

**UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU**

SRĐAN MESAROVIĆ

**MULTIMODALNI BIOMETRIJSKI
SISTEMI**

- MAGISTARSKA TEZA -

BEOGRAD, 2007

**UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU**

MULTIMODALNI BIOMETRIJSKI SISTEMI

- MAGISTARSKA TEZA -

**MENTOR
PROF. MLADEN VEINOVIĆ**

**KANDIDAT
SRĐAN MESAROVIĆ
BR. INDEKSA II-8/2005**

BEOGRAD, 2007

Sadržaj

1. Uvod	9
1.1 Istorija biometrije	9
1.2 Autentifikacije	10
1.2.2 Metodi autentifikacije	11
1.3 Značaj biometrije.....	11
2. Trenutna situacija u svetu i kod nas	13
2.1 Kritike javnosti	13
2.2 Pregled po zemljama	14
2.2.1 Brazil.....	14
2.2.2 SAD	14
2.2.3 Nemačka	16
2.2.4 Velika Britanija.....	16
2.2.4.1 Kritike, poverenje i privatnost podataka.....	17
2.2.5 Francuska	17
2.2.5.1 Kritike, poverenje i privatnost podataka.....	17
2.2.6 Australija.....	18
2.2.7 Singapur	18
2.2.8 Izrael	18
2.2.9 Japan	19
2.2.10 Malezija	19
2.2.11 Jordan.....	19
2.2.12 Srbija.....	19
2.2.12.1 Kritike, poverenje, privatnost podataka.....	20
3. Biometrijski sistemi.....	22
3.1 Koncept biometrijske verifikacije	25
3.1.1 Prepoznavanje otiska	25
3.1.1.1 Minutiae	26
3.1.2 Kreiranje šablona	26
3.1.3 Poređenje šablona	26
3.2 Koncept biometrijske identifikacije.....	27
3.3 Performanse biometrijskih sistema.....	28
3.3.1 Performanse i greške u procesu upisa	28
3.3.2 Performanse i greške u procesu verifikacije	28
3.3.3 Performanse i greške u procesu identifikacije	31
3.4 Najčešće korišćeni biometrijski sistemi	31
3.4.1 Otisak prsta	33
3.4.1.1 Kako funkcioniše autentifikacija.	34
3.4.1.2 Prednosti i slabosti tehnologije skeniranja otiska prsta	38
3.4.2 Crte lica.....	39
3.4.2.1 Tehnologija prepoznavanja lica.....	40
Neke primene tehnologije prepoznavanja lica.....	42
3.4.3 Geometrija dlana i raspored vena.....	43
3.4.4 Skeniranje oka	44
3.4.4.1 Prednosti i slabosti tehnologije skeniranja dužice oka	46
3.4.5 Prepoznavanje glasa.....	46
3.4.6 Drugi biometrijski sistemi.....	48
4. Sigurnost biometrijskog sistema.....	50
4.1 Napadi na biometrijski sistem	50
4.1.1 Napadi na ulaznom nivou	50
4.1.2 Napadi na nivou obrade i prenosa podatka	50
4.2 Različiti načini biometrijske implementacije	52
4.2.2 Pregled sigurnosti	53
5. Multimodalni biometrijski sistemi	55

5.1 Poboljšanje performansi sistema	57
5.1.1 Opis performansi.....	58
6. Izvor i sjedinjavanje podataka.....	60
6.1 Šta sjediniti ?	60
6.2 Koje biometrijske karakteristike sjediniti ?	61
6.3 Arhitektura sjedinjavanja biometrijskih podataka	62
6.3.1 Redna arhitektura	62
6.3.2 Paralelna arhitektura	62
6.3.3 Hijerarhijska arhitektura	63
6.4 Nivoi sjedinjavanja.....	64
6.4.1 Sjedinjavanje pre poređenja.....	65
6.4.1.1 Nivo senzora.....	65
6.4.1.2 Nivo izdvajanja podataka	65
6.4.2 Sjedinjavanje posle poređenja.....	66
6.4.2.1 Nivo poređenja šablona	67
6.4.2.2 Nivo odlučivanja	69
6.5 Evaluacija multimodalnog sistema.....	69
6.6 Prednosti i mane multimodalnih biometrijskih sistema.....	70
6.7 Zaključak.....	71
7. Normalizacija rezultata	72
7.1 Potreba za normalizacijom rezultata.....	73
7.2 Izazovi normalizacije.....	75
7.2.1 Parametri lokacije i skale	76
7.3 Tehnike normalizacije	78
7.3.1 Eksperimentalni Rezultati	88
7.3.1.1 Generisanje multimodalne baze podataka	88
7.3.2 Uticaj normalizacije na performanse sjedinjavanja podataka	90
7.3.3 Analiza robustnosti metoda normalizacije	93
7.4 Zaključak.....	96
8. Soft biometrija	97
8.1 Motiv i izazovi.....	97
8.2 Prikupljanje soft biometrijskih podataka.....	98
8.3 Sjedinjavanje soft i primarnih biometrijskih informacija	100
8.3.1 Režim identifikacije.....	100
8.3.2 Režim verifikacije.....	101
8.3.2.1 Izračunavanje soft biometrijskih verovatnoća.....	102
8.4 Eksperimentalni rezultati.....	103
8.4.1 Identifikacione performanse	103
8.4.2 Verifikacione performanse.....	104
8.5 Zaključak.....	108
9. Zaključak	109
10. Budući rad.....	110
11. Literatura	111

Slike

Slika 1 – Norveški biometrijski pasoš	13
Slika 2 - ATM kompanije Brown Investments Inc.....	15
Slika 3 - Pay by Touch terminal	18
Slika 4 - Opšti model biometrijskog sistema	23
Slika 5 - ANSI X9.84 opšti model biometrijskog sistema.....	23
Slika 6 - Upis biometrijskog šablona	24
Slika 7 - Verifikacioni proces	25
Slika 8 - Proces identifikacije	26
Slika 9 - Odnos između FAR, FRR i EER.....	29
Slika 10 - Originalna i nametnuta distribucija i odnos FNMR i FMR u odnosu na treshold.....	30
Slika 11 - Najčešće korišćene biometrijske karakteristike. a) otisak prsta, b) geometrija dlana, c) dužica oka, d) rožnjača oka, e) crte lica, f) otisak šake, g) oblik uha, h) DNK, i) glas, j) hod, k) potpis, l) dinamika kicanja	32
Slika 12 - Program za identifikaciju otisaka prstiju.....	33
Slika 13 - Brazde otiska.....	33
Slika 14 - Proces od originalne slike do šablona	34
Slika 15 - Prikaz otiska zavisno od vlažnosti	35
Slika 16 - 2D ćelije kapacitivnog senzora	35
Slika 17 - Skeniranje prsta.....	35
Slika 18 - Minutiae snimljene senzorima kompanije Fidelica Microsystem.....	36
Slika 19 - FPC 1011 Area sensor i FPC 1031 Swipe sensor	36
Slika 20 - Direktno kapacitivno merenje FPC senzorima.....	36
Slika 21 - Aktivno kapacitivno merenje FPC senzorima.....	37
Slika 22 - Princip rada optičkog senzora	37
Slika 23a - Slika vlažnog prsta sa senzora osetljivog na pritisak	38
Slika 23b - Slika suvog prsta sa senzora osetljivog na pritisak	38
Slika 24 - Senzor osetljiv na otpornost.....	38
Slika 25 - Karakteristične tačke lica	39
Slika 26 - Formiranje digitalnog koda za prepoznavanje lica	41
Slika 27 - Skener lica u banci	43
Slika 28 - Tipične mere sistema za proveru geometrije dlana	44
Slika 29 - Dužica oka i njen negativ.....	44
Slika 30 - Dužica sa IrisCode u gornjem levom uglu slike	45
Slika 31 - Identifikacioni sistem UAE (skeniranje dužice oka).....	45
Slika 32 - IBM VIVA sistem za prepoznavanje glasa	47
Slika 33 - Poređenje različitih biometrijskih sistema	49
Slika 34 - Slabe tačke biometrijskog sistema	51
Slika 35 - Loš otisak prsta	55
Slika 36 - Zamagljena slika dužice oka usled gubljenja fokusa	55
Slika 37 - Nepravilna upotreba sistema.....	56
Slika 38 - : Neadekvatno osvetljenje	56
Slika 39 - Slabo izraženi otisci prstiju	57
Slika 40 - Način upotrebe lažnih otisaka prstiju	57
Slika 41 - Primer multi-biometrijskog sistema.....	60
Slika 42a - Redna arhitektura sjedinjavanja	62
Slika 42b - Paralelna arhitektura sjedinjavanja	62
Slika 42c - Hijerarhijska arhitektura sjedinjavanja.....	63
Slika 43 - Nivoi sjedinjavanja kod multi-biometrijskog sistema.....	64
Slika 44a - Nivo izdvajanja podataka.....	66
Slika 44b - Nivo poređenja šablona	67
Slika 44c - Nivo odluke.....	69
Slika 45 - Grupni prikaz tehnika sjedinjavanja kod multimodalnog biometrijskog sistema	71
Slika 46a - Distribucija rezultata poređenja crte lica.....	73
Slika 46b - Distribucija rezultata poređenja otiska prsta.....	74
Slika 46c - Distribucija rezultata poređenja geometrije dlana	74

Slika 47 - Parametri lokacije i skale: lokacija = 0, skala = 1.....	76
Slika 48 - Parametri lokacije i skale: lokacija = 10, skala = 1.....	76
Slika 49 - Parametri lokacije i skale: lokacija = 0, skala = 3.....	77
Slika 50 - Parametri lokacije i skale: lokacija = 0, skala = 0.333.....	77
Slika 51 - Distribucije originalnog i lažnog korisnika postignute nakon min-max normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana.....	79
Slika 52 - Distribucije originalnog i lažnog korisnika postignute nakon <i>Z-rezultat</i> normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana.....	81
Slika 53 - Distribucije originalnog i lažnog korisnika postignute nakon medijana-MAD normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana.....	82
Slika 54 - Dvostruka Sigmoidna normalizacija.....	83
Slika 55 - Distribucije originalnog i lažnog korisnika postignute nakon dvostruke sigmoidne normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana.....	84
Slika 56 - Tanh-estimators normalizacija.....	85
Slika 57 - Hampelova funkcija uticaja ($a=0.70$, $b=0.85$, $c=0.95$).....	86
Slika 58 - Distribucije originalnog i lažnog korisnika postignute nakon Tanh-estimators normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana.....	87
Slika 59 - ROC (eng. Receiver Operating Characteristic) krive pojedinačnih karakteristika	89
Slika 60 - ROC krive zbira rezultata tehnike sjedinjavanja pri različitim normalizacionim tehnikama.....	91
Slika 61 - ROC krive maksimalnog rezultata tehnike sjedinjavanja pri različitim normalizacionim tehnikama.....	92
Slika 62 - ROC krive minimalnog rezultata tehnike sjedinjavanja pri različitim normalizacionim tehnikama.....	93
Slika 63 - Analiza robustnosti kod min-max normalizacije	94
Slika 64 - Analiza robustnosti kod <i>Z-rezultat</i> normalizacije	95
Slika 65 - Analiza robustnosti kod Tanh normalizacije.....	96
Slika 66 - ATM uređaj snabdeven senzorom otiska prsta kao primarnim biom.identifikatorom i kamerom za dobijanje soft identifikatora.....	97
Slika 67 - Primeri soft biometrijskih pristupa.....	99
Slika 68 - Sistem za sjedinjavanje soft i primarnih biometrijskih podataka.....	101
Slika 69 - Poboljšanje identif. performansi sistema za prepoznavanje otisaka prstiju uz upotrebu <i>soft</i> osobina. a) Sa polom i etn. pripadnošću, b) Sa visinom i c) Sa polom, etn. pripadnošću i visinom	105
Slika 70 - Poboljšanje identif. performansi sistema za prepoznavanje crta lica uz upotrebu podatka o visini korisnika.....	106
Slika 71 - Poboljšanje identif. performansi multimodalnog sistema (otisci prstiju i crte lica) uz upotrebu <i>soft</i> osobina	106
Slika 72 - Poboljšanje identif. performansi sistema za prepoznavanje otisaka prstiju uz upotrebu <i>soft</i> osobina. a) Sa polom i etn. pripadnošću, b) Sa visinom i c) Sa polom, etn. pripadnošću i visinom	107
Slika 73 - Poboljšanje identif. performansi sistema za prepoznavanje crta lica uz upotrebu podatka o visini korisnika.....	107
Slika 74 - Poboljšanje identif. performansi multimodalnog sistema (otisci prstiju i crte lica) uz upotrebu <i>soft</i> osobina	107

Tabele

Tabela 1 - Greške kod najčešćih biometrijskih karakteristika.....	28
Tabela 2 - Procentualna zastupljenost biometrijskih tehnika na tržištu	31
Tabela 3 - Poređenje biometrijskih sistema	48
Tabela 4 - Slabe tačke biometrijskih sistema	52
Tabela 5 - Kombinacija mesta čuvanja podataka, i mesta	52
Tabela 6 - Kombinacije biometrijskih karakteristika	61
Tabela 7 - Karakteristike tehnika normalizacije.....	88
Tabela 8 - GAR različitih tehnika normalizacije i sjedinjavanja podataka pri FAR = 0.1%	90

Sažetak

Dobro je poznato da su određene osobine ljudskog tela, kao što su DNK, otisak prsta i sl., karakteristične za svaku osobu, Sama biometrija predstavlja upotrebu bioloških karakteristika (lice, dužica oka, otisak prsta) ili osobina kao što su glas ili potpis sa ciljem potvrde identiteta osobe. Isto tako, predstavlja zamenu i daleko sigurniju varijantu zaštite od sistema zaštite zasnovanih na lozinkama.

Biometrija, raspoznavanje zasnovano na različitim ličnim crtama, ima sve veće šanse da postane nezamenjivi deo svakog sistema identifikacije. Iako se uspešno pokazala u određenim oblastima, za sada još nije u potpunosti dorađena po pitanju automatskog prepoznavanja ljudskih fizičkih karakteristika. Kao i svaka nova tehnologija, sa sobom je unela i niz ranjivosti u računarski sistem. Sa sve pristupačnijom računarskom opremom i biometrijskim senzorima, počinju da se nameću i pitanja tipa: kako efikasno prepoznati biometrijski šablon, kako možemo biti sigurni da skenirani podaci neće biti ukradeni, da li ugrađena aplikacija, šablon koristi isključivo u navedene svrhe itd. ? Rešavanjem tih ključnih pitanja i problema, biometrija će sigurno na široka vrata ući u svet zaštite bez dovođenja u pitanje ljudske privatnosti i ljudskih sloboda.

Cilj ovog rada je rešiti sporna pitanja vezana za autentifikaciju identiteta upotrebom biometrijskih informacija. Fokusiraću se na sintezu više biometrijskih sistema, prednostima i manama istog kao i upotrebu tzv.*soft* biometrijskih identifikatora. Takođe, osvrnuću se i na samu biometriju, trenutno stanje u svetu sa pravne i praktične strane, različite tehnologije raspoznavanja, sigurnost, prednosti i mane u odnosu na druge sigurnosne sisteme kao i poverenje ljudi u ovaj oblik autentifikacije.

Abstract

It is well known that determine characteristics of the human body are unique for the every person, just as is the DNA, fingerprint etc. Biometrics present the usage of physiological (the face image, iris, fingerprint...) and/or behavioral characteristic just as is the voice or the signature with the aim to confirms the identity of individual. Likewise, presents replacement and more secure kind of protection unlike the system with protection based on passwords.

Biometrics, recognition based on different personal attributes, has the growing chance to becomes unreplaceable part of every identification system. Although successfully was showed in some domains, for now, it has not been finished completely in consideration of the automatic recognizing of human physical characteristics. As well as every new technologies, is brought the vulnerability into the computer system. With the more and more accessible computer equipment and biometric sensors, it is impossible to not propound questions: how to efficient recognize biometric template, how can be sure that scanned data will not be stolen, is built application uses templates only in suggested purposes etc. ? Solving of this key questions and problems, biometrics certainly enters the world of protections without compromise the human privacy and human freedoms.

Aim of this work is to determine disputable issues based on identity authentication using biometric informations. I'll focus on the synthesis of two or more biometric systems, advantages and defects of the same as well as the usage of the soft biometric identifiers. Also, I'll review biometrics itself, state-of-the-art, in terms of legal and practical side, different technologies of recognition, security, advantages and defects in respect to other security systems as well as a confidence of people in this kind of authentication.

1. Uvod

Biometrija predstavlja način automatskog prepoznavanja osobe na osnovu određenih fizičkih osobina. Unimodalni biometrijski sistemi prepoznavanje baziraju na proveru jedne ulazne osobine što često dovodi do problema, a samim tim, i pogrešnih rezultata. Problemi koji mogu nastati, najčešće se odnose na pojavu šuma, na otežano očitavanje, visok nivo sličnosti očitanih karakteristika kod više osoba, mogućnost relativno jednostavne obmane sistema itd. Uvođenjem multimodalnih biometrijskih sistema, odnosno sistema zasnovanih na upotrebi više različitih ulaznih podataka, koji se u određenom trenutku sjedinjavanju, veći deo pomenutih problema može biti rešen ili bar umanjen na prihvatljiv nivo. U praksi, kao najbolji pristup, pokazalo se sjedinjavanje podataka na nivou poređenja šablona¹ (trenutak kad se dobiju rezultati poređenja iz svakog modul za proveru).

U tezi, pažnja će biti posvećena još dvema bitnim stvarima i to: normalizaciji kao postupku homogenizacije rezultata poređenja, različitim metodama normalizacije i njenom uticaju na efikasnost i robustnost sistema kao i tzv. *soft* biometrijskim osobinama. Takođe, biće prikazano kako *soft* biometrijske osobine, kao što su: pol, etnička pripadnost, starost i sl. samostalno ne mogu, dovoljno pouzdano, obezbediti prepoznavanje osoba ali u kombinaciji sa klasičnim osobinama (npr. otisak prsta ili crte lica), predstavljaju značajan faktor u podizanju opšteg nivoa efikasnosti multimodalnog biometrijskog sistema.

Veći deo opisanih eksperimenata u ovoj tezi, vezanih za tzv. *soft* biometriju i normalizaciju, izvršen je od strane Karthik Nandakumara, studenta MSU (*Michigan State University*) tokom 2005. godine u laboratoriji za prepoznavanje šablona i obradu slike (eng. *The Pattern Recognition and Image Processing, PRIP*) na odakle su i preuzeti rezultati istraživanja.

1.1 Istorija biometrije

Reč biometrija izvedena je iz grčkih reči *bios* (život) i *metria* (meriti). Automatizovani biometrijski sistemi dostupni su poslednjih nekoliko decenija, zbog značajnog napretka na polju računarske obrade, ali se mnoge od automatizovanih tehnika baziraju na idejama starim stotinama ili čak hiljadama godina.

Jedan od najstarijih i najosnovnijih primera karakteristika, koje se koriste za prepoznavanje od strane drugih ljudi, je lice. Od samih početaka civilizacije, ljudi koriste lice za prepoznavanje osoba. Koncept prepoznavanja ljudi od strane ljudi vidljiv je i u npr. prepoznavanju govora (govornika, onoga koji govori), kao i u ostalim primerima prepoznavanja karakteristika svakodnevnog ponašanja.

Ostale karakteristike, korišćene za prepoznavanje tokom istorije civilizacije su mnogo formalnije. Neki od primera su: otisci šake na slikama u pećinama, za koje se smatra da ih je ostavio praistorijski čovek pre 31000 godina, otisci prstiju kojima su rani kineski trgovci potvrđivali poslovne transakcije, na isti način kao i trgovci u Vavilonu oko 500 godine pre nove ere itd.

Sredinom devetnaestog veka, sa naglim razvojem gradova i industrijskom revolucijom, dolazi do sve veće mobilnosti populacije i pojavljuje se potreba za pouzdanom identifikacijom ljudi. Prvi pokušaj je vezan za *Bertillon*-ov sistem merenja različitih karakteristika tela, koje je on nazvao antropometrija. Drugi pokušaj je formalno korišćenje otisaka prstiju od strane policije. Prvi robustni sistem za indeksiranje otisaka prstiju razvijen je u Indiji za Edvarda Henrija,

¹ Biometrijski šablon – matematički prikaz biometrijskog uzorka koji omogućuje algoritmima najbrži mogući rad konvertujući relevantne informacije u niz bitova i bajtova. Ovde je bitna brzina poređenja i veličina šablona.

generalnog inspektora policije u Bengalu. Ovaj sistem, koji se naziva *Henrijev sistem*, kao i njegove varijacije, još uvek se koriste za klasifikaciju otisaka prstiju.

Biometrijski sistemi su dobili na značaju u drugoj polovini dvadesetog veka, što koincidira sa značajnim prodorom računarskih sistema. Devedesetih godina dvadesetog veka dolazi do eksplozije u ovoj oblasti, tako da su biometrijske aplikacije u svakodnevnoj upotrebi već početkom dvadeset prvog veka.

1.2 Autentifikacije

Svako poseduje osobine koje tu osobu čine jedinstvenom i koje omogućavaju da se identifikuje ili potvrdi identitet neke osobe. U kompjuterskom svetu identitet je definisan kao „*jedinstveni naziv osobe, uređaja ili oba prepoznat od strane sistema*“. Čest jedinstven naziv za identifikaciju i verifikaciju je autentifikacija.

Situacija u svetu danas čini bezbednost sve važnijom stavkom u našim životima pa samim tim i svakodnevna autentifikacija ima daleko veći značaj danas nego u ranijem periodu.

Kada sistem ili osoba proverava identitet druge osobe ili sistema, vrši se autentifikacija što znači da svako ko je autentifikovan može da potvrdi da je ono što bi trebao biti. Važno je pomenuti da autentifikacija samo potvrđuje identitet i ništa dalje ne čini sa njime niti definiše njegova prava pristupa.

Postoje dva osnovna tipa autentifikacije [63]:

- Verifikacija.
- Identifikacija;

Verifikacija

Kod verifikacije vrši se potvrđivanje identiteta neke osobe u smislu poređenja dobijenog podatka sa tačno određenim uzorkom u bazi podataka. Ovaj oblik autentifikacije predstavlja 1:1 sistem.

Identifikacija

U slučaju identifikacije, vrši se provera podudaranja dobijenog uzorka sa svim sačuvanim uzorcima u bazi podataka s ciljem dobijanja podatka o identitetu neke osobe. Ovaj sistem predstavlja 1:N (1:više) sistem autentifikacije.

Oba tipa autentifikacije se koriste kod biometrijskih autentifikacionih sistema, a koji će biti upotrebljen zavisi konkretno od aplikacije.

Pored ova dva osnovna tipa, postoji još i tzv. negativna identifikacija gde korisnik treba da potvrdi da njegov identitet ne odgovara traženom identitetu. U ovom slučaju, gde se takođe vrši 1:N pretraga, pozitivan odgovor o podudaranju se dobija samo u slučaju da se uneti podatak u najvećoj mogućoj meri poklapa sa sačuvanim šablonom, u suprotnom se prihvata tvrdnja korisnika da nije ta osoba koja se traži. Sistem se često koristi na aerodromima gde se putnici proveravaju da li su eventualno na „crnim listama“. Ukratko rečeno, sistemi negativne identifikacije odgovaraju na pitanje „*Da li si ti onaj za kojeg kažeš da nisi?*“. Za razliku od verifikacije koja može biti izvršena putem lozinke ili PIN²-a, negativna identifikacija se može obezbediti isključivo putem biometrijske provere.

² PIN-lični identifikacioni broj (eng. *Personal Identification Number*)

1.2.2 Metodi autentifikacije

Danas postoje tri metoda autentifikovanja sebe drugoj osobi ili sistemu [61, 64].

- Bazirana na znanju („šta znaš“)
- Bazirana na objektu („šta imaš“)
- Bazirana na biometriji („šta si“)

Bazirana na znanju

Metoda se zasniva na tome da korisnik pamti neki podatak. Najčešće je to lozinka ili PIN kôd. Veliki sigurnosni problem je u tome što korisnici radi lakšeg pamćenja zadaju predvidljive lozinke retko menjaju i koje je lako pogoditi ili ih zapisuju na papir.

Bazirana na objektu

Metoda se zasniva na posedovanju nečega što će potvrditi identitet osobe. To su najčešće ID kartice, pasoši, platne kartice...Dobra osobina je ta što korisnik nema potrebe da pamti bilo kakve informacije ali isto tako identifikacioni objekat se može izgubiti ili ukrasti, a samim tim i falsifikovati. Jedina prednost u ovome je što korisnik odmah vidi da više ne poseduje objekat pa može brzo reagovati kako bi sprečio eventualne posledice.

Bazirana na biometriji

Metoda se zasniva na tome da korisnik poseduje određeni biometrijski identifikator (otisak prsta, crte lica...) koji toj osobi pripada samim rođenjem i koji se tokom života ne menja ili se menja veoma malo. Ovde ne postoji mogućnost gubljenja ili zaboravljanja identifikatora, a i mogućnost falsifikovanja je neuporedivo manja nego kod prethodno pomenute dve metode autentifikacije.

1.3 Značaj biometrije

Kao što je u prethodnom poglavlju rečeno, postoje tri osnovna oblika identifikacije danas. Prvi je prema nečemu što osoba poseduje, kao što je kartica. Drugi je nešto što zna, kao što su lozinka ili PIN dok je treći nešto što ta osoba jeste, kao npr. otisak prsta ili nešto što radimo, npr. potpis ili glas. Taj treći oblik identifikacije naziva se biometrija. Sama biometrija predstavlja upotrebu bioloških karakteristika (lice, dužica oka, otiska prsta i sl.) ili osobina (glas ili potpis) sa ciljem potvrde identiteta osobe. Isto tako, predstavlja zamenu i daleko sigurniji oblik zaštite od sistema zaštite zasnovanih na lozinkama. Kao takva, biometrija, raspoznavanje zasnovano na različitim ličnim crtama, ima sve veće šanse da postane nezamenjivi deo svakog sistema identifikacije.

Biometrija predstavlja automatizovan metod utvrđivanja identiteta osobe na osnovu fizioloških karakteristika kao što su lice, otisak prsta, geometrija dlana, dužica ili mrežnjača oka, raspored vena ili glas. Kako raste potreba za višim nivoom sigurnosti, tako su biometrijski sistemi sve manji, precizniji, pouzdaniji i brži i nalaze sve veću primenu u svim delatnostima gde je neophodno nedvosmisleno utvrditi ili potvrditi identitet osobe. Ljudski faktor i dalje predstavlja osnovnu „rupu“ u sigurnosti brojnih sistema: nemaštovite lozinke u vidu datuma rođenja ili imena partnera, lozinke zalepljene na papiru s donje strane tastature ili na monitoru, PIN-ovi zapisani na ceduljicama u novčaniku... Sve veća potreba za pamćenjem lozinke i brojeva primorava nas na upotrebu istih šifara ili onih lakih za pamćenje. Biometrija eliminiše potrebu za pamćenjem lozinke jer istu predstavljamo mi sami. Ono što je nekada predstavljalo osnovni trik u naučnofantastičnim filmovima, danas postaje uobičajena slika u predvorjima zgrada velikih kompanija, u državnim institucijama i na aerodromima tehnološki naprednog Zapada, a odskora i kod nas. Potreba za biometrijom naročito je porasla posle terorističkih napada u Americi 11. septembra 2001. godine. Od tog perioda, kada se javila

potreba da se iz mase izdvoje potencijalni teroristi, drastično su pooštrene kontrole na aerodromima. Ovaj događaj je, pored brojnih uticaja na dešavanja u celom svetu, pospešio razvoj i intenzivirao primenu biometrijskih sistema. Biometrijski sistem za identifikaciju posmatra osobu analizirajući njeno ponašanje ili fizičke osobine. Identifikacioni dokument na kome se nalaze biometrijski podaci osobe, može da koristi samo osoba čiji su podaci na dokumentu.

Neke od prednosti biometrijskog sistema za identifikaciju su:

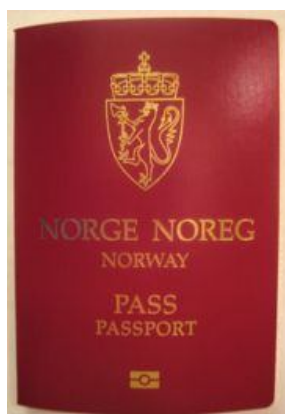
- Manji troškovi administracije;
- Integritet identifikacije;
- Integritet informacije;
- Brži pristup podacima;
- Brže izvršavanje servisa i ukazivanje pomoći;
- Precizniji statistički i istraživački podaci;
- Viši nivo sigurnosti.

2. Trenutna situacija u svetu i kod nas

Osnovni oblici upotrebe biometrije, kako u svetu tako i kod nas, su identifikacione kartice (lične karte, vozačke dozvole, zdravstvene knjižice i sl.), elektronski pasoši koji predstavljaju kombinaciju papirnog i digitalnog identifikacionog dokumenta kao i ID kartice za evidenciju i kontrolu zaposlenih u firmama. Izdavanje elektronskih dokumenata postalo je jedan od načina na koji se vlade razvijenih zemalja sveta bore protiv terorističkih napada i ilegalne emigracije. Veliki broj zemalja već izdaje ili planira izdavanje elektronskih dokumenata, pre svega identifikacionih kartica (koje zamenjuju lične karte) i e-pasoša. Najvažniji deo tih dokumenata je ugrađeni čip za radiofrekventnu identifikaciju u kome se čuvaju lični podaci vlasnika dokumenta - uglavnom je to njegovo ime, prezime, mesto i datum rođenja, pol, broj pasoša i određeni biometrijski podaci, kao što su digitalna slika vlasnika, otisci njegovih prstiju i dlanova i skenirane slike dužice ili rožnjače oka.

Trenutno je u 16 evropskih zemalja (Nemačka, Grčka, Holandija, Norveška, Švedska, Danska, Austrija, Belgija, Francuska, Island, Finska, Litvanija, Portugal, Velika Britanija, Poljska, Irska i Italija) počelo izdavanje ovakvih pasoša kao i u SAD, Australiji, Kanadi, Singapuru, Japanu, Tajlandu i na Novom Zelandu. Za sada ni jedan od ovih pasoša ne sadrži otisak prsta kao biometrijski podatak. Na slici 1 je prikazan norveški biometrijski pasoš.

Što se tiče nacionalnih biometrijskih ID kartica, one će po svemu sudeći među prvim da se pojave u Srbiji. Nova lična dokumenta u Srbiji su među najmodernijim rešenjima u svetu. Nekoliko zemalja već primenjuje elektronski nacionalni ID dokumenat, dok je u drugim zemljama ovaj projekat u toku. Posebno daleko u razvoju ove tehnologije otišli su Belgija, Estonija, Finska, Italija, Austrija, Makao, Malezija, Izrael, Kanada, Velika Britanija i delimično SAD [71].



Slika 1: Norveški biometrijski pasoš

2.1 Kritike javnosti

Elektronski dokumenti su od prvog dana "na udaru" organizacija za zaštitu ljudskih prava (zbog navodnog ugrožavanja građanskih prava i privatnosti pojedinaca), ali i stručnjaka za bezbednost koji smatraju da ti dokumenti ne pružaju stopostotnu bezbednost. Jedan od zagovornika protiv upotrebe elektronske identifikacije, prof. dr Rodžer Klark sa australijskog državnog univerziteta istakao je da „biometrija koja se, može koristiti pri testiranju toga da li je moguće da osoba koja prilaže karticu ista kao osoba kojoj je ta kartica izdata, takođe se može koristiti kao način otključavanja šifrovanih ključeva smeštenih u istom čipu. Biometrija mnogim ljudima izgleda nametljiva i opasna. Zavisno od primene, ne mora samo izgledati tako, već i jeste tako“. Takođe, dr Klark, dao je svoje mišljenje i po

pitanju smeštanja podataka u centralnu bazu: „Nadzor podataka je sistematska upotreba ličnih sistema podataka u istraživanju ili snimanju radnji ili komunikacija jedne ili više osoba. Lični nadzor predstavlja nadgledanje identifikovane osobe. Masovni nadzor je nadzor više grupa ljudi, naročito velikih grupa, obično da bi se identifikovale osobe koje pripadaju određenoj interesnoj sferi ili da bi se možda potisnulo njihovo ponašanje. Organizacije dobijaju moć nad osobama kroz akumulaciju podataka o njima. One mogu povećati tu moć crpljenjem podataka iz više izvora. Pojedinci su uglavnom nemoćni da isprave netačne podatke, pogrešne procene i nerazumne odluke. Na nivou društva kao celine, dalji ozbiljni problemi izbijaju na površinu, pošto preovladava opšta sumnja, dok samo opredeljenje i

raznolikost bivaju ugušeni efektom sveobuhvatnog nadziranja“. Kao zaključak, naveo je „Iz sprovedene analize izgleda neizbežno da će identifikacione šeme bazirane na čipovima ugroziti privatnost i da postoji direktan sukob između primene čipova u identifikacionim karticama i preživljavanja relativno slobodnog i demokratskog društva kome teže napredne nacije“³ [64].

2.2 Pregled po zemljama

U ovom poglavlju biće opisana situacija u nekim zemljama sveta koje imaju razvijene biometrijske sisteme ili gde su sistemi blizu faze upotrebe. Najveća koncentracija upotrebe biometrije je u oblastima kontrole granica, aerodroma, nacionalnih ID kartica i finansijskih servisa pa će kao takvi i biti opisani kroz aktuelne primere.

2.2.1 Brazil

Još od početka 20-og veka brazilski građani koriste identifikacione kartice (u daljem tekstu: ID kartice). Svakoj državi Brazila dozvoljeno je da samostalno izdaje ID kartice uz uslov da njihov izgled i sadržaj budu identični. ID kartice su potpuno digitalizovane upotrebom 2D bar kôda sa informacijama koje identifikuju njenog vlasnika. 2D bar kodira kolor sliku, potpis, dva otiska prsta i ostale podatke vezane za prebivalište. Ova tehnologija uvedena je u upotrebu 2000. godine sa ciljem povećanja sigurnosti brazilskih ID kartica.

Krajem 2005. godine brazilska vlada počela je sa radom na novim digitalizovanim pasošem koji će, kad uđe u upotrebu, sadržati potpis, sliku i otiske svih deset prstiju koji će biti uzeti prilikom podnošenja zahteva za izdavanje pasoša. Svi podaci biće sačuvani prema **ICAO⁴ E-passport** standardu. To će omogućiti beskontaktno elektronsko očitavanje sadržaja pasoša i verifikaciju kartice dok će šablon otisaka prstiju i slika omogućiti vizuelnu identifikaciju. Planirano je da projekat uđe u operativnu fazu u drugoj polovini 2006. godine.

2.2.2 SAD

Vlada SAD-a poslednjih godina postala je veliki zagovornik uvođenja biometrijske identifikacije u cilju povećanja bezbednosti. Počevši od 2005. godine, radi se na izdavanju pasoša sa biometrijskim podacima što predstavlja razlog za mnoge kritike od strane raznih aktivista koji se zalažu za zaštitu privatnosti i ljudskih sloboda. Trenutno, kako u SAD tako i u EU postoji bojazan da se podaci sa takve legitimacije mogu “skinuti” od strane raznih kriminalnih grupa što bi predstavljalo neku vrstu krađe identiteta. Takođe, postoji još dosta tehničkih problema za uvođenje biometrijskih pasoša kao što su kompatibilnost čitača podataka, kao i dogovor oko podataka koje je potrebno digitalizovati. Dok SAD i Velika Britanija teže ka tome da se samo digitalizuje slika, članice EU se zalažu dodatno i za upotrebu otisaka prstiju u svom **RFID⁵** biometrijskom čipu.

³ Rodžer Klark: Elektronska identifikacija-izazovi i opasnosti, 19.8.2006. www.vidovdan.org

⁴ International Civil Aviation Organization, agencija u okviru UN zadužena za potvrđivanje principa i tehnika u međunarodnoj vazdušnoj navigaciji i podstrekivanje planiranja i razvoja sigurnosnih mehanizama u pomenutoj oblasti u međunarodnom vazdušnom transportu.

⁵ Radio Frequency Identification, automatski identifikacioni metod zasnovan na čuvanju i daljinskom očitavanju podataka upotrebom uređaja nazvanih RFID tag-ovi (objekat koji može biti pripojen ili ugrađen u proizvod, životinju ili osobu kako bi se obezbedila identifikacija upotrebom radio talasa) ili transponderi. Standardi za RFID su definisani od strane ICAO i opisani u “ICAO Document 9303, Part 1, Volumes 1 and 2 (6. izdanje, 2006)”. ICAO se poziva na ISO 14443 RFID čipovima e-pasoša kao “beskontaktnim elektronskim kolima”.

Počevši od 2006. RFID tagovi su uključeni u nove pasoše Velike Britanije kao i u neke pasoše SAD-a. Tokom, 2005. i 2006. godine u SAD je izdato 23 miliona pasoša koji u svom čipu sadrže sve one informacije koje su inače i odštampane kao i digitalnu sliku vlasnika. Čipovi američkih pasoša biće veličine 64KB i za očekivati je da će svi pasoši biti zamenjeni tokom 2006. ili početkom 2007. godine. Prema istraživanjima javnosti naručenog od firme TRUSTe, 82% Amerikanaca podržava uvođenje biometrijskih e-pasoša, 75% biometrijskih vozačkih dozvola i 72% stanovništva podržava uvođenje biometrijskih podataka u kartice socijalnog osiguranja. 52% ispitanika smatra da će se tim merama drastično otežati teroristička delatnost na teritoriji SAD.

Govor američkog predsednika Džordža Buša 15. maja 2006. godina predstavlja putokaz daljem razvoju sistema provere imigranata: *“Svako ko od sada bude želeo da legalno radi u SAD moraće pri ulasku u zemlju da ostavi svoje otiske prstiju. Osnovni deo ovog sistema je izdavanje novih biometrijskih ID kartica svakom strancu, legalno zaposlenom u SAD”*⁶.

Ministarstvo odbrane SAD (DoD) izdaje tzv. *Common Access Card*, koja predstavlja ID karticu za sve zaposlene i saradnike u ministarstvu. Kartica sadrži biometrijske podatke i digitalizovane slike. Takođe, sadrži laserski ugravirane slike i holograme kako bi se smanjila mogućnosti falsifikovanja. Trenutno je u opticaju oko 10 miliona istih.



Slika 2: ATM kompanije Brown Investments Inc

SAD su jedine uz Ujedinjene Arapske Emirate uspostavile potpunu biometrijsku kontrolu granice dok je u EU sistem tek u povoju.

U svetu finansija, poslednji novitet (januar 2007. godine) predstavlja novi tip višenamenskog ATM terminala projektovanog od strane *Brown Investments Inc.* kompanije iz Nešvila, država Tenesi. ATM, koji će se prodavati po ceni od 25995 \$, predstavlja tzv. *10 in 1* kiosk sa mogućnošću da skenira ID kartice, slika korisnika, uzima otisak prsta, skenira čekove i potvrđuje njihovu autentičnost, izdaje platne kartice sa deponovanom količinom novca prikazanoj na čeku i umanjenoj za malu proviziju omogućavajući svim korisnicima da koriste ATM terminal. U budućnosti se planira dodavanje opcija kao što je plaćanje u supermarketima, stanicama svih vidova prevoza i sl. Kiosk takođe, omogućava *OffLine* plaćanje ka 34 zemlje širom sveta.

Istraživanje javnosti od strane kompanije Diebold, Inc., na uzorku od 2000 ispitanika, po pitanju spremnosti ljudi na upotrebu biometrijske autentifikacije u bankarskom sektoru, dalo je sledeće rezultate: 72% smatra da bi upotreba biometrije kod ATM autentifikacije bio dobar potez svake banke, dok bi 68% ispitanika imalo pozitivnije mišljenje o svojoj finansijskoj instituciji kad bi na ovaj način povećala sigurnost.

Takođe, u decembru 2006. godine, kompanija NCR ponudila je tržištu biometrijsku tehnologiju otiska prsta kompanije *DigitalPersona Inc.* integrisanu u svoje POS (*point of sale*) terminale koji će omogućiti trgovcima da, koristeći autentifikaciju upotrebom otiska prsta, kreiraju zapis, jedinstven za svakog korisnika, podložan proveru koji će olakšati autentifikaciju i kontrolu pristupa POS terminalu, a samim tim i registrovati prisustvo zaposlenih. Time će se smanjiti najčešći problemi u maloprodajnim objektima koji se odnose na obmane sistema za kontrolu vremena i prisustva.

⁶ Džordž W. Buš, povodom imigracionih reformi, 15.5.2006.

2.2.3 Nemačka

Očekuje se da će do enormnog rasta "biometrijskog tržišta" doći do 2009. godine sa stopom rasta sa 12 miliona € (2004) na 377 miliona EUR" (2009). Glavnu ulogu u celoj priči vodiće vlada. U maju 2005. godine, nemački Gornji Dom parlamenta dozvolio je implementaciju tzv. *ePass*-a, tj. e-pasoša za sve nemačke državljane koji će sadržati biometrijske podatke. *ePass* je u upotrebi od novembra 2005. godine i sadrži čip u kojem se, za početak, nalazi digitalna slika vlasnikovog lica. Od marta 2007. godine, na čipu će takođe biti smešteni i otisci prstiju, po jedan sa obe ruke. Skenirana slika dužice oka predstavlja treći deo identifikacije koji će biti dodat u nekoj narednoj fazi. Jedan od razloga za ovakav pristup je, osim bezbednosti nemačkih državljana i američki rok za izdavanje biometrijskih pasoša u onim zemljama čiji su državljani oslobođeni traženja američke vize za ulazak u SAD. Kao dodatak, nemačka vlada je promenila proceduru i pravila za izdavanje viza onima koji žele da uđu u Nemačku u smislu da će svi oni koji imaju nameru da se u Nemačkoj zadrže duže od 90 dana morati da prođu novi biometrijski sistem registracije. Isto se odnosi i na one koji apliciraju za radnu vizu.

Nemačka je takođe jedna od prvih zemalja koja je implementirala biometrijsku tehnologiju u cilju zaštite nemačkih sportista na olimpijskim igrama u Atini 2004. godine. Svi akreditovani posetioci (takmičari, treneri, menadžeri i predstavnici medija) dobili su biometrijske ID kartice koje su im omogućile da uđu u nemački kamp.

Što se tiče nacionalnih biometrijskih ID kartica, dozvoljeno je da se u čip kartice učitaju biometrijski podaci ali se oni neće nalaziti i u centralnoj bazi podataka.

Jedna od karakterističnih upotreba biometrijske identifikacije u Nemačkoj je i identifikacija prepoznavanjem lica u mnogim nemačkim kockarnicama. Identifikacioni sistem *FaceSnap/FaceCheck* kompanije *Cross Match Technologies, Inc* putem specijalnih video kamera proverava svakog posetioca bez direktnog kontakta. Svaki sumnjivi-registrovani posetilac biva odbijen na ulazu.

2.2.4 Velika Britanija

Prošle godine (2006) je počeo da se realizuje plan razvoja Britanske nacionalne ID kartice zasnovane na biometriji sa ciljem da se sve postojeće kartice zamene u narednih 10-ak godina. Aktom *Identity Cards Act 2006* definisano je 50 kategorija podataka koje će **National Identity Register** (NIR, baza podataka sa ID kartica) moći da sadrži o svakom državljaninu, uključujući maksimalno deset otisaka prstiju, digitalizovanu sliku lica i dužice oka, trenutno i prethodna prebivališta na teritoriji Velike Britanije i izvan nje.

Za razliku od elektronskih pasoša (počeo da se izdaje od aprila 2006.), stvar sa biometrijskim ID karticama ide daleko teže. 21 od 25 zemalja EU imaju neki oblik ID kartice ali ni jedna nije biometrijska niti se podaci nalaze u jedinstvenoj bazi podataka. Za razliku od pasoša, u prvom periodu, kartica bi kao dodatak sadržala i otisak prsta. Velika Britanija bi bila tek 5. zemlja, pored zemalja pod nekadašnjom britanskom jurisdikcijom kao što su Kipar, Hong Kong, Malezija i Singapur, koja bi usvojila upotrebu ovakvih kartica u mirnodopsko vreme. Osnovni razlozi uvođenja biometrijskih ID kartica bi ovog puta bili borba protiv terorizma, ilegalnih imigranata i radnika kao i organizovanog kriminala. Smatra se da bi na ovaj način kriminalci bili sprečeni da koriste više identiteta iako je već došlo do kopiranja elektronskog pasoša u Nemačkoj i Holandiji.

Osnovni problemi sa kojim se suočavaju nadležni predstavljaju veoma visoki troškovi uvođenja novog sistema ID kartica. Zvanično procenjeni troškovi su oko 5.5 biliona funti za 10 godina odnosno 584 miliona godišnje dok nezavisni izvori procenjuju troškove na 12-18

milijardi funti s obzirom da je predviđena redovna zamena legitimacija svakih pet godina zbog delimične izmene biometrijskih informacija.

Jedan od javnih biometrijskih sistema koji je od skoro počeo da funkcionišen je tzv. *miSense*, biometrijski aerodromski sigurnosni sistem na londonskom aerodromu Heathrow. Sistem poseduje sigurnosnu tehnologiju (šifrovanje i zaštita baza podataka) kompanije *nCipher plc*, zasnovanu na otisku prsta, skeniranju lica i dužice oka. Cilj upotrebe sistema je pojednostavljivanje i ubrzanje prijave putnika kao i povećanje opšte sigurnosti. U probnom periodu, narednih nekoliko meseci, na letovima ka Hong Kongu i Dubaiu kompanijama *Cathay Pacific* i *Emirates* putnici će moći dobrovoljno da koriste sistem.

2.2.4.1 Kritike, poverenje i privatnost podataka

Pored visokih troškova, veliki problem je i veoma mala podrška javnosti.

Prema nekim istraživanjima 2003. godine, dok je još bila "borba protiv globalnog terorizma" u punoj snazi, 61% anketiranih je imalo pozitivan stav prema uvođenju biometrijskih legitimacija, 38% protiv i 1% neutralnih. Međutim, u julu 2006. godine, podrška je opala na svega 46%, dok je 51% anketiranih bilo protiv i 3 % neutralnih.

Časopis *Daily Telegraph*, 4. decembra 2006. godine izvršio je istraživanje na istu temu uz polovične rezultate: 50% ZA, 39 % PROTIV po pitanju uvođenja ovakvih legitimacija međutim, daleko je manje poverenje za jednu bazu podataka na nacionalnom nivou (41% ZA i 52% PROTIV). Samo je 11% anketiranih građana iskazalo poverenje u vladu kad je u pitanju zaštita privatnosti, a čak 3.12% građana je bilo spremno da bude lišeno slobode po cenu da ne prihvati novu ID karticu.

U zajednici postoji i veoma veliko podozrenje kad se govori o očuvanju privatnosti. Osnovni problem je u, kao što je prethodno prikazano, mali procenat poverenja u policiju, a takođe postoji i bojazan da će policija moći da evidentira svaki npr. ulazak u bilo koju zgradu gde se tražila identifikacija karticom odnosno, da će kontrolisati svaki korak. Isto tako, NIR bazi, koja će biti praktično neograničenog kapaciteta, moći će da pristupa 265 vladinih odeljenja, 48000 akreditovanih organizacija, a mesto u njoj će naći i 163 miliona osoba što predstavlja atraktivnu metu hakerima jer je svaki sistem, koji kotroliše čovek, podložan proboju.

2.2.5 Francuska

Težnje vlade su da svi francuski građani poseduju ovakve kartice tokom 2007. godine. Beskontaktni čip na kartici će osim osnovnih podataka sadržati i otisak prsta i sliku. Kombinacija ova dva podatka nije korišćena još od nekih prošlih vremena. Od II sv.rata do 1987. osnovni lični podaci nisu bili centralno čuvani, a čak i posle toga, izmena adrese prebivališta nije morala nužno da se prijavi s obzirom da ID kartica nije bila obavezna.

Od 1. juna 2005. godine, *Air France* uveo je u upotrebu sistem biometrijske (otisak prsta) identifikacije na aerodromu *Šarl De Gol* u Parizu na terminalu 2F. Projekat pod nazivom "*Pegaz* (Pegasus)" je na dobrovoljnoj bazi i njegov cilj je ubrzanje granične kontrole i protoka ljudi registrovanih za isti. Projekat je organizovan u kooperaciji sa graničnom policijom sa dozvolom CNIL (Commission nationale de l'informatique et des libertés).

2.2.5.1 Kritike, poverenje i privatnost podataka

Na konferenciji za novinare održanoj 26. maja 2005. godine u Parizu, šest organizacija je diglo glas protiv uvođenja biometrijske obavezne ID kartice. Udruženja pravnika, sudija, liga

za ljudska prava (*Human Rights League*, LDH), IRIS-član EDRI grupe (*European Digital Rights*), DELIS (koalicija više od 60 udruženja za odbranu privatnosti i zaštitu ličnih podataka) i francuska asocijacija demokratskih advokata započeli su kampanju protiv poretanja projekta, pod pokroviteljstvom francuskog MUP-a, uvođenja obaveznih biometrijskih ID kartica.. Osnovna kritika je bila ta da francuska vlada želi da izgradi centralni sistem koji će sadržati biometrijske podatke kao i identifikacione podatke, socijalna prava i možda čak i privatne transakcije građana koji će moći da se koriste bez njihovog znanja. Takođe se jedna od kritika odnosila i na obmanjivanje javnosti pričom da se prema ICAO međunarodnom standardu od 13. decembra 2004. zahteva od EU da uvede biometrijske ID kartice iako se to odnosilo samo na pasoše i putna dokumenta.

2.2.6 Australija

Svi budući posetioци Australije mogli bi uskoro postati “žrtve” biometrijske autentifikacije koja će obezbediti vezu između pasoša i izdate vize. Za sada su već neki biometrijski podaci aplikacija za vize sakupljeni od strane imigracionog odeljenja. Biometrijski pasoši predstavljeni su u oktobru 2005. godine i od biometrijskih informacija sadrže samo digitalnu sliku.

2.2.7 Singapur



Slika 3: Pay by Touch terminal

Immigration & Checkpoints Authority (ICA) služba je u avgustu 2006. godine predstavila biometrijski pasoš tzv. *BioPass* čime je ispunjen rok za *US Visa Waiver Programme* koji podrazumeva da sve zemlje od kojih se ne zahtevaju vize za ulazak u SAD moraju do 26. oktobra 2006. godine izdaju biometrijske pasoše.

U novembru 2006. godine, singapurska *Citi* banka omogućila je upotrebu, nakon dugog ispitivanja sigurnosti, otiska prsta kao sredstva za plaćanje vlasnicima platinaste kreditne kartice *Citi* banke. Klijenti će u nekoliko filijala banke moći da registruju svoj otisak prsta kao i digitalnu sliku i 7-cifrenu lozinku kojom će autorizovati svaku kasniju transakciju [70]. Servis biometrijske kreditne kartice razvijen od strane *Citi* banke i *Pay by Touch*

postavlja novi standard za brzinu, udobnost i sigurnost⁷. Na slici 3. prikazan je novi terminal kompanije *Pay by Touch* [72].

2.2.8 Izrael

Biometrija se u Izraelu koristi intenzivno već nekoliko godina. Na graničnim prelazima ka oblastima Gaze i Zapadne obale, dozvoljeno je da u Izrael uđu samo autorizovani Palestinci za koje se smatra da ih i do 90000 (u ”špicu” i do 15000/h) svakodnevno prelazi u Izrael da radi. Svaki od njih poseduje ID karticu izdatu od strane Izraelskih službi zaduženih za registraciju kao i od vojske. ID kartica predstavlja pametnu karticu koja sadrži biometrijske podatke kao što su: otisci prstiju, geometriju lica i dlana. Takođe, na kartici se nalazi i slika koja je u digitalnom obliku smeštena i u čip.

⁷ Džon Rodžers, osnivač, predsednik i CEO, Pay by Touch na konferenciji za štampu

Aerodrom Ben Gurion u Tel Avivu ima najbrži sisem prijave putnika zasnovan na upotrebi pametnih kartica koji sadrži otiske prstiju i dlana. Kompletna procedura provere traje oko 10s.

Imigraciona policija na aerodromu koristi sistem registracije stranih radnika koji je zasnovan na slici, otiscima prstiju i šablonu geometrije lica, a ne podatke iz pasoša pridošlice. Postoje mobilni sistemi koji policiji omogućavaju proveru osobe u svakom trenutku.

2.2.9 Japan

Nekoliko banaka u Japanu razvilo je sistem autentifikacije putem dlana na svojim ATM uređajima. Ova tehnologija, razvijena od strane kompanije *Fujitsu*, ima za cilj da smanji pogrešno odbacivanje (na oko 0.01%) kao i prihvatanje pogrešnog pina (manje od 0.00008%).

Finansijske institucije u Japanu trenutno prihvataju autentifikaciju ili putem rasporeda vena prsta ili dlana odakle sledi da će i ATM uređaji biti kompatibilni samo sa jednim oblikom autentifikacije što onemogućava njihovu širu upotrebu te se teži izradi pametnih kartica kompatibilnim sa oba metoda.

Japanska bankarska asocijacija (JBA) izvršila je reviziju svoje *IC Cash Card* specifikacije u martu mesecu u cilju otvaranja mogućnosti za takve pametne kartice koje bi prihvatile oba metoda autentifikacije.

Kao rezultat svega, početkom godine, *Dai Nippon Printing Co. Ltd.* (DNP) kompanija razvila je pametnu platnu karticu kompatibilnu sa sistemom za autentifikaciju putem rasporeda vena prsta i dlana usled čega se nekoliko finansijskih institucija opredelilo za ove kartice što je dovelo do toga da je kompanija drastično pojačala svoje marketinške akcije ka ostalim finansijskim institucijama u Japanu (trenutno su stigle narudžbine od oko 100 institucija sa težnjom ka daljem porastu tražnje). Ove kartice dolaze kao MULTOS™, Java Card™ ili kao *dual-interface* multi-aplikativne kartice sa interfejsom koji može da prihvati oba OS. Takođe, predviđeno je da se karticama mogu dodati još neke funkcije kao što je generisanje trenutnih lozinki koje povećavaju sigurnost kod e-bankarstva.

2.2.10 Malezija

RFID tagovi prvi put su u pasošima korišćeni od 1998. godine u Maleziji. Malezijski e-pasoši sadržali su podatke o prethodnim putovanjima (vreme i mesto ulazaka i izlazaka iz zemlje).

2.2.11 Jordan

Rukovodstvo civilnog vazduhoplovstva Jordana dalo je dozvolu za početak projekta *eGATE* koji će omogućiti brži protok putnika u avio saobraćaju. Projekat se zasniva na upotrebi pametnih kartica koje će sadržati „istoriju“ putnika kao i njegov otisak prsta u cilju potvrde identiteta.

* Većina prethodno navedenih podataka preuzeta je sa sajta <http://en.wikipedia.org> [74]

2.2.12 Srbija

Novu ličnu kartu sa ugrađenim čipom građani Srbije trebali su, nakon nekoliko odlaganja, da dobiju od kraja januara 2007. godine. Međutim rok je opet pomeren. Predviđeno je da zamena starih ličnih karti traje pet godina. Lična karta će biti bazirana na tehnologiji višenamenskih PKI pametnih kartica sa isto tako primenljivim operativnim sistemom i neophodnim hardverskim i softverskim mehanizmima za zaštitu.

Prema ranijim navodima nakon donošenja Zakona o ličnoj karti, početkom 2007. godine, trebala je biti započeta zamena starih ličnih karata. Brojni su faktori nekoliko puta odlagali uvođenje dokumenata sa čipom. Na odlaganja je uticalo nemanje zakonske regulative, novac, ali i odliv stručnih kadrova. Nadležni odbijaju svaku mogućnost da će novim dokumentima, preko čipa, država, ali i pojedinci, pratiti građane i u svakom trenutku znati gde se ko nalazi. Čip može da se locira samo na čitaču, a i to se aktivira tek kada vlasnik ukuca PIN kod. Prema tvrdnjama istih, svi podaci o građanima biće bezbedniji nego danas: „*Nema šta da se zloupotrebi jer građani neće davati nikakve podatke osim koje država već ima o njima što je i regulisano zakonom*“. Na novim, kao i na starim dokumentima, biće ime, prezime, JMBG, mesto rođenja, državljanstvo, dok će u čipu, zbog eventualnih promena biti samo mesto prebivališta. U čip neće ulaziti nikakve lične stvari o vlasnicima dokumenta niti će ih prilikom predaje dokumenata, kao i do sada, na šalterima policije pitati o privatnim stvarima. Kartice će biti štampane na uređajima u Zavodu za izradu novčanica, a gotovo ih je nemoguće falsifikovati. Imaće višestruku vidljivu, ali i nevidljivu zaštitu. Za zaštitu će se koristiti UV štampa, optički promenljive boje, kinegrami... U središtu kinegrama su vrlo složeni sistemi zaštite. I da neko uspe da pronađe sve vidljive zaštite, ne bi mogao da napravi karticu. Takođe, bezbednosni akcenat stavljen je i na centralizovanu bazu podataka. Sve će biti digitalizovano. Tu će ulaziti samo provereni zaposleni i to tek posle prolaska stroge bezbednosne procedure – od legitimisanja do otisaka prstom kojim se otvaraju vrata. Sve će biti potpuno izolovano, snimaće se video i tonski, a svaki ulazak u sistem biće registrovan. Kompiuterski sistem, uz pomoć koga će se izrađivati nova dokumenta, potpuno je izolovan i radi samo u srpskoj policiji. Nema dodira sa spoljnim korisnicima niti bojazni od upada hakera u sistem.

2.2.12.1 Kritike, poverenje, privatnost podataka

Osnovne kritike povodom izdavanja biometrijskih ličnih karata u Srbiji ogledaju se u deset tačaka tzv. Žičkog sipmोजijuma održanog 26. marta 2005. godine u Kraljevu, prvog stručnog skupa koji je obradio problematiku uvođenja biometrijskih ličnih karti na nacionalnom nivou. Zaključci su sledeći:

1. Biometrijske lične karte kao obavezujući dokument na nacionalnom nivou su uvedene u nekoliko država sveta, uglavnom dalekoistočnih. U Evropskoj uniji velika većina zemalja nema takve lične karte, one nisu uslov za ulazak u Evropsku uniju niti njihovo uvođenje doprinosi bržem ulasku. Očigledan primer je Slovenija, koja pre ulaska u EU nije uvela takve karte (iako je postojala mogućnost), već obične plastične sa višim nivoom zaštite.

2. Zemlje koje su planirale ili planiraju da uvođe biometrijske lične karte suočene su sa otporom akademske javnosti i društvene zajednice uopšte. U Velikoj Britaniji je pokušaj uvođenja biometrijskih ličnih karti doveo do višemesečnih debata u parlamentu i burnih reakcija akademskih građana, dok je u Kanadi od strane zvanične parlamentarne komisije odbačen na neodređeno vreme, kao skup, neopravdan i potencijalno opasan.

3. Svetski stručni organi, kakav je Zajednički komitet za ljudska prava britanske vlade, procenjuju da je projekat uvođenja biometrijskih ličnih karti na nacionalnom nivou potencijalno u koliziji sa evropskom Konvencijom o ljudskim pravima, a zvanične studije o izvodljivosti pokazuju da takve lične karte ne garantuju stoprocentnu pouzdanost i autentičnost. Sudovi nekih zemalja (Japan i Tajvan) su reagovali sa presudama da projekat biometrijskih ličnih karti krši prava građana i odredbe Ustava, u skladu sa čime su doneti i suspenzivni akti.

4. U Srbiji je projekat nabavke opreme za izradu biometrijskih ličnih karti postao aktuelan krajem 2003. godine. Srbija je jedinstven primer da je prvo kupljena oprema za biometrijsku identifikaciju građana, a posle toga (tačnije posle tri godine) pokrenuta skupštinska procedura

za predlog zakona o biometrijskim ličnim kartama, zbog čega je sebe svrstala u red totalitarnih država sa voluntarističkim pravnim uređenjem.

5. Američka firma koja je MUP-u Srbije prodala sistem za biometrijsku identifikaciju građana ima posebne ugovore sa američkom vojskom i centralno obaveštajnom službom (CIA), te niko ne može da garantuje da ne postoji mogućnost odliva podataka stranim službama. Takođe je osnovano pretpostaviti da pomenute službe veoma lako mogu kreirati lažne lične karte za svoje potrebe, koje će od strane našeg računarskog sistema biti prepoznate kao potpuno validne. Indikativna je činjenica da u Americi državna uprava nije ni pokušala sa uvođenjem biometrijskih ličnih karti među svojim stanovništvom, jer bi to sigurno dovelo do velikog otpora javnosti.

6. Nije tražena masovna saglasnost građana Srbije za proširivanje baze podataka koju će država o njima voditi niti su organizovane javne debate i diskusije po tom pitanju.

7. Projekat direktno ugrožava privatnost građana kao jedno od fundamentalnih ličnih prava današnjice i otvara prostor za elektronski šifrovane tajne arhive.

8. Birokratski aparat dobija mogućnost gotovo trenutnog manipulisanja ogromnim brojem podataka preko centralizovane baze i prodaje delova baze trećim licima.

9. Zlonamerni upadi spolja ili namerno ispravljanje centralizovane baze iznutra nose ogromnu opasnost po integritet ličnosti koje su njima obuhvaćene.

10. Usvajanje ovog projekta u budućnosti vodi ka mnogo totalitarnijim konceptima sjedinjavanja svih dokumenata u jedan, čime bi se izbrisala anonimnost tokova novca i otvorio put totalnom nadzoru države nad pojedincem.

Kao posledica sve većih kritika javnosti [64], početkom 2007. godine, objavljeno je da će lične karte sa biometrijskim čipom dobiti oni koji to žele, dok će ostali dobiti osnovne elektronske identifikacione kartice.

U prvoj fazi predviđena je zamena samo lične karte, a potom i saobraćajne i vozačke dozvole, kao i dozvola za posedovanje i nošenje oružja. Na novi izgled sačekajte i pasoš, za čiju izradu nedostaju mašine za elektronsku personalizaciju kao i Zakon o putnoj ispravi. Biometrijske identifikacije su sprovedene u još nekoliko firmi gde se na taj način registruju prisustva zaposlenih. Kao primer, navešćemo još primer iz našeg okruženja. U GAK „*Narodni front*” instaliran je čitač otisaka prstiju kako bi se sprečila zloupotreba radnog vremena. Dok je magnetnu karticu moguće dati kolegi da je provuče kroz čitač kad provlači i svoju, s otiskom prsta to više nije moguće. Naravno, odmah su počele priče o tome kako je taj aparat opasan po zdravlje jer zrači (iz navedenog principa rada čitača otisaka vidi se da nikakvog zračenja nema). Jasno je da ovaj uređaj može da smeta samo onima koji ne žele da rade jer je sistem sada nemoguće prevariti. Inače, sistem čitača otiska prstiju uspešno se koristi i u RTS-u, korporaciji *Lola* i preduzeću *Jaffa* iz Crvenke.

3. Biometrijski sistemi

Biometrija (engl. *Biometrics*) je opšti izraz, koji se koristi alternativno da bi se opisala karakteristika ili proces.

Kada se koristi za opis **karakteristike**, izraz označava merljivu biološku (anatomsku ili fiziološku) karakteristiku ili karakteristiku ponašanja, koja se može koristiti za automatsko prepoznavanje.

U slučaju da se koristi za opis **procesa**, izraz označava automatizovan metod za prepoznavanje osoba, baziran na biološkim (anatomskim ili fiziološkim) karakteristikama ili karakteristikama ponašanja.

Biometrijski sistemi su razvijani i testirani poslednjih nekoliko decenija, ali su tek odnedavno u javnoj upotrebi, zbog visokog profila aplikacija. Njihova primena raste iz dana u dan. Osim u državnim institucijama, i u mnogim kompanijama je otpočeto sa primenom biometrijskih sistema za zaštitu osetljivih zona, unpređenje korisničkih servisa i sl. Na primer, kompanija *Disney World* koristi biometrijski sistem za sezonske karte, kako bi uprostila ulazak u svoje parkove i bila sigurna da se karta koristi od strane osobe kojoj je izdata. Postoji mnoštvo aplikacija biometrijskih sistema i za sada je težište postavljeno na kontrolu fizičkog i logičkog pristupa. Oblasti u kojima se koriste su:

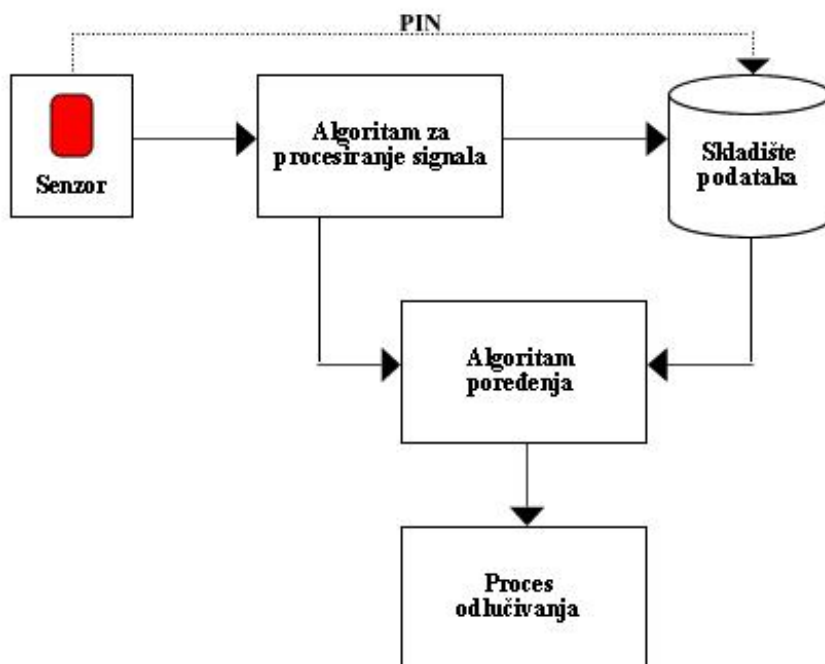
- Bankarsko/finansijski servisi /ATM, terminali za plaćanje...);
- IT sigurnost (prijava na sistem, Internet transakcije...);
- Zdravstvena zaštita (privatnost podataka...);
- Imigracija (kontrola granica...);
- Red i zakon (ID kartice, glasanje, kontrola upotrebe oružja...);
- Kontrola ulaza;
- Telekomunikacije;
- Evidencija vremena prisustva (firme, škole...).

Biometrijski sistem je, u suštini sistem za prepoznavanje prema uzorku (*engl. Pattern Recognition System*), koji prepoznavanje osobe vrši na osnovu autentičnosti specifičnih bioloških karakteristika i/ili karakteristika ponašanja, koje već poseduje o toj osobi.

Najvažnije pitanje prilikom izgradnje biometrijskog sistema je na koji način će osoba biti prepoznata. U zavisnosti od konteksta aplikacije, ovi sistemi se dele na verifikacione i identifikacione.

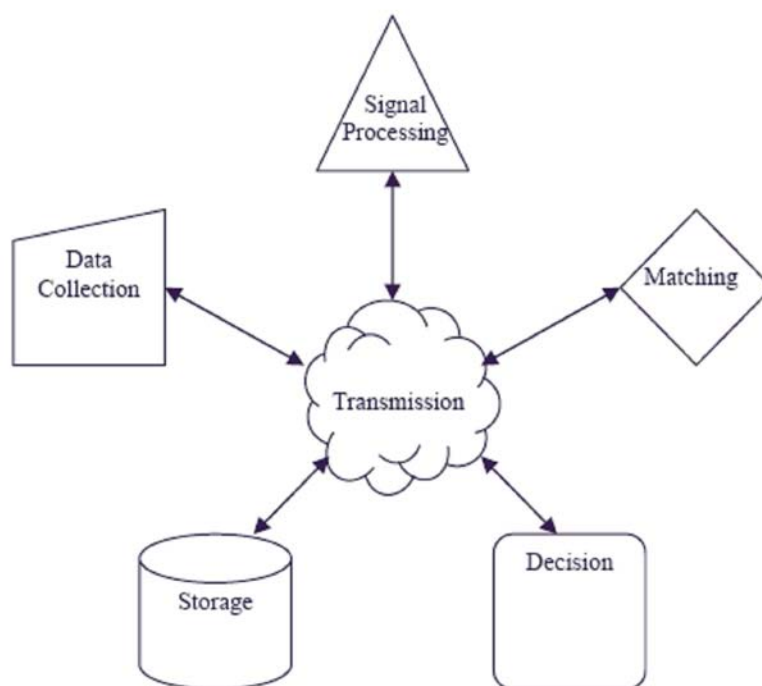
Tipičan biometrijski sistem (slika 4) se sastoji od pet integrisanih komponenti:

- **Senzora**, koji se koristi za prikupljanje podataka i konvertovanje informacija u digitalni oblik;
- **Algoritma za obradu signala**, koji izvršavaju kontrolu kvaliteta i razvijaju biometrijski šablon;
- **Komponenta za skladištenje podataka**, koja skladište informacije, sa kojima će se novi biometrijski šabloni biti poređeni;
- **Algoritma poređenja**, kojim se upoređuju novi biometrijski šabloni sa jednim ili više već postojećih šablona u skladištu podataka;
- **Procesa odlučivanja**, automatizovanog ili podpomognutog od strane čoveka, koji koristi rezultate algoritma poređenja, za donošenje sistemskih odluka.



Slika 4: Opšti model biometrijskog sistema

Na slici 5 prikazan je opšti ANSI model biometrijskog sistema [67].

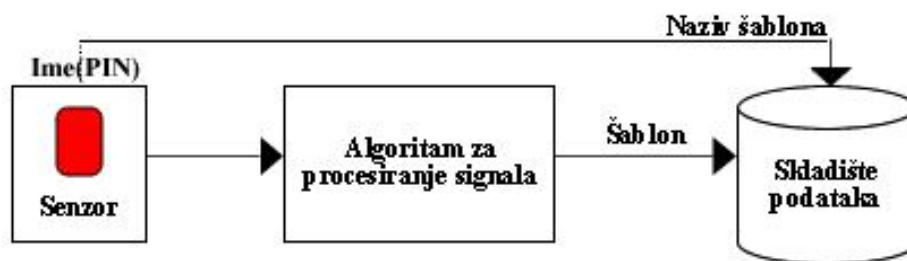


Slika 5: ANSI X9.84 opšti model biometrijskog sistema

Prvi korak u korišćenju biometrijskog sistema je upis biometrijskog šablona (slika 6) određene osobe u bazu podataka sistema. Tokom faze upisa u sistem, biometrijske karakteristike pojedinca se prvo snimaju na biometrijskom senzoru, da bi se dobila njihova digitalna reprezentacija. Preko algoritma za obradu signala, kontroliše se kvalitet skeniranja i razvija biometrijski šablon, koji se upisuje u bazu podataka sistema (skladište podataka).

Zavisno od aplikacije, šablon može biti smešten u [67]:

- Centralnoj bazi podataka;
- Lokalnoj bazi podataka;
- Na portabl uređaju (pametna kartica koja se izdaje osobi koja se upisuje);
- Na senzoru.



Slika 6: Upis biometrijskog šablona

Prednosti i mane lokacija za smeštanje šablona su sledeće:

Centralna baza podataka

Prednost centralne baze biometrijskih podataka u sistemima gde se korisnik može autentifikovati sa više različitih lokacija je velika jer je baza povezana sa mnoštvom senzora omogućavajući time udaljenu autentifikaciju. Takođe, daleko je jednostavnije i upravljanje podacima koji se nalaze na jedinstvenoj lokaciji. Međutim, centralna baza je uvek atraktivna meta za napadače naročito ako nije dovoljno zaštićena šifrovanjem. Kompromitacijom baze, kompromitovani su i svi šabloni smešteni u njoj.

Lokalna baza podataka

Predstavlja arhitekturu koja podrazumeva smeštanje baze na lokalni računar na koji je priključen biometrijski senzor. Na taj način daleko se sužava mogućnost napada sa strane ali isto tako ne postoji mogućnost udaljene autentifikacije osim ako se kopija korisnikovog šablona ne nalazi na svakoj pristupnoj tački, što opet izaziva redudansu podataka kao i komplikovano upravljanje.

Portabl uređaj

Smeštanje podataka na portabl uređaju, kao što je pametna kartica, izgleda kao najbolje rešenje. Sam korisnik, tj. vlasnik kartice, odgovoran je za sigurnost i privatnost svojih podataka, a kako se podaci ne prenose mrežom nema ni tolike opasnosti upada sa strane. Nedostatak je nešto veća cena implementacije jer svaki senzor mora biti opremljen čitačem kartica. Isto tako, administrator ne može biti siguran da li možda postoji duplikat kartice (korisnik može prijaviti isti otisak prsta pod dva različita identiteta) što se može rešiti samo rigoroznom kontrolom pri izdavanju kartice.

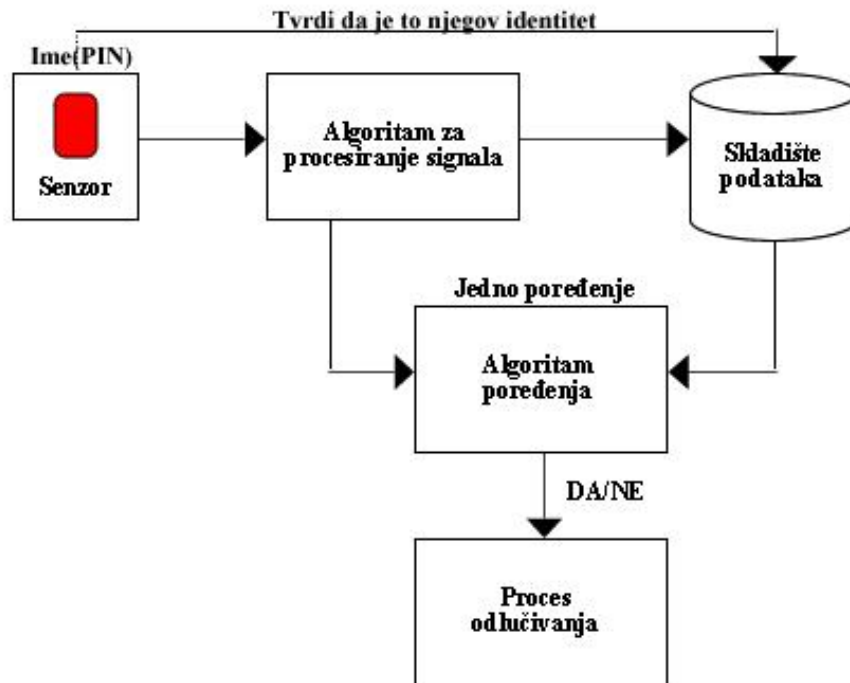
Senzor

Smeštanjem šablona na senzor omogućava se veoma brzo dobijanje odgovora sistema ali se ovaj sistem ne može koristiti za autentifikaciju sa više lokacija. Isto tako, ako je senzor malih dimenzija i nije obezbeđen, može biti ukraden čime dolazi do kompromitacije

podataka u njemu, odnosno šablona. Sistem se pre svega koristi kad korisnik koristi uvek isti senzor za fizički ili logički pristup

3.1 Koncept biometrijske verifikacije

Verifikacija (slika 7) obavlja se na taj način što korisnik unosi svoje ime ili, najčešće, PIN, kojim tvrdi da je to njegov identitet. Zatim se korisniku uzimaju biometrijske karakteristike i pretvaraju se u digitalnu reprezentaciju (šablon). Ovaj novi šablon se, preko algoritma za poređenje, poredi sa već postojećim (povučenim iz baze podataka na osnovu PIN-a).



Slika 7: Proces verifikacije

Drugim rečima, osnovni koraci uključeni u biometrijsku verifikaciju su [69]:

- Uzimanje slike – koriste se skeneri dostupni na tržištu;
- Prepoznavanje slike – koriste se standardni algoritmi;
- Kreiranje šablona – koriste se standardni algoritmi;
- Poređenje – koriste se namenske aplikacije i standardni algoritmi.

3.1.1 Prepoznavanje otiska

Prepoznavanje otiska je takođe poznato i pod nazivom “prikupljanje slike”. U ovom koraku, korisnik postavlja svoj prst na skener pri čemu se prikupe brojne slike njegovog otiska. Najbitnije je obuhvatiti, pre svega, središnji deo otiska s obzirom da on sadrži najveći broj korisnih informacija. Sve prikupljene slike se konvertuju u crno-bele verzije.

3.1.1.1 Minutiae

Otisak se sastoji od mnoštva brazdi i dolina koji predstavljaju osnovu za linije, lukove, uvojke i slične oblike koje su vidljivi na otisku. Brazde i doline se često prekidaju i nastavljaju i to predstavlja tzv "*minutiae*" koji čine jedinstvenost svakog otiska. Postoje dva tipa:

- Krajevi brazdi (mesto gde se brazde završavaju);
- Grananje (mesto gde od jedne brazde nastaju dva).

3.1.2 Kreiranje šablona

Vrši se na osnovu jedinstvenih oblika nađenih u "*minutiae*". Ono što čini svaki šablon su lokacija, pozicija, tip i kvalitet "*minutiae*". Svaka tehnologija prepoznavanja otisaka ima svoj skup algoritama za kreiranje i poređenje šablona.

3.1.3 Poređenje šablona

Sistem će pokušati ili da verifikuje ili da identifikuje osobu poredeći dobijen otisak sa prthodno sačuvanim šablonom.

Svaka aplikacija za autentifikaciju sa biometrijskim sistemom povezana je tzv. BioAPI ili BAPI koji predstavlja skup funkcija, pisanih pretežno u C programskom jeziku, koje treba da omoguće sve osnovne biometrijske funkcionalnosti kao što su:

- Prijava korisnika;
- Autentifikaciju;
- Pretragu identiteta.

Lokacija za poređenje šablona sa unetim biometrijskim podatkom je veoma važan faktor koji utiče na performanse sistema. Lokacije se mogu klasifikovati u četiri kategorije:

- Poređenje na centralnom serveru;
- Poređenje na lokalnom računaru;
- Poređenje na senzoru;
- Poređenje na pametnoj kartici.

Poređenje na centralnom serveru

Predstavlja dobru opciju kad su šabloni smešteni u centralnoj bazi podataka. Malu zabrinutost predstavlja mogućnost upada u mrežnu komunikaciju između servera i senzora.

Poređenje na lokalnom računaru

Može funkcionisati sa centralnim i lokalnim bazama s tim da se bolje performanse dobijaju u drugom slučaju.

Poređenje na senzoru

Sistem obezbeđuje brz rad i visok nivo sigurnosti iz razloga izolovanosti istog i nepostojanja komunikacije sa spoljnim svetom.

Poređenje na pametnoj kartici

Mehanizam obezbeđuje kompletnu sigurnost s obzirom da je sistem izolovan. Jedina slabost koja se može javiti je komunikacija između čitača kartice i nje same.

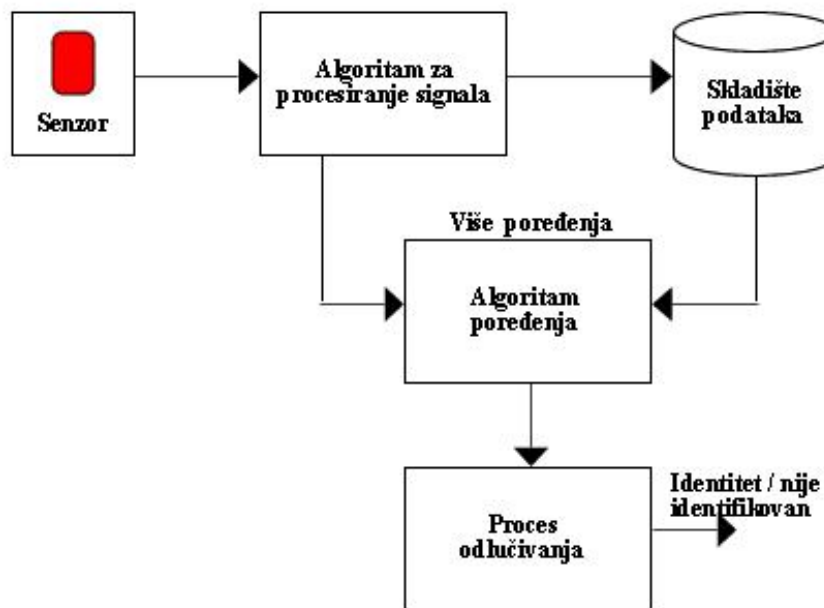
3.2 Koncept biometrijske identifikacije

U slučaju **identifikacije** (slika 8), osoba ne unosi svoj PIN. Sistem poredi uzete biometrijske karakteristike sa šablonima svih osoba upisanih u bazu podataka. Kao izlaz iz procesa identifikacije, dobija se identitet upisane osobe ili upozorenje da osoba nije identifikovana. Ovakav način identifikacije je veoma skup i zahteva mnogo računarskog vremena, pa se u tu svrhu koriste različite tehnike klasifikacije i indeksiranja, kako bi se dobio limitirani broj šablona, koji će se porediti sa ulaznim šablonom.

Biometrijski sistemi mogu da rade u *OnLine* i *OffLine* načinu rada.

OnLine sistemi zahtevaju brzo prepoznavanje i trenutni odgovor (npr. *LogOn* operacija na računaru). Ovi sistemi su, tipično, potpuno automatizovani, od senzora do procesa odlučivanja.

OffLine sistemi ne zahtevaju da prepoznavanje bude završeno odmah i dozvoljen je duži period odziva sistema. Iz ovih razloga, oni su obično poluautomatizovani, zahtevaju nadzor kod upisa biometrijskih podataka, manuelnu kontrolu kvaliteta, a algoritam poređenja može dati listu mogućih kandidata, na osnovu koje će eksperti doneti konačnu (ljudsku, a ne mašinsku) odluku. Ovi sistemi se obično koriste u forenzičkim i kriminološkim aplikacijama.



Slika 8: Proces identifikacije

Aplikacije koje se koriste u biometriji mogu da rade u pozitivnom ili negativnom režimu prepoznavanja:

- **Pozitivan režim prepoznavanja** - sistem utvrđuje da li je osoba ona za koju se (implicitno ili eksplicitno) predstavlja. Svrha pozitivnog prepoznavanja je da spreči više ljudi da koriste isti identitet.
- **Negativan režim prepoznavanja** - sistem utvrđuje da li je osoba ona za koju tvrdi da nije. Svrha ovog načina je da spreči jednu osobu da koristi više identiteta. Sistem je opširnije opisan na strani 8.

Tradicionalni metodi autentifikacije korisnika, kao što su lozinka, PIN i tokeni mogu da rade samo u pozitivnom režimu. Negativni režim se može uspostaviti samo biometrijom. Aplikacije sa pozitivnim režima prepoznavanja mogu da izvršavaju i verifikacione i identifikacione zadatke, dok aplikacije sa negativnim režimom prepoznavanja ne mogu da izvršavaju verifikacione zadatke.

3.3 Performanse biometrijskih sistema

Performanse biometrijskih sistema se mere, kvantifikuju i izražavaju korišćenjem različitih vrsta parametara. Razlikuju se performanse i greške koje se događaju u biometrijskim sistemima tokom procesa upisa, verifikacije i identifikacije.

3.3.1 Performanse i greške u procesu upisa

Tokom procesa upisa, može doći do teškoća kod prikupljanja podataka za neke osobe. Ove teškoće mogu biti kvantifikovane parametrima koji se u literaturi nazivaju FTA (eng. *Failure to Acquire* – greška kod uzimanja podataka) i FTE (eng. *Failure to Enroll* – greška kod upisa).

- **FTA** – Označava procenat korisnika za koje sistem nije u mogućnosti da prezentuje korisne biometrijske uzorke tokom procesa upisa. FTA pokriva FTE i kvalitativno prihvatanje biometrijskih šablona.
- **FTE** - Predstavlja procenat korisnika za koje sistem nije u mogućnosti da generiše šablon dovoljnog kvaliteta za upis, zbog limita tehnologije.

Za kvantifikaciju procesa upisa, koristi se i **TTE** (eng. *Time to Enroll*) pokazatelj, koji označava trajanje procesa upisa od uzimanja biometrijskih osobina do kreiranja šablona.

3.3.2 Performanse i greške u procesu verifikacije

Tokom procesa verifikacije vrši se poređenje preuzetih biometrijskih karakteristika i već uskladištenog šablona, za određenu osobu. Perfektno poređenje nikada nije ostvareno ni u jednom sistemu, jer na proces utiču različite okolnosti, od uslova upisa do interne varijabilnosti u uređajima. U tabeli 1, prikazan je rezultat istraživanja procenta greške koji se javljaju kod najčešće korišćenih biometrijskih osobina.

	Test	Parametar	Pogrešno odbijanje	Pogrešno prihvatanje
Otisak prsta	FVC 2004 [2]	Veliko deformisanje kože, rotacija prsta	2%	2%
	F _p VTE 2003 [3]	Zvanični podatak	0.1%	1%
Crte lica	FRVT 2002 [4]	Izmena osvetljenja	10%	1%
Glas	NIST 2004 [5]	Nezavisan tekst na više jezika	5-10%	2-5%

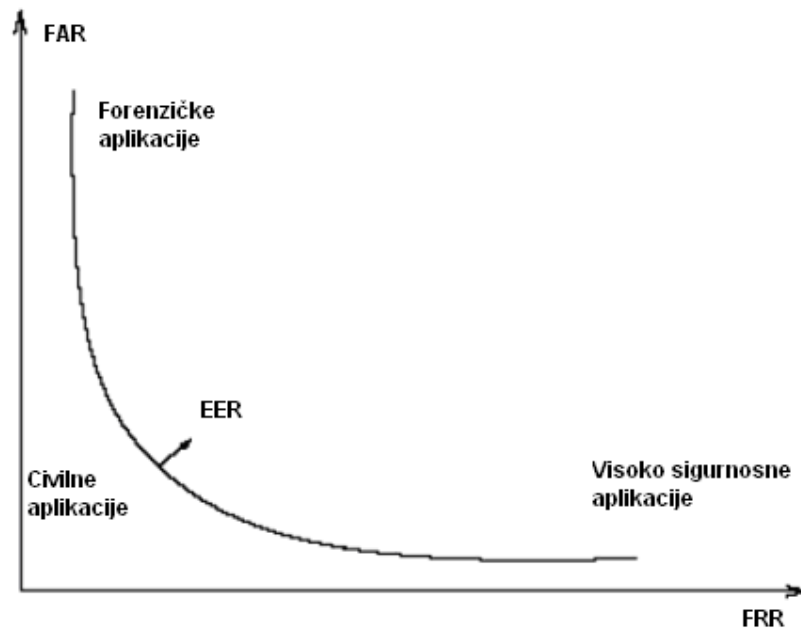
Tabela 1: Greške kod najčešćih biometrijskih karakteristika

Kako šablon i biometrijski uzorci nikada nisu isti, sistem mora da kvantifikuje i proceni sličnost između njih i da, na osnovu određenih parametara, donese odluku o prihvatanju, odnosno neprihvatanju. Rezultat poređenja (eng. *matching score*) označava se sa s i vrednost mu je u intervalu $[0,1]$. Sistemske odluke se donose na osnovu vrednosti koja se naziva **threshold** i označava se sa t , tako što su vrednosti iznad t prihvatljive (prepoznavanje uspešno), a vrednosti ispod t neprihvatljive.

Rezultati odlučivanja mogu biti neadekvatni, tj. sistem može da generiše dve vrste grešaka tokom odlučivanja, koje se opisuju pokazateljima [63]:

- **FRR** (eng. *False Rejection Rate* – greška odbijanja), poznata i kao greška I vrste. Trebala bi biti što manja.
- **FAR** (eng. *False Acceptance Rate* – greška prihvatanja), poznata i kao greška II vrste. Trebala bi biti što manja.
- **EER** (eng. *Equal Error Rate*), predstavlja vezu između FAR i FRR odnosno, tačku preseka FAR i FRR. Trebalo bi biti što manja što oslikava dobar balans osetljivosti sistema. EER je vrednost *threshold*-a na mestu gde su FRR i FAR ekvivalentni. Manja vrednost EER donosi bolje performanse.

Odnosi između navedenih grešaka prikazani su dijagramom na slici 9.



Slika 9: Odnos između FAR, FRR i EER

Ove greške su karakteristične za pozitivan režim rada, kada se korisnik, implicitno ili eksplicitno, predstavlja. U negativnom režimu rada (kada se korisnik ne predstavlja) pojavljuju se greške, koje se opisuju parametrima:

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

Biometrijski verifikacioni problem može biti formulisan na sledeći način:

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

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

$H_1: I = T$, ulaz odgovara šablonu.

Asocirane odluke u ovom slučaju su:

D_0 : Osoba nije ona za koju tvrdi da jeste

D_1 : Osoba je ona za koju tvrdi da jeste

Proces verifikacije uključuje poređenje T i I korišćenjem mere približnosti (eng. *similarity measure*) $s(T, I)$. Ako je rezultat poređenja manji od *threshold*-a (t), tada se smatra da je D_0 tačno. U protivnom, prihvata se D_1 .

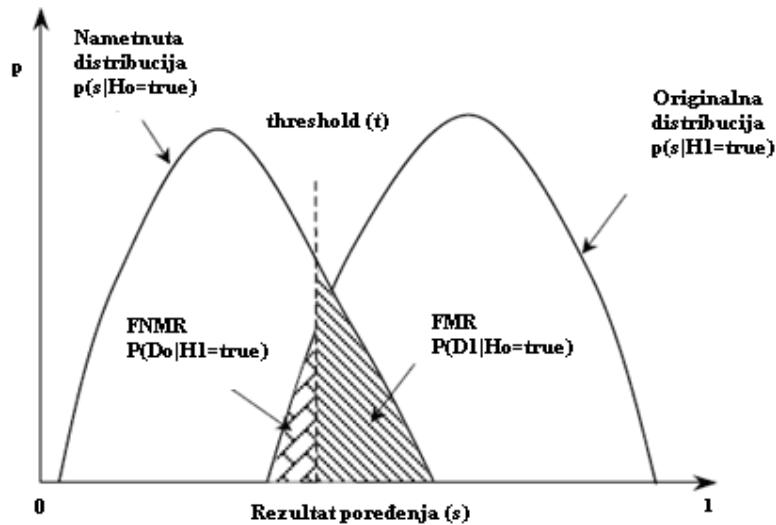
Prilikom testiranja hipoteza može doći do dve vrste grešaka:

- Greška I vrste – *False Match* – kada se donese odluka D_1 , a tačna je hipoteza H_0
- Greška II vrste – *False Non-Match* – kada se donese odluka D_0 , a tačna je H_1

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

$$\begin{aligned} \text{FMR} &= P(D_1 | H_0 = \text{True}) \\ \text{FNMR} &= P(D_0 | H_1 = \text{True}) \end{aligned} \quad [1]$$

Da bi se procenila tačnost biometrijskog sistema, moraju se obraditi podaci velikog broja poređenja u kojima šablon odgovara uzorku (distribucija $p(s | H_1 = \text{True})$), kao i poređenja u kojima to nije slučaj (distribucija $p(s | H_0 = \text{True})$). U prvom slučaju distribucija se naziva originalnom (eng. *genuine distribution*), a u drugom nametnutom tj. lažnom (eng. *impostor distribution*) – slika 10.



Slika 10: Originalna i nametnuta distribucija i odnos FNMR i FMR u odnosu na threshold

Sa slike 10. vidljivo je da se FNMR i FMR mogu izraziti na sledeći način:

$$\text{FNMR} = \int_0^t p(s | H_1 = \text{True}) ds \quad [2]$$

$$\text{FMR} = \int_t^1 p(s | H_0 = \text{True}) ds$$

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

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

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

3.3.3 Performanse i greške u procesu identifikacije

Za određivanje performansi identifikacionih sistema, mogu se, pod određenim pretpostavkama, koristiti parametri verifikacionih sistema.

Ako pretpostavimo da sistemska baza sadrži N šablona i da postoji samo jedan šablon za svakog od korisnika u sistemu, tada:

$$\begin{aligned}\text{FNMR}_N &= \text{FNMR} \\ \text{FMR}_N &= 1 - (1 - \text{FMR})^N\end{aligned}\quad [3]$$

Ako je FMR veoma malo, tada se FMR_N može aproksimovati sa $N \cdot \text{FMR}$, što bi značilo da verovatnoća greške ove vrste raste linearno sa veličinom baze.

Ovaj rezultat ima snažne implikacije na razvoj velikih identifikacionih sistema, čak više nego računarska brzina. Na primeru baze od 10.000 korisnika, za prihvatljivo FNMR i FMR od 10^{-5} , FMR_N biće približno 10%, što je jako veliki procenat.

Ako su šabloni klasifikovani/indeksirani, tada se samo deo baze podataka pretražuje, te to rezultira drugačijim formulama za FNMR_N i FMR_N :

$$\text{FNMR}_N = \text{RER} + (1 - \text{RER}) \cdot \text{FNMR}, \quad [4]$$

gde je RER – *Retrieval Error Rate* – verovatnoća da je povučen pogrešan šablon. Ako šablon nije korektno povučen (događa se sa verovatnoćom RER), tada se uvek generiše FNM, a u slučaju da je korektno povučen (verovatnoća $1 - \text{RER}$), FNMR sistema je FNMR.

$$\text{FMR}_N = 1 - (1 - \text{FMR})^P, \text{ gde je } P - \text{procenat baze koja se pretražuje.} \quad [5]$$

3.4 Najčešće korišćeni biometrijski sistemi

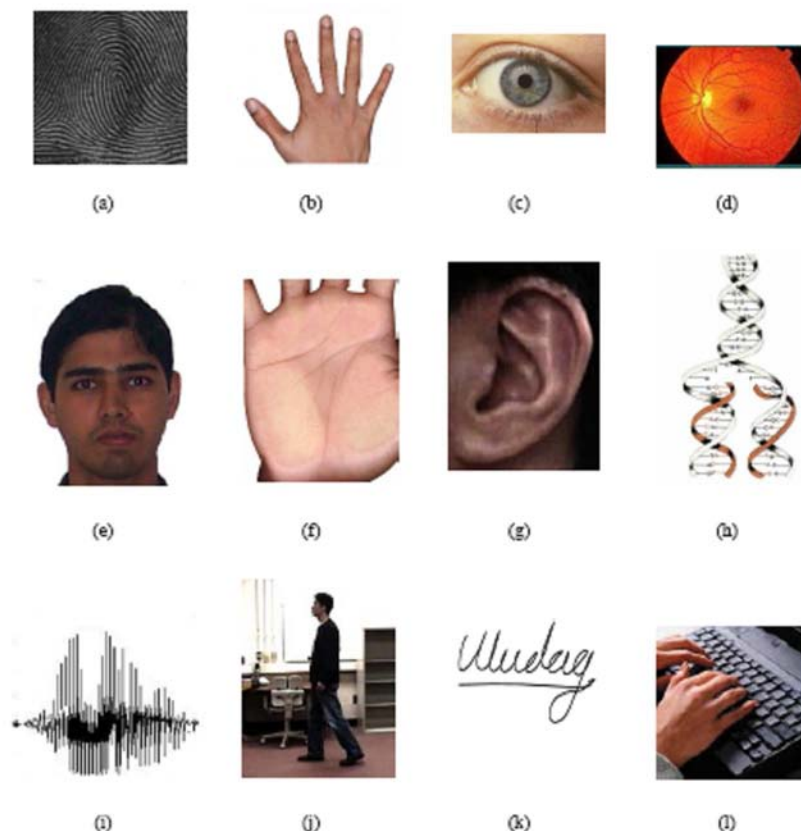
Kao što je ranije već rečeno, u biometrijskim identifikacionim sistemima prepoznavanje korisnika vrši se na osnovu njegovih fizičkih i/ili karakteristika ponašanja. Biometrijski sistemi se, shodno tome, mogu podeliti u dve osnovne kategorije i to:

- Sistemi zasnovani na prepoznavanju fizičkih karakteristika;
- Sistemi zasnovani na prepoznavanju karakteristika ponašanja.

Trenutno postoji više različitih biometrijskih identifikacionih tehnika, čiji su nazivi i dostupni procenti korišćenja na tržištu (iz 2002.g.) dati u tabeli 2. Biometrijske identifikacione tehnike koje su u tabeli 1. ispisane tamnijim slovima (**bold**), danas se najviše koriste i u njihov razvoj ulažu se najveći naponi, te će njihov opis biti dat u ovom radu.

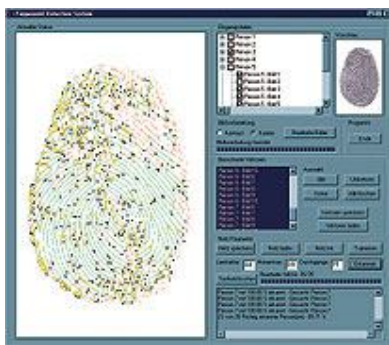
Biometrijski sistemi	
Fizičke karakteristike	Ponašanje
Otisak prsta (52.1 %)	Prepoznavanje glasa (4.4 %)
Prepoznavanje lica (12.4 %)	Potpis (2.1 %)
Geometrija dlana (10.0 %)	Način hodanja
Skeniranje dužice oka (5.8 %)	Dinamika otkucaja na tastaturi
Skeniranje mrežnjače	
DNK	
Vaskularni obrasci (rasporedi vena)	
Termografija lica	

Tabela 2: Procentualna zastupljenost biometrijskih tehnika na tržištu



Slika 11: Najčešće korišćene biometrijske karakteristike. a) otisak prsta, b) geometrija dlana, c) dužica oka, d) rožnjača oka, e) crte lica, f) otisak šake, g) oblik uha, h) DNK, i) glas, j) hod, k) potpis, l) dinamika kicanja

3.4.1 Otisak prsta



Slika 12: Program za identifikaciju otisaka prstiju

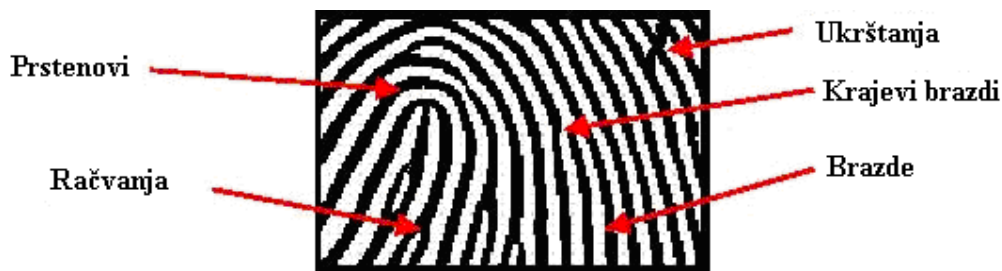
S obzirom da je otisak prsta najkorišćenija metoda identifikacije kod biometrijskih pametnih kartica, u ovom delu detaljnije će biti objašnjen postupak.

Prva primena na koju se pomisli kada se pomene biometrija jeste digitalno očitavanje otiska prsta. Otisak prsta je metoda koja se koristi za identifikaciju pojedinca još od najranije istorije. Od 1897. godine, kad se koristio samo za identifikaciju kriminalaca, pa tako današnjih dana, postoji velika baza otisaka prstiju. Ovaj način određivanja identiteta je međunarodno rasprostranjen i prihvaćen. Iako se otisci prstiju koriste od 19-og veka, moderna autentifikacija putem otisaka prstiju nema mnogo veze sa ustaljenim stereotipom

o mastilu i prstu. Kako bi bila jasna moderna tehnika identifikacije otisaka prstiju potrebno je razumeti neke osnove.

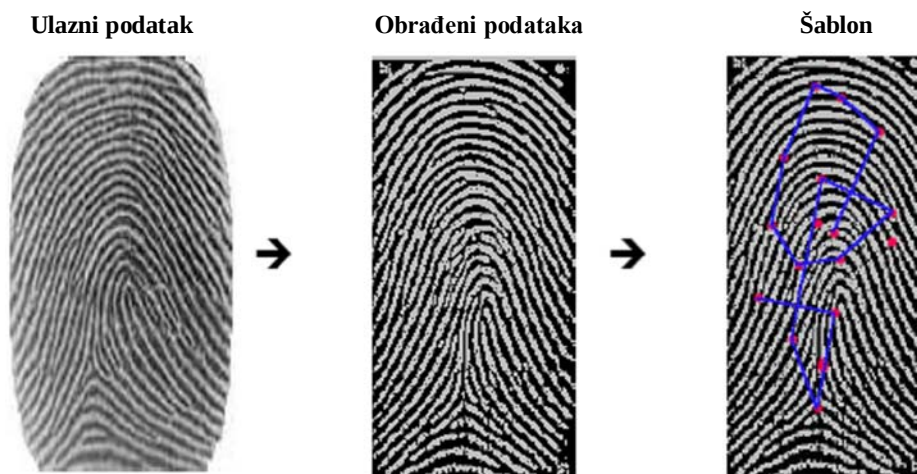
Svaka osoba ima jedinstven otisak prsta koji se sastoji od dolina i brazdi (udubljenja i ispupčenja respektivno) koji definišu različite šablone. Brazde mogu biti različitih oblika kao što je prikazano na slici 13.

Detalji (engl.*minutiae*) se završavaju rubovima i mogu izgledati kao krajevi brazdi, račvanje, ukrštanje i sl.



Slika 13: Brazde otiska

Autentifikacija je zasnovana na kompletnim podacima prikupljenim sa otiska. Podaci se sažimaju (upotrebom određenog algoritma) kako bi se izdvojio zapis zasnovan na prostranim vezama. Na primer, podatak može biti tako obrađen da se izdvoji samo određeni tip detalja ili određeni niz brazdi. Kao rezultat dobija se fajl sa podskupom karakterističnih tačaka (prikazano na slici 14), a ne čuva se ceo otisak niti se on može rekonstruisati iz fajla što i predstavlja osnovnu razliku u odnosu na autentifikaciju upotrebom otisaka koji su uzeti upotrebom mastila i gde se koristi ceo otisak. Kod modernih sistema za proveru otisaka, za pretrage tipa 1:N koriste se fajlovi sa podacima veličine 100-250 KB koji zahtevaju višesatnu ili višednevnu obradu dok se za pretrage tipa 1:1 koriste fajlovi manji od 1 KB. Samim tim, pretraga se obavlja za par sekundi. [56]



Slika 14: Proces od originalne slik do šablona

3.4.1.1 Kako funkcioniše autentifikacija.

Autentifikacija putem otisaka prsta je veoma jednostavna. Prvo, korisnik se prijavi na sistem dajući svoj uzorak otiska. Senzor skenira prst. Dobijena slika se određenim algoritmima obradi i postavi u fajl na glavnom računaru ili lokalnom procesoru kod mobilnih uređaja. Sačuvani podatak predstavlja tzv. šablon korisnikovog otiska prsta. Pri verifikaciji otiska, podaci o otisku se upotrebom algoritma porede sa prethodno sačuvanim podatkom iz čega se kao odgovor dobija podudaranje ili ne podudaranje otisaka. Cela procedura se odvija brzinom od 1-2 s [65].

Postoje dva osnovna pristupa prilikom analize otiska prsta. Prvi analizira samo ukrštanja i završetke zavijutaka otiska, dok drugi prati celokupan pravac svake linije. Otisak skeniran prvom metodom zauzima oko 250 B, dok drugom metodom otisak zauzima oko 100 KB. Naravno, postoji i razlika u brzini prepoznavanja otiska jer se u prvoj metodi upoređuje nekoliko karakterističnih tačaka, dok se u drugoj metodi upoređivanje vrši u kompletnoj bazi podataka, što može da traje satima ili danima.

Različita je i tehnologija kojom se skenira otisak i ona se najčešće bazira na kapacitivnim, optičkim ili ultrazvučnim senzorima.

Senzori bazirani na silikonskoj tehnologiji

S ciljem smanjenja sistema za očitavanje otiska prstiju kako po pitanju gabarita, tako i po pitanju cene, razvojem tehnologije bilo je nemoguće izostaviti senzore bazirane na silikonskoj tehnologiji. Postoji više mogućih pristupa međutim, osnovni i najkorišćeniji pristup je upotreba kapacitivnih senzora (pojavi su se kasnih '90-ih godina XX veka) koji kao osnovu koriste CMOS mikročipove.

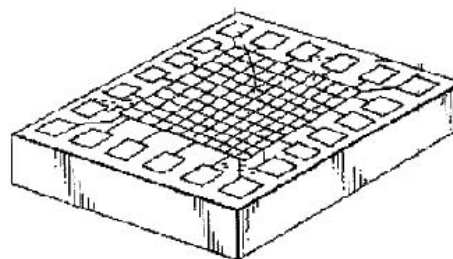
Kapacitivni senzori. Pritiskom prsta na senzor koji je sastavljen od niza kondenzatora, brazde i doline otiska menjaće njihovu kapacitivnost. Prednost ove metode je što zahteva pravi otisak prsta, ali se javljaju problemi s mokrim i suvim prstima. Mokri prsti će dati tamnu, a suvi svetlu sliku (slika 15)



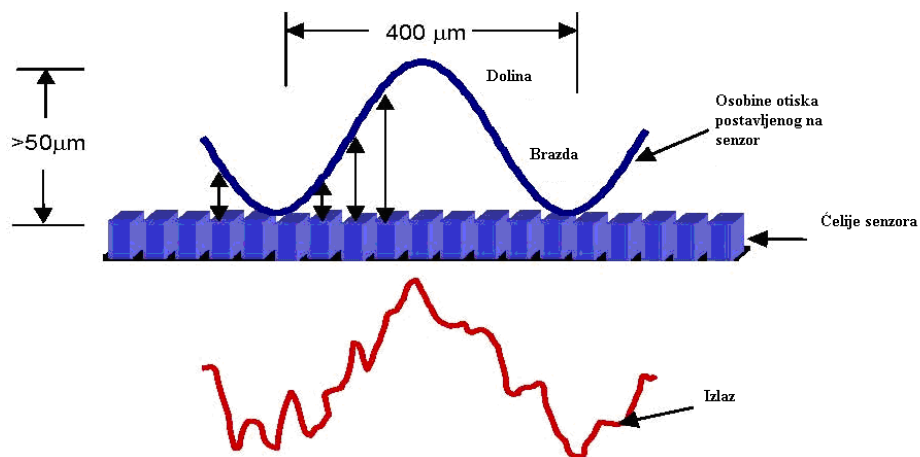
Slika 15: Prikaz otiska zavisno od vlažnosti

Sadrži 2D niz ćelija prikazanih na slici 16. Veličina i razmak između ćelija tako su dizajnirani da svaka ćelija predstavlja mali deo razmaka između brazdi otiska. Veličina i razmak je reda veličine $50\text{ }\mu\text{m}$, uz sposobnost senzora da proizvede sliku po FBI standardima od 500 dpi.

Pritiskom na senzor, aktiviraju se tranzistori ispod svake ćelije što dovodi do skeniranja dela prsta. Svaka ćelija zasebno skenira tačno onaj deo koji se nalazio iznad nje kao što je prikazano na slici 17.

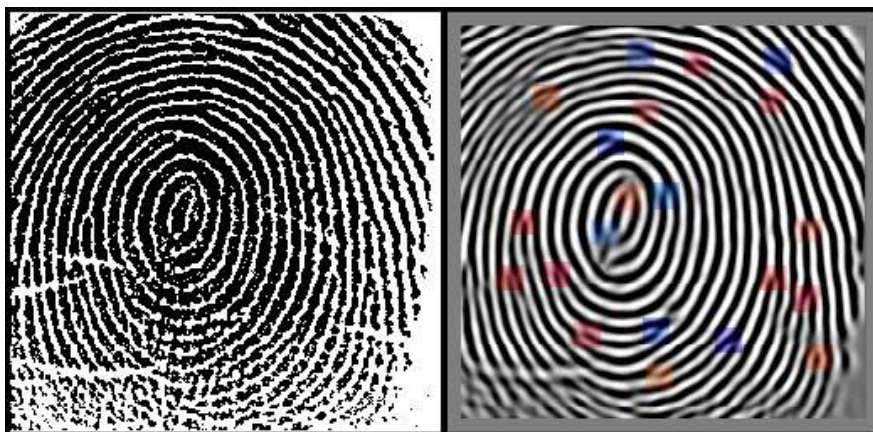


Slika 16: 2D ćelije kapacitivnog senzora



Slika 17: Skeniranje prsta

Različiti proizvođači koriste različite metode za merenje udaljenosti delova prsta od senzora tako da mogu da se jave određene slabosti sistema. Dobijena slika se, upotrebom posebnih algoritama, u binarnom obliku čuva kao fajl. Na slici 18. prikazan je izgled otiska prsta uzetog sensorima kompanije *Fidelica Microsystems* i izgled nakon obrade algoritmom za obeležavanje karakterističnih detalja.



Slika 18: Minutiae snimljene senzorima kompanije Fidelica Microsystem

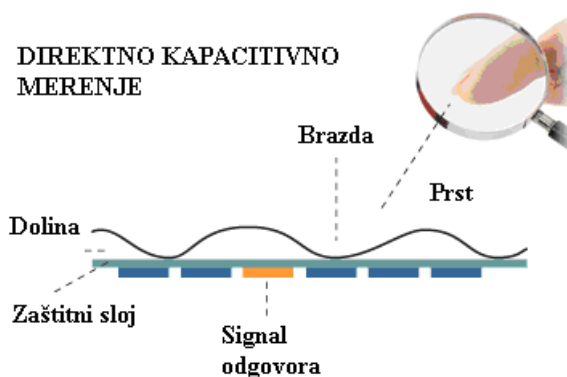
Senzori kompanije *Fingerprint cards* (slika 19, [56]) sadrže 10000 malih kapacitivnih pločica, pri čemu svaka od njih ima sopstveno električno kolo ugrađeno u čip. Pritiskom na senzor, stvara se veoma mali električni naboj, stvarajući šablon između brazdi i doline na prstu i pločica na senzoru. Koristeći podatke o ovom naboju, meri se kapacitivnost duž površine senzora. Dobijene vrednosti se digitalizuju i šalju mikroprocesoru.



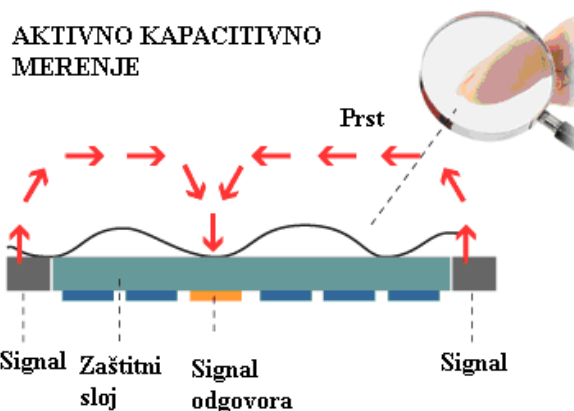
Slika 19: FPC 1011 Area sensor

FPC 1031 Swipe sensor

Površina senzora predstavlja uređen niz pločica sa mogućnošću merenja kapacitivnosti između njegove površine i konture otiska prsta. Ovo se može učiniti ili direktnim punjenjem pločica (slika 20) ili električnim signalom prosleđenim otisku prsta (slika 21).



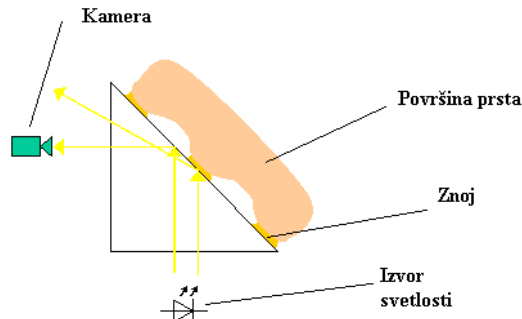
Slika 20: Direktno kapacitivno merenje FPC senzorima



Slika 21: Aktivno kapacitivno merenje FPC sensorima

Ovaj drugi metod se naziva aktivan ili reflektivan metod i donosi neke prednosti. Upotrebom programabilnih logičkih kola senzor je moguće tako podesiti da prihvata različite tipove kože prsta. Druga prednost je u tome da pojačan signal između površine prsta i senzora obezbeđuje snažan zaštitni sloj površine senzora, do 25-30x deblji nego kod drugih proizvođača kapacitivnih senzora,.

Uz kapacitivnost, **optička metoda** je najkorišćeniji način skeniranja otiska prsta. Obično sadrži optičku prizmu sa izvorom svetlosti (LED dioda) sa jedne strane i kamerom (CCD senzor) koja na drugoj strani prihvata predatu svetlost odnosno, CCD senzor beleži sliku prsta prislonjenog na staklo, a LED diode osvetljavaju brazde i doline otiska. Princip rada je prikazan na slici 22.



Slika 22: Princip rada optičkog senzora

Prednosti ove metode su jednostavnost i niska cena, a nedostatak su tzv. „latentni otisci”. Naime, na senzorima na koje se prst prislanja celom površinom ostaje otisak prsta kao i na svakoj drugoj površini. To može da ometa sledeće skeniranje, ali isto tako predstavlja i sigurnosni rizik jer je taj otisak moguće skinuti.

Postavljanjem prsta na prizmu izvor svetlosti odašilja svetlost ka CCD. Postavljanjem prsta na prizmu, kontakt se uspostavlja putem znoja na površini brazdi na otisku prsta [68].

Prosečna brzina registracije korisnika u slučaju upotrebe kapacitivnih senzora je <5s, dok je vreme verifikacije < 2s. FAR je oko 0.2%, dok je FRR reda veličine 1%

Ultrazvučni senzori koriste zvučne talase i još su u fazi razvoja.

Termoelektrična metoda je prilično retka. Senzor meri razliku u temperaturi brazdi na otisku i vazduha uhvaćenog u dolini kada je prst prslonjen uz senzor. Zahvaljujući tome, dobija se slika visoke rezolucije (oko 500 tpi, sa 256 nijansi sive), čak i kada je prst prljav ili otisak plitak. Prilikom skeniranja neophodno je prevući prst preko senzora, pa se tako rešava i problem čišćenja senzora i latentnih otisaka. Mane ove metode su to što korisnik mora da zna kako da koristi senzor i potreba za zagrevanjem senzora kako bi se izbeglo poklapanje temperature senzora i prsta, što povećava potrošnju.

E-Field senzori mere električno polje ispod gornjeg sloja kože, to jest tamo gde otisak počinje. Ova metoda je prilično osetljiva i beleži suve, istrošene i zaprljane otiske. Njeni nedostaci su mala rezolucija snimka i malo polje skeniranja što povećava procenat greške.

Senzori osetljivi na pritisak beleže samo brazde otiska kada prst dođe u kontakt sa senzorom. To se dešava zahvaljujući upotrebi piezoelektričnih kristala koji pod pritiskom ili uvijanjem generišu struju. Nedostatak je lošija rezolucija u odnosu na optičke senzore i što je očitani podatak jednobitni (ima/nema odnosno crno/belo). Međutim, ovi senzori podjednako dobro rade sa suvim i vlažnim prstima što se može videti na slikama 23a i 23b., a i površina skeniranja je prilično velika.



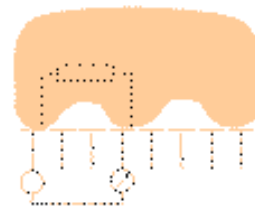
Slika 23a: Slika vlažnog prsta sa senzora osetljivog na pritisak



Slika 23b: Slika suvog prsta sa senzora osetljivog na pritisak

Senzori osetljivi na otpornost

Sastoje se od elektroda koje detektuju i mere otpornost koju izaziva površina kože (slika 24, [68]).



Slika 24: Senzor osetljiv na otpornost

3.4.1.2 Prednosti i slabosti tehnologije skeniranja otiska prsta

Biometrijska identifikacija pomoću otiska prsta ima brojne prednosti. Pre svega, kao što smo rekli, otisci prstiju se beleže još od davnina, a sve zemlje sveta imaju ogromne baze otisaka prstiju. Prelazak na novu tehnologiju je zbog toga izuzetno jednostavan. Isto tako, ljudima je ovaj način identifikacije poznat i ne izaziva podozrenje. Senzori se mogu ugrađivati u prenosne računare, tako da senzorsko polje bude površina *touchpada*. Mogu se ugrađivati na tastature ili gornje površine miša. Čitači se mogu praviti u vidu USB priveška koji će se dati svakom zaposlenom u firmi, recimo, tako da on može da pristupi resursima s bilo kojeg kompjutera, čak i van firme. Čitači otiska prsta eliminišu potrebu za bilo kakvim ključem. Oni se mogu ugrađivati na akten-tašne za koje bi bilo moguće definisati skup ljudi koji može da ih otvori, ili na sefove, ili u automobile, ili na kućna vrata, ili...

Najveći problem tehnologije prepoznavanja otiska prsta jeste mogućnost falsifikovanja otiska. Nijedan od trenutno raspoloživih čitača nije u mogućnosti da pouzdano razlikuje stvarni prst od dobro urađene kopije. Kopija otiska može se uraditi uz saradnju vlasnika ili bez nje. Tehnologija prepoznavanja otiska, je u poređenju sa drugim biometrijskim tehnologijama, najpodložnija mogućnosti dobijanja kopije otiska bez znanja vlasnika.

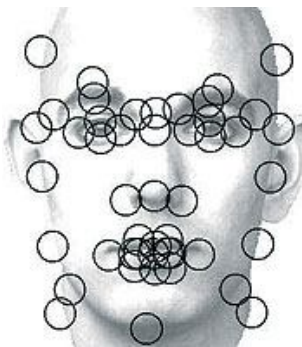
Falsifikat otiska prsta može se napraviti pomoću tanke silikonske oblande, koja je, u stvari, kopija otiska. Ovakav falsifikat moguće je napraviti bez puno opreme za nekoliko sati. Prilično lako se može nalepiti na prst, i veoma ga je teško detektovati.

Glavni izazov koji se postavlja pred proizvođače senzora je razlikovanje veštačkog materijala od prirodnog epiderma prsta. U toku su mnoga istraživanja sa ciljem da se obezbedi da samo prst, bez ikakvih dodatnih veštačkih delova, može biti identifikovan. Pažnja se usredsređuje na osobine kao što su temperatura, provodljivost, puls, krvni pritisak, itd. U cilju detektovanja falsifikata, u mnogim uređajima za prepoznavanje otisaka prstiju, dodati su senzori koji mere provodljivost prsta, temperature, puls, dielektrične konstante i sl.

Kao zaključak može se reći da, i pored postojanja brojnih metoda razvijenih u cilju razlikovanja veštačkog i stvarnog otiska prsta, mogućnost falsifikovanja nije eliminisana. Usled potrebe da čitač ispravno radi za prilično široke granice svih parametara, ipak može doći do zavaravanja i dodatnih testova. Za dobijanje višeg stepena sigurnosti identifikacije, poželjno je biometrijski sistem zasnovan na prepoznavanju otiska prsta kombinovati sa nekim klasičnim identifikacionim sistemom (lozinka, pametna kartica, itd.).

3.4.2 Crte lica

Do nedavno su se za prepoznavanje ljudskog lica koristili predstavnici reda i zakona koji su u ruci držali papir sa slikom osumnjičenog. Od skoro to rade obične televizijske kamere i softver. Lice je deo čovekove spoljašnjosti na osnovu kojeg su se ljudi oduvek međusobno prepoznavali. Ljudi imaju urođenu sposobnost prepoznavanja lica. U poslednjih desetak godina čine se intenzivni naponi da se takva sposobnost razvije i kod kompjutera. Osim u slučaju identičnih blizanaca, svako lice posедуje skup jedinstvenih fizičkih karakteristika, koje je moguće meriti i međusobno porediti.



Slika 25: Karakteristične tačke lica

U procesu prepoznavanja lica ne zahteva se fizički kontakt sa skenerom. Prilikom implementacije sistema za prepoznavanje lica koristi se postojeća standardna oprema kao što su: web kamera, sigurnosna kamera itd.

Prednost ovog načina identifikacije je to što je, za razliku od starog, neupadljiv, efikasniji i teže ga je prevariti. Ljudsko lice je u najvećem broju slučajeva različito i predstavlja osnovni način na koji se razlikuju i pamte osobe, ali treba napomenuti da se u tom slučaju ljudsko lice doživljava kao celinu. Prilikom softverskog prepoznavanja lica ono se razlaže na oko 80 karakteristika (slika 25), kao što su, recimo, rastojanje između očiju, širina i dužina nosa, jagodice, brada, oblik vilice... Sve te karakteristike se zatim pretvaraju u numerički oblik, a taj niz cifara se naziva otisak lica. Za uspešno prepoznavanje potrebno je poklopiti između 15 i 20 karakteristika, tako da se pojedinac može identifikovati čak i posle izvršene plastične operacije, a da ne pominjemo farbanje kose ili upotrebu naočara za sunce. [56]

Proces identifikacije obavlja se u nekoliko koraka. Softver pretražuje snimak sa video-kamere u potrazi za licima. Lice se na slici traži grubo, u niskoj rezoluciji, a na visoku rezoluciju se

prelazi kada se pronade oblik u vidu lica. Zatim se određuje veličina i položaj lica u odnosu na kameru. Lice mora da bude pod uglom od barem 35 stepeni u odnosu na kameru. Zatim se vrši normalizacija, to jest lice se rotira i menja mu se veličina kako bi se izvršilo upoređivanje. Podaci o licu se prebacuju u numerički oblik, a zatim se vrši upoređivanje sa podacima u bazi. Pošto otisak lica u takvom obliku zauzima samo 84 bajta (prosečna originalna veličina slike je 1.3Kb, [49]), sistem je u stanju da uporedi između 15 i 60 miliona otisaka u minutu.

Danas se u svetu veliki broj kompanija i naučnih ustanova bavi razvojem tehnologije prepoznavanja lica. Razvijeno je više algoritama. Na primer, kompanija *Visionics* iz New Jersey-a je razvila softver za prepoznavanje lica, nazvan *FaceIt*, dok kompanija *Biometrix* nudi softver *BioFace*. Ovi softveri su u stanju da izaberu lice iz mase, izdvoje to lice iz ostatka scene, izmere njegove karakteristike i porede ih sa karakteristikama već uskladištenim u bazama podataka. Od naučnih ustanova treba pomenuti *Colorado State University*, gde je razvijeno više algoritma za prepoznavanje lica.

Najveću primenu softver za prepoznavanje lica nalazi u službi reda i zakona, to jest za pronalaženje osumnjičenih u masi. Ovaj sistem je prvi put masovno upotrebljen u januaru 2000. na bejzbol utakmici u Floridi. Softver *FaceIt* je pušten probno na godinu dana u gradu Tampa u Floridi, a na osnovu njega nije izvršeno nijedno hapšenje, iako je na pomenutoj utakmici identifikovano 19 osoba sa podebljim dosijeima. Isti softver korišćen je u Meksiku da bi se izbegli dupli glasovi na predsedničkim izborima. Ranije se dešavalo da se ljudi registruju u biračke spiskove pod različitim imenima kako bi mogli da glasaju više puta. U toku predsedničkih izbora 2000. godine ovaj sistem je korišćen za prepoznavanje ranije prijavljenih glasača.

Moguće primene sistema su takođe zanimljive. Ugrađene kamere na ATM uređajima bi mogle da se iskoriste za identifikaciju korisnika kartice i tek ukoliko se identitet poklapa s onim koji je zapisan na kartici, isplata će biti izvršena. U Velikoj Britaniji policija ima drugačiju zamisao primene ove tehnologije. Oni žele da je upotrebe u identifikaciji žrtava jer su po razbijanju lanca dečje pornografije konfiskovali oko tri miliona slika za koje bi ručno sortiranje oduzelo previše vremena.

Tehnologija prepoznavanja lica izuzetno je zanimljiva jer, slično otiscima prstiju, postoje velike baze slika ili se mogu lako napraviti (slike za lične karte ili vozačke dozvole). Takođe, proces identifikacije je jednostavan, a pojedinac čak nije ni svestan da se vrši određivanje njegovog identiteta. Međutim, tehnologija prepoznavanja lica još uvek je u razvoju i oslanja se i dalje u velikoj meri na ljudskog operatera.

3.4.2.1 Tehnologija prepoznavanja lica

Kao što je već rečeno, svako lice ima svoje posebne karakteristike koje mu daju prepoznatljivost. Karakteristike lica koje se mogu meriti i koristiti za kasniju identifikaciju nazivaju se ključni detalji. Postoji oko 80 ključnih detalja na ljudskom licu. Neki od tih detalja su:

- Rastojanje između očiju;
- Širina nosa;
- Dubina očnih udubljenja;
- Jagodice;
- Vilična linija;
- Brada.

Ključni detalji se mere i formira se numerički kod, odnosno niz brojeva, koji predstavlja lice u

bazi podataka - "*faceprint*". Obično algoritmi za prepoznavanja lica ne koriste svih osamdeset ključnih detalja. Na primer, *Visionics*-ov *FaceIt* softver koristi od 14 do 22 ključna detalja.

Kao i kod drugih biometrijskih identifikacionih sistema i ovde se razlikuju procesi upisivanja i procesi verifikacije i identifikacije.

Faza upisivanja obično traje 20 do 30 sekundi, tokom kojih se uzima nekoliko slika istog lica. Idealno je da se slike uzimaju sa blago različitim uglovima lica prema kameri. Nakon uzimanja slika, izdvajaju se karakteristične osobine lica i kreira *faceprint*.

Postoje različiti algoritmi za prepoznavanja lica ali, uglavnom, svi oni sadrže sledeće faze:

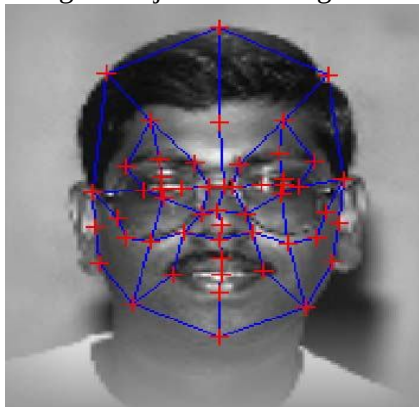
- Fazu detekcije;
- Fazu podešavanja;
- Fazu normalizacije;
- Fazu kodiranja;
- Fazu poređenja.

U fazi detekcije softver za prepoznavanje lica, traži lice u polju vidljivosti kamere. Kada se detektuje oblik koji podseća na ljudsku glavu, softver prebacuje kameru u režim rada sa visokom rezolucijom. Pouzdanost identifikacije presudno zavisi od kvaliteta slike.

Nakon faze detekcije prelazi se na fazu podešavanja. U ovoj fazi određuje se pozicija, veličina i orijentacija glave. Zatim se vrši prevođenje 3D prikaza glave u dvodimenzionalnu nefrontalnu sliku. Na kraju, 2D nefrontalna slika se prevodi u 2D frontalnu sliku.

Najveći broj sistema za prepoznavanje lica vrši prepoznavanje iz tzv. "mirne slike". Pod "mirnom slikom" se podrazumijeva frontalna slika, sa uobičajenim izrazom čovečijeg lica. U odnosu na korišćenje "žive slike", ovo, u prvom redu, značajno smanjuje veličinu numeričkog koda kojim se slika predstavlja u bazi podataka. Da bi se dobila "mirna slika" nakon faze podešavanja potrebno je normalizovati frontalnu sliku. Pod normalizacijom se podrazumijeva statistička tehnika kojom se vrši korekcija razlika u licu iste osobe, na različitim slikama. Normalizacione korekcije donekle umanjuju razlike između različitih lica. Ipak, dosadašnja ispitivanja su pokazala da sistemi koji za identifikaciju koriste tzv. "živu sliku" ne postižu značajno bolje rezultate.

Nakon faze normalizacije pristupa se fazi kodiranja, koja je i ključna faza u procesu prepoznavanja lica. U fazi kodiranja vrši se merenje, odnosno prevođenje ključnih detalja sa normalizovane 2D frontalne slike glave u jedinstveni digitalni kod (slika 26).



Slika 26: Formiranje digitalnog koda za prepoznavanje lica

Dobijeni digitalni kod (*faceprint*), se, u fazi poređenja, koristi za poređenje sa drugim raspoloživim kodovima iz baze podataka.

Pouzdanost sistema za prepoznavanja lica je funkcija kvaliteta slika, kao i demografskih karakteristika populacije koja koristi sistem. Eksperimentalno je pokazano da je lakše prepoznati muškarce nego žene, kao i da je lakše prepoznati starije nego mlađe ljude. Rezultati takođe pokazuju da razlike u lakoći prepoznavanja muškaraca i žena, opadaju sa njihovim starenjem.

Poznato je da protok vremena uslovljava stalne promene na licu. Usled toga, od trenutka upisivanja *faceprint*-a u bazu podataka, pouzdanost prepoznavanja lica opada. U ovom pogledu tehnologija prepoznavanja lica zaostaje u odnosu na tehnologiju prepoznavanja dužice oka i tehnologiju prepoznavanja otiska prsta.

Kao i u slučaju tehnologije prepoznavanja otiska prsta i tehnologija prepoznavanja lica je prilično ugrožena mogućnošću falsifikovanja.

Prosečna brzina registracije korisnika u slučaju upotrebe 2D kamere je <5s, dok je vreme verifikacije < 2s. FAR je oko 0.4%, dok je FRR reda veličine 5%

Neke primene tehnologije prepoznavanja lica

Prvi korisnici sistema za prepoznavanje lica bile su organi za sprovođenje zakona kao što su policija i sudovi. Policija ove sisteme često koristi za nadzor određenih prostora. Nadzor se sastoji u proveru identiteta slučajno odabranog lica iz mase.

Poznatiji sistemi za sigurnosni nadzor koji koriste tehnologiju prepoznavanja lica su *Virginia Beach Surveillance*, *City of Brentwood Police Department*, *Zurich Airport Face*, *Manchester NH Visage*.

Osim za sigurnosni nadzor, sistemi za prepoznavanje lica se koriste i za druge namene kao što su: sprečavanje lažnog glasanja na izborima, provera identiteta prilikom upotrebe automata za keširanje novca, umesto lozinke za pristup računarskim sistemima.

Jedna od prvih značajnijih primena sistema za prepoznavanje lica u cilju sprečavanja lažnog glasanja na izborima, bila je od strane meksičke vlade, za predsedničke izbore 2000. godine. Da bi se uticalo na ishod izbora, mnogi ljudi su bili registrovani pod različitim imenima i mogli su glasati više puta. Konvencionalni metodi za sprečavanje ovakvih postupaka nisu davali željene rezultate. Upotrebom tehnologije prepoznavanja lica, u trenutku glasanja, mogla se vršiti potraga za duplikatima po glasačkoj bazi podataka. Novi *faceprint* se upoređivao sa već zabeleženim i tako se otkrivao pokušaj višestrukog glasanja.

Proverom identiteta, korišćenjem tehnologija prepoznavanja lica, može se povećati sigurnost aparata za keširanje novca. Ukoliko se, pored identifikacione kartice i PIN koda, vrši i provera *faceprint*-a korisnika, mogućnost zloupotrebe i neovlašćenih transakcija je znatno smanjena.

Biometrijska tehnologija prepoznavanja lica može se upotrebiti i za kontrolu pristupa računarskim sistemima. Instaliranjem web kamere i odgovarajućeg softvera na računar, korisnikovo lice može da zameni lozinku za pristup računaru ili da se koristi u kombinaciji sa njom. IBM je ugradio ovu tehnologiju unutar *screensaver*-a za A, T i X serije *Thinkpad* laptop-ova.

Prepoznavanje crta lica je generalno gledano prihvaćena od društvene zajednice, jednostavna je za upotrebu i ima niske troškove eksploatacije. Nedostatak je u tome što je tehnologija dovoljno precizna za verifikaciju-autentifikaciju ali je nedovoljan za identifikaciju. Takođe performanse zavise i od samog lica, tj. upotrebe šminke, naočara, drukčije frizure, a naročito

je problem što je nemoguće napraviti razliku kod provere blizanaca.



Slika 27: Skener lica u banci

Neki primeri primene:

- Leading Banka, Ženeva (80 tačaka, 2000 zaposlenih)
- Filip Moris (30 tačaka, 2000 zaposlenih)
- Skupština, Kuvajt (12 tačaka, 500 korisnika)
- Odeljenje za inf.tehnologije u policiji, V.Britanija
- Vladina zgrada za vanredne situacija, Malezija
- Naftna kompanija Vitol, Singapur

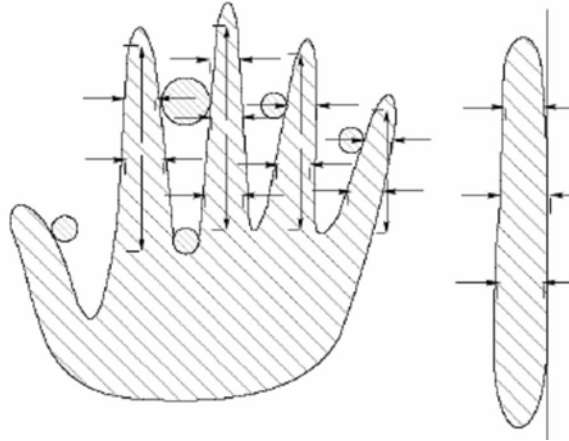
3.4.3 Geometrija dlana i raspored vena

Geometrija dlana, posle otiska prsta, drugi najčešće korišćen način biometrijske autentifikacije [63] je proces u kojem se vrši analiza oblika dlana i dužine prstiju. Prilikom analize ruke, uzima se oko 90 parametara. Za razliku od otiska prsta,ometrija dlana nije jedinstvena za svakog pojedinca. Zbog toga se ovi sistemi koriste za verifikaciju identiteta, a ne za samu identifikaciju. Samim tim pogodni su za verifikaciju identiteta velikog broja pojedinaca, recimo prilikom kontrole na granici. Kada se radi o identifikaciji,ometrija dlana se najčešće upotrebljava u kombinaciji s nekom drugom metodom. Ova metoda može da se primenjuje i u firmama, gde zaposleni prijavljuju dolazak i odlazak sa posla skeniranjem ruke.

Geometrija dlana može da se kombinuje sa analizom rasporeda vena na šaci. Slično otisku prsta, ova metoda traži mesta ukrštanja vena koja prave karakterističnu šaru. Primenu već počinje da nalazi. Recimo, *Fujitsu* je napravio čitač vena koji bi trebalo da se upotrebljava u nekoliko banaka u Japanu. Jedna od njih je *Tokyo-Mitsubishi*, treća po veličini u Japanu. Čitači funkcionišu tako što se dlan postavi na nekoliko centimetara iznad površine skenera. Korisnicima u Japanu se ova ideja dopada iz higijenskih razloga jer nema nikakvog kontakta sa čitačem, kao što je slučaj sa čitačima otiska. Još jedna primena čitača vena mogla bi da bude ugradnja na kvake koje bi automatski otključavale vrata ili na vatreno oružje koje bi moglo da opali samo ukoliko ga vlasnik drži u ruci. [56]

Za sada sistem je dobar za verifikaciju ali i nedovoljno precizan za indentifikaciju što i predstavlja dobru zamenu za otisak prsta u sredinama gde postoji nepoverenje po pitanju

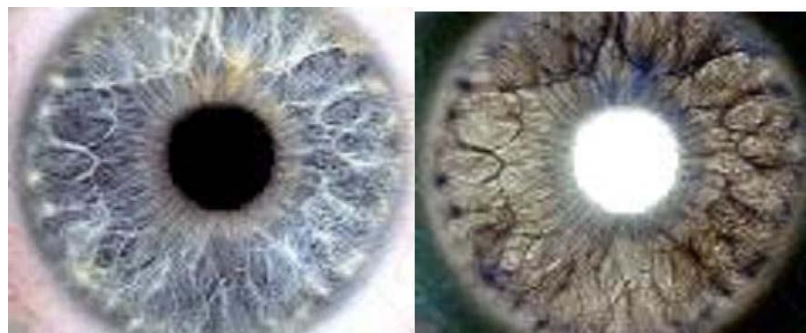
očuvanja privatnosti podataka. Dobre osobine su mogućnost upotrebe od strane velike većine ljudi i visok nivo prihvatanja ali ipak se mogu javiti problemi sa ljudima koji su npr. oboleli od artritisa. Veličina fajla je veoma mala i iznosi oko 9b [49].



Slika 28: Tipične mere sistema za proveru geometrije dlana

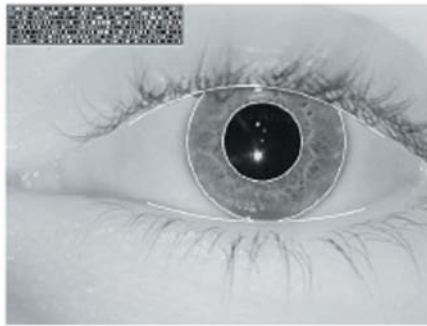
3.4.4 Skeniranje oka

Postoje dve metode prilikom određivanja identiteta pomoću oka – skeniranje dužice (slika 29) i skeniranje mrežnjače (retine) oka. Skeniranje dužice se zasniva na analizi pojedinosti prstena u boji koji okružuje zenicu (irisa). Dužica oka je obojeno tkivo koje okružuje zenicu (slika 29.). Dužica poseduje preko 200 detalja koji se mogu upotrebiti za poređenje i identifikaciju, kao što su prsteni, brazde i pegice. Te šare su jedinstvene za svakog pojedinca, čak se levo i desno oko iste osobe razlikuju. Zbog toga se ova metoda uspešno može koristiti i za identifikaciju, a ne samo za verifikaciju. Za snimanje dužice dovoljna je obična kamera. Snimanje se može obaviti sa izvesne daljine (čak i do pola metra) i kroz naočare. Prilikom skeniranja dužice oka, korisnik staje ispred čitača, na način da na uređaju može videti refleksiju svojih očiju. Vreme verifikacije je obično manje od 5 sekundi [65]. Da bi se izbeglo korišćenje veštačkog oka, sistem može da osvetli oko i da vidi da li dolazi do skupljanja zenice odnosno, nakon izvršenog skeniranja, čitač uključuje vidljivu svetlost i varira njen intezitet. To radi u cilju detekcije dilatacije zjenice. Dilatacija zenice je prirodna osobina oka koja se ne može preneti na falsifikat. Ukoliko dilatacija postoji, čitač sa sigurnošću konstatuje da je reč o prirodnom oku.



Slika 29: Dužica oka i njen negativ

Proces identifikacije započinje utvrđivanjem ima li oka u vidokrugu čitača. Ukoliko se oko detektuje, vrši se precizno lociranje unutrašnjih i spoljašnjih granica dužice (zenice i limbusa). Zahvaljujući podesnoj kružnoj geometriji, određivanje granica dužice može se izvršiti na sirovoj slici dobijenoj od strane skenera. U cilju pronalaženja prelazaka sa dužice na limbus i sa dužice na zenicu, vrši se radijalno pretraživanje slike. Nakon određivanja granica sprovodi se analiza, odnosno, pronalaženje karakterističnih tačaka po površini dužice. Dr Daugmanov⁸ algoritam obezbeđuje 3-4 bita podataka po kvadratnom milimetru (prečnik dužice je oko 11 milimetara). Na kraju analize, vidljive karakteristike dužice konvertuju se u 256/512B *IrisCode* profil (uzorak, slika 30, [58]). U slučaju upisivanja korisnika, dobijeni profil se zapisuje, smešta u bazu podataka, i dalje koristi za verifikaciju, dok se u slučaju identifikacije profil poredi sa raspoloživim profilima.



Slika 30: Dužica sa IrisCode u gornjem levom uglu slike



**Slika 31:
Identifikacioni
sistem UAE
(skeniranje dužice
oka)**

Ovaj sistem je primenu našao još 1994. godine u nekoliko zatvora u Americi za identifikaciju zatvorenika ili kao sigurnosna provera zaposlenih. Na frankfurtskom aerodromu ovaj sistem se koristi za identifikaciju tzv. „čestih letača” i njihovo brzo propuštanje kroz aerodromske kontrole. Skeniranje dužice se najviše primenjuje u Ujedinjenim Arapskim Emiratima, gde se svi stranci koji ulaze u zemlju skeniraju, a zatim se njihove dužice upoređuju s onima iz baze, kako bi se izdvojili pojedinci koji su proterani iz UAE (slika 31). Oko 7000 putnika se svakog dana upoređuje sa oko 550.000 osoba u bazi. Za pretragu je potrebno oko dve sekunde. Do sada je ovom metodom pronađeno oko 22.500 osoba i njihovi identiteti su daljom istragom potvrđeni. [56]

Prednost ove metode je njena pouzdanost i relativna jednostavnost.

Nedostatak je to što je za skeniranje oka glavu potrebno držati na tačno određenom mestu, što nije naročito zgodno ako neko to ne želi da uradi svojevolejno. Takođe, baze skeniranih dužica ne postoje, već bi morale da se prave „od nule”.

Prosečna brzina registracije korisnika u slučaju skeniranja dužice oka je <5s, dok je vreme verifikacije < 2-10s. FAR je oko 0.00008%, dok je FRR reda veličine 0.1%

⁸ Dr John Daugman, profesor na Harvardu, 1989. godine počinje sa razvojem algoritama za prepoznavanja dužice. 1994. godine, Dr Daugman je patentirao ove algoritme. Patenti su danas vlasništvo Iridian Technologies, Inc.

Skeniranje mrežnjače koristi individualnost krvnih sudova na dnu oka. Ovaj vid identifikacije je najpouzdanija od svih biometrijskih metoda: pošto ne postoji način da se mrežnjača falsifikuje, ona se ne menja tokom celog života osobe, a mrežnjača mrtve osobe toliko brzo propada da nisu neophodne dodatne mere utvrđivanja da li je osoba živa ili ne. Za uspešno skeniranje je potrebno skinuti naočare, oko treba da je blizu skeneru i neophodno je fokusirati se na određenu tačku. Proces skeniranja traje između 10 i 15 sekundi i za to vreme je oko osvetljeno svetlošću slabog intenziteta. Jasno je da je ovo komplikovaniji i neugodniji način utvrđivanja identiteta od svih ranije pomenutih. Zbog toga, a i zbog visoke cene i pouzdanosti, skeniranje mrežnjače koristi se samo za instalacije visokog nivoa sigurnosti, kao što su vojna postrojenja, banke ili elektrane. Prosečna veličina fajla je 96b [49].

3.4.4.1 Prednosti i slabosti tehnologije skeniranja dužice oka

U odnosu na ostale biometrijske tehnologije, skeniranje dužice ima bitnih prednosti. Jedna od ključnih prednosti je izolovanost i zaštićenost dužice od spoljašnje sredine, za razliku od, recimo, tehnologije skeniranja otiska prsta. Šara dužice poseduje visok stepen slučajnosti i nezavisna je od genetskog porekla. Šare dve dužice, koje potiču od istog genotipa, razlikuju se. Fiziološka reakcija dužice na svetlo predstavlja prirodni test za detekciju falsifikata. Slična povoljnost ne postoji kod drugih delova čovečijeg tela, koji se koriste za identifikaciju. Ova osobina čini da je identifikacija na osnovu prepoznavanja dužice jedna od najpouzdanijih, danas.

Falsifikovanje, dužice, hirurškom intervencijom je veoma komplikovano i nosi neprihvatljiv rizik gubljenja vida. Sa druge strane, hirurške intervencije sa ciljem falsifikovanja znatno su izvodljivije na prstu ili licu .

Karakteristike dužice se ne menjaju sa protokom vremena. U ovom pogledu dužici može parirati jedino glas. Šara dužice je vidljiva i sa rastojanja što donosi prednost u odnosu na tehnologiju identifikacije mrežnjače.

Enkodiranje i prepoznavanje dužice se može prilično lako realizovati. Vreme koje je potrebno za analizu slike može se svesti i na oko jednu sekundu, dok brzina pretraživanja, uz upotrebu starih procesora na 300MHz, je oko 100.000 IrisCode profila u sekundi.

Kao nedostatak, može se navesti to što je veličina dužice svega 1cm pa njeno skeniranje zahteva striktnu saradnju korisnika. Za vreme skeniranja korisnik mora stajati mirno u propisanom položaju. Skeniranje dužice otežava i njena pokretljivost. Povremeno spuštanje očnih kapaka takođe ometa proces skeniranja.

Promene veličine zenice izazivaju neelastične deformacije dužice. Usled toga, prilikom skeniranja najčešće se koristi infracrvena svetlost.

3.4.5 Prepoznavanje glasa

Prepoznavanje glasa predstavlja tehnologiju koja dopušta korisniku da upotrebljava sopstveni glas kao ulazni uređaj. Prepoznavanje glasa može biti korišćeno za diktiranje ili zadavanje komandi računaru ili npr. mobilnom telefonu. Ranije je bilo potrebno da se svaka reč izgovara razgovetno i odvojeno od naredne dok novi sistemi dopuštaju tečan govor tj. Obraćanje računaru uz mogućnost prepoznavanja i do 160 reči u minuti. Sistemi za prepoznavanje govora koriste neuronske mreže i “uče” kako se izgovara svaka reč. Drugim rečima, system mapi kako svaka osoba izgovara reči tako da se drastično umanjuje mogućnost pogrešnog tumačenja.

Prepoznavanje glasa je veoma česta biometrijska tehnologija koja se često koristi kod sistema kojima se upravlja bez upotrebe ruku, kao što je *hands-free* kod mobilnih telefona. Verifikacija glasa zasniva se na poređenju korisnikovog zvučnog zapisa sa prethodno snimljenim zapisom i ima za cilj da odredi o kojoj se osobi radi. Verifikacija i prepoznavanje glasa beleži ritam, frekvenciju, visinu, tonalitet glasa i sl. Za snimanje glasa moguće je koristiti i običan ili telefonski mikrofonski, mada se pouzdanost skeniranja povećava upotrebom kvalitetnijih mikrofona. Ovo nije naročito pouzdana metoda, pa se tako koristi u verifikacione, a ne identifikacione svrhe. Vreme verifikacije je oko pet sekundi. Veličina dobijenog zvučnog zapisa je reda veličine 2-10Kb [49]. Kako bi se izbegao falsifikat korišćenjem snimka, sistem traži istovremeno i visoke i niske frekvencije zvuka jer je to u većini snimaka nemoguće reprodukovati, tačnije, one se mogu naći samo u pravom glasu. Takođe, neki sistemi generišu nasumičan niz brojeva koji osoba treba da izgovori. Prednost ove metode je što je potrebna oprema izuzetno jeftina i svaki današnji kompjuter, uz odgovarajući softver, može da se iskoristi kao platforma za prepoznavanje glasa. Međutim, nizak nivo pouzdanosti prepoznavanje glasa čini dopunskom metodom uz neku drugu, pouzdaniju biometrijsku metodu. [56]

Osnovni faktori koji mogu uticati na greške pri autentifikaciji su [63]:

- Godište-glas se menja godinama;
- Bolest-glas se menja u slučaju da je osoba npr. prehladna;
- Akustika-zavisiti od sredine u kojoj se vrši autentifikacija;
- Pogrešno pročitane i izgovorene unapred definisane reči ili fraze;
- Emotivno stanje osobe koje može biti narušeno usled npr. stresa ili hapšenja;
- Položaj ili udaljenost od mikrofona kao i upotreba drugog tipa mikrofona.

Tehnologija prepoznavanja glasa se danas najčešće koristi u sistemima u kojima se zahteva identifikacija na daljinu. Kao primer se mogu navesti automatizovani pozivni centri i sistemi za obradu transakcija putem telefona ili računara. Popularne aplikacije iz ove oblasti su finansijske transakcije (pristup računu, transfer sredstava, plaćanje menica) i podrška sigurnosti u poslovanju kreditnim karticama.

Kao primer primene tehnologije prepoznavanja glasa, može poslužiti *Voice Identification and Verification Agent* (VIVA), proizvod IBM-ovog istraživačkog tima. VIVA omogućava verifikaciju korisnika putem telefona. Verifikacija se vrši kombinovanjem dva izvora informacija: karakteristike glasa korisnika ("*voice print*") i znanja korisnika (lozinka i/ili lične informacije). Kombinacijom ova dva izvora, povećava se pouzdanost verifikacije. Proces verifikovanja sastoji se iz jedne ili nekoliko kratkih konverzacija. Tokom konverzacije VIVA korisniku postavlja slučajna pitanja, proverava dobijene odgovore kao i "*voice-print*" korisnika. Trajanje identifikacije zavisi od tačnosti odgovora i procene "*voice-print*"-a korisnika. U slučaju kada je na telefonskoj liniji regularni korisnik, konverzacija obično kratko traje i sastoji se od svega jednog pitanja. Usled dobrog poklapanja glasovnih profila VIVA odmah zaključuje da je reč o pravom korisniku (slika 32.).



Slika 32: IBM VIVA sistem za prepoznavanje glasa

U slučaju pokušaja lažnog predstavljanja konverzacija traje znatno duže. Zbog nepodudaranja glasovnih profila VIVA postavlja više pitanja sve dok potencijalni korisnik ne da pogrešan odgovor ili VIVA ne zaključi da su glasovni profili definitivno različiti.

3.4.6 Drugi biometrijski sistemi

Pored prethodno pomenutih i opisanih sistema postoji još nekoliko sistema za autentifikaciju i identifikaciju ljudi kao što su: potpis, DNK analiza, termalni otisak lica (termogram), raspored vena na članku ili spoljnom delu šake, način hodanja, dinamika kucanja na tastaturi, oblik uha ili miris tela. Umesto da se koristi samo jedna tehnologija, radi povećanja pouzdanosti, u praksi se, kako opada cena računarske opreme, sve češće koriste multimodalni sistemi koji podržavaju i kombinuju više tehnologija. U tabeli 3. dat je pregled i poređenje većeg broja biometrijskih sistema [60].

Sistem	Univerzalnost	Jedinstvenost	Trajnost	Prikupljivost	Performanse	Prihvatljivost	Mogućnost podvale
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	V
Geometrija dlana	S	S	S	V	S	S	S
Dinamika kucanja	N	N	N	S	N	S	S
Raspored vena dlana	S	S	S	S	S	S	V
Dužica	V	V	V	S	V	N	V
Mrežnjača	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N
Miris	V	V	V	S	V	N	N
Oblik uha	S	S	V	S	S	V	S
Način hodanja	S	N	N	V	N	V	S
Termogram lica	V	V	N	V	S	V	V
DNK	V	V	V	S	V	N	N

V-visok; S-srednji; N-nizak

Tabela 3: Poređenje biometrijskih sistema

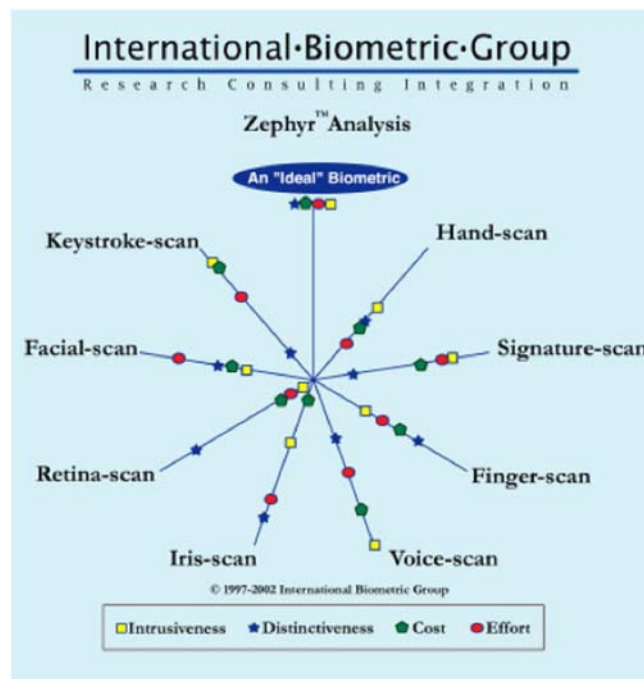
Za što bolji autentifikacioni sistem, potrebno je ispuniti neke uslove. Za dobar autentifikacioni sistem, potrebno je da budu ispunjeni uslovi kao što su: univerzalnost, jedinstvenost, trajnost i prikupljivost podataka. Kako bi biometrijski autentifikacioni sistem bio što praktičniji, treba najozbiljnije uzeti u obzir i performanse, prihvatljivost od strane korisnika kao i mogućnost da dođe do zloupotrebe. Još neki dodatni poželjni uslovi su: jednostavnost upotrebe i implementacije kao i cena koštanja sistema.

Potrebni uslovi:

1. **Univerzalnost** –svaka osoba mora sadržati neki biometrijski identifikator. Problem može biti taj što postoji mogućnost da osoba izgubi deo tela potreban za identifikaciju.
2. **Jedinstvenost** –dve osobe moraju imati dovoljno različitosti po pitanju biometrijskih identifikatora. Mogući problem mogu biti što identični blizanci imaju identičnu DNK strukturu i isti otisak lica.
3. **Trajnost** –identifikatori vremenski mogu biti dovoljno dugotrajni. Problem je taj što je ranjavanjem moguće da dođe do izmene lica, glasa, prstiju...
4. **Prikupljivost** –biometrija može biti kvantitativno izmerena. Problemi je kako odrediti koji se biometrijski podaci mogu lako prikupiti.
5. **Performanse** –preciznost sistema, brzinu, robustnost... Problem je kako iz mnoštva biometrijskih sistema treba odrediti koji je najbolji.

6. **Prihvatljivost** – podrazumeva dozu prihvatljivosti od strane ljudi u njihovom svakodnevnom životu. Sve prisutniji problem je što mnogi ljudi ne žele da daju svoje biometrijske podatke zbog sumnje u očuvanje privatnosti podataka.
7. **Mogućnost podvale** –koliko je komplikovano/jednostavno „probiti“sistem. Konstantna opasnost je u tome što neke sisteme je lako falsifikovati kao što je potpis ili glas.
8. **Pouzdanost** – odnosi se na osetljivost senzora, ograničenja procesa obrade kao i stabilnost u procesu autentifikacije. Najveći problemi je u tome što ni jedan sistem nije 100% siguran i pouzdan pa tako uvek postoji mogućnost za napredak po pitanju sveukupne bezbednosti.
9. **Jednostavnost upotrebe** – koliko je biometrijski sistem jednostavan za upotrebu od strane korisnika. Postavlja se pitanje može li sistem biti toliko jednostavan da korisnici ne moraju da razmišljaju o sigurnosnim aspektima.
10. **Jednostavnost implementacije** – podrazumeva se da sistem bude što jednostavniji za implementaciju i sjedinjavanje sa postojećim okruženjem. Problemi koji mogu nastati su ti da sjedinjavanje nekad može biti komplikovana ili čak i nemoguća, a sama implementacija i veoma skupa.
11. **Cena** – obuhvata više parametara kao što su: oprema, instalacija, obuka, kao i izrada samog sistema. Ono što može predstavljati veliki problemi je taj što bez obzira na cenu pomenutih parametara, ipak najveću cenu ima izgubljenno poverenje u slučaju da dođe do „pada“ i „probijanja“ sistema.

Biometrijski sistemi autentifikacije se ugrađuju u sve više sistema, kao što su mobilni telefoni, tastature i sl. i nije jednostavno odrediti koji je sistem „najbolji“. Međunarodna grupa za biometriju (*The International biometric group*) razvila je grafički model koji pokazuje koliko se svaki od navedenih sistema razlikuje od idealnog biometrijskog sistema. Na slici 33. prikazan je odnos različitih biometrijskih sistema po pitanju cene, sigurnosti, jednostavnosti upotrebe i nenametljivosti [63].



Slika 33: Poređenje različitih biometrijskih sistema

4. Sigurnost biometrijskog sistema

Biometrija poseduje snagu za dodavanje sigurnosti mnoštvu aplikacija. Već sada, biometrija se koristi za zaštitu ličnih računara, ATM terminala, transakcija platnim karticama, e-transakcija, aerodroma, nuklearnih postrojenja i međunarodnih granica. Pa ipak, iako biometrijski sistem ima ulogu povećanja sigurnosti, on, kao i svaki drugi sistem, ima i svojih slabosti.

4.1 Napadi na biometrijski sistem

Ovaj odeljak se odnosi pre svega na sisteme za skeniranje otisaka prstiju i dužice oka kao osnovne biometrijske sisteme autentifikacije. Sami napadi se mogu grupisati u tri kategorije i to [67]:

- Napadi na ulaznom nivou;
- Napadi na nivou obrade i prenosa podataka;
- Napadi na nivou čuvanja podataka.

4.1.1 Napadi na ulaznom nivou

Odnose se na faze uzimanja uzorka i početka obrade. Osnovna dva oblika napada su obmana (eng. *spoofing*) i premošćavanje (eng. *bypassing*).

Pored ta dva oblika, veoma je čest slučaj i izazivanje preopterećenja (eng. *overloading*) oštećujući ulazni uređaj ili primoravajući ga da generiše greške. Kao primer može se uzeti kratko povezivanje ili kvašenje poluprovodničkih senzora ili izlaganje senzora otiska ili crta lica bljesku svetlosti.

4.1.2 Napadi na nivou obrade i prenosa podatka

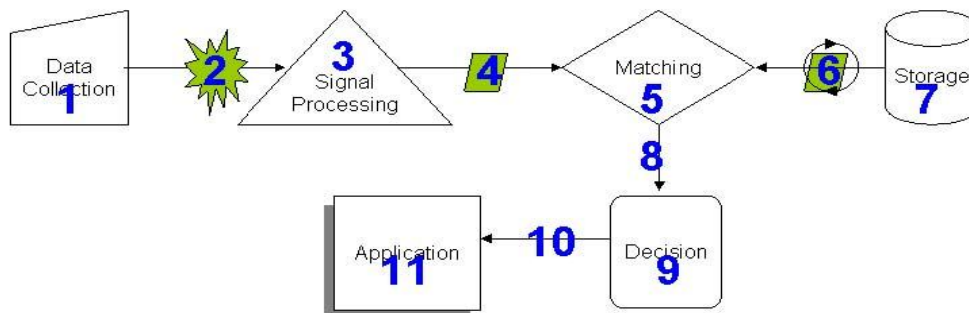
Ovaj oblik napad takođe zaokuplja pažnju. Kako mnogi biometrijski sistemi sliku ili šablon podatka šalju ka lokalnom ili udaljenom računaru na obradu, od velike je važnosti da ovaj prenos bude siguran u smislu da prenos ne bude prekinut, očitao ili izmenjen. Većina biometrijskih sistema šifrjuje podatke pri prenosu ali se to ne odnosi uvek na same aplikacije i uređaje. Sami razvijaoци sistema prema tome koja slika ili šablon mogu biti izloženi kompromitaciji i u skladu sa potrebama definišu najbolja rešenja. Anti-spoofing mere kao i enkriptovanje podataka pri prenosu predstavljaju kritične tačke biometrijske sigurnosti koje se mogu unaprediti tzv više-faktornom autentifikacijom i randomizacijom.

Više-faktorna autentifikacija se može predstaviti u dva oblika, kao kombinacija više biometrijskih metoda ili kombinacija biometrije i pametnih kartica ili PIN-a. Oba metoda redukuju mogućnost neželjene autentifikacije. Sam *spoofing* postaje vremenski zahtevniji i izazovniji ako je potrebno kopirati ili imitirati više ljudskih karakteristika.

Randomizacija je takođe nešto što povećava nivo sigurnosti. Na primer, verifikacioni podaci mogu biti randomizovani pa tako, za autentifikaciju, jedan dan se mogu tražiti tri prsta, drugi dan dva, treći dan druga kombinacija prstiju itd.

Jedna od novijih tehnika za slabljenje posledica napada je IBM-ov koncept tzv.poništavajućeg biometrijskog sistema. Koncept predviđa upotrebu algoritama koji će uneti deformisanost na sačuvani šablon. Za slučaj da se naruši integritet šablona, šablon se uklanja sa liste onih kojima je dozvoljen pristup i legalni korisnik će moći ponovo da se prijavi pri čemu će se kreirati njegov novi šablon sa dodatim deformitetom. Originalna slika

se nikad ne čuva. Sve dok je algoritam dobro zaštićen i različit zavisno od kompanije ili čak i samog sistema, ovo rešenje vodi ka smanjenju eventualno nastale štete. Rešenje ipak, nije potpuno sigurno. Ako se dođe do originalne slike, teoretski moguće je izvršiti ponovnu prijavu uz generisanje novog izobličenog šablona. I pored toga, kreiranje poništavajućeg biometrijskog sistema je korak u dobrom pravcu. Ako biometrijsko društvo nastavi otvoreno i agresivno da identifikuje slabosti i nastavi da razvija načine za jačanje sistema, korist za celokupno društvo biće nemerljiva. Na slici 34. i u tabeli 4. prikazane su glavne slabe tačke u procesu biometrijske autentifikacije [67].



Slika 34: Slabe tačke biometrijskog sistema

Tačka	Pretnje	Kontra-mere
1 Prikupljanje podataka	Obmana	Provera živosti
	Upotreba uređaja bez poverenja	Obostrana autentifikacija uređaja i servera
	Preopterećenje	Upotreba snažnih uređaja
2 Prenos originalnih podataka	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
3 Obrada signala	Umetanje lažnih podataka	Upotreba snažnih algoritama
4 Prenos obrađenih podataka	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
5 Poređenje	Umetanje lažnih podataka	Upotreba snažnih algoritama

6 Uzimanje šablona	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
7 Čuvanje	Kompromitacija baze podataka	Snažnija zaštita šifrovanjem servera za smeštanje šablona. Smeštanje šablona na pametne kartice ili slične uređaje.
8 Prikaz rezultata poređenja	„Hill climbing“ napad	Inkrementalna povratna sprega
9 Odlučivanje	„Hill climbing“ napad	Inkrementalna povratna sprega
10 Komuniciranje sa aplikacijom	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
11 Aplikacija	Maliciozni kôd	Poštovati standarde (BioAPI, CBEFF)

Tabela 4: Slabe tačke biometrijskih sistema

4.2 Različiti načini biometrijske implementacije

Sa sigurnosnog aspekta, dva osnovna elementa biometrijskog sistema su:

- Čuvanje (u centralnoj bazi, u lokalnoj bazi, u portabl uređaju-pametna kartica, u senzoru)
- Poređenje (u centralnom serveru, u lokalnom računaru, u senzoru, na pametnoj kartici)

Zavisno od kombinacija ovih elemenata, različiti su i sigurnosni rezultati. U tabeli 5. prikazane su kombinacije čuvanja i poređenja šablona otiska prsta. Neke od kombinacija (obeležene sa X) se ne koriste u komercijalne svrhe pa kao takve nisu ni uzete u razmatranje [61].

Mesto poređenja	Mesto čuvanja			
	Centr. baza	Lok. baza	Senzor	Pametna kartica
Centralni server	A	X	X	B
Lokalni server	X	C	X	D
Senzor	X	X	E	F
Pametna kartica	X	X	X	G

Tabela 5: Kombinacija mesta čuvanja podataka, i mesta

4.2.2 Pregled sigurnosti

A - Poređenje na centralnom serveru / Čuvanje u centralnoj bazi

Poređenje u centralnom serveru podrazumeva poređenje u zaštićenom okruženju. Administrator ima mogućnost da kontroliše sistem i detektuje pokušaje napada. Čuvanje šablona na serveru u centralnoj bazi podrazumeva, takođe, da je šablon zaštićen od zloupotrebe spolja. Jedan od sigurnosnih problema je prenos šablona od skenera-senzora do servera što zahteva sigurnu Internet sesiju ili kriptografsko rešenje.

Zaključci:

- + Administrator ima punu kontrolu nad bazom podataka;
- Moguće je nasilno narušavanje integriteta;
- Rešenje zahteva kompletno novu infrastrukturu;
- Otisci prstiju se prenose putem otvorene mreže.

B - Poređenje na centralnom serveru / Čuvanje na pametnoj kartici

U ovom slučaju, šablon ostaje kod korisnika na pametnoj kartici, dok je prenos i smeštanje šablona na server van kontrole korisnika. Drugi problem kod servera je taj što se prenos podataka kroz nepouzdanu mrežu povećava. Sad se prenose i originalna slika i šablon što bi trebalo rešiti šifrovanjem veze.

Zaključci

- Moguće je narušavanje integriteta;
- Rešenje zahteva kompletno novu infrastrukturu;
- Otisci prstiju se prenose putem otvorene mreže iako je veza šifrovana.

C - Poređenje u lokalnom računaru / Čuvanje u lokalnoj bazi

Ovo je česta kombinacija kod koje se šablon čuva na hard disku na kojem se vrši i poređenje. Kako lokalni računar ne spada u sigurna okruženja postoji realna opasnost da šablon ili lozinka mogu biti ukradeni. Isto tako, problem može biti i mobilnost, odnosno, korisnik se može prijaviti samo na računaru na kojem se nalazi šablon.

Zaključci:

- + Korisnik ima kontrolu nad šablonom;
- Lokalni računar nije sigurno okruženje za osetljive podatke;
- Rešenje nije skalabilno čak ni u lokalnoj mreži.

D - Poređenje u lokalnoj bazi / Čuvanje na pametnoj kartici

Ova kombinacija rešava neke probleme iz prethodne (c) kombinacije. U slučaju pametne kartice, čest pristup zaštićenoj zoni unutar iste predstavlja kritičnu tačku. Razlog za to je sledeći: pristup je dozvoljen samo ako se unese tačan PIN za pristup kartici (PIN se proverava na samoj kartici) međutim, ovde se i PIN i šablon prenose od kartice do lokalnog računara kako bi se u lokalnoj bazi proverio šablon. Ako uneta slika odgovara šablonu, PIN se vraća nazad do kartice kako bi se omogućio pristup. Do šablona je nemoguće doći dok god se nalazi na kartici ali, osetljive informacije, kao što su šablon i PIN mogu biti meta napada u fazi slanja na lokalni računar.

Zaključci:

- + Korisnik brine o svom šablonu;
- + Korisnik može iskoristiti karticu za pristup mnogim sistemima;
- Šablon je izložen spoljnim napadima tokom verifikacije;
- Rešenje se ne može koristiti za osiguranje mrežnih transakcija.

E - Poređenje u senzoru / Čuvanje u senzoru

U ovom slučaju, sve informacije se nalaze u senzoru što drastično otežava zloupotrebu s tim da ovde i sam vlasnik ne može doći do svog šablona..

Zaključci:

- + Korisnik ima kontrolu nad šablonom;
- + U slučaju obezbeđenog uređaja, šablon nikad nije izložen spoljnim uticajima;
- Ograničena je prenosivost jer se šablon nalazi u senzoru i ne može mu se pristupiti putem nekog drugog uređaja.

F - Poređenje u senzoru / Čuvanje na pametnoj kartici

Ovde se poređenje vrši na takođe sigurnijem mestu od PC-a, na samom senzoru. I dalje postoje PIN ili lozinka za pristup pametnoj kartici. Kad se potvrdi autentičnost otiska prsta, PIN ili lozinka se vraćaju pametnoj kartici kako bi omogućili pristup.

Zaključci:

- + Šablonu se može pristupiti sa svakog uređaja;
- + Korisnik kontroliše sopstveni šablon;
- Šablon je izložen spoljnim napadima tokom verifikacije;
- Postoji sigurnosna rupa kod upotrebe pametne kartice za smeštanje sertifikata (PKI), s obzirom da se PIN za otključavanje kartice, i koji se nalazi na njoj, šalje do senzora pre nego što se dozvoli pristup kartici.

G - Poređenje na pametnoj kartici / Čuvanje na pametnoj kartici

Predstavlja najsigurniju opciju gde šablon nikad ne napušta karticu i ne postoji nikakva informacija, kao što je PIN, koji može biti ukraden kao u prethodno opisanim slučajevima jer se uspešnim poređenjem unete slike i šablona omogućava upotreba sertifikata bez ikakve potrebe za PIN-om ili lozinkom. Ovaj metod predstavlja najsigurniji način biometrijske zaštite računara, mreža i generalno digitalnih podataka.

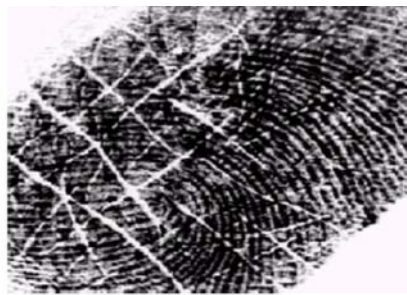
Zaključci:

- + Pametnoj kartici se ne može pristupiti bez odgovarajuće biometrijske autentifikacije;
- + Šablon nikad nije izložen nesigurnom okruženju;
- + Korisnik kontroliše svoj šablon;
- + Rešenje je zasnovano na PKI bez potrebe za novom infrastrukturom.

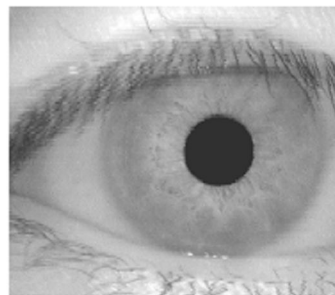
5. Multimodalni biometrijski sistemi

Biometrijska autentifikacija, kao što je poznato, predstavlja automatsko prepoznavanje korisnika prema njegovim biološkim odnosno, fizičkim karakteristikama. Pored očiglednih prednosti koje donosi, razvoj biometrijske autentifikacije se suočava sa većim ili manjim poteškoćama. Unimodalni biometrijski sistemi instalirani u realnim aplikacijama obezbeđuju prepoznavanje korisnika na podacima dobijenim iz jednog izvora biometrijskih podataka. Jedan od osnovnih problema ovakvih sistema je nedovoljna preciznost. Kod upotrebe lozinke, ako je ona tačna, sistem će je prihvatiti dok kod biometrijske autentifikacije, čak iako je identifikator tačan, ne postoji garancija da će biti prihvaćen od strane sistema. Najčešći razlozi za to su [62]:

- **Greška u očitanim podacima** – javlja se usled lošijih senzora ili nepovoljnih uslova. Kao primer može se uzeti postojanje ožiljka na prstu (slika 35) ili je glasa izmenjenog usled niske temperature sredine. Isto tako, razlozi lošeg očitavanja ulaznih podataka mogu biti i zaprljan senzor kod očitavanja otiska prstiju ili izmenjen položaj dužice oka (slika 36).



Slika 35: Loš otisak prsta



Slika 36: Zamagljena slika dužice oka
usled gubljenja fokusa

- **Loša interakcija sistema i korisnika** – javlja se kod nepravilne upotrebe sistema ili kod izmene karakteristika istog. Najčešće, biometrijski podaci, uneti u procesu verifikacije neće biti identični onima unetim tokom prijavljivanja na sistem. Ovaj slučaj je poznat i pod nazivom „varijacije unutar razreda“ (eng. *Intra-Class-Variations*) i može nastati usled loše interakcije korisnika i senzora (različita sila pritiska senzora ili različiti položaji prsta ili lica pred senzorom (slika 37). Isto tako, promene spoljnih uslova (neadekvatno osvetljenje, slika 38)

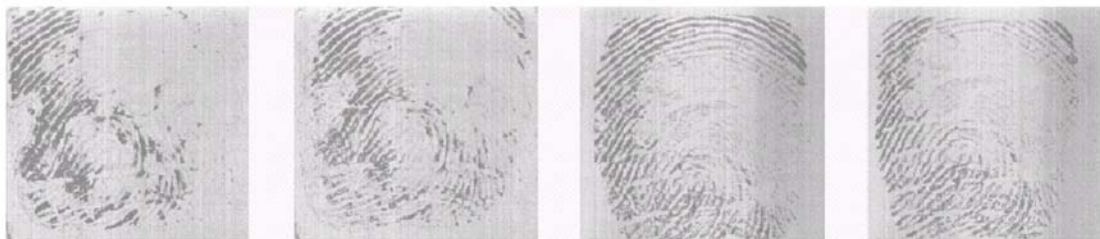


Slika 37: Nepravilna upotreba sistema



Slika 38: Neadekvatno osvetljenje

- **Nizak nivo različitosti** – iako se očekuje da među osobama postoji značajan nivo različitosti po pitanju biometrijskih karakteristika, to nije slučaj. Kao primer može se uzeti sistem zasnovan na očitavanju crta lica korisnika. Ovakav sistem je dosta ograničen. Jednostavno, često postoji velika sličnost između blizanaca, roditelja i deteta i sl. Što prouzrokuje visok stepen greške odnosno, pogrešan rezultat poređenja šablona (eng. *FMR*, *False Match Rate*).
- **Ne-univerzalnost** – iako bi svaka osoba trebala da poseduje sebi svojstvene biometrijske podatke, to nije uvek slučaj. Primer su otisci prstiju lošeg kvaliteta (slika 39) što se, prema istraživanjima, odnosi na 4% svetske populacije.



Slika 39:Slabo izraženi otisci prstiju

- **Napadi obmanjivanjem sistema.**



Slika 40: Način upotrebe lažnih otisaka prstiju

Isto tako, postoji mogućnost da, onaj ko se lažno predstavio, ipak bude regularno prihvaćen od strane sistema tako da je povećanje sigurnosnih performansi, više nego poželjno.

Kroz ove praktične prikaze, vide se problemi sa kojima se suočavaju unimodalni biometrijski sistemi i koji su, usled grešaka koje proizvode, neprihvatljivi u sigurnosnim aplikacijama.

5.1 Poboljšanje performansi sistema

Kako poboljšati performanse? Jednostavno, postoje određene faze razvoja sistema kad je nemoguće više poboljšati performanse unetog identifikatora tako da uvek postoji potreba i potraga za drugim izvorima podataka gde za ta poboljšanja ima mogućnosti.

Integracioni pristup kod poboljšanja performansi može se realizovati na više načina. Neki od navedenih problema, u prethodnom poglavlju, mogu se prevazići kombinacijom biometrijskih karakteristika i ne-biometrijskih podataka, zasnovanih na posedovanju ili znanju. Kombinovanje biometrijskog identifikatora i npr. pametne kartice, značajno se povećava sigurnost celokupnog sistema za slučaj lažnog predstavljanja. Ipak, ovaj oblik prate problemi svojstveni svim sistemima zasnovanim na posedovanju (krađa ili gubljenje identifikatora i sl.). Iz svega rečenog proizilazi da je potrebno izvršiti integraciju tj. sjedinjavanje više biometrijskih identifikatora, odnosno upotrebljavati sistema sa višestrukom biometrijskom autentifikacijom. To su tzv. multimodalni biometrijski sistemi.

Pretpostavke o univerzalnosti, prikupljivosti, pristupačnosti i integritetu podataka daleko su realnije ako su zasnovane na informacijama od više biometrijskih identifikatora.

Multimodalni biometrijski sistemi obezbeđuju viši nivo sigurne autentifikacije upotrebom većeg broja biometrijskih izvora informacija, smanjuje nivo greške kao i mogućnost obmanjivanja sistema lažnim predstavljanjem. Međutim, isto tako ovi sistemi često zahtevaju i duže vreme autentifikacije (uz veću efikasnost pretraživanja), zahtevaju snažnije računarske

resurse i imaju višu cenu. Na slici 41, prikazane su neke od kombinacija biometrijskih karakteristika.

5.1.1 Opis performansi

Za dobro razumevanje prednosti multibiometrijskog pristupa date aplikacije, nužno je objasniti značenje termina „performanse“ i „povećanje performansi“. Kriterijumi kao što su tražena tačnost, cena i brzina sistema, od značaja su za procenu performansi. Međutim, kako su cene sve snažnijih procesora i biometrijskih senzora drastično snižene, fokus kod procene performansi, sigurno će većim delom biti na traženoj tačnosti tj. preciznosti očitavanja podataka. Iz razloga jednostavnijeg prikaza, ova dva parametra nisu uzeta u obzir.

Biometrijski sistem može proizvesti dva tipa grešaka: pogrešno prihvatanje (FA) kad se prihvati korisnik koji se lažno predstavio i pogrešno odbijanje (FR), kad se odbije regularan korisnik. Treba napomenuti da je procenat grešaka važna ali ne i sastavni deo evaluacije performansi sistema. Takođe, bitno je reći i da cena pogrešnog odbijanja i pogrešnog prihvatanja nije ista i zavisi prevashodno od domena upotrebe aplikacije. Na primer, aplikacije za kontrolu pristupa visoko osetljivim instalacijama zahtevaju što manje pogrešno prihvatanje dok je to obrnuto kod forenzičkih aplikacija kod kojih se vrši provera načina pristupa u cilju hvatanja kriminalca. Samim tim, forenzičke aplikacije pretežno zahtevaju upotrebu sistema koji proizvode greške pogrešnog prihvatanja.

Za naredni prikaz, pretpostavka je da je cena grešaka ista, da je učestanosti lažnog predstavljanja identična učestanosti ispravnog predstavljanja

Pretpostavimo da je B posmatrani biometrijski sistem, a $T^1, T^2, ..T^n$ predstavljaju šablone n prijavljenih korisnika na sistem. Radi jednostavnijeg računa pretpostavićemo da svaki korisnik ima sačuvan samo jedan šablon, za svaku biometrijsku karakteristiku iz čega proizilazi da šablon za i -og korisnika, $T^i = \{T_1^i, T_2^i, ..T_m^i\}$, sadrži m komponenti gde su $T_1^i, T_2^i, ..T_m^i$ šabloni različitih biometrijskih karakteristika, a m broj upotrebljenih istih. Neka (T^0, I) označava biometrijsku karakteristiku i identitet I korisnika. Šablon T^0 kao što je prethodno rečeno, sadrži m komponenti. Identitet I pripada ili W_t ili W_n kategorijama gde W_t predstavlja tačan (originalni korisnik), a W_n netačan odgovor (lažni korisnik). Biometrijski sistem B poredeći T^0 sa T^i , određuje kojoj grupi će pripasti identitet I .

$$I \in \begin{cases} W_t & \text{ako } F(T^0, T^i) > \varepsilon \\ W_n & \text{drugo} \end{cases} \quad [6]$$

Gde je $F(T^0, T^i)$ proizvoljna promenljiva koja prikazuje sličnost između T^0 i T^i , a ε je tzv. *threshold*.

Prikažimo $F(T^0, T^i) > \varepsilon$ jedinstvenom oznakom R . Procenti grešaka usled pogrešnog odbijanja $FR(R)$ i pogrešnog prihvatanja $FA(R)$ u funkciji od R su:

$$\begin{aligned} FR(R) &= 1 - \int_R f(I|W_t) dI \\ FA(R) &= \int_R f(I|W_n) dI \end{aligned} \quad [7]$$

gde $f(I|W_t) dI$ i $f(I|W_n) dI$ predstavljaju funkcije uslovne gustine verovatnoće originalnog i lažnog korisnika. Ukupan rizik $E(R)$ je:

$$E(R) = C_{FR} \cdot FR(R) + C_{FA} \cdot FA(R) \quad [8]$$

gde C_{FR} i C_{FA} predstavljaju troškove usled grešaka. U situaciji kad su $C_{FR} = C_{FA} = 1$, rizik je jednak ukupnom riziku. Minimalan ukupan rizik $E(R_{min})$ definisan je kao:

$$E(R_{min}) = \text{Min}_R \{ C_{FR} \cdot FR(R) + C_{FA} \cdot FA(R) \} \quad [9]$$

Uzeti sada multibiometrijski scenario sa dva biometrijska sistema. Neka B_i , $i=1,2$ budu dva ta biometrijska sistema od kojih svaki koristi različite biometrijske identifikatore, FR , FA , E i E_{min} biće [57]:

$$FR_i(R_i) = 1 - \int_R f_i(I_i | W_i) dI_i$$

$$FA_i(R_i) = \int_R f_i(I_i | W_n) dI_i \quad [10]$$

$$E_i(R_i) = C_{FR} \cdot FR_i(R_i) + C_{FA} \cdot FA_i(R_i)$$

$$E_i(R_{mini}) = \text{Min}_R \{ C_{FR} \cdot FR_i(R_i) + C_{FA} \cdot FA_i(R_i) \}$$

6. Izvor i sjedinjavanje podataka

Dizajn multi-biometrijskog sistema je veoma zavisan od scenarija aplikacije. Broj multimodalnih biometrijskih sistema zavisi od njihove arhitekture, količine i izbora biometrijskih identifikatora, nivoa na kojem će se podaci integrisati kao i od metoda samog sjedinjavanja odnosno, fuzije ulaznih podataka tj. identifikatora. Odnosno, potrebno je sagledati mnoštvo faktora pre dizajniranja sistema što obuhvata:

- **Broj biometrijskih osobina** - zavisi od same aplikacije kao i veze između samih osobina korisnika koje se snimaju. Kod mobilnog telefona opremljenog kamerom, najjednostavnije je kombinovati crte lica i glas. Kod ATM terminala, je najjednostavnija kombinacija otisak prsta i crte lica;
- **Nivo unutar sistema na kojem će se informacije integrisati** - postoje četiri osnovna nivoa i to: nivo senzora, nivo izdvajanja šablona ulaznih podataka, nivo poređenja i nivo odlučivanja. Iako je za očekivati da je najbolja opcija sjedinjavanja na ulaznom nivou, pri izdvajanju biometrijskih podataka, to nije uvek slučaj iz više razloga. Pre svega, većina komercijalnih sistema ne dozvoljava pristup informacijama na tom nivou, drugo, a i sami podaci možda nisu međusobno kompatibilni. Sjedinjavanje na nivou odlučivanja je problematično iz razloga nedostatka informacija. Odnosno, na nivou odlučivanja figuriraju samo dve informacije: „Prihvaćen“ i „Odbijen“. Iz prethodno navedenih razloga, sjedinjavanje se najčešće obavlja na nivou poređenja šablona i predstavlja kompromis druga dva modela;
- **Način sjedinjavanja podataka;**
- **Cena**

6.1 Šta sjediniti ?



Slika 41: Primer multi-biometrijskog sistema

Multimodalni biometrijski sistem prevazilazi neka ograničenja unimodalnih biometrijskih sistema sjedinjavanjem biometrijskih karakteristika sa više izvora. Ti izvori mogu biti, kao što je prikazano na slici 41.:

- **Više senzora** – veći broj senzora za unos istog podatke. Na primer, upotreba optičkog i kapacitivnog senzora za očitavanje otiska prsta;
- **Više biometrijskih karakteristika** – kombinacija, na primer, otiska prsta i crta lica korisnika. U procesu verifikacije, na ovaj način se povećava sigurnost dobijenog rezultata dok se izborom odgovarajuće šeme sjedinjavanja može drastično ubrzati i sam postupak verifikacije. Važan aspekt ovakvog sjedinjavanja je i proces normalizacije rezultata. Normalizacija najčešće obuhvata mapiranje rezultata iz različitih u zajednički domen pre njihovog kombinovanja;
- **Više snimaka iste biometrijske karakteristike** – odnosi se na uzimanje više uzoraka istog podatka radi dobijanja što boljeg primerka;
- **Više uzoraka iste biometrijske karakteristike** – uzimanje otiska dva ili više prstiju ili uzimanje slike dužice oba oka iste osobe koji se mogu kombinovati;
- **Više načina obrade istog biometrijskog podatka** – podrazumeva više načina uzimanja podataka i obradu istog podatka sa više različitih algoritama itd.

Upotreba više senzora može umanjiti nivo greške ali svi ostali problemi, koji se javljaju kod unimodalnih sistema, ostaju. Upotreba više snimaka biometrijskih karakteristika kao i više uzoraka iste biometrijske karakteristike, odnosno, upotreba više algoritama za obradu podataka takođe može unaprediti performanse sistema. Međutim, sve ove metode i dalje pate od nekih problema unimodalnih biometrijskih sistema. Istovremena upotreba više različitih biometrijskih karakteristika rešava veći deo problema i kao takva, zaokuplja najveći deo pažnje dizajnera sistema.

6.2 Koje biometrijske karakteristike sjediniti ?

Kao što je rečeno u prethodnom poglavlju, izbor biometrijskih karakteristika koji će se kombinovati u jedan multimodalni biometrijski sistem, veoma je bitan i nije u potpunosti proizvoljan nego na njega utiče kompatibilnost istih. U tabeli 6. prikazane su najčešće kombinacije biometrijskih karakteristika kod multimodalnih biometrijskih sistema.

Kombinacija 1	Glas	Crte lica	
Kombinacija 2	Glas	Pomeranje usana	
Kombinacija 3	Glas	Crte lica	Pomeranje usana
Kombinacija 4	Otisak prsta	Crte lica	
Kombinacija 5	Otisak prsta	Crte lica	Glas
Kombinacija 6	Otisak prsta	Crte lica	Geometrija dlana
Kombinacija 7	Otisak prsta	Glas	Geometrija dlana
Kombinacija 8	Otisak prsta	Geometrija dlana	
Kombinacija 9	Termogram lica	Crte lica	
Kombinacija 10	Dužica oka	Crte lica	
Kombinacija 11	Otisak šake	Geometrija dlana	
Kombinacija 12	Oblik uha	Glas	

Tabela 6: Kombinacije biometrijskih karakteristika

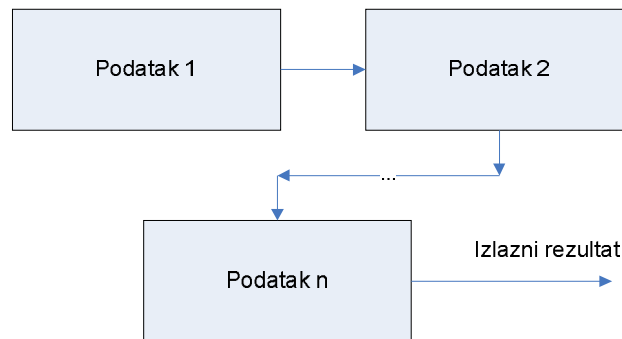
6.3 Arhitektura sjedinjavanja biometrijskih podataka

Arhitektura multimodalnih biometrijskih sistema odnosi se na onaj deo u kojem se podaci za autentifikaciju prikupljaju i obrađuju. Uglavnom, arhitektura može biti redna i paralelna ali, pored njih kao dodatni oblik, figurira i hijerarhijska arhitektura.

Na slikama 42a, 42b i 42c prikazana je moguća arhitektura sjedinjavanja različitih biometrijskih karakteristika.

6.3.1 Redna arhitektura

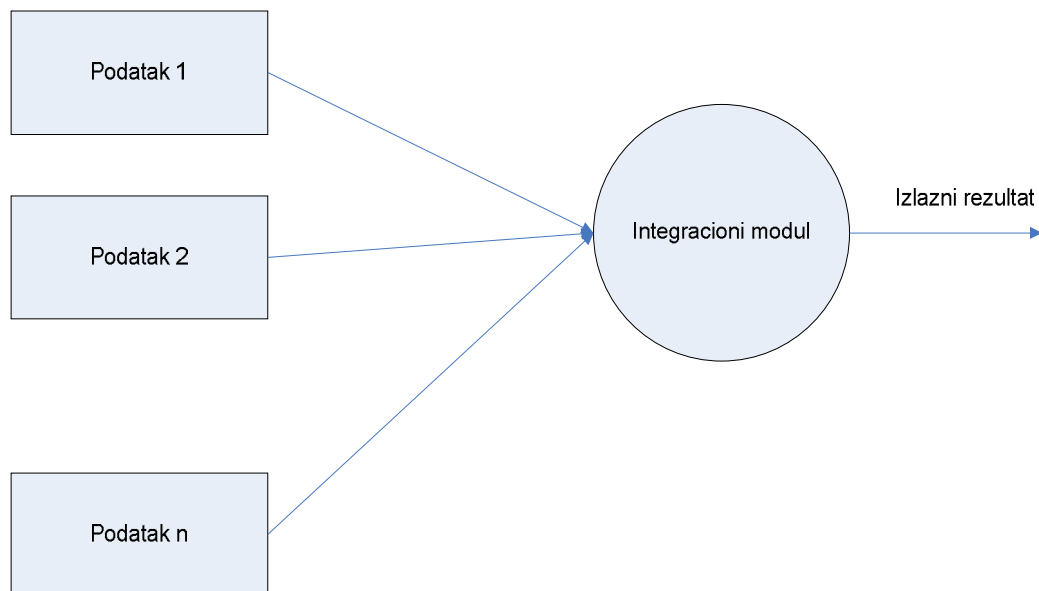
Kod redne arhitekture, obrada ulaznih podataka, potrebnih za autentifikaciju, obavlja se serijski, a rezultat obrade svakog podatka utiče na rezultat narednog podatka koji se obrađuje.



Slika 42a: Redna arhitektura sjedinjavanja

6.3.2 Paralelna arhitektura

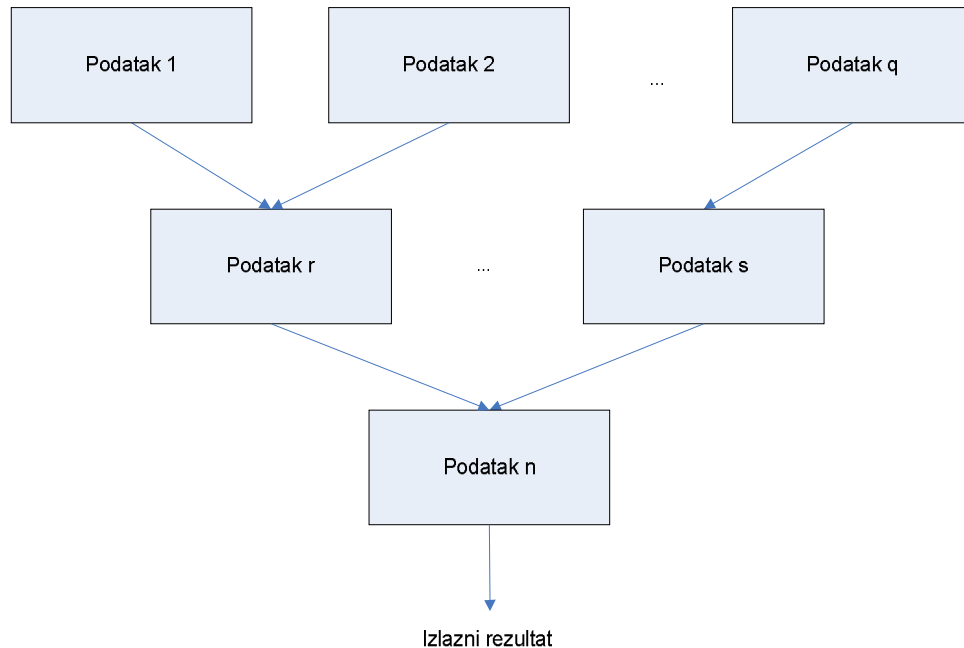
Kod paralelne arhitekture, različiti podaci deluju međusobno nezavisno i njihovi rezultati se sjedinjuju po određenoj šemi.



Slika 42b: Paralelna arhitektura sjedinjavanja

6.3.3 Hijerarhijska arhitektura

Hijerarhijska arhitektura predstavlja kombinaciju redne i paralelne arhitekture.



Slika 42c: Hijerarhijska arhitektura sjedinjavanja

I redni i paralelni oblik arhitekture ima svojih prednosti i mana.

Kod redne arhitekture, moguće je značajno povećati udobnost upotrebe, gledajući sa strane korisnika sistema kao i efikasno ubrzati pretragu u mnoštvu identifikacionih podatak. Na primer, kad se redni multimodalni biometrijski sistem dovoljno uveri u identitet korisnika nakon obrade prvog ulaznog podatka, korisnik neće morati da unosi i drugi podatak. Isto tako, sistem može da dozvoli korisniku da sam odabere koji biometrijski podatak će, kao prvi, predati sistemu na obradu kako bi se proverio identitet. Konačno, ako je sistem suočen sa pretragom za identitetom u velikoj bazi podataka, prvi obrađen podatak može iskoristiti kao filter za ubrzanje rada i povećanje efikasnosti samog sistema. Uopšte, redna arhitektura sistema obezbeđuje veću udobnost korisnika i veću brzinu rada od paralelne arhitekture. Pa ipak, redni sistem zahteva snažan i robustan algoritam koji će obraditi različite sekvence događaja.

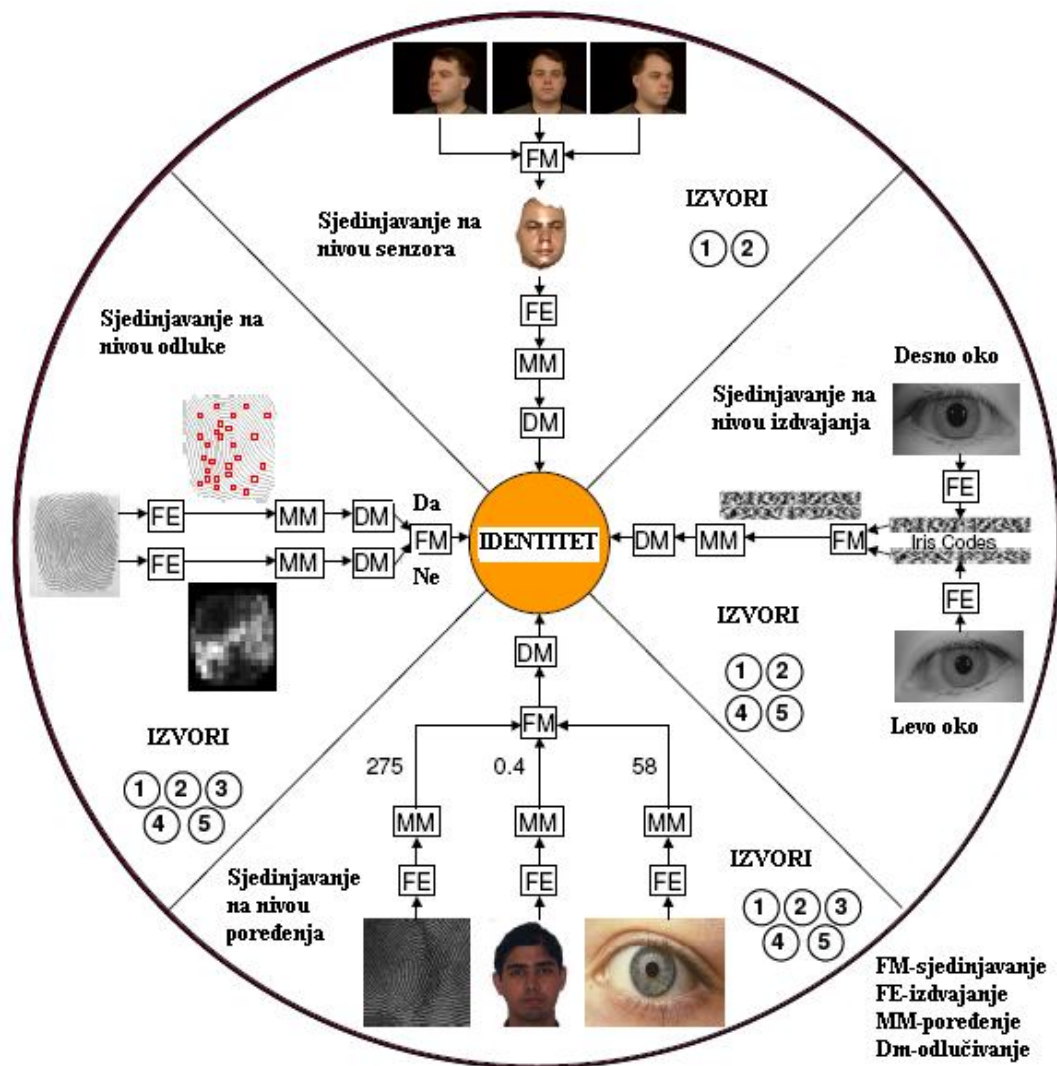
Primer rednog sistema predstavljen je od strane Honga i Džejn u [7]. U njihovom sistemu, prepoznavanje lica je korišćeno za dobijanje prvih i osnovnih n rezultata, a otisak prsta je imao ulogu potvrđivanje prethodnih rezultata i davanje konačne odluke o identitetu korisnika.

Kod paralelne arhitekture, u pitanju je ipak veći nivo tačnosti s obzirom da se koristi više podataka za autentifikaciju. Većina predloženih multimodalnih biometrijskih sistema ima paralelnu arhitekturu jer je primarni cilj dizajnera sistema, smanjenje grešaka [6] i [8].

Izbor arhitekture zavisi od potreba aplikacije. Korisnički orijentisani i, po pitanju sigurnosti, manje kritični ATM terminali mogu koristiti rednu arhitekturu dok, na primer, pristup vojnim instalacijama, koji zahteva najviši mogući nivo sigurnosti, trebalo bi da koristi paralelnu arhitekturu sistema.

Kod hijerarhijske arhitekture zastupljena je kombinacija prednosti koje donose redna i paralelna. Može biti tako dizajnirana da bude robusna i snažna, a da istovremeno još rešava probleme nedostatka ili pojave sitnih šumova odnosno, grešaka pri očitavanju koje figuriraju u biometrijskim sistemima. Ipak, ovaj oblik arhitekture, nikad nije ozbiljnije razmatran od strane dizajnera.

6.4 Nivoi sjedinjavanja



Slika 43: Nivoi sjedinjavanja kod multi-biometrijskog sistema

Jednostavan biometrijski sistem se sastoji od četiri osnovna elementa:

- **Senzorski modul** – obezbeđuje prikupljanje podataka od korisnika;
- **Modul izdvajanja podataka** – obezbeđuje obradu prikupljenih podataka i kreiranje šablona;

- **Modul poređenja podataka** – obezbeđuje poređenje novokreiranog šablona sa šablonom sačuvanim u bazi podataka;
- **Modul odlučivanja** – obezbeđuje dobijanje konačnog rezultata autentifikacije na osnovu operacije izvršene u modulu poređenja. Odgovor sistema je „Prihvaćen-Odbijen“.

Ova četiri nivoa mogu biti kategorisani u dve kategorije:

- **Pre poređenja**
- **Posle poređenja**

Na slikama 44a, 44b i 44c prikazani su nivoi sjedinjavanja kod paralelne arhitekture.

6.4.1 Sjedinjavanje pre poređenja

Pre poređenja, sjedinjavanje ulaznih podataka može se obaviti ili na nivou senzora ili na nivou izdvajanja podataka (kreiranje šablona).

6.4.1.1 Nivo senzora

Veoma se retko koristi iz razloga što sjedinjavanje podataka na ovom nivou zahteva njihovu potpunu kompatibilnost što je veoma redak slučaj. Poređenje na nivou senzora se može obaviti samo u slučajevima da se koriste iste biometrijske karakteristika unete putem različitih ali kompatibilnih senzora ili više slika iste biometrijske karakteristike unete putem istog senzora. Kao primer, može se uzeti skeniranje lica posredstvom više kamera što može omogućiti stvaranje 3D slike istog lica ili stvaranje mozaika od više slika otiska prsta kako bi se dobila kompletnija informacija. Bitno je da na nivou senzora, podaci ne mogu biti sjedinjeni ako nisu kompatibilni. Nemoguće je, na primer, sjediniti slike lica dobijene kamerama sa različitim rezolucijama.

6.4.1.2 Nivo izdvajanja podataka

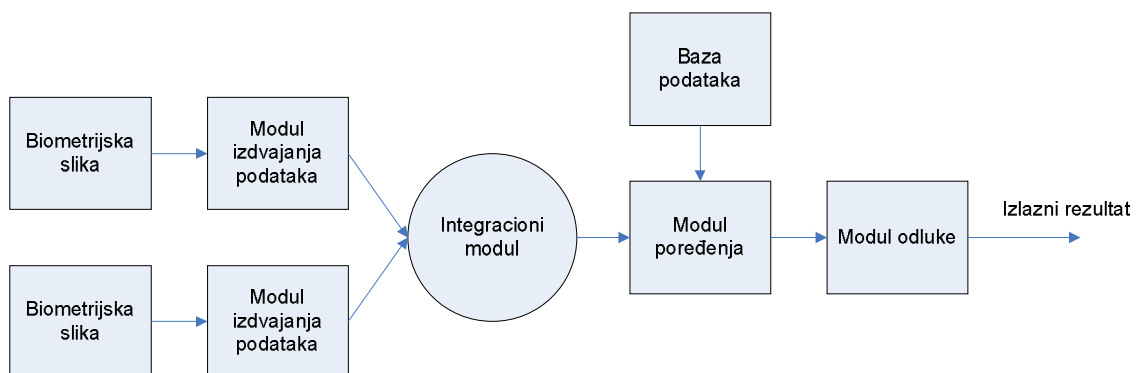
Vrši se kombinacija vektora različitih karakteristika dobijanih iz sledećih izvora: različiti senzori za istu biometrijsku karakteristiku, više slika ili uzoraka iste (ili više različitih) karakteristike. Kada su vektori karakteristika homogeni (npr. više slika otiska prsta), rezultatni vektor može biti izračunat kao prosek korisnikovih pojedinačnih vektora karakteristika. Kad vektori nisu homogeni (kad za ulazne podatke koristimo na primer geometriju dlana i sliku lica) mogu se konkatenerati u oblik jedinstvenog vektora karakteristika. Međutim, kad su ulazni podaci nekompatibilni (npr. svojstveni koeficijenti lica i „*minutiae*“ prsta) onda konkatencija nije moguća. Neki od pokušaja kombinovanja otiska šake i geometrije dlana [9] ili crta lica sa geometrijom šake [10], završili su se sa ograničenim uspehom.

Ukratko rečeno ovde se zasebni podaci izdvojeni iz senzora enkoduju u zajednički vektor koji se zatim poredi sa šablonom unetim prilikom prijave korisnika na sistem u bazu podataka. Na izlazu se dobija jedinstven rezultat kao kod unimodalnih biometrijskih sistema [66].

Kako čak ni opširnija literatura ne sadrži značajnija istraživanja o sjedinjavanju na ovom nivou, zaključuje se da je ovaj pristup u daleko manjoj praktičnoj upotrebi nego ostala dva, koja će biti opisana. Iako nam logika nalaže da bi bilo daleko jednostavnije i efikasnije sjedinjavati podatke u što ranijoj fazi, dok još sadrže svoje originalne karakteristike, sjedinjavanje podataka na nivou izdvajanja podataka to ne ispunjava.

Osnovni problemi kod ovog pristupa su sledeći:

- Vektori biometrijskih karakteristika koji se sjedinjuju mogu biti nekompatibilni što se može rešiti pažljivo dizajniranim sistemom ili neki od njih može biti nedostupan (dešava se da korisnik ne može da obezbedi potreban podatak) što je problem koji je poznat još od standardnih sistema:
- Problematično je generisanje rezultata. Čak i kod unimodalnih biometrijskih sistema, teško je dobiti kvalitetan podatak koji bi obezbedio reprezentativan rezultat baziran na poređenju vektora biometrijske karakteristike korisnika i šablona smeštenog u bazi podataka. Kod multimodalnih biometrijskih sistema, cela priča je još složenija i komplikovanija:
- Konkatencijom više vektora može se dobiti rezultujući vektor koji je predimenzioniran [62];
- Nekada ne postoje veze između vektora karakteristika dva biometrijska sistema, a opet, ako se ta veza zna unapred, iz predostrožnosti potrebno je karakteristike sa velikom međusobnom zavisnošću izbaciti iz obzira. To podrazumeva dodatno korišćenje algoritama koji će izvršiti selekciju karakteristika pre klasifikacije.
- Većina proizvođača komercijalnih biometrijskih sistema ne omogućava pristup vektorima karakteristika koje koriste tako da veoma mali broj istraživača radi na ovom nivou sjedinjavanja nego se uglavnom orijentišu na nivoe posle poređenja.



Slika 44a: Nivo izdvajanja podataka

6.4.2 Sjedinjavanje posle poređenja

Šema sjedinjavanja nakon poređenja šablona sastoji se od četiri faze:

- **Dinamički izbor podataka** – šema obezbeđuje izbor podataka (klasifikatora) za koje se pretpostavlja da će dati najtačnije rezultate. Ova faza je poznata i kao „*Pobednik uzima sve*“ (eng. *Winner-Takes-All*) pristup, a uređaj koji obezbeđuje selekciju poznat je pod nazivom „Asocijativni prekidač“ (eng. *Associative Switch*);
- **Sjedinjavanje na nivou odluke (apstraktni nivo)** – dolazi do izražaja kad sistem za proveru svakog unetog podatka ima najbolji mogući rezultat na svom izlazu. Metode kao što su većinski izbor [12], težinski izbor zasnovani na *Dempster-Šeferovoj* teoriji dokaza [13], AND ili OR pravilo [14] i sl. mogu biti iskorišćeni za dobijanje konačne odluke;
- **Sjedinjavanje na nivou rangiranja** – sjedinjavanje na ovom nivou može biti izvršeno kad je izlaz svakog biometrijskog sistema za proveru podskup mogućih

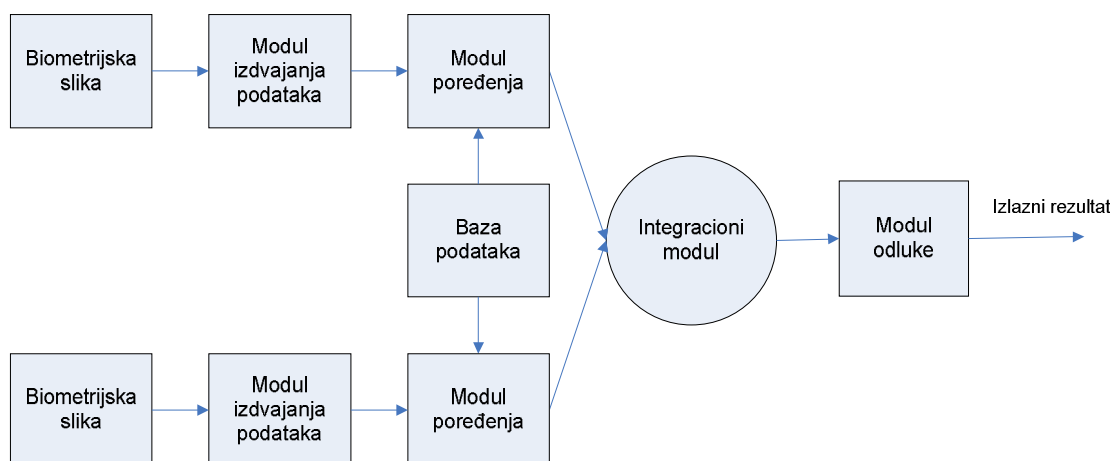
tačnih odgovora sortiranih po opadajućem redosledu prema poverenju koje ima.. T.K.Ho je u [15] opisao tri načina kombinovanja ranga dodeljenih od strane različitih sistema za potvrdu. Po metodi najvišeg ranga, rezultatu svake pozitivne provere dodeljuje se najviši rang izračunat od strane različitih sistema za proveru, a zatim se na osnovu kombinacija privremenih mesta na listi, definiše konačna odluka. *Borda* računaska metoda upotrebljava sumu svih rangova dodeljenih od strane pojedinačnih sistema za proveru kako bi se izračunala kombinacija istih. Metoda logističkog povratka stanja predstavlja generalizaciju prethodno opisane metode gde se najznačajnija suma pojedinačnih rangova izračunava i značaj svake se određuje logističkom regresijom (povratkom stanja);

- **Sjedinjavanje na nivou poređenja** – vrši se kad rezultat sistema za proveru bude skup mogućih pozitivnih provera sa kvalitetom svake potvrde. Ova faza takođe je poznata i kao sjedinjavanje na nivou merenja ili na nivou poverenja.

6.4.2.1 Nivo poređenja šablona

Kod multi-biometrijskog sistema zasnovanog na ovoj arhitekturi, vektori biometrijskih karakteristika kreiraju se nezavisno za svaki senzor i zatim se zasebno porede sa šablonima koji se nalaze u bazi podataka. Na osnovu izvršenog poređenja, generišu se rezultati svakog poređenja da bi se nakon toga, rezultati iskombinovali u zajednički rezultat putem modula odlučivanja.

Sama procedura za svaki podsistem je identičana onoj kod klasičnog biometrijskog sistema što omogućava upotrebu standardnih algoritama kreiranja i poređenja šablona. Tehnike, kao što je logistički povratak stanja (engl. *logistic regression*) se koriste za kombinovanje rezultata sa dva senzora i za pokušaj smanjenja FRR za dati FAR.



Slika 44b: Nivo poređenja šablona

U pogledu verifikacije, postoje dva različita pristupa. U prvom pristupu, sjedinjavanje je viđeno kao klasifikacija problema koja podrazumeva da se vektor rezultata generiše na osnovu izlaza poređenja pojedinačnih biometrijskih podataka i taj rezultat može biti klasifikovan u dve kategorije: „Prihvaćen“ ili „Odbijen“. Kod drugog pristupa se kombinuju izlazi poređenja više biometrijskih karakteristika, a zatim se generiše jedinstveni skalarni rezultat koji se koristi za donošenje konačne odluke. Pristup koji će biti korišćen zavisi od slučaja do slučaja.

Klasifikacioni pristup

Za donošenje konačnog rezultata i odluke, koristi se nekoliko klasifikatora (ulaznih podataka). Y.Wang je u [16] je predvideo 2D rezultujući vektor koji se sastoji od rezultata modula prepoznavanja dužice oka i crta lica. Za klasifikaciju je korišćena *Fišerova diskriminaciona analiza* i neuronska mreža kao klasifikator sa radialnom bazisnom funkcijom. Verlinde i Šole [17] kombinovali su rezultate dva ekspertna sistema za prepoznavanje crta lica i jedan za prepoznavanje glasa upotrebom tri klasifikatora: k-NN klasifikator upotrebom vektorske kvantizacije, klasifikator zasnovan na „stablu odlučivanja“ i klasifikator zasnovan na modelu logističkog povratka stanja. Kacis [18] je koristio fazi logiku za sjedinjavanje rezultata dobijenih iz dva biometrijska sistema. Ros i Džejn [6] su upotrebljavali „stablo odlučivanja“ i diskriminacioni klasifikator za kombinovanje crta lica, geometrije dlana i otiska prsta.

Kombinacioni pristup

Kitler [19] je razvio teorijsku osnovu za sjedinjavanje različitih klasifikatora koristeći šeme pravila zbira, proizvoda, minimalne, maksimalne i srednje vrednosti kao i pravilo većinskog izbora (eng. *sum rule, product rule, min rule, max rule, median rule, majority voting*). Za razvoj ovih šema potrebno je rezultate provere konvertovati u susedne verovatnoće koje odgovaraju kako originalnom tako i lažnom korisniku. Problem se sastoji u klasifikovanju ulaznog uzorka X u jedan od m mogućih razreda (u verifikacionom sistemu $m=2$) zasnovanom na podatku dobijenom od R različitih klasifikatora ili sistema za potvrđivanje. Pretpostavimo da je x_i vektor biometrijske karakteristike (dobijen iz ulaza X) predstavljen i -om sistemu za potvrđivanje. Neka izlaz svakog pojedinačnog sistema za potvrđivanje bude $P(w_j|x_i)$, susedna verovatnoća da razred w_j daje vektor x_i . Pretpostavimo da je $c \in \{w_1, w_2, \dots, w_m\}$ razred kojem pripada ulazni uzorak X . Sledeća pravila se mogu koristiti za dobijanje c :

- **Pravilo proizvoda** – zasniva se na pretpostavci statističke nezavisnosti vektora $x_1, x_2, \dots, x_R$. Pravilo proizvoda dodeljuje ulazni uzorak razredu c na sledeći način:

$$c = \arg \max_j \prod_{i=1}^R P(w_j|x_i) \quad [11]$$

U suštini, različite biometrijske karakteristike korisnika su međusobno nezavisne što omogućava upotrebu pravila proizvoda zasnovanog na pretpostavci nezavisnosti.

- **Pravilo zbira** – efikasnije je od pravila proizvoda kad velika doza šuma, odnosno greške pri očitavanju predstavlja dodatni teret problemu klasifikacije. Pravilo zbira dodeljuje ulazni uzorak razredu c na sledeći način:

$$c = \arg \max_j \sum_{i=1}^R P(w_j|x_i) \quad [12]$$

- **Pravilo maksimuma** – približava srednje vrednosti susednih verovatnoća maksimalnoj vrednosti. Pravilo maksimuma dodeljuje ulazni uzorak razredu c na sledeći način:

$$c = \arg \max_j \max_i P(w_j|x_i) \quad [13]$$

- **Pravilo minimuma** – dobija se ograničavanjem proizvoda vrednosti susednih verovatnoća.

$$c = \arg \max_j \min_i P(w_j|x_i) \quad [14]$$

Prabkar i Džejn [20] su dokazali da pretpostavka o statističkoj nezavisnosti skupova biometrijskih osobina ne mora biti uvek tačna kod multi-bimetrijskih sistema koji koriste

različite slike i različite algoritme za poređenje istog biometrijskog podatka. Šema im je bila zasnovana na ne-parametarskom kombinovanju rezultata dobijenih od četiri algoritma za proveru otisaka prsta i koristeći test određivanja odnosa mogućnosti kako bi se donela konačna odluka.

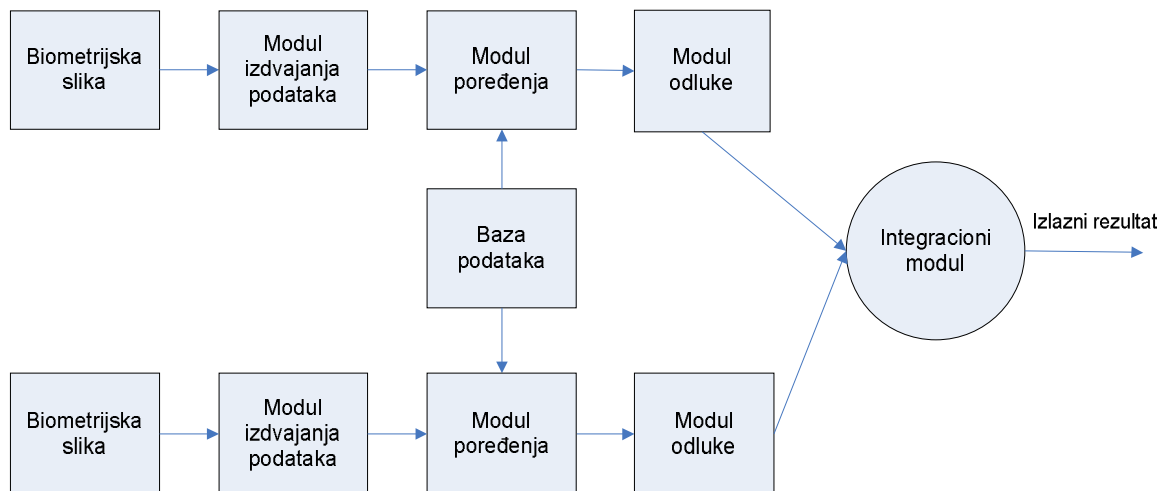
Kombinovan rezultat može biti dobijen kao težinski zbir (zbir značaja) rezultata poređenja pojedinačnih sistema poređenja [16,33]. Džejn i Ros [21] predložili su upotrebu nivoa značaja dodeljenog od strane korisnika svakom od ulaznih podataka. Razlog za teko nešto je što neke karakteristike, iz određenih razloga, ne poseduju svi korisnici pa bi se dodeljivanjem većeg prioriteta drugim karakteristikama smanjio nivo greške koji može prouzrokovati taj nedostatak. Na primer, od korisnika sa veoma suvim prstima, ne može se dobiti kvalitetan uzorak otiska pa se ovom podatku dodeljuje nizak nivo važnosti dok se viši nivo dodeljuje drugim traženim podacima od strane multi-biometrijskog sistema.

6.4.2.2 Nivo odlučivanja

Kod ovog oblika sjedinjavanja, posebna autentifikaciona odluka se donosi za svaki unet podatak, a zatim se te dve odluke kombinuju i generišu konačnu odluku.

Sjedinjavanje na nivou odlučivanja predstavlja slobodniji oblik arhitekture gde se svaki podsistem celim svojim tokom ponaša kao zaseban sistem klasične biometrijske autentifikacije te je veoma popularan. Metod je takođe, podržan BioAPI standardom [66].

Kako se sjedinjavanje vrši tek u poslednjoj fazi, teško je proceniti da li dolazi po poboljšanja performansi kao kod, npr. sjedinjavanja na nivou poređenja šablona, osim možda pod nekim specifičnim uslovima pod kojima se poboljšanje performansi može garantovati [1].



Slika 44c: Nivo odluke

6.5 Evaluacija multimodalnog sistema

Performanse biometrijskog sistema kao što su tačnost, propusna moć i skalabilnost mogu se prihvatiti sa velikim stepenom poverenja samo kad je sistem testiran na velikom broju reprezentativnih uzoraka. Na primer, otisci prstiju [3] i crte lica[4] testirani su nad bazom sa više od 25000 korisnika različitih grupa populacije pod različitim uslovima okoline. Za razliku od toga, neki noviji multimodalni biometrijski sistemi se testiraju na uzorcima od samo 1000 korisnika. Isto tako, baze podataka mogu biti fizičke i virtualne. Kod fizičkih,

biometrijski podaci su sakupljeni od iste osobe dok se kod virtualnih multimodalnih baza zapisi dobijaju povezivanjem podataka iz više drugih baza unimodalnih biometrijskih sistema. Samo kreiranje takvih virtualnih korisnika zasnovano je na pretpostavci da su biometrijski podaci različitih karakteristika iste osobe međusobno nezavisni iako ta pretpostavka do danas nikad nije u potpunosti istražena.

6.6 Prednosti i mane multimodalnih biometrijskih sistema

Multimodalni biometrijski sistemi rešavaju neke od problema koji se javljaju kod unimodalnih sistema (ne-univerzalnost, obmanjivanje sistema i sl.). Multimodalni biometrijski sistem može integrisati podatke na različitim nivoima od kojih je najpopularniji oblik sjedinjavanja na nivou poređenja.

Odluka o upotrebi multi-biometrijskog sistema zavisi od sledećih, mogućih prednosti:

- Manji FRR;
- Manji FAR;
- Manji broj ljudi koji ne može da se prijavi na sistem;
- Prilično pogodna upotreba;
- Manja šansa za prevaru.

Ali, sa druge strane, ni jedan sistem nije bez mana od kojih, takođe, zavisi svrsishodnost uvođenja ovakvog sistema. Osnovni nedostaci sistema su:

- Veća cena senzora, licenci i implementacije;
- Potrebno veće osnovno znanje o performansama biometrijskih sistema;
- Složenost sistema;
- Komplikovaniji razvoj.

Sam šablon koji se kod multibiometrijskih sistema smešta u bazu podataka, daleko je obuhvatniji nego kod unimodalnih sistema pa je samim tim još atraktivnija meta potencijalnih napadača. Prodavci tvrde da se na osnovu šablona ne može regenerisati originalan podatak, međutim, to je nemoguće proveriti s obzirom da algoritmi nisu dostupni javnosti.

Kod tradicionalnih sistema zasnovanih na lozinkama, u slučaju kompromitacije lozinke, jednostavno može biti zamenjena. Kod unimodalnih biometrijskih sistema to nije tako jednostavno, kod kompromitovanog otiska prsta mogli bi eventualno iskoristiti drugi prst kao novi podatak za prijavu na sistem ali je količina i mogućnost zamene ograničena. Kod multimodalnih biometrijskih sistema je sve još daleko teže.

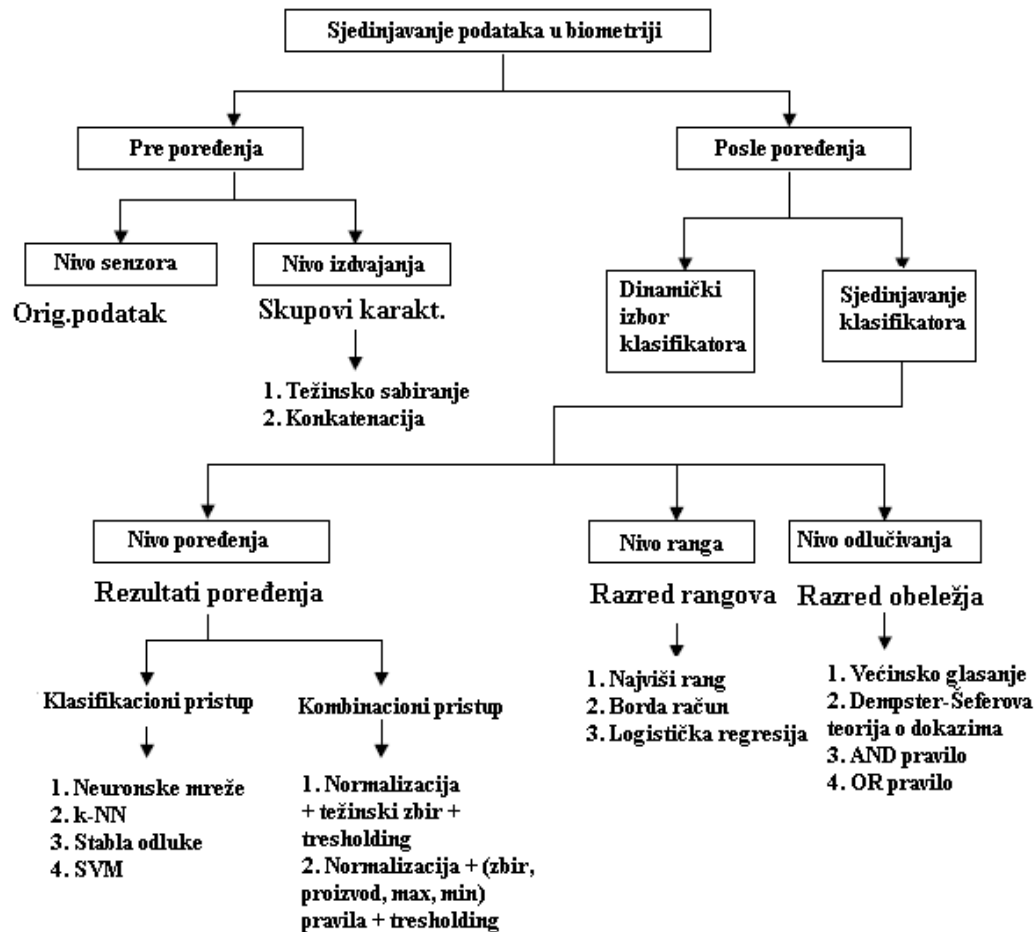
Problem je takođe, iz ugla korisnika, i kod upotrebe. Prikupljanje podataka potrebnih za autentifikaciju može da se obavlja jedan po jedan ili istovremeno. Oba pristupa imaju svoje mane. U prvom slučaju, drastično se produžava vreme za prijavu čime se smanjuje produktivnost dok, s druge strane, poznato je da je za uspešnu autentifikaciju potreban kvalitetan uzorak, pa treba zamisliti situaciju gde korisnik istovremeno namešta glavu pred skenerom lica ili oka i postavlja prst na senzor za uzimanje otiska.

Naravno, ovo su samo neki primeri i ne odnose se na sve multi-biometrijske sisteme, a i treba uvek imati na umu i prednosti koje nam donose takvi sistemi.

Ono što je takođe bitno, ceo sistem zahteva, pored viših novčanih ulaganja, i dodatno vreme kao i komplikovaniju obradu podataka tako da je, pre dizajniranja sistema, potrebno detaljno sagledati sve ove aspekte.

6.7 Zaključak

U prethodnom delu teze sagledani su svi važniji aspekti i pristupi kod sjedinjavanja više biometrijskih podataka u multimodalnim biometrijskim sistemima autentifikacije. Na slici 45, prikazan je kompletan prikaz upotrebljenih tehnika za sjedinjavanje podataka.



Slika 45: Grupni prikaz tehnika sjedinjavanja kod multimodalnog biometrijskog sistema

Većina dizajnera praktikuje sistem koji obezbeđuje sjedinjavanje podataka na nivou poređenja šablona kao i kombinacioni pristup na ovom nivou. Pa ipak, i dalje postoji mnoštvo nerešenih pitanja, i dalje ne postoje standardne procedure za konverziju u verovatnoću kao ni za postupak normalizacije rezultata dobijenih iz više algoritama za poređenje. Sistematska evaluacija različitih tehnika normalizacije nije moguća. Isto tako, većina tehnika na nivou poređenja ne može biti kvalitetno odrađena ako pojedinačni sistemi nemaju dobra svojstva prepoznavanja. Ne mogu da koriste tzv. *soft* biometrijske identifikatore, koji su manje verodostojni, bez obzira na veći broj podataka o nekoj osobi ako time ona nije dovoljno precizno autentifikovana. Na primer, mogu se uzeti *soft* identifikatori kao što su visina ili boja kose koji nam mogu dati neke smernice u pretrazi ali ne i konačan rezultat ko je u pitanju. Trenutno ne postoji mehanizam koji uspešno koristi samo podatke tog tipa u procesu autentifikacije.

7. Normalizacija rezultata

U ovom slučaju, posmatraćemo biometrijski verifikacioni sistem koji obezbeđuje sjedinjavanje podataka na nivou poređenja rezultata. Teorijsku osnovu ovog sistema razvio je Kitler [19] koja može biti implementirana samo ako je svaki izlaz u obliku $P(original|X)$ tj. susedna verovatnoća ulaznog biometrijskog uzorka originalnog korisnika. U praksi, većina multimodalnih biometrijskih sistema daje rezultat s koji je po Verlinde-u [22] u vezi sa $P(original|X)$ na sledeći način:

$$s=f(P(original|X) + \eta(X)) \quad [15]$$

gde je f jednolična funkcija, a η greška sistema koja zavisi od ulaza X i koja se javlja usled npr. smetnji pri unosu, odnosno loše uzete biometrijske karakteristike ili usled grešaka nastalih pri obradi ulaznog podatka.

Ako pretpostavimo da $\eta = 0$ normalno je aproksimirati $P(original|X)$ sa $P(original|s)$ što redukuje proračunavanje i zahteva procenu uslovne gustine $P(s|original)$ i $P(s|lažni)$). Snelik [23] je za pretpostavku uzeo normalnu distribuciju rezultata poređenja $P(s|original) \sim N(\mu_q, \sigma_q)$ i $P(s|lažni) \sim N(\mu_i, \sigma_i)$ gde μ_q , σ_q , μ_i i σ_i predstavljaju parametre. Susedna verovatnoća rezultata dobijenog od originalnog korisnika se izračunava na sledeći način:

$$P(original|s) = \frac{P(s|original)}{P(s|original) + P(s|lažni)} \quad [16]$$

Ovakav pristup ima određene nedostatke. Dva osnovna su sledeća. Pretpostavka normalne distribucije rezultata često ne mora biti tačna. Na primer, u određenim testovima koji su vršeni sa otiscima prstiju i geometrijom dlana, rezultati nisu prihvatili normalizaciju. Zatim, ovaj pristup ne koristi podatke o prethodnoj verovatnoći, originalnog i lažnog korisnika, koji mogu biti dostupni u sistemu. Iz tih razloga se za procenu uslovne gustine rezultata originalnog i lažnog korisnika koristi tzv. Parzenov metod procene gustine prozora [11] da bi se nakon toga primenila Bajeva formula za izračunavanje susednih verovatnoća rezultata originalnog korisnika:

$$P(original|s) = \frac{P(s|original) * P(g)}{P(s)} \quad [17]$$

gde je

$$P(s) = P(s|original) * P(g) + P(s|lažni) * P(i) \quad [18]$$

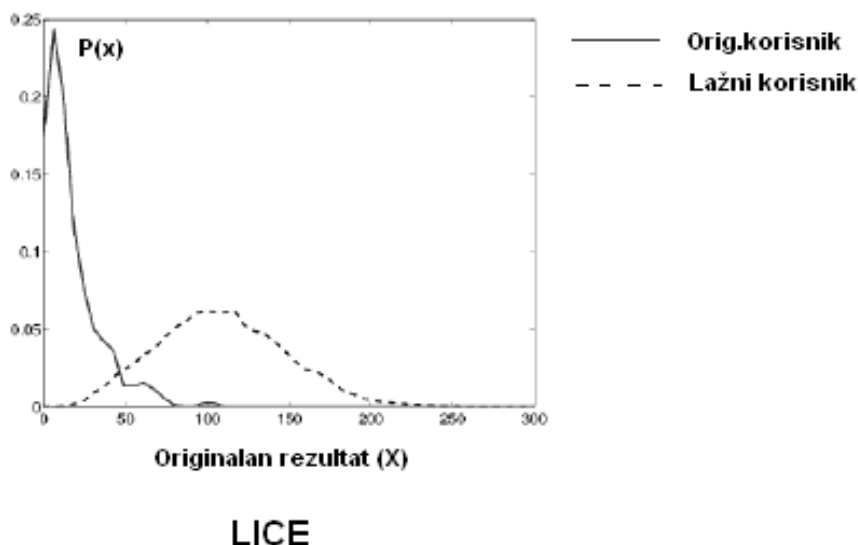
Ovde $P(g)$ i $P(i)$ predstavljaju prethodne verovatnoće originalnog i lažnog korisnika, respektivno. Iako ova Parzenova metoda značajno redukuje količinu grešaka u proceni $P(original|s)$, ona ipak nije 100% tačna zbog ograničenog izbora optimalne širine prozora u procesu procene gustine.

Isto tako, procena da je $\eta = 0$ (zavisi od X) nije realna u većini praktičnih rešenja. U nedostatku pouzdanijih, izračunata vrednost $P(original|s)$ nije najbolja procena $P(original|X)$ što može dovesti do loših performansi prepoznavanja ulaznog podatka.

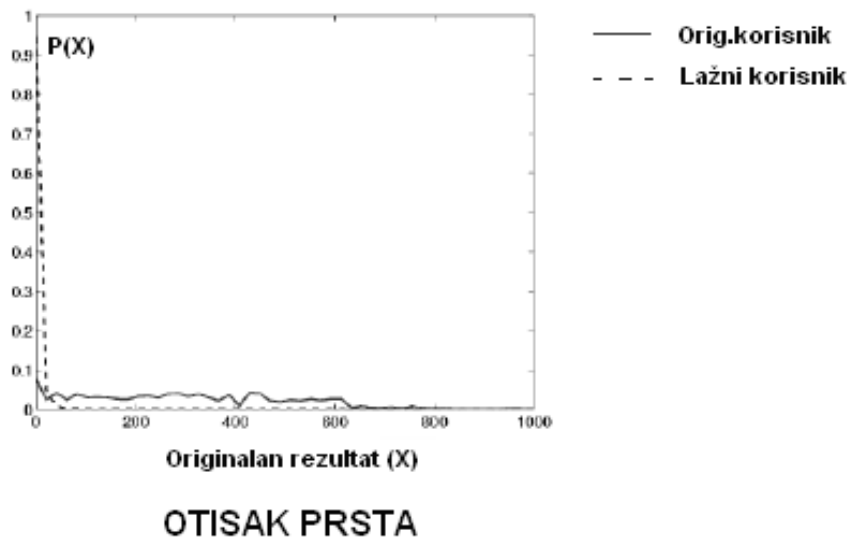
7.1 Potreba za normalizacijom rezultata

Normalizaciju podataka treba razmotriti pre sjedinjavanja podataka u jedinstven rezultat. Rezultati dobijeni iz zasebnih modula za poređenje mogu biti ne-homogeni u smislu da su slični ili različiti, na skali se nalaze u različitim opsezima, npr. [0,100] i [0,1000], a isti ti rezultati mogu biti praćeni različitim statističkim distribucijama. Iz tih razloga se praktikuje upotreba normalizacije, kako bi se rezultati doveli na nivo na kojem se mogu sjediniti, a sama procedura predstavlja jedan od najkritičnijih delova dizajniranja sistema za sjedinjavanje podataka na nivou poređenja rezultata. Kako bi se donekle olakšala normalizacija, potrebno je izmeniti vrednosti parametara lokacije i skale distribucije svakog od dobijenih zasebnih rezultata kao i vršiti transformaciju nad podacima koji se nalaze u oblasti preklapanja distribucije originalnog i lažnog korisnika.

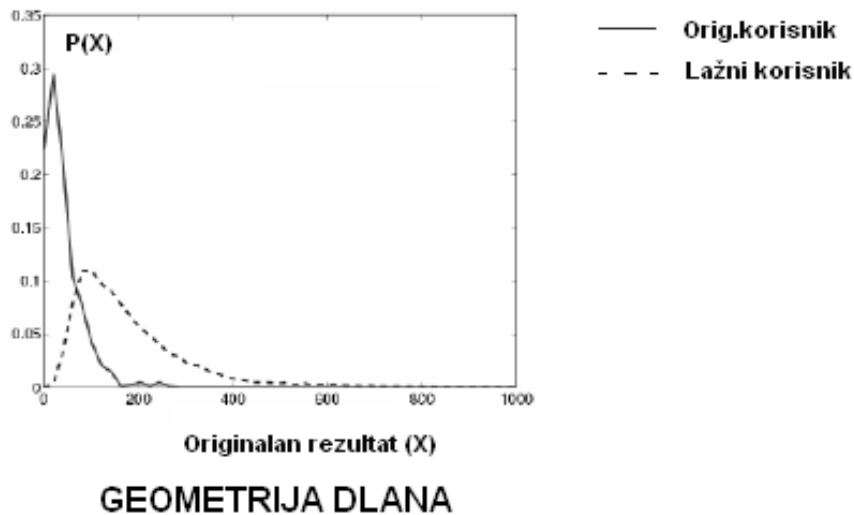
Na slici 46a, 46b i 46c prikazane su distribucija rezultata poređenja tri karakteristike: crte lica, otiska prsta i geometrije dlana, respektivno [59]. Rezultati dobijeni poređenjem dlana i lica su rezultati različitosti, dok su oni dobijeni poređenjem otiska prsta, rezultati sličnosti što znači da jedan podatak ne odgovara ostalima te je potrebno izvršiti normalizaciju pre sjedinjavanja.



Slika 46a: Distribucija rezultata poređenja crte lica



Slika 46b: Distribucija rezultata poređenja otiska prsta



Slika 46c: Distribucija rezultata poređenja geometrije dlana

Sa slike 46a, vidi se da postoji značajno preklapanje između originalne i lažne distribucije ulaznog rezultata crta lica što objašnjava slabe performanse modula za prepoznavanje lica . Slika 46b. pokazuje da je većina rezultata lažnih otisaka prstiju blizu nule, a da se rezultati originalnih korisnika šire kroz širokog raspon vrednosti. Osim toga, preklapanje između dve uslovne gustine je mali i zato su performanse sistema za prepoznavanje otisaka prstiju bolje nego kod onih za prepoznavanje crta lica i geometrije dlana. Preklapanje između distribucija originalnih i lažnih korisnika kod sistema za prepoznavanje geometrije dlana je najveći uzimajući u obzir sve tri ulazne karakteristike kao što je prikazano na slici 46c. Iz tog razloga sistemi za prepoznavanje geometrije dlana su u dalekom zaostatku po pitanju efikasnosti u odnosu na druga dva pomenuta sistema.

7.2 Izazovi normalizacije

Kao što je ranije rečeno, normalizacija ima za cilj izmenu parametara lokacije i skale (eng. *location and scale parameters*) distribucija rezultata poređenja na izlazu zasebnih modula za poređenje kako bi se rezultati dobijeni iz tih modula doveli na isti nivo.

Parametri lokacije pomeraju distribuciju, dok je parametri skale šire. Kad su parametri uzeti iz fiksnog skupa, u pitanju je tzv. *normalizacija fiksnog rezultata* [24]. U takvom slučaju, skup se pretražuje kako bi se izabrao model koji će odgovarati datoj distribuciji i na osnovu kojeg će se odrediti parametri.

Kod tzv. *adaptivne normalizacije rezultata* normalizacioni parametri su zasnovani na trenutnom vektoru karakteristike (ulazni podatak). Ovaj pristup ima mogućnost prilagođavanja varijacija ulaznih podataka kao što su promene dužine izlaznog signala kod sistema za prepoznavanje zvuka.

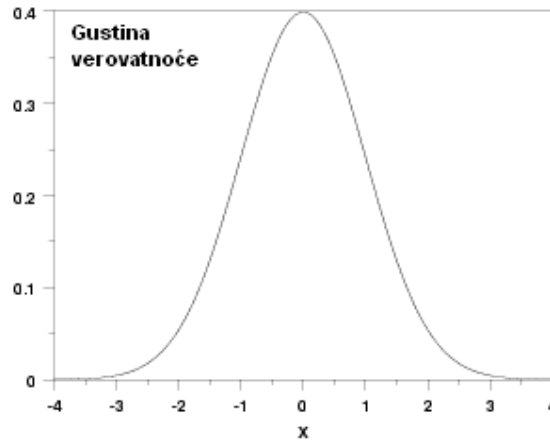
Problemi normalizacije kod multimodalnih biometrijskih sistema su identični onima koji se javljaju kod *meta pretraživanja*⁹. Jedne od najpopularnijih tehnika normalizacije kod *meta pretraživanja* su *Min-max* normalizacija kao i *Z-rezultat* (eng. *Z-score*) normalizacija. Ovde je distribucija relevantnih rezultata aproksimirana *Gausovom* distribucijom sa velikom standardnom devijacijom dok su ne-relevantni rezultati distribuirani eksponencijalnom distribucijom. Rezultati dobijeni u istraživanju, čiji podaci su korišćeni u ovoj tezi, pokazali su da distribucija rezultata poređenja otisaka prstiju originalnog i lažnog korisnika u velikoj meri odgovara onoj kod *meta pretraživanja* što se ne može reći za preostala dva ulazna podatka.

Za dobru normalizacionu šemu, procena vrednosti i položaja parametara mora biti robustna tj. neosetljiva na prisustvo netipičnih rezultata i efikasna u smislu približavanja dobijenih procena optimalnim vrednostima kad je poznata distribucija. Pojmove robustnosti i efikasnosti kod statističkih procedura opisao je P.J.Huber u [25]. Bez obzira što se normalizacija može izvršiti na više načina, cilja je odabrati metod koji istovremeno ispunjava zahteve po pitanju robustnosti i efikasnosti.

⁹ Metoda kombinovanja relevantnih rezultata pretraživanja dokumenata od strane više različitih pretraživačkih servisa u cilju povećanja performansi pretraživanja [46].

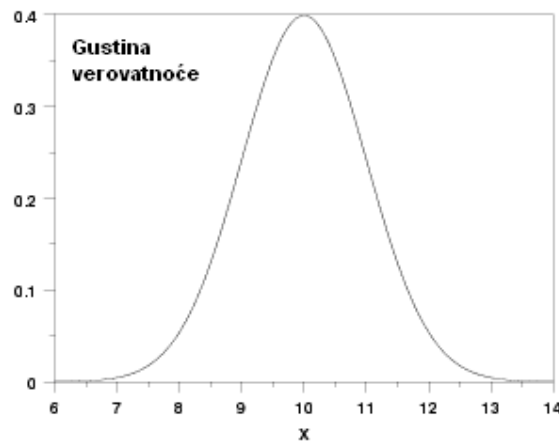
7.2.1 Parametri lokacije i skale

Distribucija verovatnoće okarakterisana je parametrima lokacije i skale. Na sledećem primeru data je funkcija gustine verovatnoće kod standardne normalne distribucije gde je parametar lokacije postavljen na 0, a parametar skale na 1 (slika 47).



Slika 47: Parametri lokacije i skale: lokacija = 0, skala = 1

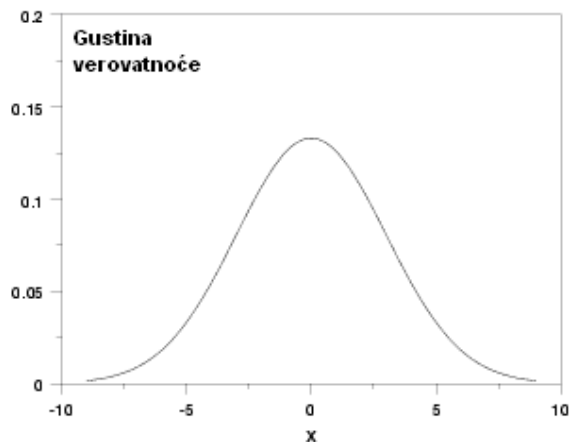
Sledeći primer (slika 48) nam prikazuje distribuciju sa parametrom lokacije 10 i parametrom skale 1.



Slika 48: Parametri lokacije i skale: lokacija = 10, skala = 1

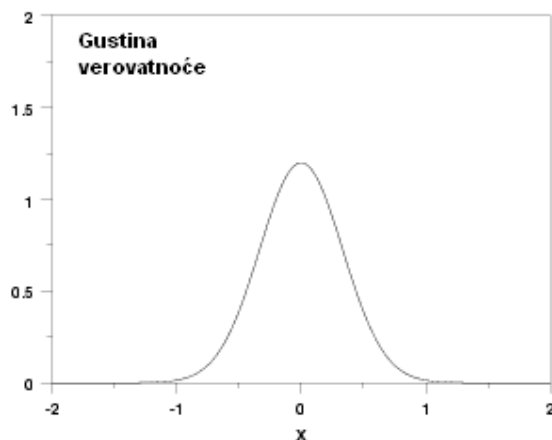
Uloga parametra lokacije je da pomera grafik po X osi u jednom ili drugom smeru. Za vrednost parametra 10, grafik će se pomeriti 10 tačaka na desnu stranu, a za vrednost parametra -10, pomeraj će biti 10 tačaka na levu stranu na X osi.

Na sledećem grafiku, (slika 49), parametar skale je 3 (parametar lokacije je 0) i ima ulogu širenja grafika. Maksimalna dostignuta vrednost na Y osi je oko 0.13, za razliku od 0.4 na prethodnom grafiku (gde je parametar skale bio 1).



Slika 49: Parametri lokacije i skale: lokacija = 0, skala = 3

Na slici 50 prikazan je isti grafik, sa izmenjenom vrednošću parametra skale za koji je u ovom slučaju uzeta vrednost 0.333 čime je maksimalno dostignuta vrednost funkcije 3 puta veća nego u prvobitnom slučaju, odnosno, maksimalna vrednost funkcije je 1.2 za razliku od početnih 0.4.



Slika 50: Parametri lokacije i skale: lokacija = 0, skala = 0.333

Iz ovog se može zaključiti da što je veća vrednost parametra, srazmerno je veće i širenje funkcije.

Standardne vrednosti svake distribucije su 0 za parametar lokacije i 1 za parametar skale. Takođe, važno je reći da parametar lokacije i parametar skale, kod normalne distribucije, odgovaraju srednjoj i standardnoj devijaciji¹⁰, respektivno [74].

¹⁰ Standardna devijacija-apsolutna mera disperzije u osnovnom skupu. Govori o tome koliko, u proseku, elementi skupa odstupaju od aritmetičke sredine skupa.

7.3 Tehnike normalizacije

Najjednostavnija normalizaciona tehnika je **Min-max** normalizacija koja je najbolje prilagođena za slučaj gde su granice (maksimalne i minimalne vrednosti) rezultata dobijenih od strane modula za poređenje poznate. U ovom slučaju, se na jednostavan način mogu menjati minimum i maksimalni rezultata prema 0 i 1, respektivno. Odnosno, neobrađeni podaci se mapiraju u opseg [0 , 1]. Međutim, čak i ako odgovarajući rezultati nisu ograničeni, mogu se proceniti minimalne i maksimalne vrednosti za skup odgovarajućih rezultata i tada primeniti *Min-max* normalizaciju. Pustimo da s_{ij} predstavlja j-ti izlazni rezultat i-tog ulaza, gdje $i=1,2..R$ i $j=1,2..M$. R predstavlja broj ulaza, a M broj raspoloživih rezultata. Rezultat normalizacije za probni rezultat s_{ik} je dat

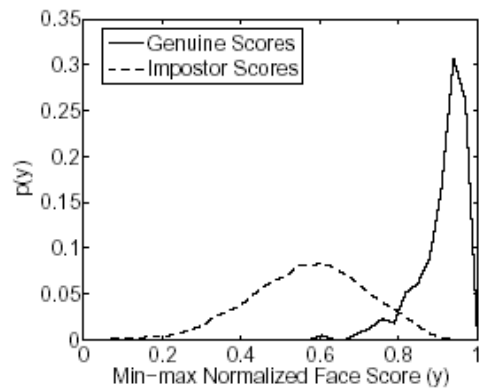
$$s'_{ik} = \frac{S_{ik} - \min(\{s_i\})}{\max(\{s_i\}) - \min(\{s_i\})} \quad [19]$$

Kada su minimalne i maksimalne vrednosti procenjene iz datog skupa odgovarajućih rezultata, ova metoda nije snažna (npr. metoda je visoko osetljiva na netipične vrednosti u podacima koje je upotrebila za procenjivanje). *Min-max* normalizacija zadrži izvornu distribuciju rezultata osim preračunavanja faktora i transformisanja svih rezultata u običan opseg [0,1]. Postignute udaljenost mogu se pretvarati u sličnost oduzimanjem od rezultata normalizacije od 1. Slika 51. prikazuje distribucije lica, otiska prsta i geometrije dlana postignute nakon *Min-max* normalizacije.

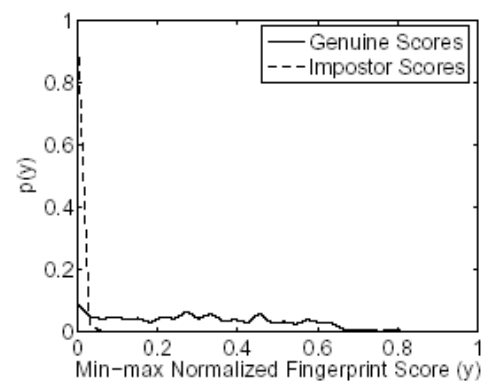
Kada se rezultati različitih modula poređenja razlikuju za određeni logaritamski faktor javlja se tzv. **decimalno skaliranje**. Na primer, ako jedan modul postigne rezultat u rasponu [0,1], a drugi [0,100], sledeća normalizacija će se moći primeniti.

$$s'_{ik} = \frac{s_{ik}}{10^n} \quad [20]$$

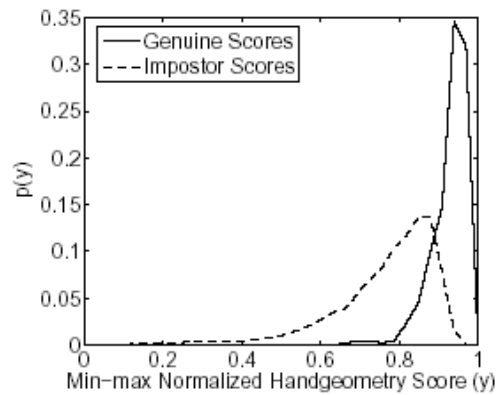
gdje je $n = \log_{10} \max(\{s_i\})$.



(a)



(b)



(c)

Slika 51: Distribucije originalnog i lažnog korisnika postignute nakon min-max normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana

[21]

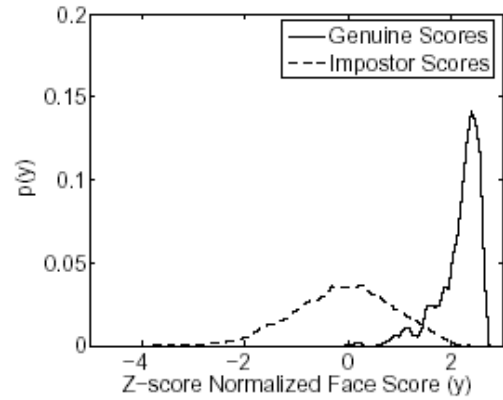
Problemi s ovim pristupom su manjak izdržljivost i pretpostavka da rezultati tih modula variraju zavisno od logaritamskog faktora. U primenjenim eksperimentima, rezultati sva tri poređenja nisu razdeljeni na logaritamskoj skali i zato ova normalizaciona tehnika ne može biti primenjena.

Najčešće korišćen metod normalizacije rezultata je **Z-rezultat** koji koristi aritmetičku sredinu i standardnu devijaciju datih podataka. Ova šema transformiše rezultate u distribuciju sa $\mu = 0$ i $\sigma = 1$ i može dati dobar rezultat ako je raspoloživo predznanje o prosečnom rezultatu i rezultatu varijacije od modula poređenja. Ako ne postoji bilo koje predznanje o prirodi odgovarajućeg algoritma, potrebno je proceniti srednju i standardnu devijaciju rezultata dobijenih iz skupa rezultata modula poređenja. Rezultati normalizacije dati su sa:

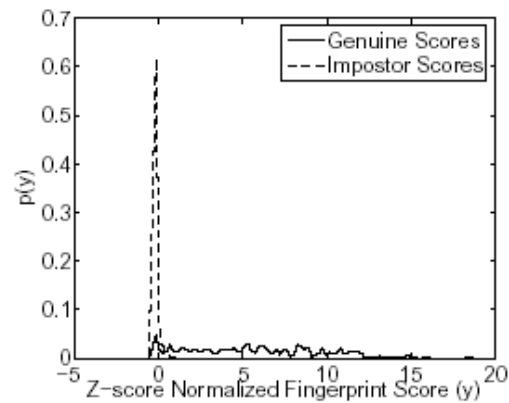
$$s'_{ik} = \frac{s_{ik} - \mu}{\sigma} \quad [22]$$

Gde μ predstavlja aritmetičku sredinu, a σ standardnu devijaciju datih podataka. S obzirom da su i srednja i standardna devijacija osetljive na netipične vrednosti, ovaj metod se ne može uzeti za robustan. *Z-rezultat* normalizacije ne garantuje prost numerički opseg normalizovanih rezultata različitih modula poređenja. *Z-rezultat* normalizacija na svom izlazu neće sadržati ulaznu distribuciju ako distribucija rezultata nije Gausova obzirom da srednja i standardna devijacija predstavljaju optimalne parametre samo kod Gausove distribucije.

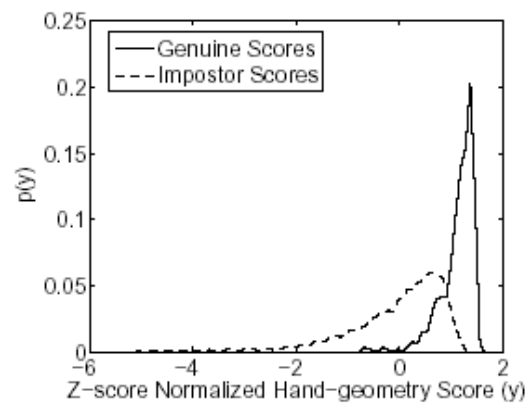
Distribucija rezultata poređenja tri ulazne karakteristike nakon primene ovog tipa normalizacije prikazana je na slici 52. Rezultati dobijeni skeniranjem lica i geometrije dlana, konvertovani su u slične rezultate oduzimanjem od velikih vrednosti (u eksperimentu je to 300 za lice i 1000 za dlan) pre primene normalizacije. Na slici 3.3 vidi se kako je *Z-rezultat* normalizacija odbila da transformiše rezultate drukčijih ulaznih karakteristika u prost numerički opseg, a takođe i ne zadržava originalnu distribuciju rezultata za slučaj otiska prsta.



(a)



(b)



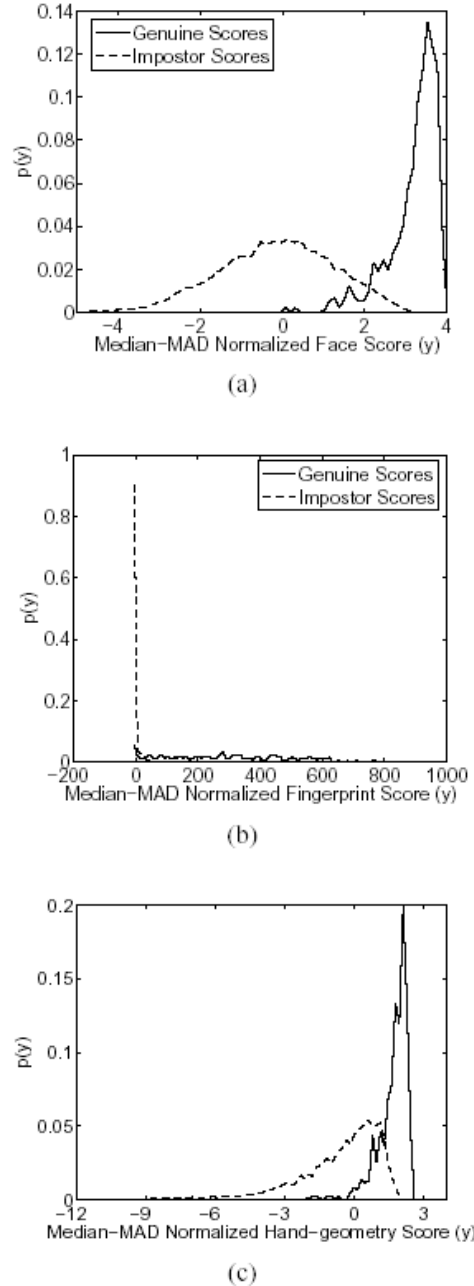
(c)

Slika 52: Distribucije originalnog i lažnog korisnika postignute nakon Z-rezultat normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana

Medijana i srednja apsolutna devijacija (eng. *Median absolute deviation, MAD*) je neosetljiva na netipične vrednosti i tačke u ekstremnim oblastima distribucije i za normalizaciju koja koristi MAD može se reći da je robustna. Takva normalizacija prikazana je sa:

$$s'_{ik} = \frac{s_{ik} - \text{median}}{MAD} \quad [23]$$

gde je $MAD = \text{median} (\{ S_i - \text{median} (\{ S_i \}) \})$. Ipak, procenitelji srednje i MAD nisu produktivno upoređeni sa proceniteljima srednje i standardne devijacije tj. kad distribucija rezultata nije Gausova, *Medijana i MAD* loše procenjuju lokacione i parametre skaliranja. iz tog razloga, ova tehnika normalizacije ne čuva podatke o ulaznoj distribuciji i ne transformiše rezultate u prost numerički opseg. Slučaj je prikazan na slici 53. kroz distribuciju normalizovanih rezultata uzoraka crta lica, otisaka prsta i geometrije dlana.

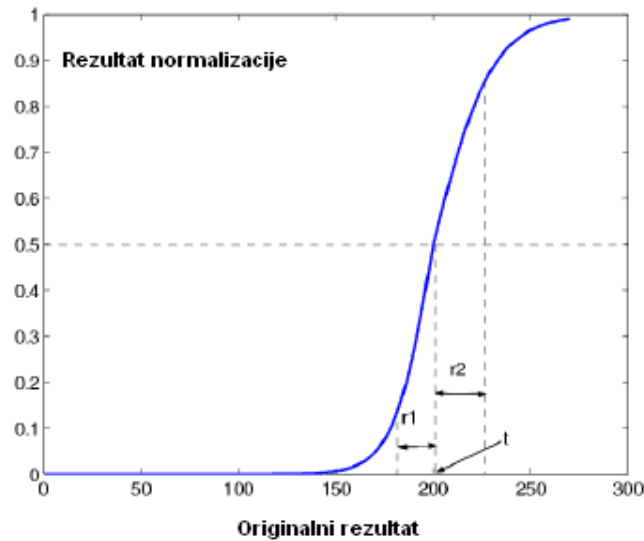


Slika 53: Distribucije originalnog i lažnog korisnika postignute nakon medijana-MAD normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana

U [26], R. Kapeli koristio je tzv. *dvostruku sigmoidnu*¹¹ funkciju kod kombinovanja različitih rezultata otisaka prstiju. Rezultat normalizacije predstavljen je kroz:

$$s'_{ik} = \begin{cases} \frac{1}{1 + \exp(-2(\frac{s_{ik} - t}{r_1}))} & \text{ako } s_k < t \\ \frac{1}{1 + \exp(-2(\frac{s_{ik} - t}{r_2}))} & \text{u drugom slucaju} \end{cases} \quad [24]$$

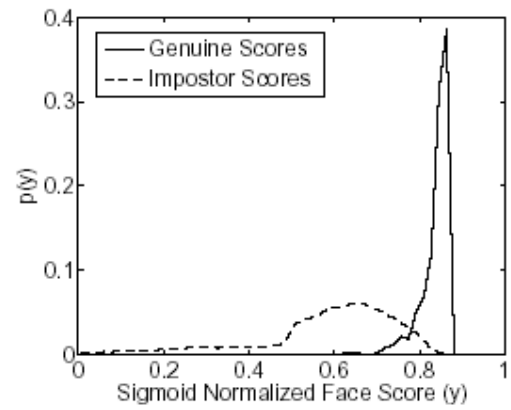
gde je t referentna operativna tačka, a r_1 i r_2 granične vrednosti unutar kojih je funkcija linearna. Sama *sigmoidna funkcija* prikazuje linearne karakteristike u intervalu $(t-r_1, t-r_2)$. Na slici 54. prikazan je primer dvostruke sigmoidne linearne funkcije gde su rezultati iz opsega $[0,300]$ mapirani, uz $t=200$, $r_1=20$ i $r_2=30$, u opseg $[0,1]$ što, ipak, zahteva fino podešavanje parametara kako bi se dobili što bolji rezultati.



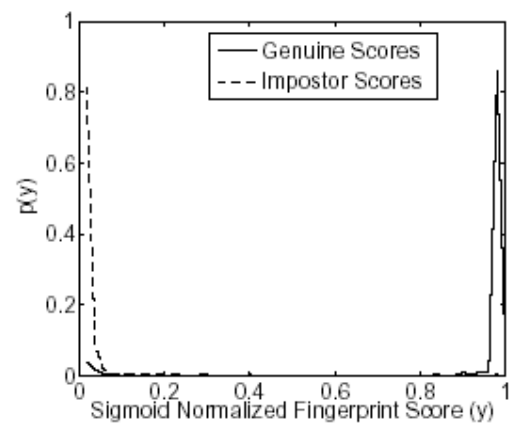
Slika 54: Dvostruka Sigmoidna normalizacija

Vrednost za t je uzeta iz oblasti preklapanja distribucije rezultata originalnog i lažnog korisnika, dok parametri r_1 i r_2 odgovaraju granicama preklapanja te dve distribucije. Ova normalizaciona tehnika obezbeđuje linearnu transformaciju rezultata unutar oblasti preklapanja, dok se vrednosti van ove oblasti, transformišu nelinearno. Na slici 55. prikazani su rezultati ove tehnike nad tri biometrijske karakteristike.

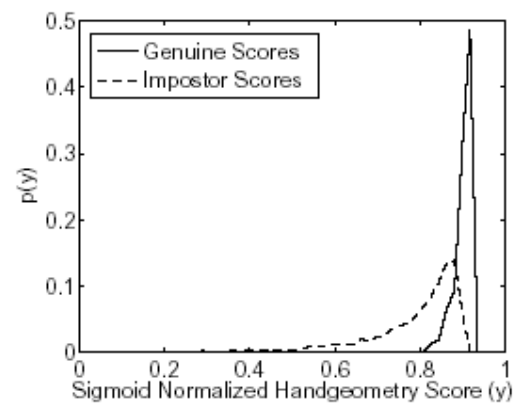
¹¹ Sigmoidna funkcija – definiše se kao striktno rastuća funkcija koja ima osobine glatkosti i asimptote. Predstavlja oblik tzv. aktivacione funkcije.



(a)



(b)



(c)

Slika 55: Distribucije originalnog i lažnog korisnika postignute nakon dvostruke sigmoidne normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana

Rezultati crta lica i geometrije dlana konvertovani su u slične rezultate oduzimanjem normalizacionih rezultata od 1. Upotrebljeni parametri su izabrani tako što je t uzeto kao centar oblasti koja predstavlja preklapanje distribucija originalnog i lažnog korisnika dok r_1 i r_2 predstavljaju minimalnu vrednost originalnog korisnika i maksimalnu vrednost lažnog korisnika, respektivno. Rezultat poređenja za koji se podjednako mogu uzeti podaci od oba korisnika, uzimaju se iz sredine oblasti preklapanja (t). U tom slučaju, r_1 predstavlja razliku između t i minimalne vrednosti originalnog, a r_2 razliku između maksimalne vrednosti lažnog korisnika i vrednosti t . Kako bi sistem mogao da se prihvati kao robustan, oko 2% rezultata sa ekstremnih, krajnjih granica se zanemaruje pri proračunu r_1 i r_2 .

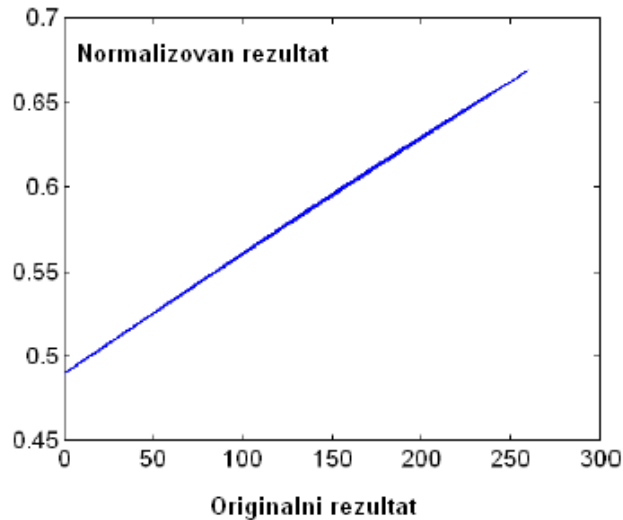
Treba napomenuti da se ova metoda ne koristi ako postoje višestruka preklapanja distribucija oba korisnika. Iako ova šema transformiše sve rezultate u prost numerički opseg $[0,1]$, ne čuvaju se podaci o originalnom obliku distribucije rezultata otiska prsta.

Tanh-estimators normalizaciona tehnika pripada robustnim i veoma efikasnim tehnikama. data je sledećim izrazom:

$$s'_{ik} = \frac{1}{2} \left\{ \tanh(0.01(\frac{s_{ik} - \mu_{GH}}{\sigma_{GH}})) + 1 \right\} \quad [25]$$

gde μ_{GH} i σ_{GH} predstavljaju procene srednje i standardne devijacije, respektivno, Distribucije rezultata originalnog korisnika dobijene su Hampelovim sistemom za procenu (eng. *estimator*)¹² koji je zasnovan na sledećoj Ψ funkciji uticaja (eng. *influence function*):

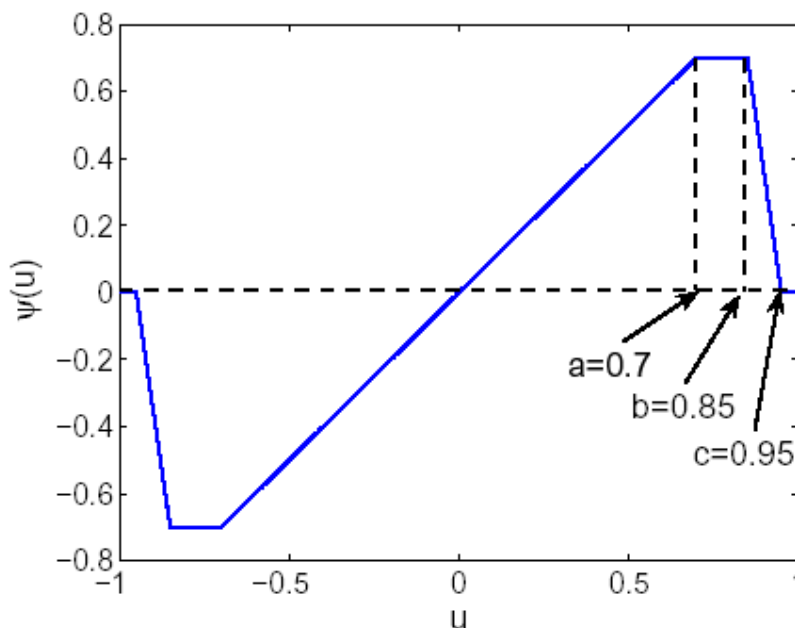
$$\psi(u) = \begin{cases} u & 0 \leq |u| < a \\ a \cdot \text{sign}(u) & a \leq |u| < b \\ a \cdot \text{sign}(u) \cdot \left(\frac{c - |u|}{c - b} \right) & b \leq |u| < c \\ 0 & |u| \geq c \end{cases} \quad [26]$$



Slika 56: Tanh-estimators normalizacija

¹² U eksperimentu su korišćeni podaci o srednjoj i standardnoj devijaciji za oba korisnika ali je u ovom prikazu uzet u obzir samo originalni korisnik iz razloga dobijanja kvalitetnijih rezultata poređenja.

Prikaz Hampelove funkcije dat je na slici 57.



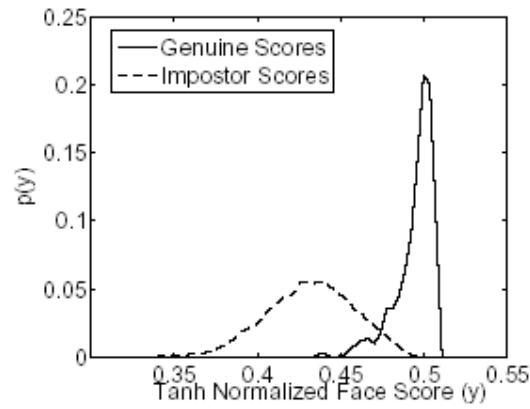
Slika 57: Hampelova funkcija uticaja ($a=0.70$, $b=0.85$, $c=0.95$)

Hampelova funkcija redukuje uticaj ekstremnih vrednosti distribucije (a , b i c) tokom procene lokacionih i parametara skaliranja iz čega proističe da ova metoda nije osetljiva na netipične vrednosti. Ako se, sledeći tu logiku, previše vrednosti odbaci, za sistem se može reći da je robustan ali ne i efikasan (optimalan). U suprotnom sistem ne bi bio robustan ali bi rasla njegova efikasnost. Kad se sve, prethodno rečeno, uzme u obzir, jasno je da parametre a , b i c treba pažljivo izabrati rukovodeći se potrebom za nivoom robustnosti s obzirom da isti imaju uticaja i na količinu "šuma" tj. smetnji kod ulaznih podataka. U izvršenom eksperimentu, vrednosti za a su izabrane tako da je 70% rezultata u intervalu $(m-a, m+a)$, 85% u intervalu $(m-b, m+b)$ i 95% u intervalu $(m-c, m+c)$ gde m predstavlja srednju vrednost. rezultati dobijeni posle *Tanh-estimators* normalizacije, prikazani su na slici 58. Sličnost je dobijena oduzimanjem normalizacionih rezultata od 1. Priroda ovog oblika normalizacije je takva da distribucija originalnog korisnika ima srednju vrednost od 0.5, dok je njegova standardna devijacija otprilike 0.01 gde konstanta 0.01 predstavlja raspon normalizovanih rezultata originalnih korisnika. U eksperimentu su dobijeni sledeći rezultati standardne devijacije:

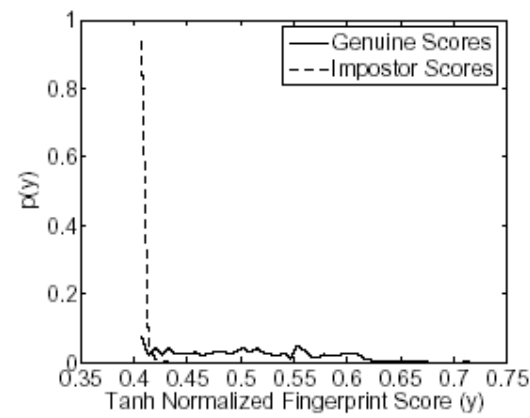
- crte lica – 16.7
- otisak prsta – 202.1
- geometrija dlana – 38.9

Iz prethodnog se vidi da je razlika između dobijenih vrednosti za otisak prsta veća u proseku 10 puta u odnosu na podatke dobijene za druge dve biometrijske karakteristike. Iz navedenog razloga, konstanta, za slučaj otiska prsta, je promenjena na 0.1 što je takođe 10 puta veće od konstante za preostala dva podatka. Ova modifikacija obezbeđuje čuvanje informacija sadržanih u rezultatu dobijenih za otisak prsta, čak i posle normalizacije, čime se poboljšavaju performanse sistema.

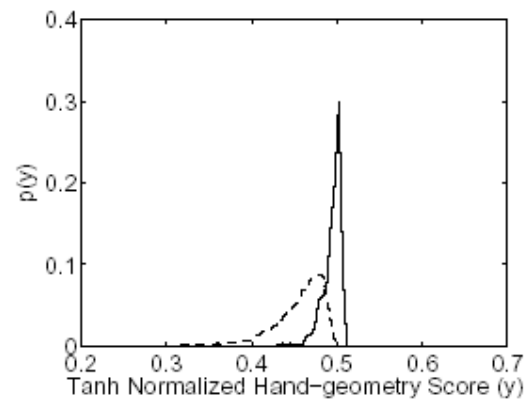
F. Mosteler i J.W. Turki u [27] predstavili su **dvotežinske procenitelje** lokacije i skaliranja koji su istovremeno robustni i efikasni. Međutim, ova metoda normalizacije funkcioniše samo sa Gausovom distribucijom podataka, a rezultati su dosta slični onima koje proizvodi *Z-rezultat* normalizacija tako da nije ni uzimana u detaljnije razmatranje u ovom slučaju.



(a)



(b)



(c)

Slika 58: Distribucije originalnog i lažnog korisnika postignute nakon Tanh-estimators normalizacije; a) Lice, (b) Otisak prstiju i (c) Geometrija dlana

Karakteristike osnovnih tehnika normalizacije prikazane su u tabeli 7.

Tehnika	Robustnost	Efikasnost
Min-Max	NE	N/A
Decimalno skaliranje	NE	N/A
Z-rezultat	NE	VISOKA (za Gausovu distrib.)
Medijana i MAD	DA	Umerena
Dvostruka sigm.funkcija	DA	VISOKA
Tanh estimatori	DA	VISOKA
Dvotežinski estimatori	DA	VISOKA

Tabela 7: Karakteristike tehnika normalizacije

7.3.1 Eksperimentalni Rezultati

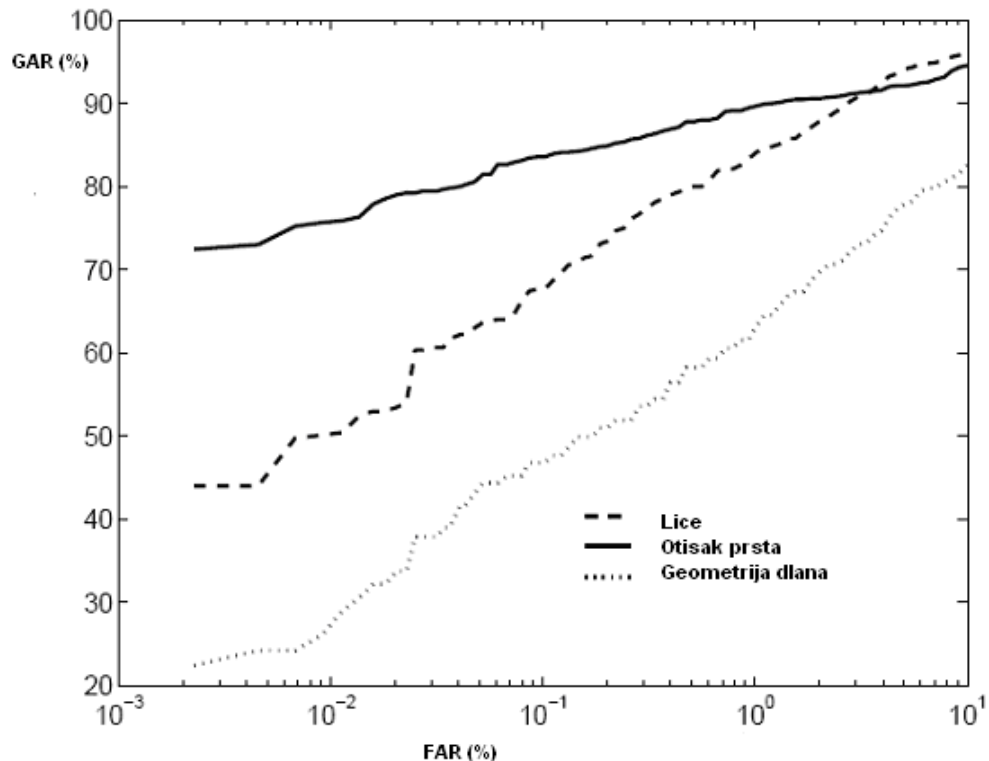
Snelik je u [8] se razvio opšte test okruženje koje dopušta sistemskim dizajnerima procenu multimodalnih biometrijskih sistema koji obuhvataju različite faktore kao što su biometrijska obeležja, usklađivanje algoritama, normalizacione šeme, metode sjedinjavanja i baze podataka. Radi ilustracije ove test metodologija, oni su procenili performanse multimodalnog biometrijskog sistema koji je upotrebio lice i otiske prstiju. Normalizacione tehnike kao *Min-max*, *Z-rezultat*, *medijana* i *MAD* i *Tanh* procenitelji su bili korišćeni za transformisanje rezultata u prost domen. Pretvoreni rezultati su zatim bili kombinovani pomoću metoda sjedinjavanja kao prost zbir, maksimalan rezultat, minimalan rezultat, suma susednih verovatnoća (pravilo sume) i proizvod susednih verovatnoća (pravilo proizvoda). Njihovi eksperimenti, zasnovani na bazi podataka sa više nego 1,000 korisnika, pokazali su da *Min-max* normalizacija praćena sumom rezultata metodom sjedinjavanja generalno pruža bolje performanse prepoznavanja nego druge šeme. Međutim, razlozi za takvo ponašanje nisu bili predstavljeni od ovih autora. U ovom radu, pokušana je analiza razloga za pojavu razlike u performansama drugačijih normalizacionih šema. Eksperimentom je pokušano sistematično proučavanje različitih normalizacionih tehnika kako bi se potvrdila njihovu ulogu u performansama multimodalnog biometrijskog sistema koji se sastoji od crta lica, otiska prsta i geometrije dlana. Pored četiri normalizacione tehnike iskorišćene u [8], takođe analizirana je *Dvostruka Sigmoidna* normalizaciona tehnika.

7.3.1.1 Generisanje multimodalne baze podataka

Multimodalna baza podataka, upotrebljena u ovim eksperimentima, bila je sagrađena sjedinjavanjem dve odvojene baze (od 50 korisnika svaka) čiji su podaci sakupljeni pomoću različitih senzora u različitim vremenskim intervalima. Prva baza podataka (opisana u [6]) je bila kreirana na sledeći način: Pet slika lica i pet otisaka prsta (istog prsta) dobijeni su iz skupa od 50 korisnika. Slike lica su kreirane pomoću *Panasonic CCD* kamere (640× 480), a otisci prstiju pomoću digitalnog biometrijskog senzora (500dpi, 640× 480). Pet slika geometrije dlana, uzete takođe od 50 korisnika (neki korisnici su prisustvovali u oba skupa), prikupljene supomoću *Pulnix TMC-7EX* kamere. Uzajamna nezavisnost biometrijskih obeležja dopustila je nasumično uparivanje korisnika iz dva skupa. Na ovaj način, multimodalna baza podataka sastavljena od 50 virtuelnih korisnika od kojih je svaki imao pet biometrijskih šablona svakog oblika. Biometrijski podaci dobijeni od svakog korisnika su upoređeni sa podacima svih korisnika u bazi podataka vođenih jednim originalnim rezultujućim vektorom i 49 vektora lažnih rezultata za svaki različit unos. Na taj način je 500

(50×10) originalnih rezultujućih vektora i 24500 (50×10×49) vektora lažnih rezultata dobijeno iz ove baze podataka. Druga baza podataka takođe se sastojala od 50 korisnika čije crte lica su dobijene pomoću Sonijeve video kamere (256× 384), a otisci prstiju pomoću Identix senzora (500dpi, 255× 256). *Pulnix TMC-7EX* kamera je bila korišćena za dobijanje slike geometrije dlana. Ova baza podataka je takođe narasla na 500 originalnih i 24,500 lažnih vektora. Sjedinjavanjem rezultata ove dve baze podataka dobijena je nova koja se sastojala od 100 korisnika sa 1,000 originalnih 49,000 lažnih rezultujućih vektora. Rezultat vektorski je 3-zapis $\{s_{1k}, s_{2k}, s_{3k}\}$, gdje s_{1k} , s_{2k} , i s_{3k} odgovaraju prema k-tom rezultatu poređenja dobijenom od modula poređenja crta lica, otiska prsta i geometrije dlana, respektivno. Vektori rezultata od 10 originalnih i 10× 49 lažnih korisnika raspoloživih za svakog korisnika, vektori rezultata 6 originalnih i 6 lažnih korisnika su bili nasumično izabrani i upotrebljeni za tzv. obuku (za obračunavanje parametara svake normalizacione tehnika ili za proračunavanje gustine kod Parzenove metode prozora). Preostali rezultati 4 originalna i 4× 49 lažna korisnika svakog korisnika su bili korišćeni za testiranje performansi sistema. Opet je pretpostavljena nezavisnost tri tehnologije, stvorena su 43 "virtuelna" korisnika od svakog realnog korisnika, kod razmatranja svih mogućih kombinacije rezultata ove tri karakteristike. Tako, dobijamo 64,000 (100×43) vektora originalnih i 313600 (100×43×49) lažnih korisnika za analizu performansi sistema. Ovo razdvajanje baze podataka u skupove za tzv. testiranje je bilo ponovljeno 40 puta kao rezultat čega su dobijene prosečne vrednosti performansi. Poređenje otiska je izvršeno na osnovu "*minutiae*" [28] i izlaz modula za poređenje je imao rezultat sličnosti (eng. *similarity score*). Svojsveni koeficijenti su bili korišćeni za predstavljanje karakteristika crta lica [29]. Euklidova udaljenost između svojsvenih koeficijenata šablona crta lica i tih ulaznih crta lica je korišćena kao rezultat poređenja.

Prepoznavanja performansi crta lica, otiska prsta i geometrije dlana kod unimodalnih biometrijskih sistema prikazani su na slici 59.



Slika 59: ROC (eng. Receiver Operating Characteristic) krive pojedinačnih karakteristika

7.3.2 Uticaj normalizacije na performanse sjedinjavanja podataka

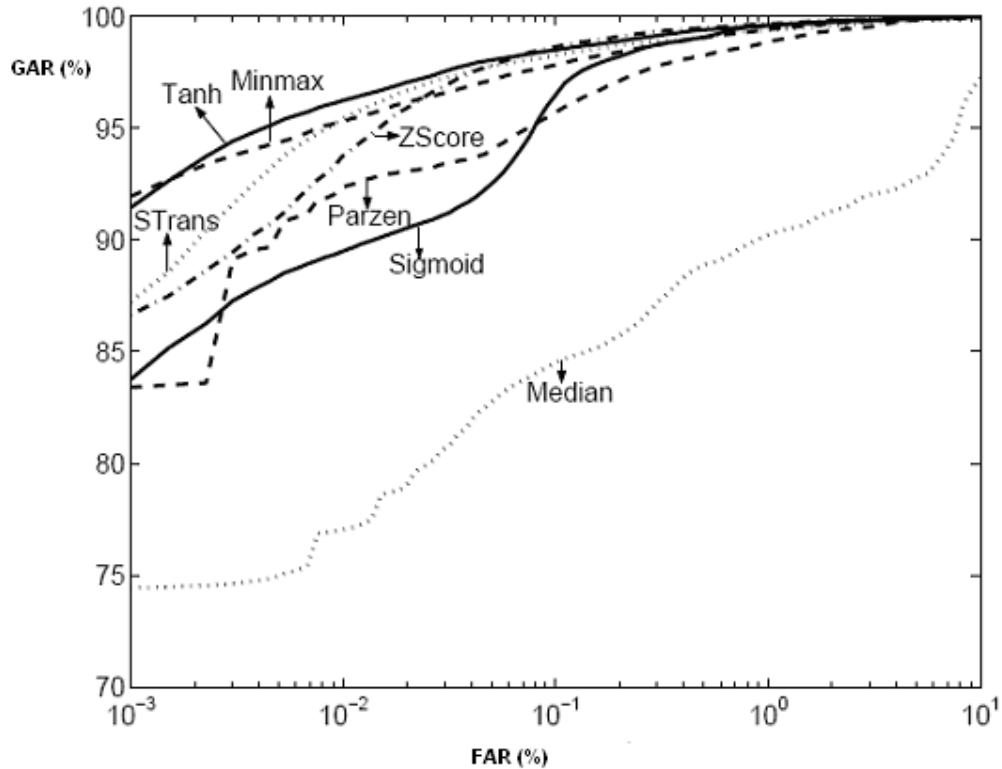
Performanse multimodalnog sistema su proučavane u okviru različitih normalizacionih i tehnika sjedinjavanja. Jednostavno sabiranje rezultata, kao i metode minimalnog i maksimalnog rezultata sjedinjavanja (opisanih u [8]), izvršeni su nad normalizacionim rezultatima. Rezultati normalizacije su dobijeni tehnikama kao što su tzv. različit ka sličnom transformacija (eng. *Distance to similarity transformation*) bez izmena u skali (*STran*), *Min-max* normalizacija, *Z-rezultat* normalizacija, *Medijana-MAD* normalizacija, *Dvostruka Sigmoidna* normalizacija, *Tanh* normalizacija kao i *Parzenova*¹³ normalizacija. U tabeli 7. grupisane su prosečne vrednosti (od 40 pokušaja) prihvatljivosti originalnog korisnika (eng. *Genuine Acceptance Rate, GAR*) multimodalnog sistema uz standardnu devijaciju *GAR*-a (navedeno u zagradama) za različite vidove normalizacije i metode sjedinjavanja podataka pri grešci prihvatanja, *FAR* od 0.1%.

NORMALIZACIJA	Tehnike sjedinjavanja		
	Zbir rezultata (%)	Max. rezultat (%)	Min.rezultat (%)
STrans	98.3 (0.4)	46.7 (2.3)	83.9 (1.6)
Min-Max	97.8 (0.6)	67.0 (2.5)	83.9 (1.6)
Z-rezultat	98.6 (0.4)	92.1 (1.1)	84.8 (1.6)
Medijana	84.5 (1.3)	83.7 (1.6)	68.8 (2.2)
Sigmoidna norm.	96.5 (1.3)	83.7 (1.6)	83.1 (1.8)
Tanh norm.	98.5 (0.4)	86.9 (1.8)	85.6 (1.5)
Parzenova norm.	95.7 (0.9)	93.6 (2.0)	83.9 (1.9)

Tabela 8: *GAR* različitih tehnika normalizacije i sjedinjavanja podataka pri *FAR* = 0.1%

Na slici 60. prikazane su performanse sistema za prepoznavanje kod kojeg su rezultati kombinovani korišćenjem metode zbira rezultata. Zapaža se da multimodalni sistem koristeći navedenu metodu proizvodi bolje rezultate od najboljeg klasičnog biometrijskog sistema za slučaj svih tehnika normalizacije, osim *Medijana-MAD* tehnike. Ako za primer uzmemo da je za otisak prsta vrednost *GAR*-a oko 83.6% pri *FAR* = 0.1%, kod *Z-rezultat* tehnike normalizacije, kod multimodalnih sistema, taj isti *GAR* = 98.6%. Ta razlika je značajna i predstavlja prednost multimodalnog sistema.

¹³ Konverzija rezultata poređenja u susedne verovatnoće metodom Parzenovog prozora nije prava tehnika normalizacije



Slika 60: ROC krive zbira rezultata tehnike sjedinjavanja pri različitim normalizacionim tehnikama

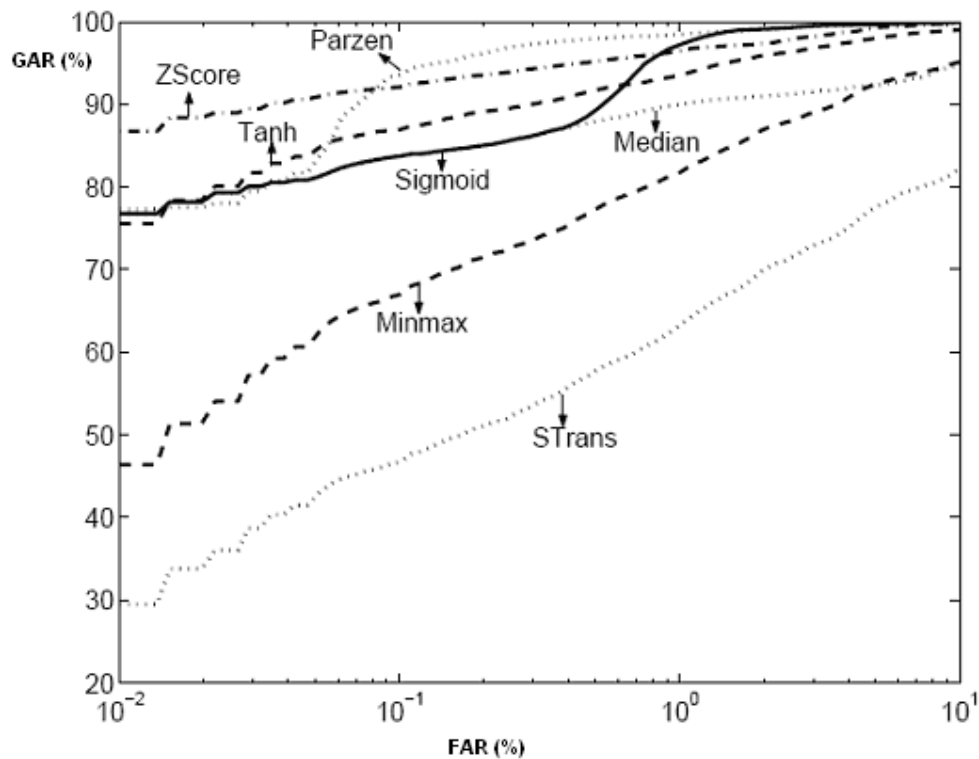
Sa slike se vidi da pri manjim vrednostima FAR-a, *min-max* i *Tanh* tehnike daju bolje rezultate GAR-a što se menja u korist *Z-rezultat* normalizacione tehnike povećanjem FAR-a. Kod multimodalnih sistema, pri metodi zbira rezultata, kombinovani rezultat s_k predstavlja linearnu transformaciju rezultujućeg vektora $\{s_{1k}, s_{2k}, s_{3k}\}$ itd.

$$s_{k1} = (a_1 s_{1k} - b_1) + (a_2 s_{2k} - b_2) + (a_3 s_{3k} - b_3) \quad [27]$$

gde s_{1k} , s_{2k} i s_{3k} odgovaraju k-tim rezultatima poređenja dobijenih analizom crta lica, otiska prsta i geometrije dlana, respektivno. Cilj upotrebe različitih normalizacionih tehnika je da se odrede vrednosti za težine (značaj) a_1 , a_2 i a_3 kao i faktora uticaja b_1 , b_2 i b_3 . Iako je *MAD* rezultat kod otiska prsta dosta manji nego u prethodnim slučajevima, ova tehnika dodeljuje otisku prsta daleko veći nivo značaja tj $a_2 \gg a_1, a_3$ što je direktna posledica slabije efikasnosti *Medijana-MAD* sistema za procenu. Distribucija rezultata poređenja otisaka prstiju direktno odstupa od Gausove pretpostavke pa kao takve, *Medijana* i *MAD* nisu dobre mere za parametre lokacije i skale, respektivno. Na ovaj način se kombinovani rezultat dovodi skoro na istu vrednost koja se dobija samo poređenjem otisaka prstiju što nije slučaj sa drugim tehnikama gde se uzimaju optimalne vrednosti sva tri faktora uticaja čime se dobijaju i bolji rezultati. Naravno, ova pretpostavka važi za slučaj da su ulazni podaci, odnosno biometrijske karakteristike kompatibilne.

Prema istraživanjima sprovedenim u [8], kad se u prosti zbir normalizovanih rezultata poređenja otisaka prstiju, dodaju vrednosti težinskih faktora, performanse se vidno poboljšavaju za vrednosti FAR od 0.01-10%.

Na slici 61. prikazan je multimodalni sistem koji koristi metodu maksimalnog rezultata kod sjedinjavanja podataka.

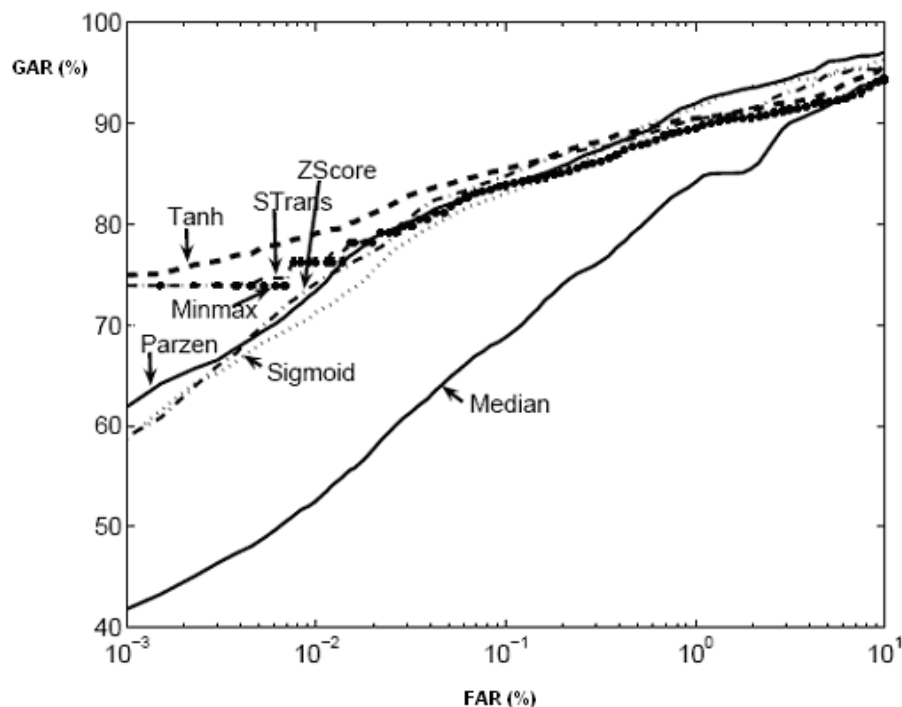


Slika 61: ROC krive tehnike maksimalnog rezultata sjedinjavanja pri različitim normalizacionim tehnikama

Ovde *Parzenova* metoda i *Z-rezultat* normalizacija daju bolje rezultate u odnosu na one koje daje sistem za poređenje otisaka prstiju. Ako se koristi samo tzv. “različit ka sličnom” metoda, rezultati poređenja geometrije dlana preuzimaju primat. Kod *min-max* normalizacije, crte lica i geometrija dlana su kompatibilne karakteristike pa samim tim i daju bolje rezultate poređenja što i objašnjava situaciju da ovakav multimodalni sistem daje rezultate bliske sistemu za poređenje crta lica. Međutim, kod normalizacionih tehnika kao što su *Dvostruka Sigmoidna* funkcija, *Tanh*¹⁴ ili *Medijana-MAD*, otisci prstiju preuzimaju primat po efikasnosti poređenja i dobijeni rezultati su veoma blizu onima koje proizvodi sistem specijalizovan za poređenje isključivo otisaka prstiju. Kod *Z-rezultat* tehnike, sva tri ulazna podatka su kompatibilna pa rezultati zavise od svih njih. Na kraju, *Parzenova* metoda praćena sjedinjavanjem, upotrebom metode maksimalnog rezultata, obezbeđuje veoma visok nivo prihvatljivosti (GAR) i korisnik se odbija samo u slučaju da sva tri sistema prijave grešku pri proceni.

Slika 62. prikazuje multimodalni sistem koji koristi sistem minimalnog rezultata kod sjedinjavanja podataka. Kod *Medijana-MAD* normalizacije najniže rezultate daje poređenje crta lica tako da je ovaj multimodalni sistem vrlo blizak specijalizovanom sistemu za poređenje crta lica. Kod svih drugih normalizacionih tehnika, rezultati poređenja otisaka prstiju imaju manje vrednosti od ostalih tako da je u ovom slučaju sistem, prema dobijenim informacijama, blizak sistemu za poređenje otisaka prstiju.

¹⁴ Tanh – hiperbolični tangens

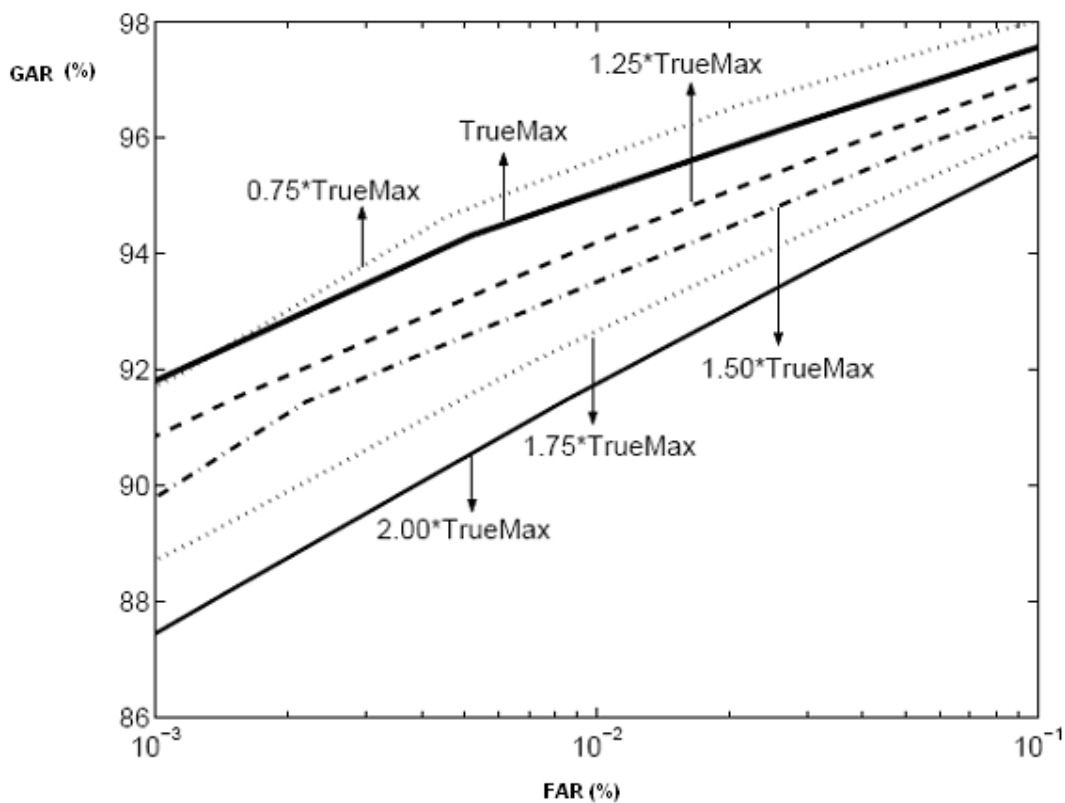


Slika 62: ROC krive minimalnog rezultata tehnike sjedinjavanja pri različitim normalizacionim tehnikama

7.3.3 Analiza robustnosti metoda normalizacije

Kod metode zbira rezultata sjedinjavanja vidi se da su performanse robustnih tehnika kao što je *Tanh* skoro identične onim ne-robustnim, kao što je tehnika minimalnog rezultata ili *Z-rezultat*. Pa ipak, performanse ovi drugih su veoma zavisne od procene vrednosti parametara lokacije i skale. Rezultati dobijeni u prethodnom eksperimentu nemaju granicu i teoretski mogu imati bilo koju vrednost, a isto tako i statističke vrednosti (prosečna i standardna devijacija) nisu poznate što iziskuje njihovu procenu koristeći postojeće podatke.

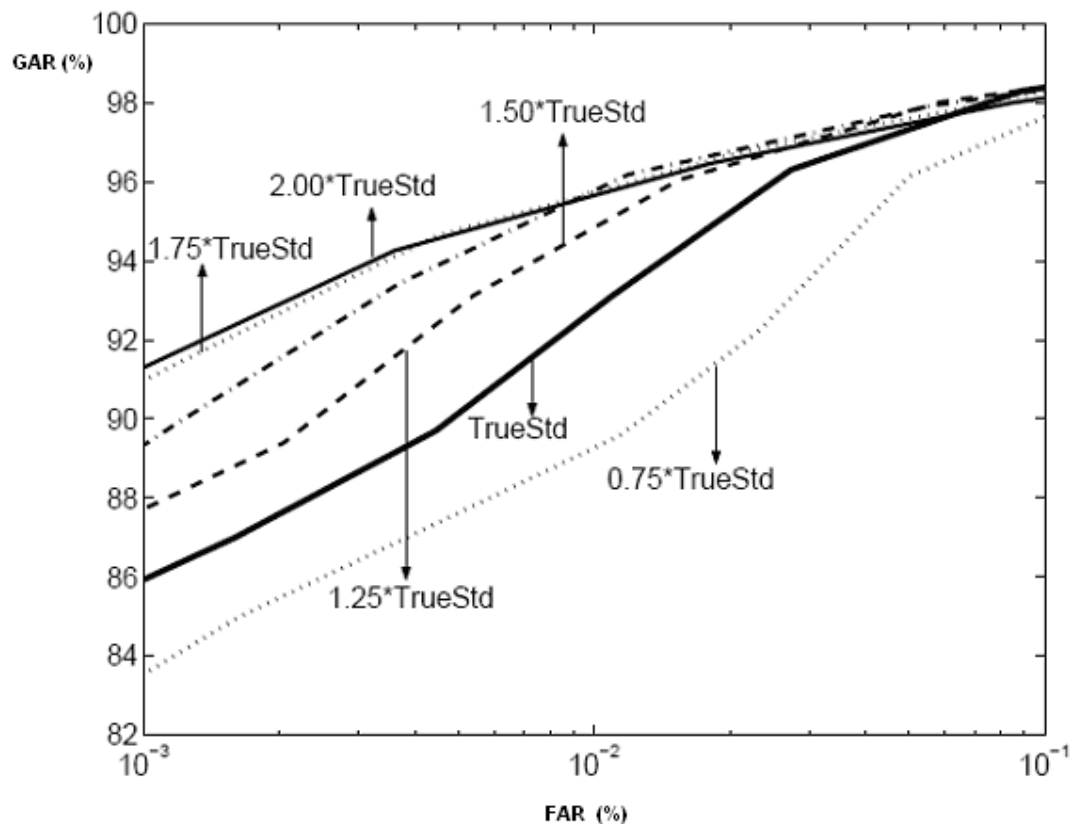
Obzirom da ti podaci nisu sadržali nikakve netipične vrednosti, performanse ne-robustnih sistema nisu izmenjene. Međutim, kako bi demonstrirali njihovu osetljivost na netipične vrednosti, unete su izmene u rezultate dobijene poređenjem otisaka prstiju, odnosno, rezultati su povećani za 25%, 50%, 75% ili 100%. Na slici 63. prikazane su performanse sistema nakon izmene ovih vrednosti.



Slika 63: Analiza robustnosti kod min-max normalizacije

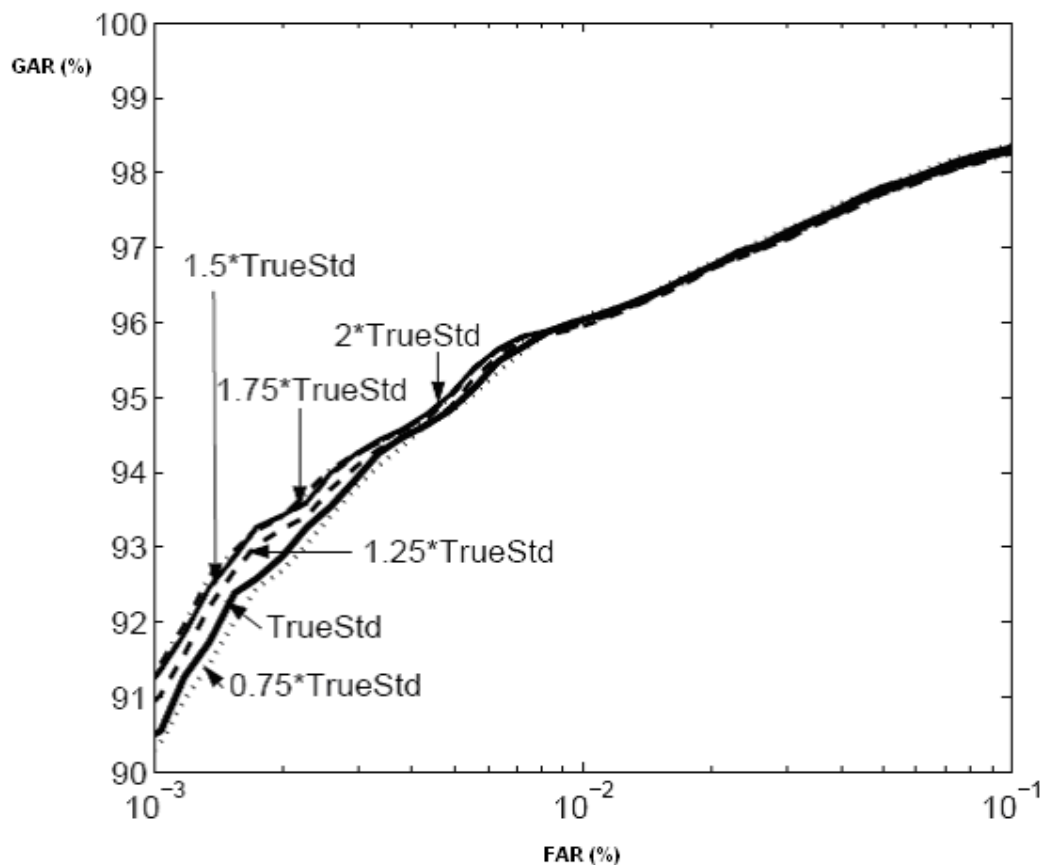
Sa slike se može zaključiti da postoji velika osetljivost maksimalnih vrednosti od ove izmene, tj. uvećanjem rezultata za 25%, efikasnost prepoznavanja opada za 3-5 % i razlika je veća povećanjem FAR-a.

Kod *Z-rezultat* normalizacije, u cilju eksperimenta, standardna devijacija rezultata poređenja otiska prstiju je povećana takođe za 25%, 50%, 75% i 100% dok je neki od velikih originalnih rezultata smanjen na 75% svoje vrednosti. Rezultat ispitivanja prikazan je na slici 64.



Slika 64: Analiza robustnosti kod Z-rezultat normalizacije

Sve dok je početna standardna devijacija mala, otisku prsta se dodeljuje visok nivo uticaja u odnosu na druge karakteristike, međutim, kako se standardna devijacija povećava smanjuje se i uticaj rezultata poređenja otisaka prstiju što dovodi do povećanja efikasnosti sistema. Cilj eksperimenta je bio da se prikaže osetljivost sistema na one procenjene parametre koji mogu biti lako izmenjeni. Sličan eksperiment je izvršen i za slučaj *Tanh* normalizacije (slika 65.) gde nije bilo znatnijih odstupanja unošenjem izmena u rezultate čime se dokazuje robustnost ovog sistema.



Slika 65: Analiza robustnosti kod Tanh normalizacije

7.4 Zaključak

Normalizacija rezultata predstavlja veoma važan deo pri sjedinjavanju podataka na nivou poređenja i kao takva ima veliki uticaj na performanse samog sistema. U ovom delu rada prikazani su efekti raznih tehnika normalizacije na performanse multimodalnog sistema, dokazano je da se normalizacijom kao prethodnici sjedinjavanja, povećava efikasnost sistema prepoznavanja koji koristi kao ulazne podatke crte lica, otisak prsta i geometriju dlana. Z-rezultat, min-max i Tanh normalizacione tehnike, u odnosu na ostale, proizvele su najveće vrednosti GAR-a, a takođe je dokazano i da su prve dve navedene tehnike osetljive na unos netipičnih vrednosti rezultata. Za razliku od njih, Tanh normalizacija je istovremeno i efikasna i robustna.

Ako su parametri lokacije i skale upoređenih rezultata (minimum i maksimum kod min-max i srednja, odnosno standardna devijacija kod Z-rezultat) individualnih modula unapred poznati onda normalizacione tehnike tipa min-max i Z-rezultat nisu potrebne. Ali, ako je potrebna procena ovih parametara upotrebom tzv. rezultata obuke i ako ti rezultati nisu savršeni potrebno je izabrati neku robustnu tehniku normalizacije. Takođe, pomenuta je i upotreba ne-parametarskog pristupa kao što je Parzenova metoda procene gustine prozora u cilju konvertovanja rezultata poređenja u susedne verovatnoće i zatim njihovog kombinovanja upotrebljavajući neke od metoda sjedinjavanja. Ovim načinom se izbegava potreba za bilo kakvim znanjem o distribuciji rezultata poređenja.

8. Soft biometrija

Postojeći biometrijski sistemi, jednostavno rečeni, nisu savršeni. I dalje procenat greške nije jednak nuli, a takođe se pojavljuju i smetnje pri očitavanju osetljivih podataka. Većinu ovih problema rešavaju robustni multimodalni biometrijski sistema koji opet, s druge strane, zahtevaju duže vreme prijavljivanja i obrade podataka. Kao dodatak celoj priči, u nekim situacijama se u cilju povećanja efikasnosti, multimodalnim biometrijskim sistemima dodaju još neki podaci koji ne izazivaju nelagodnost kod korisnika sistema. Rešenje je bazirano na upotrebi individualnih karakteristika korisnika, kao što su: etnička pripadnost, boja očiju, visina, godina rođenja, pol i sl.

Na slici 66. prikazan je primer ATM terminala koji koristi kao dodatak, i tzv. soft biometrijske karakteristike u procesu verifikovanju korisnika.



Slika 66: ATM uređaj snabdeven senzorom otiska prsta kao primarnim biom. identifikatorom i kamerom za dobijanje soft identifikatora

8.1 Motiv i izazovi

Koristan uticaj soft biometrije može biti prikazan sledećim primerom. Pretpostavimo da imamo tri osobe koje se prijavljuju na sistem za proveru otiska prsta. Neka su osobe A, B i C visine 180 cm (muškarac), 170 cm (žena) i 160 cm (muškarac), respektivno. Pri ostavljanju svog uzorka X otiska prsta sistemu, uzorak osobe A se poredi sa uzorcima ostalih osoba i računaju se vrednosti susednih verovatnoća. Pretpostavimo da su izlazne vrednosti poređenja $P(A|X) = 0.42$, $P(B|X) = 0.43$ i $P(C|X) = 0.15$. U ovom slučaju bi naš korisnik bio odbijen zbog podjednake verovatnoće da je on osoba A i B ili bi greškom bio verifikovan kao osoba B. Ako se sad kao dodatne informacije uzmu visina (koja je procenjena na 178 cm) i pol korisnika, sa istima, nema sumnje da će osoba A biti pravilno verifikovana.

Prvi biometrijski sistem ovog tipa razvio je 1883. godine Alfons M. Bertilon koristeći ljudske osobina kao što su dužina i visina glave i uha, dužina srednjeg prsta i stopala, visina itd. koje su uz poznavanje osobina kao što su ožiljci, tetovaže i boja očiju, bili dovoljni za proveru ljudi. Iako neke od ovih osobina podležu promenama tokom vremena, njihovom kombinacijom se mogao postići, za to doba, zavidan nivo preciznosti. Kao naslednik ovog sistema javio se Henrijev¹⁵ sistem identifikacije putem otisaka prstiju i to iz tri osnovna razloga: vremenska zavisnost karakteristika, nedostatak preciznosti – boja očiju i etnička

¹⁵ Edvard Henri, generalni inspektor policije u Bengalu, Indija

pripadnost nisu pogodni za ljude iz istog okruženja i kao treće, vreme potrebno za uzimanje svih mera. Sličan sistem Bertilonu, razvio je i Hekatorn u [31]. Kasnije, Alisto u [32] prikazao je kako se ljudske mere, kao što su visina, težina, boja očiju i sl.) mogu nenametljivo prikupiti putem zdravstvenih centara. U svakom slučaju, sve ove metode omogućavaju neki oblik identifikacije ali sa nedovoljnim nivoom preciznosti što i dovodi do toga da se ove osobine nazivaju „*soft* biometrijske karakteristike“. *Soft* karakteristike predstavljaju, iz tog razloga, samo dodatak standardnim biometrijskim podacima u cilju povećanja preciznosti, za šta same ipak nisu dovoljne.

Neke osobine *Soft* biometrijskih karakteristika se mogu primeniti (Vajmen [33]) kao filter velikih baza podataka prilikom pretrage za identitetom korisnika. Tako, ako se može utvrditi okvirno godište korisnika ili njegova etnička pripadnost, proveru se može suziti i usmeriti samo u tom pravcu što drastično skraćuje vreme obrade. Isto tako, njihova dobra primena je i za podešavanje parametara biometrijskog sistema. Postoje indicije da su mlade azijske osobe zaposlene u rudarstvu najnepogodnije osobe za proveru otisaka prstiju [34] što stvara potrebu za podešavanjem parametara sistema kao što je *threshold* kod klasičnih unimodalnih sistema ili *threshold* i težinski faktor kod multimodalnih biometrijskih sistema kako bi se postigle optimalne performanse za određenog korisnika ili grupu.

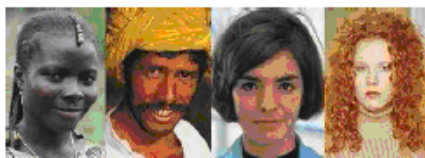
Iz svega rečenog proističe da filtriranje i podešavanje parametara sistema zahtevaju visoku tačnost sistema za izdvajanje originalnih *soft* biometrijskih podataka. Iz prethodnog se vidi da je prvi izazov automatizovano i pouzdano izdvajanje *soft* podataka na način koji neće izazvati neprijatnost kod korisnika što i predstavlja najveći razlog propasti Bertilon sistema.

U nastavku teze biće analizirano nekoliko tehnika za izdvajanje (prikupljanje) podataka: pol, etnička pripadnost, godište, visina i boja očiju. Takođe, u kratkim crtama biće opisana vizija sistema koji bi trebalo iz video zapisa u realnom vremenu da izvuče prethodno pomenute podatke. Kad se podaci izdvoje, izazov je ukombinovati ih sa standardnim biometrijskim podacima i pri tome im povećati preciznost.

8.2 Prikupljanje *soft* biometrijskih podataka

Svaki pristup koji obezbeđuje identifikacije o nečijem identitetu bez potpune sigurnosti u njega, može biti tretiran kao *soft biometrijski pristup*. Neki od pristupa prikazani su na slici 67. Mogu biti dobijeni iz velikog broja različitih biometrijskih aplikacija u praksi. Za primer se mogu uzeti demografske attribute kao što su pol, etnička pripadnost, starost, boja očiju, boja kože i sl. Kao i fizičke karakteristike (npr. ožiljci) koje se mogu dobiti iz sistema za prepoznavanje crta lica. Klasa šablona slika otisaka prstiju, koja obuhvata leve i desne krive, zavojnice i lukove i slično, takođe predstavlja *soft* biometrijski pristup. Pol, naglasak i približna starost govornika mogu biti pronađeni u sistemu za prepoznavanje glasa dok se boja očiju može dobiti iz slike rožnjače. U svakom slučaju, dobijanje ovih podataka predstavlja mukotrpan postupak.

U nastavku ove teme će biti opisani razvoji tehnika za izdvajanje informacija kao što su: visina, pol, etnička pripadnost i boja očiju.



Pol, Boja kože, Boja kose

http://anthro.palomar.edu/adapt/adapt_4.htm
© Corel Corporation, Ottawa, Canada



Visina

<http://www.altonweb.com/history/wadlow/p2.html>
© Alton Museum of History and Art



Težina

<http://www.laurel-and-hardy.com/goodies/home6.html> © CCA



Boja očiju

<http://ology.amnh.org/genetics/longdefinition/index3.html>
© American Museum of Natural History, 2001

Slika 67: Primeri soft biometrijskih pristupa

U prethodnom periodu bilo je pokušaja nekih istraživača da prethodno pomenute podatke dobiju iz slika crta lica. Guta je u [35] predstavio sistem koji se sastoji od grupe radialnih baznih funkcija za klasifikaciju pola, etničke pripadnosti i položaja ljudskih lica. Postignuti rezultati su sledeći: klasifikator pola (muški-ženski) - 96% uspešnosti, klasifikator etničke pripadnosti (bela rasa, crna rasa, južno i istočno azijska rasa) – 92% uspešnost. Rezultati su dobri zahvaljujući slikama dobijenim iz FERET¹⁶ baze podataka koja je sadržala veoma malo izmena po pitanju izraza i položaja lica. Nad istom bazom, Mogadam i Jang [36] pokazali su da se greške klasifikovanja pola mogu smanjiti na 3.4% upotrebom klasifikatora pola baziranog na izgledu koji koristi tzv. Vektorsku mašinu sa nelinearnom podrškom (eng. *Support Vector Machine* (SVM))¹⁷. Šaknarović [37] je razvio šemu za demografsku klasifikaciju kojom se izdvajaju izgledi lica iz neograničene video sekvence i zatim klasifikuju prema polu i etničkoj pripadnosti. *AdaBoost* algoritmi koji se koriste za izdvajanje, čak i u ovim okolnostima (neograničena sekvenca) obezbeđuju više od 75% tačnosti (Azijati / ne-Azijati klasifikacija). Za iste podatke, kod Mogadama i Janga, SVM klasifikator je postigao slične rezultate s tim da se daleko veća greška javljala kod osoba ženskog pola od 28%. Balči i Atalaj [38] postigli su tačnost od 86% kod klasifikatora pola koji koristi PCA (eng. *Principal Component Analysis*)¹⁸ za izdvajanje karakteristika i višestruko filtriranje za klasifikaciju. Džejn i Lu [39] predstavili su šemu zasnovanu na Linearnoj diskriminantnoj analizi (eng. *Linear Discriminant Analysis*, (LDA)) za rešavanje problema prepoznavanja etničke pripadnosti iz crta lica. Korisnici su identifikovani kao Azijati ili ne-azijati više-skalnom analizom ulaznih slika lica. Kompletно okruženje zasnovano na pravilu proizvoda, korišćeno je za integraciju LDA analize u različite skale. Šema je postigla tačnost od 96.3% na uzorku od 263 osobe sa približno istim brojem osoba oba pola. Hajaši [40] je predložio da se podaci kao što su tekstura i boja kože, koji se koriste za određivanje starost i pola, dobijaju iz slike lica. Rezultati nikada nisu objavljeni.

¹⁶ FERET – standardna baza lica koja se koristi za evaluaciju sistema za prepoznavanje crta lica. FERET program je realizovan u periodu 1993. – 1997. godine pod pokroviteljstvom US ministarstva odbrane u cilju razvoja sistema za automatsko prepoznavanje lica u bezbednosne svrhe.

¹⁷ SVM – tehnika za klasifikaciju podataka. www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf

¹⁸ PCA – analiza glavnih komponenta koji opisuju globalne sadržaje slike

Automatsko određivanje starosti je komplikovanije nego određivanje pola ili etničke pripadnosti. Bjukenon [41] je proučavao sistem koji bi preko hemijskog sastava otiska prsta mogao napraviti razliku između deteta i odrasle osobe. Kvon i Lobo [43] pokazali su algoritam za određivanje starosti iz slika lica baziran na analizi koštano-mišićnih promena kojim su pokušali da izvrše klasifikaciju na: bebe, mlađe odrasle i starije odrasle ali bez javnih rezultata o tačnosti. U skorije vreme, Lanitis je u [43] obezbedio kvantitativnu evaluaciju tri klasifikatora koji bi obezbedili automatsko određivanje starosti iz slike lica. Ovi klasifikatori koristili su tzv. *sopstveno lice* (eng. *Eigenface*)¹⁹ dobijeno PCA-om kao ulaznim podatak. Kvadratni model, klasifikator „najmanje distance“ klasifikator neuronskih mreža, hijerarhijski procenjivač starosti korišćeni su za procenu starosti korisnika. Najbolji algoritam imao je prosečnu grešku od 3.82 godine koja je veoma bliska grešci koju je načinio ljudski faktor (3.64 godine). U [44], Minemacu je pokazao da se približna starost govornika može automatski proceniti iz glasnih zapisa. Sve ovo govori da je automatska procena starosti moguća iako tehnologija na današnjem nivou nije pouzdana.

Podaci o težini korisnika se mogu dobiti navođenjem istog da stane na senzor dok se identifikuje primarnim biometrijskim sistemom. Visina se može dobiti sjedinjavanjem slika. Primer predstavlja istraživanje Su-Kima [45] koji je pomoću geometrijskih podataka izračunavao visinu objekta. Razvojem tehnologije, očekuje se i veliki napredak u postupcima izdvajanja (dobijanja) *soft* biometrijskih podataka.

8.3 Sjedinjavanje *soft* i primarnih biometrijskih informacija

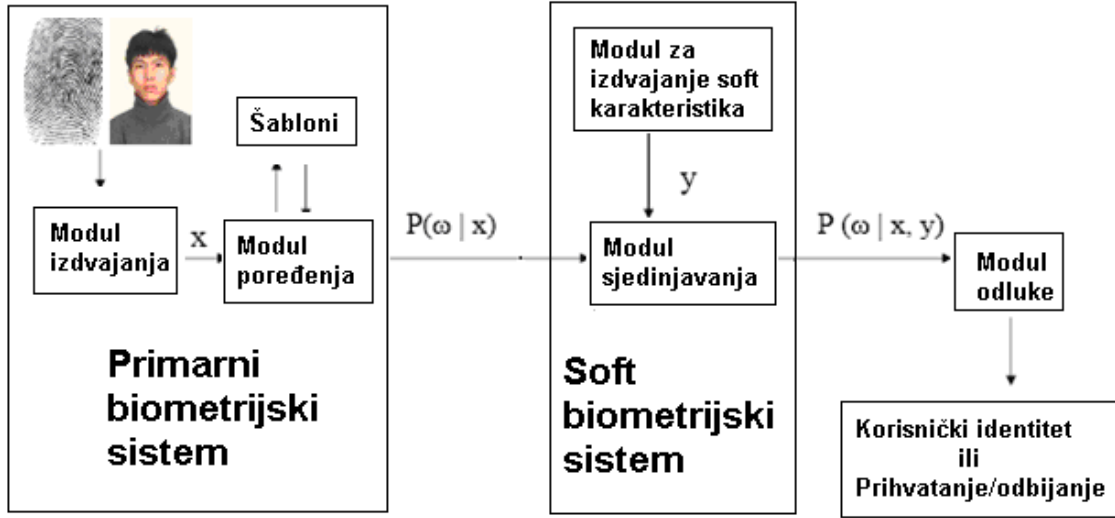
8.3.1 Režim identifikacije

Na slici 68. prikazano je okruženje biometrijskog identifikacionog sistema za integraciju primarnih i *soft* biometrijskih informacija. Primarni biometrijski sistem zasnovan je na $m(m \geq 1)$ tradicionalnih biometrijskih identifikatora (otisak prsta, geometrija dlana, crte lica, dužica oka i sl.). *Soft* biometrijski sistem zasnovan je na $n(n \geq 1)$ *soft* atributa (pol, starost, boja očiju, etnička pripadnost i sl.).

Neka da $w, w, \dots, w$ predstavlja korisnike prijavljene u bazi, a $x = [x, x, \dots, x]$ kolekciju vektora primarnih biometrijskih karakteristika. Kao primer može da posluži multimodalni sistem sa crtama lica i otiskom prsta ($m=2$), tada x_1 predstavlja vektor karakteristika lica, a x_2 vektor karakteristika otiska prsta. Neka $p(x_j|w_i)$ predstavlja mogućnost osmatranja vektora primarne biometrijske karakteristike x_j korisnika w . Ako izlaz modula svakog biometrijskog sistema predstavlja skup rezultata $s = [s_1, s_2, \dots, s_n]$ isti može aproksimirati $p(x_j|w_i)$ sa $p(s_j|w_i)$ obezbeđujući time poznavanje distribucije rezultata originalnog korisnika svakog modula.

Uzmimo da je $y = [y_1, y_2, \dots, y_n]$ vektor *soft* biometrijskih karakteristika gde je npr. y_1 pol, a y_2 boja očiju. Potrebno je proceniti susednu verovatnoću korisnika w_i koji daje x i y .

¹⁹ Eigenface – jedinstveni skup brojeva koji se određenim softverom dobija iz crta lica



Slika 68: Sistem za sjedinjavanje soft i primarnih biometrijskih podataka

Verovatnoća se može izraziti Bajesovim pravilom:

$$P(w_i | x, y) = \frac{p(x, y | w_i) P(w_i)}{p(x, y)} \quad [28]$$

Ako bi svi korisnici podjednako želeli da pristupe bazi, onda sledi

$$P(W) = \frac{1}{R}, \forall i \quad [29]$$

Ako pretpostavimo da su svi vektori primarnih biometrijskih karakteristika ($X_1, X_2, \dots, X_n$) i sve *soft* biometrijske promenljive ($Y_1, Y_2, \dots, Y_n$) međusobno nezavisni za identitet korisnika W_i , diskriminantna funkcija $g_i(X, Y)$ za korisnika W_i može biti predstavljena na sledeći način:

$$g_i(x, y) = \sum_{j=1}^m \log p(x_j | w_i) + \sum_{k=1}^n \log p(y_k | w_i) \quad [30]$$

8.3.2 Režim verifikacije

U ovom modu se pokušaj autentifikacije klasifikuje kao pokušaji originalnog i lažnog korisnika. Za slučaj verifikacije, Bajesovo pravilo odlučivanja može biti predstavljeno na sledeći način:

$$\frac{P(\text{originalni} | x, y)}{P(\text{lažni} | x, y)} = \frac{p(x, y | \text{originalni})P(\text{originalni})}{p(x, y | \text{lažni})P(\text{lažni})} \geq \tau \quad [31]$$

gde τ predstavlja *threshold* parametar. Povećanjem njegove vrednosti, redukuje se FAR i povećava FRR i obrnuto. Ako su vrednosti prethodnih verovatnoća oba tipa korisnika jednake, i ako pretpostavimo nezavisnost vektora oba sistema, diskriminantna funkcija može biti zapisana na sledeći način:

$$g(x, y) = \sum_{j=1}^m \log\left(\frac{p(x_j|\text{originalni})}{p(x_j|\text{lažni})}\right) + \sum_{k=1}^n \log\left(\frac{p(y_k|\text{originalni})}{p(y_k|\text{lažni})}\right) \quad [32]$$

Ako je izlaz svakog modula primarnog biometrijskog sistema skup $S=[S_1, S_2, \dots, S_m]$ isti može aproksimirati $p(X_j|\text{originalni})$ i $p(X_j|\text{lažni})$ sa $p(S_j|\text{originalni})$ i $p(S_j|\text{lažni})$ obezbeđujući time poznavanje rezultujućih distribucija svakog modula oba tipa korisnika.

8.3.2.1 Izračunavanje soft biometrijskih verovatnoća

Jednostavan način izračunavanja *soft* biometrijskih verovatnoća $p(Y_k|W_i)$, pri $k=1,2,\dots,n$ je njihovom procenom, zasnovanom na sistemima za procenu *soft* biometrijskih podataka. Na primer, ako je tačnost klasifikatora pola α onda:

- $P(\text{pretpostavka da je pol muški} \mid \text{tačan pol je muški}) = \alpha$
- $P(\text{pretpostavka da je pol ženski} \mid \text{tačan pol je ženski}) = \alpha$
- $P(\text{pretpostavka da je pol muški} \mid \text{tačan pol je ženski}) = 1 - \alpha$
- $P(\text{pretpostavka da je pol ženski} \mid \text{tačan pol je muški}) = 1 - \alpha$

Slično toma, ako je prosečna greška u merenju visine μ_e i standardna devijacija greške σ_e , logično je pretpostaviti da $p(\text{pretpostavljena visina} \mid w_i)$ prati Gausovu distribuciju sa sredinom $(h(w_i) + \mu_e)$ i standardnom devijacijom σ_e gde $h(w_i)$ predstavlja pravu visinu korisnika w_i . Ipak, postoje određeni problemi kad su verovatnoće procenjene samo na osnovu tačnosti *soft* sistema za izdvajanje potrebnih karakteristika. Diskriminantna funkcija u formuli 30 dominantna je kod *soft* biometrijskih izraza zbog velikih dinamičkih raspona logaritamskih vrednosti verovatnoće. Na primer, ako je klasifikator pola 98% tačan ($\alpha=0.98$), logaritamska verovatnoća će biti -0.02 ako je klasifikacija tačna ili -3.91 ako nije. Ovolika razlika se javlja zbog većeg broja *soft* biometrijskih karakteristika. Kako bi se razlika ublažila, predstavljen je faktor skaliranja β , $0 \leq \beta \leq 1$ kako bi se „ispeglala“ distribucija verovatnoće svakog *soft* biometrijskog pristupa. Ako je q_{ki} procena verovatnoće $p(y_k|w_i)$ zasnovana na tačnosti sistema za izdvajanje karakteristika, težinska verovatnoća p' se može predstaviti kao:

$$p'(y_k|w_i) = \frac{q_{ki}^{\beta_k}}{\sum_k Y_k q_{ki}^{\beta_k}} \quad [33]$$

gde Y_k predstavlja skup mogućih vrednosti diskretnih promenljivih y_k , a β_k težinski faktor dodeljen k -toj *soft* biometrijskoj karakteristici. Ako je y_k kontinualna sa standardnom devijacijom σ_k , verovatnoća može biti skalirana zamenom σ_k sa σ_k / β_k . Ovaj „težinski“ pristup se često koristi kod prepoznavanja glasa u smislu procene susednih verovatnoća reči zasnovanih na jezičkim pravilima. Ovaj metod izračunavanja ima, takođe i implicitnih prednosti. Lažni korisnik može lako obmanuti *soft* biometrijski sistem jer je relativno jednostavno prilagoditi traženi *soft* atribut kozmetičkim intervencijama i adekvatnom odećom.

U ovom slučaju težinski faktor može izigravati meru verodostojnosti čija vrednost zavisi od samog okruženja. Ako je u pitanju okruženje sklono obmanjivanju, vrednost faktora β_k trebala bi biti što bliža nuli. Diskriminantne funkcije 30 i 32 su optimalne za slučaj međusobno nezavisnih biometrijskih karakteristika. U suprotnom, funkcija je sub-optimalna i trebalo bi poboljšati rezultate prepoznavanja odabirom odgovarajuće vrednosti faktora β_k .

8.4 Eksperimentalni rezultati

Izvršeni eksperimenti prikazali su prednost upotrebe informacija o polu, etničkoj pripadnosti i visini kao dodatak primarnim biometrijskim identifikatorima. Za eksperiment korišćen je podskup JMD (eng. *Joint Multibiometric Database*) prikupljen od strane univerziteta zapadne Virdžinije. Isti sadrži četiri slike lica i četiri prikaza prsta uzetih na uzorku od 263 osobe tokom perioda od šest meseci. Za poređenje lica, korišćen je *Identix faceIT®SDK*²⁰. Poređenje otisaka prstiju je bilo zasnovano na algoritmu opisanom u [28].

Klasifikator etničke pripadnosti, predstavljen u [39] takođe je korišćen u eksperimentima sa ciljem testiranja korisnika da li su Azijati ili ne sa tačnošću procene od 82.3%. Ako je uključena i opcija „odbijanje“ (eng. *Rejected*), verovatnoća pogrešne procene je smanjena na manje od 2% po cenu odbijanja 25% slika. Klasifikator pola izrađen je metodologijom opisanom u [39] za klasifikaciju etničke pripadnosti i može se reći da su im performanse slične. Procenat odbijanja je oko 25%, a tamo gde su klasifikatori izvršili odbijanje, odgovarajuća informacija nije korišćena za *update*-ovanje diskriminantne funkcije odnosno, ako je podatak dodeljen k-tom *soft* biometrijskom pristupu „odbijen“, izraz sa logaritamskom verovatnoćom koji odgovara k-toj karakteristici u formulama 30 i 32 će biti postavljen na nulu. Tokom prikupljanja podataka za WVU multimodalnu bazu, takođe su bile zabeležene i aproksimacije visine svakog korisnika. Visine u eksperimentu nisu merene nego procenjivane za svakog korisnika w_i iz normalne distribucije sa sredinom $h(w_i) + \mu_e$ i standardnom devijacijom σ_e gde je $h(w_i)$ prava visina korisnika w_i , $\mu_e = 2$ cm, a $\sigma_e = 5$ cm.

8.4.1 Identifikacione performanse

Kako bi se proverile identifikacione performanse sistema, po jedna slika lica i otiska prsta svakog korisnika uzeti su kao šabloni dok su po ostala tri primerka uzeta kao probni uzorci. Razdvajanje baza lica i otisaka prstiju u galeriju i skup za probu je ponovljen 50 puta i prosek je uzet kao rezultat. Težinski faktor, korišćen kod izračunavanja *soft* biometrijske verovatnoće dobijen je detaljnom pretragom baze za probu (eng. *Training database*). Multimodalna baza iz [46] korišćena je za procenu faktora. Za svaki *soft* podataka, faktor β_k povećavan je za 0.05 i uzeta je vrednost koja maksimalno uvećava procenat uspešnosti prepoznavanja biometrijskog sistema (upotrebom crta lica, otisaka prstiju i odgovarajućih *soft* informacija). Ovom procedurom, za pol, etničku pripadnost i visinu, kao najbolje, uzete su vrednosti 0.1, 0.1 i 0.5, respektivno.

Istražen je i uticaj *soft* biometrijskih identifikatora na performanse tri primarna sistema, otisak prsta, crte lica i multimodalni sistem koji koristi iste identifikatore. Slika 69. prikazuje tzv. kumulativnu karakteristiku tačnih poređenja (eng. *Cumulative match Characteristic*, CMC) sistema i poboljšanje performansi upotrebom *soft* biometrijskih informacija. Upotreba podataka o etničkoj pripadnosti i polu dovela je do poboljšanja performansi za 1.3% (slika

²⁰ Identix FaceIT® SDK – obezbeđuje programerima razvoj sopstvenih biometrijskih rešenja i vršenje validacije istog zasnovanu na Identix tehnologiji. Identix nudi šablone (vektorski, LFA-5.2KB i STA-6.7KB optimizovane po pitanju brzine i performansi. Tehnologija je zasnovana na kombinaciji LFA (eng. *Local feature analysis*) i STA (eng. *Surface texture analysis*) što obezbeđuje viši nivo robustnosti sistema.

69a). Sa slike 69b. vidi se da i podatak o visini donosi poboljšanje performansi za približno 1% što dovodi do toga da se njihovom kombinacijom rezultati poboljšavaju do 2.5% (slika 69c).

Etnička pripadnost i pol nisu, u pogledu statistike, obezbedili neka značajna poboljšanja kod sistema za prepoznavanje lica što se može zaključiti iz toga što je *FaceIT*® algoritam te podatke već uključio s obzirom da se 90% grešaka javljalo u slučajevima istih polova, etničke pripadnosti ili oba istovremeno. S druge strane, informacije o visini, koja ne zavise od svojstva lica, mogu biti od pomoći za nekih 0.5 - 1% (slika 70). beskorisnost informacija o etničkoj pripadnosti mogu biti od koristi samo ako su *soft* informacije komplementarne sa primarnim biometrijskim informacijama.

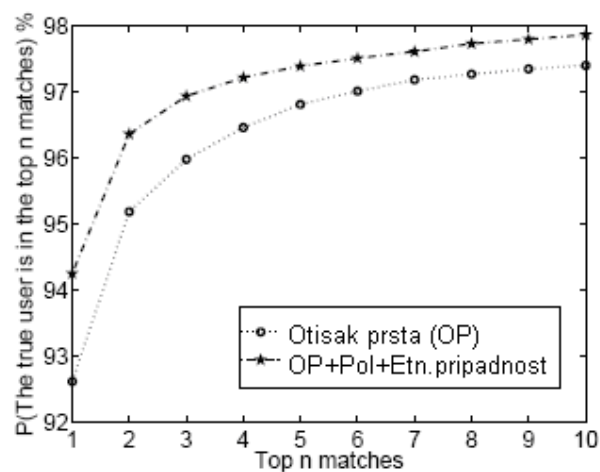
Slika 71. prikazuje performanse sistema koji kombinuje soft identifikatore sa crtama lica i otiscima prstiju zajedno. Iako je multimodalni sistem koji koristi crte lica i otiske prstiju visoko kotiran na lestvici uspešnosti sa 97% prepoznavanja, dodatnih 1 - 2% se mogu dobiti kombinacijom sa soft biometrijskim informacijama.

8.4.2 Verifikacione performanse

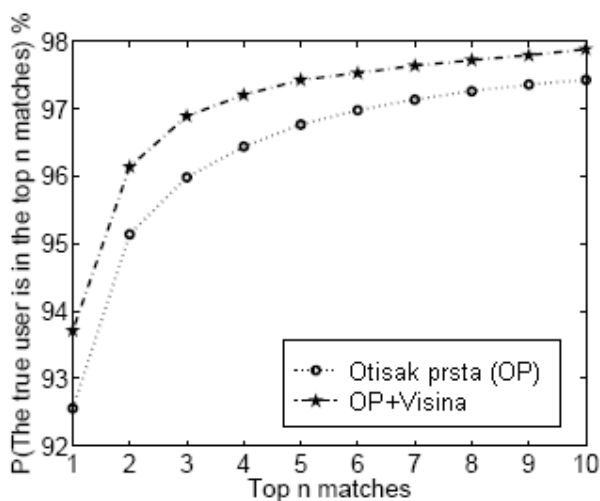
Rezultati originalnog i lažnog korisnika dobijeni su izračunavanjem sličnosti među svim različitim parovima uzoraka. Zatim su konvertovani u odnose logaritamskih verovatnoća upotrebljavajući procedure opisane u [46]. Ovaj pristup uključuje ne-parametarsku procenu generalizovanih gustina rezultata oba tipa korisnika za svaku karakteristiku. Težinski faktor korišćen u prethodnom slučaju je procenjen sličnom tehnikom kao kod identifikacije s tim da su vrednosti uzete tako da maksimiziraju GAR pri FAR = 0.1%. Najbolje vrednosti težinskog faktora su 0.5, 0.5 i 0.75 za pol, etničku pripadnost i visinu, respektivno. Razliku koja se javila u vrednostima težinskog faktora u identifikacionom i verifikacionom režimu treba pripisati upotrebi različitih diskriminantnih funkcija za sjedinjavanje datim u izrazima 30 i 32.

Slika 70. prikazuje ROC krivu gde je otisak prsta primarni identifikator, Pri nižim FAR vrednostima, performanse su dosta lošije iz razloga velike sličnosti nekoliko otisaka lažnog korisnika. Uvođenjem *soft* identifikatora, GAR se povećava za više od 20% pri FAR = 0.001% (slika 72).

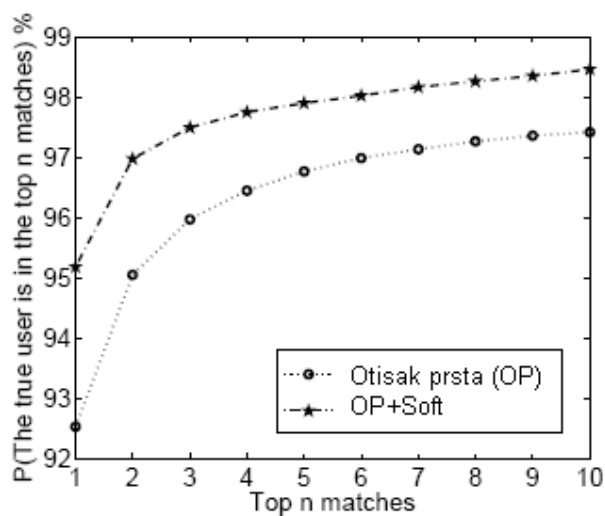
Kod sistema za prepoznavanje lica, upotrebom crta lica i otiska, poboljšanje GAR-a je oko 2% pri FAR = 0.001% (slike 73 i 74). Ova promena je od značaja ako uzmemo da je u ovom režimu vrednost GAR-a visoka sama po sebi.



(a)

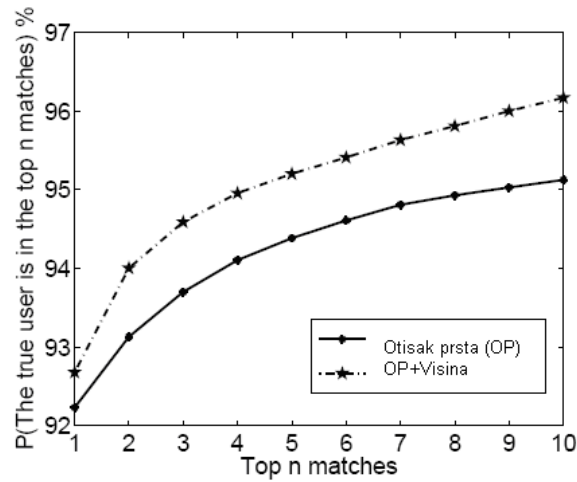


(b)

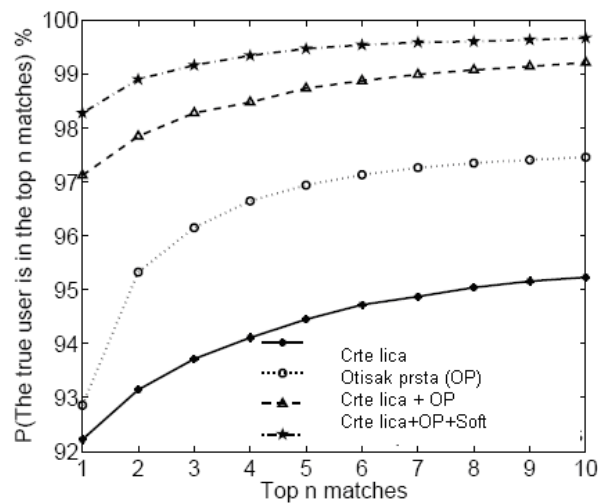


(c)

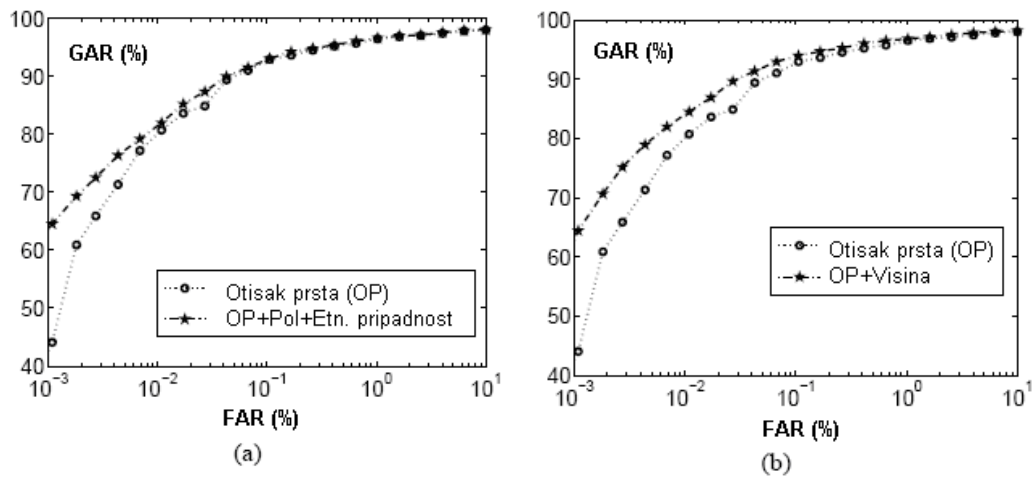
Slika 69: Poboljšanje identif. performansi sistema za prepoznavanje otisaka prstiju uz upotrebu soft osobina. a) Sa polom i etn. Pripadnošću, b) Sa visinom i c) Sa polom, etn. Pripadnošću i visinom

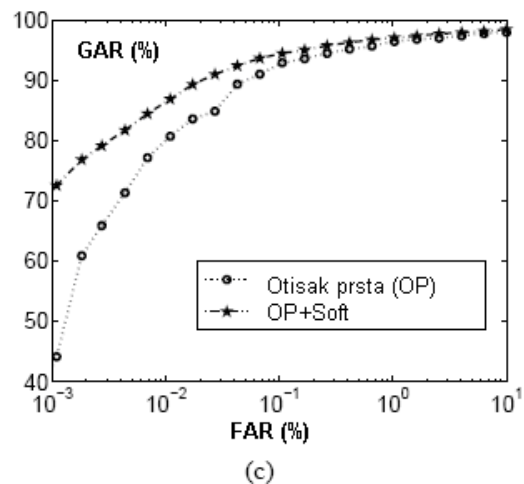


Slika 70: Poboljšanje identif. performansi sistema za prepoznavanje crta lica uz upotrebu podatka o visini korisnika

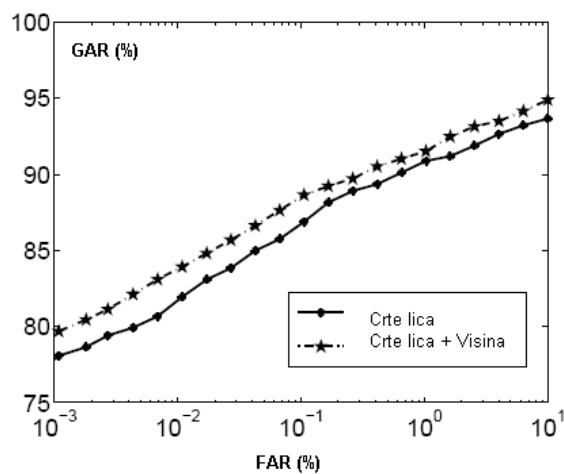


Slika 71: Poboljšanje identif. performansi multimodalnog sistema (otisci prstiju i crte lica) uz upotrebu soft osobina.

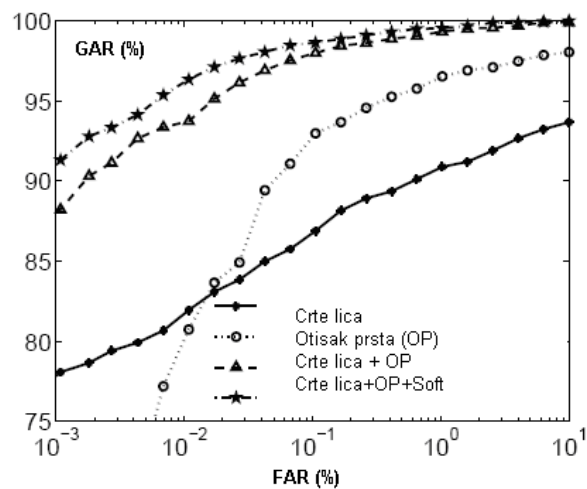




Slika 72: Poboljšanje identif. performansi sistema za prepoznavanje otisaka prstiju uz upotrebu soft osobina. a) Sa polom i etn. pripadnošću, b) Sa visinom i c) Sa polom, etn. pripadnošću i visinom



Slika 73: Poboljšanje identif. performansi sistema za prepoznavanje crta lica uz upotrebu podatka o visini korisnika



Slika 74: Poboljšanje identif. performansi multimodalnog sistema (otisci prstiju i crte lica) uz upotrebu soft osobina.

8.5 Zaključak

Cilj prethodne teme je bio da dokazivanje da upotreba *soft* biometrijskih identifikatora kao što su pol, etnička pripadnost i visina mogu biti korisni kod prepoznavanja osoba čak i ako nema 100%-ne garancije po pitanju tačnosti dobijenih rezultata. Da bi se zaokružila priča, eksperimentalno je razvijeno Bajesovo okruženje²¹ koje kombinuje informacije primarnih i *soft* identifikatora u cilju postizanja većeg nivoa sigurnosti u postupku određivanja korisnikovog identiteta.

Eksperimenti su pokazali da *soft* biometrijska osobina može biti od pomoći ako je komplementaran primarnom biometrijskoj osobini. Takođe je prikazan i razvoj tehnika za automatsko izdvajanje *soft* biometrijskih podataka.

²¹ Bajesovo okruženje formalizuje dizajn ličnog identifikacionog sistema koji može prilagodljivo povišiti odnosno, sniziti sigurnosni nivo u skladu sa potrebama fizičkih karakteristika korisnika.

9. Zaključak

Iako biometrija postaje sastavni deo sistema za upravljanje identitetima, za sada, ipak ne obezbeđuje 100% tačnost. Faktori koji utiču na to su spoljni uticaji, neuniverzalnost, nesvojstvenost i nedostatak dovoljno nepromenljivih informacija. Biometrijski sistemi su takođe osetljivi i na napade spolja. Sistem koji integriše višestruku zaštitu može prevazići neke od prethodno pomenutih poteškoća i proizvesti bolje performanse.

Ovo obimno istraživanje izvedeno je u cilju pronalaženja što boljeg metoda za kombinaciju informacija dobijenih iz različitih izvora. Teža opcija, koja je često i nemoguća, je sjedinjavanje podataka na početnim nivoima tj. nivoima senzora i izdvajanja podataka. Nivo odlučivanja je takođe nepraktičan zbog manjka potrebnih informacija. Iz tih razloga se sjedinjavanje najčešće vrši na nivou poređenja što ujedno predstavlja i najbolji kompromis između, sa jedne strane, količine i dostupnosti informacija i, sa druge strane, jednostavnosti postupka sjedinjavanja.

Problem koji se može javiti na nivou rezultata je nekompatibilnost modula poređenja. Rezultati mogu biti različitog karaktera pa su nužne određene korekcije upotrebom neke od normalizacionih tehnika. Drugi problem je nemogućnost upravljanja *soft* biometrijskim informacijama, naročito kad nisu dovoljno pouzdane. U tezi su sistematično obrađena ova dva osnovna problema.

Takođe, razmotrena je detaljna evaluacija različitih normalizacionih tehnika u pogledu njihovih efikasnosti i robustnosti. Za početak, razmotren je uticaj različitih normalizacionih tehnika na performanse multimodalnog biometrijskog sistema (crte lica, otisak prsta i geometrija dlana). Istraživanja su pokazala da najbolje rezultate pružaju *Z-rezultat*, *Min-max* i *Tanh* normalizacione tehnike, pri čemu, *Z-rezultat* i *Min-max* nisu dovoljno robustne ako podaci za dobijanje normalizacionih parametara sadrže netipične vrednosti. Za razliku od njih, *Tanh* tehnika je daleko robustnija zahvaljujući funkciji uticaja koja smanjuje efekat „šuma“. Međutim, za efikasnost tehnike potreban je brižljiv izbor parametara. S druge strane, neparametarska procena gustine, koja je teorijski dobar metod, u praksi se nije pokazao kao dobro rešenje iz razloga ograničene dostupnosti rezultata (za proveru) i problema sa izborom odgovarajućeg jezgra.

Jedan od značajnijih doprinosa teze je razvoj sistema koji koristi tzv. *soft* biometrijske informacije koje imaju za cilj povećanje opšteg nivoa sigurnosti i performansi klasičnih biometrijskih sistema. Ove informacije, iako same po sebi nisu dovoljne, kao dodatak osnovnim biometrijskim informacijama, obezbeđuju viši nivo određivanja identiteta korisnika. Takođe, kao primer, razvijen je i model zasnovan na Bajesovoj teoriji odlučivanja koji je moguće integrisati u klasičan biometrijski sistem. Eksperimenti, većim delom izvedeni u PRIP laboratoriji državnog univerziteta u Mičigenu, izvedeni od strane Karthik Nandakumara, studenta postdiplomskih studija, na razumnoj količini podataka potvrdili su korisnost *soft* biometrijskih identifikatora.

10. Budući rad

Budući rad zasnivaće se na istraživanju novih i efikasnijih multimodalnih biometrijskih sistema i normalizacionih šema kao i rešavanju određenih problema kod *soft* biometrijske autentifikacije.

Neke od normalizacionih šema funkcionišu isključivo za određene distribucije rezultata (*Z-rezultat* šema pri Gausovoj distribuciji) pa bi bilo poželjno razviti pravila koja će svakom praktičaru, nakon analize distribucija rezultata originalnog i lažnog korisnika, omogućiti izbor odgovarajuće normalizacione šeme prema rezultatima analize. Isto tako, bilo bi dobro istražiti mogućnost upotrebe različitih normalizacionih tehnika za rezultate različitih modaliteta kao i napraviti uputstva za izbor normalizacionih parametara.

Za postojeće tehnike sjedinjavanja na nivou rezultata može se reći da ne deluju dovoljno „matematički čvrsto“ te je verovatno bolji pristup izračunavanja odnosa verovatnoće na osnovu procena distribucija rezultata oba tipa korisnika.

Kako se može primetiti, za većinu nepreciznosti koje su dobijene istraživanjem i efikasnost sistema krivicu snosi nedovoljan broj biometrijskih podataka. Odnosno, za povećanje efikasnosti sistema, potreban je veći broj rezultata poređenja šablona.

Kad se govori o *soft* biometriji, za neki ozbiljniji rad potrebno je koristiti daleko preciznije mehanizme prikupljanja podataka nego što je to učinjeno u opisanom eksperimentu. Isto tako, metod iscrpne pretrage za težinskim koeficijentima je računski neefikasan i zahteva više „radnih podataka“. Kako se isti ti koeficijenti koriste pre svega za redukovanje opsega logaritamskih vrednosti verovatnoće, moguće je razviti jednostavniji sistem za efikasno izračunavanje težinskih faktora.

Bajesovo okruženje, pomenuto na kraju teze, trenutno ne može da podrži vremenski promenljive *soft* podatke, kao što su starost ili visina tako da neko dalje istraživanje može ići u pravcu pronalaženja rešenja ovog problema.

11. Literatura

- [1]. NIST report to the United States Congress. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability. Available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf, November 2002.
- [2]. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2004: Third Fingerprint Verification Competition. In *Proceedings of International Conference on Biometric Authentication*, pages 1–7, Hong Kong, China, July 2004.
- [3]. C. Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. NIST Internal Report 7123; available at http://fpvte.nist.gov/report/ir_7123_summary.pdf, June 2004.
- [4]. P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. FRVT2002: Overview and Summary. Available at <http://www.frvt.org/FRVT2002/documents.htm>.
- [5]. D. A. Reynolds, W. Campbell, T. Gleason, C. Quillen, D. Sturim, P. Torres-Carrasquillo, and A. Adami. The 2004 MIT Lincoln Laboratory Speaker Recognition System. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, PA, March 2005.
- [6]. A. Ross and A. K. Jain. Information Fusion in Biometrics. *Pattern Recognition Letters, Special Issue on Multimodal Biometrics*, 24(13):2115–2125, 2003.
- [7]. L. Hong and A. K. Jain. Integrating Faces and Fingerprints for Personal Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(12):1295–1307, December 1998.
- [8]. R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. K. Jain. Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3):450–455, March 2005.
- [9]. A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain. Personal Verification Using Palmprint and Hand Geometry Biometric. In *Proceedings of Fourth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 668–678, Guildford, U.K., June 2003.
- [10]. A. Ross and R. Govindarajan. Feature Level Fusion Using Hand and Face Biometrics. In *Proceedings of SPIE Conference on Biometric Technology for Human Identification*, volume 5779, pages 196–204, Florida, U.S.A., March 2005.
- [11]. [25] R. O. Duda, P. E. Hart, and D. G. Stork. *Pattern Classification*. John Wiley & Sons, 2001.
- [12]. L. Lam and C. Y. Suen. Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 27(5):553–568, 1997.
- [13]. L. Xu, A. Krzyzak, and C. Y. Suen. Methods for Combining Multiple Classifiers and their Applications to Handwriting Recognition. *IEEE Transactions on Systems, Man, and Cybernetics*, 22(3):418–435, 1992.
- [14]. J. Daugman. Combining Multiple Biometrics. Available at <http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html>.
- [15]. T. K. Ho, J. J. Hull, and S. N. Srihari. Decision Combination in Multiple Classifier Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 16(1):66–75, January 1994.
- [16]. Y. Wang, T. Tan, and A. K. Jain. Combining Face and Iris Biometrics for Identity Verification. In *Proceedings of Fourth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 805–813, Guildford, U.K., June 2003.
- [17]. P. Verlinde and G. Cholet. Comparing Decision Fusion Paradigms using k-NN based Classifiers, Decision Trees and Logistic Regression in a Multi-modal Identity Verification Application. In

- Proceedings of Second International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 188–193, Washington D.C., U.S.A., March 1999.
- [18]. V. Chatzis, A. G. Bors, and I. Pitas. Multimodal Decision-level Fusion for Person Authentication. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 29(6):674–681, November 1999.
 - [19]. J. Kittler, M. Hatef, R. P. Duin, and J. G. Matas. On Combining Classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3):226–239, March 1998.
 - [20]. S. Prabhakar and A. K. Jain. Decision-level Fusion in Fingerprint Verification. *Pattern Recognition*, 35(4):861–874, 2002.
 - [21]. [39] A. K. Jain and A. Ross. Learning User-specific Parameters in a Multibiometric System. In *Proceedings of International Conference on Image Processing*, pages 57–60, New York, USA, September 2002.
 - [22]. P. Verlinde, P. Druyts, G. Cholet, and M. Acheroy. Applying Bayes based Classifiers for Decision Fusion in a Multi-modal Identity Verification System. In *Proceedings of International Symposium on Pattern Recognition “In Memoriam Pierre Devijver”*, Brussels, Belgium, February 1999.
 - [23]. R. Snelick, M. Indovina, J. Yen, and A. Mink. Multimodal Biometrics: Issues in Design and Testing. In *Proceedings of Fifth International Conference on Multimodal Interfaces*, pages 68–72, Vancouver, Canada, November 2003.
 - [24]. R. Brunelli and D. Falavigna. Person Identification Using Multiple Cues. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12(10):955–966, October 1995.
 - [25]. P. J. Huber. *Robust Statistics*. John Wiley & Sons, 1981.
 - [26]. R. Cappelli, D. Maio, and D. Maltoni. Combining Fingerprint Classifiers. In *Proceedings of First International Workshop on Multiple Classifier Systems*, pages 351–361, June 2000.
 - [27]. F. Mosteller and J. W. Tukey. *Data Analysis and Regression: A Second Course in Statistics*. Addison-Wesley, 1977.
 - [28]. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. An Identity Authentication System Using Fingerprints. *Proceedings of the IEEE*, 85(9):1365–1388, 1997.
 - [29]. M. Turk and A. Pentland. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.
 - [30]. A. K. Jain, A. Ross, and S. Pankanti. A Prototype Hand Geometry-based Verification System. In *Proceedings of Second International Conference on Audio- and Videobased Biometric Person Authentication (AVBPA)*, pages 166–171, Washington D.C., USA, March 1999.
 - [31]. D. D. Heckathorn, R. S. Broadhead, and B. Sergeyev. A Methodology for Reducing Respondent Duplication and Impersonation in Samples of Hidden Populations. In *Annual Meeting of the American Sociological Association*, Toronto, Canada, August 1997.
 - [32]. H. Aillisto, M. Lindholm, S. M. Makela, and E. Vildjiounaite. Unobtrusive User Identification with Light Biometrics. In *Proceedings of the Third Nordic Conference on Human-Computer Interaction*, pages 327–330, Tampere, Finland, October 2004.
 - [33]. J. L. Wayman. Large-scale Civilian Biometric Systems - Issues and Feasibility. In *Proceedings of Card Tech / Secur Tech ID*, 1997.
 - [34]. E. Newham. The Biometrics Report. SJB Services, 1995.
 - [35]. S. Gutta, J. R. J. Huang, P. Jonathon, and H. Wechsler. Mixture of Experts for Classification of Gender, Ethnic Origin, and Pose of Human Faces. *IEEE Transactions on Neural Networks*, 11(4):948–960, July 2000.
 - [36]. B. Moghaddam and M. H. Yang. Learning Gender with Support Faces. *IEEE Transaction, on Pattern Analysis and Machine Intelligence*, 24(5):707–711, May 2002.
 - [37]. G. Shakhnarovich, P. Viola, and B Moghaddam. A Unified Learning Framework for Real Time Face Detection and Classification. In *Proceedings of International Conference on Automatic Face and Gesture Recognition*, Washington D.C., USA, May 2002.

- [38]. K. Balci and V. Atalay. PCA for Gender Estimation: Which Eigenvectors Contribute? In *Proceedings of Sixteenth International Conference on Pattern Recognition*, volume 3, pages 363–366, Quebec City, Canada, August 2002.
- [39]. X. Lu and A. K. Jain. Ethnicity Identification from Face Images. In *Proceedings of SPIE Conference on Biometric Technology for Human Identification*, volume 5404, pages 114–123, April 2004.
- [40]. J. Hayashi, M. Yasumoto, H. Ito, and H. Koshimizu. Age and Gender Estimation based on Wrinkle Texture and Color of Facial Images. In *Proceedings of the Sixteenth International Conference on Pattern Recognition*, pages 405–408, Quebec City, Canada, August 2002.
- [41]. M. V. Buchanan, K. Asano, and A. Bohanon. Chemical Characterization of Fingerprints from Adults and Children. In *Proceedings of SPIE Photonics East Conference*, volume 2941, pages 89–95, November 1996.
- [42]. Y. H. Kwon and N. V. Lobo. Age Classification from Facial Images. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, pages 762–767, April 1994.
- [43]. A. Lanitis, C. Draganova, and C. Christodoulou. Comparing Different Classifiers for Automatic Age Estimation. *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, 34(1):621–628, February 2004.
- [44]. N. Minematsu, K. Yamauchi, and K. Hirose. Automatic Estimation of Perceptual Age using Speaker Modeling Techniques. In *Proceedings of the Eighth European Conference on Speech Communication and Technology*, pages 3005–3008, Geneva, Switzerland, September 2003.
- [45]. J. S. Kim et al. Object Extraction for Superimposition and Height Measurement. In *Proceedings of Eighth Korea-Japan Joint Workshop on Frontiers of Computer Vision*, January 2002.
- [46]. A. K. Jain, K. Nandakumar, X. Lu, and U. Park. Integrating Faces, Fingerprints and Soft Biometric Traits for User Recognition. In *Proceedings of Biometric Authentication Workshop, LNCS 3087*, pages 259–269, Prague, Czech Republic, May 2004.
- [47]. S. C. Dass, K. Nandakumar, and A. K. Jain. A Principled Approach to Score Level Fusion in Multimodal Biometric Systems. In *Proceedings of Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA) (To appear)*, New York, U.S.A., July 2005.
- [48]. <http://www.biometrics.org>
- [49]. <http://www.biometricgroup.com>
- [50]. <http://fingerprint.nist.gov>
- [51]. <http://www.fingerprints.com>
- [52]. <http://www.precisebiometrics.com>
- [53]. <http://www.biometricwatch.com>
- [54]. <http://whitepapers.techrepublic.com.com>
- [55]. http://research.microsoft.com/aboutmsr/presskit/Biometric_ID_Cards.aspx
- [56]. <http://www.sk.co.yu/2005/03/skpr02.html>
- [57]. L. Hong, A. Jain, S. Pankanti. Can Multibiometrics Improve Performance ?.
- [58]. John Dougman's web site <http://www.cl.cam.ac.uk/~jgd1000/>
- [59]. A. Ross. Multibiometrics-Part 2, *Lecture on 3/17/2005*, West Virginia University, Morgantown, 2005
- [60]. <http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/biometric.html#mozTocId579434>
- [61]. M. Pettersson, M. Obrink. How secure is your biometric solution ? *Precise Biometrics White Paper*, Lund, Sweden, February 2002.
- [62]. A. Jain and A. Ross. Multibiometric systems. *Communication of the ACM*. Vol 47, No 1, January 2004.
- [63]. H. Gravnas. User's trust in biometric Authentication Systems, *Master's thesis*, Gjøvik University College, Norway, 2005.
- [64]. www.vidovdan.org

- [65]. R.Volner, P.Boreš. Multi-Biometrics Techniques, Standards Activities and Experimenting, *Electronics and Electrical Engineering No 8.*, Czech Technical University in Prague, 2006.
- [66]. U.M.Bubeck. Multibiometric Authentication, *Term Project CS 574*, San Diego State University, 2003.
- [67]. Ad Hoc Group on Biometric in E-Authentication (AHGBEA). Study Report on Biometric in E-Authentication, *INCITS M1/06-0112*, INCITIS and ITI, Washington, USA, February, 2006.
- [68]. M.Kakona. Drawbacks of Biometric Methods, 2001.
- [69]. California Software Labs, Biometric Authentication System-an Overview Whitepaper, <http://www.cswl.com/whitepapers/biometrics-technologies.html#01>, October, 2004.
- [70]. L.Sumner, Citibank debuts biometric pay system, *IDG News Service, InfoWorld*, http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/06/11/21/HNcitiban_kbiometrics_1.html, November, 2006.
- [71]. <http://www.answers.com/biometrics%20passport>
- [72]. <http://www.0-apr-creditcards.com/blog/biometric-credit-card-citibank-1st-to-offer-it.html>
- [73]. <http://www.itl.nist.gov/div898/handbook/eda/section3/eda364.htm>
- [74]. <http://en.wikipedia.org>