost. Sa druge strane, skoro ga je nemoguće falsifikovati tako da je izuzetno otporan sa stanovišta zavaravanja.

Geometrija šake nema visoku jedinstvenost, tako da ima primenu samo sa aspekta verifikacije identiteta, ne menja se značajno sa protokom vremena, ali može da bude otežana primena ovog sistema usled povrede ili bolesti. Relativno je lak za realizaciju sa aspekta prikupljanja i performansi sistema, ima solidnu prihvatljivost, ali nivo preciznosti mu je takav da postoji potencijal zavaravanja.

Otisak dlana ima visoku jedinstvenost, ne menja se sa protokom vremena, ali može biti oštećen ili uništen usled povrede, tako da to utiče na univerzalnost. Relativno je lak za prikupljanje, prirodan je i prihvatljivost mu je na zadovoljavajućem nivou. Performanse sistema su na adekvatnom nivou, kao i otpornost na zavaravanje.

Raspored krvnih sudova, dlana, prsta ili uopšte, ima relativno visoku jedinstvenost i univerzalnost, ne menja se sa protokom vremena, dosta je zaštićen, mada postoji mogućnost promene usled povrede. Prikupljanje zahteva odgovarajuću opremu, ali nije teško, i performanse sistema su adekvatne, ima veću prihvatljivost i veliku otpornost na zavaravanje.

DNK ima visoku jedinstvenost, sem u slučajevima identičnih blizanaca, univerzalan je, otporan na promene i ne menja se sa starenjem. Teži je za prikupljanje jer zahteva specijalizovanu opremu i stručan kadar, a i sistemi se kompleksni, pa to utiče na performanse. Pored toga, sadrži privatne informacije o ličnosti, tako da postoji negativna strana sa aspekta prihvatanja, i ranjiv je sa aspekta zavaravanja, jer se uzorak može i neovlašćeno prikupiti.

Uvo je univerzalan parametar, za koga se smatra da je jedinstven ali je to još predmet razmatranja, koji se ne menja sa starenjem ali može biti oštećen, usled povrede. Relativno je lak za prikupljanje, ali su sistemi predmet daljeg razvoja, tako da je teško diskutovati o performansama. Prihvatljivost je na visokom nivou, ali ne i otpornost na zavaravanje.

Glas ima određeni nivo jedinstvenosti, i dosta veliku univerzalnost , ali moguće su promene na njemu usled protoka vremena, povrede, bolesti ili emocionalnog stanja. Lak je za prikupljanje i ima visok nivo prihvatanja, performanse su zadovoljavajuće ali je i izuzetno lak za neovlašćeno prikupljanje, a sistemi, u zavisnosti od realizacije, mogu da budu osetljivi na zavaravanje.

Potpis, kao obrazac ponašanja, je predmet razmatranja sa apekta jedinstvenosti, ali se smatra da je ona dosta visoka, univerzalnost je na određenom nivou, a moguće su promene usled protoka vremena, emocionalnog stanja i drugih razloga. Prikupljanje zahteva odgovarajuću opremu, ali nije teško za realizaciju, performanse su na zadovoljavajućem nivou, a u zavisnosti od realizacije sistema zavisi i otpornost na zavaravanje.

Dinamika otkucaja na tastaturi je specfičan parametar, smatra se da ima odgovarajuću jedinstvenost i visoku univerzalnost, moguće su promene sa protokom vremena ali ne u toj meri da utiču na sistem. Lak je za prikupljanje, prihvatljiv, performanse su zadovoljavajuće za određene namene, a i poseduje relativnu otpornost je na zavaravanje.

Hod je isto parametar koji je predmet razmatranja, smatra se da ima visoku jedinstvenost, visoku univerzalnost, ali moguće su promene usled emocionalnog stanja i

povrede, dok se manje menja usled protoka vremena. Lak je za prikupljanje , prihvatljiv i performanse su na određenom nivou, a i relativno je otporan na zavaravanje.

Kao što se vidi iz navedenog, svi biometrijski parametri imaju svoje specifične karakteristike, i prednosti i mane, i to je neophodno uzeti u obzir prilikom njihovog izbora i implementacije u funkcionalne sisteme.

3.4 Kriptografija

Reč kriptografija je nastala od grčkih reči kriptos (sakriven) i graphein (pisati) i koristi se da označi metodologiju obezbeđivanja tajnosti podataka u komunikaciji dve ili više strana, kada u tu komunikaciju mogu da ostvare uvid i neovlašćena lica. Pri tome, smatra se da je potrebno obezbediti ispunjenje sledećih uslova [3]:

- Tajnost – da obezbedi da uvid u podatke imaju samo ovlašćena lica.
- Integritet – da obezbedi integritet podatka, odnosno da onemogući neovlašćene izmene podataka, kao što su brisanje, zamena ili izmene na podacima.
- Autentifikacija – da obezbedi uzajamno identifikovanje svih strana i podataka u komunikaciji.
- Neporecivost – da onemogući negaciju preuzete obaveze ili izvršene radnje.

Može se reći da je osnovni zadatak kriptografije obezbeđivanje bezbednih komunikacija preko nesigurnih kanala [4]. Prve kriptografske tehnike su tu bezbednost postizale primenom određenih načina šifrovanja, pri čemu je tajnost podataka direktno zavisila od tajnosti tog načina šifrovanja. Međutim, te metode se nisu pokazale dovoljno bezbednim, tako da se savremene tehnike šifrovanja zasnivaju na primeni ključa. Ključ predstavlja niz podataka na osnovu koga se vrše izmene da podacima koji se štite i time čine nerazumljivim za treća lica. Kod ovih tehnika, kriptografski algoritam sam po sebi nije tajan, ali je za šifrovanje i dešifrovanje potrebno poznavanje ključa. U zavisnosti od toga kakav ključ se koristi kriptografske algoritme delimo na simetrične (sa tajnim ključem) i asimetrične (sa javnim i privatnim ključem).

Simetrični algoritmi koriste isti ključ i za šifrovanje i za dešifrovanje, pri čemu je za efikasnu primenu istih taj ključ potrebno predhodno bezbedno razmeniti na određeni način, što je i njihov najveći nedostatak. Simetrični algoritmi se dalje dele na sekvencijalne, koji šifruju podatke u nizu (A5/1, A5/2, RC4...) i blokovske, koje podatke dele u blokove koje onda šifruju (DES, 3DES, IDEA, RC5, AES...).

Dijagram 1: Simetrični algoritam



Asimetrični algoritmi koriste javni ključ za šifrovanje, a privatni za dešifrovanje i ne zahtevaju bezbednu inicijalnu razmenu ključeva, nego je to moguće obaviti i preko nesigurnih kanala. Svoje funkcionisanje zasnivaju na jednosmernim funkcijama, kod kojih je skoro nemoguće na bazi krajnjeg rezultata doći do početnih vrednosti promenljivih, tako da se na bazi javnog ključa (koji je, kako mu samo ime kaže, javno objavljen i nije tajan) ne može doći do privatnog (tajnog) ključa. Nedostak asimetričnih algoritama je u tome što su sporiji i što nisu toliko pogodni za šifrovanje velikog obima podataka, a i prilikom implementacije mora se rešiti pitanje međusobne autentifikacije. Karakteristični predstavnici su RSA i El Gamal.

Dijagram 2: Asimetrični algoritam



Savremena kriptografska rešenje najčešće kombinuju i simetrične i asimetrične algoritme, na taj način što se asimetrični algoritmi koriste za incijalnu razmenu ključeva za simetrične algoritme, koji se onda dalje koriste za šifrovanje podataka.

Takođe, pored algoritama, bitnu primenu imaju i kriptografske heš (hash) funkcije. Heš funkcije su jednosmerne funkcije koje vrše sažimanje određenog niza podataka, varijabilne veličine, na izlaznu vrednost (hash) fiksne veličine, pri čemu i najmanja promena u orginalnom nizu podataka dovodi do velikih promena u izlaznoj vrednosti. To svojstvo im omogućava da se koriste za osiguranje integriteta, neporecivosti i autentifikaciju. Karakteristični predstavnici su MD5, SHA-0, SHA-1, SHA-3 itd.

3.5 Digitalni potpis

Digitalni potpis predstavlja određenu tajnu vrednost poznatu samo izvoru poruke, koja je uz to zasnovana na sadržaju poruke koja se potpisuje, i koja se može verifikovati od strane trećeg lica bez ostvarivanja uvida u pomenutu tajnu vrednost izvora [3]. Suštinski, to je elektronska zamena za običan potpis, koja za cilj ima da jasno identifikuje izvor (Autentifikacija), da onemogući izmenu sadržaja ili poruke u celosti (Integritet) i da onemogući negaciju poslate poruke ili izvršene radnje (Neporecivost).

Digitalne potpise delimo na dva osnovna tipa [3]:

Digitalni potpisi sa dodatkom (digital signature schemes with appendix), koji su zasnovani na korišćenju kriptografskih heš vrednosti i koji verifikaciju vrše na osnovu sadržaja originalne poruke.

Digitalni potpisi sa povraćajem poruke (digital signature schemes with message recovery), kod kojih se originalna poruka može izvesti iz samog potpisa, i koji se uglavnom koriste za kratke poruke.

3.6 Steganografija, digitalni vodeni žig i vizuelna kriptografija

Reč steganografija je nastala od grčkih reči steganos (zaštićen, pokriven) i graphein (pisati) i koristi se da označi tehnike skrivanja poruke na taj način da niko sem pošiljaoca i primaoca ne zna ni da poruka uopšte postoji. Prednost steganografije u odnosu na kriptografiju se ogleda u činjenici da ne privlači pažnju na komunikaciju samim tim što ne postoji vidljiva primena šifrovanja ili uopšte razmene poruka, tako da se smanjuje i verovatnoća otkrivanja i presretanja tih poruka. Digitalna steganografija podrazumeva sakrivanje informacija u digitalnim formama, tj. dokumentima, slikama, zvučnim i video zapisima i dr. Tehnike koje se koriste su [4]: sakrivanje poruka u najmanje značajnim bitovima, sakrivanje poruka u postojećem šifratu, preslikavanje statističkih osobina, usporavanje ili promena redosleda toka paketa u računarskim mrežama, blog steganografija i sl.

Digitalni vodeni žig (digital watermark) podrazumeva ubacivanje označavajućeg podatka, tzv. vodenog žiga u određenu digitalnu formu (dokument, slika, zvučni ili video zapis...), a sa ciljem dokazivanja autentičnosti ili izvora tih podataka. Delimo ih na vidljive (ubacivanje vidljive forme na digitalni oblik), i nevidljive (ubacivanje nekog niza podataka u digitalni oblik, pri čemu je za detektovanje potrebna primena posebnih algoritama) [5]. Nevidljivi digitalni vodni žigovi se dalje dele na [5]:

- robusne (nelomljive), koji se ne uništavaju ili menjaju sa izmenama na originalnom podatku, i koji se koriste za zaštitu autorskih prava i kontrolu pristupa
- lomljive, kod kojih izmene originalnog podatka uništavaju vodeni žig i pokazuju da je podatak menjan, pa se koriste za autentifikaciju i obezbeđivanje integriteta podataka
- polu-lomljive, kod kojih se tolerišu manje promene na originalnom podatku, ali ih veće izmene takođe uništavaju, i koji se isto koriste za autentifikaciju i obezbeđivanje integriteta podataka

Vizuelna kriptografija je tehnika šifrovanja podataka u okviru slika, pri čemu je dešifrovanje moguće golim okom, ukoliko se primeni pravilna kombinacija dve ili više slika u okviru kojih se nalaze segmenti podataka. Same po sebi, ove slike ne pružaju mogućnost da se dođe do originalnog podatka, već je za to neophodna njihova kombinacija.

4. Biometrijski sistemi

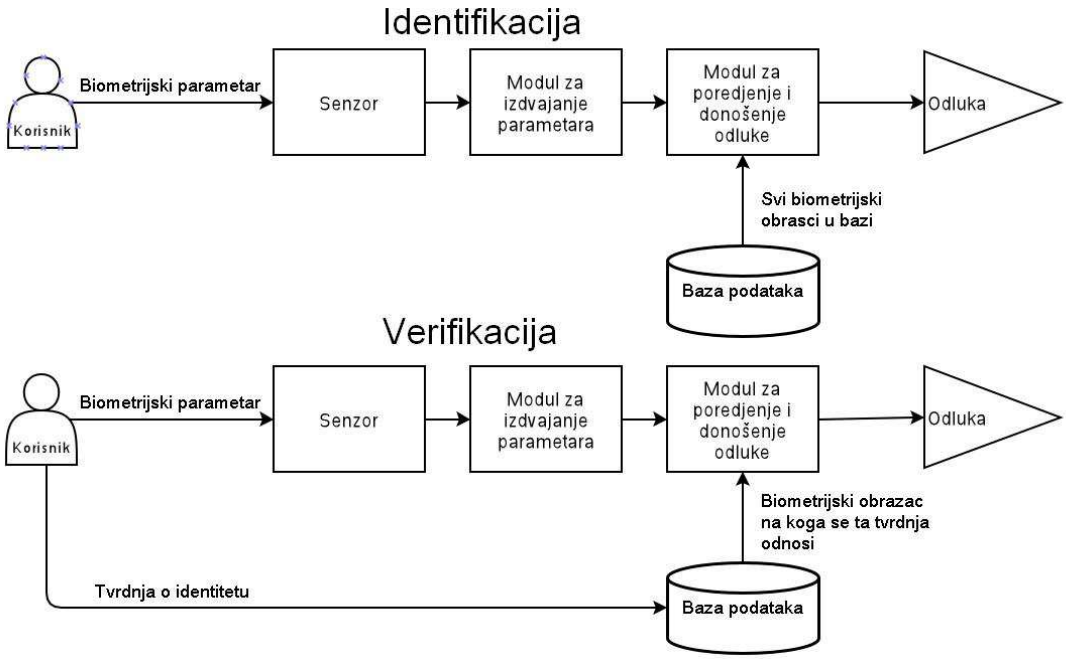
4.1 Biometrijski sistem – pojam i način rada

Biometrijski sistem predstavlja sistem koji funkcioniše tako što prikuplja biometrijske podatke od korisnika, iz tih podataka izdvaja karakteristične detalje, koje onda poredi sa karakterističnim detaljima sadržanim u obrascu uskladištenom u bazi podataka [6]. U zavisnosti od funkcionalnih zahteva, on može da radi na dva načina, za potrebe verifikacije ili za potrebe identifikacije, pri čemu je u oba slučaja prvo potrebno izvršiti prikupljanje podataka [6]:

Prvi način rada je verifikacija, kada sistem utvrđuje nečiji identitet tako što vrši poređenje prikupljenog biometrijskog uzorka te osobe sa njenim uskladištenim obrascem. Korisnik izjavljuje neku tvrdnju o svom identitetu, putem PIN broja, korisničkog imena ili smart kartice, a sistem onda vrši poređenje uzorka i obrasca i utvrđuje da li je ta tvrdnja tačna. Putem verifikacije se realizuje pozitivno prepoznavanje, odnosno onemogućava da više ljudi koristi isti identitet.

Drugi način rada je identifikacija, gde sistem prepoznaje korisnika, tako što pretražuje sve obrasce u bazi podataka, i utvrđuje da li postoji poklapanje, bez potrebe da se korisnik izjasni o svom identitetu. Putem identifikacije se realizuje negativno prepoznavanje, odnosno onemogućeva da jedan korisnik koristi više identiteta, i primena biometrijskih parametara je jedini način da se to realizuje.

Dijagram 3: Identifikacija i verifikacija



Prikupljanje podataka je početna faza, u okviru koje se vrši pribavljanje biometrijskih parametara korisnika i njihovo skladištenje u bazu podataka, kao osnova za kasniju verifikaciju ili identifikaciju.

4.2 Osnovni elementi biometrijskog sistema

Osnovni elementi od kojih se, uopšteno posmatrano, sastoji svaki biometrijski sistem jesu senzorski modul, modul za utvrđivanje kvaliteta i izdvajanje karakterističnih detalja, modul za poređenje i donošenje odluke i modul baze podataka, i oni imaju sledeće funkcije [7]:

Senzorski modul predstavlja element koji vrši prikupljanje biometrijskih parametara koji će se koristiti u biometrijskom sistemu, i ima veliki značaj, jer od kvaliteta njegove realizacije zavisi i kvalitet uzorka biometrijskog parametra, i, samim tim, i performanse sistema uopšte. Tu spadaju čitači otiska prsta, razne vrste kamera, ili određeni, specifični uređaji.

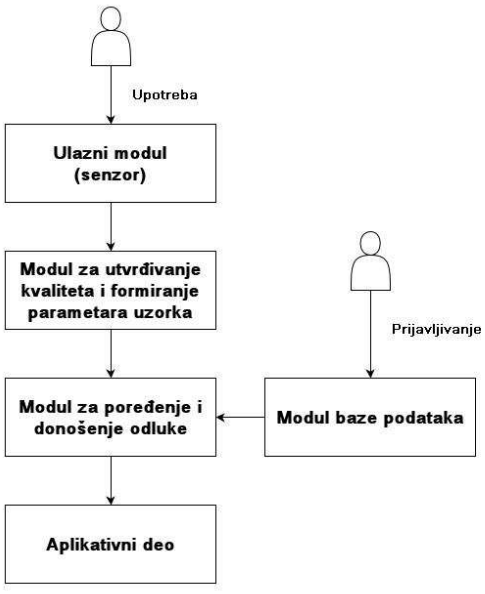
Modul za utvrđivanje kvaliteta i izdvajanje karakterističnih detalja obavlja dvojnu funkciju. Prvo, mora da ustanovi da li je prikupljeni uzorak zadovoljavajućeg kvaliteta, da ga eventualno obradi i onda, na osnovu njega, izdvoji karakteristične detalje i formira biometrijski obrazac, koji se skladišti u bazi podataka i služi za kasnije poređenje.

Modul za poređenje i donošenje odluke vrši poređenje prikupljenog uzorka biometrijskog parametra sa biometrijskim obrascem iz baze, i na bazi predhodno definisanih kriterijuma funkcionisanja, donosi ocenu poklapanja, na osnovu koje funkcioniše deo za donošenje odluke, koji onda potvrđuje identitet ili prezentuje niz potencijalnih mogućnosti.

Modul baze podataka predstavlja deo u okviru koga se vrši skladištenje formiranih biometrijskih obrazaca i odgovarajućih podataka o korisniku, kao što su ime, PIN broj i dr.

U zavisnosti od organizacije sistema, ti podaci mogu biti uskladište u glavnoj bazi biometrijskog sistema, ili mogu biti izdvojeni na poseban uređaj (token), koji korisnik nosi sa sobom.

Dijagram 4: Moduli biometrijskog sistema



4.3 Pokazatelji performansi biometrijskih sistema

Jedan od problema biometrijskih sistema je u tome što dva uzorka biometrijskog parametra, uzeta od iste osobe, usled raznih faktora, kao što su uslovi okruženja, manje promene na biometrijskom parametru ili njegovoj poziciji pri prikupljanju, nikad nisu ista, tako da oni funkcionišu na bazi ocene poklapanja, koja kvantitativno izražava sličnost između prikupljenog uzorka i obrasca u bazi podataka [8]. Ovo i jeste osobina po kojoj se biometrijski sistemi izdvajaju, jer se većina sistema koji se koriste za identifikaciju ili verifikaciju (npr. lozinka ili kartica) zasniva na potpunom poklapanju unete i uskladištene vrednosti, i na osnovu tog poklapanja donose jedinstvenu odluku, kojom se nečiji identitet potvrđuje ili negira.

Ovakav način funkcionisanja biometrijskih sistema nužno dovodi do manjih ili većih razlika, i do pojave greški, koje utiču i na performanse sistema. Osnovni pokazatelji performansi kod biometrijskih sistema, su [9]:

Stopa lažnog poklapanja (False match rate ili FMR), koja pokazuje procenat slučajeva kada biometrijski sistem pogreši i biometrijske parametre od dva različita korisnika prihvati kao da se odnose na jednu osobu, i na osnovu toga, donese pogrešnu odluku o poklapanju.

Stopa lažnog nepoklapanja (False nonmatch rate ili FNMR) koja pokazuje procenat slučajeva kada biometrijski sistem pogreši i biometrijske parametre od istog korisnika tretira kao da se radi o različitim osobama, i na bazi toga, donese pogrešnu odluku o nepoklapanju.

Zatim, imamo greške vezane za interakciju korisnika sa biometrijskim sistemom, koje takođe imaju veliki uticaj, i koje se izražavaju preko sledeći pokazatelja [9]:

Stopa neuspeha pri upisu, (Failure to enroll ili FTE), koji pokazuje procenat slučajeva neuspešnog upisa korisnika u biometrijski sistem, usled neadekvatnih ulaznih podataka, uglavnom zbog nepravilnog korišćenja biometrijskog sistema.

Stopa neuspeha pri sakupljanju, (Failure to acquire ili FTA, a još se označava i kao Failure to capture, ili FTC), koja pokazuje procenat slučajeva kada biometrijski sistem ne uspeva da prikupi uzorak biometrijskih parametara zadovoljavajućeg kvaliteta, koji je neophodan za njegovo funkcionisanje.

Pored ovih pokazatelja, imamo specifične pokazatelje u zavisnosti od namene biometrijskog sistema. Kada se radi o biometrijskim sistemima formiranim u cilju verifikacije, koriste se modifikovani pokazatelji, prilagođeni tom načinu funkcionisanja sistema, i tu spadaju [10]:

Stopa lažnog prihvatanja, (False accept rate, ili FAR), koja pokazuje procenat verifikacionih zahteva, koji bivaju lažno prihvaćeni kao tačni, i na osnovu kojih se, samim tim, odobrava pristup pogrešnom licu. Formira se u zavisnosti od stope lažnog poklapanja i stope neuspeha pri sakupljanju.

Stopa lažnog odbijanja (False reject rate, ili FRR), koja pokazuje procenat verifikacionih zahteva, koji bivaju lažno odbijeni kao netačni, i na osnovu kojih se, samim

tim, onemogućava pristup legitimnom korisniku. Formira se u zavisnosti od stope lažnog nepoklapanja i stope neuspeha pri sakupljanju.

Kada je u pitanju identifikacija, takođe imamo specifične pokazatelje, u koje spadaju [10]:

Stopa lažne pozitivne identifikacije (False positive identification error rate, ili FPIR), koja pokazuje procenat identifikacionih zahteva, kada sistem donosi i prosleđuje lažnu odluku o identitetu, a korisnik nije upisan u sistem. Formira se u zavisnosti od stope lažnog poklapanja i stope neuspeha pri sakupljanju.

Stopa lažne negativne identifikacije (False negative identification error rate, ili FNIR), koja pokazuje procenat identifikacionih zahteva, kada sistem ne donosi i ne prosleđuje tačnu odluku o identitetu, a korisnik je upisan u sistem. Formira se u zavisnosti od stope lažnog nepoklapanja i stope neuspeha pri sakupljanju.

Stopa tačne identifikacije, (Correct identification rate, ili CIR) koja pokazuje procenat identifikacionih zahteva od strane korisnika upisanih u sistem, u kojima sistem donosi i prosleđuje tačnu odluku o identitetu.

Pored navedenih, a u cilju lakšeg donošenja odluka, koriste se i grafički prikazi, kako bi se lakše predstavili odnosi između navedenih pokazatelja, i olakšalo donošenje odluka bitnih za dizajn i funkcionisanje sistema.Tu spadaju [10]:

ROC (Receiver operating characteristic) kriva, koja omogućeva poređenje različitih sistema pod istim uslovima, ili jednog sistema pod različitim uslovima. Na ovaj način se predstavljaju i porede opšti pokazatelji, kao i specifični pokazatelji kod identifikacije i verifikacije, tako što se pokazuje odnos između tačnih i netačnih odluka (1-FNMR prema FMR, 1-FRR prema FAR i sl.).

DET (Detection error trade off) kriva, se takođe koristi za predstavljanje i poređenje opštih i specifičnih pokazatelja, i koja predstavlja modifikovanu ROC krivu, jer se pokazatelji direktno predstavljaju i porede (FMR prema FNMR, FAR prema FRR i sl.).

CMC (Cumulative match characteristic) kriva, kojom se predstavljuju performanse identifikacionog sistema, prikazivanjem određenih rangova i odgovarajućih verovatnoća identifikacije.

4.4 Primena biometrijskih sistema

Biometrijski sistemi mogu biti iskorišćeni za realizaciju različitih funkcionalnih zahteva, tako da, posmatrano sa aspekta njihove uloge, imamo sledeće primene [11]:

Fizička kontrola pristupa, kada se oni koriste za kontrolu pristupa u specifične objekte ili prostore (nuklearne elektrane, sefovi banaka ...).

Logička kontrola pristupa, kada se oni koriste za kontrolu pristupa kompjuterima, serverima, bazama podataka ili čak i individualnim programima.

Autentifikacija transakcija, kada se koriste kao element autentifikacije bilo kod lokalnih ili kod udaljenih transakcija.

Kontrola pristupa uređajima, kad se koriste za kontrolu pristupa kod laptop kompjutera, PDA uređaja, mobilnih telefona i dr.

Kontrola prisutnosti i radnog vremena, kada se koriste za evidentiranje prisustva zaposlenih na radnom mestu, kao i broja radnih sati.

Za identifikacione potrebe stanovništva, kada se koristi za sprečavanje zloupotreba, odnosno onemogućavanje korišćenja više identiteta ili pojave dupliranih stavki.

Za identifikacione potrebe sa aspekta forenzike, u smislu identifikacije počinioca ili žrtve, za potrebe istražnih radnji...

Takođe, primene biometrijskih sistema možemo podeliti i sa aspekta velikih oblasti funkcionisanja na komercijalne (e-trgovina, zaštita podataka, kontrola pristupa i dr.), državne (lične karte, vozačke dozvole, pasoši, kontrola granica i dr.) i forenzičke (identifikacija tela, nestalih lica, za potrebe krivičnih istraga i dr.) [7].

4.5 Klasifikacija biometrijskih sistema

U zavisnosti od radnog okruženja, namene i korisnika, biometrijske sisteme možemo podeliti prema sledećim kriterijuma [12]:

Na očite i prikrivene, prema tome da li je korisnik svestan da se prikuplja njegov biometrijski parametar ili ne. Kod kontrole pristupa i drugih verifikacionih sistema, korisnici su svesni prisustva i korišćenja biometrijskih parametara, dok sistemi koji se primenjuju za potrebe bezbednosti i forenzičke potrebe mogu da budu prikriveni.

Na sisteme za naviknute i nenaviknute korisnike, u zavisnosti od korisnika sistema. Prvi tip sistema podrazumeva korišćenje od strane korisnika koji su se već prilagodili korišćenju tog sistema, posle izvesnog vremenskog perioda, dok drugi tip podrazumeva korišćenje od strane korisnika koji nemaju iskustvo u radu sa sistemom.

Pod nadzorom i bez nadzora, u zavisnosti od toga da li će neko biti zadužen da rukovodi korišćenjem biometrijskog sistema, ili će on funkcionisati samostalno, u skladu sa predhodno definisanim programom.

Na sisteme za standardna i nestandardna okruženja, u zavisnosti od radnog okruženja. Pod standardnim se podrazumevaju sistemi namenjeni za upotrebu u zatvorenom prostoru, dok su nestandardni prilagođeni radu u težim uslovima i posebnim namenama.

Javni ili privatni, u zavisnosti od toga da li su predviđeni za korišćenje od strane javnih korisnika (klijenata) ili privatnih korisnika (npr. zaposleni u određenom preduzeću).

Otvoreni ili zatvoreni, u zavisnosti od potreba povezivanja sa drugim biometrijskim sistemima. Otvoreni se prilagođavaju određenim standardima prikupljanja podataka koji su

zajednički i omogućuju razmenu informacija, dok zatvoreni mogu da funkcionišu na osnovu svojih individualnih parametara.

4.6 Biometrijski sistemi i privatnost

Jedan od bitnih elementa koji utiče na potencijalne primene, rasprostranjenost i uopšte prihvatanje biometrije jeste njen uticaj na privatnost. Budući da svoje funkcionisanje zasniva na fiziološkim karakteristikama i obrascima ponašanja, koji su neodvojivi deo ljudskog bića, njen uticaj na privatnost je predmet brojnih razmatranja.

Generalno gledano, privatnost se može definisati kao pravo ili intres pojedinica, usmereno na kontrolu načina na koji će se podaci o njemu prikupljati, ustupati i koristiti, i kojim se obuhvataju sledeće kategorije [13]:

- Informaciona privatnost, koja se odnosi na prikupljanje i upotrebu bitnih ličnih podataka a kojom se obuhvataju sledeći pojmovi: prikupljanje podataka koji nisu neophodni, neovlašćeno prikupljanje podataka, neovlašćeno otkrivanje podataka i proširivanje funkcije, odnosno primena u druge svrhe od deklarisanih. Imajući u vidu da biometrijski sistemi funkcionišu na osnovu fizioloških karakteristika i obrazaca ponašanja, i da često pored toga integrišu i bitne lične podatke, te karakteristike imaju veliki uticaj na ovu privatnost.

- Telesna privatnost, koja se odnosi na zaštitu od invazivnih procedura. Budući da biometrijski sistemi funkcionišu na osnovu prikupljanja uzoraka biometrijskih parametara, i budući da su neki od tih načina dosta invazivni (npr. prikupljanje slike mrežnjače) ili zahtevaju neposredni kontakt, postoji veliki uticaj i na ovaj vid privatnosti.

- Teritorijalna privatnost, koja se odnosi na sagledavanje aktivnosti na određenim lokacijama, a koja je ugrožena kombinovanjem sistema nadzora i identifikacije na osnovu biometrijskih parametara.

- Komunikaciona privatnost, koja se odnosi na lične komunikacije, a koja takođe može biti ugrožena u određenim situacijama, npr. primenom sistema za prepoznavanje glasa.

Imajući u vidu navedeno, može se reći da, sa aspekta privatnosti, postoji niz specifičnosti biometrijskih podataka koji mogu da imaju negativan uticaj [14]:

- mogu da budu prikupljeni i ustupljeni bez pristanka, ili neke posebne svrhe
- podaci prikupljeni za potrebe jednog sistema, mogu da budu iskorišćeni u nekom drugom ili u više sistema, bez odobrenja i znanja korisnika
- podaci mogu da budu iskorišćeni i u neku drugu svrhu, ili se mogu obrađivati kako bi se došlo do dodatnih informacija o korisniku
- mogu da se neovlašćeno prikupe i zloupotrebe
- mogu da se koriste iako nema potrebe ili dovoljnog opravdanja za tim

- mogu da otkriju bitne lične podatke, kao što su pol, etnička pripadnost, određene medicinske informacije
- mogu da budu iskorišćeni za pronalaženje i praćenje ljudi, da se povežu sa ličnim identifikacionim podacima, a u cilju nadzora, profilisanja i kontrole
- njihova upotreba u kriminalističke svrhe, može da stvori negativnu percepciju i da smanji njihovu prihvatljivost.
- mogu da se prenose ili skladište na neadekvatan način, usled čega mogu da budu predmet spoljašnjih napada ili unutrašnjih zloupotreba.

U zavisnosti od odnosa prema privatnosti, odnosno načina na koji koriste biometrijske podatke, biometrijske sisteme delimo na [15]:

Invazivne, koji prikupljaju biometrijske podatke bez znanja i odobrenja lica, a zatim ih koriste za neobjavljene svrhe ili im proširuju opseg upotrebe (sistemi za nadzor i sl.).

Neutralne, čije korišćenje biometrijskih podataka nema veliki uticaj na privatnost (pristup ličnom računaru i sl.).

Blagonaklone, koji štite biometrijske podatke od neovlašćenog pristupa i korišćenja (npr. aplikativni programi).

Zaštitni, koji koriste biometrijske podatke da bi zaštitili važne lične podatke od neovlašćenog pristupa i zloupotrebe (poslovne transakcije, zaštita računa i sl.).

U cilju formiranja sistema koji se klasifikuju kao blagonakloni ili zaštitni prema privatnosti, predlaže se niz mera, čijom implementacijom u funkcionalne biometrijske sisteme se može postići visok nivo zaštite privatnosti. Te mere se odnose na sledeće segmente, iznete u radu [15]:

Opseg i mogućnosti sistema, gde se predlaže:

- ograničavanje opsega sistema, kako bi se sprečilo proširavanje funkcije, i primena u druge svrhe
- ograničavanje zadržavanja biometrijskih podataka, odnosno čuvanje samo inicijalno prikupljenih podataka, uz odbacivanje naknadnih uzoraka koji se koriste u funkcionisanju sistema
- ograničavanje skladištenja originalnih biometrijskih podataka, odnosno odbacivanje originalnih slika, snimaka i drugih uzoraka, koji sadrže bitne lične podatke, neposredno po generisanju biometrijskih obrazaca
- ograničavanje prikupljanja i skladištenja dodatnih informacija, odnosno korišćenje minimalne količine nebiometrijskih podataka, samo do nivoa neophodnog za funkcionisanje sistema
- formiranje procedure za ukidanje sistema, kojom se u slučaju potrebe, na bezbedan način prekida njegovo funkcionisanje i odbacuju podaci, bez ugrožavanja privatnosti korisnika sistema

Zaštitu podataka, gde se predlaže:

- korišćenje bezbednosnih alata u cilju zaštite biometrijskih podataka u svim segmentima sistema. U te svrhe, mogu se primeniti kriptografske metode, mere fizičke i logičke kontrole pristupa i dr.
- zaštita konačnih odluka sistema, odnosno primena adekvatnih zaštitnih mera kako bi se izbeglo menjanje finalnih odluka od strane neovlašćenih lica, i potencijalno ugrožavanje bezbednosti i funkcionisanja sistema
- ograničavanje pristupa sistemu, odnosno obezbeđivanje da samo mali broj pouzdanih lica ima pristup biometrijskim podacima, kako bi se sprečila zloupotreba

Kontrolu korisnika nad ličnim podacima, gde se predlaže:

- korišćenje sistema na dobrovoljnoj bazi i postojanje mogućnosti da se istupi iz sistema, odnosno omogućavanje prava izbora korisnicima
- obezbediti da korisnici mogu da ostvare uvid u svoje podatke i da eventualno izvrše korekcije istih, ukoliko ustanove da postoje neka neslaganja ili neki problem sa unetim podacima

Objavljivanje, revizija i odgovornost, gde se predlaže:

- objavljivanje namene i ciljeva sistema, odnosno objašnjavanje kako će sistem funkcionisati, da li će biti obavezan ili ne i kakva će prava i mogućnosti imati korisnici
- definisati odgovornost za zloupotrebe sistema, odnosno odrediti zaduženja i odgovornosti, i obezbediti način rešavanja problema i nesporazuma do kojih može doći
- objaviti upotrebu sistema, kada se on nalazi u funkciji, kako bi korisnici bili svesni da pristupaju biometrijskom sistemu
- formirati procedure za reviziju i nadzor od strane referentne institucije, kako bi se postigao i održao visok nivo bezbednosti i profesionalan pristup ka funkcionisanju sistema

4.7 Prednosti i mane biometrijskih sistema

Biometrijski sistemi, zbog svoje prirode, imaju određene, specifične prednosti u odnosnu na alternativna rešenja, ali takođe, i svoje mane. Pre svega, zasnivaju se na nekoj fiziološkoj karakteristici ili obrascu ponašanja neke osobe, pa ne postoji mogućnost da budu zaboravljeni ili izgubljeni, da budu ustupljeni nekom ili da se negira korišćenje sistema. Istovremeno, to je i velika mana, zato što u slučaju da budu neovlašćeno prikupljeni i zloupotrebljeni, ne mogu biti promenjeni, kao što je slučaj sa nekim drugim vidovima autentifikacije, i to predstavlja trajan i ozbiljan problem.

Pored toga, iako biometrijski sistemi predstavljaju faktor bezbednosti, i njihova bezbednost je često ugrožena. Neki sistemi su osetljivi na neovlašćeno prikupljanje, i moguće ih je prevariti prezentovanjem lažne biometrije, negde je moguće izvršiti uticaj na

sistem primenom nekih tehnika napada, tako da to predstavlja veliki izazov pri dizajniranju i implementaciji ovih sistema.

Generalno gledano, njihovo korišćenje postavlja manje zahteve pred korisnike, tako da u nekim slučajevima i podižu bezbednost i pojednostavljuju ceo proces, funkcionišući kao zamena za neki komplikovaniji sistem, koji nije pokazao zadovoljavajuće performanse ili bio pozitivno prihvaćen od strane korisnika. Pored toga, primena biometrijskih sistema predstavlja način da se obezbedi negativno prepoznavanje, i da se time spreče potencijalne zloupotrebe ili ugrožavanja bezbednosti. Međutim, kao negativna strana, pojavljuje se i faktor njihovog prihvatanja, jer kod nekih korisnika izazivaju nelagodnost i odbojnost prema korišćenju takvog sistema, a postavlja se i pitanje njihovog negativnog uticaja na privatnost.

5. Individualni biometrijski sistemi

5.1 Otisak prsta

Otisak prsta predstavlja najviše korišćen biometrijski parametar u savremenim biometrijskim sistemima, koji , zbog svojih karakteristika, ima primenu u realizaciji većeg broja funkcionalnih zahteva, kao što su identifikacija, kontrola pristupa, generisanje ključeva i dr. Rasprostranjenost ovog parametra se javlja kao rezultat istorijskog razvoja, budući da se počeci njegovog korišćenja javljaju još u starim civilizacijama, Vavilonu, Egiptu i Kini, da bi u 19. veku počela njegova primena u kriminalistici, koja je predstavljala osnovu za dalji razvoj.

Velika prednost otiska, i karakteristika koje je dovela do njegove trenutne pozicije, je njegova jedinstvenost.Proces formiranja otisaka se dešava tokom razvoja fetusa, uz uticaj većeg broja faktora usled čega postoje određene razlike i kod identičnih blizanaca.Takođe, tokom života se ne menjaju, izuzev u slučaju povreda i oštećenja, tako da imaju dugoročni potencijal za primenu sa aspekta biometrijskih sistema.



Slike 1: Jagodica prsta[1]



Slika 2: Otisak papilarnih linija[2]

Otisak prsta se sastoji od niza ispučenja, koje se nazivaju papilarne linije, i udubljenja, na površini jagodice prsta, čiji oblik i specifičnosti imaju visoku jedinstvenost i samim tim, i visoku pogodnost za primenu u biometrijskih sistemima. Postoje tri osnovna tipa karakteristika koje se koriste [11]:

U prvu grupu karakteristika spadaju globalne karakteristike, kao što je obrazac kretanja papilarnih linija, zajedno sa karakterističnim oblastima, poput lukova, petlji i vrtloga, a takođe i oblik prsta, orijentacija i gustina tih linija. Ove karakteristike se mogu koristiti za klasifikaciju, ali nisu dovoljno precizne za potrebe poređenja.

U drugu grupu karakteristika spadaju lokalne karakteristike, odnosno karakteristični detalji papilarnih linija, koji se još nazivaju i minucije (završeci, račvanja papilarnih linija i

[1] Izvor slike: http://en.wikipedia.org/wiki/Fingerprint (pristup 06.04.2014)
[2] Ibid.

dr.). Njihov raspored i orijentacija su karakteristike sa visokom jedinstvenošću, i mogu se koristiti za potrebe poređenja.

U treću grupu spadaju izuzetno sitni detalji u okviru papilarnih linija, kao što su njihova širina, oblik, ivice, znojne pore i dr. koji su jedinstveni, ali njihovo prikupljanje zahteva izuzetno preciznu opremu, tako da nisu u raširenoj upotrebi.

Svaka od ovih grupa karakteristika ima svoju namenu, i njihovo korišćenje obezbeđuje određene funkcionalne zahteve. Globalne karakteristike omogućavaju brzo pretraživanje i formiranje preliminarnih rezultata, i na taj način poboljšavaju performanse sistema i smanjuju zahteve, ali na osnovu njih se ne može doneti pouzdan zaključak. Lokalne karakteristike obezbeđuju dovoljnu količinu jedinstvenih podataka za potrebe precizne identifikacije ili verifikacije, ali su zbog svoje strukture, i kompleksnije za obradu. Ukoliko se teži izuzetnoj preciznosti, onda se mogu inkorporirati i izuzetno sitni detalji, npr. znojne pore, ali to zahteva specifičnu opremu i veći utrošak resursa sistema.

Biometrijski sistemi zasnovani na otisku prsta mogu da funkcionišu na osnovu predhodno prikupljenih podataka ili u realnom vremenu [11]. Kod prvog načina, otisak prsta, otisnut mastilom na papiru npr. se digitalizuje i unosi u sistem. Takođe, u ovu kategoriju spadaju i takozvani latentni otisci, koji ostaju na površinama koje se dodirnu, i oni imaju izuzetno bitnu ulogu u forenzici i kriminalistici. Kod sistema koji funkcionišu u realnom vremenu, potrebna je implementacija odgovarajućih senzora za prikupljanje tog otiska prsta.

Kod prikupljanja podataka o karakeristikama otiska prsta, bitno je imati u vidu da od kvaliteta senzora zavisi i količina prikupljenih informacija, koje se dalje mogu procesirati i koristiti. Senzori mogu biti [11]:

Optički, kojih ima više vrsta, mogu da funkcionišu na bazi refleksije svetla sa otiska, koje snima CMOS ili CCD kamera, ili da inkorporiraju optička vlakna ili direktno snimanju, uz pomoć kamere visoke rezolucije. Takođe, mogu se koristiti i elektrooptički senzori ili multispektralni, koji snimaju na različitim talasnim dužinama svetla.

Kapacitativni, koji se sastoje od niza kondenzatora koji mere provodljivost, i u zavisnosti od razlika između pojednih delova generišu sliku otiska.

Termalni, koji funkcionišu na sličan način, s tim što sliku otiska prsta generišu na osnovu malih razlika u temperaturi.

Senzori električnog polja, koji mere električno polje ispod kože prsta, i na bazi toga formiraju uzorak otiska.

Piezoelektrični senzori, koji funkcionišu tako što pri pritisku generišu struju niskog intenziteta i na bazi razlika u jačini pritiska, a samim tim i struje, formiraju sliku otiska prsta.

Ultrazvučni koriste zvučne talase, tj. njihov eho za izračunavanje distanci, i na taj način formiraju sliku otiska prsta.

Prikupljeni uzorci otiska prsta se zatim obrađuju, kako bi se istakli i izdvojili karakteristični detalji koji se onda koriste za poređenje. Tri najčešće korišćene tehnike su [11]:

Na osnovu uzajamne povezanosti, gde se odluka donosi na osnovu celog otiska prsta, odnosno direktnog poklapanja između dva obrasca, uz uračunavanje određenog nivoa difuznosti.

Na osnovu karakterističnih detalja (minucija), gde se odluka donosi na osnovu poklapanja tih karakterističnih detalja na uzorku i obrascu, pri čemu se traži što veći broj detalja koji se poklapaju.

Na osnovu ostalih, globalnih karakteristika papilarnih linija, kao što su njihovi oblici, orijentacija, gustina i dr., koje nisu toliko unikatne ali su lakše za prikupljanje.



Slika 3: Senzor za uzimanje otiska prsta[3]

5.2 Lice

Lice predstavlja jednu od glavnih karakteristika po kojoj se ljudi međusobno prepoznaju, tako da je ova automatska funkcija ljudske svesti idejni pokretač istih biometrijskih sistema. Međutim, taj način funkcionisanja ljudske svesti je izuzetno teško reprodukovati sa aspekta funkcionalnih sistema, tako da je problematika prepoznavanja lica izuzetno kompleksno područje sa velikim opsegom istraživanja i razvoja.

Lice sadrži veliki broj karakteristika koje se mogu iskoristiti za potrebe biometrijskih sistema, i njih možemo podeliti u tri grupe [9]:

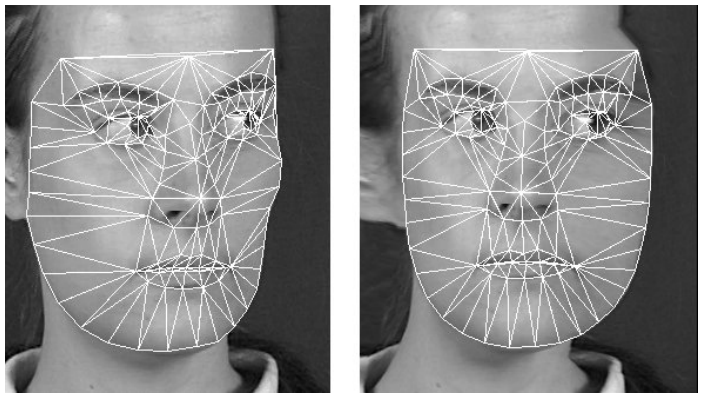
U prvu grupu spadaju globalne karakteristike, kao što su oblik lica, boja kože i dr. koje su lako uočljive i koje se mogu uočiti i na ulaznim podacima niskog kvaliteta.

U drugu grupu spadaju lokalne karakteristike, kao što su struktura glavnih segmenata lica, njihovi međusobni odnosi kao i precizniji oblik lica, koji obezbeđuju solidnu osnovu za poređenje, ali i zahtevaju viši kvalitet ulaznog materijala.

[3] Izvor slike: http://en.wikipedia.org/wiki/Fingerprint (pristup 06.04.2014)

U treću grupu spadaju sitni detalji, kao što su pege, mladeži, suptilne promene na koži, ožiljci i dr. i koji zahtevaju uzorke sa visokim nivoom detalja, ali zato obezbeđuju visok nivo preciznosti.

U zavisnosti od opšte namene sistema, kao i definisanih funkcionalnih zahteva, zavisiće i izbor karakteristika na osnovu kojih će se bazirati funkcionisanje sistema. Globalne karakteristike zahtevaju najmanje resursa ali nude i najmanju preciznost, i pogodne su za sužavanje polja pretrage ili za pružanje nekog zaključka, u slučaju da se raspolaže samo sa ulaznim podacima niskog kvaliteta. Lokalne karakteristike omogućavaju adekvatnu preciznost, uz odgovarajuće performanse, a korišćenje sitnih detalja je moguće, u slučaju da postoji potreba za izuzetnom preciznošću, što naravno umanjuje performanse i povećava zahteve sistema.



Slika 4: Karakteristične tačke lica[4]

Osnovni elementi funkcionisanja ovih sistema jesu [9]:

Prikupljanje uzoraka, koje se vrši uz pomoć senzora koje mogu da obezbede dvodimenzionalne slike (mogu biti na vidljivim talasnim dužinama, infracrvenim ili mogu da se koriste termalne slike), trodimenzionalne modele lica (na osnovu lasera, ili primenom stereografije) ili video snimak (koji obezbeđuje niz slika i informacije o dinamici pokreta lica).

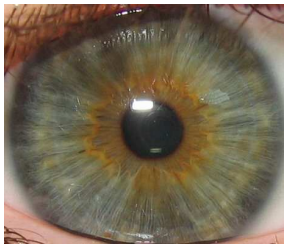
Detekcija lica, koje podrazumeva primenu adekvatnih algoritama za izdvajanje regiona lica sa slike.

Izdvajanje karakterističnih detalja i poređenje, koje podrzumeva obradu prikupljenog materijala posle faze detekcije, koje se vrši tehnikama na bazi izgleda, modela ili tekstura. Tehnike na bazi izgleda podrazumevaju predstavljanje slike lica kao funkcije niza različitih lica u osnovnom skupu, pri čemu se poređenje vrši na osnovu odgovarajućih ponderisanih vrednosti. Tehnike na bazi modela se zasnivaju na kreiranju dvodimenzionalnog ili trodimenzionalnog modela, koji može da se koristi nezavisno od držanja lica, i koji pri tom uzima u obzir određene lokalne karakteristike lica i time postiže veću kompleksnost u odnosu na predhodne tehnike. Tehnike na bazi tekstura podrazumevaju izbor adekvatnih tekstura lica na koje ne utiče držanje ili osvetljenje.

[4] Izvor slike: http://cvssp.org/faceweb/facialBiometric/ (pristup 06.04.2014)

5.3 Iris

Iris predstavlja obojeni deo ljudskog oka, koji se nalazi između beonjače i zenice. Ima izuzetno kompleksnu strukturu i smatra se da je jedinstven za svakog čoveka i da se razlikuje i kod identičnih blizanaca. Zbog svoje prirode, više je zaštićen od spoljašnjih uticaja, i ne menja se značajno usled starenja, izuzev eventualno u slučaju povreda oka, tako da je izuzetno pogodan za upotrebu u biometrijskim sistemima.



Slika 5: Iris[5]

Sistemi zasnovani na irisu, generalno obuhvataju četiri segmenta, i to su [16]:

Prikupljanje slike irisa, gde se uz pomoć odgovarajućih kamera dolazi do slika irisa. Te kamere uglavnom funkcionišu u bliskom infracrvenom spektru, zato što on ne izaziva fiziološke reakcije oka, mada je moguće i korišćenje običnih kamera.

Predhodna obrada slike, gde se nad slikom vrše segmentacija i normalizacija. Segmentacija podrazumeva tačno određivanje regiona irisa u okviru slike oka, uz nastojanje da se jasno razgraniče svi detalji na slici. Potom, vrši se normalizacija, koja ima za cilj da prstenasti oblik oblasti irisa transformiše u pravolinijski format pogodan za dalju obradu.

Izdvajanje karakterističnih detalja, koje podrazumeva primenu odgovarajućih tehnika kako bi se došlo do vektora karakteristka, koji mogu da budu u formi realnih vrednosti ili binarni, koji formiraju obrasac koji je lakši za poređenje.

Poređenje, gde se vrši poređenje tih vektora karakteristika, odnosno biometrijskih obrazaca, za potrebe verifikacije ili identifikacije, utvrđivanjem da li se međusobna odstupanja nalaze unutar odgovarajućih granica.

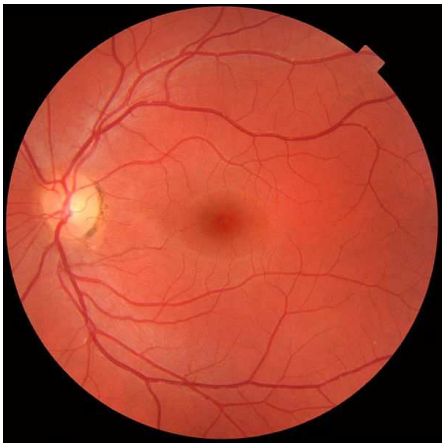


Slika 6: Uređaj sa skeniranje irisa[6]

[5] Izvor slike: http://en.wikipedia.org/wiki/Iris_recognition (pristup 06.04.2014)
[6] Ibid.

5.4 Mrežnjača

Mrežnjača predstavlja unutrašnji deo ljudskog oka, osetljiv na svetlost, u okviru kojeg se formira slika spoljašnjeg sveta i prosleđuje mozgu. Za biometrijske potrebe je bitno to što se u okviru mrežnjače nalazi mreža krvnih sudova koje je unikatna za svaku osobu, pa čak i za svako oko. Zbog toga gde se nalazi, dosta je zaštićena od spoljnih uticaja, a po svojoj prirodi je izuzetno stabilan i trajan biometrijski parametar. Povreda ili bolest mogu da utiču na pogodnost za biometrijske potrebe, ali takve situacije nisu zastupljene u tolikom obimu da bi to imalo veći uticaj.



Slika 7: Mrežnjača[7]

Biometrijski sistemi na osnovu mrežnjače su jedni od prvih koji su se pojavili u funkcionalnoj upotrebi, i podrazumevali su korišćenje odgovarajućih kamera u kombinaciji sa izvorom osvetljenja. U početku, korišćeno je intenzivno svetlo, kako bi se osvetlilo očno dno i istakla mreža krvnih sudova, ali to je bilo izuzetno neprijatno za korisnika a i izazivalo je reakciju skupljanja zenica, što je opet otežavalo funkcionisanje sistema, tako da se prešlo na upotrebu infracrvenog svetla, koje jasno ističe mrežu krvnih sudova, a kod savremenih sistema se koriste i laseri niskog intenziteta.

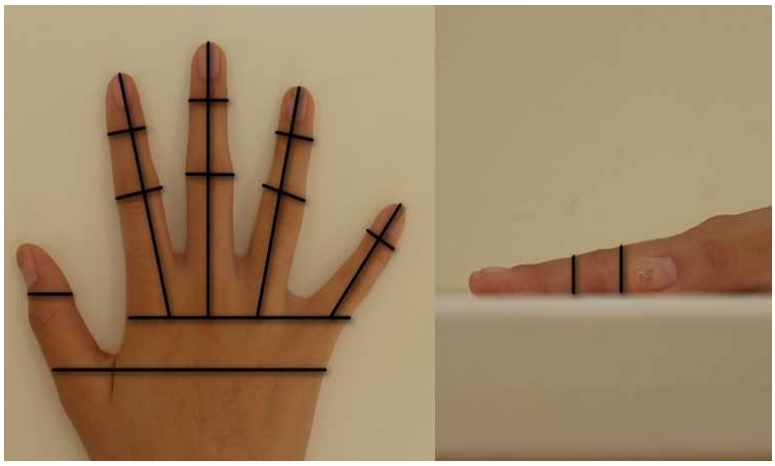
Osnovni elementi ovog sistema su deo za slikanje, zatim deo za prikupljanje podataka i njihovu obradu, koji od snimka kamere prave digitalni oblik, deo za poređenje, koji poredi obrazac sa prikupljenim uzorkom, i prezentacioni deo, koji obuhvata obrasce mrežnjača i identifikacijske podatke korisnika [17]. Po uzimanju uzorka, vrši se obrada istog kako bi se otklonio uticaj različitih pozicija koje korisnik može da zauzme, određuju bitne karakteristike i na kraju vrši poređenje, na osnovu ocene poklapanja.

Generalno gledano, za poređenje može da se koristi cela mreža krvnih sudova, odnosno obrazac formiran na taj način, ili može da se vrši izdvajanje karakterističnih detalja (račvanja, završetaka, pozicija delova krvnih sudova po završenim transformacijama i sl.) i da se oni koriste u procesu poređenja i donošenja odluke [18].

[7] Izvor slike: http://en.wikipedia.org/wiki/Retina (pristup 06.04.2014)

5.5 Geometrija šake

Geometrija šake je biometrijski parametar sa relativno niskom jedinstvenošću, i shodno tome, nije pogodan za identifikaciju, ali zbog svojih ostalih karakteristika, ima primenu u biometrijskim sistemima. Funkcionisanje sistema se zasniva na geometrijskim karakteristikama ljudske šake, odnosno dlana i prstiju, a kao karakteristike na osnovu kojih se vrši poređenje koriste se dužina, širina i debljina prstiju, dimenzije dlana, njihova relativna pozicija i dr.



Slika 8: Geometrija šake[8]

Prikupljanje uzorka se obično vrši na osnovu kamera ili digitalnog skenera, dok novija rešenja koriste i 3D skenere.

Kod ranijih sistema, prikupljanje uzorka se vršilo na osnovu odgovarajućih, prilagođenih uređaja. Jedno od predloženih rešenja je primena posebnog uređaja u okviru koga se nalazi kamera, koji na predviđenoj površini ima niz čivija kojima se fiksira položaj šake, a koji takođe sadrži i bočno ogledalo, koje omogućava da se na dobijenoj slici nalazi i bočni profil šake, i izvor svetla [19].

Dalji razvoj ovih sistema obuhvata rešenja koje ne zahtevaju fiksiran položaj šake uz pomoć čivija, već koriste obične slike šake na određenoj površini, zatim, potpuno beskontaktne metode, kod kojih je dovoljno postaviti šaku ispred kamere, kao i razvoj 3D sistema [20].

Dobijena slika, odnosno više njih, se zatim koristi za izračunavanje tih karakterističnih mera, na osnovu kojih se kreira biometrijski obrazac, u formi vektora, a poređenje između uskladištenog obrasca i novog, prikupljenog uzroka se vrši na osnovu mera razdaljine, npr. Euklidovska, Hemingova i dr. [21].

[8] Izvor slike: http://en.wikipedia.org/wiki/Hand_geometry (pristup 06.04.2014)



Slika 9: Čitač geometrije šake[9]

5.6 Otisak dlana

Dlan predstavlja unutrašnji deo ljudske šake koji se, isto kao i otisak prsta, sastoji od niza ispupčenja i udubljenja na koži, koje formiraju više karakterističnih struktura, i koji ima kompleksan obrazac i visoku jedinstvenost, tako da predstavlja pogodnu osnovu za korišćenje sa aspekta biometrijskih sistema.



Slika 10: Otisak dlana[10]

Za razliku od otiska prsta, otisak dlana sadrži mnogo više karakterističnih detalja koji se mogu iskoristiti [22]:

- geometrijske karakteristike, pod kojima se podrazumevaju oblik i dimenzije dlana
- karakteristike glavnih linija dlana, odnosno njihove lokacije i oblici, koje su bitne zato što se jako malo menjaju sa protokom vremena

[9] Izvor slike: http://en.wikipedia.org/wiki/Access_control (pristup 06.04.2014)
[10] Izvor slike: http://biometrics.cse.msu.edu/projects/latent_palmprint.html (pristup 06.04.2014)

- karakteristike nabora na koži, koji su tanji, ali brojniji i sa nepravilnom strukturom
- krajnje tačke, koje se nalaze na ivicama dlana, a određuju se na osnovu glavnih linija dlana, i koje jasno razgraničavaju oblast otiska i mogu se koristiti za procenu dimenzija
- račve, koje predstavlju karakteristične obrasce kože koji se formiraju pri korenu prsta
- minucije, odnosno karakteristični detalji papilarnih linija

Kao i kod otiska prsta, i ovi sistemi mogu da funkcionišu u realnom vremenu ili na bazi predhodno prikupljenih otisaka. Funkcionisanje u realnom vremenu zahteva korišćenje adekvatnih senzora, dok se predhodno prikupljeni otisci prebacuju u digitalni oblik preko skenera [22].

Savremene tehnologije su, pored standarnog prepoznavanja slike u niskoj rezoluciji, dovele i do formiranje novih oblasti, kao što su multispektralni sistemi, koji koriste različite talasne dužine (vidljiva svetlost, bliska infracrvena i infracrvena, pa čak i samo pojedine talasne dužine) za dobijanje kvalitetnih slika dlana, korišćenje 3D otiska dlana, a izuzetno bitan segment je i prepoznavanje latentnih otisaka, koji su značajni za kriminalistiku [23].

Po prikupljanju slike, nekim od navedenih metoda, vrši se predhodna obrada, kako bi se ustanovilo poravnjanje i definisala koordinatna mreža, posle čega se izdvajaju karakteristični detalji i vrši poređenje, pri čemu imamo tri osnovna pristupa [23]:

Holistički, koji tretiraju otisak dlana kao sliku ili višedimenzionalni vektor, i za poređenje koriste klasifikacione tehnike.

Pristup zasnovan na karakterističnim detaljima, gde se vrši izdvajanje karakterističnih detalja sa slike otiska dlana (glavne linije, nabori, minucije, 3D ili multispektralni elementi i dr.), i poređenje sa uskladištenim obrascima.

Kombinovani, koji koristi oba navedena pristupa i kombinuje njihove tehnike u cilju podizanja preciznosti ili brzine prepoznavanja.

5.7 Raspored krvnih sudova ruke ili prsta

Podkožni raspored krvnih sudova ruke ili prsta je biometrijski parametar koji ima visoku jedinstvenost, i smatra se da je različit i kod identičnih blizanaca, a odlikuje ga i trajnost, jer nije podložan promenama usled protoka vremena, izuzev u slučaju povrede. Pored toga, zahteva posebnu opremu da bi se uopšte video, pa je samim tim skriveniji i manje pogodan za neovlašćeno prikupljanje. Za potrebe biometrijskih sistema, uglavnom se koristi raspored krvnih sudova na poleđini šake, u okviru dlana, ili u okviru prsta.



Slika 11: Raspored krvnih sudova u ruci[11]

Ovi sistemi svoje funkcionisanje zasnivaju na karakteristikama apsorpcije svetlosti od strane hemoglobina prisutnog u venama, usled čega pri korišćenju bliskog infracrvenog svetla, te oblasti imaju tamniju boju, tako da se za prikupljanje uzorka koriste izvor tog svetla i odgovarajuća kamera, pri čemu sistem može da funkcioniše na dva principa [24]:

Na osnovu refleksije, kada se oblast osvetljava frontalno, a izvor svetla i kamera se nalaze jedno pored drugog, što je prednost jer obezbeđuje manju veličinu sistema.

Na osnovu transmisije, kada se oblast osvetljava sa druge strane, ili bočno, tako da su izvor svetla i kamera odvojeni.

U oba slučaja, sistem ne zahteva nikakav kontakt, nego samo prezentovanje predviđene oblasti ispred senzora.

Dobijene slike se zatim obrađuju, izdvaja se raspored krvnih sudova, i on se koristi kao osnov za formiranje obrasca za poređenje. Poređenje se vrši na osnovu ocene poklapanja, a kao elementi za formiranje te ocene mogu da se koriste pozicije karakterističnih detalja, kao što su račve ili završeci krvnih sudova, ili može da se vrši utvrđivanje poklapanja obrazaca, poređenjem vrednosti piksela na uskladištenoj slici i prikupljenom uzorku [25].

5.8 DNK

Dezoksiribonukleinska kiselina ili DNK je nukleinska kiselina koja sadrži niz genetskih instrukcija kojima se određuje razvoj i funkcionisanje svih živih organizama. Zbog svoje kompleksne strukture, može se iskoristiti za pouzdano prepoznavanje, izuzev kod identičnih blizanaca, tako da predstavlja perspektivan biometrijski parametar.

Kod ovog parametra, na bazi prikupljenih uzoraka, primenom specijalizovanih tehnika i uređaja, formira se DNK profil, koji je jedinstven identifikator i koji predstavlja obrazac za dalje poređenje.

[11] Izvor slike: http://fingerchip.pagesperso-orange.fr/biometrics/types/vein.htm (pristup 06.04.2014)

Međutim, još uvek nema razvijenu primenu u biometrijskim sistemima, zbog sledećih nedostataka [9]:

- značajna osetljivost i mogućnost kontaminacije, relativno je lako neprimećeno prikupiti uzorak i zloupotrebiti ga.
- trenutno ne postoji automatizovan način za prikupljanje, jer zahteva specijalizovane uređaje i visoko obučeno osoblje
- značajno ugrožava privatnost, jer otkriva potencijalne lične informacije.

5.9 Uvo

Oblik ljudskog uva je karakteristika koja ima kompleksnu strukturu, ne menja se sa starenjem, lako se prikuplja i nije toliko podložna povredama. Smatra se da ima visoku jedinstvenost, iako je to još uvek predmet razmatranja, i predmet je intezivnog istraživanja i razvoja a u cilju primene u biometrijskim sistemima. Sistemi zasnovani na ovom biometrijskom parametru obuhvataju sledeće faze [26]:

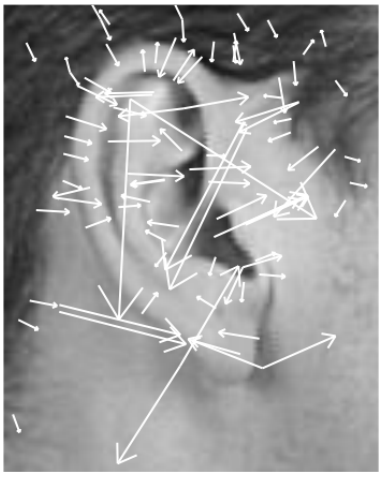
Detekcija i segmentacija oblasti uva sa prikupljenog uzorka.

Obrada i normalizacija, kako bi se formirao pogodan materijal za izdvajanje detalja.

Izdvajanje karakterističnih detalja, u okviru koje se vrši formiranje profila, odnosno vektora karakteristika kojim se izražavaju ti detalji.

Poređenje, gde se na osnovu obrasca i uzorka donosi ocena poklapanja.

Odlučivanje, u okviru koje se , u zavisnosti od ocene poklapanja, donosi pozitivna ili negativna odluka, ili se rangiraju mogući identiteti.



Slika 12: Karakteristični detalji uva[12]

Kao izvori podataka mogu da se koriste dvodimenzionalne slike ili trodimenzionalni modeli. Prvo se vrši detekcija i segmentacija uva, pri čemu postoji veliki

[12] Izvor slike: http://www.cspc.ecs.soton.ac.uk/ear (pristup 06.04.2014)

broj tehnika (poklapanje obrazaca, na bazi oblika, na bazi kontura uva i dr.), da bi se zatim prešlo na dalju obradu, izdvajanje karakteristika i poređenje, u zavisnosti od tehnike koja se koristi kod prepoznavanja (na osnovu intenziteta, vejvlet transformacije, Gaborovi filteri i dr.) [26].

5.10 Glas

Glas predstavlja biometrijski parametar koji se klasifikuje kao obrazac ponašanja, ali treba imati u vidu da na njegovo formiranje utiču ljudski obrasci ponašanja, ali i fiziološke karakteristike ljudskog glasovnog sistema. Biometrijski sistemi zasnovani na glasu, koriste specifične karakteristike glasa, kao što su visina tonova, ritam, boja glasa i sl.

Glas kao biometrijski parametar može da se koristi za realizaciju niza zahteva, i u zavisnosti od svrhe, ove zahteve delimo na [27]:

Verifikacija na bazi glasa, kada se glas koristi za potvrđivanje identiteta osobe, koja iznosi neku tvrdnju o svom identitetu (putem korisničkog imena, kartice i sl.).

Identifikacija na bazi glasa, kada se na bazi glasa utvrđuje identitet osobe, poređenjem sa svim raspoloživim uzorcima, koja može da se vrši nad određenim i neodređenim skupom. Kod određenog skupa, ako nema potpunog poklapanja, kao rezultat se bira obrazac sa najvećom sličnošću, bez obzira na stepen različitosti od uzorka. Kod neodređenog skupa, utvrđuje se sličnost između obrazaca i uzorka, a onda se vrši verifikacija potencijalnih mogućnosti, i rezultat se formira samo ako postoji dovoljno poklapanje.

Klasifikacija na bazi glasa, kada se vrši grupisanje sličnih zvukova, npr. klasifikacija po polovima, starosti i sl.

Segmentacija na bazi glasa, koja podrazumeva izdvajanje glasovnih segmenata u nekom zvučnom signalu, odnosno njihovo razdvajanje od šumova, muzike, i drugih zvukova.

Detekcija na bazi glasa, koja podrazumeva otkrivanje jednog ili više govornika u nekom zvučnom signalu.

Praćenje na bazi glasa, koje podrazumeva praćenje jednog ili više govornika u nekom zvučnom signalu, tokom njegovog trajanja.

Biometrijski sistemi, kojima se realizuje neki funkcionalni zahtev, mogu da funkcionišu u sledećim načinima rada [27]:

U zavisnosti od teksta, kada je neophodno izgovaranje određene fraze za potrebe, pre svega, verifikacije.

Nezavisno od teksta, kada sistem ne uzima u obzir ni neki tekst, niti karakteristike jezika, već funkcioniše samo na osnovu karakteristika glasa, i kojim mogu da se realizuju svi navedeni zahtevi.

Na bazi traženog teksta, kada sistem traži da se izgovori specifičan tekst u određenom trenutku, kojim se otklanja slabost sistema koji funkcionišu na osnovu određenog teksta, tako što se onemogućava neovlašćeno prikupljanje i prezentovanje određenog teksta.

Na osnovu znanja, kada se integrišu karakteristike sistema koji funkcionišu nezavisno od teksta, sistema koji traže određeni tekst, sa modulom za prepoznavanje govora i razumevanje karakteristika jezika, kako bi formirao kompleksan sistem.



Slika 13: Poređenje uzoraka ljudskog glasa[13]

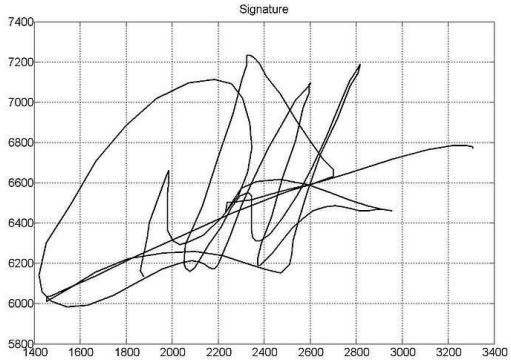
Glas se predstavlja putem određenog talasnog oblika (waveform), koji pokazuje odnos između jačine zvuka i vremenske dimenzije i preko spektrograma, koji pokazuje odnos između frekvencije zvuka i vremenske dimenzije, pri čemu se on, za potrebe prepoznavanja, konvertuje u digitalni oblik.

Prikupljanje uzorka kod ovog sistema je izuzetno jednostavno, i može se vršiti i običnim mikrofonom, pri čemu se prikupljeni podaci obrađuju i porede primenom različitih tehnika (vektorska kvantizacija, HMM i DTW modeli i dr.) [1].

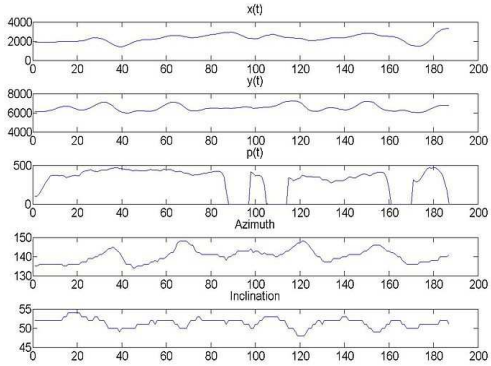
5.11 Potpis

Potpis, kao jedan od obrazaca ponašanja, sadrži niz karakterističnih detalja koji se mogu iskoristiti za potrebe verifkacije. Kod ovog parametra razlikujemo poređenje na osnovu predhodno prikupljenih podataka, odnosno na osnovu slike potpisa, i poređenje u realnom vremenu, kada se pored detalja potpisa, uz pomoć posebnih uređaja prikupljaju i dinamički parametri, kao što su kretanje, jačina pritiska i dr.

[13] Izvor slike: http://www.nist.gov/itl/iad/biometrics-011413.cfm/ (pristup 06.04.2014)



Slika 14: Dinamički uzorak potpisa[14]



Slika 15: Dinamičke informacije potpisa[15]

Prikupljanje uzoraka, kod sistema za verifikaciju potpisa u realnom vremenu, vrši se na osnovu uređaja koji imaju ekran osetljiv na dodir, ili odgovarajućih olovki, posle čega se vrši izdvajanje detalja, gde imamo dva pristupa [28], na bazi karakteristika, gde se formira vektor kojim se predstavlja skup globalnih karakteristika dobijenih iz obrasca potpisa, i na bazi funkcija, gde se koriste vremenske dimenzije lokalnih karakteristika potpisa. Pri prikupljanju, može se vršiti formiranje niza obrazaca sa karakterističnim detaljima ili statističkog modela ponašanja određenog korisnika, posle čega se poređenje vrši na osnovu mera rastojanja, statističkih modela i dr. [28].

5.12 Dinamika otkucaja na tastaturi

Dinamika otkucaja na tastaturi predstavlja ljudski obrazac ponašanja za koga se pretpostavlja da je specifičan za određenu osobu, i da se može iskoristiti za potrebe verifikacije ili, u manjoj meri, identifikacije. Kao osnov za formiranje obrazaca i poređenje, mogu se koristiti sledeće karakteristike [29]:

- vreme između pritisaka na tastere,
- dužina trajanja pritiska na taster
- brzina kucanja
- frekvencija greški
- korišćenje dodatnih tastera
- redosled pritisaka na tastere kod promene veličine slova
- snaga pritiska, ako se koristi posebna tastatura koja može da meri taj parametar

[14] Izvor slika: http://en.wikipedia.org/wiki/Signature_recognition (pristup 10.04.2014)
[15] Ibid.



Slika 16: Dinamika otkucaja na tastaturi[16]

Ovaj biometrijski sistem može da se koristi za potrebe [29]:

Verifikacije, kod koje se obično analizira način i dinamika otkucaja korisničkog imena i lozinke kada se pristupa sistemu, gde se u fazi prikupljanja formira profil, koji se zatim koristi za poređenje, pri čemu se za klasifikaciju koriste statistički metodi, neuronske mreže, Bajesovi klasifikatori i dr.

Identifikacije, kada se utvrđuje identitet korisnika na osnovu profila kucanja, formiranog obradom velike količine predhodno prikupljenih informacija o načinu i dinamici kucanja svakog individualnog korisnika, među većim brojem korisnika.Korisna karakteristika ovog sistema je što može da obezbeđuje kontinuirani nadzor, odnosno da konstantno prati karakteristike kucanja i reaguje u slučaju da dođe do promena.

5.13 Hod

Ljudski hod predstavlja kompleksan obrazac ponašanja koji ima veliki broj elemenata koji se mogu iskoristiti za potrebe prepoznavanja. Iako je njegova jedinstvenost još uvek predmet razmatranja, smatra se da je dovoljno specifičan za određene namene, posebno zato što omogućava prepoznavanje i na rastojanju, kada drugi biometrijski parametri ne mogu doći do izražaja. Prikupljanje uzoraka kod ovog sistema se vrši na osnovu video snimaka, ili putem specijalnih senzora.

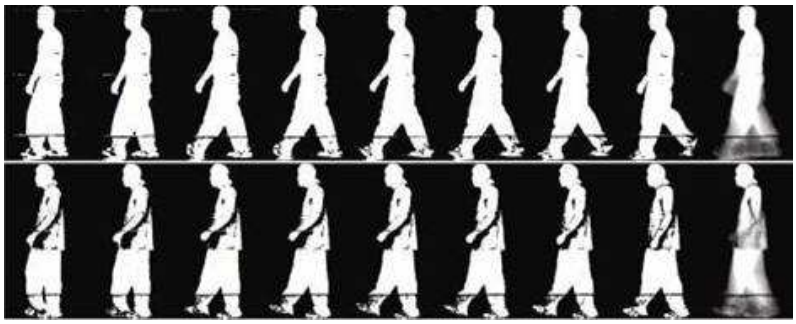
Kao izvor karakterističnih detalja koriste se oblik koji telo zauzima u različitim fazama hoda i dinamički parametri koji se javljaju u tim fazama kretanja, pri čemu imamo sledeće pristupe [30]:

Na osnovu vremenske usklađenosti, kada se uzimaju u obzir i oblik i dinamički parametri, posmatrani kroz određenu vremensku sekvencu.

Na osnovu silueta, gde se koriste sličnosti između silueta, a zanemaruju se dinamički parametri.

Na osnovu statičkih karakteristika, gde se koriste određeni pokazatelji (dužina koraka, ritam, telesne karakteristike i dr.) kako bi se izrazila dinamika hoda.

[16] Izvor slike: http://www.deakin.edu.au/research/cisr/research-areas/pma-lab.php (pristup 06.04.2014)



Slika 17: Analiza načina hoda[17]

5.14 Biometrijski parametri koji imaju potencijalnu primenu

Miris, koji predstavlja kombinaciju niza jedinjenja koja se može osetiti uz pomoć ljudskog čula mirisa, je predmet razmatranja, u cilju korišćenja u biometrijskim sistemima. Sa tog aspekta, iako se smatra da je ljudski miris specifičan i da postoji potencijal za korišćenje za potrebe prepoznavanja, njegova primena za te svrhe zahteva još istraživanja i razvoja. Prikupljanje i poređenje mirisa uopšte vrši se uz pomoć specifičnih uređaja (electronic nose, ENose) koji koriste odgovarajuće senzore za prikupljanje (spektrometar, hemijski senzori i dr.) i adekvatne algoritme za poređenje (statistički i dr.), [31] tako da postoji tehnološka osnova takvog procesa.

Rukopis, koji predstavlja dalji razvoj sistema za prepoznavanje potpisa, gde se koriste karakeristični detalji rukopisa za potrebe prepoznavanja. Karakteristike i predložene modele funkcionisanja imamo u radovima [32] i [33].

Pokreti usana, gde se za potrebe biometrijskih sistema predlaže korišćenje karakterističnih detalja pokreta usana tokom govora. Karakteristike ovog parametra, i primenljivost sa biometrijskog aspekta. su predmet istraživanja i razvoja, i razmatranja njegovog korišćenja imamo u radovima [34] i [35].

Elektrokardiogram (EKG), koji predstavlja prikaz električne aktivnosti srca u određenom vremenskom periodu, je još jedna karakteristika za koju se smatra da ima jedinstvene karakteristike i da se stoga može koristiti za potrebe prepoznavanja. Takođe je predmet velikog broja istraživanja, i predložena rešenja imamo u radovima [36] i [37].

Elektroencefalogram (EEG), koji predstavlja prikaz električne aktivnosti mozga u određenom vremenskom periodu.Takođe se smatra da je dovoljno specifičan za potrebe prepoznavanja, i da nudi velike prednosti, i stoga je predmet razmatranja, a predložene koncepte imamo u radovima [38] i [39].

Nokat, gde se razmatra primena karakterističnih detalja koji se formiraju pri rastu nokta, i za koje smatra da imaju visoku jedinstvenost. Mogućnosti i karakteristike ovog parametra se razmatraju u radovima [40] i [41].

Stisak šake, koji se razmatra kao faktor bezbednosti kod vatrenog oružja, podrazumeva šemu pritiska šake kao osnov za prepoznavanje, i koji je predložen je u radu [42].

[17] Izvor slike: http://www.cris.ucr.edu/Biometric_Examples.php (pristup 06.04.2014)

Dinamika pokreta miša, koja, slično kao i dinamika otkucaja na tastaturi, podrazumeva korišćenje parametara koji proizilaze iz načina korišćenja kompjuterskog miša za potrebe prepoznavanja. Razmatranje korišćenje ovog biometrijskog parametra imamo u radovima [43] i [44].

5.15 Meke biometrijske karakteristike

Meke biometrijske karakteristike obezbeđuju određenu količinu informacija o osobi, ali nemaju dovoljnu različitost i trajnost da bi se na osnovu njih vršilo razlikovanje, tako da služe da bi se poboljšalje peformanse nekog osnovnog biometrijskog sistema, i u njih spadaju [45]:

- visina
- težina
- godište
- pol
- etnička pripadnost
- boja očiju i dr.

Integracijom ovih karakteristika, iako one nemaju dovoljnu specifičnost same po sebi, u već postojeći biometrijski sistem, obezeđuje se dodatni niz informacija, koji može u određenoj meri da podigne nivo funkcionisanja osnovnog sistema, i da se iskoristi kao dodatni faktor bezbednosti.

6. Multibiometrijski sistemi

6.1 Pojam i razlozi nastanka

Multibiometrijski sistemi predstavljaju kompleksnije sisteme koji se formiraju integracijom više različitih elemenata i izvora biometrijskih informacija, a u cilju povećanja pouzdanosti i preciznosti rada, i otklanjanja specifičnih nedostataka individualnih sistema.

Osnovne mane individualnih biometrijskih sistema, usled kojih se i razvijaju multibiometrijska rešenja, jesu [46]:

Difuznost prikupljenih podataka, nastala usled oštećenja na biometrijskom parametru ili senzoru, ili zbog uslova okruženja, usled čega može da dođe do neuspešnog prepoznavanja legitimnog korisnika.

Varijacije unutar klase, koje se javljaju kod istog korisnika, usled nepravilnog korišćenja sistema, suptilnih promena na biometrijskom parametru usled vremena, ili zbog uticaja stresa, npr. kod obrazaca ponašanja.

Sličnosti između klasa, kada usled poklapanja određenih karakteristika, dolazi do pojave sličnosti između različitih korisnika, sa čim raste i stopa lažnog poklapanja.

Nedostatak univerzalnosti, kada se javljaju teškoće u prikupljanju biometrijskog parametra, usled njegovih karakteristika, u određenom broju slučajeva.

Interoperabilnost, odnosno njen nedostatak, usled nemogućnosti ili otežanog poređenja biometrijskih parametara prikupljenjih različitim tipovima senzora.

Napadi zavaravanjem, kada se promenama na biometrijskom parametru, ili pak falsifikovanjem i prezentovanjem istog, utiče na prepoznavanje.

Ostali napadi, kojima se utiče na funkcionisanje sistema na različitim nivoima, i koji takođe mogu da negativno utiču na rad sistema.

6.2 Komponente multibiometrijskih sistema

Kako bi se otklonili navedeni nedostaci i povisio nivo funkcionisanja sistema, multibiometrijski sistemi koriste više izvora biometrijskih podataka i elemenata sistema, i oni mogu da integrišu [46]:

Veći broj senzora, kada se istovremeno koriste različiti senzori za prikupljanje biometrijskog parametra, a u cilju povećavanja fonda podataka za obradu (npr. korišćenje 2D kamere i 3D senzora kod prepoznavanja lica).

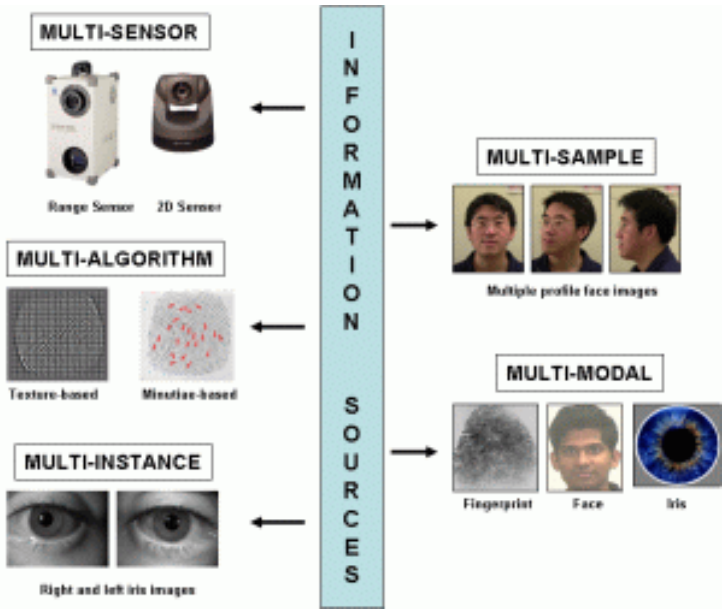
Veći broj algoritama, kada se nad prikupljenim podacima primenjuje više algoritama (npr. istovremeno korišćenje algoritama koji funkcionišu na osnovu karakterističnih detalja i algoritama koji funkcionišu na bazi celog otiska prsta).

Veći broj slučajeva, kada se koristi više slučajeva biometrijskog parametra (npr. oba irisa, obe mrežnjače, više otisaka prstiju).

Veći broj uzoraka, kada se prikuplja veći broj uzoraka jednog biometrijskog parametra, zbog varijacija i kompletnosti.

Veći broj biometrijskih parametra, kada se koristi više različitih biometrijskih parametara za potrebe identifikacije ili verifikacije (npr. kombinovanje lica i otiska prsta, ili lica i otiska prsta i rasporeda vena prsta i sl.). Ovi sistemi se još nazivaju i multimodalni biometrijski sistemi.

Veći broj predhodno navedenih mogućnosti, kada se kombinuju neke od predhodno navedenih opcija, (npr. integrisanje više uzoraka i više algoritama u okviru jednog sistema i dr.). Ovi sistemi se još nazivaju i hibridnim.



Slika 18: Multibiometrijski sistemi[18]

6.3 Bitni segmenti rada

Kod implementacije navedenog, prilikom dizajniranja sistema, potrebno je voditi računa da se elementi međusobno ukomponuju na odgovarajući način, kako bi se obezbedila lakoća korišćenja, efikasno funkcionisanje i zadovoljavajuće performanse sistema. U tom cilju, neophodno je definisati sledeće redoslede [46]:

Redosled prikupljanja, kojim se određuje redosled na osnovu koga će se vršiti prikupljanje informacija iz ranije pomenutih izvora. Prikupljanje može da se odvija

[18] Izvor slike: http://www.cse.msu.edu/~rossarun/research.shtml (pristup 06.04.2014)

sekvencijalno, kada se iz svakog izvora pojedinačno pribavlja podatak, sa određenim vremenskim razmacima između njih, ili odjednom, kada se pribave podaci iz svih izvora istovremeno, u cilju ubrzavanja celog procesa.

Redosled obrade, kojim se određuje redosled na osnovu koga će se vršiti obrada prikupljenih informacija. Obrada može da se vrši serijski, kada se prikupljeni podaci obrađuju svaki u svom segmentu, jedan za drugim, sve dok se ne dobije dovoljno informacija za donošenje odluke. što je pogodno jer omogućuje brži rad sistema. Drugi način je paralelna obrada, gde se informacije istovremeno obrađuju u svim segmentima, a onda spajaju na bazi predefinisane šeme, čime se omogućava veća preciznost usled većeg fonda podataka. Pored navedenog, moguće je vršiti i hijerarhijsku obradu, koja podrazumeva kombinovanje predhodnih metoda, tako što se u određenim segmentima obrada vrši serijski, a u određenim paralelno, kako bi se što bolje iskoristila izabrana kombinacija biometrijskih izvora.

Procesirane informacije, koje služe za donošenje odluke, moraju se spojiti u jednu celinu. U zavisnosti od sekvence tog spajanja, a na osnovu koje se definiše i količina podataka koja cirkuliše jer se ona značajno smanjuje posle poređenja, sistemi se dele na [9]:

Sisteme kod kojih se spajanje vrši pre faze poređenja, u šta spadaju [9]:

Spajanje na nivou senzora podrazumeva da se podaci spajaju posle prikupljanja, pre faze izdvajanja karakterističnih detalja, sa ciljem da se obezbedi veći fond podataka za obradu, i takvo spajanje je moguće primeniti samo kod multibiometrijskih sistema sa više senzora ili više uzoraka.

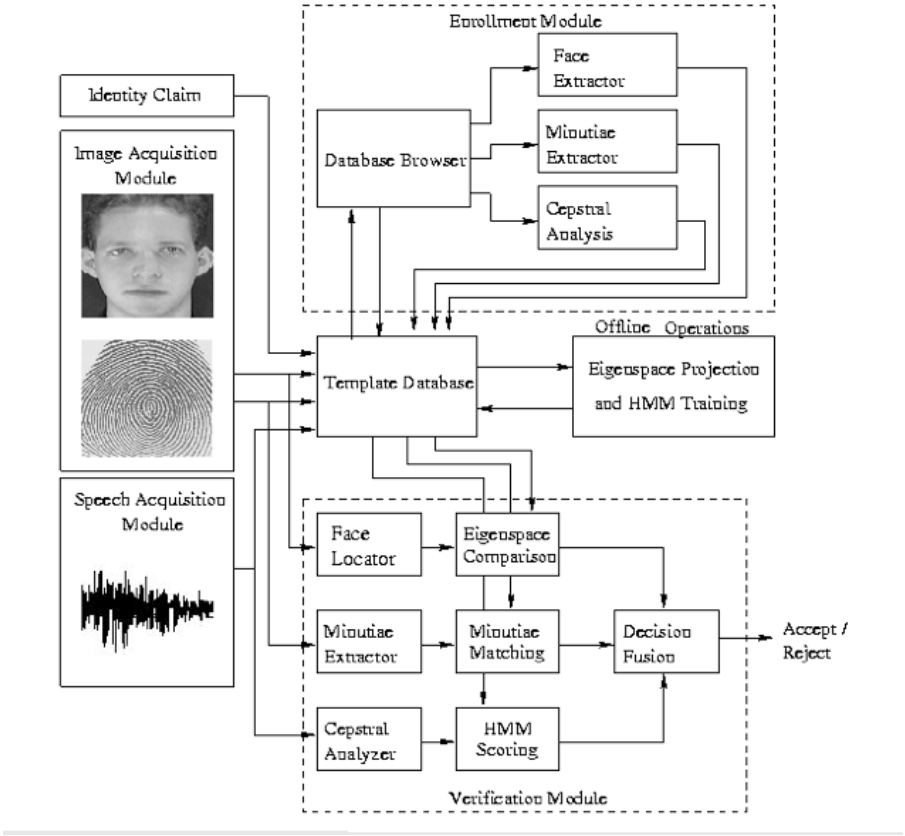
Spajanje na nivou izdvajanja karakterističnih detalja, podrazumeva spajanje bitnih karakteristika iz više prikupljenih podataka istog korisnika, i ono može biti homogeno i heterogeno. Homogeno podrazumeva da se spajaju biometrijski podaci dobijeni na osnovu višestrukih uzoraka istog biometrijskog parametra, obrađenih istim algoritmom, a u cilju ažuriranja ili unapređivanja biometrijskog obrasca u bazi. Heterogeno podrazumeva spajanje karakteristika dobijenih različitim algoritmima na osnovu različitih biometrijskih parametra.

Sisteme kod kojih se spajanje vrši posle faze poređenja, u šta spadaju [9]:

Spajanje na nivou ocene podrazumeva spajanje ocena dobijenih iz više poređenja kako bi se formirala konačna odluka, i, u zavisnosti od načina klasifikacije, dele se na one koji su zasnovani na odnosu verovatnoća, na transformacijama i na ostalim pristupima. Pristup na osnovu odnosa verovatnoća podrazumeva primenu teorija odluke i statističkog testiranja hipoteza, pristup na osnovu tranformacija podrazumeva primenu minimalne stope greške, a pored ovoga moguće je primena i drugih tehnika (linearno diskriminantna analiza, neuralne mreže...). Takođe, treba imati u vidu da se razlikuju tehnike spajanja na nivou ocene i u zavisnosti od toga da li se sistem koristi za identifikaciju ili za verifikaciju.

Spajanje na nivou ranga, podrazumeva da se vrši rangiranje identiteta na osnovu procene koliko su ispunjeni kriterijumi, i formiranje opadajućeg niza mogućih rešenja, a potom, spajanje tih rang listi, kako bi se onda dobila zbirna rang lista mogućih identiteta. To može da se vrši na osnovu najvišeg ranga, zbira individulanih rangova, ili pak ponderisanog zbira rangova.

Spajanje na nivou odluke, podrazumeva da se posle individualnih poređenja u okviru segmenata prosleđuju samo odluke, koje se onda spajaju i na bazi toga formira finalna odluka sistema.To može da se vrši primenom i/ili pravila, na osnovu većine ili ponderisane većine glasova i dr.



Slika 19: Primer multibiometrijskog sistema zasnovanog na licu, otisku prsta i glasu[19]

Kombinovanjem više biometrijskih parametara u jedinstven sistem ostvaruje se niz prednosti nad individualnim biometrijskim sistemima. Primenom više izvora biometrijskih informacija i elemenata sistema, moguće je obezbediti višestruko veći fond podataka, kako za izdvajanje karaketrističnih detalja, tako i za poređenje i donošenje odluka, i samim tim, značajno podići tačnost sistema. Zatim, postojanje više različitih izvora biometrijskih informacija i elemenata sistema podiže kompleksnost funkcionisanja sistema na viši nivo, i samim tim, i otpornost sistema na falsifikovanje ili neki drugi vid napada, jer je sinhronizovano zavaravanje više različitih elementa izuzetno teško za realizaciju. Takođe, navedene karakteristike pozitivno utiču na reagovanje na greške, zbog veće tolerancije usled obima podataka, a i povećava se univerzalnost korišćenja.

[19] Izvor slike: http://biometrics.pbworks.com/w/page/14811351/Authentication%2520technologies (pristup 06.04.2014)

7. Bezbednosni problemi i specifičnosti biometrijskih sistema

7.1 Specifične karakteristike i zahtevi kod biometrijskih sistema

Biometrijski parametri imaju mnogo prednosti, obezbeđuju jednostavan način za realizaciju autentifikacije, budući da ne zahtevaju nošenje ili pamćenje nečega, onemogućavaju da se autentifikacioni podaci prenesu ili podele sa neovlašćenom osobom, obezbeđuju neporecivost, tako da korisnik ne može da negira pristup nekom sistemu ili podacima, i negativno prepoznavanje, tako da lice ne može da prikriva identitet. Međutim, imaju i nedostatke, od kojih je najbitniji nepromenljivost biometrijskog parametra. U slučaju narušavanja bezbednosti i krađe tih podataka, nemoguće ih je jednostavno zameniti, kao lozinku ili token, tako da to može trajno da ugrozi bezbednost i privatnost korisnika. Zatim, u okviru biometrijskih podataka se potencijalno nalaze i lične informacije o licu od koga potiču, a i u nekim slučajevima mogu se prikriveno prikupiti, bez znanja tog lica, što takođe može da ugrozi bezbednost i privatnost.

Biometrijski sistemi, uzimajući u obzir sve prednosti i nedostatke, treba da obezbede uspešnu realizaciju servisa identifikacije ili verifikacije, uz zaštitu biometrijskih podataka, i uz zadovoljavajuće performanse.

Osnovni zahtevi vezani za privatnost, koje biometrijski sistemi treba da ispune, prema autorima [47], su:

- Zaštita identiteta – sistem treba da obezbedi lične podatke korisnika povezane sa biometrijskim podacima , i da onemogući zloupotrebu.
- Nepovratnost – sistem treba da obezbedi da se na osnovu podataka koji se čuvaju (obrazaca) ne mogu rekonstruisati originalni biometrijski parametri, čak i u slučaju kada je dostupno više različitih uzoraka istog biometrijskog parametra, iz različitih sistema.
- Nepovezivost – sistem treba da onemogući da se na bazi biometrijskih podataka ustanove veze između različitih sistema u kojima se nalaze lični biometrijski podaci korisnika.

Osnovni zahtevi vezani za bezbednost, koje biometrijski sistemi treba da ispune, prema autorima [47], su:

- Poverljivost – sistem treba da spreči neovlašćeni pristup biometrijskim podacima, i u komunikacionim tokovima i pri čuvanju u bazama podataka, primenom kriptografskih i drugih tehnika.
- Integritet – sistem treba da obezbedi tačnost i potpunost podataka koji se u njemu nalaze, npr. primenom digitalnih potpisa i sl.
- Otkazivost i obnovljivost – sistem treba da omogući laku zamenu obrazaca za poređenje u slučaju da ti podaci budu kompromitovani.

7.2 Bezbednosni problemi

Jedan od osnovnih razloga funkcionisanja i implementacije biometrijskih sistema je upravo obezbeđivanje realizacije određenih bezbednosnih ciljeva. Međutim, biometrijski sistemi nisu sami po sebi sigurni, već je i njihovo funkcionisanje ugroženo određenim bezbednosnim problemima, koji mogu da dovedu do narušavanja njihovog rada i do ugrožavanja bezbednosti sistema i podataka povezanih sa njima.

Prvi problem sa kojim se biometrijski sistemi susreću, a koji može da naruši bezbednost, proizilazi iz njihovog načina funkcionisanja i već pomenute, inherentne stope greške. Zbog varijacija koje se javljaju kod biometrijskih podataka, može da dođe do odobravanja pristupa neovlašćenom licu, do uskraćivanja pristupa ovlašćenom licu, ili do pogrešne identifikacije.

Zatim, imamo opšte bezbednosne probleme, sa kojima se susreću svi sistemi, i u koje spadaju [48]:

Onemogućavanje korišćenja, (Denial of service - DOS), kada se blokira sistem, i onemogućuje pristup legitimnim korisnicima. Ovakav oblik napada podrazumeva slanje velike količne nepravilnih zahteva ili podataka, kojima se preopterećuju resursi nekog sistema i onemogućava pristup, ili pak onemogućivanje funkcionisanja nekog ulaznog uređaja.

Zaobilaženje, kada se koriste propusti u softveru, hardveru ili organizaciji sistema kako bi se čitav bezbednosni segment zaobišao, i ostvario neovlašćeni pristup podacima, ili zloupotrebio sistem za realizaciju nekog specifičnog cilja.

Poricanje, kada ovlašćeni korisnik negira korišćenje sistema, ili izvršavanje određenih aktivnosti u okviru sistema.

Neovlašćeno prikupljanje i lažno prezentovanje, kada se pribavljaju autentifikacioni podaci ovlašćenog korisnika na prikriven i neovlašćen način, i onda zloupotrebljavaju.

Dosluh, kada korisnik koji ima ovlašćenje da utiče na rad sistema (npr. administrator sistema), to zloupotrebi i u dogovoru sa trećim licima omogući neovlašćen pristup ili zloupotrebu sistema.

Prinuda, kada se ovlašćeni korisnik pod pretnjom primorava da omogući pristup ili upotrebu funkcija sistema nekom neovlašćenom licu.

Pored navedenog, biometrijski sistemi su meta specifičnih napada, koje, u zavisnosti od dela sistema prema kome su usmereni, možemo podeliti na [49]:

Prezentovanje lažne biometrije na senzoru, koja podrazumeva predstavljanje falsifikovanog biometrijskog podatka na samom senzoru (lažni otisak prsta, fotografija lica, snimak glasa i sl.)

Ponovno slanje predhodno poslatog uzorka, kada se presreću ispravni biometrijski podaci koje šalje senzor modulu za izdvajanje karakterističnih detalja i onda ponovo

prosleđuju, po potrebi. Ovaj napad ne zahteva ni izmene niti ostvarivanje uvida u podatke, već samo ponovno slanje presretnutih podataka, koji čak mogu i biti šifrovani.

Izmene na modulu za izdvajanje karakterističnih detalja, kada se zamenom programskog dela postiže da on, po potrebi, proizvede predefinisan set informacija.

Promene na podacima o karakterističnim detaljima, koja podrazumeva zamenu originalnih izdvojenih detalja sa nekim drugim, specifično dizajniranim.

Izmene na modulu za poređenje i donošenje odluke, gde se takođe, zamenom programskog dela, može definisati njegovo dalje funkcionisanje.

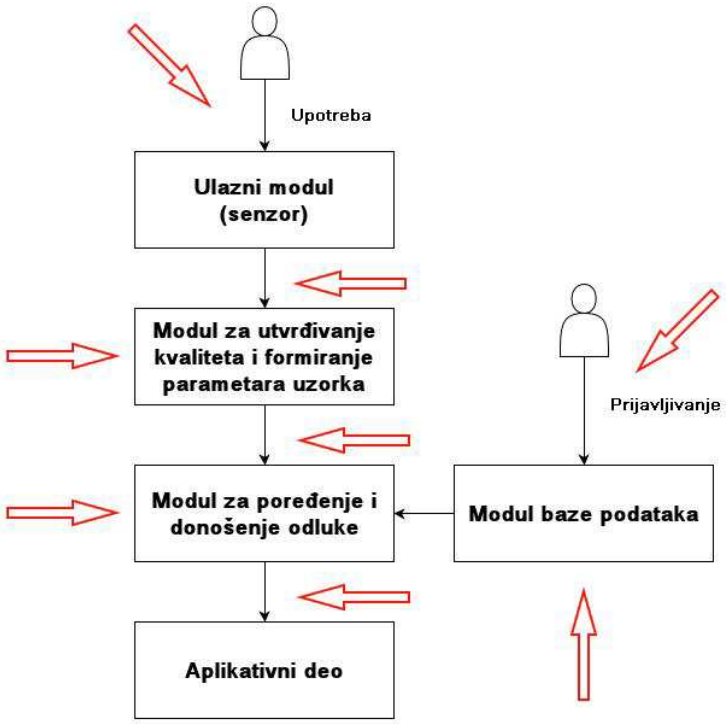
Izmene uskladištenih biometrijskih obrazaca, koji se nalaze u bazi podataka, koja može da se nalazi na centralnom serveru, ili više njih, ili lokalno, na uređaju.

Napad na nivou komunikacionih kanala između modula za poređenje i baze podataka, gde se podaci, odnosno biometrijski obrasci, koji se šalju tim kanalom presreću, menjaju i onda ponovo prosleđuju, u zavisnosti od potrebe.

Izmene krajnje odluke, kada se neovlašćenim pristupom i zloupotrebom, vrši menjanje odluke sistema.

Ovako klasifikovane napade možemo grupisati u napade na senzor, na komunikacione kanale, na module i na bazu podataka.

Dijagram 5: Napadi na biometrijski sistem



7.3 Napadi na elemente sistema

Senzor, kao najizloženiji segment biometrijskog sistema, je zbog toga predmet različitih napada, a sa ciljem da se utiče na funkcionisanje biometrijskog sistema. Uopšteno gledano, postoji više različitih načina vršenja uticaja na inicijalni biometrijski podatak, koji se prikuplja putem senzora i prosleđuje dalje, i tu spadaju [9]:

Lažno predstavljanje, kada neovlašćeni korisnik nastoji da se predstavi kao legitimni, a koje može biti slučajno, kada se slučajno bira identitet i ne menja biometrijski parametar koji koristi, ciljano, kada se se bira korisnik sa sličnim karateristikama, koji je lak za oponašanje, i sa modifikacijama, kada se vrši prilagođavanje biometrijskog parametra (npr. promena boje glasa, lažni potpis i sl.).

Obfusckacija, koja podrazumeva namerno prilagođavanje biometrijskog parametra u cilju onemogućivanja biometrijskog sistema da donese odluku, kako bi se izbegla identifikacija ili uticalo na funkcionisanje sistema kod verifikacije (promena izraza lica, promena boje glasa i sl.).

Falsifikovanje, kada se koristi neovlašćeno prikupljen i falsifikovan biometrijski parametar neke osobe (fotografija lica ili irisa, snimak glasa, imitacija otiska prsta i sl.) koji se prezentuje na senzoru, u nadi da će zavarati sistem. Do uzorka biometrijskog parametra, koji se onda zloupotrebljava na ovaj način, može se doći različitim metodama.

Pored navedenog, senzor može da bude i mete fizičkih napada, preduzetih kako bi se on oštetio ili uništio, i time onemogućilo funkcionisanje sistema, ili pak modifikacija ili zamena, a kako bi izvršio uticaj na podatake koje on prosleđuje ostatku sistema.

Sledeći bitan segment bezbednosnih sistema koji je predmet napada, jesu komunikacioni kanali. Njima se obezbeđuje tok informacija od senzora, između modula, baze podataka, kao i prosleđivanje finalne odluke sistema, i samim tim, imaju izuzetno bitnu ulogu u funkcionisanju sistema, čijim narušavanjem, mogu da se realizuju različiti ciljevi. Tim napadima se ostvaruje uvid u podatke, vrši njihovo prikupljanje , manipuliše sa njima, i ponovo prezentuje kako bi se uticalo na funkcionisanje sistema. Glavni tipovi napada na komunikacione kanale, su [14]:

Neovlašćeno prikupljanje podataka koji se šalju kroz kanale komunikacija i, na taj način, dolaženje do bitnih informacija o biometrijskim parametrima.

„Čovek u sredini” (man in the middle) napad, koji podrazumeva da se neovlašćena strana neprimećeno ubacuje u komunikacioni kanal između dva elementa sistema, i preuzima kontrolu nad tokom podataka, pri čemu se ostavlja utisak da postoji direktna komunikacija između elementa. Ovaj pristup obezbeđuje mogućnost neovlašćenog i neprimetnog prikupljanja bitnih podataka, ili njihovog menjanja u skladu sa ciljevima napada, i prosleđivanja ka odredištu.

Napad iscrpnom pretragom, (brute force), koji podrazumeva prezentaciju velikog broja biometrijskih podataka u nadi da će neki od njih biti dovoljno sličan legitimnom korisniku i omogućiti donošenje odluke sistema.

„Penjanje uz brdo” (hill climbing) napad, koji je sličan napadu iscrpnom pretragom, s tim što se u ovom slučaju podrazumeva da napadač ima pristup i ocenama poklapanja.

Ovaj način napada podrazumeva ubacivanje nekog biometrijskog podatka, beleženje njegove ocene poklapanja, zatim menjanje tog biometrijskog podataka, ponovno slanje, i utvrđivanje nove ocene poklapanja, pri čemu se taj proces ponavlja više puta, i postepeno generiše adekvatan biometrijski obrazac, čija ocena poklapanje će biti viša od tražene, i koji će na taj način biti prihvaćen od strane sistema [9].

Napad ponavljanjem, koji podrazumeva neovlašćeno prikupljanje podataka poslatih kroz komunikacioni kanal, i njihovo ponovno slanje u odgovarajućem momentu, bez menjanja, tako da je ovaj napad moguće realizovati i ako se podaci šifruju, kako bi se zaštitili.

Napad na ocene poklapanja, kada se vrši izmena podataka koji se odnose na ocene poklapanja.

Napad na finalnu odluku, kada se vrši izmena podataka koji se odnose na finalnu odluku sistema, koja se dalje prosleđuje.

Zatim, imamo napade na module sistema, u okviru kojih se vrši izdvajanje karakterističnih detalja i poređenje. Budući da su oni zasnovani na softverskim i hardverskim komponentama, napadi podrazmevaju direktne izmene ili modifikacije na njima, kako bi se uticalo na njihovo funkcionisanje, ili pak korišćenje malicioznih programa, kojima se preuzima kontrola nad funkcijama u okviru modula i obezbeđuje dalji uticaj na rad sistema.

Na kraju, imamo napade na bazu podataka, kada se neovlašćenim pristupom ostvaruje uvid u uskladištene biometrijske obrasce i bitne lične podatke korisnika, ili vrši njihova modifikacija ili zamena, kako bi se narušilo funkcionisanje sistema.

8. Rešenja bezbednosnih problema

8.1 Funkcionalni problemi koji utiču na bezbednost

Prvi tip problema, koji su vezani za funkcionisanje na osnovu ocene poklapanja, i samim tim, pojavu lažnih poklapanja i lažnih nepoklapanja, iako mogu da ugroze bezbednost, spadaju u domen funkcionalnih problema biometrijskih sistema. Samim tim, predložena rešenja ovog problema se nalaze u sferi razvoja tehnologija i algoritama, implementaciji multibiometrijskih sistema ili pak u kombinaciji biometrijskih i nekog nebiometrijskog metoda (token, lozinka i sl.).

8.2 Opšti bezbednosni problemi

Drugi tip problema su opšti bezbednosni problemi sa kojima se susreću svi zaštitni sistemi. Budući da nisu specifični za biometrijske sisteme, oni ne predstavljaju novi izazov, nego očekivane pojave sa već poznatim modalitetima zaštitnih mera koje se primenjuju i koje je potrebno imati u vidu pri formiranju biometrijskog sistema. To podrazumeva integrisanje fizičkog i tehničkog obezbeđenja, izbor adekvatnih hardverskih rešenja, kao i pravilan izbor algoritama na kojima se sistem bazira. Takođe, potrebna su adekvatna kadrovska rešenja i uvođenje pravila korišćenja i funkcionisanja, kao i mehanizama kontrole korišćenja sistema. Iako je priroda ovih bezbednosnih problema takva da oni nikad ne mogu biti u potpunosti otklonjeni, adekvatna implementacija pomenutih bezbednosnih mera, omogućava njihovu prevenciju ili, ako do njih dođe, otkrivanje i sprečavanje zloupotreba.

8.3 Specifični napadi na elemente biometrijskih sistema

Kada je u pitanju narušavanje bezbednosti na nivou senzora, falsifikovanjem i prezentovanjem lažne biometrije, rešenja se ogledaju u softverskim algoritmima i hardverskim implementacijama usmerenim ka tzv. detekciji živosti (liveness detection), odnosno potvrđivanju da se na senzoru nalazi prava osoba sa svojim biometrijskim podacima, gde imamo sledeće primere [50]:

- merenje obrasca znojenja prsta
- merenje protoka krvi i kiseonika, kod otiska prsta
- merenje spektralnih karakteristika
- spektrografske tehnike, kod irisa
- merenja toplotog odraza
- kretanje glave, lica, oka i zenica
- korišćenje trodimenzionalnih informacija i dr.

Kada se radi o napadu ponavljanjem, slanjem već poslate informacije, kao i izmenama informacija na nivou komunikacionih kanala i napadu na krajnju odluku, postoji

veliki broj tehnika kojima se može podići nivo bezbednosti i sprečiti napadi. U te tehnike spadaju [50]:

- korišćenje kriptografskih algoritama (npr. 3DES, AES) za šifrovanje informacija, čime se onemogućava ostvarivanje uvida ili menjanje podataka od strane neovlašćenih lica.
- korišćenje digitalnih potpisa, kako bi se potvrdila autentičnost podataka.
- korišćenje vremenskih oznaka (timestamping), ubačenih u podatke, da bi se verifikovao vremenski sled.
- korišćenje izazov/odgovor (challenge/response) tehnika, koje zahtevaju davanje pravilnog odgovora na postavljeni upit, kako bi se sprečilo ponovno slanje biometrijskih podataka.
- ograničavanje broja pokušaja u jedinici vremena, kako bi se sprečili napadi iscrpnom pretragom i sl.
- zaokruživanje ocena poklapanja, kako bi se znatno otežala primena tehnika „penjanja uz brdo“.
- korišćenje steganografskih i tehnika digitalnog vodenog žiga u cilju sakrivanja ili obezbeđivanja integriteta podataka [51].

Napad zamenom modula: rešenja se ogledaju u korišćenju specifičnog, prilagođenog hardvera i posebno prilagođenog softvera, kako bi se onemogućila zamena programskog koda i uticanje na rezultate.

Napad na biometrijske podatke u bazi, odnosno na biometrijske obrasce: verovatno najozbiljniji problem za uspešnu primenu biometrijskih sistema, jer baze podataka sadrže velike količne bitnih ličnih informacija, u ovom slučaju, nepromenljivih biometrijskih karakteristika, i samim tim predstavljaju objekat od izuzetnog značaja za svakog potencijalnog napadača. Pri tom, zbog samog funkcionisanja sistema, osim standardnih zaštitnih mera , nije moguće organizaciono i tehnički onemogućiti pristup tim podacima, tako da se koriste kriptografski algoritami i drugi metodi, koji će biti predmet razmatranja u posebnom segmentu ovog rada.

9. Bezbednost biometrijskih obrazaca

Kao što je već navedno, zaštita biometrijskih obrazaca uskladištenih u bazama podataka je izuzetno kompleksna oblast, i postoji više različitih načina za postizanje određenih nivoa bezbednosti. Biometrijske obrasce možemo štititi primenom sledećih metoda:

- kriptografski algoritmi
- izdvajanje na smart kartice
- steganografske tehnike
- digitalni vodeni žigovi
- tehnike vizuelne kriptografije
- transformacije podataka
- biometrijski kriptosistemi
- kombinacije transformacija podataka i biometrijskih kriptosistema

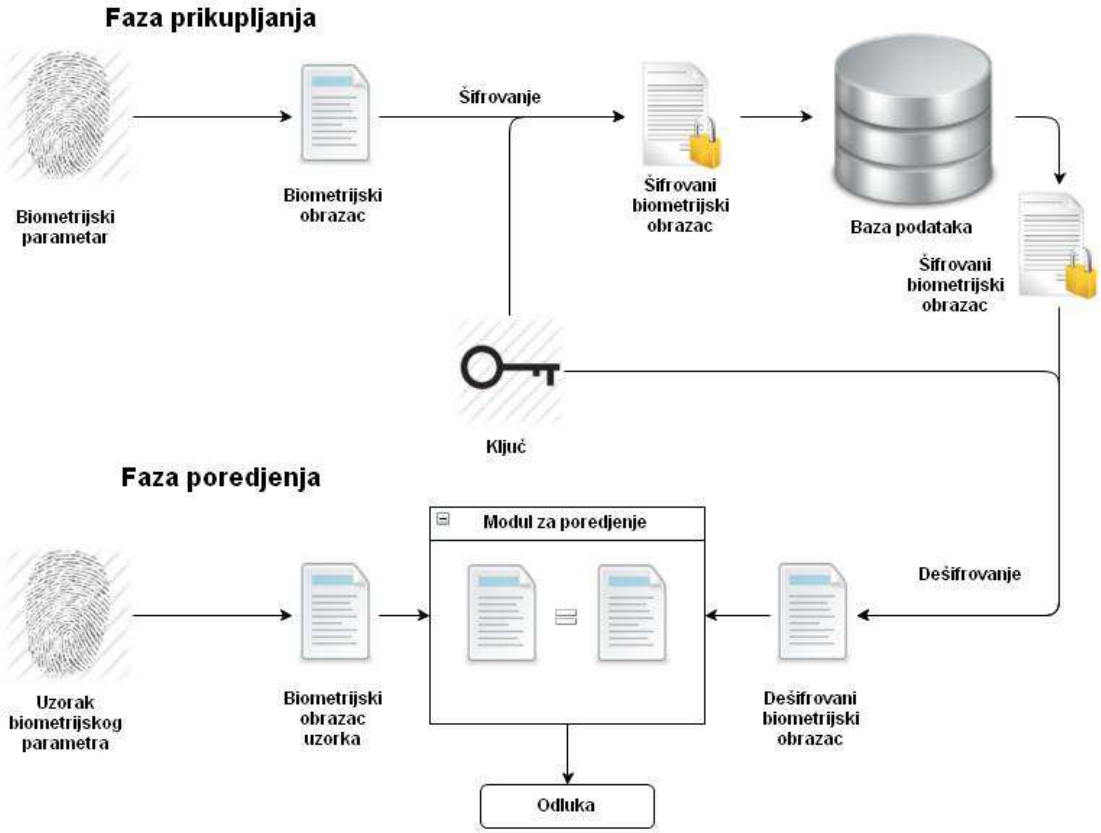
9.1 Primena kriptografskih algoritama

Jedan od osnovnih načina zaštite podataka je njihovo šifrovanje. Primenom standardnih kriptografskih algoritama, bilo simetričnih ili asimetričnih, moguće je postići visok nivo bezbednosti uskladištenih podataka. Međutim, tu se javlja problem koji proizilazi iz same prirode biometrijskih parametara. Naime, kao što je već naglašeno, skoro je nemoguće dobiti iste vrednosti biometrijskog parametra pri prikupljanju (čak štaviše, identične vrednosti biometrijskog parametra kao u bazi bi mogle da ukažu na napad ponavljanjem) tako da se zaključak donosi na osnovu dovoljne sličnosti između obrazaca, odnosno na osnovu ocene poklapanja. Šifrovanje u potpunosti menja podatke obrasca, tako da čak i najmanja razlika između obrasca koji se čuva i obrasca-uzorka proizvodi potpuno drugačije šifrovane vrednosti, koje se ni na koji način ne mogu porediti. Samim tim, nije moguće obezbediti funkcionisanje biometrijskog sistema zasnovanog na poređenju šifrovanih vrednosti, korišćenjem standardnih algoritama.

Biometrijski podaci se mogu obezbediti primenom standardnih kriptografskih algoritama, tako što bi se u nad prikupljenim i obrađenim podacima primenjivalo šifrovanje i te vrednosti skladištile u bazi podataka, a kasnije, u fazi poređenja, vršilo dešifrovanje , pri čemu bi se poređenje obavljalo nad otvorenim biometrijskim podacima u okviru modula za poređenje i donošenje odluke.

Ovakav vid organizacije sistema podiže stepen bezbednosti, ali i u ovom slučaju je biometrija u jednom trenutku prisutna u sistemu u potpuno otvorenom obliku, a samim tim i izložena riziku. Takav sistem nije težak za realizaciju, ukoliko bi mu namena bila da se koristi za potrebe verifikacije. Korišćenje ovako koncipiranog sistema za potrebe identifikacije bi bilo složenije za realizaciju, zbog velikog broja kriptografskih operacija, što bi značajno uticalo na hardverske zahteve i performanse sistema.

Dijagram 6: Zaštita biometrijskih obrazaca klasičnim kriptografskim algoritmima



Kao jedno od rešenja ovog problema, predlaže se nov koncept, a to je homomorfno šifrovanje (homomorphic encryption) [52]. Homomorfno šifrovanje je tip šifrovanja koji omogućava vršenje matemačkih operacija nad šifrovanim podacima, i dobijanje rezultata koji je, kad se dešifruje, identičan kao kad bi te matematičke operacije bile sprovedene nad istim, nešifrovanim podacima. U slučaju biometrijskih podataka, ovakvo šifrovanje omogućava poređenje podataka u šifrovanom obliku. U svom radu [53], autori iznose koncept anonimnog biometrijskog sistema za kontrolu pristupa koji koristi homomorfno šifrovanje i algoritam sličnosti, baziran na računanju Hamingovog rastojanja, za autentifikaciju. U radu, [54], autori predlažu korišćenje RSA algoritma, koji je delimično homomorfan i omogućava korišćenje operacija množenja, i specifične raspodele operacija između klijenta i servera, uz poseban način formiranja određenih slučajnih vrednosti, za potrebe biometrijske autentifikacije. Zatim, kompanija Fujitsu je objavila koncept sistema za biometrijsku autentifikaciju [55], koji se zasniva na korišćenju specifičnog oblika homomorfnog šifrovanja, kod koga se formira određeni redosled i podaci šifruju u blokovima, što značajno povećava performanse.

Takođe, dosta rasprostranjen metod zaštite, kod lozinki na primer, je da se ne čuvaju lozinke uopšte, već samo njihove heš vrednosti, koje se pored toga generišu uz dodatak pomoćnih informacija, na osnovu kojih se ne može doći do originalne lozinke. Međutim, zbog već navednih razlika koje se javljaju u prikupljanju (i osobina heš funkcija da i najmanja razlika u ulaznom podatku proizvodi ogromne razlike u konačnoj heš vrednosti) primena klasičnih kriptografskih jednosmernih funkcija na biometrijskim podacima, ne obezbeđuje vrednosti koje se mogu porediti i na osnovu kojih se može vršiti autentifikacija.

9.2 Izdvajanje biometrijskih podataka na smart kartice

Jedna od predloženih tehnika, kojom se može podići nivo bezbednosti biometrijskih obrazaca, ili celog biometrijskog sistema, jeste i njihovo izdvajanje i pohranjivanje na prenosive uređaje. Smart kartica je plastična kartica koja sadrži posebne elemente koji omogućavaju skladištenje, procesiranje i obezbeđivanje bitnih podataka, uz laku prenosivost, usled čega je pogodna za različite primene. Integrisanje biometrijskih sistema i smart kartica može se vršiti na više načina [56]:

Izdvajanje biometrijskog obrasca na karticu, kada se kartica koristi samo za skladištenje biometrijskog obrasca i određenih bitnih nebiometrijskih podataka, uz primenu kriptografskih tehnika kako bi se te podaci zaštitili i obezbedila uzajmna autentifikacija prilikom korišćenja kartice u okviru biometrijskog sistema.

Poređenje na kartici, kada se na kartici skladišti biometrijski obrazac i integriše modul za poređenje. Kod ovog načina, inicijalni biometrijski podaci i naknadni uzorci se prikupljaju putem ulaznih i procesnih modula biometrijskog sistema, zatim prosleđuju na karticu gde se skladište i vrši poređenje, da bi se zatim biometrijskom sistemu, putem sigurnih kanala, prosledila konačna odluka. Ovakav načina realizacije takođe zahteva primenu kriptografskih tehnike u cilju bezbednog funkcionisanja.

Poređenje na kartici uz distribuciju procesiranja, kada se modifikuje predhodno navedeni način, tako što se procesno zahtevne operacije dostavljaju biometrijskom sistemu na obradu, koji zatim vraća rezultate, a oni se onda koriste u procesu poređenja na kartici, kako bi se formirala konačna odluka.

Izdvajanje kompletnog biometrijskog sistema na karticu, tako da se u okviru kartice integriše i senzor, moduli za izdvajanje karakterističnih detalja, poređenje i donošenje odluke, i lokalno skladište podataka, u koje se pohranjuju biometrijski obrasci i bitni nebiometrijski podaci. Samim tim, celokupno funkcionisanje se odvija u okviru kartice, dok je konačna odluka jedini element koji se prosleđuje dalje, kako bi se realizovalo funkcionisanje u okviru neke od oblasti primena. Takođe, potrebna je primena kriptografskih i drugih tehnika, i eventualno posebno prilagođenog hardvera za uspešnu realizaciju ovog sistema.

Izdvajanje biometrijskog obrasca na karticu podiže bezbednost biometrijskog sistema, a i obezbeđuje dvofaktorsku autentifikaciju, jer se za funkcionisanje sistema koristi nešto što korisnik jeste i nešto sa čim raspolaže. Samim tim, za zloupotrebu je potrebno neovlašćeno prikupiti uzorak tog biometrijskog parametra korisnika (uz pretpostavku da je obrazac u kartici u izmenjenom obliku i da se na osnovu njega ne može rekonstruisati originalna biometrija), kao i kopirati ili otuđiti karticu sa uskladištenim obrascem, a zatim sve to zajedno prezentovati na adekvatan način, kako bi se zavarao neki sistem, što predstavlja čitav niz prepreka za potencijalnog napadača.Takođe, ovakva integracija biometrije i kartica, kao što je već napomenuto, zahteva primenu adekvatnih kriptografskih i drugih tehnika u celom biometrijskom sistemu, kako bi se obezbedili sigurni kanali komunikacija i sprečili drugi mogući napadi.

Poređenje na kartici dodatno podiže nivo bezbednosti sistema, jer se čitav jedan segment izdvaja i samim tim, otežava pristup potencijalnom napadaču, ali i on zahteva

primenu adekvatnih bezbednosnih rešenja u ostatku sistema, da bi se isključili različiti mogući napadi.

Izdvajanje celog sistema na karticu je najkompleksnije i najzahtevnije rešenje, ali samom svojom realizacijom, onemogućava čitav niz napada i zloupotreba, mada ih ne otklanja u potpunosti, i takođe zahteva određene bezbednosne preduslove, kako bi se postigao visok nivo bezbednosti.

9.3 Steganografija, digitalni vodeni žigovi i vizuelna kriptografija

Kao što je već navedeno, steganografija predstavlja skrivanje poruke na takav način, da niko osim pošiljaoca i primaoca ne zna ni da poruka postoji. Samim tim, primena steganografskih tehnika može da obezbedi zaštitu biometrijskih podataka njihovim skrivanjem u okviru drugih podataka, čime se značajno otežava ili sprečava da neko neovlašćen dođe u njihov posed.

Primer imamo u radu [51], gde autori, između ostalog, iznose i dve tehnike zaštite biometrijskih podatka korišćenjem steganografskih tehnika. Prva tehnika podrazumeva sakrivanje biometrijskih podataka (npr. podaci o karakterističnih detaljima otiska prsta) u slici, koja može da bude generička slika otiska prsta, slika lica ili neka slučajno izabrana slika, tako da potencijalni napadač ne bude svestan da uopšte postoje podaci o karakteristikama, ili da pomisli da je ta slika u stvari biometrijski obrazac. Druga predložena tehnika podrazumeva sakrivanje biometrijskih podataka formiranih na osnovu slike lica u slike otisaka prstiju, koji se zatim skladište na kartici, pri čemu se oba biometrijska parametra koriste u procesu verifikacije.

Zatim, u radu [57], autori predlažu sistem zaštite biometrijskih obrazaca, sakrivanjem predhodno šifrovanih biometrijskih podataka (karakteristični detalji otiska prsta) na slučajno izabranim pozicijama u određenom nosećem zvučnom signalu (govor, muzika...), pri čemu je za njihovo izdvajanje neophodno posedovanje tajnog ključa.

U radu [58], autori predlažu zaštitu biometrijskih podataka formiranih na osnovu slike irisa, njihovim sakrivanjem u određenoj izabranoj slici, korišćenjem pseudoslučajnih nizova za šifrovanje biometrijskih podataka i podataka o poziciji, pri čemu nije potrebno posedovanje originalne slike za povraćaj podataka.

Digitalni vodeni žig se koristi za označavanje jednog skupa podataka, ubacivanjem izabranih podataka u njega, a kako bi se taj skup podataka zaštitio. U slučaju biometrijskih podataka, integrisanjem vodenog žiga sa informacijama o samim podacima, moguće je sprečiti izmene na njima, ili omogućiti utvrđivanje njihovog porekla, u slučaju zloupotrebe.

Primer je dat u radu [59], gde autori predlažu korišćenje tehnike nevidljivih lomljivih žigova za potrebe verifikacije integriteta podataka, ubacivanjem digitalnog vodenog žiga u slike otisaka prstiju u cilju sprečavanja njihove izmene ili zamene.

Zatim, u radu [60], autori predlažu korišćenje tehnika difuzije, kako bi se izmenio biometrijski obrazac, u koji se zatim ubacuje slika lica nosioca biometrije u obliku digitalnog vodenog žiga, i na taj način obezbeđuje tajnost i bezbednost biometrijskih podataka.

U radu [61], autori predlažu dve tehnike ubacivanja digitalnih vodenih žigova u slike otisaka prstiju, pri čemu se jedna može primeniti pre faze izdvajanja karakterističnih detalja, a druga posle, kako bi se osigurao njihov integritet.

Vizuelna kriptografija podrazumeva podelu podataka koji se štite u dve ili više slika na takav način da se celovit podatak dobija tek njihovom kombinacijom.

Primer ovog sistema je dat u radu [62], gde autori predlažu zaštitu biometrijskih podataka formiranih na osnovu slika lica njihovom podelom u dve slike, koje se skladište na različitim serverima, i koje same po sebi ne omogućavaju da se dođe do originalnog biometrijskog podatka. Takođe, sličnu tehniku je moguće primeniti na slike otisaka prstiju ili irisa. Nedostatak ovog sistema je što ipak u jednom trenutku formira originalni otisak, u fazi poređenja, što otvara mogućnost za njegovu kompromitaciju.

Slično rešenje se predlaže i u radu [63], gde se originalni podaci dele u dve slike, s tim što se onda te slike šifruju u cilju postizanja višeg nivoa zaštite.

U radu [64], predlaže se primena vizuelne kriptografije u biometrijskom sistemu zasnovanom na otisku prsta, tako što se slika otiska prsta deli na dva dela, pri čemu se jedan skladišti na ID kartici kod korisnika, a drugi smešta u bazu podataka, a u fazi poređenja se spajaju i upoređuju sa novim, prikupljenim uzorkom.

U radu [65], predlaže se način zaštite biometrijskih obrazaca formiranih na osnovu slike irisa, primenom metoda vizuelne kriptografije, tako što se slika irisa kombinuje sa drugom, izabranom slikom i deli na dva dela, od kojih se jedan skladišti na ID kartici, a drugi u bazi podataka, da bi se u fazi poređenja vršilo spajanje i poređenje sa prikupljenim uzorkom.

Takođe, moguće je napraviti razne kombinacije kriptografskih i steganografskih tehnika, i vodenih žigova, i na taj način značajno podići nivo bezbednosti podataka.

9.4 Primena transformacija podataka i biometrijskih kriptosistema

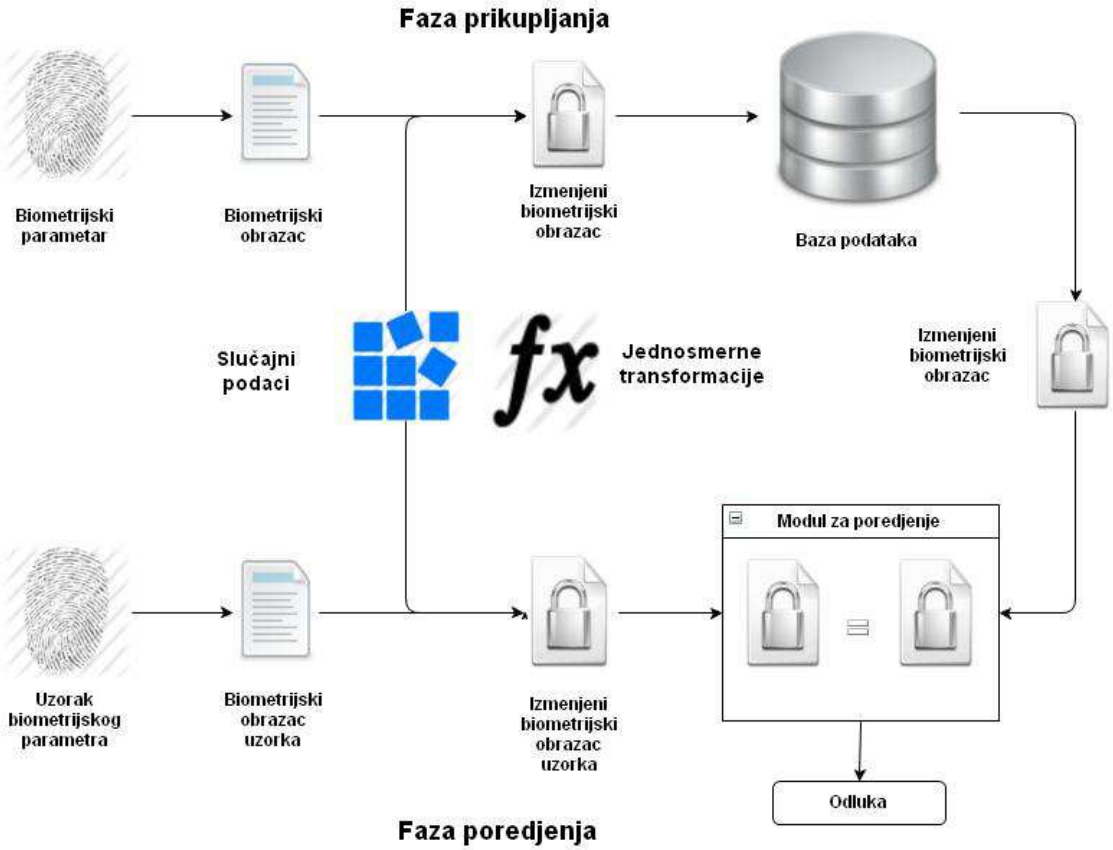
Bezbednost biometrijskih obrazaca, zbog navedenih specifičnosti, ne može se u potpunosti ostvariti uobičajenim metodama zaštite. Klasične kriptografske metode podižu bezbednost sistema na viši nivo, ali ni one ne nude potpunu bezbednost biometrijskih podataka. Usled toga, ova tema je predmet brojnih razmatranja i istraživanja, tako da postoji veliki broj predloženih rešenja sa različitim konceptima postizanja zadovoljavajućeg nivoa bezbednosti.

Prema autorima [66], sisteme kojima se postiže bezbednost biometrijskih obrazaca delimo na sisteme bazirane na transformacijama podataka, biometrijske kriptosisteme i na kombinovane sisteme.

9.4.1 Sistemi bazirani na transformacijama podataka

Kod ovih sistema, bezbednost se postiže tako što se nad originalnim biometrijskim podacima primenjuje transformaciona funkcija, na bazi određenog ključa, i na taj način formira izmenjeni (transformisani) biometrijski obrazac, koji se zatim skladišti u bazi podataka [66]. Kod poređenja, primenjuje se ista funkcija, na osnovu istog ključa, i na uzorku biometrijskog podatka, i tako se dobija transformisani obrazac uzorka, koji se onda poredi sa obrascem iz baze podataka.U zavisnosti od primenjene funkcije, ove sisteme delimo na sisteme koji koriste slučajne podatke (biometric salting) i sisteme koji koriste jednosmerne transformacije.

Dijagram 7: Sistemi bazirani na transformacijama podataka



Sistemi koji koriste slučajne podatke [66] funkcionišu tako što vrše izmene na biometrijskim podacima, transformišući ih na osnovu funkcije zasnovane na određenim slučajnim podacima, koji predstavljaju ključ. Kod ovih sistema, čuvaju se izmenjeni biometrijski obrazac i ključ, mada ne nužno na istom mestu, odnosno u istoj bazi. Kod faze poređenja, novi uzorci biometrijskih podataka se takođe transformišu taj način, korišćenjem istog ključa, i onda se vrši poređenje. Korišćenje ključa smanjuju stopu lažnog poklapanja i omogućava formiranje različitih obrazaca za određenu osobu, na osnovu različitih ključeva, i obezbeđuje da se uskladišteni izmenjeni biometrijski obrazac po potrebi lako može povući i zameniti novim. Nedostatak ovog sistema se ogleda u tome što je potrebno čuvati i taj ključ, tako da, ukoliko on bude kompromitovan, postoji mogućnost da napadač dođe do originalnih biometrijskih podataka. Takođe, treba voditi računa da izabrani način menjanja podataka ne naruši funkcionisanje biometrijskog sistema.

Primer ovog sistema dat je u radu [67], gde autori predlažu kombinovanje pseudo slučajnih podataka, uskladištenih u tokenu, i biometrijskih podataka formiranih na osnovu otiska prsta, za stvaranje specifičnog niza podataka (BioHashing), koji se koristi za potrebe autentifikacije. Ovakvo kombinovanje podiže nivo bezbednosti biometrijskih podataka, ukoliko napadač ne dođe do pseudo slučajnih vrednosti, ili do tokena, omogućava laku zamenu obrazaca izmenom tokena i podiže nivo funkcionisanja biometrijskog sistema.

Zatim, u radu [68], predlaže se kombinovanje biometrijskih podataka na osnovu otiska dlana i pseudoslučajnih podataka, kako bi se generisao odgovarajući obrazac (PalmHash), koji se zatim skladišti, u bazi podataka ili na prenosnim uređajima, poput tokena ili smart kartice. Ovakva organizacija obezbeđuje mogućnost generisanja većeg broja tih kombinovanih obrazaca, korišćenjem različitih slučajnih vrednosti, njihovu laku zamenu u slučaju potrebe, i takođe podiže funkcionalni nivo sistema u odnosu na korišćenje samo biometrijskog parametra.

U radu [69], predlaže se tehnika zaštite biometrijskih podataka formiranih na osnovu slika lica, korišćenjem slučajnih podataka. Predloženo rešenje podrazumeva primenu odgovarajućih transformacija nad prikupljenim slikama, pri čemu se na osnovu unetog PIN broja od strane korisnika, korišćenjem pseudoslučajnog generatora brojeva, generiše odgovarajući šablon za te transformacije. Zatim se tako izmenjene slike objedinjuju u jedinstven filter, koji se skladišti, i koristi za poređenje. U slučaju potrebe, lako se formira drugačiji šablon za transformacije i vrši zamena uskladištenog filtera.

U radu [70], predlaže se tehnika zaštite biometrijskih podataka formiranih na osnovu slike irisa, ubacivanjem veštačkih šema, a kako bi se formirao obrazac koji se lako može zameniti. Mogu se koristiti čisto slučajnih podaci, slučajna šema slična teksturi irisa ili veštački generisani irisi, pri čemu se kombinovanjem sa originalnim slikama irisa, dobijaju izmenjeni obrasci koji se zatim skladište. Za funkcionisanje sistema neophodna je istovremena prezentacija originalnog irisa i konkretno korišćene veštačke šeme, koja ima ulogu ključa.

Bitna karakateristika ovih sistema je da obezbeđuju otkazivost i obnovljivost, tako da se u slučaju narušavanja bezbednosti lako vrši izmena biometrijskih obrazaca koji se čuvaju.

Sistemi koji koriste jednosmerne transformacije [66] postižu bezbednost biometrijskih podataka tako što ih transformišu koristeći pri tome jednosmerne funkcije. Jednosmerne funkcije su matematičke funkcije kod kojih je lako izračunati rezultat na bazi određenih promenljivih, ali je izuzetno teško, skoro nemoguće, samo na bazi rezultata doći do vrednosti tih promenljivih. Njihovo funkcionisanje se određuje odgovarajućim parametrima, definisanim putem ključa, koji je takođe potrebno čuvati. Prednost se ogleda u tome što je, čak i da i promenjeni biometrijski obrazac i ključ budu kompromitovani, izuzetno teško doći do originalnih biometrijskih podataka zbog same prirode jednosmernih funkcija. Nedostatak ovog sistema je u teškoći realizacije funkcije koja omogućava čuvanje prepoznatljivih karakteristika originalnog biometrijskog obrasca, uz obezbeđivanje nepovratnosti.

Primer ovog sistema dat je u radu [71], gde se nad biometrijskim podacima, dobijenim iz otiska prsta, primenjuje određena transformacija (Kartezijanska, polarna ili savijanja površina), koja menja strukturu podataka tako da se na osnovu dobijenog izlaznog niza podataka može vršiti poređenje, ali ne i doći do izvorne biometrije.

U radu [72], predlaže se korišćenje specifičnih jednosmernih funkcija koje se prilagođavaju individualnim biometrijskim parametrima korisnika (robust hashing) u kombinaciji sa kriptografskim heš funkcijama u cilju formiranja obrazaca za skladištenje, i razmatra se njihova primena u cilju zaštite biometrijskih podataka formiranih na osnovu slike lica. Osim izmenjenih obrazaca, kod ovog metoda se skladište i parametri tih specifičnih jednosmernih funkcija, koji se izdvajaju na token ili smart karticu.

U radu [73], predlaže se način izdvajanja biometrijskih karakteristika otisaka prsta, formiranjem podskupova minucija (karakterističnih detalja), koje se koriste za poređenje, nad kojima se onda vrši primena jednosmernih funkcija, tako da se u bazu pohranjuju samo izmenjeni obrasci. Poređenje celih otisaka prstiju se vrši na osnovu niza poklapanja pomenutih podskupova sa sličnim parametrima transformacija.

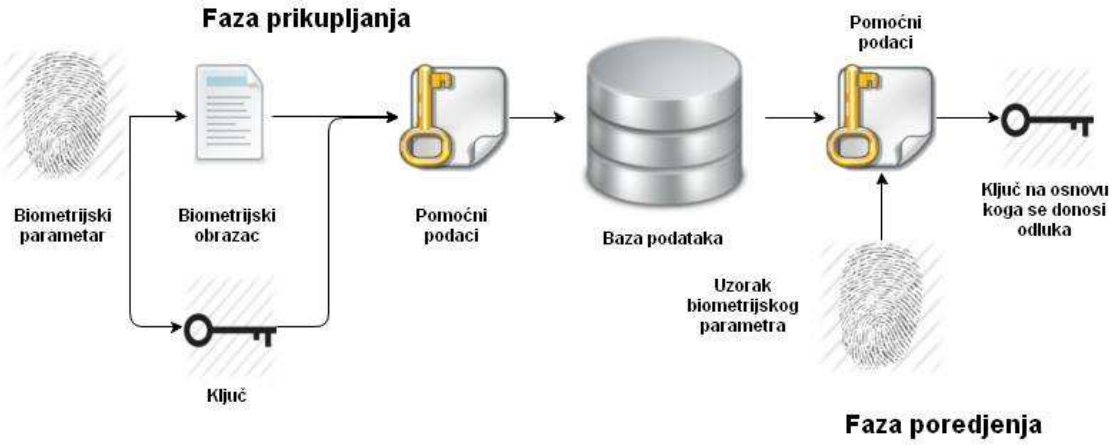
U radu [74], predlaže se poseban pristup (BioConvolving), koji uključuje primenu niza jednosmernih transformacija nad biometrijskim podacima, kako bi se kreiralo više izmenjenih obrazaca, i razmatra primena ovog metoda nad biometrijskim podacima formiranim na bazi prepoznavanja potpisa u realnom vremenu, a kako bi se osigurala njihova bezbednost i omogućila laka zamena u slučaju potrebe.

9.4.2 Biometrijski kriptosistemi

Biometrijski kriptosistemi (ili biometrijsko šifrovanje) [75], predstavljaju zajednički naziv za niz tehnika kojima se osigurava ključ, vezujući ga za biometrijske podatke, ili kojima se generiše ključ, na osnovu biometrijskih podataka, čime se otklanja potreba za čuvanjem biometrijskih obrazaca. Kod ovih tehnika, skladište se samo obrasci formirani njihovom primenom, koji se još nazivaju i „pomoćnim podacima“ (helper data), i na osnovu kojih se ne može rekonstruisati ni originalni biometrijski podatak niti ključ. Prezentovanjem pravog biometrijskog parametra pri verifikaciji, vrši se dešifrovanje i dolazi se do ključa, koji se dalje koristi, u zavisnosti od potreba sistema. Biometrijske kriptosisteme delimo na sisteme koji vezuju ključ i sisteme koji generišu ključ.

Sistemi koji vezuju ključ [75] funkcionišu tako što spajaju ključ sa biometrijskim podacima, i na taj način kreiraju pomoćne podatke, koji se skladište. U fazi prikupljanja, generiše se slučajni ključ koji nije povezan sa biometrijskim podacima i koji se uvek može promeniti, a koji se primenom ovih tehnika vezuje sa biometrijskim podacima, i na osnovu toga formiraju pomoćni podaci, koji se čuvaju u bazi podataka, na kartici i sl. Po formiranju tih podataka, i ključ i biometrijski podaci se odbacuju, čime se sprečava neovlašćeni pristup, da bi se zatim kod verifikacije, na osnovu uzorka originalne biometrije, vršilo ponovno kreiranje ključa, za korišćenje u funkcionisanju sistema, uz ponovno odbacivanje uzorka biometrijskog parametra. Kako bi se obezbedilo funkcionisanje i pored difuzne prirode biometrijskih podataka, koriste se kodovi za korekciju grešaka, koji koriguju određeni nivo grešaka, očekivanu kod legitimnog korisnika, ali ne i veće razlike, koje se javljaju u slučaju drugih lica. Takođe, u određenim slučajevima, kod ovih sistema se čuva i heš vrednost tog ključa, kako bi se osigurala preciznost, jer se rezultat prosleđuje samo u slučaju potpunog poklapanja uskladištene heš vrednosti i heš vrednosti ponovno kreiranog ključa.

Dijagram 8: Biometrijski kriptosistemi



Prednosti ovih sistema su sledeće [75]:

- ne skladište se ni biometrijski obrasci, niti originalni biometrijski podaci u bilo kom obliku
- originalni biometrijski podaci se ne mogu rekonstruisati iz uskladištenih pomoćnih podataka
- pružaju mogućnost generisanja velikog broja različitih pomoćnih podataka na bazi istog biometrijskog parametra, tako da mogu da se koriste za više namena
- ne može se izvršiti povezivanje korisnika u različitim primenama biometrijskog parametra, na osnovu uskladištenih pomoćnih podataka
- pomoćni podaci se lako menjaju, u slučaju kompromitacije
- lako se integrišu u postojeće kriptografske sisteme
- obezbeđuju pouzdaniju autentifikaciju i viši nivo bezbednosti podataka usled bliskog povezivanja ličnih biometrijskih parametara i sistemskih vrednosti
- zbog svoje prirode, otporni su na napade zamenom, na neovlašćene modifikacije, maliciozne programe, menjanje konačne odluke, a i teže ih je zavarati
- pogodni su za upotrebu u slučajevima velikog broja korisnika, a u bazi se skladište samo pomoćni podaci, koji sami po sebi ne otkrivaju bitne informacije.

Primer ovog sistema je tzv. „fuzzy commitment scheme“ [76], gde autori predlažu predstavljanje ključa kodnom reči koda za korekciju grešaka i njeno spajanje sa biometrijskim podacima, pri čemu se čuvaju ti kombinovani podaci i heš vrednost te kodne reči. Pri poređenju, na osnovu biometrijskog uzorka i korišćenjem kodova za ispravljanje

grešaka nad izvedenim podacima, dolazi se do kodne reči i vrši poređenje njene heš vrednosti sa uskladištenom i na bazi toga donosi odluka, odnosno oslobađa ključ.

Sledeći primer je tzv. „fuzzy vault“ [77], gde se predlaže kombinovanje izabranog tajnog podatka, odnosno ključa, i biometrijskih podataka, predstavljanje korišćenjem polinoma i integracija slučajnih tačaka (chaff points), kako bi se sakrili originalni elementi, u podatke koji se čuvaju. Pri poređenju, na bazi biometrijskog uzorka, ukoliko postoji dovoljno poklapanje, dolazi se do podataka nad kojima se primenjuju kodovi za ispravljanje grešaka i tako formira tajni podatak, odnosno ključ, i dalje koristi. Prednost ovog sistema je što je pogodan za neuređene podatke, jer njihov raspored ne utiče na njegovo funkcionisanje.

Zatim, predlaže se i korišćenje zaštitnih funkcija (shielding functions) [78], odnosno primenu odgovarajućih funkcija, nad kombinovanim tajnim podatkom, odnosno ključem, i biometrijskim podacima, kako bi se formirali pomoćni podaci koji se skladište, i koji se kasnije koriste.

Sistemi koji generišu ključ [66] formiraju pomoćne podatke na osnovu biometrijskog obrasca, i u procesu generisanja ključa koriste te pomoćne podatke i uzorak biometrijskog parametra. Korišćenjem pomoćnih podataka, u ovom slučaju, omogućava se zamena tih ključeva, u slučaju da dođe do njihove kompromitacije.

Ovaj koncept se razmatra u radu [79], i predlažu rešenja kojima bi se omogućilo korišćenje difuznih podataka za potrebe generisanja kriptografskih ključeva i obezbeđivanje pouzdane autentifikacije na bazi biometrijskih podataka. U tom cilju, predlažu se dva tehnike. Prva, tzv. „fuzzy extractor“ tehnika, omogućava generisanje niza slučajnih podataka sa jednakom raspodelom na osnovu nekog ulaznog podataka, pri čemu se ti podaci ne menjaju u slučaju manjih promena na ulaznom podatku, čime se omogućava korišćenje ove tehnike za generisanje kriptografskih ključeva na osnovu biometrijskih parametara. Druga, tzv. „secure sketch“ tehnika, omogućava formiranje pomoćnih podataka koji sami po sebi ne otkrivaju informacije o ulaznom podataku, ali na osnovu kojih se, uz prezentovanje odgovarajućeg, dovoljno sličnog, biometrijskog parametra, može rekonstruisati originalni biometrijski podatak. Takođe, u radu se razmatraju i njihove forme, u slučajevima kad se kao mere sličnosti podataka koriste Hemingovo rastojanje, rastojanje uređivanja i razlika između skupova.

Dalje razmatranje „fuzzy extractor“ tehnike imamo u radu [80], gde se predlaže primena ovog koncepta za formiranje autentifikacine šeme zasnovane na otisku prsta.

Zatim, u radu [81], razmatra se korišćenje navedenih tehnika u slučajevima kada postoje razlike u kvalitetu podataka, u fazi prikupljanja i kod ponovnog uzimanja uzorka, kao i uticaj takvog asimetričnog pristupa na jačinu formiranih ključeva i nivo zaštite identiteta.

U radu [82], razmatra se primena „fuzzy extractor“ koncepta na kontinuirane distrbucije biometrijskih podataka, i mogućnosti generisanja kriptografskih ključeva.

U radu [83], razmatra se pitanje zaštite biometrijskih obrazaca primenom „secure sketch“ tehnike, prednosti i mane ovog sistema, i analizira se primena ove tehnike u cilju zaštite biometrijskih obrazaca formiranih na osnovu slike lica. Takođe, razmatra se i primena ove tehnike za potrebe multifaktorske autentifikacije.

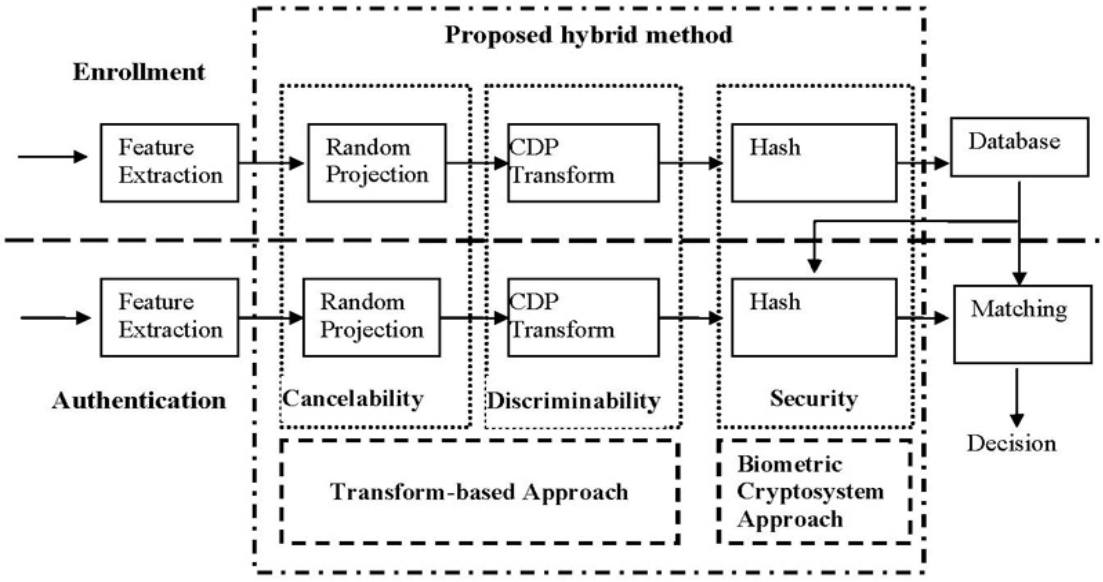
Kod kriptosistema koji generišu ključ, bitan problem je postizanje dovoljne različitosti u podacima, tako da su dva bitna faktora kod ovih sistema postojanost ključa i entropija ključa [66]. Postojanost ključa se odnosi na mogućnost ponovnog generisanja ključeva na osnovu biometrijskih podataka, a entropija na broj ključeva koje je moguće generisati. Viši nivo jednog, obično negativno utiče na nivo drugog faktora, tako da je istovremeno obezbeđivanje lakog rekonstruisanja ključa i zadovoljavajućeg opsega mogućih ključeva, problem sa kojim se suočavaju ovi sistemi.

Problematika generisanja ključeva na osnovu biometrijskih parametara je oblast koja je predmet intezivnih istraživanja i razvoja, sa različitim predloženim rešenjima i brojnim razmatranjima prednosti i mana, i shodno tome, biće detaljnije razmatrana u posebnom segmentu ovog rada.

9.4.3 Kombinovani sistemi

Kombinovani ili hibridni sistemi podrazumevaju kombinovanje korisnih karakteristika oba tipa sistema, npr. integrisanje slučajnih podataka uz primenu sistema za vezivanje ili generisanje ključa [66].

Primer ovakvog sistema se navodi u radu [84], gde se predlaže primena sistema zasnovanog na transformacijama, primenom tehnika slučajne projekcije (random projection) i transformacije uz očuvanje različitosti (discriminability preserving transform), i biometrijskog kriptosistema, koji vezuje ključ, primenom koncepta „fuzzy commitment scheme“, nad biometrijskim podacima formiranim na osnovu slike lica.



Slika 20: Primer sistema navedenog u radu [84], sa predloženim tehnikama[20]

Zatim, u radu [85], predlaže se primena hibridnog sistema u cilju zaštite biometrijskih podataka zasnovanih na otisku prsta. Kod ovog primera, vrši se kombinovanje jednosmernih transformacija, kojima se transformišu regioni oko minucija, i

[20] Izvor slike: http://www.comp.hkbu.edu.hk/~ycfeng/project/project.html (pristup 04.05.2014.)

biometrijskog kriptosistema, implementacijom „fuzzy vault“ tehnike, korišćenjem linearnih jednačina i slučajnih podataka (chaff points).

U radu [86], predlaže se kombinovanje transformacija, kako bi se kreirali otkazivi biometrijski obrasci, na osnovu kojih se generišu ključevi, pri čemu se kao osnova koriste podaci dobijeni na osnovu rasporeda vena dlana, odnosno karakteristični detalji račvanja i završetaka tih vena.

10. Generisanje kriptografskih ključeva na osnovu biometrijskih parametara

10.1 Generisanje kriptografskih ključeva

Kriptografski ključ, kao što je već navedeno, predstavlja niz podataka na osnovu koga se vrše izmene na podacima koji se štite i time čine nerazumljivim za treća lica. Savremeni kriptografskih sistemi svoje funkcionisanje zasnivaju na ključevima, koji predstavljaju osnovu za šifrovanje i dešifrovanje, za formiranje digitalnih potpisa, autentifikacionih kodova i sl. Pri tome, algoritmi na osnovu kojih ti kriptografskih sistemi funkcionišu su uglavnom javno dostupni i dobro poznati, tako da se bezbednost podataka ostvaruje isključivo korišćenjem adekvatnih ključeva odgovarajuće dužine.

Kao mera te adekvatnosti, koristi se tzv. entropija. Entropija predstavlja meru neodređenosti neke varijable, tako da što je viša entropija to je veća i neodređenost, a manja mogućnost dolaska do zaključka o toj varijabli. Idealno, izborom odgovarajućeg ključa treba obezbediti da jedan bit niza sadrži jedan bit informacije, i u tom slučaju imamo apsolutnu slučajnost, bez mogućnosti da se predvidi ishod.

Za generisanje ključeva, uzimajući pri tom u obzir navedene zahteve, koriste se generatori ključeva. Generatori ključeva su uređaji ili algoritmi koji generišu određeni niz brojeva ili simbola koji deluje slučajno, i u zavisnosti od načina na koji postižu taj efekat slučajnosti, delimo ih na generatore slučajnih brojeva (RNG) i generatore pseudoslučajnih brojeva (PRNG).

Generatori slučajnih brojeva kao izvor entropije koriste neku pojavu koja ima slučajne karakteristike (buka, radijacija..), a generisanje ključa se vrši na osnovu prikupljnih podataka u određenom vremenskom periodu. Generatori pseudoslučajnih brojeva su algoritmi koji tu slučajnost u nizu postižu primenom kompleksnih operacija na osnovu neke zadate inicijalne vrednosti.

Za kriptografske potrebe, koriste se posebno prilagođeni generatori, koji se nazivaju kriptografski sigurni generatori pseudoslučajnih brojeva (CSPRNG) [87]. Prilagođavanje se ogleda u tome što se oni kreiraju na osnovu specifičnih zahteva, kako bi bili otporni na primenu kriptoanalitičkih metoda ili direktne napade. U ove svrhe mogu da se koriste blokovski ili sekvencijalni simetrični kriptografski algortimi ili specijalizovana rešenja (Blum Blum Shub, Fortuna, FIPS 186-2...).

Korišćenje ovih tehnika za generisanje ključeva, i njihovu dalju upotrebu, i pored nesumnjive i dokazane korisnosti, zahteva ispunjavanje niza uslova i formiranje i usvajanje kompleksnih metodologija funkcionisanja, kako bi se sastavio efikasan i bezbedan sistem zaštite. Upravo je ta kompleksnost i uzrok razmatranja alternativnih rešenja generisanja ključeva, poput primene biometrijskih parametara.

10.2 Primena biometrijskih parametara za potrebe generisanja ključeva

Kao što je već napomenuto, usled kompleksnosti postojećih rešenja tehnika generisanja ključeva, kao predmet razmatranja javljaju se i alternativni načini, koji opet imaju svoje prednosti ali i mane. Biometrijski parametri predstavljaju alternativno rešenje sa velikim potencijalom, ali i određenim slabostima, i njihova primena u te svrhe je predmet kontinuiranog razmatranja i istraživanja, a u cilju razvoja funkcionalnih tehnika koje će maksimalno iskoristiti prednosti, uz otklanjanje nedostataka.

Prednosti biometrijskih parametara su njihova kompleksna struktura, koja nudi veliki opseg mogućnosti za odabir neke grupacije karakteristika i njihovo korišćenje kao osnove za generisanje ključeva. Uz to, sa stanovišta daljeg korišćenja i regeneracije tih ključeva, jedinstvenost i nepromenljivost biometrijskih parametara su takođe prednosti koje dolaze do izražaja u funkcionisanju tih sistema, jer omogućavaju pouzdanu autentifikaciju korisnika tih ključeva, i njihovo ponovo generisanje, u skladu sa potrebama. Zatim, biometrijski parametri su neodvojivi deo korisnika, pa su uvek i prisutni, tako da ovi sistemi ne zahtevaju pamćenje i nošenje nečeg kako bi se generisao ključ.

Nedostaci biometrijskih parametara su, paradoksalno, baš i one osobine koje spadaju u prednosti. Naime, njihova struktura, iako je kompleksna, opet je ograničene veličine, i samim tim, bez primene nekih pomoćnih informacija, može da obezbedi generisanje samo određene količine ključeva. Sledeći nedostatak je ta jedinstvenost i nepromenljivost, jer ako dođe do kompromitovanja procesa generisanja ključa i napadač dođe do originalnih biometrijskih podataka korisnika, to predstavlja trajan i nepromenljiv gubitak, koji potencijalno može da ima ozbiljne posledice. Zatim, biometrijski parametri nisu skriveni, i mogu biti i neovlašćeno prikupljeni od strane trećih lica, i zloupotrebljeni, a postoji i više tehnika napada na biometrijske sisteme, i to opet može da ugrozi njihovu svrhu.

Sistemi za generisanje ključeva na bazi biometrijskih parametara, uopšteno gledajući, obuhvataju dva segmenta [88]. Prvi segment obuhvata registraciju, odnosno prikupljanje biometrijskih podataka, formiranje biometrijskog obrasca i generisanje ključa. Drugi segment obuhvata generisanje ključeva, na osnovu biometrijskog obrasca i novog, prikupljenog uzorka biometrijskog parametra. U okviru sistema postoje četiri tipa podataka [88], biometrija, na osnovu koje se generiše ili štiti ključ, biometrijski obrazac, u okviru koga se čuvaju podaci neophodni za ponovno generisanje ključa, kriptografski ključ, koji se koristi za šifrovanje i dešifrovanje podataka, i ostali podaci, koji se pojavljuju u procesu i na osnovu kojih se može ugroziti sigurnost ključa ili biometrije.

U praksi, sistem funkcioniše tako što se prvo prikuplja uzorak biometrijskog parametra, bilo za potrebe registracije bilo za potrebe regenerisanja ključa. Zatim, vrši se obrada uzorka biometrije, primenom različitih tehnika i filtera, kako bi se jasno istakli karakteristični detalji, koji se onda odgovarajućim algoritmima izdvajaju, transformišu i grupišu kako bi se formirao biometrijski obrazac. Nad tim biometrijskih obrascem se takođe primenjuju algoritmi i specifične tehnike, kako bi se dobio niz podataka koji služi kao ključ ili kao osnova za generisanje istog. Dobijeni kriptografski ključ se zatim koristi za šifrovanje ili dešifrovanje, a po potrebi se regeneriše.

Kod generisanja ključeva na osnovu biometrijskih parametara, treba imati u vidu sledeće kriterijume, i težiti ka što većem stepenu njihovog ispunjavanja [88]:

- Slučajnost ključa – da se na osnovu obrasca i raspoloživih ostalih podataka ne može doći do bilo kakvih podataka o ključu, odnosno da ključ mora da izgleda kao slučajan podatak.
- Slaba biometrijska privatnost - da se na osnovu obrasca i raspoloživih ostalih podataka ne može doći do bilo kakvih podataka o korišćenom biometrijskom parametru. odnosno da se ne može rekonstruisati bilo koji segment originalne biometrije.
- Jaka biometrijska privatnost – da se na osnovu obrasca, ostalih podataka i samog ključa, ne može doći do bilo kakvih korisnih podataka.

Imajući u vidu navedene karakteristike, primena biometrijskih parametara za potrebe generisanja ključeva je jedna od mogućnosti, koja može biti izabrana za realizaciju, ukoliko se pri analizi i formiranju celokupnog sistema, dođe do zaključka da pomenute prednosti imaju veću korisnost i efekat u odnosu na nedostatke.U zavisnosti od otvorenosti sistema, definisanih ciljeva zaštite, nivoa interakcije kao i drugih mehanizama bezbednosti, te negativne strane dolaze manje ili više do izražaja, i one zahtevaju dalje razmatranje i razvijanje adekvatnih tehnika kojima će se umanjiti njihov uticaj.

10.3 Otisak prsta

Korišćenje otisaka prstiju za generisanje kriptografskih ključeva podrazumeva njihovo prikupljanje uz pomoć senzora (optički, kapacitativni,termalni i dr.), posle čega se obično vrši segmentacija, odnosno izdvajanje regiona otiska sa slike, da bi zatim usledila primena odgovarajućih filtera i transformacija, pri čemu se u određenim slučajevima sprovode i dodatne operacije, a kako bi se istakli karakteristični detalji koji se onda izdvajaju, grupišu i transformišu, i koriste za potrebe generisanja kriptografskih ključeva. U zavisnosti od sistema, u određenim slučajevima se na osnovu njih formira i biometrijski obrazac, kao deo tog procesa. Za generisanje ključeva se uglavnom koriste podaci o minucijama, pre svega njihove koordinate, ali određena rešenje inkorporiraju u određenoj meri i druge karakteristike. Takođe, kako bi se obezbedila mogućnost regeneracije ključeva, i obezbedilo funkcionisanje usled difuznosti biometrijskih uzoraka, u nekim slučajevima se vrši i implementacija kodova za korekciju grešaka.



Slika 21: Minucije na otisku prsta[21]

[21] Izvor slike: http://biometrics.sabanciuniv.edu/privacy.html (pristup 10.04.2014)

Zbog svoje jedinstvenosti i trajnosti, pogodnosti za prikupljanje i prirodnosti korišćenja, otisci prstiju predstavljaju jedan od najrasprostranjenih i najviše korišćenih biometrijskih parametara, tako da postoji veliki broj predloženih rešenja za njihovu primenu za potrebe generisanja kriptografskih ključeva. Nedostatak se ogleda u određenoj dozi ranjivosti, zbog postojanja različitih napada na ovaj sistem, ukoliko se ne implementiraju adekvatni mehanizmi zašite, što može da ugrozi i generisane ključeve.

Primer korišćenje ovog parametra imamo u radu [89], gde se predlaže metodologija generisanja nepovratnih kriptografskih ključeva na osnovu otkazivog biometrijskog obrasca otiska prsta. Prvo, vrši se izdvajanje minucija iz slike otiska prsta. Ova faza obuhvata segmentaciju, odnosno obradu slike tako da se izdvoji deo sa otiskom prsta, određivanje orijentacionog polja, koje pokazuje orijentaciju i smer kretanja papilarnih linija, obradu dobijene slike primenom filtera kako bi se jasnije istakli karakteristični detalji, i izdvajanje minucija primenom binarizacije i morfoloških operacija. Zatim, vrši se formiranje otkazivih biometrijskih obrazaca, tako što se izračunavaju, sortiraju i prikazuju udaljenosti između pojedinih karakterističnih tačaka. Na kraju, taj otkazivi biometrijski obrazac se deli na dva dela, koja se međusobno mešaju, da bi se na osnovu te kombinacije formirao vektor, i iz njega matrica, koja predstavlja osnovu za generisanje nepovratnog kriptografskog ključa.

Zatim, u radu [90], predlaže se korišćenje otkazivih biometrijskih obrazaca otisaka prsta za generisanje ključa. Sistem funkcioniše kroz tri faze, tako što se prvo vrši izdvajanje podataka o minucijama, zatim generisanje obezbeđene matrice karakteristika (Secured Feature Matrix) i na kraju generisanje ključa na osnovu te matrice. Izdvajanje minucija podrazumeva predhodnu obradu slike otiska prsta, koja uključuje tehnike izjednačavanja histograma i primene Gaborovih filtera, da bi se zatim primenile binarizacija i morfološke operacije, i na osnovu tako obrađenih podataka izdvojili podaci o minucijama. Zatim, generiše se obezbeđena matrica karakteristika, tako što se ti podaci (predstavljeni u vidu vektora) transformišu u vektor ključa, na osnovu koga se formira matrica koja se šifruje primenom AES algoritma. U poslednjoj fazi, generiše se kriptografski ključ dešifrovanjem obezbeđenje matrice karakteristika i transformacijom podataka, na osnovu kojih se formira finalni vektor ključa, koji je nepovratan.

U radu [91], predlaže se način generisanja privatnog ključa, primenom statističke konverzije na biometrijskom obrascu otiska prsta, a za potrebe digitalnog potpisivanja transakcija. Predloženi sistem se zasniva na korišćenju smart kartica na kojima se nalaze moduli za generisanje ključa i određeni podaci, dok se privatni ključ generiše po potrebi, prezentovanjem otiska prsta na uređaju. Biometrijski obrazac koji se koristi pri tome se formira tako što se više uzastopnih otisaka prstiju statistički analizira, kako bi se izračunao tzv. region autentifikacije, kome se dodeljuje tzv. ID vrednost. Inicijalno, ID vrednost se kombinuje sa nekim izabranim brojem, i nad tom kombinovanom vrednošću se primenjuje heš funkcija kako bi se dobio privatni ključ. Na osnovu privatnog ključa se izračunava javni ključ i sve to dostavlja sertifikacionom telu, koje verifikuje identitet korisnika i sastavlja digitalni sertifikat. Kada se ukaze potreba za potpisivanjem poruke privatnim ključem, otisak prsta ovlašćenog korisnika obezbeđuje povraćaj ID vrednosti koji se onda koristi za generisanje privatnog ključa i dalje potpisivanje.

U radu [92], iznosi se koncept sistema za generisanje ključeva na osnovu topoloških pokazatelja okruženja karakterističnih detalja otisaka prsta. Kod ovog sistema se takođe prvo vrši obrada slike otiska prsta, primena filtera, binarizacija, i izdvajanje minucija i smerova kretanja brazdi. Zatim se vrši detaljna analiza okruženja minucija, tako

što se povlači linija koja preseca smer kretanja brazdi i određuju tzv. topološki pokazatelji u neposrednom okruženju, koji imaju već dodeljene numeričke vrednosti. Na osnovu tih vrednosti se generiše preliminarni ključ, u okviru kojeg se nalazi i određeni procenat grešaka, tako da se nad njim primenjuje neki od kodova za ispravljanje grešaka kako bi se došlo do finalnog ključa. U zavisnosti od predhodno izabranih parametara moguće je generisanje ključeva različitih veličina.

U radu [93], predlaže se generisanje ključa na osnovu vektora dobijenih formiranjem isečaka koji obuhvataju oblast sa izdvojenim minucijama, pri čemu se za generisanje koriste udaljenosti između određene centralne tačke i izdvojenih minucija. Kod ovog sistema, prvo se vrši određivanje referentne tačke otiska prsta, koja definiše ceo koordinatni sistem tog otiska, i to na bazi simetričnosti. Potom, vrši se izdvajanje minucija, sa dodeljivanjem koordinata u okviru kojih se računa i udaljenost od referentne tačke. Po završetku toga, vrši se formiranje vektora na osnovu veličine oblasti isečaka i broja minucija u okviru te oblasti, a spajanjem tih podataka dobijamo vektore na osnovu kojih se generiše ključ.

10.4 Lice

Lice, kao biometrijski parametar, ima široku primenu, i takođe može da posluži kao izvor podataka za generisanje kriptografskih ključeva. Kao osnov za generisanje, služi slika lica ili 3D model, i kao i kod drugih sistema, prvo se vrše standardne operacije, kao što su izdvajanje regiona lica na slici, zatim primena odgovarajućih transformacija, filtera i algoritama, u zavisnosti od sistema, da bi se na kraju došlo do traženih karakterističnih detalja koji se onda takođe podvrgavaju određenim promenama kako bi se na osnovu njih došlo do konačnog ključa. Prednost ovog sistema se ogleda u lakoći korišćenja i prirodnosti, ali je istovremeno i relativno ranjiv na potencijalne napade i neovlašćeno prikupljanje, što dovodi u pitanje i primenljivost u kriptografske svrhe.

Primer korišćenja ovog sistema za potrebe generisanja ključeva imamo u radu [94], gde se predlaže koncept sistema koji funkcioniše kroz dve faze, faze izdvajanja karakterističnih detalja i formiranja tzv. FaceHash vrednosti i faze izvođenja kriptografskog ključa iz tih podataka. Prvo, vrši se obrada slike lica primenom vejvlet transformacija, da bi se zatim nad tim podacima primenila metoda diskretizacije u cilju izdvajanja karakterističnih detalja, koji su istaknuti kod jednog lica, a dosta se razlikuju kod drugih, i ta vrednost se naziva FaceHash. U drugoj fazi se vrši formiranje kriptografskog ključa, na osnovu šeme deljenja tajni, kombinovanjem FaceHash vrednosti i uskladištenih kriptografskih podataka.

U radu [95], predlaže se korišćenje transformacija na osnovu korisnika, u cilju generisanja kompaktnih i stabilnih vrednosti koje se mogu iskoristiti za generisanje kriptografskih ključeva veće dužine. Prvo, na osnovu slike lica individualnog korisnika, biraju se odgovarajuće transformacije (linearno diskriminantna analiza, GSMMS kriterijum) kako bi se došlo do karakterističnih detalja po kojima se razlikuju od drugih. Svaki od tih detalja, u zavisnosti od svoje prepoznatljivosti, dodaje par bita informacije u ukupan zbir koji se onda koristi za generisanje ključa. Taj proces generisanja podrazumeva određivanje granica za svaki detalj i segmentaciju u okviru tih granica, a sam ključ se formira na osnovu niza segmenata autentičnog regiona iz ukupnog fonda podataka.

Zatim, radu [96], predlaže se korišćenje 3D modela lica za potrebe generisanja ključeva pogodnih za primenu u AES algoritmu. Ovaj metod podrazumeva izdvajanje karakterističnih detalja na osnovu entropije, kombinovanje sa Rid Solomonovim kodovima za korekciju grešaka i dobijanje nizova podataka na osnovu odgovarajuće jednosmerne transformacije. Prvo, vrši se primena Radonovih i Furijeovih transformacija, u nizovima, kako bi se dobili podaci na osnovu kojih se kreiraju matrice, nad kojima se zatim vrši binarizacija, kako bi se podaci pretvorili u oblik pogodan za selekciju na osnovu njihove entropije, i odabrali odgovarajući bitovi za formiranje ključa (bio-key). Tako formiran ključ se dalje koristi u kriptografske svrhe.

10.5 Iris

Kao što smo već naveli, iris predstavlja obojeni deo ljudskog oka, koji se nalazi između beonjače i zenice, sa izuzetno kompleksnom strukturom. Ima visoku jedinstvenost, i pri tom je zaštićen od spoljnih uticaja tako da predstavljaja solidnu osnovu za generisanje kriptografskih ključeva. Pored toga, nije toliko osetljiv na različite napade, kao neki drugi parametri, što pozitivno utične i na kriptografske primene.

Kod korišćenja irisa, po prikupljanju uzorka, vrše se standardne operacije, kao što su segmentacija (izdvajanje oblasti irisa), normalizacija, i primena odgovarajućih filtera i transformacija da bi se došlo do jasno istaknutih karakterističnih detalja, koji se onda grupišu u odgovarajuće kodove ili vektore, koji opet predstavljaju osnovu za generisanje ključeva. I kod ovog parametra postoji mogućnost da se skladište biometrijski obrasci, i da se primenjuju kodovi za korekciju grešaka.

Primer korišćenja irisa nalazimo u radu [97], gde se predlaže korišćenje segmenata tzv. kodova irisa (IrisCodes) za formiranje kriptografskih ključeva dovoljne dužine, koji se mogu otkazivati i obnavljati, pri čemu se ne skladišti ni orginalni biometrijskih obrazac niti njegova šifrovana verzija. Prvo, vrši se utvrđivanje dela slike u kom se nalazi iris i njegovo izdvajanje, nakon čega sledi procesiranje i formiranje kodova irisa primenom metoda diskretizacije na blokovima podataka. U sledećem koraku vrši se analiza tih kodova i utvrđivanje karakterističnih i konstantnih detalja, koji služe kao osnova za generisanje ključa. Za potrebe funkcionisanja ovog sistema u bazi se skladište obrasci koji predstavljaju kombinaciju tzv. bit maski koje služe za povezivanje ključa sa konkretnim korisnikom i samog kriptografskog ključa spojenog sa kodom za korekciju grešaka.

Sledeći primer imamo u radu [98], gde se predlaže metodologija generisanja privatnog ključa korisnika za korišćenje u asimetričnim kriptografskim sistemima na osnovu irisa. Prvo, vrši se izdvajanje irisa (segmentacija) i normalizacija, da bi se zatim primenili Gaborovi filteri i izdvojili karakteristični detalji za formiranje koda irisa. Na bazi toga koda irisa kao i izabranih prostih brojeva generišu se javni i privatni (tajni) ključ, a na osnovu njih se zatim formira i digitalni sertifikat koji se dalje koristi.

Zatim, u radu [99], predlaže se generisanje kriptografskih ključeva na osnovu primene heš funkcija nad kombinovanim podacima formiranim na osnovu karakterističnih detalja irisa i kodova za korekciju grešaka. Prvo, vrši se procesiranje slike irisa i izdvajanje karakterističnih detalja primenom Gaborovih filtera, da bi se kreirao vektor karakterističnih detalja irisa. Sledeći korak je računanje Rid Solomonovih kodova za korekciju grešaka na bazi tog vektora, nakon čega sledi primena heš funkcije (npr. MD5) nad tim vektorom da

bi se generisao ključ, koji se onda koristi za šifrovanje poruke nekim algortimom (npr. AES). Rid Solomonovi kodovi se koriste u fazi dešifrovanja tako što se primene nad vektorom karakterističnih detalja uzorka, kako bi se dobila korigovana vrednost biometrijskog parametra nad kojom je moguće primeniti heš funkciju i na taj način ponovo doći do kriptografskog ključa.

10.6 Mrežnjača

Kao što je ranije navedeno, mrežnjača predstavlja unutrašnji deo ljudskog oka, sa unikatnom mrežom krvnih sudova, koja se razlikuje čak i između dva oka. Isto ima visoku jedinstvenost, i isto je zaštićena od spoljnih uticaja kao i iris tako da i ovaj parametar ima određene prednosti sa aspekta generisanja kriptografskih ključeva.Takođe, zbog svoje prirode, jako ga je teško neovlašćeno prikupiti i prezentovati, što pogoduje kriptografskim primenama.

Kada je mrežnjača u pitanju, za potrebe generisanja ključeva se koriste karakteristični detalji mreže krvnih sudova, odnosno tačke u kojima se oni račvaju ili završavaju. Nad slikom mrežnjače se primenjuje binarizacija, i odgovarajuće transformacije, kako bi se dobila jasno istaknuta mreža krvnih sudova i pomenutih detalja, da bi se onda njihove koordinate iskoristile kao osnova za generisanje kriptografskog ključa.

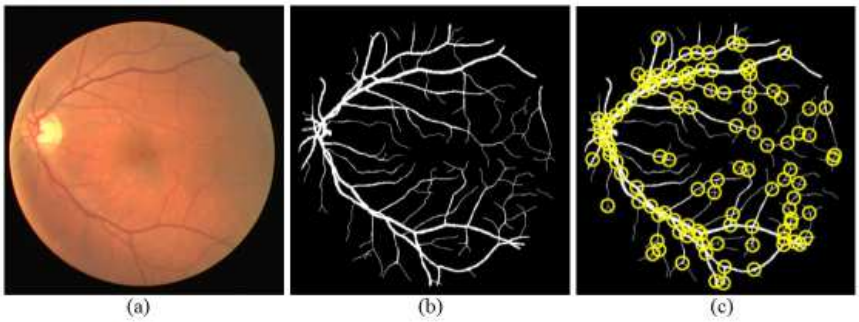


Figure 1: (a) Color retinal image. (b) Blood vessels segmentation. (c) Vascular bifurcation detection.

Slika 22: Mreža krvnih sudova i karakteristične tačke[22]

Primer ovog sistema imamo u radu [100], gde se predlaže se korišćenje mreže krvnih sudova u mrežnjači za potrebe generisanja ključeva. Kod ovog sistema prvo se nad slikom mrežnjače primenjuje binarizacija i tako dolazi do slike mreže krvnih sudova, od kojih se biraju glavni, jasno definisani krvni sudovi. Ta mreža krvnih sudova se onda proređuje, i jasno se utvrđuju tačke račvanja kao i tačke gde se pojedini krvni sudovi završavaju, i određuju se njihove koordinate. Te završne tačke, tj. njihove koordinate se zatim koriste za potrebe generisanja ključeva računanjem njihove sume po odgovarajućoj formuli, i pretvaranjem te sume u binarnu vrednost.

Sledeći primer imamo u radu [101], gde se isto na bazi mreže krvnih sudova mrežnjače generiše ključ. Slično kao i kod predhodnog sistema, polazi se od slike mrežnjače, nad kojom se vrši proređivanje i pridruživanje kako bi se jasno istakla mreža

[22] Izvor slike: http://www.cs.rug.nl/is/Research/Students (pristup 10.04.2014)

krvnih sudova, s tim što se kod ovog sistema za generisanje ključa koriste tačke račvanja krvnih sudova, tj. njihove koordinate. Ta formirana mreža krvnih sudova, sa određenim tačkama račvanja, se zatim podvrgava permutacijama i translacijama kako bi se obezbedili parametri za generisanje kriptografskog ključa.

10.7 Otisak dlana

Otisak dlana ima velike sličnosti sa otiskom prsta, čak je i kompleksniji i samim tim, pruža više potencijalnih mogućnosti za izvođenje odgovarajuće količine detalja, potrebnih za generisanje ključeva. Kod ovih sistema, polazi se od slike dlana, koja se mora normalizovati, da bi se otklonile razlike nastale usled ugla koji zauzima dlan pri prikupljanju uzorka i usled dimenzija slike, i da bi se dobila osnovna slika, iz koje se izdvaja tačno definisani segment, koji onda služi za određivanje karakterističnih detalja. Pored toga, ovi sistemi podrazumevaju i primenu heš funkcija i kodova za korekciju grešaka, kako bi se postigla funkcionalnost. Kao i kod otiska prsta, postoji mogućnost neovlašćenog prikupljanja i prezentovanja lažne biometrije, ali je to značajno teže za realizaciju, zbog veće kompleksnosti i prirode samog parametra.

Primer korišćenja ovog parametra nalazimo u radu [102], gde se na osnovu otiska dlana, primenom diferencijalnih operacija izdvaja binarni niz veličine 1024 bita, na osnovu koga se, primenom heš funkcije, generiše 128-bitni ključ ali i formira kod za korekciju grešaka. Pri fazi dešifrovanja ponovo se formira 1024 bitni niz, koji se ispravlja na osnovu tog koda za korekciju grešaka, da bi se zatim primenom heš funkcije ponovo generisao ključ.

Sledeći primer imamo u radu istih autora [103], gde se parametri formirani na bazi karakterističnih detalja otisaka dlana, tzv. DoG kodovi koriste u kriptografske svrhe. Kodovi se formiraju tako što se nad biometrijskim parametrima otiska dlana primenjuju Gausovi filteri, kako bi se formirala matrica koja predstavlja taj otisak. Zatim, vrši se kombinovanje tih vrednosti i Rid Solomonovih kodova za korekciju grešaka i logičkih XOR operacija za potrebe šifrovanja i dešifrovanja podataka.

10.8 Raspored krvnih sudova

Podkožna mreža krvnih sudova ruke ili prsta, slično kao i kod mrežnjače, može da se iskoristi za potrebe generisanja ključeva. Kao osnova za to se koriste ili konture vena, ili pak karakteristične tačke, odnosno račvanja i završeci vena, koje se dobijaju iz osnovne slike, primenom odgovarajućih transformacija, uz eventualnu implementaciju kodova za korekciju grešaka.

Primer korišćenja ovog parametra nalazimo u radu [104], gde se predlaže tehnika za generisanje neopozivog kriptografskog ključa na bazi biometrijskog obrasca a u cilju autentifikacije smart kartice. Kao osnovni parametar za generisanje tog ključa koristi se raspored vena dlana, tj. karakteristični detalji tog rasporeda, u vidu račvanja i završnih tački.

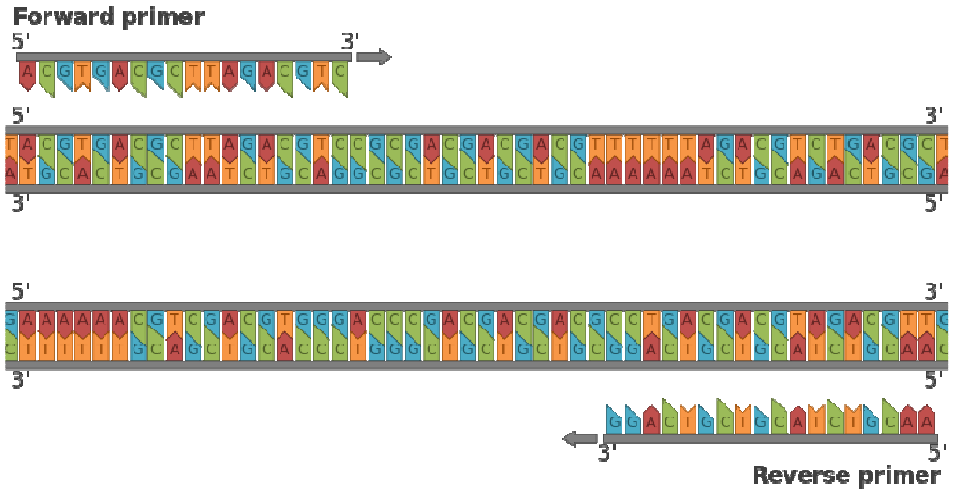
Zatim, u radu [105], predlaže se korišćenje rasporeda vena prstiju za generisanje ključeva. Kao osnov za formiranje ključa služi raspored vena više prstiju, pri čemu

promena njihovog redosleda pri obradi omogućeva generisanje novih ključeva. Prikupljeni podaci se obrađuju primenom morfoloških funkcija, a nad tako obrađenim podacima se zatim primenjuje algoritam za praćenje kontura koji generiše delimične ključeve. Takvi ključevi se zatim kombinuju sa kodovima za korekciju grešaka, kako bi se obezbedilo funkcionisanje i pored varijabilnosti biometrijskih podatka, a zatim se vrši spajanje više delimičnih ključeva u finalni kriptografski ključ, koji se zatim normalizuje.

10.9 DNK

Kao što smo već naveli, DNK predstavlja skup genetskih instrukcija kojima se određuje razvoj i funkcionisanje nekog živog organizma. Zbog svoje izuzetno kompleksne strukture, i mogućnosti obuhvatanja velike količine informacija, ovaj biometrijski parametar je predmet izuzetno obimnih istraživanja, i na osnovu njega je formirana čitava podoblast kriptografije, nazvana DNK kriptografija [106].

U okviru tih istraživanja se razmatraju različite metodologije kombinovanja kriptografije i kompleksnih DNK parametara, pri čemu se obuhvata i formiranje ključeva. Nedostatak ovog metoda se ogleda u teškoći prikupljanja, jer zahteva specijalizovane uređaje i visok nivo stručnosti, a pri tom, loša realizacija bi potencijalno mogla da ugrozi vitalne i nepromenljive podatke, koji uz to sadrže i dosta privatnih informacija o korisniku.



Slika 23: DNK segmenti[23]

U vezi sa tim, u radu [107], predlaže se metodologija šifrovanja podataka na osnovu strukture DNK uopšte. Kao jedan od segmenata, predlaže se formiranje ključa za šifrovanje na osnovu para PCR (Polymerase Chain Reaction) segmenata i javnog ključa, dok se ključ za dešifrovanje formira na osnovu tih PCR segmenata i privatnog ključa.

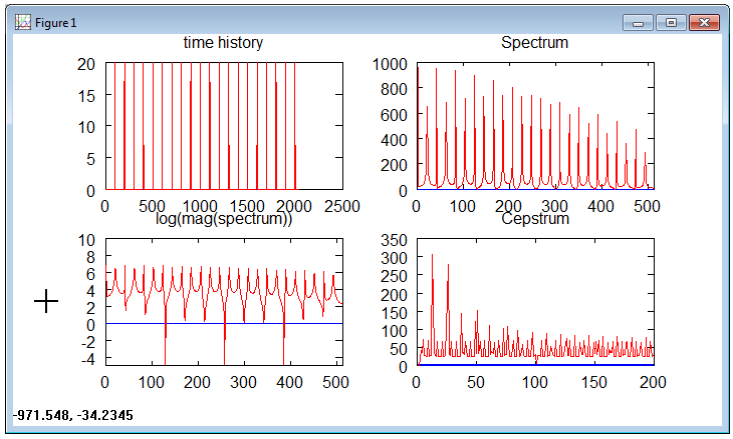
Zatim, u radu [108], predlaže se formiranje simetričnog kriptografskog algoritma baziranog na DNK strukturi, pri čemu se ključevi za šifrovanje i dešifrovanje generišu na osnovu DNK sondi (malih segmenata DNK), a sam šifrat se skladišti u specijalno dizajniranom DNK čipu, koji se formira pri šifrovanju. Dešifrovanje se vrši na osnovu

[23] Izvor slike: http://en.wikipedia.org/wiki/Primer_(molecular_biology) (pristup 10.04.2014)

DNK hibridizacije, tj. na osnovu tehnike merenja sličnosti između segmenata DNK podataka.

10.10 Glas

Glas, kao biometrijski parametar, ima dosta kompleksnu strukturu, i stoga ima potencijal za primenu u svrhe generisanja ključeva. Kao i kod prepoznavanja, sisteme možemo podeliti na one koji koriste određenu, tačno izgovorenu rečenicu (tekst zavisni) i na one koji koriste karakteristike glasa uopšte (tekst nezavisne). Po uzimanju uzorka, on se obrađuje i izdvajaju se karakteristični detalji za dalje generisanje ključa. Jedan od bitnih nedostataka primene ovog parametra za potrebe generisanja ključeva je i njegova ranjivost na neovlašćeno prikupljanje, što može negativno da utiče na bezbednost celog procesa.



Slika 24: Kepstrum[24]

Primer korišćenja ovog sistema nalazimo u radu [109], gde se razmatra tehnika generisanja kriptografskog ključa na osnovu glasa korisnika dok izgovara odgovarajuću lozinku. Prvo, prikupljaju se uzorci glasa, koji se zatim dele na sekcije, na osnovu kojih se određuje odgovarajući sklop kepstruma. Niz tih sklopova se zatim koristi za kreiranje opisne funkcije, na osnovu koje se sastavlja indeksna tabela, koja opet predstavlja osnovu za generisanje tzv. izvedenog ključa.

Zatim, u radu [110], predlaže se generisanje ključeva na bazi glasa korisnika primenom metode slučajnih biometrijskih obrazaca. Ovaj metod podrazumeva prikupljanje uzoraka glasa, izdvajanje karakterističnih detalja tih uzoraka, primenom PLP i delta analize, kako bi se došlo do vektorskih vrednosti, na osnovu kojih se određuju koordinate, čijom segmentacijom se dolazi do niza karakterističnih detalja na osnovu kojih se generiše kriptografski ključ i biometrijski obrazac.

[24] Izvor slike: http://en.wikipedia.org/wiki/Cepstrum (pristup 10.04.2014)

10.11 Potpis

Kod primene potpisa, kao osnov za generisanje ključa mogu da budu iskorišćeni statički (oblik, specifični detalji) i/ili dinamički elementi (pritisak, pravac kretanja, ubrzanje). U zavisnosti od toga, uzorak potpisa može da bude predstavljen slikom, npr. kada se radi o statičkim sistemima, a može da zahteva i specijalizovane uređaje za prikupljanje uzorka potpisa. Potpis je, kao biometrijski parametar, kompleksan i relativno jedinstven, i, u slučaju dinamičkih sistema, teško ga je neovlašćeno prikupiti, što ide u prilog bezbednosti celog procesa.

Primer nalazimo u radu [111], gde se predlaže tehnika generisanja privatnog ključa na osnovu dinamičkog potpisa. Prvo, vrši se poređenje potpisa sa obrascem u bazi, u cilju sprečavanja falsifikovanja, zatim se vrši izdvajanje karakterističnih detalja, i svakom se dodeljuje određena decimalna vrednost, a te vrednosti se na kraju sjedinjuju u jedinstven niz. Taj niz predstavlja osnovu za generisanje privatnog ključa, koji dobijamo primenom SHA1 heš funkcije nad tim nizom, a zatim na osnovu privatnog računamo i javni ključ.

Zatim, u radu [112], predlaže se korišćenje pseudo potpisa, tj. rukom crtanih grafičkih formi i dinamičkih informacija njihovog kreiranja, za potrebe generisanja ključeva. Kako bi se obezbedila sličnost između inicijalnog unosa i naknadno prikupljenog uzorka, predlaže se prezentovanje niza vizuelnih simbola koji predstavljaju osnov za asocijaciju i pamćenje potrebnih formi. Za potrebe generisanja ključa sistem koristi informacije o formama, kao i dinamičke parametre (početne tačke, smerovi, brzina) pisanja, nad kojima se primenjuju kodovi za ispravljanje grešaka i heš funkcije.

10.12 Multibiometrijski sistemi

Kada su u pitanju multibiometrijski sistemi, njihove funkcionalne prednosti u odnosu na individualne sisteme, dolaze do izražaja i kod korišćenja u svrhe generisanja kriptografskih ključeva. Formiranjem multibiometrijskih sistema, mogu se implementirati već pomenute kombinacije, odnosno više senzora, algoritama, primera, uzoraka ili različitih biometrijskih parametara i na taj način izuzetno povećati kompleksnost i uopšte nivo funkcionisanja sistema, što opet ima veliki uticaj i na kriptografske primene. Mogućnosti za kombinovanje su velike, a samim tim se povećava i opseg ključeva koji se može generisati bez primene nekih pomoćnih podataka, kao i pouzdanost i preciznost regeneracije ključeva, usled prisustva velikog broja faktora za poređenje.Takođe, umanjuje se mogućnost negativnog uticaja na sistem usled neovlašćenog pristupa ili prikupljanja, i značajno uvećava fond raspoloživih podataka koji potencijalni napadač mora da uzme u obzir, pri kriptoanalizi dostupnih podataka.

Primer korišćenja ovakvog sistema nalazimo u radu [113], gde se predlaže generisanje ključeva na osnovu kombinovanog sistema zasnovanog na otisku prsta i irisu. Prvo, vrši se izdvajanje karakterističnih detalja i otiska prsta i irisa, koji se zatim spajaju u jednu celinu, tj. multibiometrijski obrazac, na osnovu koga se zatim generiše 256-bitni AES ključ. Kod otisaka prstiju, prvo se vrši preliminarno procesiranje, zatim segmentacija, određivanje orijentacije i poboljšavanje kvaliteta slike, i na kraju se izdvajaju karakteristični detalji (minucije). Kod slike irisa, vrši se segmentacija, normalizacija i izdvajanje teksture irisa. Sledeći korak predstavlja spajanje tih izdvojenih podataka,

predstavljenih u vidu vektora, tako što se individualni vektori mešaju, pa se vrši njihovo povezivanje, da bi finalni korak bio njihovo spajanje u multibiometrijski obrazac, predstavljen određenim decimalnim vrednostima. Te vrednosti se takođe predstavljaju u vidu vektora, a njihovom selekcijom se dobija niz podataka, koji se zatim transformiše u kriptografski ključ.

Sledeći primer imamo u radu [114], gde se iznosi koncept biometrijskog kriptosistema koji obuhvata karakteristike lica, otiska prsta i rasporeda vena. Kod ovog sistema, prvo se vrši izdvajanje karakterističnih detalja kod otiska prsta i slike lica i formiraju se vektori kojima se ti podaci predstavljaju. Zatim, izdvajaju se karakteristični detalji rasporeda vena i formira obrazac, koji se deli na dva dela, a zatim se matematičkim operacijama podaci iz delova međusobno mešaju da bi se na kraju formirala matrica iz koje se izdvaja neopozivi kriptografski ključ. Dalje funkcionisanje ovog sistema podrazumeva upotrebu tog ključa za šifrovanje vektora podataka otiska prsta, i kodovanje tog šifrovanog niza u sliku lica, primenom steganografskih metoda.

Zatim, u radu [115], predlaže se korišćenje multibiometrijskog sistema koji integriše otisak prsta, lice, iris i potpis, i na osnovu kojih generiše eliptičnu krivu i ključ primenom specifične metodologije šifrovanja, tzv. kriptografije eliptične krive. Pomenuti biometrijski parametri, tj. njihove slike, se spajaju u jednu sliku, a zatim se na osnovu karakterističnih detalja te slike formira matrica vrednosti. Na osnovu te matrice vrednosti, i uz primenu genetskog algoritma i matematičkih formula, formira se eliptična kriva i ključ. Eliptična kriva se zatim integriše sa formiranom spojenom slikom, određuju se karakteristični detalji te kombinacije, nad kojima se primenjuje predhodno generisani ključ i na osnovu toga dolazimo do lozinke za jednokratnu upotrebu, koja se dalje koristi u bezbednosne svrhe.

11. Zaključak

Savremeni biometrijski sistemi predstavljaju tehnologiju koja ima veliki potencijal za primenu u bezbednosnim sistemima, obezbeđujući visok nivo bezbednosti uz relativnu jednostavnost korišćenja. Budući da funkcionišu na bazi onoga što čovek jeste, oni pojednostavljuju čitav spektar procesa u bezbednosnim oblastima, što direktno utiče na povećanje efikasnosti, povećanje brzine i smanjenje troškova funkcionisanja. Pri tom, zbog svoje kompleksnosti, omogućavaju implementaciju složenijih bezbednosnih sistema nego što bi to bilo moguće sa nekim nebiometrijskim alternativama. Uzevši u obzir da funkcionisanje savremenog društva i poslovnih procesa, podrazumeva sve obimnije i kompleksnije tokove informacija, i sve veće bezbednosne zahteve, biometrijski sistemi se nameću kao logično rešenje.

Sa druge strane, biometrijski sistemi imaju i velike nedostatke. Pre svega, svoje funkcionisanje zasnivaju na nepromenljivim fiziološkim karakteristikama i obrascima ponašanja, što otvara čitav niz pitanja, vezanih za uticaj na privatnost, religijska uverenja, bezbednost njihovog korišćenja i sl. i time znatno utiče na njihovo prihvatanje od strane korisnika, zahtevajući adekvatan razvoj društvene svesti i zakonske regulative kako bi se našli zadovoljavajući odgovori.Zatim, biometrijski parametri su, uglavnom, zbog svoje prirode, osetljivi na neovlašćeno prikupljanje, što predstavlja ozbiljan nedostatak za koji je izuzetno teško naći adekvatno rešenje, i koji se mora imati u vidu prilikom formiranja sistema. Pored toga, suočavaju se sa brojnim funkcionalnim problemima, usled teškoća obezbeđivanja pouzdanog i preciznog funkcionisanja na osnovu difuznih biometrijskih parametara, i zahtevaju adekvatna tehnička i organizaciona rešenja kako bi se formirali sistemi sa odgovarajućim karakteristikama. Kao moguća rešenja ovog problema, uz razvoj novih tehnika i tehnologija, javljaju se multibiometrijski sistemi, ili sistemi koji integrišu još neki vid utvrđivanja ili potvrđivanja identiteta, što opet uslovljava kompleksnije funkcionisanje, i zahteva veće investicije u sisteme.

Bezbednost funkcionisanja biometrijskih sistema je isto veliki problem za koji je potrebno naći odgovarajuća rešenja. Imajući u vidu jedinstvenost i nepromenljivost fizioloških karakteristika i obrazaca ponašanja, ugrožavanje bezbednosti podataka o njima bi moglo da prouzrokuje trajne i nesagledive posledice. Primena biometrijskih sistema, bez neophodnih mera zaštite, otvara vrata za narušavanje bezbednosti, različite zloupotrebe i ugrožavanja privatnosti, bez mogućnosti da se izgubljeni podaci nekako promene ili stave van upotrebe.

Kako bi se ta bezbednost osigurala, potrebno je implementirati niz zaštitnih mehanizama u cilju obezbeđivanja ulaznih tačaka sistema, linija komunikacija neophodnih za funkcionisanje i samih podataka koji se skladište. Korišćenje klasičnih kriptografskih algoritama omogućava postizanje bezbednog funkcionisanja određenih delova, ali ne i sistema u celosti, tako da se javlja potreba kombinovanja i implementacije specifičnih rešenja u pojedinim segmentima, a kako bi se osiguralo optimalno funkcionisanje sistema na zadovoljavajućem nivou bezbednosti. To podrazumeva primenu specifičnih softverskih i hardverskih rešenja, organizacionih tehnika, korišćenja naprednih kriptografskih algoritama, biometrijskih kriptosistema i sistema zasnovanih na transformacijama, kao i steganografskih i drugih tehnika. Primena navednih metoda omogućava podizanje bezbednosti biometrijskih sistema na adekvatan nivo, sa tendencijom daljeg poboljšanja, uzevši u obzir da su biometrijski sistemi trenutno aktuelno polje istraživanja i razvoja, tako da se može očekivati i dalji napredak u oblasti njihove bezbednosti.

Slična situacija se javlja i kod primene biometrijskih parametara za potrebe generisanja kriptografskih ključeva. Zbog svoje kompleksnosti, i činjenice da su neodvojivi deo ličnosti, biometrijski parametri se izdvajaju kao potencijalno rešenje. Njihova kompleksna struktura, u kombinaciji sa odgovarajućim algoritmima, obezbeđuje dovoljnu količinu podataka za potrebe generisanja ključeva, i time obezbeđuje jedan od preduslova za uspešno rešavanje pomenutog problema. Zatim, dolazi do izražaja i to što su biometrijskih parametri neodvojivi deo ličnosti, pa ih samim tim nije moguće zaboraviti, ili pak preneti na neku drugu, neovlašćenu ličnost, a takođe obezbeđuju i neporecivost, što su značajne prednosti sa aspekta generisanja i daljeg funkcionisanja tih ključeva.S druge strane, javlja se i pitanje njihovih nedostataka. Pre svega, njihova nepromenljivost se javlja kao izuzetno bitan faktor, jer sama po sebi ograničava opseg mogućnosti generisanja ključeva, a i zahteva komplikovane modalitete zaštite koji se moraju inkorporirati u algoritam, kako bi se onemogućilo da se na osnovu ključa dođe do originalnog biometrijskog podatka. Zatim, činjenica da su podložni neovlašćenom prikupljanju, može značajno da utiče na bezbednosne aspekte njihove primene u svrhe generisanja ključeva. Pored toga, njihova kompleksna struktura, u kombinaciji sa određenom dozom difuznosti koja je inherentna kod biometrijskih parametara, predstavlja i problem, zbog razlika koje se javljaju kod svakog prikupljanja uzoraka, i koje se moraju uzeti u obzir pri kreiranju algoritama.

Imajući u vidu sve navedeno, može se doći do zaključka da primena biometrijskih parametara u cilju generisanja kriptografskih ključeva ima određeni potencijal i niz prednosti, ali takođe i niz nedostataka, i takvo stanje zahteva još istraživanja, razvoja i tehnološkog napretka kako bi se došlo do funkcionalnih modela koji u potpunosti zadovoljavaju profesionalne zahteve sa kojima se suočavaju.

Literatura

[1] Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). Biometrics: Identity assurance in the information age. New York: McGraw-Hill/Osborne

[2] Jain, A. K., Bolle, R., & Pankanti, S. (Eds.). (1999). Biometrics: personal identification in networked society. Springer.

[3] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

[4] Veinović M., Adamović S. (2013). Kriptologija I: Osnove za analizu i sintezu šifarskih sistema, Univerzitet Singidunum, Beograd.

[5] Zhao, Y. (2003). Dual domain semi-fragile watermarking for image authentication (Doctoral dissertation, University of Toronto).

[6] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions on, 14(1), 4-20.

[7] Jain, A. K., Flynn, P., & Ross, A. A. (2007). Handbook of biometrics. Springer.

[8] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy, 1(2), 33-42.

[9] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer.

[10] Jang, J., & Kim, H. (2009). Performance Measures. In Encyclopedia of Biometrics (pp. 1062-1068). Springer US.

[11] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer.

[12] Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (2005). Biometric systems: technology, design and performance evaluation. Springer.

[13] Sim, T. M. (2009). Privacy Issues. Encyclopedia of Biometrics, 1092-1098.

[14] Campisi, P. (2013). Security and Privacy in Biometrics: Towards a Holistic Approach. In Security and Privacy in Biometrics (pp. 1-23). Springer London.

[15] International Biometric Group, BioPrivacy Initiative, Identifying and Reducing Privacy Risks in Biometric System, http://www.bioprivacy.org/CFP_2003.pdf (pristup 03.05.2014.)

[16] Rathgeb, C., Uhl, A., & Wild, P. (2012). Iris biometrics: from segmentation to template security (Vol. 59). Springer.

[17] Hill, R. B. (2002). Retina identification. Biometrics: Personal Identification in Networked Society, 123-141.

[18] Ortega, M., Rouco, J., & Barreira, N. (2009). Retinal verification using a feature points-based biometric pattern. EURASIP Journal on Advances in Signal Processing, 2009.

[19] Ross, A., & Jain, A. K. (1999, March). A prototype hand geometry-based verification system. In Proceedings of 2nd Conference on Audio and Video Based Biometric Person Authentication (pp. 166-171).

[20] Li, H., & Toh, K. A. (2012). Advanced Topics in Biometrics. L. Li (Ed.). World Scientific.

[21] Bača, M., Grd, P., & Fotak, T. (2012). Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics.

[22] Zhang, D. D. (2004). Palmprint authentication (Vol. 3). Springer.

[23] Zhang, D., Zuo, W., & Yue, F. (2012). A comparative study of palmprint recognition algorithms. ACM Computing Surveys (CSUR), 44(1), 2.

[24] Watanabe, M. (2008). Palm vein authentication. In Advances in Biometrics (pp. 75-88). Springer London.

[25] Choi, A. H., & Tran, C. N. (2008). Hand vascular pattern technology. In Handbook of biometrics (pp. 253-270). Springer US.

[26] Abaza, A., Ross, A., Hebert, C., Harrison, M. A. F., & Nixon, M. S. (2013). A survey on ear biometrics. ACM Computing Surveys (CSUR), 45(2), 22.

[27] Beigi, H. (2011). Fundamentals of speaker recognition. Springer.

[28] Fierrez, J., & Ortega-Garcia, J. (2008). On-line signature verification. In Handbook of biometrics (pp. 189-209). Springer US.

[29] Ilonen, J. (2003). Keystroke dynamics. Advanced Topics in Information Processing–Lecture, 03-04.

[30] Sarkar, S., & Liu, Z. (2008). Gait recognition. In Handbook of biometrics (pp. 109-129). Springer US.

[31] Korotkaya, Z. (2003). Biometric person authentication: Odor. Inner report in Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology. in "Advanced Topics in Information Processing: Biometric Person Authentication.

[32] Schomaker, L. (2007, September). Advances in writer identification and verification. In Document Analysis and Recognition, 2007. ICDAR 2007. Ninth International Conference on (Vol. 2, pp. 1268-1273). IEEE.

[33] Schlapbach, A., & Bunke, H. (2004, October). Using HMM based recognizers for writer identification and verification. In Frontiers in Handwriting Recognition, 2004. IWFHR-9 2004. Ninth International Workshop on (pp. 167-172). IEEE.

[34] Cetingul, H. E., Yemez, Y., Erzin, E., & Tekalp, A. M. (2005, March). Robust lip-motion features for speaker identification. In Proc. of ICASSP (pp. 72-77).

[35] Faraj, M. I., & Bigun, J. (2006, June). Person verification by lip-motion. In Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on (pp. 37-37). IEEE.

[36] Silva, H., Lourenço, A., Canento, F., Fred, A., & Raposo, N. (2013). ECG biometrics: Principles and applications. In Proc. of the 6th BIOSIGNALS Conf.

[37] Ye, C., Coimbra, M. T., & Kumar, B. V. (2010, September). Investigation of human identification using two-lead electrocardiogram (ECG) signals. In

Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on (pp. 1-8). IEEE.

[38] Campisi, P., La Rocca, D., & Scarano, G. (2012). EEG for Automatic Person Recognition. Computer, 45(7), 87-89.

[39] Khalifa, W., Salem, A., Roushdy, M., & Revett, K. (2012, May). A survey of EEG based user authentication schemes. In Informatics and Systems (INFOS), 2012 8th International Conference on (pp. BIO-55). IEEE.

[40] Barbosa, I. B., Theoharis, T., Schellewald, C., & Athwal, C. (2013, September). Transient biometrics using finger nails. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on (pp. 1-6). IEEE.

[41] Garg, S., Kumar, A., & Hanmandlu, M. (2012, November). Biometric authentication using finger nail surface. In Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on (pp. 497-502). IEEE.

[42] Veldhuis, R. N., Bazen, A. M., Kauffman, J. A., & Hartel, P. (2004, June). Biometric verification based on grip-pattern recognition. In Electronic Imaging 2004 (pp. 634-641). International Society for Optics and Photonics.

[43] Jorgensen, Z., & Yu, T. (2011, March). On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 476-482). ACM.

[44] Ahmed, A. A. E., & Traore, I. (2007). A new biometric technology based on mouse dynamics. Dependable and Secure Computing, IEEE Transactions on, 4(3), 165-179.

[45] Jain, A. K., Dass, S. C., & Nandakumar, K. (2004). Soft biometric traits for personal recognition systems. In Biometric Authentication (pp. 731-738). Springer Berlin Heidelberg.

[46] Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). Handbook of multibiometrics (Vol. 6). Springer.

[47] Breebaart, J., Yang, B., Buhan-Dulman, I., & Busch, C. (2009). Biometric template protection. Datenschutz und Datensicherheit-DuD, 33(5), 299-304.

[48] Prabhakar, S., Maltoni, D., Maio, D., & Jain, A. K. (2003). Handbook of fingerprint recognition, Springer.

[49] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001, January). An analysis of minutiae matching strength. In Audio-and Video-Based Biometric Person Authentication (pp. 223-228). Springer Berlin Heidelberg.

[50] Roberts, C. (2007). Biometric attack vectors and defences. Computers & Security, 26(1), 14-25.

[51] Jain, A. K., & Uludag, U. (2003). Hiding biometric data. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(11), 1494-1498.

[52] Pötzelsberger, G., & Eng, B. (2013). KV Web Security: Applications of Homomorphic Encryption. http://www.fim.uni-linz.ac.at/Lva/Web_Security/Abgaben/Poetzelsberger-Homomorphic.pdf (pristup 01.05.2014)

[53] Luo, Y., Cheung, S. C. S., & Ye, S. (2009, June). Anonymous biometric access control based on homomorphic encryption. In Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on (pp. 1046-1049). IEEE.

[54] Upmanyu, M., Namboodiri, A. M., Srinathan, K., & Jawahar, C. V. (2009). Efficient biometric verification in encrypted domain. In Advances in Biometrics (pp. 899-908). Springer Berlin Heidelberg.

[55] Fujitsu Develops World's First Homomorphic Encryption Technology that Enables Statistical Calculations and Biometric Authentication, http://www.fujitsu.com/global/news/pr/archives/month/2013/20130828-01.html (pristup 06.02.2014.)

[56] Pang, C. T., Yun, Y. W., & Jiang, X. (2009). On-Card Matching. In Encyclopedia of Biometrics (pp. 1014-1021). Springer US.

[57] Khan, M. K., Xie, L., & Zhang, J. (2007). Robust hiding of fingerprint-biometric data into audio signals. In Advances in Biometrics (pp. 702-712). Springer Berlin Heidelberg.

[58] Na, W., Chiya, Z., Xia, L., & Yunjin, W. (2010, June). Enhancing Iris-feature Security with steganography. In Industrial Electronics and Applications (ICIEA), 2010 the 5th IEEE Conference on (pp. 2233-2237). IEEE.

[59] Yeung, M. M., & Pankanti, S. (2000). Verification watermarks on fingerprint recognition and retrieval. Journal of Electronic Imaging, 9(4), 468-476.

[60] Bhatnagar, G., Jonathan Wu, Q. M., & Raman, B. (2010). Biometric Template Security based on Watermarking. Procedia Computer Science, 2, 227-235.

[61] Gunsel, B., Uludag, U., & Murat Tekalp, A. (2002). Robust watermarking of fingerprint images. Pattern Recognition, 35(12), 2739-2747.

[62] Ross, A., & Othman, A. (2011). Visual cryptography for biometric privacy. IEEE transactions on information forensics and security, 6(1), 70-81.

[63] James, D., & Philip, M. (2012). A Novel Security Architecture for Biometric Templates Using Visual Cryptography and Chaotic Image Encryption. In Eco-friendly Computing and Communication Systems (pp. 239-246). Springer Berlin Heidelberg.

[64] Rao, Y. S., Sukonkina, Y., Bhagwati, C., & Singh, U. K. (2008, November). Fingerprint based authentication application using visual cryptography methods (improved id card). In TENCON 2008-2008 IEEE Region 10 Conference (pp. 1-5). IEEE.

[65] Revenkar, P. S., Anjum, A., & Gandhare, W. Z. (2010). Secure iris authentication using visual cryptography. arXiv preprint arXiv:1004.1748.

[66] Anil K, J., Karthik, N., & Abhishek, N. (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008.

[67] Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 37(11), 2245-2255.

[68] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. Information Processing Letters, 93(1), 1-5.

[69] Savvides, M., Kumar, B. V., & Khosla, P. K. (2004, August). Cancelable biometric filters for face recognition. In Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on (Vol. 3, pp. 922-925). IEEE.

[70] Zuo, J., Ratha, N. K., & Connell, J. H. (2008, December). Cancelable iris biometric. In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on (pp. 1-4). IEEE.

[71] Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating cancelable fingerprint templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), 561-572.

[72] Sutcu, Y., Sencar, H. T., & Memon, N. (2005, August). A secure biometric authentication scheme based on robust hashing. In Proceedings of the 7th workshop on Multimedia and security (pp. 111-116). ACM.

[73] Tulyakov, S., Farooq, F., & Govindaraju, V. (2005). Symmetric hash functions for fingerprint minutiae. In Pattern Recognition and Image Analysis (pp. 30-38). Springer Berlin Heidelberg.

[74] Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., & Neri, A. (2010). Cancelable templates for sequence-based biometrics with application to on-line signature recognition. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 40(3), 525-538.

[75] Cavoukian, A., & Stoianov, A. (2009). Encryption, Biometric. In Encyclopedia of Biometrics (pp. 260-269). Springer US.

[76] Juels, A., & Wattenberg, M. (1999, November). A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security (pp. 28-36). ACM.

[77] Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2), 237-257.

[78] Linnartz, J. P., & Tuyls, P. (2003, January). New shielding functions to enhance privacy and prevent misuse of biometric templates. In Audio-and Video-Based Biometric Person Authentication (pp. 393-402). Springer Berlin Heidelberg.

[79] Dodis, Y., Reyzin, L., & Smith, A. (2004, January). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Advances in cryptology-Eurocrypt 2004 (pp. 523-540). Springer Berlin Heidelberg.

[80] Arakala, A., Jeffers, J., & Horadam, K. J. (2007). Fuzzy extractors for minutiae-based fingerprint authentication. In Advances in Biometrics (pp. 760-769). Springer Berlin Heidelberg.

[81] Li, Q., Guo, M., & Chang, E. C. (2008, June). Fuzzy extractors for asymmetric biometric representations. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on (pp. 1-6). IEEE.

[82] Buhan, I., Doumen, J., Hartel, P., & Veldhuis, R. (2007, March). Fuzzy extractors for continuous distributions. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 353-355). ACM.

[83] Sutcu, Y., Li, Q., & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. Information Forensics and Security, IEEE Transactions on, 2(3), 503-512.

[84] Feng, Y. C., Yuen, P. C., & Jain, A. K. (2010). A hybrid approach for generating secure and discriminating face template. Information Forensics and Security, IEEE Transactions on, 5(1), 103-117.

[85] Chen, H., & Chen, H. (2010). A hybrid scheme for securing fingerprint templates. International Journal of Information Security, 9(5), 353-361.

[86] Prasanalakshmi, B., & Kannammal, A. (2009, November). A secure cryptosystem from palm vein biometrics. In Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human (pp. 1401-1405). ACM.

[87] Veinović, M., Ćajić, M., & Brkić, B. (2011). Upravljanje kriptološkim ključevima. Naučni skup sa međunarodnim učešćem Sinergija.

[88] Ballard, L., Kamara, S., & Reiter, M. K. (2008, July). The Practical Subtleties of Biometric Key Generation. In USENIX Security Symposium (pp. 61-74).

[89] Lalithamani, N., & Soman, K. (2009). An effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. Int. J. Comput. Sci. Netw. Secur, 9(3), 183-193.

[90] Gaddam, S. V., & Lal, M. (2010). Efficient Cancelable Biometric Key Generation Scheme for Cryptography. IJ Network Security, 11(2), 61-69.

[91] Shibata, Y., Mimura, M., Takahashi, K., & Nishigaki, M. (2006). Mechanism-based PKI-a real-time key generation from fingerprints. In Proceedings of Conference on Security & Management, SAM'06 (pp. 468-474).

[92] Gudkov, V. Y., & Ushmaev, O. (2010, August). A Topologic Approach to User-Dependent Key Extraction from Fingerprints. In ICPR (pp. 1281-1284).

[93] Altarawneh, M. S., Khor, L. C., Woo, W. L., & Dlay, S. S. (2006, July). Crypto Key Generation Using Slicing Window Algorithm. In 5th IEEE Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP'06), Patras, Greece.

[94] Teoh, A. B., Ngo, D. C., & Goh, A. (2004). Personalised cryptographic key generation based on FaceHashing. Computers & Security, 23(7), 606-614.

[95] Chang, Y. J., Zhang, W., & Chen, T. (2004, June). Biometrics-based cryptographic key generation. In Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on (Vol. 3, pp. 2203-2206). IEEE.

[96] Chen, B., & Chandran, V. (2007, December). Biometric based cryptographic key generation from faces. In Digital Image Computing Techniques and Applications, 9th Biennial Conference of the Australian Pattern Recognition Society on (pp. 394-401). IEEE.

[97] Rathgeb, C., & Uhl, A. (2009, December). Context-based texture analysis for secure revocable iris-biometric key generation. In Crime Detection and Prevention (ICDP 2009), 3rd International Conference on (pp. 1-6). IET.

[98] Shamsi, M., Saad, P. B., & Rasouli, A. (2009). Creation of a Unique Private Crypto Key from Iris Image. In Proceeding of Postgraduate Annual Research Seminar, UTM.

[99] Wu, X., Qi, N., Wang, K., & Zhang, D. (2008, October). A novel cryptosystem based on iris key generation. In Natural Computation, 2008. ICNC'08. Fourth International Conference on (Vol. 4, pp. 53-56). IEEE.

[100] Tajuddin, M., & Nandini, C. (2013). Cryptographic Key Generation using Retina Biometric Parameter. eye, 3(1).

[101] Saraswathi, K., Jayaram, B., & Balasubramanian, R. (2011). Retinal Biometrics based Authentication and Key Exchange System. International Journal of Computer Applications, 19.

[102] Wu, X., Zhang, D., & Wang, K. (2007). A palmprint cryptosystem. In Advances in Biometrics (pp. 1035-1042). Springer Berlin Heidelberg.

[103] Wu, X., Wang, K., & Zhang, D. (2008, December). A cryptosystem based on palmprint feature. In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on (pp. 1-4). IEEE.

[104] Prasanalakshmi, B., & Kannammal, A. (2010, February). Secure cryptosystem from palm vein biometrics in smart card. In Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on (Vol. 1, pp. 653-657). IEEE.

[105] Venckauskas, A., & Nanevicius, P. (2013). Cryptographic Key Generation from Finger Vein. In (C) International Journal of Engineering Sciences & Research Technology (733-738).

[106] Xiao, G., Lu, M., Qin, L., & Lai, X. (2006). New field of cryptography: DNA cryptography. Chinese Science Bulletin, 51(12), 1413-1420.

[107] Cui, G., Qin, L., Wang, Y., & Zhang, X. (2008, September). An encryption scheme using DNA technology. In Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008. 3rd International Conference on (pp. 37-42). IEEE

[108] Lu, M., Lai, X., Xiao, G., & Qin, L. (2007). Symmetric-key cryptosystem with DNA technology. Science in China Series F: Information Sciences, 50(3), 324-333.

[109] Monrose, F., Reiter, M. K., Li, Q., & Wetzel, S. (2001). Cryptographic key generation from voice. In Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on (pp. 202-213). IEEE.

[110] Carrara, B., & Adams, C. (2010, August). You are the key: generating cryptographic keys from voice biometrics. In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on (pp. 213-222). IEEE.

[111] Feng, H., & Wah, C. C. (2002). Private key generation from on-line handwritten signatures. Information Management & Computer Security, 10(4), 159-164.

[112] Ballard, L., Chen, J., Lopresti, D., & Monrose, F. (2008, August). Biometric key generation using pseudo-signatures. In Proceedings of The 11th International Conference on Frontiers in Handwriting Recognition.

[113] Jagadeesan, A., & Duraiswamy, K. (2010). Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. arXiv preprint arXiv:1003.1458.

[114] Prasanalakshmi, B., Kannammal, A., & Sridevi, R. (2011). Multimodal Biometric Cryptosystem Involving Face, Fingerprint and Palm Vein. International Journal of Computer Science Issues (IJCSI), 8(4).

[115] Mahalakshmi, U., & Shankar Sriram, V. S. (2013). An ECC Based Multibiometric System for Enhancing Security. Indian Journal of Science & Technology, 6(4).