



Департман за последипломске студије
САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

МАСТЕР СТУДИЈЕ
- Мастер теза-

САВРЕМЕНИ ТРЕНДОВИ У МУЛТИМОДАЛНОЈ
БИОМЕТРИЈИ

Ментор
Проф. Др. Младен Веиновић

Кандидат
Радован Скенцић 410057/09



1.	Увод	1
2.	Историјат.....	2
2.1.	XIV Век Кина	2
2.2.	XIX Век Француска – Развој Антопометрије.....	2
2.3.	Касни XIX Век : Узимање отисака почиње	3
2.4.	Касни XX Век : Аутоматизоване биометричке технике	3
3.	Идентификација и аутентификација	4
3.1.	Идентификација	4
3.2.	Био-идентификатори могу бити подељени у три категорије:.....	4
3.3.	Идентификација биометријом	5
3.4.	Аутентификација.....	6
3.5.	Степен грешке биометријских техника	7
4.	Биометријске технике	8
4.1.	Отисци прстију (Fingerprinting).....	8
4.2.	Глас	9
4.3.	Лице	9
4.4.	Ирис.....	10
5.	Биометријски системи у употреби	12
5.1.	Биометријско надгледање	14
5.2.	Препреке за увођење биометријских система.....	15
5.3.	Предности и мане великог биометријског система.....	16
5.4.	Централизована база података.....	16
6.	Биометријска безбедност оперативних система.....	17
6.1.	Пријављивање на оперативни систем („Winlogon“)	18
6.2.	Закључавање десктопа (“Desktop lockdown“)	18
6.3.	ГИНА	20
7.	Биометријски кључеви са довољном дужином за сигурне апликације: будуће могућности.....	21
8.	Могућности апликација.....	22
8.1.	Биометријске базе података.....	22
8.2.	Биометријска аутентикација у вези са банкоматима (АТМ)	22
9.	Биометријске исправе	26
9.1.	Биометријске личне карте.....	26
9.2.	Биометријски пасоши	28
10.	Мултимодална биометрија	31
11.	Нивои стапања	34
12.	Сценарији стапања.....	36
13.	Начини рада.....	38
14.	Смернице за постављање система.....	39
15.	Дизајн	40
16.	Закључак.....	41
17.	Литература	42



Сажетак

Познато је да су одређене особине људског тела (ДНК, отисак прста, ирис и сл.) уникатни за сваку особу. Биометрија као наука се бави употребом биолошких карактеристика или особина са циљем провере идентитета особе. Да ли заиста можемо биометријске податке назвати сигурнијом заштитом од обичних лозинки? Да ли су права замена?

Унимодални биометријски системи морају да се боре са мноштвом разноврсних проблема као што су нечисти подаци, варијације шаблона, ограничени нивои слободе, немогућност универзалне применљивости, прикривених напада и неприхватљивих нивоа грешака. Наведена ограничења се могу решити мултимодалним биометријским системима јер прикупљају информације са различитих извора. Покушаћемо да објаснимо неколико могућих ситуација у којима се систем може наћи, нивое стапања који су могући и стратегије за постављање система који би могао да сабере све информације.

Рад представља хронолошки преглед биометријских технологија и њихов развој до савремених трендова у мултимодалној биометрији. За циљ има утврђивање одговора на питања у вези са идентификацијом и верификацијом идентитета биометријом.

Abstract:

It's well known that certain traits of human body (such as DNA, fingerprint, iris, etc) are unique for each individual. Biometry as science is dealing with usage of biometric characteristics or traits in purpose of checking individual's identity. Can we really name biometric data as more secure protection than regular passwords? Are they real substitution?

Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information. The various scenarios that are possible in multimodal biometric systems, the levels of fusion that are plausible and the integration strategies that can be adopted to consolidate information are discussed in this paper.

This paper represents chronological review of biometric technologies and their development to modern trends in multimodal biometry. Its aimed on determining the answers to questions regarding the identification and biometric verification of identity.



1. Увод

Биометрија се једноставно дефинише као аутоматско препознавање особе користећи јединствене одлике. Биометричка идентификација користи неке уникатне психолошке карактеристике и карактеристике понашања, које су недељиве са другим појединцима, ради поузданог идентификовања индивидуе. Те особине су тада забележене као скуп функција минуте или "ситнице". Те особине су похрањене у одређеном уређају путем физичког контакта метода и / или електромагнетског скенирања ока (Ириса) или фидерпринтингом (узимање отиска).

Многе компаније купују такву опрему да би је применили у њиховом свакодневном пословању. Задатак који је пред нама сад, је да поверене биометријске податке и сачувамо од нежељених упада и евентуалне крађе, јер једном изгубљен биометријски податак не може да се додели поново попут шифре. Он је уникатан за сваку особу и представља ненадокнадив губитак.

У овом мастер раду под називом анализира се развитак биометрије као науке све до данашњих биометријских система. Представља упоређивање унимодалних са системима који користе мултимодалну биометрију.

Унимодални биометријски системи морају да се боре са мноштвом разноврсних проблема као што су нечисти подаци, варијације шаблона, ограничени нивоии слободе, немогућност универзалне применљивости, прикривених напада и неприхватљивих нивоа грешака. Наведена ограничења се могу решити мултимодалним биометријским системима јер прикупљају информације са различитих извора.

Први део рада бави се историјатом биометрије, појашњавањем појмова идентификације и аутентификације.

Други део рада ближе објашњава биометријске технике које су у употреби (отисак прста, глас, ирис итд.) и системе у којима се они употребљавају.

У трећем делу описани су трендови употребе унимодалних биометријских система у оперативним системима, банкоматима и биометријским исправама.

Последњи део рада се бави мултимодалном биометријом. Мултимодална биометрија подразумева комбиновање свих претходно наведених биометријских техника. У пракси се користе у граничним прелазима за контролу уласка или изласка, за контролу приступа неком простору, цивилној идентификацији, мрежној безбедности.



2. Историјат

“Кад би МекДоналдс понудио Биг Мек у замену за узорак ДНК, редови би се пружали неколико блокова” –Брус Шнејер (Bruce Schneier), амерички криптограф, писац и специјалиста за компјутерску заштиту.

Биометрија (грч. *биос* - живот, *метрон* - мера) представља скуп аутоматизованих метода за јединствено препознавање људи базирано на једној или већем броју њихових физичких и понашајних карактеристика. Иако се биометрија првенствено користи за потребе аутентификације, иста се примењује и у другим областима као што је препознавање гласа корисника у сврху бржег писања.

У 21. веку, готово интуитивно је размишљати, да су наша тела природни индентификациони системи специфичности нас самих. Идеја да су наша тела, очи, лица и прсти идентификатори, развила се током времена радом много људи.

2.1. XIV Век Кина

По једном од извора зачеци биометрије воде у Кину, у 14. век, где су трговци користили дечије дланове и отиске ногу, како би их међусобно разликовали.

2.2. XIX Век Француска – Развој Антропометрије



Други повезују почетке биометрије са Алфонсом Бертиљоном (Alphonse Bertillon). Он је био припадник полиције који је радио као чиновник у родном Паризу, кад је измислио антропометрију у смирају 19. века: употреба мера тела да се идентификују криминалци. Бертиљонов систем је такође укључивао бележење покрета осумњичених и обележја на њиховом телу као што су тетоваже и израслине на кожи. Британска и Америчка полиција је прихватила овај систем који је назван Бертиљинаж (Bertillonage), да би сузили број осумњичених које су тражили. Ипак, мерења нису могла да се направе прецизно, те су различити позорници увек мерили благо другачије (па чак би и иста особа мерила другачије у различитим навратима).

Слика 1: Антропометрија



2.3. Касни XIX Век : Узимање отисака почиње

Слика 2: Отисак прста



Постоји много корака у историји узимања отисака као начина за идентификацију криминалаца. Бертиљон је укључио узимање отисака у његов систем, али не као важан елемент. Аргентински полицијски званичник је био први који је почео да чува документа са отисцима прстију. Класификовао је отиске по систему који је установио Сер Френсис Галтон (Sir Francis Galton), антрополог у сродству са Чарлсом Дарвином. Галтон је касније објавио књигу “Отисци” („Fingerprints”) која је садржала класификациони систем. Његово откриће да не постоје две особе које деле исти отисак прста и његова класификација детаља особног отиска прста се махом користи и данас. До 1920-их, идентификација помоћу отиска је коришћена у америчкој војсци и у ФБИ као начин идентификације.

2.4. Касни XX Век : Аутоматизоване биометричке технике

Иако се узимање отисака и даље користи, компјутерске технике су почеле убрзан развој у задњој четвртини 20-ог века. Ове технике стреме ка мерењу наших руку, прстију, ириса, лица и гласа. Кад су идеје предложене, развој је нагло убрзан. На пример, 1985. идеја да је Ирис јединствен је предложена, развој система идентификације је почео 1993, 1994. је први алгоритам за препознавање патентиран, а годину дана после тога комерцијални производи за мерење ириса су постали доступни. Скенери ириса су већ тестирани као додаци у безбедносном споју у великом броју земаља, као и на комерцијалном тржишту.



Слика 3: Однос биометријских техника у пракси



3. Идентификација и аутентификација

С обзиром да људско друштво стреми ка аутоматизацији послова, јер се аутоматизацијом посао убрзава и смањује се могућност грешке, у овом раду ће бити више речи о аутоматизованим биометријским системима који прикупљене биометријске податке смештају у електронској форми, у одређену базу података.

Могућности нових технологија могу бити максимално искоришћене даљим усавршавањем рачунарских система. То ипак отвара даља питања колико је развитак технологија заиста добронамеран, а колико владе будућности у ствари желе тоталну контролу и један вид „Великог брата”.

Лично сматрам да је сваки напредак добар, и да заједно морамо подносити одређене жртве и уступке зарад бољитка живота свих нас.

3.1. Идентификација

Идентификација у ствари значи упоређивање постојећих података са непознатом особом која покушава да приступи систему (посматрано са гледишта које обрађујем у овом раду).

Биометрички апарати раде на принципу поклапања карактеристичних својстава са онима које су забележени у меморију одређеног апарата. Појединац обично има идентификациону картицу или ПИН број који се уноси и пореди се са биометричким својством које је забележено на уређају.

3.2. Био-идентификатори могу бити подељени у три категорије:



Идентификатори понашања – То су све активности које особа ради на начин који је доследан и учестао. Пример ових идентификатора су препознавање гласа, рукопис и динамика на тастатури.



Тополошки идентификатори – Психолошке карактеристике које остају непроменљиве кроз цео животни век. Пример су лице, геометрија руке и рукопис.



Дискретни идентификатори – Немају везе ни са понашањем ни са топологијом. Пример је очна јабучица.



3.3. Идентификација биометријом

У пракси она се постиже нечим што поседујемо (картица са чипом), нечим што знамо (шифра, пин код) и нечим што јесмо (отисак прста). У литератури све картице са чипом (лична карта, возачка дозвола, пасош, било у каквом да су облику) се називају токени.

Постоје две методе идентификације:

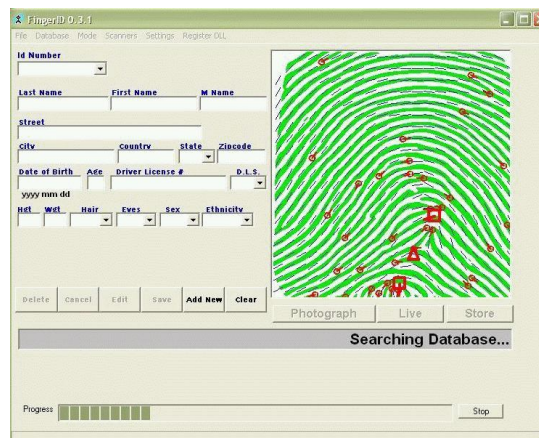
-  1 према Н (један према више) – Идентитет особе се утврђује претрагом по предефинисаној бази и поређењем са подацима прочитаним на апарату узетим од особе са лица места;
-  1 према 1 – Не постоји предефинисана база, већ се врши поређење података са картице и биометријског податка узетог на лицу места.

Дакле, у зависности од ова два модела, приликом провере идентитета (рецимо, узимањем отиска прста на скенеру) подаци се могу упоређивати:

- 1) пролазом кроз комплетну базу података чија величина зависи од броја корисника;
- 2) само са претходно унетим подацима за одређену особу који се налазе на токен-у (микроконтролери карте, рецимо);
- 3) комбинованим начином, уколико један од претходно наведених закаже из неког разлога.

Постоје два принципа идентификације: позитивна и негативна идентификација.

Код позитивне идентификације, циљ је потврдити да нека особа заиста јесте та за коју се представља, тј. да не постоје две особе са истим карактеристикама. Системи засновани на овом принципу најчешће користе 1 према 1 методу идентификације.



Слика 4: Негативна идентификација

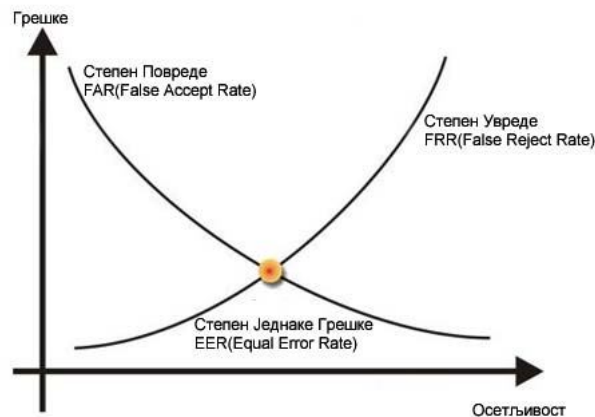
Код негативне идентификације, полази се од претпоставке да нека особа није та за коју се представља, тј. унети подаци са апарата се упоређују са подацима већ похрањеним у бази података. Овим се у ствари спречава могућност да једна особа има више уноса у базу података под различитим именом.



Биометрија је нешто „што ви јесте”, метод аутентификације или по Шнејеровим бесмртним речима „Ви сте Ваш кључ”.

3.4. Аутентификација

је поступак препознавања неке особе (или програма) који покушава да приступи систему. Биометрија је наравно подложна грешкама и оне се мере степеном повреде и степеном увреде.



Слика 5: Учинак биометријских показатеља

-  Степен повреде неког система се дефинише као могућност да нека особа буде аутентификована да приступи систему иако за то нема право (Систем препознаје особу Б као особу А);
-  Степен увреде неког система се дефинише као могућност да систем не препозна особу и одбије приступ, иако особа има право да приступи систему (Систем не препознаје особу А као особу А)

Нажалост савршен систем не постоји, јер су ова два степена међусобно повезани и обрнуто пропорционални што значи да се повећањем степена увреде смањује степен повреде и обратно. Зато је неопходно одредити златну средину према потребама система. Она се назива степен једнаке грешке. Што је она нижа систем се сматра прецизнијим.



Слика 6: Пример аутентификације отиском прста

3.5. *Степен грешке биометријских техника*

У делокругу биометричких система заснованих на отисцима прстију, степен једнаке грешке је око 5%, док геометрија руке има степен од 10^{-3} . Иако ово делује изненађујуће, већина справа за отиске прстују су прилично јефтине, као што је миш са отиском палца. С друге стране, биометричке направе за геометрију шаке су много скупљи и префињенији уређаји. Као последица свега тога биометрија отисака прстију вероватно неће бити ни близу правог потенцијала те технологије.

У теорији, читавање ириса има степен једнаке грешке од око 10^{-5} . Али у стварности је прилично тешко постићи такве резултате. Ситуација је таква, јер фаза узимања узорка мора да буде изузетно тачна у настојању да се постигну скоро-оптимални степени грешке. У пракси, људи задужени за узорковање (као и сама опрема) сигурно неће бити у лабораторији у савршеним условима где су теоретски резултати направљени.

У пракси, већина других биометријских метода су лошије од отисака прстију, и имају велике проблеме и слабе резултате на пољу идентификације.

Биометрија има велики потенцијал као замена за лозинке, али биометрија није нерањива. Узимајући то у обзир огромне проблеме са лозинкама и великим потенцијалом биометрије, изненађујуће је да биометрија већ није широко распрострањена и у употеби. Да би се то десило, биометрија мора да постане у будућности много поузданија и јефтинија.



4. Биометријске технике

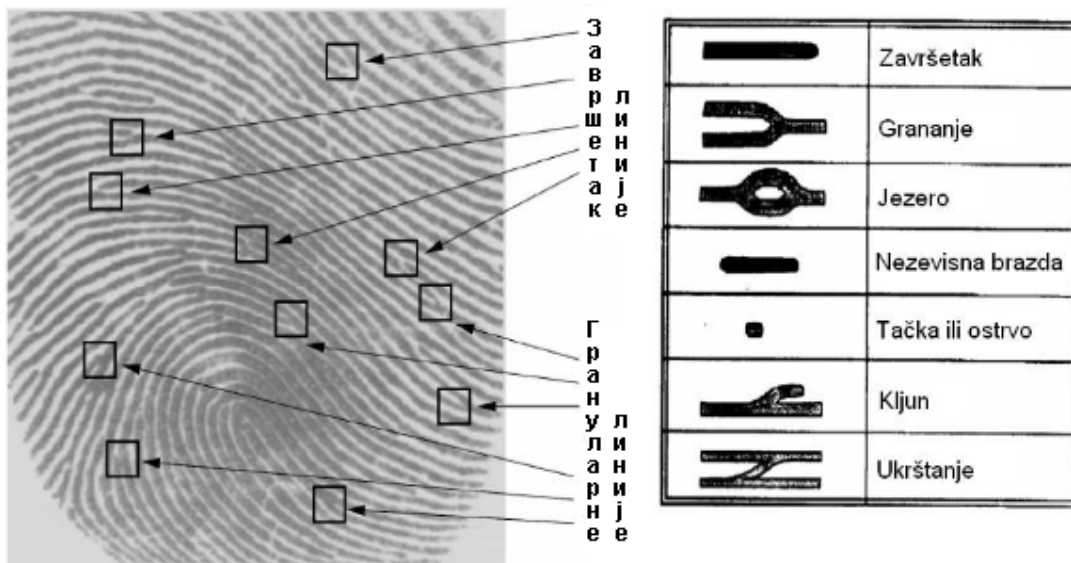
4.1. Отисци прстију (*Fingerprinting*)

Дактилоскопија је грана биометрије која се бави проучавањем отисака прстију. У употреби је од почетка двадесетог века због тога што су отисци прстију:

1. једнозначни (не постоје две особе, чак ни једнојајчани близанци, који имају једнаке отиске прстију);
2. временски непроменљиви;
3. потпуно неприкладни за кривотворење.

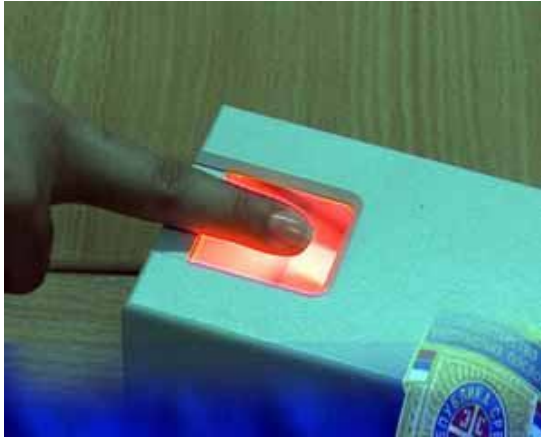
Пре готово 100 година, сер Едвард Хенри је приметио да се сви отисци прстију, без обзира колико различити међу собом они били, могу поделити у четири основне групе:

-  Лукови
-  Омче
-  Вијуге
-  комбинације претходне три



Слика 7: Карактеристични детаљи („Minutiae“)

Поступак идентификације се врши сврставањем у одређени тип отиска на основу локалних (деталјних) карактеристика. Потребно је не мање од 10 - 12 детаља за позитивну идентификацију. Док се раније прст умакао у маст приликом издавања личне карте, данас се то чини на много елегантнији начин, скенирањем вашег прста што даје дигиталну слику на рачунару, која се потом смешта на вашу нову биометријску исправу.

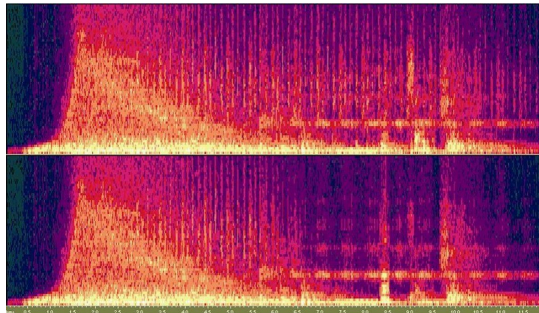


Слика 8: Скенирање прста приликом издавања биометријских докумената

4.2. Глас

Препознавање гласа бележи ритам, фреквенцију, висину и тоналитет гласа. За снимање гласа могуће је користити и обичан или телефонски микрофон, мада се поузданост скенирања повећава употребом квалитетнијих микрофона. Ово није нарочито поуздана метода, па се тако користи у верификационе, а не идентификационе сврхе. Време верификације је око пет секунди. Како би се избегао фалсификат коришћењем снимка, систем тражи истовремено и високе и ниске фреквенције звука јер је то у већини снимака немогуће репродуковати, тачније, оне се могу наћи само у правом гласу. Такође, неки системи генеришу насумичан низ бројева који особа треба да изговори.

Предност ове методе је што је потребна опрема изузетно јефтина и сваки данашњи компјутер, уз одговарајући софтвер, може да се искористи као платформа за препознавање гласа. Међутим, низак ниво поузданости препознавање гласа чини допунском методом уз неку другу, поузданију биометријску методу.



Слика 9: Поређење два записа звука и упоређивање гласа

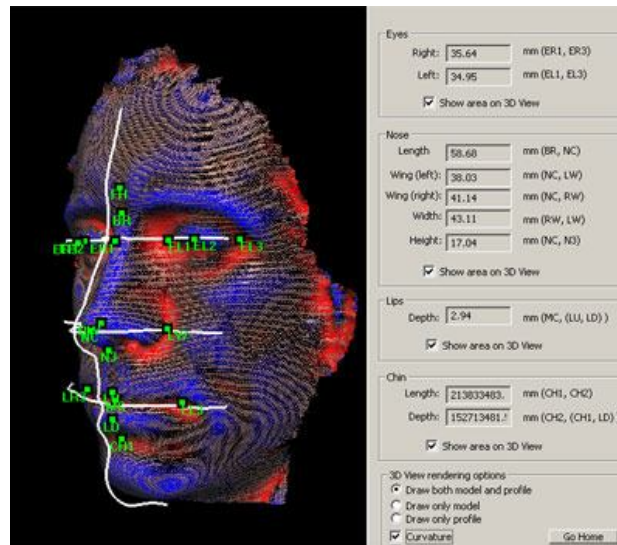
4.3. Лице

Донедавно су се за препознавање људског лица користили представници реда и закона који су у руци држали папир са фотографијом осумњиченог. Одскора то раде обичне телевизијске камере и софтвер. Предност овог начина идентификације је та што је, за разлику од старог, неупадљив, ефикаснији и теже га је преварити. Људско лице је у највећем броју случајева различито и представља



основни начин на који разликујемо и памтимо особе, али ми људско лице доживљавамо као целину. Приликом софтверског препознавања лица оно се разлаже на око 80 карактеристика, као што су, рецимо, растојање између очију, ширина и дужина носа, јагодице, брада, облик вилице итд.

Све те карактеристике се затим претварају у нумерички облик, а тај низ цифара се назива отисак лица. За успешно препознавање потребно је покlopити између 15 и 20 карактеристика, тако да се појединац може идентификовати чак и после извршене пластичне операције, а да не помињемо фарбање косе или употребу наочара за сунце.



Слика 10: Софтвер за препознавање лица

Највећу примену софтвер за препознавање лица налази у служби реда и закона, то јест за проналажење осумњичених у маси. Овај систем је први пут масовно употребљен у јануару 2000. на бејзбол утакмици у Флориди. Софтвер ФацеИт је пуштен пробно на годину дана у граду Тампа у Флориди, а на основу њега није извршено ниједно хапшење, иако је на поменутој утакмици идентификовано 19 особа са подебљим досијеима. Исти софтвер коришћен је у Мексику да би се избегли дупли гласови на председничким изборима.

Технологија препознавања лица изузетно је занимљива јер, слично отисцима прстију, постоје велике базе фотографија или се могу лако направити (слике за личне карте или возачке дозволе). Такође, процес идентификације је једноставан, а појединац чак није ни свестан да се врши одређивање његовог идентитета. Међутим, технологија препознавања лица још увек је у развоју и ослања се и даље у великој мери на људског оператера.

4.4. Ирис

Постоје две методе приликом одређивања идентитета помоћу ока - скенирање дужице (ириса) и скенирање мрежњаче (ретине) ока. Скенирање дужице се заснива на анализи појединости прстена у боји који окружује зеницу (ириса). На дужици постоји више од 200 тачака које се могу искористити за идентификацију, као што су прстени, бразде и пегице. Те шаре су јединствене за сваког појединца,



чак се лево и десно око исте особе разликују. Због тога се ова метода успешно може користити и за идентификацију, а не само за верификацију. За снимање дужице довољна је обична камера. Снимање се може обавити са извесне даљине (чак и до пола метра) и кроз наочаре. Да би се избегло коришћење вештачког ока, систем може да осветли око и да види да ли долази до скупљања зенице.

Предност ове методе је њена поузданост и релативна једноставност. Недостатак је то што је за скенирање ока главу потребно држати на тачно одређеном месту, што није нарочито zgodno ако неко то не жели да уради својевољно. Такође, базе скенираних дужица не постоје, већ би морале да се праве "од нуле".

Скенирање мрежњаче користи индивидуалност крвних судова на дну ока. Овај вид идентификације је најпоузданија од свих биометријских метода: пошто не постоји начин да се мрежњача фалсификује, она се не мења током целог живота особе, а мрежњача мртве особе толико брзо пропада да нису неопходне додатне мере утврђивања да ли је особа жива или не. За успешно скенирање је потребно скинути наочаре, око треба да је близу скенеру и неопходно је фокусирати се на одређену тачку. Процес скенирања траје између 10 и 15 секунди и за то време је око осветљено светлошћу слабог интензитета.

Јасно је да је ово компликованији и неугоднији начин утврђивања идентитета од свих раније поменутих. Због тога, а и због високе цене и поузданости, скенирање мрежњаче користи се само за инсталације високог нивоа безбедности, као што су војна постројења, банке или електране.



Слика 11: Скенирање Ириса



5. Биометријски системи у употреби

Зашто уопште уводити биометријске системе? Сваки биометријски систем има низ карактеристика које га чине бржим и поузданијим са развојем технологије због следећих параметара:

-  Универзалност - свака особа треба да има карактеристике;
-  Јединственост - је колико добро биометрија раздваја појединце међусобно;
-  Сталности - мери колико добро подаци биометрије одолевају старењу и променама током времена;
-  Доступност прикупљања - лакоћу прикупљања узорака за мерење.
-  Перформансе - тачност, брзина и робусност искоришћених технологија;
-  Прихватљивост - степен прихватљивости технологије;
-  Заобилажење - лакоћу употребе замена.

Биометријски систем може да ради на следећа два начина:

Верификација

Један на један поређење похрањених биометријских података са сачуваним узорцима да бисте потврдили да је појединац заиста онај који тврди да јесте. Може да се уради у споју са смарт картицама, корисничким именом или идентификационим бројем.

Идентификација

Представља поређење један према више, похрањених биометријских података непознатог појединца са сачуваним узорцима, у покушају да се појединац идентификује. Идентификација успева само у случају идентификације појединца, ако се поређење са уписаним податком у бази врши по претходно постављеном прагу осетљивости.

Прво коришћење биометријског система од стране корисника назива се уписивање. Током уписа, биометријске информације особе се похрањују у базу података. У наредним коришћењима, биометријске информације се тумаче и упореде са информацијама које су претходно похрањене. Да би биометријски систем био поуздан и сигуран, веома је важно да складиштење и преузимање информација буде заштићено.

Први блок (сензор) је интерфејс између реалног света и система. Он мора да прикупи све потребне податке. Најчешће је то систем прикупљања слика, али може да се промени у складу са жељеним карактеристикама.

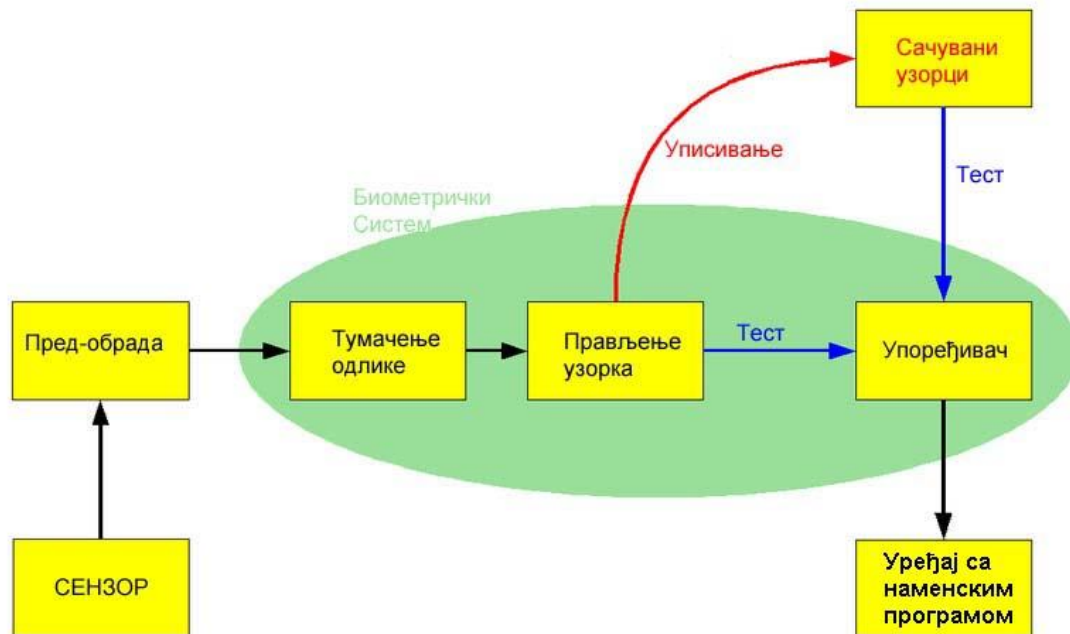
Други блок извршава све потребне пред-обrade: он узима узорак из сензора,



побољшава унос (нпр. уклањања спољашње сметње), врши нормализацију узорка, итд.

У трећем блоку врши се тумачење узорка. Овај корак је важан да би се узорци издвојили на оптималан начин. Вектор бројева или слика са одређеним својствима се користи за креирање шаблона узорка. Шаблон је синтеза релевантних карактеристика издвојених из извора. Елементи биометријских мерења који се не користе у односу на алгоритам се одбацују из шаблона да би се смањила величина датотеке и заштитио идентитет корисника који приступа систему.

Слика 12: Дијаграм биометријског система



Ако се врши упис узорак се једноставно похрањује и чува негде (на картици или у оквиру базе података, или на оба места). Уколико се врши фаза упоређивања прикупљени узорак се прослеђује упоређивачу да га пореди са постојећим узорцима, процењујући разлику између њих помоћу било ког алгоритма (нпр. Хамингова удаљеност). Програм ће анализирати узорак из базе са улазним узорком. То ће онда дати резултат за одређену намену или употребу (нпр. улаз у заштићено подручје).



5.1. Биометријско надгледање

Биометријско надгледање је у вези са технологијама које мере и анализирају људске физичке и / или карактеристике понашања за аутентификацију, идентификацију или у сврхе сортирања.



Слика 13: Отисци се скенирају приликом добијања визе за САД

Препознавање лица је употребљавање јединствених контура нечијег лица ради прецизне идентификације, најчешће са снимка надзорних камера. Америчке агенције за безбедност улажу велика средства у развитак система за препознавање лица. Покренут је програм Људска идентификација са даљине, до сада је развијена технологија која је способна да препозна особу на 150 метара по њиховим контурама лица.

Још један облик надгледања је могућност рачунара да препознају емоционално стање на основу анализе мимике лица, брзине којом причају, тоном и висином њиховог гласа, њиховим држањем и сл. Ова технологија се може искористити за предвиђање понашања сумњивих особа (осматрање кришом, напета и љута мимика лица, махање рукама итд.).

ФБИ тренутно улаже милијарду долара да направи нову биометричку базу података која ће имати похрањен ДНК, податке за препознавање лица, податке скенираног ириса, отиске прстију, отиске дланова и друге биометричке податке људи који живе у САД. Фарма рачунара на којој ће база бити смештена су у подземном постројењу величине фудбалског терена.

Термографи лица се тренутно развијају. Они ће омогућити уређајима да препознају одређене емоције код људи као што су страх или стрес, мерећи температуру коју ствара крвоток у различитим деловима лица.



5.2. Препреке за увођење биометријских система

„Овде је мудрост. Ко има ум нека израчуна број звери; јер је човеков број. А њен је број шест шездесет и шест." (Отк. 13:18)

Прву препреку можете лако наћи сами. Укуцајте у вашем омиљеном претраживачу: „жиг звери библија чип" наћи ћете прегршт сајтова и форума који расправљају о новим биометријским исправама.

„Библија прориче долазак једног моћног човека који ће господарити светом. У његовим рукама ће бити политичка, економска и религијска моћ. Сви народи ће га прихватити као „спаситеља" човечанства и сви ће му се клањати као некоме ко је виши од човека. Овај вођа ће увести посебан систем контроле својих поданика, нарочити жиг или печат који ће морати да прими сваки његов поданик - грађанин његовог царства.

Они који одбију да приме жиг биће прогањани као непријатељи новог система и убијани, или неће моћи да "купују и продају" - обављају трговину."¹

Будући да је религија велики део нашег живота и да свако има право на своје мишљење, окренућемо се ипак другим препрекама и потешкоћама за биометријске системе.

Један од најважнијих фактора за успех биометријских система је корисничко прихватање уређаја. Он не сме да проузрокује ни неудобност ни бригу за корисника. Ако се људи плаше да користе апарат, онда га вероватно неће правилно ни користити, што може довести да кориснику не буде одобрен приступ. Такође постоји велика бојазан од могућности крађе података или измене. Касније у раду биће речи и о једној од највећих бојазни – праћење путем исправа са чипом.

Биометријски уређај мора радити исправно. Када правилно функционише, то значи две ствари: да може да задржи неовлашћено лице, а омогући приступ овлашћеним лицима. Нажалост ниједан уређај није савршен.

Фрустрације које се могу појавити због великог броја одбачених, а овлашћених корисника, довешће до потраге за савршенијим системом уколико се ове мане не предвиде и отклоне унапред.

Иако Британци критикују амерички систем скенирања прста приликом уласка у земљу, доста Шпанаца подржава такав систем идентификације приликом уласка у воз уплашени недавним нападима терориста.

Истраживања такође показују да се младима од 20 до 30 година више допада узимање отиска прста, док је људима преко 40 година веродостојније скенирање ириса.

Обичним људима је у крви да се боје онога што не разумеју. Почевши од природних непогода које су објашњавали гневом богова па све до биометрије данас. Као и свака нова технологија и ова носи са собом одређене митове. Што више људи знају о биометрији, мање ће је се плашити и лакше ће је прихватити. У томе јој морају помоћи научници који ће тему демистификовати и приближити обичном човеку, да би је лакше разумео, а да се притом не изгуби у нејасним бројкама и компликованим речима.

¹ <http://siont.net/u-hristu/clanci/mark-beast.php> - Јан Варца



5.3. *Предности и мане великог биометријског система*

Идеја смештања свих биометријских података у једну велику базу омогућава брз приступ, велику доступност и прегледност огромне количине података. Документа више неће бити изгубљена у бескрајним орманима пуним папира које ће заузимати огроман простор, а потрага за правим подацима неће трајати недељама, већ ће зависити од брзине рачунара којим се приступа бази. Нажалост, од сигурности једног рачунара у том систему, зависи сигурност целог система, са непроцењивим подацима.

Ваша биометричка сигурност је ипак сигурнија у компјутерском систему. Ако погледамо у назад, ваш досије у полицији или било којој установи је била хрпа папира чија је сигурност зависила од неподмитљивости службеника и јачине катанаца на згради. Било који податак је могао без трага да нестане, а лоповима би тешко могло да се уђе у траг ако они то не желе (гомила докумената које су '90-их нестале у Србији су само један од примера). Мислим да је ипак много теже провалити у компјутерски систем непримећено, неголи раније изменити читав досије.

Ипак замене идентита и даље има и поред напредније технологије. Намерна или не то је ипак дискутабилно питање. Уколико би неко и успео да уђе у систем, сагласан сам да последице по особу у систему могу бити погубне. Биометрички подаци једном измерени, прате нас цео живот, те убацивање лажних података може некога ослободити кривице за неке злочине, а другу особу "сахранити". Биометрију је лако украсти и ван система, али је повезати са подацима унутар система ипак представља подухват, поготово ако су подаци унутар базе кодирани и у облику шаблона. То је само још један од начина (уз децентрализацију) додатне заштите ваших биометријских података.

Крађа идентита постоји и сад, постојаће и кад (ако) се уведу биометријски системи. Заједничким одрицањем одређених слобода, идемо ка даљем напретку друштва, које није стало ни у средњем веку када су научници спаљивани на ломачи, па ни сада уз сву неповерљивост према биометрији.

5.4. *Централизована база података*

Према ICAO (International Civil Aviation Organization) документима, државе унутар сопствених граница (за пасоше издате својим грађанима), треба да чувају биометријски узорак или узорке на путној исправи уз слику. На тај начин идентитет путника може бити верификован на локацијама где приступ централној бази података није доступан и у државама где је стално централизовано складиштење биометријских података незаконито. Неке државе су законски ограничене од узимања и чувања биометријских шаблона, и не постоји други избор осим коришћења слике и биометријског податка на исправи.



Централна база података је рањива са две стране:



Упадом у систем неауторизоване особе



Упадом у систем ауторизованог службеника ради малициозног мењања података

Иако би се компликованим алгоритмом, упад могао спречити, то не спречава корумпиране службенике да са кључевима дођу до одређених информација које су више него интересантне на тржишту криминалних организација. Стога и селекција радника мора да буде веома строга. Овај проблем се у литератури зове Хуверов проблем.

Друга слаба тачка централне базе је конекција између апарата за читавање биометријских података и саме базе, која може бити мета напада тројанцима па чак и могућност напада кроз саму апликацију.

Трећа ставка противника овог система почива на томе да се друштво са централном базом биометричких података приближава друштву из Орвелове "1984" у којој држава има потпуну контролу над животима својих житеља. Иако се на западу организације за људска права и информатичари упозоравају на овај проблем, источно-европске земље које су у комунизму већ имале централни регистар могу ово само видети као надоградњу постојећег система.

6. Биометријска безбедност оперативних система

За обезбеђивање био-сигурности за оперативне системе, потребно је проучити само пријављивање („logon“) на систем. Постоје 3 могућа начина за пријављивање на систем:

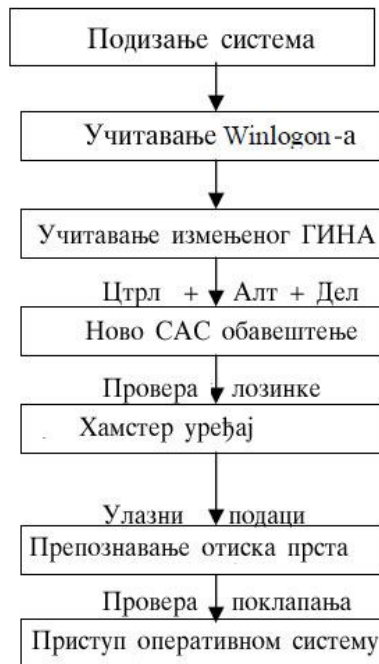
Систем се подиже → Пријављивање на оперативни систем („Winlogon“) → Покретање система

Систем се подиже → „Winlogon“ → „ГИНА“² → ЦАД (Ctrl+Alt+Del) → Покретање система

Систем се подиже → „Winlogon“ → Измењен „ГИНА“ → Био-омогућена сигурност → ЦАД → Покретање система

У последњем случају, корисник мора да угради нов фајл „MsGina.DLL“, који ће бити користан за интерактивно пријављивање са свим својим функцијама.

² ГИНА - Graphical Identification and Authentication component



Слика 14: Главни кораци биометријске безбедности

6.1. Пријављивање на оперативни систем („Winlogon”)

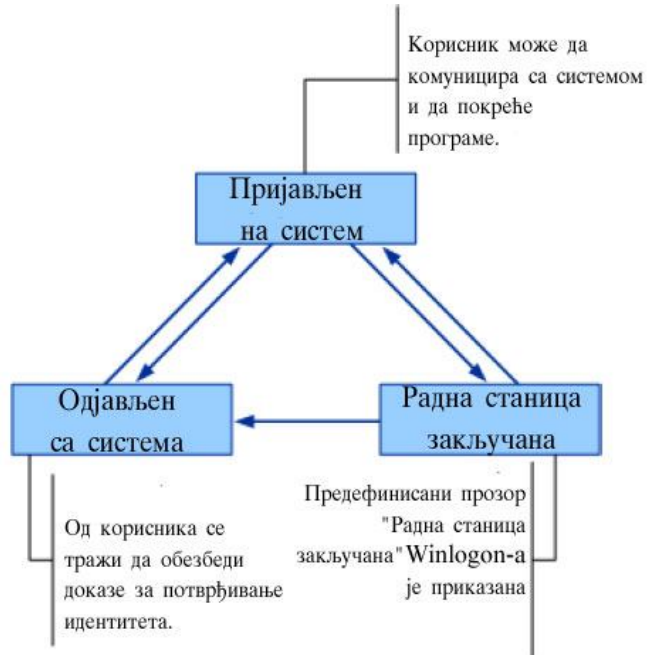
„Winlogon” (windir%\System32\Winlogon.exe) представља извршни фајл који је одговоран за управљање безбедних корисничких односа.

„Winlogon” покреће процес пријављивања за Windows Server 2003, Windows 2000, Windows XP, и Windows NT 4.0. Одговоран је за следеће задатке:

- ✚ Закључавање десктопа
- ✚ Стандардно САС препознавање
- ✚ САС рутину отправаљања
- ✚ Учитавање корисничког профила
- ✚ Контролу „Screen saver“-а
- ✚ Подршку за провајдера вишеструких мрежа

6.2. Закључавање десктопа (“Desktop lockdown”)

„Winlogon” помаже у спречавању неовлашћених корисника, да приступе ресурсима система, закључавањем радне површине рачунара. У било ком тренутку „Winlogon” је у једном од три могућа стања: пријављен, одјављен или закључана радна станица, као што је приказано на слици.



Слика 15: Стања „Winlogon”-а

„Winlogon” има три врсте радних површина: „Winlogon”, „Screen-saver“ и подразумевану – у зависности од његовог стања и активности корисника. Табела која следи представља листу ових радних површина са њиховим описима. „Winlogon” међусобно делује са „ГИНА“ током рада система.

Радна површина	Опис
„Winlogon”	Такође се назива “Сигурна радна површина”. Постоји пет предефинисаних прозора, који су приказани у следећој табели.
„Screen-saver“	У употреби док је покренут чувар екрана („Screen-saver“).
Подразумевана	Приказује се када је корисник успешно пријављен на систем и почиње комуникацију са оперативним системом. Сви програми раде на овој радној површини.

Табела 1: Радне површине „Winlogon”-а



<i>Радна површина</i>	<i>Опис</i>
Добродошли у Windows	Приказује се приликом почетног стартовања рачунара, док ниједан корисник није ушао у САС ³ , или у случају одјављивања корисника са система.
Пријављивање на Windows	Приказује се кад корисник притисне ЦТРЛ+АЛТ+ДЕЛ и ниједан корисник тренутно није пријављен на систем.
Безбедност Windows – а и промена лозинке	Приказује се када корисник притисне ЦТРЛ+АЛТ+ДЕЛ а радна станица није закључана. ИЛИ Када радна станица није закључана и корисник притисне ЦТРЛ+АЛТ+ДЕЛ, а затим Промени лозинку (Change Password) .
Компјутер закључан	Приказује се када је радна станица закључана искључиво од стране корисника или када је чувар екрана постављен као сигурносна мера.
Откључај рачунар	Приказује се када корисник притисне ЦТРЛ+АЛТ+ДЕЛ док је радна станица закључана.

Табела 2: Предефинисани прозори радне површине „Winlogon”

Мењајући радне површине за различите задатке приликом пријављивања „Winlogon” осигурава да ће његови процеси бити невидљиви за програме ван процеса пријављивања, и на тај начин спречава могућност компромитовања података за пријављивање.

6.3. ГИНА

ГИНА, (DLL компонента коју учитава „Winlogon”) уграђује правила аутентикације у интерактивни модел пријављивања. Он извршава сву интеракцију током идентификације и аутентификације корисника. „Msgina.dll”, стандардна ГИНА коју обезбеђује Микрософт, а коју учитава „Winlogon” може бити замењена ГИНА – ом, коју је трећа страна прилагодила.

ГИНА је опциони део „Winlogon”-а који треће стране могу да замене у настојању да прилагоде функционалност или кориснички интерфејс пријављивања на Windows®. Изменом ГИНА – е, можете изабрати аутентикациони механизам који ће Windows® користити за кориснике.

Ово је често корисно за смарт картице или биометријско логовање. Знање о интерактивним системима пријављивања је потребно за уграђивање оваквог система. Код нове ГИНА – е мора садржати код за интеракцију са „Hamster”

³ SAS - Secure attention sequence



уређајем за препознавање отиска прстију. За ово је потребно простудирати све функције и услове за имплементацију нове ГИНА-е. У овом случају прво се приликом подизања система покрене „Winlogon”, који затим позива нашу замењену ГИНА-у и затим ће према њој, затражити притискање Ctrl+Alt+Del (CAD). У том тренутку ће нам затражити лозинку и уколико је она исправна, контрола се пребацује на „Hamster” уређај на којем се врши поређење отиска прстију. Ако се резултати поклопе(норма је до 95% сличности узорка), дозвољена нам је употреба ОС.



Слика 16: „Hamster” уређај

У овом делу нам је описано како направити био-заштиту ОС, који ће значајно бити сигурнији и прилично ослобођен ризика од хакера.

7. Биометријски кључеви са довољном дужином за сигурне апликације: будуће могућности

Предуслов за безбедно коришћење биометријских кључева је да барем један од следећих алтернативних техничких развитака дозволи добијање довољно дугачких биометријских кључева:

1. Техничке перформансе биометријских система се морају значајно побољшати
2. “Мулти – модална” биометрија мора бити искоришћена. тј- биометријски кључ добијен из више од једног биометријског својства, нпр. Неколико отисака прстију
3. Искористити нова биометријска својства, која дозвољавају добијање више информација.

Биометрија је незрела и млада технологија!

Опција 1 – Значајна побољшања квалитета шаблона, могу се очекивати у будућности.

Опција 2 – Добијање биометријских кључева из више од једног својства, делује обећавајуће нарочито у случају отисака прстију.

Опција 3 – би могла бити реализована као нпр. Биометријски систем базиран на ДНК. Људски геном садржи око 2,5 Мбајта стабилних дискриминаторних информација. Издвајањем само маленог дела ове информације у



реалном времену би било довољно за њену употребу у сврхе биометријских кључева. У прототип систему за заштиту биометријских шаблона, биометријски кључеви са дужином од 70 бита и степеном одбијања (“false rejection rate”) испод 1% су издвојени из стварних генетичких отисака прстију. Принципијена изводљивост криптографске заштите је на тај начин приказана.

8. Могућности апликација

8.1. Биометријске базе података

Нужност увођења биометријских технологија је уствари стварање нових поља апликације где су биометријски шаблони сачувани нпр. У централизованим или децентрализованим базама података.

Већ постоје форензичке и базе података биометријског материјала за медицинска истраживања. Заштита биометријских шаблона криптографијом и методом исправљања грешака, је делотворна против мера претњама које се тичу приватности и сигурности биометријских шаблона.

8.2. Биометријска аутентикација у вези са банкоматима (АТМ)

У банкарству употреба биометријских шаблона, у вези са банкоматима или системима продаје, је још увек у свом развоју. Постојала су нека експериментална тестирања у вези са банкоматима на крају 20ог века (нпр. “Dresdner” Банка, Банка “United of Texas” и друге.)

Последњих година банкарске организације широм света су увеле нове “Чип картица и ПИН аутентикација” шеме у своје банкомате, у настојању да смање трошкове превара са картицама. Од тад нове врсте напада на ове шеме су објављене (погледајте примере из Енглеске и Израела).

Због ових сигурносних претњи, око 40 јапанских банки, су увеле технологију биометријске аутентикације вена у длану у око 19.000 банкомата. Вена је споља веома невидљива биометријска особина, и стога, тешка за копирање. Постоје такође, пројекти у Бразилу и Аустрији.

У европи, банкарске трансакције банкомата се шаљу компјутерском центру банке која је издала картицу и тамо се корисникова аутентикација врши централно. Због тога, у овом случају, је препоручљиво, да се спречи складиштење незаштићених биометријских шаблона у централној бази података. Посебно, методи заштите биометријских шаблона, методом исправљања грешака и криптографским методама, би могли бити спроведени на начин описан у тексту који следи.

Вредности степена грешке прихватања (**FAR**) за системе са аутентикацијом вена, коју су објавили произвођачи, између 0,00008% и 0,0001%. Према формули ($\log_2 k \leq -\text{FAR}$), горња граница добијене “дужине биометријског кључа” лежи испод 21 бита.



Препоручљиво је комбиновати биометријске методе са устаљеним ПИН и чип шемама, као у Јапану. Овај механизам осигурава тростепено решење безбедности:

Корисник даје нешто што “поседује” (картица), нешто што “зна” (ПИН) и оно што “јесу” (биометријски идентификатор), пре него што је трансакција извршена.

Један велики изазов у будућности биће да се створе нове међународне норме за личне идентификационе шеме укључујући и технологије биометријске аутентикације у настојању да се обезбеди међусобна операбилност различитих банкарских организација и земаља.

Један приступ би била генерализација постојећих међународних норми и комбиновање са приступом, заштите биометријских шаблона.

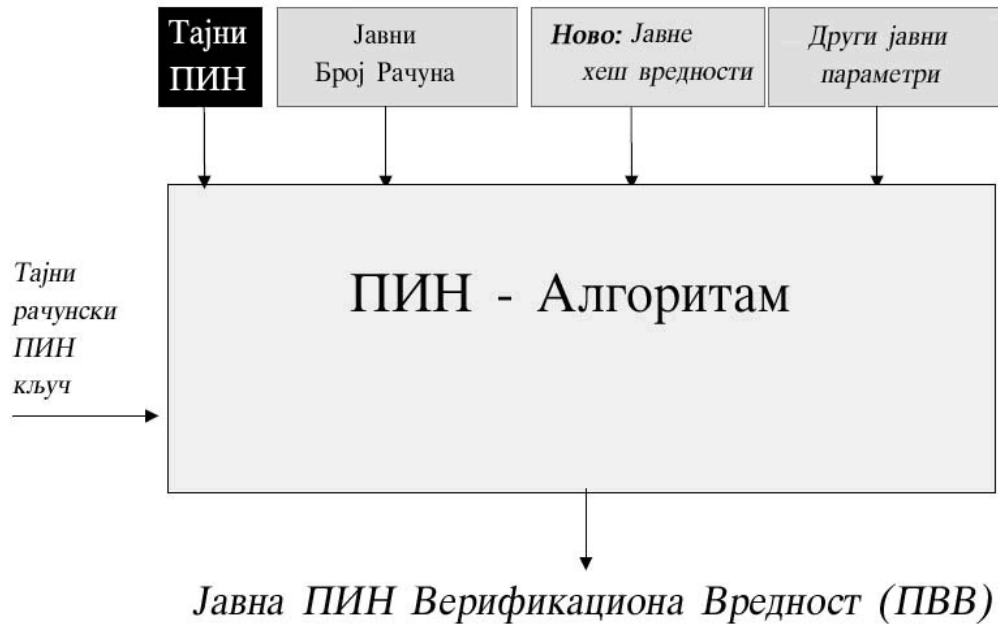
Банкарство у ствари подржава много различитих врста генерисања ПИН кодова и верификационих процедура и формата. За “VISA PVV PIN” алгоритам, који потржава јавну ПИН Верификациону Вредност (**ПВВ**), предлагемо генерализацију ПИН процедуре на следећи начин: увођењем биометријских технологија. Главни циљ ове генерализације је да дозволи увођење биометријских технологија са минималним променама постојећих норми и постављеног хардвера.

Према шеми Џуелса и Ватенберга у центру за персонализацију кредитне картице, насумична шифра, нпр. $c = G(s)$ за насумично $s \in GF(q)^k$ се битски додаје (**XOR**) биометријском шаблону f корисника картице током уписа и резултат се чува на кредитној картици као $y = c \oplus f$.

Затим се тајна вредност s ставља у криптолошку хеш функцију да би се добила хешована вредност $H(s)$. После генерисања тајног ПИН – а, хеш вредност се користи као нови улазни параметар који производи јавну ПВВ на уопштен (генерализован) начин, комбинујући конвенционалне ПИН процедуре и биометријске технологије, као што је приказано на слици 18.



Процедура израчунавања ПВВ



Слика 17: Процедура израчунавања ПВВ у центру за персонализацију кредитне картице

Биометријски податак је уведен као један од јавних параметара. Ако корисник користи банкомати, он уноси свој тајни ПИН. Даље, биометријска одлика се добија и биометријски шаблон се генерише. У кредитној картици овај биометријски шаблон “ f^* ”, добијен од корисника, се додаје вредности “ y ” сачуваној у кредитној картици. Резултат је $f^* \oplus y = f^* \oplus c \oplus f$. Пошто радимо са кодом који исправља грешке, одговарајућа декодирајућа функција производи вредност “ s^* ”. Ако је Хамингова раздаљина између f и f^* највише “ t ”, онда је $s^* = s$, у другом случају не. После “хешовања” добијене вредности s^* , $H(s^*)$ је повезано са енкриптованим ПИН – ом у банкарској трансакцији.



Процес верификације ПИН - а



Слика 18: Процес верификације ПИН – а

Банкарска трансакција се енкриптује и шаље се ауторизационом банкарском центру, где се потом декриптује.

Енкриптован пин и хеш вредност $H(s^*)$ се добијају заједно са осталим параметрима, нпр. Са ПВВ, бројем рачуна, затим се користе као улазни параметри за процедуру верификације ПИН – а као што је приказано на слици 6. Генерализоване процедуре верификације ПИН – а стварају нову ПВВ вредност, названу **ПВВ***, одговарајућу датом ПИН – у, подацима о рачуну, хеш вредности и осталим параметрима и пореде је са улазном ПВВ. Ако је $\text{ПВВ}^* = \text{ПВВ}$, корисник је аутентификован. Ако ауторизација не успе, бројач поновних покушаја може бити ограничен малом вредношћу да би се спречили “brute force” напади.



9. Биометријске исправе

9.1. Биометријске личне карте

Реакције и мишљења о биометријским исправама су различита, чак и крајње супротна. Од тога да је стигло нешто што је свету требало, до теорија завере. „Тајмс“ је увођење биометријских исправа у Индији описао овако : „То је сигурно највећи зачет пројекат Великог Брата. Индија мора да изда сваком од 1,2 милијарде грађана, од којих милиони живе у удаљеним селима и не поседују документарни доказ о постојању, биометријске личне карте.“⁴

Обавезне националне идентификационе исправе се користе у око 100 земаља укључујући и: Немачку, Француску, Белгију, Грчку, Луксембург, Португал и Шпанију. Примера ради немачка полиција има право да задржи особе у притвору до 24 сата, уколико не носе своју исправу.

С друге стране, Аустралијаци су се одупрли таквим плановима владе великим протестима '80их, док је Бушова администрација издржала притиске после напада 11. септембра да их уведе.

Пластичним исправама је дата предност у односу на папирна документа јер се теже фалсификују и њихови поборници тврде да спречавају илегалну имиграцију и преваре. Већина исправа садржи име, пол, датум рођења и јединствени број власника, док Бразил, Јужна Кореја, Италија и Малезија имају и отисак прста на себи (од недавно и Србија). У Европској Унији се неке од исправа могу користити и за путовање уместо пасоша.

У Великој Британији, биометријске исправе су још у фази тестирања, а парламент ће морати 2013. да се изјасни да ли ће барем једна исправа морати да буде са биометријским подацима.



Слика 16: Биометријска исправа у УК

⁴ <http://www.timesonline.co.uk/tol/news/world/asia/article6710764.ece>



Наравно, морамо навести и главне забринутости будућих корисника:



Биометријска технологија прави битне разлике између појединаца лако се повезује са базом података, чинећи приватност рањивијом подложнијом оштећењима.



Неке биометријске технологије су дискриминаторске (нечији прсти не остављају добар отисак прста, што чак и низак степен грешке од 0,1%, чини на светском нивоу милионе грешака).



Прецизност биометријског система је немогуће проценити пре примене у пракси.



Цена грешке је висока – ако изгубите кредитну картицу, можете је поништити и извадити нову. Једном изгубљен биометријски податак је изгубљен за цео живот.

На блиском истоку, компаније и владе све више користе биометријске системе да идентификују особе на поседима компаније и државе, као и на граничним прелазима и аеродромима. Окружно биометријске тржиште се процењује на вредност око \$500 милиона у 2007. години. Недавно, влада УАЕ је потрошила \$55 милиона на постављање најновије биометријске технологије за национални систем исправа, које ће заузврат произвести одређене буџетске приходе.

У Србији, осим у круговима блиским СПЦ, о овој теми се није до недавно расправљало: дебата о биометрије сведена је на проблематику израде нових пасоша и личних карти. Истински јавна расправа, уз активно учешће невладиног сектора такође је изостала. Тако је 03. марта 2008. одржана јавна расправа⁵ између представника државних институција, стручњака у области биометрије, те представника цивилних друштава.

Бојана Панић из МУП Србије је истакла да полиција никоме не може узети узорак ДНК без одобрења судске власти и да су притом, у полицијској истрази биометријске карактеристике важан доказ будући да су универзалне и непроменљиве. Остаје, међутим, питање чији профил треба да се нађе у евиденцији и у ком временском периоду може да буде чуван.

Нинослав Јањић је у прилог коришћењу биометријских технологија изнео аргумент да конвенционалне шифре данас нису довољно сигурне. Зашто их користити, сматра Јањић, ако можемо да користимо податке са тела као шифре (отиске прстију, биометрију руке, дужице, боје гласа).

Заштитник грађана Саша Јанковић је неприкосновеним утврдио принцип да „ограничење права и слобода појединаца сме бити изведено само уз њихов пристанак". Тако заштита података о личности представља један сегмент права на приватност. Устав Србије познаје институт заштите података о личности, за коју се каже да се ближе уређује законом. Кључни недостатак је што је односни закон непромењен од 1998. године, те према томе Србија нема одговарајући законски оквир за регулисање ове области.

Повереник Родољуб Шабић је нагласио да свако организовано друштво мора бити свесно могућности злоупотребе информационих технологија. Једно друштво које, како се изразио, жели да буде демократско не сме сметнути са ума да је највећа вредност слобода. Та се слобода доводи у питање све док постоји поменута

⁵ <http://www.ccmr-bg.org/cms/view.php?id=2914&start=20>



могућност злоупотребе. Зато што не постоји законска регулатива, Шабић се противи примени биометријске технологије при изради личних докумената.

Најопаснија актуелна друштвена импликација примене биометрије, према Ђакону Суботићу јесте да се ствара неповерење између грађана и државе: до недавно су биометријски подаци узимани од криминалаца, а у данашње време ће се узимати и од грађана. Много су битније, сматра Суботић, будуће импликације, због чега је потребно тражити један идеалан биометријски систем идентификације. Он је закључио да је императив државе да критички размотри све могуће последице увођења биометрије јер у супротном, могући резултат може бити успостављање тоталитарног окружења.

О свим даљим активности пројекта "Повећање учешћа грађана у безбедној политици", можете се информисати на сајту www.bezbednost.org.



Слика 19: Предња страна нове личне карте



Слика 18: Задња страна нове личне карте

9.2. Биометријски пасоши

Биометријски пасош, познатији под именом е-пасош или еПасош, је комбинација обичног и електронског пасоша који користи биометрију за аутентификацију идентитета путника путем бежичне паметне картице, која садржи микопроцесорски чип (компјутерски чип) и антену (која напаја чип и служи за комуникацију) усађен на предњу или задњу корицу, или централну страницу пасоша. Карактеристике исправе и чипа су документоване у документу 9303 Интернационалне Организације за Цивилну Авијацију („International Civil Aviation Organisation's" - ICAO). Најважније информације су одштампане на страни са подацима пасоша и похрањене на чип. Инфраструктура јавног кључа („Public Key Infrastructure - PKI) се користи за аутентификацију електронски похрањених података на чип, чинећи их недодирљивим за кривотворце.

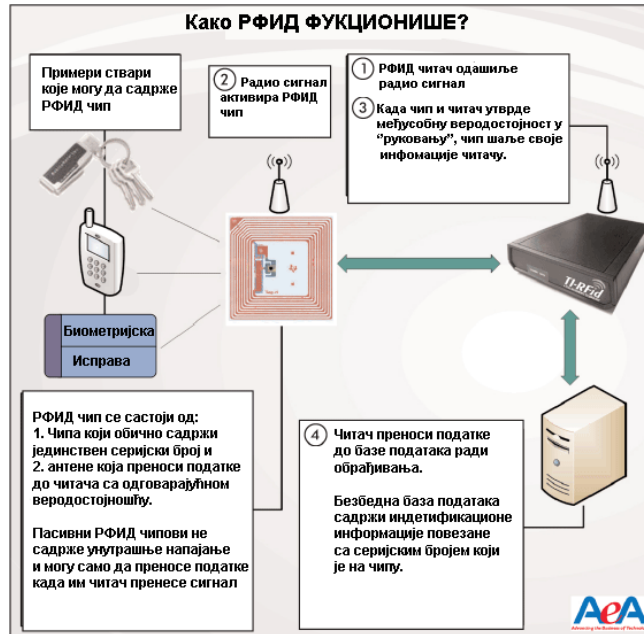
Иако САД захтева биометријско скенирање приликом уласка у земљу (а и приликом издавања визе), њихов пасош није биометријски. Он користи РФИД чип уместо технологије која је прописана ИОАЦ документом. Разлика је у томе што та технологија укључује и микропроцесор, контролу приступа података, безбедност комуникације и још неке функционалности.

Оно што је стандардизовано за овај начин идентификације су препознавање лица, отиска прста и ириса. Дигитална слика у ЈПЕГ или ЈПЕГ 2000 формату је похрањена на чипу. Остала поређења се врше на еГраницама (eBorders) и њиховим системима. За чување биометријских података потребно је минимум 32Кб ЕЕПРОМ меморије. Ови стандарди омогућавају користљивост и универзалност пасоша јер различите земље имају различите произвођаче пасоша.



Пасоши су опремљени заштитним механизмима да избегну и / или открију нападе:

-  Није могуће пратити чип – Насумични идентификатори чипа одговарају на сваки захтев са различитим бројем чипа. Ово спречава праћење чипа у пасошу. Коришћење насумичних бројева је опционално.
-  „Основна Контрола Приступа" („Basic Access Control" – BAC) – штити комуникационе канале између читача и чипа криптовањем пренесених информација. Пре него што се подаци могу прочитати са чипа, читач мора да обезбеди кључ добијен да "Простора читљивог машином" ("Machine Readable Zone") : датум рођења, датум важења исправе и број исправе. Ако се ОКП користи, нападач не може (лако) да "прислушкује" информације које се преносе, без знања кључа. Коришћење ОКП је опционално.
-  Пасивна аутентификација (ПА) - спречава модификовање података на чипу пасоша. Чип садржи документ (СОД) који чува ХЕШ вредности свих докумената похрањених у чипу (слика, отисак прста итд.) и дигитални потпис тих ХЕШ вредности. Дигитални потпис је направљен коришћењем потписног кључа документа који је "потписан" кључем земље порекла. Ако је документ у чипу (нпр. слика) промењен, то ће бити примећено због разлике у хеш вредности. Читачима је потребан приступ свим јавним кључевима држава у употреби да би могли да провере да ли је дигитални потпис направљен од стране поверљиве државе. Коришћење ПА је обавезно.
-  Активна аутентификација (АА) – спречава клонирање пасошких чипова. Чип садржи тајни кључ који не може бити прочитан или копиран, али се његово присуство лако може доказати. Коришћење АА је опционално.
-  Проширена Контрола Приступа ("Extended Access Control" – EAC) - даје функционалност која проверава веродостојност чипа и читача. Шта више, користи јачу енкрипцију од ОКП. ПКП се користи за заштиту отисака прстију и ириса. Коришћење ПКП је опционално, осим за земље Европске Уније где је од 28. Јуна 2009. обавезно.
-  Заштита чипа – спречава неовлашћено читање. Неке земље, укључујући САД, су утиснуле танку металну мрежицу у корице пасоша да се понаша као штит када се пасош затвори. Коришћење мрежице је опционално.



Слика 20: Начин функционисања РФИД чипа

Активисти који се залажу за приватност у многим земљама имају сумње и протестују због недостатка информација шта ће точно садржавати чипови пасоша и да ли ће то утицати на грађанске слободе. Главни проблем који се истиче је да се подаци са пасоша могу преносити преко бежичне РФИД технологије, што може бити главна рањивост. Иако ово омогућава компјутерима да изврше проверу исправе без физичке конекције, то може пружити прилику и свакоме са одговарајућом опремом. Уколико лични подаци и бројеви пасоша на чипу не би били шифровани, информације би доспеле у погрешне руке.

ББЦ је у децембру 2006. године прокоментарисао Британски еПасош у чланку, цитирајући горе наведене пасусе и додајући: „Скоро свака земља која издаје овај пасош има неколико сигурносних експерата који вичу из свег гласа и покушавају да упозоре:

Ово није безбедно. Користити ове технологије није добра идеја, цитирајући стручњака који наводи: То је превише компликован процес. Урађено је наопако и на погрешним местима - прво читање података, анализа података, тумачење података, и тек онда провера да ли је исправно. Постоји много техничких недостатака и постоје ствари које су само заборављене, тако да у основи не ради што треба да ради. Технологија треба да обезбеди виши ниво сигурности. Она то не ради."

С друге стране ЦНН је прокоментарисао могућност праћења путем РФИД технологије:

„Група хакера је успела на конвенцији у Лас Вегасу 2005. да очита податке са 30 метара. Заговорници РФИД-а су критиковали ово "доказивање" јер је апаратура непрактична у спољнем свету и не би радила ако су подаци на чипу шифровани – а најчешће јесу. РФИД чипови који се користе најчешће немају извор енергије и шаљу информације преко 3 метра. Поредити са телефоном на пример, који преноси идентитет и податак о тренутној локацији километрима далеко, злоупотреба РФИД-а постаје прилично тривијална сматра Кевин Ештон, председник „ThingMagic LLC“, произвођач РФИД читача.“



10. Мултимодална биометрија

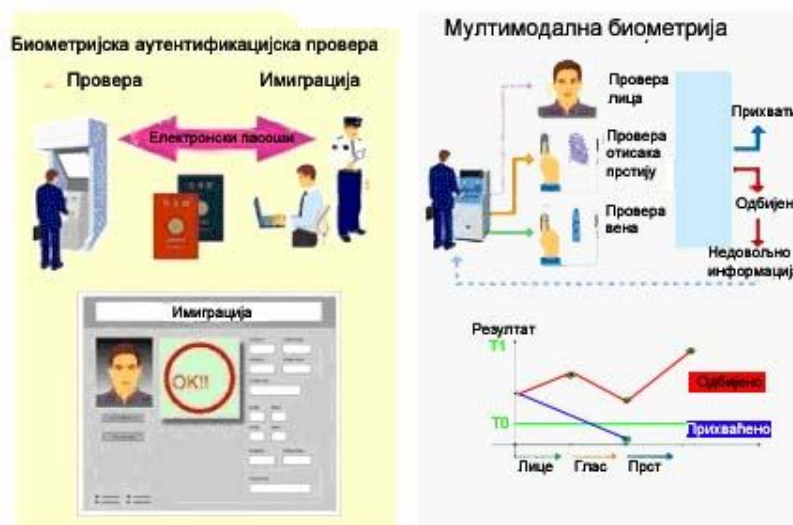
Мултимодална биометрија подразумева комбиновање свих претходно наведених биометријских техника. Уколико се у пракси користи већи број претходно набројаних техника, може да се изгради један сигурни информациони систем. У пракси је то комбинација физичких карактеристика и понашања која подразумева проверу и идентификацију.

У пракси се користе у граничним прелазима за контролу уласка или изласка, за контролу приступа неком простору, цивилној идентификацији, мрежној безбедности.

Мултимодална биометрија се користи и као подршка стандардним поступцима за проверу идентитета или уколико из изворних докумената и записа није могуће добити довољан број података којима би се описала нека особа. Препоручљива је комбинација стандардних безбедносних механизма и биометријских јер увек постоји могућност злоупотребе.

Један од примера је лажни шаблон отиска прстију. Уколико се користи само једна техника као што је препознавање отиска прстију, тада је могућа ситуација у којој трећа особа поседује лажни отисак прстију са којим обавља аутентификацију у име неке особе.

Но, уколико се користи верификација лица, или још боље распознавање ириса и провера вена, тада се са већом могућношћу може утврдити како се заиста ради о тој особи или се може препознати случај покушаја крађе идентитета.



Слика 21: Пример Мултимодалне биометрије

Унимодални биометријски системи морају да се боре са мноштвом разоврсних проблема као што су нечисти подаци, варијације шаблона, ограничени нивои слободе, немогућност универзалне применљивости, прикривених напада и неприхватљивих нивоа грешака. Наведена ограничења се могу решити мултимодалним биометријским системима јер прикупљају информације са различитих извора. Покушаћемо да објаснимо неколико могућих ситуација у којима се систем може наћи, нивое стапања који су могући и стратегије за постављање система који би могао да сабере све информације. Представимо и неколико



примера мултимодалних система који су описани у литератури.

Утврђивање идентитета особе постаје веома важно у нашем значајно повезаном друштву. Питања попут „Да ли је она стварно та за коју се издаје?“, „Да ли ова особа сме да користи ове просторије?“ и „Да ли се он налази на потерницама?“ се често постављају у разоврсним ситуацијама од издавања возачке дозволе до уласка у земљу.

Потреба за поузданим аутентикацијским техникама се увећава се повећаном забринутости за безбедност и убрзаним развојем мрежа, комуникација и покретљивости технологија.

Биометрија, описана као наука препознавања појединца заснована на његовим физичким особинама и понашањем, почиње да добија кредибилитет као метода за одређивање идентитета појединца.

Биометријски системи су тренутно постављени у разним комерцијалним, цивилним и форензичким апликацијама као средство утврђивања идентитета. Ови системи се ослањају на доказе отисака прстију, геометрију шаке, ириса, зенице, лица, распореда вена у рукама, терограма лица, потписа, гласа итд. да би или потврдили или одредили идентитет.

Већина биометријских система су унимодални, тј. ослањају се на доказе из једног извора информација за аутентикацију. Овакви системи морају да се изборе са широким спектром проблема, као што су:

- ✓ Шум у прикупљеним подацима (отисак прста са ожиљком, глас измењен прехладом...). Он може настати од покварених или неправилно одржаваних сензора (накупљена прашина на сензору за отисак прста) или лоши услови за рад (лоше осветљење лица);
- ✓ Варијације унутар класа: Обично настају од стране корисника који неправилно комуницира са сензором (неправилна позиција лица у односу на сензор) или када се карактеристике сензора мењају током аутентификације (оптички наспрам “solid-state” сензора за отисак прста);
- ✓ Сличности унутар класа: У биометријским системима састављеним од великог броја корисника, може се појавити сличност унутар класа (преклапање) у простору особина вишеструких корисника. Голфарели тврди да је број препознатљивих шаблона у два од најчешће коришћених представа геометрије руке и лица, износи само 10^5 тј. 10^3 ;
- ✓ Не-универзалност: Биометријски систем није у могућности да прикупи биометријске податке од значаја из подкупа корисника. Биометријски систем отисака прстију, на пример, може изложити некоретне особине минута из отисака прстију одређених индивидуа, због лошег квалитета „гребена“;
- ✓ Маскирани напади: Ова врста напада је нарочито битна, када се карактеристике понашања, као што су потпис или глас, користе. Међутим, физичке карактеристике, као што су отисци прстију, су такође осетљиве на маскиране нападе.

Ова ограничења које нам унимодални биометријски систем намеће, могу бити превазиђена укључивањем вишеструких извора информација за утврђивање



идентитета. Такви системи, названи мултимодални биометријски системи, би требали бити поузданији због присуства вишеструких, (прилично) независних делова доказа. Ови системи могу да испуне строге захтеве неопходне за различите апликације.

Први проблем који решавају је неуниверзалност, с обзиром да вишеструке карактеристике омогућавају довољну покривеност становништва. Такође отежавају маскирање јер је уљезу теже да маскира више биометријских особина, што оригиналном кориснику не представља проблем. Шта више, могу да пруже изазов механизмом да од корисника тражи насумичан подскуп биометријских особина и тиме обезбеде да „живи“ корисник доиста стоји поред сензора на месту прикупљања података.

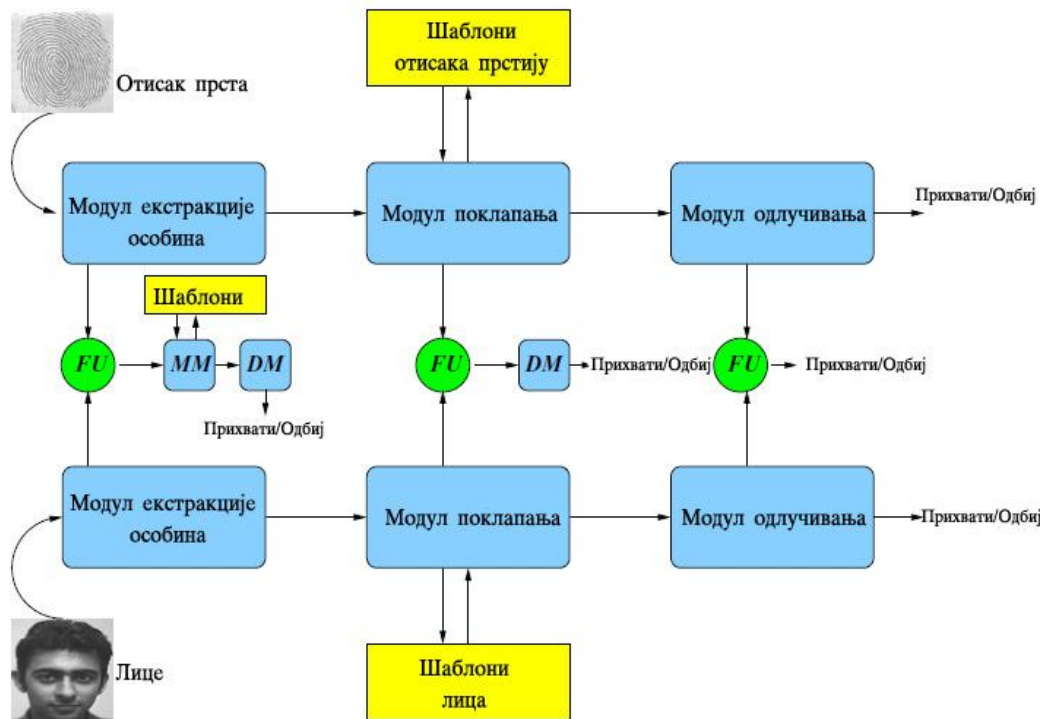
Размотрићемо нивое стапања који су могући у мултимодалним биометријским системима, разне сценарије који су могући, различите начине извршавања задатака, стратегије укључивања система које би могле бити прихваћене и проблеме у вези са дизајном и постављањем ових система.



11. Нивои стапања

Генерички биометријски систем има 4 важна модула:

1. Сензор модул који хвата особину и претвара је у биометријски податак;
2. Модул екстракције који обрађује податак да би извукао сет карактеристика које су збијени приказ особине;
3. Модул поклапања који упошљава класификатор ради поређења извученог сета карактеристика са шаблонима похрањеним у бази података, ради генерисања резултата поклапања;
4. Модул одлучивања који користи резултат поклапања да утврди идентитет или да потврди идентитет. У мултимодалном систему измирење информација се може десити у било којем од претходно поменутих модула.



Слика 22: Нивои стапања у бимодалном биометријском систему: FU: Модул стапања MM: Модул поклапања, DM: Модул одлучивања



- ✓ *Стапање на нивоу података или особина:* Сами подаци или сетови особина који потичу из вишеструких сензора-извора се стапају.
- ✓ *Стапање на нивоу резултата поклапања:* Резултати које генеришу вишеструки класификатори који се односе на различите модуларности се комбинују.
- ✓ *Стапање на нивоу одлучивања:* Коначни излази вишеструких класификатора се уједињују техникама, као што је већинско гласање. Биометријски системи који интегришу информације у раним фазама обрађивања сматрају се ефективнијим од система који спроводе интеграцију у каснијим фазама. Пошто сетови особина садрже богатије информације о улазу биометријских података од резултата поклапања или вредности излаза модула поклапања, очекује се да стапање на нивоу особина даје боље резултате препознавања. Међутим, стапање на овом нивоу је тешко за постигнути у пракси јер:
 - о Сетови особина различитих модалности нису међусобно одговарајући (нпр. Eigen-коэффициенти лица и сет минута прста)
 - о Најкомерцијалнији биометријски системи не пружају приступ сетовима особина (ни сировим подацима) које њихови производи користе.

Стапање на нивоу одлучивања сматра се крутим због доступности ограничених информација. Стога је стапање на нивоу резултата поклапања први избор, јер је релативно лако за приступање и комбиновање резултата које различити модалитети дају.



12. Сценарији стапања

У зависности од броја особина, сензора, и сетова особина који се користе, разноврсност сценарија у мултимодалном биометријском систему је могућа:



Слика 23: Сценарија у мултимодалним биометријским системима

- 1) *Једна биометријска особина, вишеструки сензори:* Више сензора записује исту биометријску особину. Стога, сирови биометријски запис података различитих сензора се прикупља. Ченг и остали⁶ прикупљају 2Д и 3Д слике лица и комбинује их на нивоу података, као и на нивоу резултата да би унапредио перформансе система за препознавање лица. Кумар и остали⁷ описују систем верификације заснован на шапи корисника која комбинује геометријске особине руке са отисцима длана на нивоу особина и на нивоу резултата. Интересантно је да у њиховим експериментима, стапање на нивоу резултата има боље перформансе, него стапање на нивоу особина. Ово може бити због високе димензионалности стопљених сетова особина и стога би примена технике редукције особина могла бити примерена.
- 2) *Једна биометријска особина, вишеструки класификатори:* За разлику од претходног сценарија, само један сензор се користи за прибављање сирових података. Ове податке користе вишеструки класификатори. Сваки од ових класификатора или ради на истом сету особина извучених из података или генерише сопствене сетове. Џејн и остали⁸ користи логистичке функције да

⁶ K. I. Chang, K. W. Bowyer, and P. J. Flynn, "Face recognition using 2D and 3D facial data," in *Proc. of Workshop on Multimodal User Authentication*, (Santa Barbara, CA), pp. 25–32, Dec 2003.

⁷ A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," in *Proc. of 4th Int'l Conf. on Audio and Video-based Biometric Person Authentication (AVBPA)*, (Guildford, UK), pp. 668–678, Jun 2003.

⁸ A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for a high security fingerprint verification system," *Pattern Recognition Letters*, vol. 20, pp. 1371–1379, 1999.



интегрише резултате поклапања прикупљене из три различита модула за поклапање отисака прстију на истим сетовима минута. Рос и остали⁹ комбинују резултате поклапања отисака прстију са минутима са резултатима модула за поклапање заснованог на текстури да би побољшао резултате поклапања. Лу и остали¹⁰ извлаче три различите врсте сетова особина из слике лица појединца (користећи ПЦА, ЛДА и ИЦА) и интегрише излазе одговарајућих класификатора на нивоу поклапања резултата.

- 3) *Једна биометријска особина, вишеструке целине:* У случају отиска прста (или ириса) могуће је интегрисати информације добијене од два или више прстију (или оба ириса) једног корисника. Ово је јефтин начин побољшања система, пошто не захтева постављање вишеструких сензора, нити укључивање додатних модула за екстракцију и или поклапање.
- 4) *Вишеструке биометријске особине:* Овде се вишеструке особине појединца користе ради утврђивања идентитета. Такви системи користе више сензора да прикупи податке који се односе на различите особине. Независност особина осигурава значајан напредак у перформансама. Брунели и остали¹¹ користе особине лица и гласа појединца за идентификацију. HyperBF мрежа се користи за комбиновање нормализованих резултата пет различитих класификатора који раде са гласовним и сетовима особина лица. Бигун и остали¹² су развили статистичку мрежу засновану на Bayesian статистици да интегрише говор (зависан од текста) и особине лица корисника. Процењене грешке сваког класификатора су узете у обзир током процеса стапања. Хонг и Џејн¹³ повезују различите мере поверљивости са модулима за поклапање појединаца приликом интеграције особина лица и отиска прста корисника. Они такође предлажу механизам индексирања у којем се информације у вези са лицем користе за преузимање сета могућих идентитета, а затим се информације о отиску прста користе за издвајање идентитета појединца. Комерцијални производ назван БиоИД користи глас, покрет усана и особине лица корисника за потврђивање идентитета.

⁹ A. Ross, A. K. Jain, and J. Reisman, "A hybrid fingerprint matcher," *Pattern Recognition*, vol. 36, pp. 1661–1673, Jul 2003.

¹⁰ X. Lu, Y. Wang, and A. K. Jain, "Combining classifiers for face recognition," in *Proc. IEEE Int'l Conf. on Multimedia and Expo (ICME)*, vol. 3, (Baltimore, MD), pp. 13–16, Jul 2003.

¹¹ R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Transactions on PAMI*, vol. 12, pp. 955–966, Oct 1995.

¹² E. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using Bayesian Statistics," in *First International Conference on AVBPA*, (Crans-Montana, Switzerland), pp. 291–300, March 1997.

¹³ L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Transactionson PAMI*, vol. 20, pp. 1295–1307, Dec 1998.



13. Начини рада

Мултимодални систем може да ради на три различита начина: серијски, паралелно или хијерархијски.

У серијском начину рада, излаз једног модалитета се најчешће користи за сужавање броја могућих идентитета, пре него што се следећи модалитет искористи. Стога вишеструки извори информација (нпр. Вишеструке особине) **не** морају да буду прикупљене истовремено. Даље, одлука се може донети и пре прикупљања **свих** особина. Ово може смањити укупно време потребно за препознавање.

У паралелном начину рада информације са различитих модалитета се користе истовремено ради препознавања.

У хијерархијској шеми, појединачни одредници се спајају у дрволикој структури. Овај начин је значајан кад је број одредница велик.



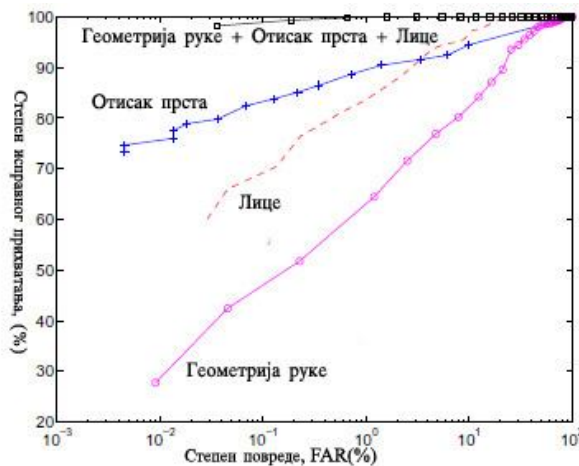
14. Смернице за постављање система

Смернице усвојене за постављање зависе од нивоа на којем је стапање извршено.

Стапање на нивоу особина се може постићи надовезивањем два међусобно одговарајућа сета особина. Технике одабирања/редукције особина могу бити у сврси регулисања „проклетства димензионалности“.

Стапање на нивоу поклапања резултата је добро проучено у литератури¹⁴. Јасне и ефикасне технике нормализације су потребне за преображавање резултата вишеструких уређаја за поклапање у заједнички домен пре њиховог сједињавања.

У контексту верификације, 2 различите стратегије постоје за стапање на овом нивоу. У првом приступу стапање се посматра као класификациони проблем у којем се прави вектор особине уз помоћ резултата поклапања различитих уређаја. Затим се тај вектор премешта у једну од 2 класе: **Прихваћено**(овлашћени корисник) или **Одбијено**(уљез)¹⁵.



Слика 24: Побољшање које настаје правилом једноставне суме

У другом приступу стапање се сматра проблемом комбинаторике у којем се појединачни резултати поклапања комбинују ради генерисања јединственог скаларног резултата који се користи за доношење коначне одлуке. Рос и Џејн¹⁶ су приказали да је правило једноставне суме довољно за добијање значајног напретка у резултатима поређења мултимодалних биометријских система(Слика 25).

¹⁴ R. P. W. Duin and D. M. J. Tax, "Experiments with classifier combining rules," in *Proc. of 1st Workshop on Multiple Classifier Systems*, vol. LNCS 1857, (Cagliari, Italy), pp. 16–29, Springer, Jun 2000.

¹⁵ 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 *Proc. of 2nd Int'l Conf. on Audio- and Video-based Person Authentication*, (Washington D.C., USA), pp. 188–193, March 1999.

¹⁶ A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, pp. 2115–2125, Sep 2003.



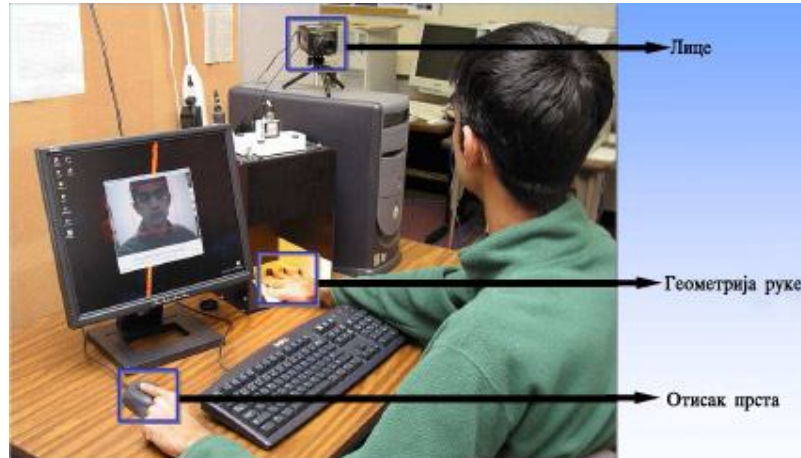
15. Дизајн

Мноштво фактора је потребно размотрити приликом израде мултимодалног биометријског система. То су:

- ✓ Избор и број биометријских особина
- ✓ Ниво у биометријском систему на којем добијене информације из различитих извора требају бити интегрисане
- ✓ Усвојити методологију за интеграцију информација
- ✓ Однос цене и квалитета поклапања

Приликом избора и броја биометријских особина највише се водимо природом саме апликације, трошкове које нам вишеструка својства изискују (рачунарске захтеве и трошкове, на пример) те односе између одабраних особина (међусобно независне информације су боље јер се стабилност и квалитет повећани у овом случају). У мобилном телефону који је опремљен камером, лакше је комбиновати лице и глас корисника, док се код банкомата лакше комбинују отисак прста са особинама лица корисника. У идентификационим системима који раде са великим бројем корисника (говорећи о милионима корисника) механизам индексирања се може унапредити мултимодалним приступом.¹⁷

Истраживачи¹⁸ тренутно проучавају добитак у перформансама који се може добити најновијим системима препознавања отиска прста и лица који се могу добити у слободној продаји, испитујући велику групу појединаца.



Слика 25: Прототип биометријског логин система

¹⁷ E. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using Bayesian Statistics," in *First International Conference on AVBPA*, (Crans-Montana, Switzerland), pp. 291–300, March 1997.

¹⁸ M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. K. Jain, "Multimodal biometric authentication methods: A COTS approach," in *Proc. of Workshop on Multimodal User Authentication*, (Santa Barbara, CA), pp. 99–106, Dec 2003.



16. Закључак

У раду је описан развитак биометрије, биометријске технике као одређени системи који су тренутно у употреби. Анализом унимодалних система и откривањем њихових слабости, дошло се до потребе за развијањем мултимодалних биометријских система.

Закључак који можемо извести после овог рада је да су мултимодални системи у значајној предности у односу на унимодалне биометријске системе. Коришћењем било којег од наведених сценарија и модула добија се већа прецизност идентификације и већа сигурност система.

Мултимодални биометријски системи се истовремено елегантно боре са неколико проблема које смо сретали у унимодалним системима. Комбиновањем вишеструких извора информација, ови системи побољшавају резултате поређења, увећавају покривеност популације, онемогућавају прикиривене нападе и олакшавају индексирање. Различити нивои стапања и исходи су могући у мултимодалним системима. Стапањем на нивоу резултата је техника која је најчешће у употреби због лакоће приступа и здруживања резултата поређења.

Добитак у перформансама се нарочито истиче када се међусобно независне особине користе у мултимодалним системима. Укључивање корисничко-одређених параметара може само побољшати учинак система.

Са све ширим распоређивањем биометријских система у цивилим и државним апликацијама, само је питање времена, пре него што мултимодални биометријски системи почну да утичу на начин на који ће се идентитет утврђивати у 21. веку(слика 26).



17. Литература

- [1] **Biometric Security** - More Swapnaja B. , Ubale Amol B. , Jondhale K.C.
- [2] **The Biometric System Models with Secure Network Protocols in Open Network Environment** - Woochang Shin, Yong-Nyuo Shin *Seokyeong Univ 1, Korea Information Security Agency2*
- [3] **Security Evaluation of Biometrics Authentications for Cellular Phones** - Hirokazu Manabe, Yuta Yamakawa, Tomohiro Sasamoto, Ryoichi Sasaki
- [4] **Multimodal biometrics: An Overview** - *Arun Ross and Anil K. Jain*
- [5] **“How to generate Strong Keys from Biometrics and Other Noisy data”** - Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin and Adam Smith
- [6] <http://www.mup.sr.gov.rs>
- [7] <http://en.wikipedia.org/>
- [8] <http://www.griaulebiometrics.com/page/en-us/book/understanding-biometrics/introduction>
- [9] www.cert.hr/filehandler.php?did=258
- [10] <http://news.bbc.co.uk>
- [11] <http://www.cnn.com>
- [12] <http://www.sk.co.rs>