

*Дипломски рад посвећујем мојим вољеним родитељима,
оцу **Властимиру (кршт. Властоју)**
и мајци **Радојки Мрдаковић***



УНИВЕРЗИТЕТ СИНГИДУНУМ
ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Биометрија приватности

- Дипломски рад -

Ментор:

Доц. др Саша Адамовић

Студент:

Миливој Мрдаковић

Бр.индекса: 2012/201777

Београд, 2014.



ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Београд, Данијелова 32

Кандидат: Миливој Мрдаковић

Број индекса: 2012/201777

Смер: Информатика и рачунарство

Тема: Биометријска читавања која могу да послуже очувању приватности

Задатак: Дедукцијом, разјашњавањем појма и суштине биометрије, историје њене употребе и категоризације биометријских отисака, разјаснити појам и важност приватности, разјаснити опозиву биометрију, приказати и објаснити шему која може омогућити аутентификацију пред службеним лицем, која не само да не угрожава приватност, већ је и унапређује.

Датум одобрења рада:
Београд, _____._____._____.

МЕНТОР

Доц. др Саша Адамовић

ДЕКАН

Проф. др Драган Цветковић

Биометрија приватности

Сажетак: Када је човек почео да броји и мери, почела је да напредује и технологија. Историјски преглед мерења биометријских података представља обиман и захтеван задатак. Сагледавање коришћења биометрије од прадавних времена до данас, опис будућих трендова, дефиниција, поделе и врсте представљају део прегледа у области истраживања. Други део посвећен је опасности од информационо-контролисаног друштва, приватности (и информационој), њеном појму и разлогу зашто је потребна, њеном законском оквиру и утемељењу. Трећи део везан је за предлог шеме употребе биометријских читавања, не за потенцијално угрожавање приватности и слобода, већ супротно, да би те исте вредности – заштитила. Рад се наслања на досадашња достигнућа у развоју алгоритама и технологија за обраду отиска прста, криптологију, рачунарске мреже и њихову безбедност, позива на развој нових и савршенијих алгоритама како би се постигла безусловна аутентификација са стопроцентном тачношћу.

Суштина рада је сагледавање онога што је познато, али из нове перспективе. Примена идеје би могла да донесе многе бенефите људским правима и слободама, спровођењу законитости, материјалну уштеду, организациона побољшања, побољшање индекса задовољства и среће човека и никако мање важно избегавање опасности тоталитаристичких идеја кроз евентуално имплантирање електронских чипова у човеково тело (ти трендови су започети одавно у западном свету), чије би последице по човечанство биле немерљиво штетне.

Кључне речи: Биометрија, приватност, аутентификација, отисак прста

Privacy Friendly Biometrics

Abstract: When the manhood began to count and measure, it was beginning of technology progress. Historical overview of the measurements of biometric data is extensive and demanding task. Consideration of the use of biometrics from ancient times to the present, a description of future trends, definitions and classification are part of the review of research. The second part is devoted to the dangers of information-controlled society, privacy, information privacy, its concepts and why it is needed, its legal framework and foundation. The third part is related to the suggestion scheme of use of biometric reading, not for potential endangering of privacy and freedom, but on the contrary, to protect these same values. The paper relies on previous achievements in the development of algorithms and technologies for fingerprint processing, cryptology, computer networks and their security, calls for the development of new and more sophisticated algorithms in order to achieve the objective - unconditional authentication with a hundred percent accuracy.

The essence of the paper is consideration scientifically known facts, but from a new perspective, that can bring many benefits to the human rights and freedoms, the implementation of legality (through efficient authentication), expenses reduction, organizational improvements, growth of index of satisfaction and happiness of man, and not least the avoidance dangers of totalitarian ideas through possible implanting electronic chips in the human body (as started long ago in the Western world), whose effects on humanity would be infinitely harmful.

Keywords: Biometrics, privacy, authentication, fingerprint

САДРЖАЈ

1	Увод.....	- 4 -
1.1	Предмет истраживања.....	- 4 -
1.2	Доприноси рада.....	- 5 -
2	Преглед у области истраживања	- 6 -
2.1	БИОМЕТРИЈА	- 6 -
2.1.1	Историја употребе биометрије.....	- 6 -
2.1.2	Историја употребе биометрије у Србији.....	- 13 -
2.1.3	Биометрија у Србији данас.....	- 16 -
2.1.4	АФИС	- 17 -
2.1.5	ИАФИС	- 21 -
2.1.6	АФИС – Интерпол.....	- 22 -
2.1.7	Нова генерација идентификационих система.....	- 22 -
2.1.8	Шта је заправо биометрија?	- 25 -
2.1.9	Врсте биометријских читавања.....	- 26 -
2.1.10	Био-морфолошки отисак прста човека.....	- 28 -
2.1.11	Класификација морфололошких облика папила.....	- 29 -
2.1.12	Класификација отисака прста	- 30 -
2.1.13	Људи без отисака.....	- 36 -
2.1.14	Биометријски отисци код животиња	- 37 -
2.2	ПРИВАТНОСТ	- 39 -
2.2.1	Појам приватности	- 39 -
2.2.2	Информациона приватност	- 40 -
2.2.3	Релативизација и добровољно одрицање од приватности	- 40 -
2.2.4	Критички поглед на технологију	- 41 -
2.2.5	Духовност и философија vs. биометрија.....	- 41 -
2.3	БИОМЕТРИЈА ПРИВАТНОСТИ	- 43 -
2.3.1	Аутентификација – опште информације.....	- 43 -
2.3.3	Биометријска аутентификација.....	- 43 -
2.3.2	Опозива биометрија	- 44 -
2.3.3	Системи биометријског шифровања	- 45 -

2.3.4 Неке слабости биометријских система.....	- 49 -
2.3.5 Предлози шема „биометрије приватности“	- 50 -
2.3.5.1 Услови функционисања система биометрије приватности.....	- 50 -
2.3.5.2 Предложена шема 1.....	- 51 -
2.3.5.3 Предложена шема 2.....	- 52 -
2.3.5.4 Предложена шема 3.....	- 53 -
3 Закључак	- 54 -
Литература.....	- 57 -
Списак слика	- 58 -
Списак табела.....	- 60 -
Списак шема.....	- 61 -

1 Увод

1.1 Предмет истраживања

Способност да се препознају одређене карактеристике окружења човека, била је кључ преживљавања. Од најранијих времена, човеку је било елементарно важно да препозна временске и географске услове, животиње и биљке и наравно да препозна људе. Како пријатеље тако и непријатеље. У цивилизовано време, оно није кључ преживљавања, али је кључ пословања и просперитета.

У савременом информатичком свету користе се неки појмови као што су идентификација, аутентификација, ауторизација... Дефинишимо за почетак те појмове кроз пример.

Замислимо да се срећете са непознатим човеком, било лично, било преко друштвених мрежа. Прво што ћете учинити (након поздрављања) је представљање. Рећи ћете: „Ја сам Марко Марковић...“ и тиме управо извршити процес идентификације. Када се то ради електронски, даје се неко корисничко име, број, неки јединствени идентификатор или слично. Следећи пут када се деси сусрет са истим човеком, доћи ће до процеса аутентификације, где ће човеков мозак покушати да позове сећање и утврди да ли сте то заиста ви. Ако га сећање служи, наставиће разговор са вама, не као непознатом, већ као према некоме кога већ познаје. Ако то учини, значи да је извршио вашу ауторизацију.

Изведимо дефиниције из овог примера:

Идентификација је процес у коме се врши „представљање“ појединца другом појединцу, групи или информатичком систему, путем одређених карактеристика појединца. Важно је да су те карактеристике јединствене, како би идентификација била несумњива.

Аутентификација је поступак који је повезан с идентификацијом, а њиме се утврђује да ли је особа заиста та којом се представља, препознавањем раније наведених (јединствених) карактеристика.

Ауторизација је процес дозвољавања комуникације и/или приступа систему или појединцу особе која је аутентификована.

Предмет истраживања овога рада су процеси који се тичу појмова идентификације, аутентификације и ауторизације уз помоћ биометријских карактеристика отиска прста. Посматраћемо већ познате алгоритме обраде тих карактеристика и разрађивати шему начина за конкретну примену досадашњих метода и већ познатих технологија како би покушали да дођемо до предлога за њихово коришћење.

Основна идеја-водиља ће нам бити очување и унапређење **приватности**, као вида човекове слободе.

1.2 Доприноси рада

Идеја за одабир теме је дошла је из потребе тј. покушаја демистификације и отклањања (умногоме оправданог) страха од нових технологија и губитка слободе. Аутор је био вођен питањем: „Ако је биометрија несумњиво један од светских информатичких трендова (не можемо је искључити), да ли постоји могућност за искориштавање њених карактеристика за очување (онога за шта је оптужују да уништава) – слободе?“

Постоје дакле, две димензије којима се бави овај рад, а то су:

- **биометрија и**
- **приватност**, која несумњиво јесте угрожена, како друштвеним трендовима који врше лажну трговину на рачун приватности, тако и нападима технолошки оспособљених појединаца и група.

Дакле, овај рад еволуира од зборника основних информација о појму и историјату биометрије, описа области и поделе биометрије (уз посебан осврт на отиске прстију).

Рад обрађује историјат биометрије у Србији, али такође и савремене тенденције у овој области. Процесом глобализације како настају нови изазови, тако се јављају и нове потребе за глобалним системом који овог момента иде само у смеру безбедности у исто време негирајући приватност. При томе се користе разне флоскуле типа „ја немам шта да кријем“, које нису ништа друго већ обичан мит, који ће овај рад покушати да демистификује.

Такође, у једном свом поглављу, истиче се важност развијања критичког погледа на развој технологије, посебно биометрије.

Куриозитет рада је предлог шеме на основу које би усавршавањем алгоритама могло доћи до система аутентификације пред службеним лицем уз очување приватности, због којег је рад и назван „Биометрија приватности“. Будући да је развој алгоритама веома обиман пројекат, шема која је централни догађај рада биће описана, објашњена а њен развој ће бити остављен неком тиму који би морао да има како финансијску, тако и друштвену (државну) подршку за њен развој, будући да би друштвене последице остварења шеме биле велике. Било би то унапређење и људских слобода и демократије, али и велика уштеда финансијских средстава државног буџета, кроз смањење бирократије и непотребних докумената.

Користећи метод дедукције, сагледавањем од општег ка појединачном, кроз овај рад долази се до конкретног предлога – шеме која сама по себи има нешто заједничко са сваком од поменутих радова, али напосто није њихова копија, већ је идеја примене оригинална.

2 Преглед у области истраживања

2.1 БИОМЕТРИЈА

2.1.1 Историја употребе биометрије

Човек као биће има онтолошку потребу за вечним. Примери пећинског сликарства из периода горњег палеолита (касног каменог доба), имају често и „потписе“ аутора. Они сведоче о потреби људи онога доба да се аутентификују, управо као и савремени човек. То су први примери коришћења биометријских карактеристика човека у те сврхе.



Слика 2-1- Отисак длана праисторијског човека на зиду пећине Шавé, јужна Француска

Тако у пећини Шавé (*fr. Chavet*)¹, у јужној Француској, можемо пронаћи неке од најранијих цртежа пећинског сликарства. Верује се да ти цртежи датирају око 31.000 година п.н.е.

У пећини Ел Кастиљо (*esp. El Castillo*)² у Шпанији, по процени изнетој у журналу „Сајенс“ (*eng. Science*), налазе се **најстарији примери** отисака длана у Европи, процењени на око 37.000 година п.н.е

¹ Photo: © Stéphane Compoint, <http://stephanecompoint.com>
<http://donsmaps.com/images28/handimprintsm.jpg>

² Photo: © Pedro Saura <http://www.voanews.com/content/ancient-cave-art-could-be-from-neanderthals/1211488.html>



Слика 2-2 - Отисак длана праисторијског човека на зиду пећине Ел Кастиљо, Шпанија.

Вавилонски трговци су (у периоду од 1900. п.н.е. па до пропасти царства 539.п.н.е.) помоћу отисака прстију потврђивали и бележили пословне трансакције, у циљу заштите од фалсификовања, уговорне стране су утискивале отисак прста у глинену таблу на којој је уговор написан. Стари Египћани су вршили мерења тела како би идентификовали неку особу.



Слика 2-3- Отисак прста у глини кориштен од Вавилонаца.

Отисци прстију су пронађени како на вавилонским глиним таблицама, тако и на печатима и грнчарији. Отисци су такође пронађени на зидовима египатских гробница и на минојској, грчкој и кинеској грнчарији, као и на циглама, цреповима из древног Вавилона и Рима. Неки су остављали отиске ненамерно, као последицу не толико педантне израде, а други су настали у процесу додавања декорације. Негде су отисци прстију су били утиснути тако дубоко у глину да се претпоставља да су служили као знак идентификације од стране произвођача .

Занимљиво је да су у доба Вавилонског краља Хамурабија (1792-1750 п.н.е.) узимали отиске прстију од људи који су прекшили закон, иако вероватно нису знали да су биометријске карактеристике сваког појединца аутентичне.

На **слици 2-4**³ налази се примерак буле (печата) из античког Рима негде између првог и другог века нове ере.



Слика 2-4 - Пример буле (печата), Римљана (са отиском прста)

До 246. п.н.е., кинески званичници су утискивали њихове отиске у печате од глинe које су користили за печатења докумената, а касније појавом свиле и папира, уговорне стране су утискивале њихове отиске на тим материјалима.

Нешто пре 851.г. нове ере, арапски трговац у Кини **Абу Заид Хасан**, у присуству кинеских трговаца помоћу отисака прстију посведочио је узети зајам (кредит). До 702.г. у Јапану је дозвољено неписменима који траже развод брака да га потпишу само "знаком" тј. отисцима прстију.

За време кинеске династије Ћин, отисци стопала као и отисци прстију су третирани као валидни докази у случајевима почињених злочина, а око 300.г. нове ере, отисци прста су били важећи у случајевима крађа.

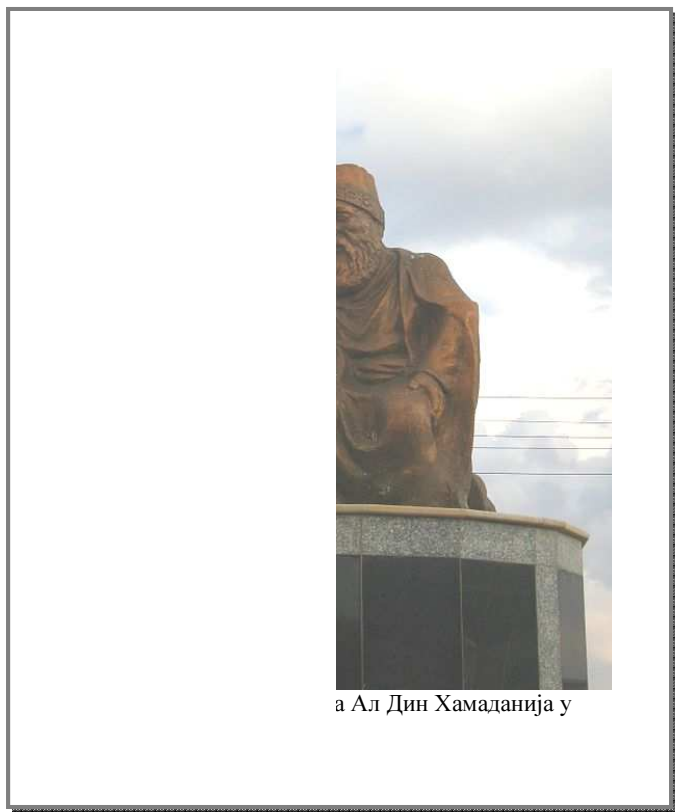


Слика 2-5– Кинески документ „потписан“ биометријским отиском

³<http://www.ancientresource.com/images/roman/bullae/bulla-bust119.jpg>

Из историјског извештаја првог великог португалског истраживача и историчара, **Жоаоа Де Бароса** (*Joao de Barros, 1496 –1570*) сазнајемо да су Кинези, користили отиске прста мастилом, на папиру како за пословне намене, тако и отиске дланова и стопала како би малу децу разликовали од друге деце.

Око 650.г. нове ере, кинески историчар **Киа КунгЈен** приметио је да би отисци прста могли бити кориштени као средство за аутентификацију људи.



а Ал Дин Хамаданија у

У својој књизи „Универзална историја (арап. *Jami al-Tawarikh*), персијски лекар **Рашид Ал Дин Хамадани**⁴ (такође познат као "Рашидедин", 1247-1318) извештава нас о кинеској пракси коришћења биометрије отиска прста у сврху идентификације појединаца, коментаришући: "Искуство показује да не постоје два појединаца који имају потпуно идентичне прсте“.

1684. године, енглески лекар и ботаничар **Немија Гру** (*Nehemiah Grew, 1641-1712*) је објавио први научни рад у коме описује структуру коже која покрива прсте и дланове.

Годину дана касније холандски лекар **Говард Бидло** (*Govard Bidloo, 1649-1713*) и

италијански лекар **Марчело Малпиги** (*Marcello Malpighi, 1628-1694*) објавили су књиге о анатомији коју су илустровали структуром гребена коже прстију.

Век касније, 1788. године, немачки анатом **Јохан Кристоф Андреас Мајер** (*Johann Christoph Andreas Mayer, 1747-1801*) је препознао чињеницу да су отисци за сваког појединца јединствени.

Професор анатомије, патологије и физиологије на Универзитету у Вроцлаву (*пољ. Uniwersytet Wrocławski*), **Јан Јеванђелиста Пуркиње** (*чеш. Jan Evangelista Purkyně*), је 1823. године, објавио своју тезу о 9 образаца отисака прстију, али није поменуо вредности отисака прстију за личну идентификацију.

Први Енглез који је почео да користи отиске је **Сер Вилијам Хершел** (*енг. Sir William Herschel*) јула 1858. године, када је као главни прекршајни судија округа Хугли (*енг. Hooghly*), у Индији, почео да користи отиске прстију на уговорима домицилног становништва. Не размишљајући у смеру ка личној идентификацији, Хершел је отиснуо длан локалног бизнисмена, на полеђини уговора.

⁴http://en.wikipedia.org/wiki/File:Rashid-al-Din_Hamadani.jpg

Његова идеја је била "...да (га) уплаши и одговори од свих помисли о одбацивању сопственог потписа." Тај „случај“ је постао пракса где је Хершел захтевао да се на сваком уговору мештана, на полеђини, понови исто. Касније, захтеван је отисак кажипрста и средњег прста.

Лични контакт са документом, је по веровањима домицилног становништва, био „више обавезујући, него да није потписан“. Дакле, може се рећи да је прва употреба „биометријског потписа“ била заснована не на науци, већ на сујеверју.

Временом, како је збирка отисака прстију расла, Хершел је почео да примећује разлике међу отисцима и чињеницу да је користећи се мастилом отиснутим прстом могуће доказати или оповргнути идентитет.



Слика 2-7 Аутопортрет (фотографија) Алфонса Бертилиона

1870.године, **Алфонс Бертилион** (*фра. Alphonse Bertillon*, 1853 – 1914)⁵, француски полицајац, истражује биометрију и уводи антропометријске методе у полицијску праксу, класификује и идентификује криминалце. Познат је као творац комбиноване полицијске фотографије (спреда, леви и/или десни профил) познатог као „магшот“ (*engl.mugshot*).

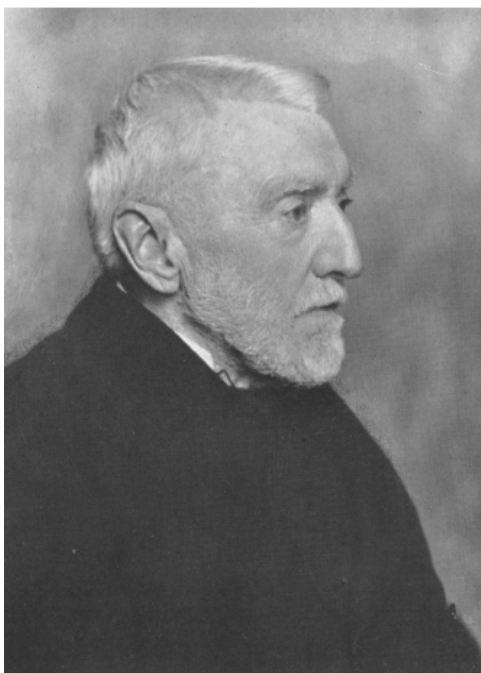
Током 1870-их, **др Хенри Фолдс**⁶ (*engl. Henry Faulds*) шкотски лекар, мисионар и научник, надзорник хирургије у болници Цукидзи (*jan. 築地*) у Токију, касних 70-тих година деветнаестог века се, сарађујући са својим америчким пријатељем, археологом Едвардом Морзеом (*engl. Edward S. Morse*) на ископавањима, први пут срео са утиснутим отисцима прстију на комадима поломљене грнчарије. То је био тренутак када се у његовом уму створила веза између отисака и њихове индивидуализације, он почиње да их проучава и препознаје не само значај отисака прстију као средства идентификације, него и осмишљава метод њихове класификације.

Фолдс је изумео метод коришћења мастила при бележењу отисака свих десет прстију на (класификационе, личне) картоне. Та колекција је постала непроцењиво важна када је полиција оптужила члана његовог медицинског особља за покушај провале, где се провалник попео уз болнички зид и ушао кроз прозор. Он је

⁵http://upload.wikimedia.org/wikipedia/commons/9/99/Bertillon_selfportrait.jpg

⁶ <http://galton.org/fingerprints/images/faulds-1920-08-27-thumb.gif>

упоредио отиске прста пронађене на зиду са отисцима прста на његовој картотеци и утврдио да отисци прста нису припадали осумњиченом члану особља. Схватајући да



Слика 2-8 Хенри Фолдс (engl. Henry Faulds)

отисци прста могу бити решење за идентификацију провалника, Фолдс је био одлучан у тврдњи да су отисци прстију тачан и поуздан начин за личну индивидуализацију. Да би доказао ову теорију, Фолдс је истраживао сталност и посебност отисака. Сакупљајући и поредећи на хиљаде отисака, утврдио је да су сви они били аутентични. Такође, да би доказао сталност папила, Фолдс и његови студенти медицине користили су различита средства: жилете, шмирглу, пловућац⁷, киселине, корозивне тј. нагризајуће материје и утврдили управо оно што су и претпостављали, да се папиларно ткиво (после оштећења) враћа у облик који потпуно одговара ономе пре изазивања оштећења.

Године 1880, свој систем класификације облика морфолошких карактеристика прста као и њихове цртеже уз објашњење, послао је сер Чарлсу Дарвину. Дарвин, у дубокој

старости и лошег здравља, обавестио др Фолдса да не би могао да му буде ни од какве помоћи, али је обећао да ће материјал проследити свом рођаку, Францису Галтону (који је по свему судећи „искористио“ рад Фолдса, а неко би то могао свакако да окарактерише уз помињање ауторских права). У научном свету још увек постоје контроверзе везане за ауторство над класификацијом

Свој рад је објавио у часопису Нејчер (engl. *Nature*) 1880.г. (Hutchins, 2011), у коме је разматрао идеје о коришћењу отиска прста као средства идентификације и предложио коришћење мастила као метод за њихово узимање. Фолдсу се приписује прва идентификација (масног) отиска прста на боци алкохола.

Године 1882, **Гилберт Томпсон** (енг. *Gilbert Thompson*) из америчког Геолошког института у Новом Мексику, користи своје отиске на документу како би спречило могуће фалсификовање. Ово је прва позната употреба биометријских отисака у Сједињеним Државама.

И у литератури **Марка Твена** (енг. *Mark Twain - Samuel L. Clemens*), 1883. године, у књизи „Живот на Мисисипију“ убица је идентификован коришћењем идентификације отиска прста. У каснијој књизи Марка Твена, "Ретардирани Вилсон", (енг. *Pudd'nhead (Pudding Head) Wilson*) дошло је до драматичног суђења на основу идентификације отиска прста. У новије време снимљен је и филм.

⁷Пловућац је лака, бела или сива, изванредно шупљикава и сунђераста стена вулканског порекла, порозности до 90%, која често може плутати по води, будући да у својој структури има мехуриће гаса заробљене у себи.

Званично признат први метод класификације отисака прстију је развијен од стране **Сер Френсис Галтона** (*engl. Sir Frensis Galton*), горепоменутог рођака Чарлса Дарвина (*engl. Charles Darwin*). Он је као неко ко је подржавао теорију еволуције и опстанак најјачих, један од твораца еугенике (уз Американца, Чарлса Девенпорта) која је доцније постала квазинаучна основа за покрет Адолфа Хитлера и идеју фашизма.

Ипак, истражујући наследне и расне карактеристике отисака прстију (али очигледно и радове Др Хенрија Фаулдса), он је успоставио прву класификацију образаца минуција прста која се користи и данас. То је учинио у часопису Краљевске Институције Велике Британије (*engl. Royal Institution Of Great Britain*), 1888. године, као и у три књиге 1892 - „Отисци прста“ (*engl. Finger Prints*), 1893- „Дешифровање замућених отисака прстију“ (*engl. Decipherment of Blurred Finger Prints*), и 1895 - „Категоризација отисака прста“ (*engl. Fingerprint Directories*).

Творац **дактилоскопије**, Хваранин, **Иван Вучетић**, са својих 26 година живота, 1884. године одлази у Аргентину, где се након четири године запошљава у полицији у Ла Плати.

Након проучавања Бертилионовог поступка идентификације и експеримената Сер Галтона, интензивно почиње истраживати и проучавати папиларне линије. Након што је проучио више постојећих метода за класификацију отисака прстију и уочио бројне недостатке, успоставио је сопствени систем за класификацију отисака прстију који је назвао **иконофалангометрија**.

1891. године Вучетић формира „**Регистар иконофалангометрије**“, где оснива прву десетопрстну збирку. Он успева да, применивши свој метод идентификације, разреши случај Франциске Ројас која је убила своје двоје деце, а затим „преклала“ сопствени врат како би оптужила љубавника за убиство. Вучетић је упоредио њене отиске прстију с крвавим отисцима прстију на дрвеном оквиру врата и утврдио њен идентитет као идентитет убице. Иначе, Вучетић је поред свога потписа увек остављао и отисак свога десног кажипрста. (Ivan Vučetić, 2013)

Године (1896), **Сер Едвард Хенри** (*енг. Sir Edward Richard Henry*) генерални инспектор полиције Бенгалу, почео је да користи Галтонов метод за биометријску идентификацију криминалаца. Хенри је створио свој метод разврстања отисака који омогућава њихово брзо претраживање. 1901. г. уводи се идентификација преступника у Енглеској и Велсу. Тако „**Хенријева класификација**“ бива усвојена у свим земљама енглеског говорног подручја.

1902. г. долази до прве системске употребе отисака прстију у САД, од стране Комисије државне службе Њујорка (*енг. New York Civil Service Commission*) за тестирање. **Др Хенри П. Дефорест** (*енг. Dr. Henry P. DeForrest*) представља америчког пионира у коришћењу биометријских отисака.

1903. године, Њујоршки државни затвор, почиње прво систематско узимање отисака прстију од криминалаца.

1904. године, Савезни затвор у Левенворту, у Канзасу (*енг. Leavenworth Federal Penitentiary in Kansas*), уз асистенцију представника Скотланд Јарда (*енг. Scotland Yard*), почиње да примењује биометрију.

Већ 1905. г. копнена војска САД (*енг. U.S. Army*), две године касније и морнарица (*енг. U.S. Navy*), а догодине и јединице мариначи (*енг. Marine Corp*)

почињу да користе биометријске отиске прстију. У наредних 25 година све више америчких служби безбедности је почињало исту праксу, а многи су почели да шаљу копије отисака у Национални биро криминалистичке идентификације (*енг. National Bureau of Criminal Identification - NCBI*)

Актом Конгреса САД, 1924. године, основано је одељење Федералног истражног бироа (*енг. Federal Bureau of Investigation - FBI*), а одељење у Левенворту формирано је као језгро базе биометријских података ФБИ-ја.

До 1946.г. ФБИ је ручно обрадио 100 милиона картица са отисцима, а до 1971. године – 200 милиона картица са отисцима. (Group, 1997-2006)

2.1.2 Историја употребе биометрије у Србији

1904. године, у Србији се при Министарству унутрашњих дела формира тзв. **антропометријско одељење**⁸. По угледу на француског полицајца Алфонса Бертилиона, 34 године касније и Србија уводи полицијске фотографије познате под именом „магшот“ (*engl.mugshot*), као и мерења и поређења одређених делова лица и тела, као и ожиљака, тетоважа и других личних карактеристика.



Слика 2-9 Аутентична историјска фотографија из криминалистичке евиденције српске полиције

Само седам година по оснивању антропометријског одељења, у Србији се полако прелази на **дактилоскопску регистрацију** (поменутог Ивана Вучетића) јер

⁸ Слика 2-8: http://www.vreme.com/g/images/1028938_Istorija_03.jpg



Слика 2-10 Др Арчибалд Рајс

су се дешавале грешке ако би два различита полицајца узимала мере осумњиченог. Тако је Србија пратила тадашње савремене трендове у биометрији (и форензици уопште).

Несумњиво најзначајнија личност у Србији која је немерљиво утицала на развој биометрије је човек кога је на почетку Првог светског рата, 1914. године, позвала влада Краљевине Србије - **др Арчибалд Рајс**⁹ (нем. *Rudolph Archibald Reiss*; Хаузах, Баден, 8. јул 1875 — Београд, 8. август 1929),

швајцарски форензичар, публициста, доктор хемије, професор на Универзитету у Лозани и један од пионира форензике да помогне у истраживању и документовању зверстава аустроугарске, немачке и бугарске војске над

српским цивилним становништвом.

Направио је преко 10.000 фотографија (везаних за I Св. рат), написао је многе књиге и радове поводом тога, а често је слао извештаје који су објављивани у угледном часопису неутралне Швајцарске, Газет (*фр. Gazette*). Тиме је као угледни професор и криминолог извештавао свет и кварио пропагандну слику Немаца и Аустроугара о Србима као дивљачком народу.

Рајс који је у то време био



Слика 2-11 Др Арчибалд Рајс: „Чујте Срби“



Слика 2-12 Урна Др Арчибалда Рајса на Кајмакчалану

познат стручњак, објавио је већ своју другу књигу о форензици „Приручник судске медицине: Крађе и убиства“ (*фр. Manuel de police scientifique (technique) : I. vols et homicides; Préface de Louis Lépine. Payot, Lausanne 1911.*), док је неколико година раније издао књигу Форензичка фотографија (*фр. La photographie judiciaire Beudel, Paris 1903.*).

Са српском војском је прешао Албанију, а после рата се вратио у Београд. Др Арчибалд Рајс, који је пре тога у Лозани основао Институт за техничку полицију и криминалистику, основао је и организовао

⁹ http://upload.wikimedia.org/wikipedia/commons/d/d2/Archibald_Reiss.gif

техничку полицију¹⁰ при Министарству унутрашњих послова нове државе по угледу на сличне установе у свету и опремио тада најмодернијом опремом. По мишљењу америчких истраживача, који су путовали по Европи циљно проучавајући овај вид полиције, тадашња криминалистичка техника је била на веома високом нивоу.

Др Арчибалд Рајс је заволео Србију, српског војника-сељака и српски народ и до краја живота остао у Србији. Чувена је његова књига „Чујте Срби“ (*фр. Ecoutez les Serbes!*)¹¹ у којој је на најотворенији, али и најискренији начин описао српску националну карактерологију и дао савет српском народу за будућност. Сви његови савети су и данас заиста актуелни. Преминуо је и био сахрањен на топчидерском гробљу у Београду, док је његово срце по његовој жељи однесено у урни¹² на Кајмакчалан, где је сахрањено заједно са осталим ослободиоцима Солунског фронта. Та урна је на жалост оштећена у Другом Св.рату приликом једном налета Бугарске војске. (Левентал, 1984.)

У међуратном периоду у Србији, поред Рајса посебно су се истакли руски емигранти Сергеј Трегубов и Александар Андонович. Трегубов је у Југославији годинама радио као криминалистичко – технички експерт у Техничкој полицији, док је за време свог живота у Русији основао неколико научно – техничких лабораторија за судске експертизе. Александар Андонович је био шеф Техничке полиције и са Трегубовим коаутор прве стручне књиге о криминалистичкој техници у домаћој



литератури, објављеној 1935. Године под насловом „Криминална техника“. (Национални криминалистичко технички центар) (forenzika-u-srbiji, 2012.)

¹⁰ [http://2.bp.blogspot.com/-](http://2.bp.blogspot.com/-NAqwSoHTWXI/Uvvp705O6QI/AAAAAAAAEAI/zq2oMuVHgeM/s1600/kt_lab_nekad-velika.jpg)

[NAqwSoHTWXI/Uvvp705O6QI/AAAAAAAAEAI/zq2oMuVHgeM/s1600/kt_lab_nekad-velika.jpg](http://2.bp.blogspot.com/-NAqwSoHTWXI/Uvvp705O6QI/AAAAAAAAEAI/zq2oMuVHgeM/s1600/kt_lab_nekad-velika.jpg)

¹¹ Слика 2-8: <http://www.politika.rs/uploads/editor/arcibald-rajs-cujte-srbi.jpg>

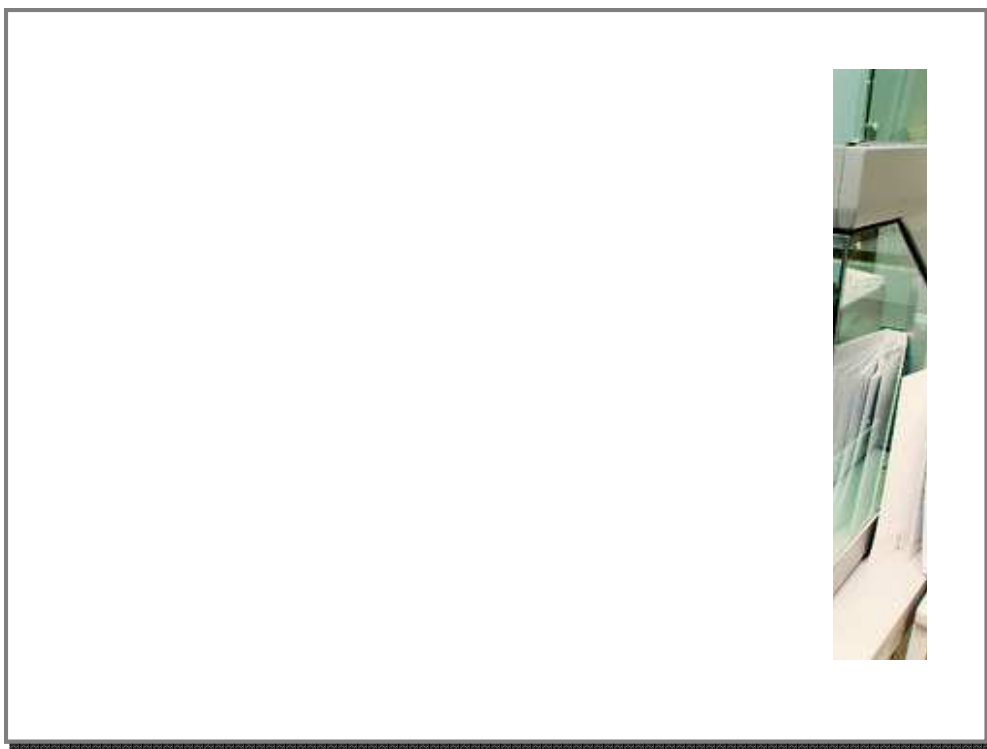
¹² http://upload.wikimedia.org/wikipedia/commons/thumb/f/f2/Sv._Petar_na_Kajmak%C4%8Dalan_%282%29.jpg/200px-Sv._Petar_na_Kajmak%C4%8Dalan_%282%29.jpg

После Другог светског рата техничка полиција постала је Биро за криминалистичку технику, који је прерастао у Криминалистичко-технички центар па у данашњи Национални криминалистичко-технички центар (НКТИЦ) у коме ради око 130 стручњака. (Видић, 2012), (Димитријевић, 2014.), (Џодан, 2014) (Зарић, 2014)

2.1.3 Биометрија у Србији данас

На темељима криминалистичке технике, које је поставио др Арчибалд Рајс са својим сарадницима, у Министарству унутрашњих послова Републике Србије данас постоји **Национални криминалистичко – технички центар**¹³, који под окриљем Управе криминалистичке полиције (УКП) суштински представља референтну установу у земљи за послове криминалистичке технике.

Данас постоје разне асоцијације на пољу рада криминалистичке технике. Једно од важнијих удружења те врсте је ENFSI (*European Network of Forensic Science Institutes*). Од априла 2009 године НКТИЦ је пуноправни члан ЕНФСИ-а.



У оквиру НКТИЦ-а се налази више лабораторија које су опремљене најсавременијим апаратима и уређајима уз помоћ којих се обавља велики број ДНК, судско-медицинских, биолошких, токсиколошких, балистичких, форензичких анализа и вештачења, као и вештачења пожара, експлозија и хаварија, докумената и рукописа, гласа и аудио записа. (Национални криминалистичко технички центар)

Током деведесетих у НКТИЦ је врло мало улагано, а форензика је за то време у свету брзо напредовала. После 2000.године НКТИЦ је био у центру пажње међународних институција и донатора, па смо захваљујући томе, и захваљујући

¹³ <http://static.politika.co.rs/uploads/rubrike/217034/i/1/dnk-2.jpg>

квалитетном кадру и препознатљивости, покренули међународну сарадњу и бројне иницијативе. Захваљујући томе, сада се примичу европском нивоу по врсти, квалитету и броју вештачења.

Захваљујући међународној сарадњи, али и делом домаћим средствима, у НКТИЦ од 2007. постоји ДНК лабораторија, једна од најсавременијих у Европи. (Видић, 2012)

Такође је захваљујући страним донацијама покренута изградња регионалних форензичких центара у Нишу, Новом Саду, а у Ужицу је отворен најсавременији Форензички центар на Балкану, и први у Србији са испуњеним стандардима за европску акредитацију. Направљена је и лабораторија за вештачење гласа, такозвана аудио-форензика, као и токсиколошка лабораторија која ових дана почиње са радом.

Ужички форензички центар једини има америчку, немачку, руску и британску опрему најновије генерације. (Н.Јанковић, 2013)

Новим технологијама попут система АФИС, по тврдњи надлежних особа у МУП-у Србије, удвостручен је број откривених криминалаца.¹⁴

Србија иначе има збирку око 200.000 регистрованих починилаца кривичних дела. Њихови отисци заједно са фотографијом и основним личним подацима ушли су у ту базу на основу одобрења суда. (Видић, 2012)

2.1.4 АФИС¹⁵

Пре индустријске револуције (у САД) и масовних миграција у градове, становништво је живело у руралним срединама где су се сви познавали и где је било мало потребе за идентификацијом. Тада, није било много полиције, није било много затвора, уз веома мали број судова. Како су градови постајали пренасељени, стопа криминала је расла, а криминал цветао у мору анонимности. Новине су са слашћу подизале тираж причама о безакоњу, законодавци су убрзо одговорили оштријим казнама (посебно за преступнике-повратнике), а полицијске управе су оптерећене обавезом идентификовања и хапшења преступника.

Системи идентификација названи „галеријама битанги“, антропометрија, Бертилионови портрети (*fra. „portrait parlé“* - портрет говори), на енглеском названи магшотовима и Хенријев систем - појавили су се и брзо проширили широм света у крајем 19. и почетком 20. века.

Касних 1960-их и раних 1970-их смо били сведоци периода грађанских немира и раста стопе криминала без преседана, у исто време, овај период се поклапа се са изумом и развојем силиконског чипа.

Наслеђени изазови у системима за идентификацију су захтевали нова решења, аутоматизовану обраду (и биометријских) података, и тако је настао **Аутоматизовани систем за идентификацију отисака – АФИС** (*енг. Automated Fingerprint Identification System - AFIS*).

1924. г. по овлашћењу Сенатске конгресне комисије САД за доделу средстава (*енг. The United States Senate Committee on Appropriations*) са рачуна Министарства правде (*енг. Department of Justice*) одобрена су средства за формирање Одељења за идентификацију у оквиру Федералног истражног бироа - ФБИ (*енг. Federal Bureau of Investigation - FBI*).

¹⁴ http://www.b92.net/info/vesti/index.php?yyyy=2006&mm=10&dd=21&nav_id=216384

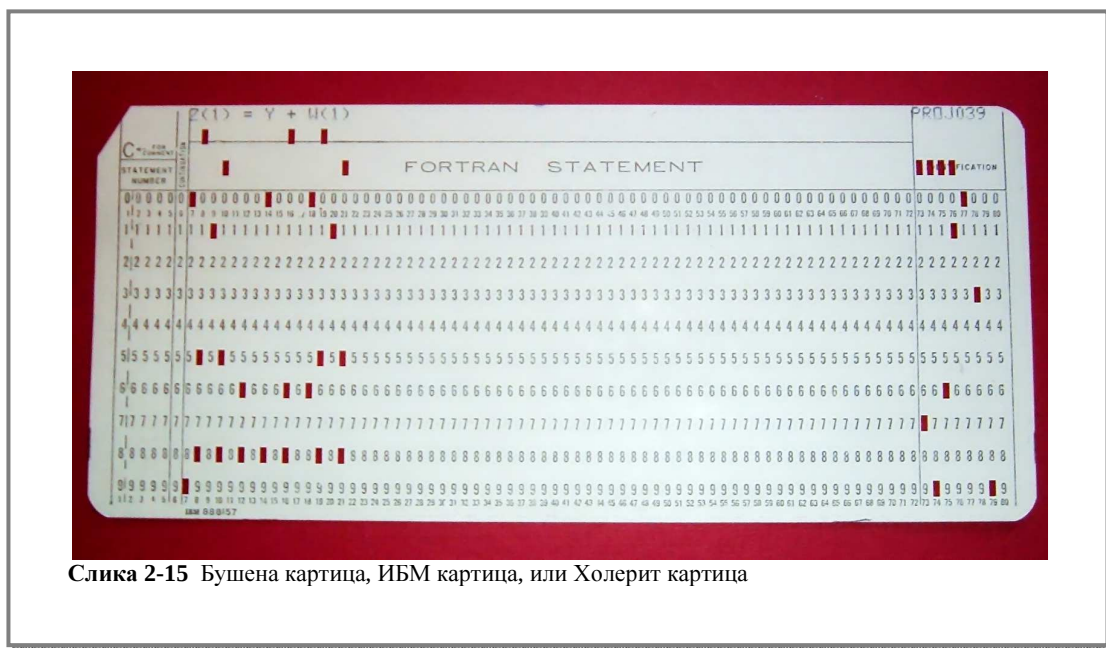
¹⁵ (Kenneth R. Moses, Peter Higgins, Michael McCabe, Salil Prabhakar, Scott Swann, 2004)

Одељење за идентификацију је формирано због потребе да се обезбеди Централни регистар података за идентификацију криминалаца, за службе безбедности (*eng. law enforcement agencies*) широм САД. Оригинална (почетна) колекција је имала 810,188 докумената, а после тога су додаване стотине хиљада докумената годишње, да би раних 1960-тих година база података ФБИ-ја садржавала податке о 15 милиона људи. Ово је био само додатак бази података грађана (некажњаваних) која је бројала 63 милина докумената, који су углавном прикупљени из војних извора из II Св. рата као и рата (САД) у Кореји.

Скоро сви кривични досијеи 15 милиона људи (из базе података Одељења за идентификацију ФБИ-ја) садржавали су 10 отисака по картици са укупно 150 милиона појединачних отисак прстију. Сви нови криминални досијеи су ручно сврставани (по Хенријевом систему) и претраживани, са отприлике 30.000 претрага дневно. Потреба за временом и људским ресурсима да би се извео дневни обим посла расла је континуирано.

Како би нека картица ушла у систем, сваки отисак прста би био сврставан у групе типова отисака, а продуктивност техничара је била око 100.000 картица на сат. Комплетно сврставање и претраживање огромне количине досијеа би било завршавано са 3,3 картице по запосленом на сат. Јасно, потребе за ресурсима за претраживање су стално расле.

Временом су додаване класификационе подгрупе како би се смањила количина криминалних досијеа које је било потребно претражити. Упркос томе, ручни систем



Слика 2-15 Бушена картица, ИБМ картица, или Холерит картица

претраживања достигао је тачку у којој ће бити немогуће обавити дневни обим посла.

Иако су „бушене картице“¹⁶ ИБМ-а (Бушена_картица, 2014)¹⁷ могле да смање број захтева за преглед обрасца отиска и осталих параметара, ипак је било

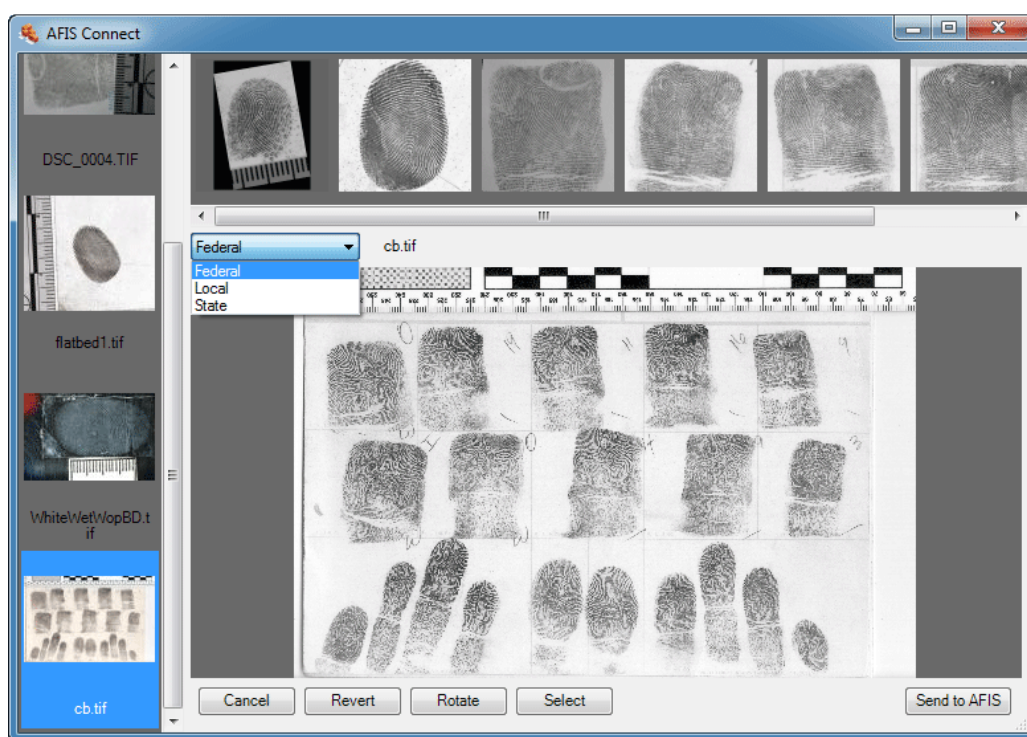
¹⁶ http://en.wikipedia.org/wiki/Punched_card#mediaviewer/File:FortranCardPROJ039.agr.jpg

¹⁷ Бушена, ИБМ или Холерит картица је картица од тврдог папира који садржи дигиталне информације на основу присуства или одсуства рупа на картици. Бушене картице су биле широко распрострањене у 19. веку за контролу текстилних разбоја. Биле су коришћене у 20. веку за снимање, обраду и чување података.

неопходно ангажовати људски фактор за испитивање сваке појединачне картице са листе потенцијалних кандидата.

Због свега овога, била је потребна потпуно нова парадигма при решавању проблема који ће зауставити даљи раст потребних људских ресурса за обраду захтева претраге. Био је потребан нови аутоматизовани приступ издвајања појединачног отиска прста са картице (која садржи десет отисака), њихова појединачна обрада како би се издвојио карактеристичан али редуковани (не детаљан) образац отиска прста, и претрага базе података која за резултат има веома смањену листу потенцијалних кандидата подударња (отиска).

Раних 1960-тих година потекла је иницијатива од стране америчког **ФБИ-ја, Канцеларије унутрашњих послова**¹⁸ Уједињеног Краљевства (*eng. Home Office in the United Kingdom*), **Париске полиције** (Француска) и **Јапанске националне полиције** да се развије аутоматизовани систем за идентификацију отисака. Суштина ове иницијативе је била намера да се у сортирање, претрагу и поређење отисака



Слика 2-16 Рач. интерфејс за приступ ИАФИС-у, фирме Фори технолојис (Foray Technologies)

прстију укључе рачунари.

До 1963. године, специјални агент ФБИ-ја, Карл Волкер (*eng. Carl Voelker*), закључује да ће ускоро доћи до колапса система ручног претраживања и у покушају решавања тог проблема обраћа се инжењерима Националног института за стандарде и технологију - НИСТ-а (*eng. National Institute of Standards and Technology - NIST*), Рејмонду Муру (*eng. Raymond Moore*) и Џоу Вегстајну (*eng. Joe Wegstein*) за помоћ у решавању тог проблема.

¹⁸ **Канцеларија унутрашњих послова** (*енгл. Home Office*) је министарско одељење Владе Уједињеног Краљевства, одговорно за имиграцију, безбедност, ред и закон. (Home Office, 2014)

Након проучавања проблема везаног за ручно поређење отисака прста, они закључују да ће бити потребно развити пре свега, скенер који ће моћи да скенира (дигитализује) постојеће отиске узете мастилом на картону. Друго, било је потребно прецизно и доследно идентификовати папиле на скенираним сликама и треће, морао се развити систем поређења минуција да би се могло утврдити да ли је отисак прста дошао од стране исте особе.

Развијање технологије скенера је ускоро успешно завршено, а иницијални алгоритам за поређење минуција се приписује Џоу Вегстајну (у радовима 1968-1982).

Након неколико година, 1974. године, са фирмом „Роквел интернешнал“ (*eng. Rockwell International*) склопљен је уговор за производњу прототипа за аутоматско претраживање отисака названог Фајндер (*eng. finder* – налазач). Ови читачи су испоручени ФБИ-ју 1975-1976. године и у следеће три године дигитализовали су 15 милиона картица отисака.

Средином седамдесетих година, Канцеларија унутрашњих послова Уједињеног Краљевства је развила читач способан да открије папиле, њихову позицију и оријентацију, да их изброји и одреди пет најближих суседних тачака сваког гребена десно од сваке папиле. То је била прва употреба бројања папила од стране АФИС система.

Из године у годину, АФИС систем се постепено ширио подржан технолошким напретком.

Америчка компанија **НЕЦ АФИС** (*NEC AFIS*)¹⁹ која је апсолутно водећа у свету АФИС технологије, на свом сајту износи податке како:

- 1 у својим базама података има преко 60 милиона биометријских записа,
- 2 дневно обавља пола милиона трансакција претрага,
- 3 обавља више претрага него сви остали системи заједно
- 4 њихови системи се налазе у многим земљама: САД, Канада, Мексико, Јапан, Кина, Тајван, Шпанија, Сингапур, Чиле, Ел Салвадор, Ангола, Аргентина, Бразил, Гренада, Индонезија, Намибија, Нови Зеланд, Филипини, Јужна Африка, Тајланд, Турска, Еквадор и Индија.

На светском тржишту се појављују бројне компаније (пored НЕЦ-а), које производе АФИС технологију, како софтвер тако и хардвер, као што су: „3МTM КАФИС“ (*3MTM CAFIS*), „Биолинк АФИС“ (*BioLink AFIS*), Марплес (*MarPless*) и др.

Најпознатије предузеће у Србији, које се бави биометријом је ЗК Софтвер²⁰ (*ZK Software*) из Београда.

У Руској федерацији, интензивна имплементација АФИС система се везује за период између 2002 – 2009. године и „Закон о националном упису отисака“. У срцу свих највећих аутоматизованих база отисака прстију и длана налази се руска ИТ компанија **АФИС Папилон Системс** (*AFIS – Papillon Systems*). На слици 2-17²¹ видимо како изгледа кориснички интерфејс система Папилон.

За тако кратко време, анализа биометријских података отисака прста и длана помогла је Министарству унутрашњих послова Русије да реши преко 500.000 случајева криминалних радњи.

Према подацима Папилон Системса, АФИС – Папилон база у Руској федерацији броји преко 55 милиона досијеа са десетопрстним отисцима.

¹⁹ <http://www.necam.com/Biometrics/doc.cfm?t=WorldwideDeployment>

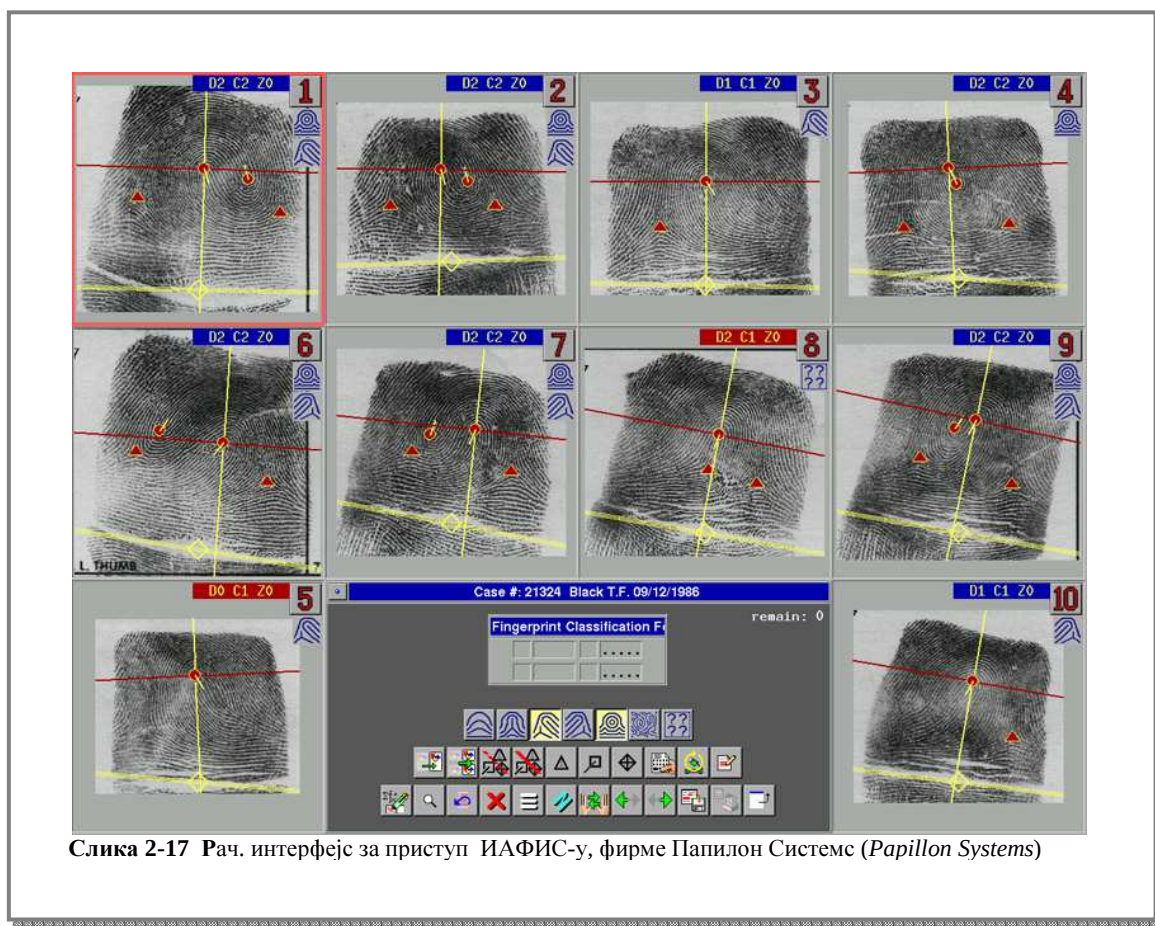
²⁰ http://www.zksoftware.rs/detail_zkteco_404.html

²¹ [Papillon%20AFIS%20presentation.pdf](#)

Инсталирани систем у Казахстану има базу од 3 милиона досијеа са десетопрстним отисцима, док систем у Абуџи (Нигерија) има базу са милион десетопрстних досијеа. У Даки (Бангладеш), Улан Батору (Монголија) и Тирани (Албанија) у Научном полицијском институту, постоје базе података са по 500.000 десетопрстних досијеа, а тврди се да је та компанија инсталирала системе у 22 земље.²² (Systems, 2010)

2.1.5 ИАФИС

28. јула 1999. у САД се формира **ИАФИС - Интегрисани аутоматизовани систем за идентификацију отисака** (Слика 2-17)²³ (IAFIS - Integrated Automated



Слика 2-17 Рач. интерфејс за приступ ИАФИС-у, фирме Папиљон Системс (Papillon Systems)

Fingerprint Identification System) који представља највећу светску базу биометријских података законских преступника, са досијеима за више од 70 милиона субјеката, (укључујући више од 73.000 познатих и осумњичених терориста) и са више од 34 милиона отисака цивила. (iafis)

У америчком ИАФИС-у, (по подацима изнетим на званичном сајту ФБИ-ја)²⁴, поред биометријских отисака прстију, чувају се и други подаци везани за криминалну историју појединаца као што су полицијске-магшот фотографије, подаци о боји косе и очију, надимцима, фотографије тетоважа и ожиљака, као и подаци о цивилним лицима (која немају криминалну прошлост), а која су углавном

²² <http://www.papillon.ru/eng/14/>

²³ http://t3.gstatic.com/images?q=tbn:ANd9GcSKqAmWWLTqFefNsEcZd5N1VOY-Th9ik5X_Or1-3bkGtANe9vv4hg

²⁴ http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

служила или служе у америчкој војсци или државним институцијама, као и подаци које су им добровољно доставиле државне, локалне или федералне службе безбедности. (iafis)

Просечна брзина одзива система на отисак осумњиченог за криминал поднет на поређење и анализу је око 27 минута, док је одзив у случају цивила око сат и 12 минута. ИАФИС је у 2010. години обрадио више од 61 милион десетопрстних досијеа. (iafis)

Треба рећи да многе земље имају интерни АФИС систем и нису у ИАФИС-у.

2.1.6 АФИС – Интерпол

Интерпол (*Interpol*) је највећа светска интернационална полицијска организација са 190 земаља чланица, која ове 2014. године слави јубилеј - 100 година међународне полицијске сарадње. То је организација која покушава да олакша полицијску сарадњу чак и међу земљама које немају успостављене дипломатске односе и функционише у границама постојећих закона у различитим земљама и у духу Универзалне декларације о људским правима. Устав Интерпола забрањује „било какву интервенцију или активности политичког, војног, верског или расног карактера“



Слика 2-18 Лого Интерпола

Интерпол (Слика 2-18)²⁵ има седам регионалних канцеларија широм света и представништво у Уједињеним нацијама у Њујорку и у Европској унији у Бриселу, а Генерални секретаријат Интерпола се налази у Лиону, у Француској, и ради 24 сата дневно, 365 дана у години. У свакој од 190 земаља Интерпола постоји Национални централни биро у коме раде високо обучени службеници за спровођење закона.

За потребе сопствених активности, Интерпол поседује 198.000 досијеа отисака прстију, закључно са децембром 2013.г. Свака национална организација Интерпола има право на приступ, преглед и поређење базе података преко глобалног (и сигурног) полицијског система “I-24/7”, који користи АФИС технологије.

Овлашћени корисници могу, готово тренутачно, да претражују и проверавају податаке са директним приступом базама података о осумњиченим криминалцима или тражених лица, украдених и изгубљених путних исправа, украдених моторних возила, отисака прстију, ДНК профила, украдених административних докумената и украдених уметничких дела. (Overwiev, Data-exchange, Databases, Forensics, 2014)

2.1.7 Нова генерација идентификационих система

По најави ФБИ-ја на неопширној страници званичног сајта²⁶, лета ове 2014-те године (тренутно је у току), очекује се следећа генерација система за идентификацију која ће наследити ИАФИС, а за коју кажу да ће бити „квантни скок“

²⁵ <http://www.svet.rs/wp-content/uploads/2014/02/Interpol-Logo-610x761.jpg>

²⁶ http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

у односу на ИАФИС. Систем је назван **НГИ - Следећа генерација идентификације** (*NGI - Next Generation Identification*), а шта он заправо носи са собом, то ћемо тек сазнати у будућности. Међу циљевима система се помињу:

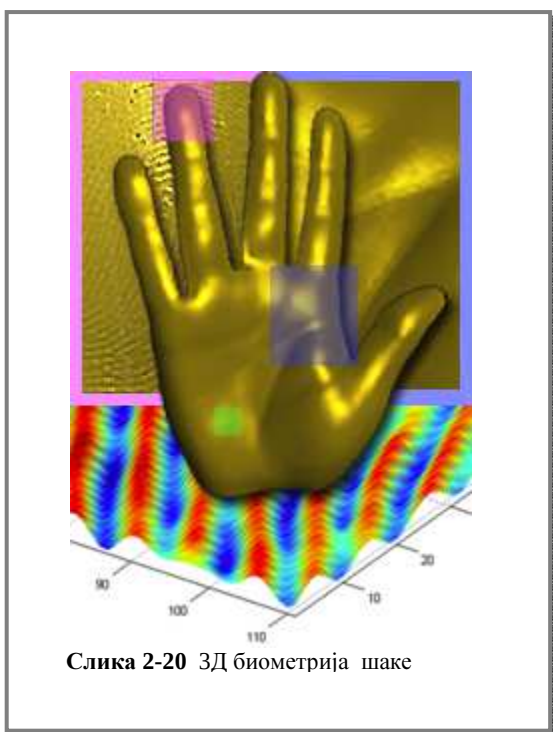
- 5
- 6 **Јавна безбедност и национална сигурност**
- 7 **Лидерство у биометрији**
- 8 **Побољшања ефикасности система**
- 9 **Приватност и заштита података**
- 10 **Мека транзиција**

Систем би требало да олакша рад око 18.000 америчких безбедносних агенција. О озбиљности идеје сведоче подаци да је извођач студије пројекта, америчка фирма Интелидајн (*eng. IntelliDyne*), у сарадњи са ФБИ-јем, консултовала 193 агенције представљене са преко хиљаду консултованих појединаца, а везано за

концептуалне захтеве будућних корисника система и „вишемилионски буџет“, а чувена хај-тек фирма Локид-Мартин (*eng. Lockheed Martin*), руководила је развојем пројекта.²⁷

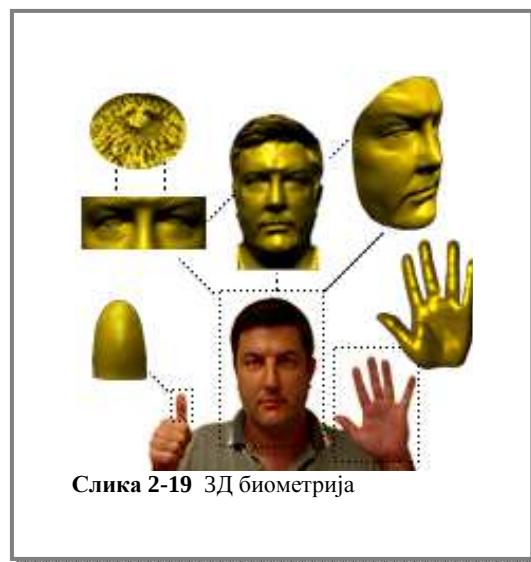
Несумњиво је да је систем заснован на биометрији како отисака прстију, шаке, ириса, мултимодалној биометрији, али надасве и на биометријском видео надзору и систему за препознавање лица.

Да ли ће бити искориштене технологије попут оне у којој је лидер америчка компанија Фотон ИКС (*eng.*



Слика 2-20 3Д биометрија шаке

Photon X) која је далеко отишла у видео надзору и 3Д биометрији?²⁸ Овога момента они поседују технологију која у року од секунде, са раздаљине преко 3 метра (без додира) може да прикупи биометријске податке свих прстију појединачно укључујући длан²⁹, док се развија могућност да то врши са још веће даљине.



Слика 2-19 3Д биометрија

²⁷ http://en.wikipedia.org/wiki/Next_Generation_Identification

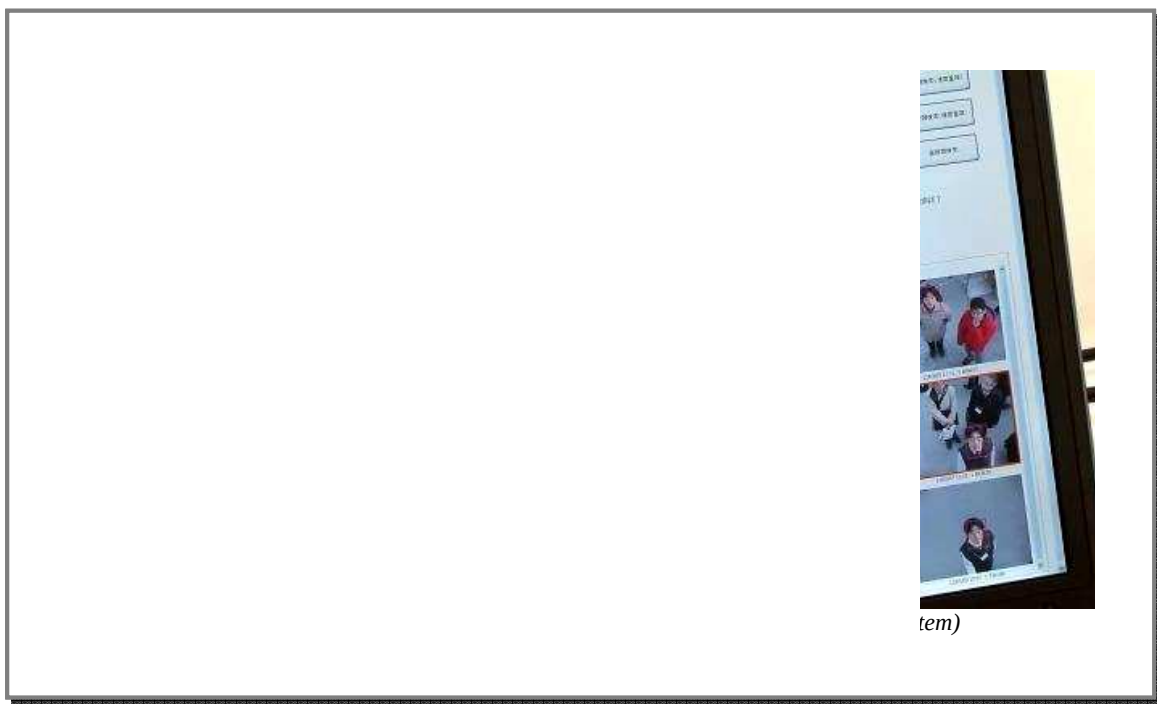
²⁸ <http://www.photon-x.com/images/Full-Bio-Set-Steve-small-fr.jpg>

²⁹ <http://www.photon-x.com/images/Full-Bio-Case-Print.jpg>

На сајту фирме Фотон Икс налази се демонстрација С.А.Ф.Е. – Система за даљинско издвајање отисака прстију (*S.A.F.E. - Standoff Automatic Fingerprint Extraction*), тј. промотивни видео снимак аутентификације са удаљености од око пола метра³⁰.

Овако прикупљени подаци су оцењени као "одлични", мерено НИСТ-овим³¹ НФИКу алгоритмом (*NIST NFIQ*), и када се упореде са истим отисцима прстију, али узетим другим НИСТ-овим алгоритмом (*BOZORTH3*) отисци прстију имају веома високу прецизност.

Са друге стране Пацифика у Јапану, фирма Хитачи (*Hitachi Kokusai Electric*) је 2012. године промовисала свој нови систем за видео надзор³² који је у стању да у року од једне секунде упореди снимљено лице са 36 милиона лица у бази података.



Хитачијев софтвер је у стању да препозна лице са до 30 степени одступања окренуто вертикално и хоризонтално од камере, уз захтев да фотографија лица има резолуцију од најмање 40x40 пиксела за тачно препознавање. (Веа, 2012)

Било која фотографија, узета преко мобилног телефона, „залеђеног“ видео снимка може бити претражена у бази података. Сличну технологију већ користи компанија Гугл (*Google*), као апликацију за мобилне телефоне под именом Гугл-гоглс (*Google Goggles*)³³ развијеној на Андроид платформи.

На слици 2-22³⁴, можемо видети како изгледа поступак идентификације преко мобилног телефонског апарата и апликације Гугл-гоглс. Корисник фотографише

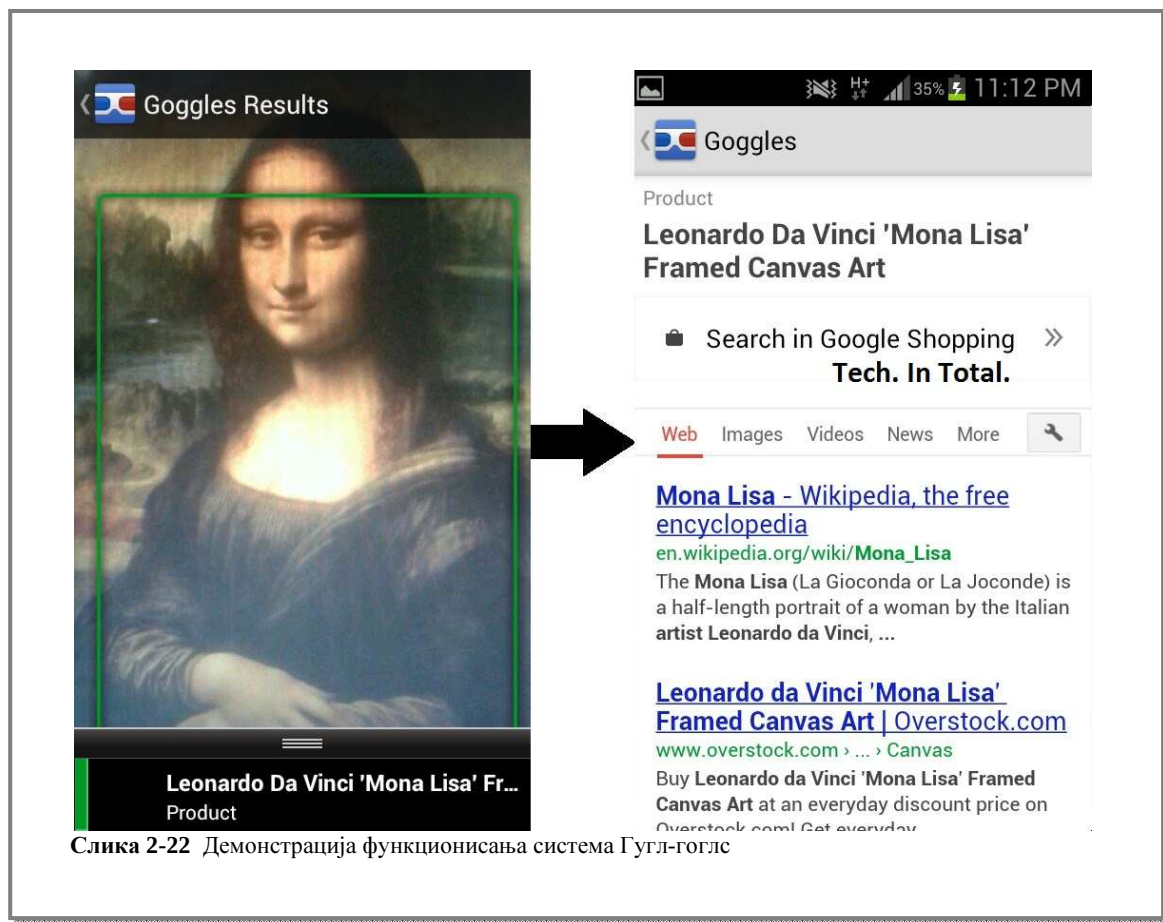
³⁰ <http://www.photon-x.com/flash/safe.html>

³¹ **НИСТ** - Национални институт за стандарде и технологију (енг. *National Institut of Standards and Technology*) је главна метролошка установа у САД, односно истраживачка агенција која дјелује у оквиру федералног Министарства трговине.

³² Image: DigInfo: http://images.gizmag.com/gallery_lrg/hitachiface.jpg

³³ http://en.wikipedia.org/wiki/Google_Goggles

³⁴ <http://1.bp.blogspot.com/-tYayRzc-1rM/UaDPNs3AO-I/AAAAAAAAABcA/DEti6PVbWiU/s640/4.jpg>



Слика 2-22 Демонстрација функционисања система Гугл-гоглес

објекат (у овом случају слику Мона Лизе, чувеном експонату из музеја Лувр), и за кратко време систем одговара чланком на Википедији у коме се описује о чему се ради. На овај начин могуће је затражити идентификацију и биљака, животиња, предела, предмета и људи...

2.1.8 Шта је заправо биометрија?

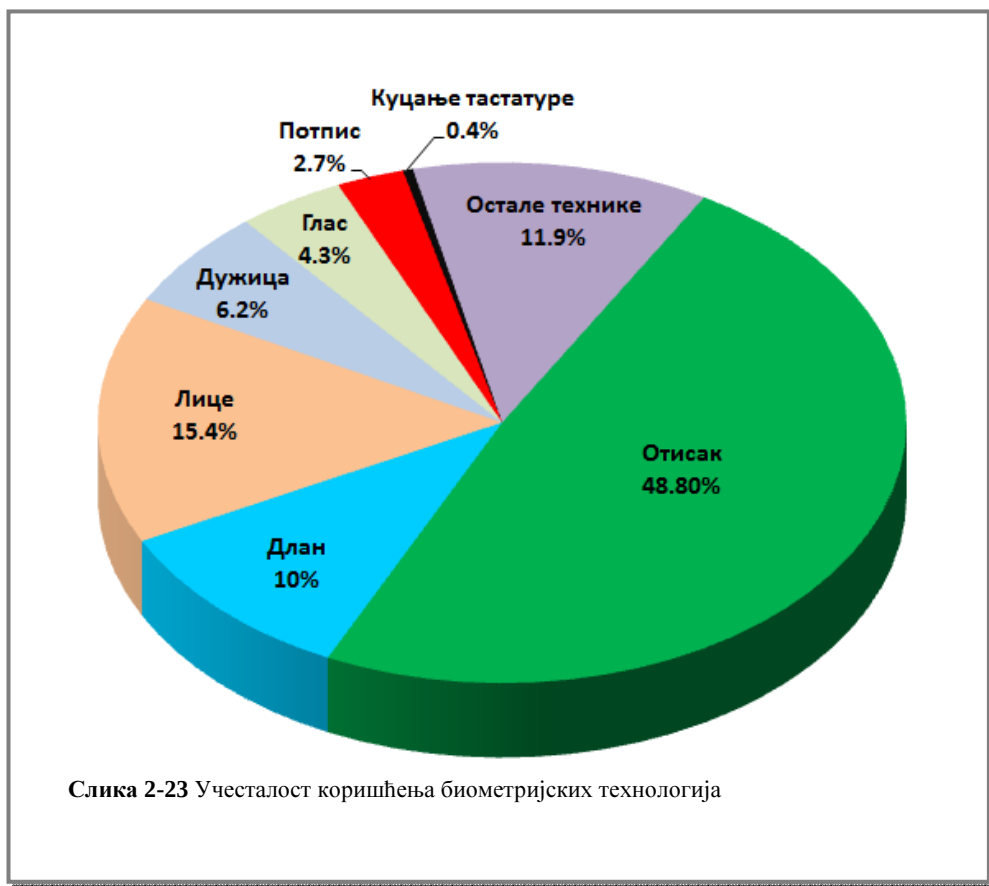
Реч „**биометрија**“ води порекло од грчке именице „биос“ - живот (*грч. βίος*) и глагола метрео – мерити (*грч. μετρέω*). Етимологија речи говори да је реч о мерењу одређених особина неког организма, а америчка Национална безбедносна агенција (*National Security Agency – NSA*) користи следећу дефиницију: „Биометрија је општи термин за опис и мерење физичких и/или понашајних карактеристика који може бити коришћен за аутоматско препознавање.“

Дакле, биометријски систем омогућава метод аутоматизованог препознавања заснованог на личним карактеристикама појединца. Користи се најчешће у контроли приступа заштићеним физичким објектима (лабораторијама, пословним зградама, банкама, апаратима за исплату готовине и др.) или одређеним виртуалним ресурсима као што су лични рачунарски налози, заштићени електронски документи и сл.

2.1.9 Врсте биометријских читавања

Различитост биометријских извора је огромна, како са аспекта технологије која се употребљава при мерењу и анализи, тако и по деловима тела и динамици при мерењу. Неки од предмета биометријског читавања су:

- Глас
- Отисци прста, длана
- Облик длана
- Васкуларни снимак ока, длана
- Дужица (ирис) ока
- Облик усне, лица, ушне шкољке
- ДНК
- Гестикулација
- Ход
- Потпис
- Термограм
- Рентгенски снимци (тела, вилице и зуба...)



Учесталост коришћења биометријских технологија³⁵ говори да је отисак прста несумњиво највише коришћен метод узимања биометријских података.

Због бројности биометријских извора, могуће је извршити и бројне поделе биометријских читавања, у зависности од угла посматрања.

Биометријска читавања са аспекта близине мерења/читавања, могу бити:

- **Контактна (отисак прста)**
- **Бесконтактна:**
- **Изблиза (снимак дужице, фотографија)**
- **На даљину (видео надзор)**

Са аспекта утицаја на човеков организам и ткива, она може бити:

- **Инвазивна (рентгенски снимак, узорак днк)**
- **Неинвазивна (фотографија)**

Са аспекта чулности читавања:

- **Тактилна (нпр. отисак прста)**
- **Аудио (снимак гласа)**
- **Визуелна (фотографија)**
- **Термичка (термограм)**
- **Микробиолошка (ДНК)**
- **Графолошка (потпис)**

Са аспекта статике и кретања:

- **Статичка (снимак дужице, отисак прста)**
- **Динамичка (видео снимак хода, покрети тела)**

Са аспекта потребе за сарадњом са објектом читавања:

- **Кооперативна (отисак прста)**
- **Некооперативна (фотографија, видео надзор)**

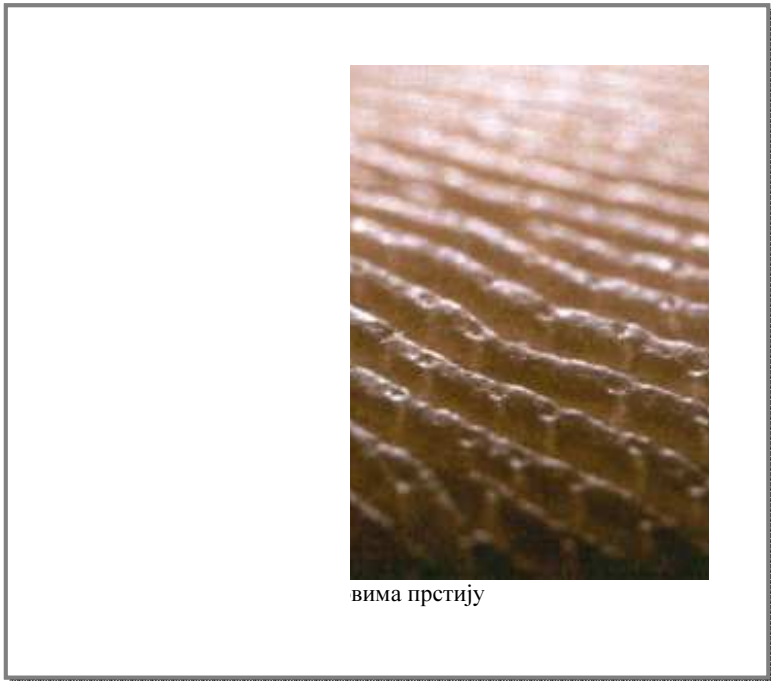
Са аспекта употребе биометријских информација:

- **Пословна (банке, е-пословање...)**
- **Безбедносна (безбедносне службе...)**

³⁵<http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2006-09-167.pdf>

2.1.10 Био-морфолошки отисак прста човека

Логично је запитати се одакле човеку шаре на длановима и стопалима. Професор на Болоњском универзитету (Италија), Марчело Малпиги (*Marcello Malpighi*, 1628-1694) италијански лекар, биолог и отац микроскопске анатомије и хистологије је у својим радовима описао карактеристике спирале, петље и гребена



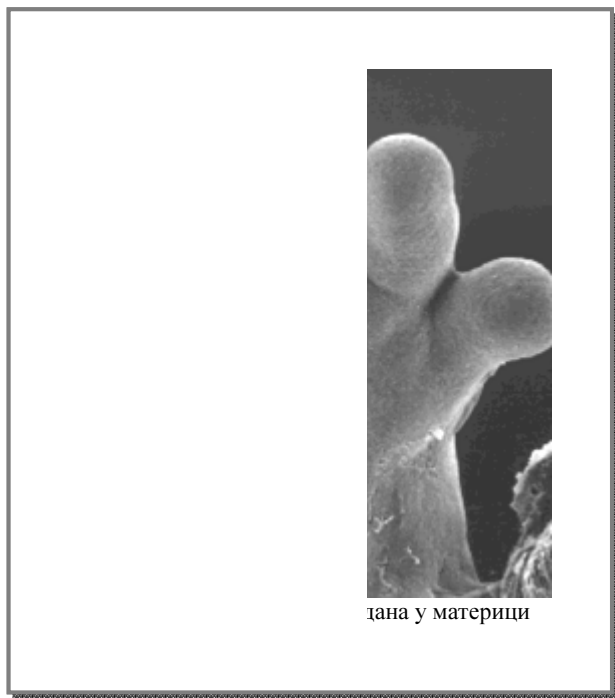
вима прстију

отисцима прстију, користећи тада новоизумљени микроскоп за своје студије. Иако никада није напоменуо вредност прстију као идентификационих алата, дао је велики допринос хистологији, а слој коже (дебљине 1,88 mm) назван је по њему „Малпигијев слој“.

Називи за „шаре на прстима“ који се могу наћи у литератури су бројни. Најчешћи су **бразде, папиле (квржице) или минуције** (Слика 2-24)³⁶.

Папиле настају још у пренаталном периоду, тачније у ембрионалној фази развоја (6-7 недеља, када је ембрион велик од око 3-10 cm (Johnston, 2014)), а потпуно се формирају до 21. недеље живота детета у телу мајке (Слика 2-25)³⁷. Еволуционисти верују да су те папиле настале као производ потребе да се повећа површина коже како би оруђе које је користио рани човек могло лакше да прионе уз длан. Други, запажају да је формирање облика папила на врховима прстију процес на који утичу безбројни фактори, као што су тачан положај плода у материци у одређеном тренутку, као и тачан састав и густина амнионске течности (плодове воде) која окружује дете, сваки додир околних структура у материци и др.

Све то утиче како ће се сваки појединачни гребен формирати, а цео процес развоја је толико хаотичан да, у целом току људске историје, практично нема шансе за понављање



дана у материци

³⁶<http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm>

³⁷<http://www.med-practic.com/uploads/161bca84b410.gif>

дословце истог обрасца два пута. (Michael Roizen, 2014)

Отисак прста настаје као последица излучивања зноја кроз поре које се налазе на линијама квржица прста. Када човек дотакне неки предмет (или се ослони на подлогу) – настаје отисак. Сам отисак је невидљив голим оком зато што је сам зној човека невидљив, а хемијски, он је сачињен од 99% воде (H_2O), затим соли натријума хлорида ($NaCl$), калијум-хлорида (KCl), сулфата, масних киселина и беланчевина.

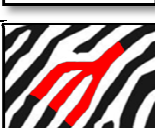
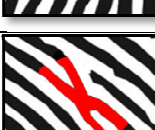
У случајевима повреде коже прстију, уколико повреде нису озбиљне – папиле које се регенеришу су – идентичне претходним.

2.1.11 Класификација морфололошких облика папила

Минуције су дакле, морфолошки облици унутрашње стране шака и табана, јединствени за сваки прст, сваког човека на планети.

Бројни су облици минуција, које можете пронаћи у литератури. У основи разликујемо брег и дољу, срце отиска и делту.



Доминантни морфолошки облици минуција		
		Завршетак минуције
		Кратак прекид минуције
		Мост
		Рачвање (бифуркација)
		Двоструко рачвање (двострука бифуркација)
		Троструко рачвање (трифуркација)
		Раскршће
		Кука или удица
		Око
		Језеро
		Острво

Табела 1

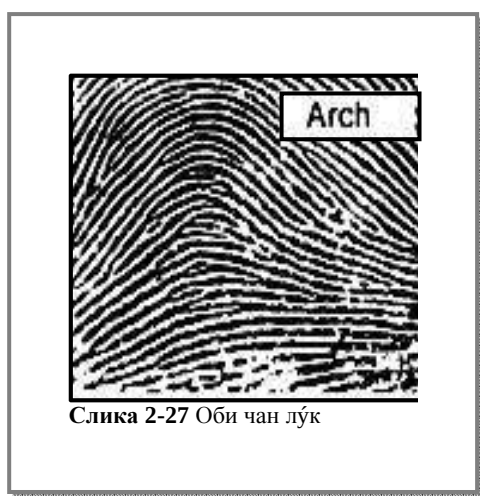
2.1.12 Класификација отисака прста

Године (1900), **Сер Едвард Хенри** (*енг. Sir Edward Richard Henry*) генерални инспектор полиције Бенгалу, ствара свој метод разврстања отисака који омогућава њихово брзо претраживање који се и данас назива „**Хенријева класификација**“. Она је општеприхваћена у свету и темељ је савремених база биометријских података.

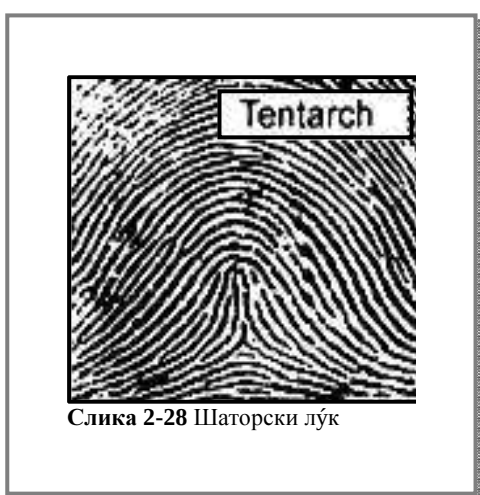
Разликујемо три основне групе отисака (четврта је комбинација прве три) по свом облику, то су:

1. **Лук (*enql. arch*)** – се као обележје налази код око 5 -7 % човечанства и има своје две подгрупе:

а) **Обичан лук (*enql. plain arch*)**³⁸ – овај облик лука је најједноставнији од свих, карактерише га блага кривина с лева на десно, као талас „по екватору“ прста.



б) **Шаторски лук (*enql. tented arch*)**³⁹ - је веома сличан обичном. Оно што га разликује је конвексност минуције која је уочљива на средини превоја.

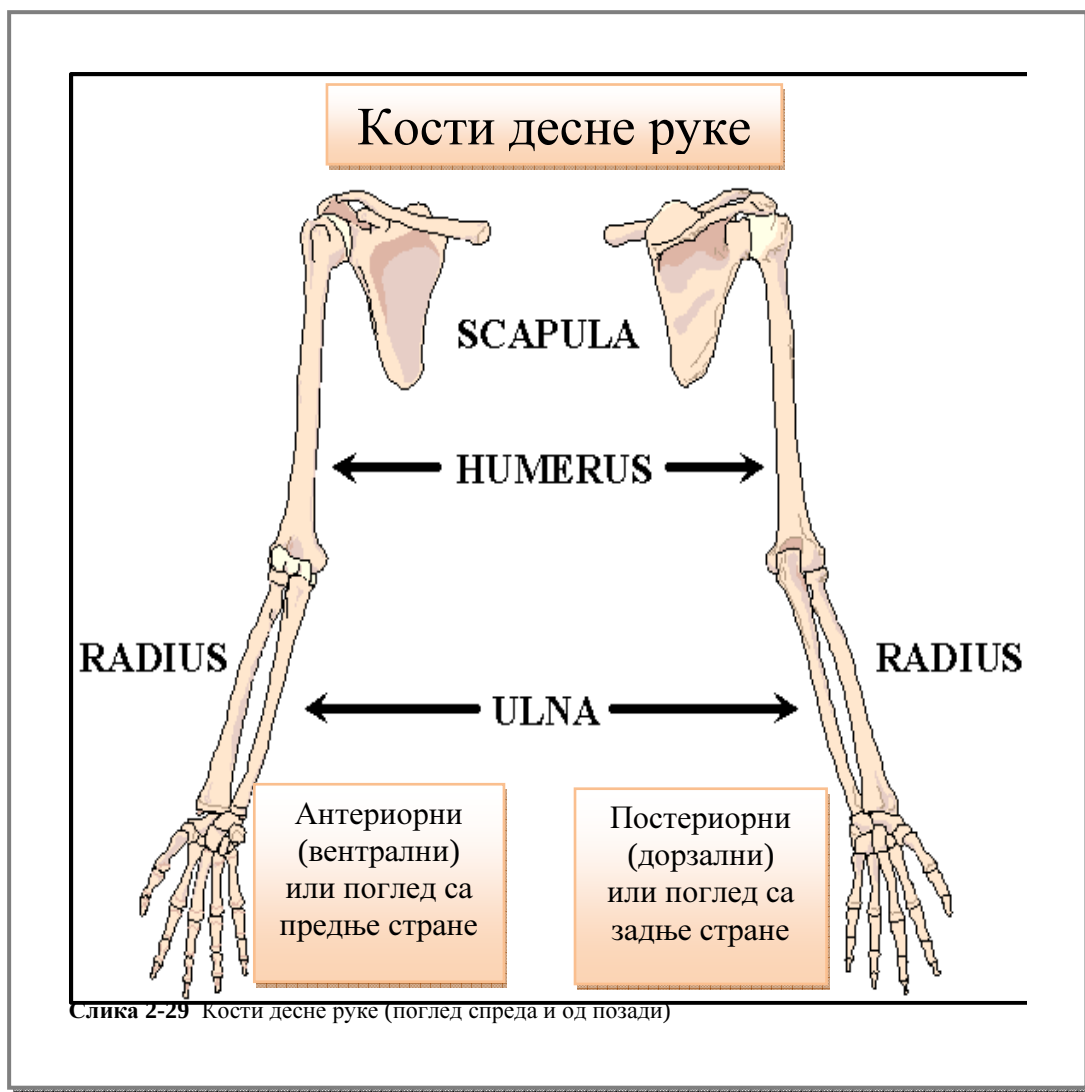


³⁸Део фотографије на линку: <http://shs2.westport.k12.ct.us/forensics/04-fingerprints/patterns.jpg>

³⁹Део фотографије на линку: <http://shs2.westport.k12.ct.us/forensics/04-fingerprints/patterns.jpg>

2. **Петља или омча (*enql. loop*)** - је врста обрасца у којој једна или више папила иду према другој страни, закривљују се (у правцу приближно север-југ), додирују или пролазе кроз замишљену линију између делте и срца отиска, и враћају се на исту страну одакле су папиле ушле. Петља има једну делту.

Изрази "радијални" и "лакатни" су изведени из речи радијус (*lat. radius*) и улна (*lat. ulna*) по латинским именима две кости подлактице које спајају надлактицу и шаку (Слика 2-29)⁴⁰. Класификација петљи је базирана на смеру нагнутости на прсти (а не на отиску на папиру).

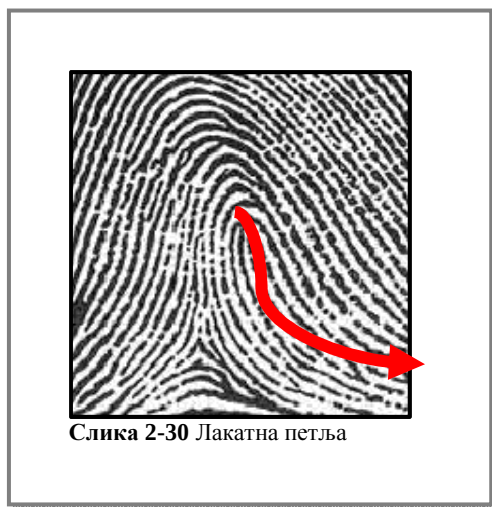


Петља је дефинитивно најбројнији образац отиска прста који се у разним варијацијама може пронаћи код 60 – 70% људи.

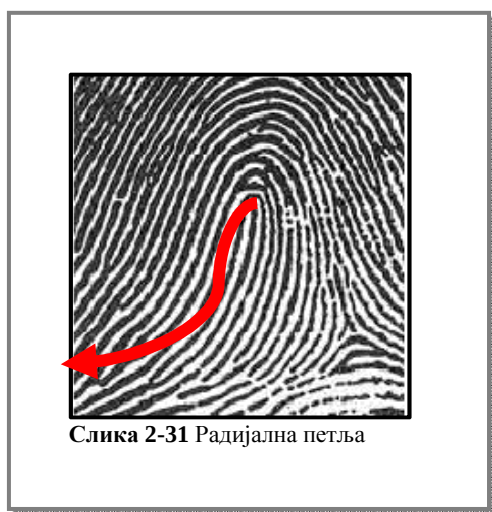
Разликујемо следеће врсте петљи:

⁴⁰ http://shs2.westport.k12.ct.us/forensics/11-forensic_anthropology/arm_&_shoulder.gif

а) **Лакатна петља или омча** (*engl. ulnar loop*)⁴¹ – (десне руке) „тече“ у смеру лакатне кости (према малом прсту). Фотографија представља отисак на папиру.



б) **Радијална петља или омча** (*engl. radial loop*)⁴² – (десне руке) се шири према палцу. Ова шара је једнако заступљена код жена и код мушкараца, али је гледајући по прстима далеко најзаступљенија на кажипрсту. Фотографија представља отисак на папиру.



Оно што треба нагласити је да све зависи о руци којој се узима отисак. Ако посматрамо леву руку, петља која се отвара са десне стране (према малом прсту), ће бити лакатна – десна, петља (слика 2-30)⁴³, док ће она који се отвара на лево (према палцу) бити радијална петља (слика 2-31)⁴⁴.

У случају десне руке, биће обратно, ако се петља „отвара“ на десну страну, биће радијална, а ако се отвара на леву страну – биће лакатна.⁴⁵

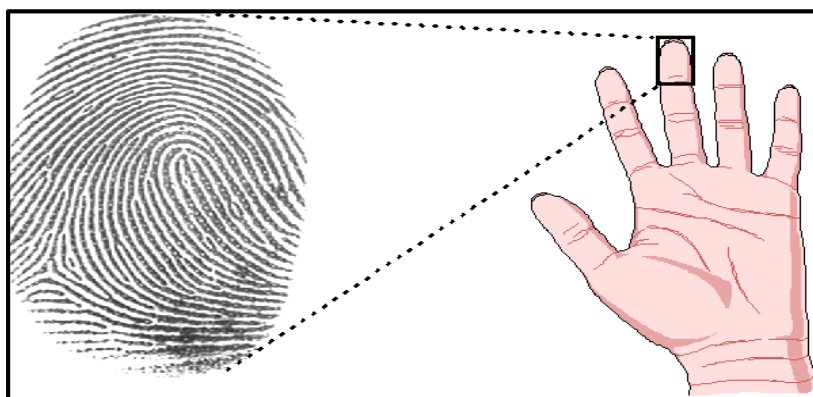
⁴¹ Део фотографије на линку: <http://lipariforensics.blogspot.com/>

⁴² Део фотографије на линку: <http://lipariforensics.blogspot.com/>

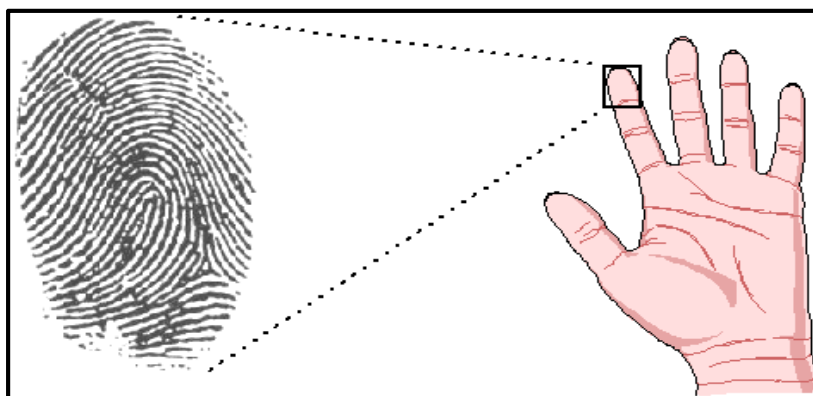
⁴³ <http://shs2.westport.k12.ct.us/forensics/04-fingerprints/ulnar%20loop.gif>

⁴⁴ http://shs2.westport.k12.ct.us/forensics/04-fingerprints/radial_loop.gif

⁴⁵ http://shs2.westport.k12.ct.us/forensics/04-fingerprints/fingerprints_handout.htm



Слика 2-32 Лакатна петља (леве руке)



Слика 2-33 Радијална петља (леве руке)

3. **Спирала (*engl. whorl*)** се уочава код 25-35% људи као образац отиска прста. Сваки образац отиска прста који садржи два или више ушћа се сматра обрасцем спирале.

Постоје две основне врсте образаца спирале:

а) **Обична спирала (*engl. plain whorl*)** се састоји од једног или више гребена који чине или теже да начине комплетан круг са две делте између којих је нацртана замишљена линија и најмање један гребен који вијуга у унутрашњем простору обрасца који је прекинут или дотакнут. Обична спирала је најједноставнији и најчешћи облик спирале.

б) **Спирала са средишњом петљом (*engl. central pocket loop whorl*)** чини потпуну петљу која може да буде спирална, овална, кружна или било ког кружног облика.



Слика 2-34 Обична спирала



Слика 2-35 Спирала са средишњом петљом

4. **Композити** (*engl. composites*) –представљају комбинацију лука и/или петље и/или спирале. Хенри Фолдс је извршио поделу композита на четири подгрупе:

в) **Спирала са двоструком пељом** (*engl. double loop whorls*) се састоји од две одвојене и различите формације петљи са два одвојена и различита рамена за свако језгро, две делте и једне или више гребена који чине потпуни круг. Између два, најмање један гребен који вијуга у унутрашњем простору обрасца и када се нацрта замишљена линија он бива прекинут или дотакнут.



Слика 2-36 Спирала са двоструком петљом

г) **Спирала случајности** (*engl. accidental whorls*) - је превише нестереотипна да би се могла класификовати. Састоји од најмање две различите врсте образаца који, имају два или више.



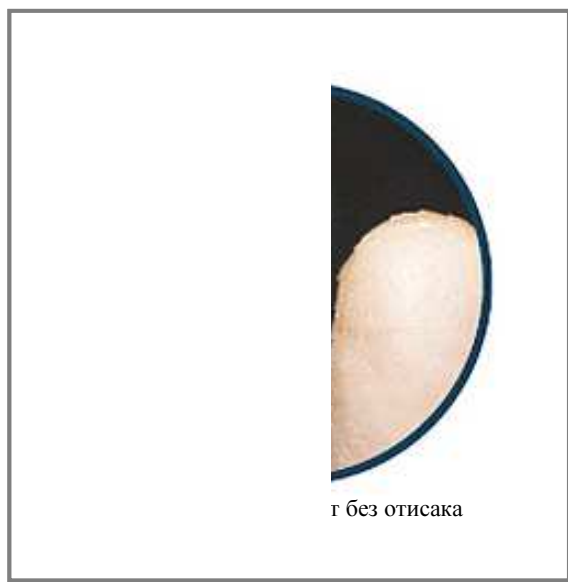
д) **Спирала са бoчним џепом**⁴⁶ (*engl. lateral pocket loop*) - када се папиле које чине петљу нагло савију са једне стране пре поновног закривљења, оне формирају бoчни међупростор или бoчни џеп који је обично попуњен папилама из друге петље. Срце петље је смештено бoчно и постоје две делте.

2.1.13 Људи без отисака

Посматрањем папила на врховима прстију, одавно је запажено да постоји извесан (веома мали) број људи који ове папиле – нема. На слици 2-39⁴⁷ видимо прсте без отиска.

Ради се о ретким генетски наследним болестима, ектодермалним дисплазијама названим синдромом Нејгели-Франческети-Џадасн (*Syndrome Naegeli-Franceschetti-Jadassohn*) који утиче на кожу, знојне жлезде, нокте и зубе.

Најважније знаци су: одсуство отисака прстију, хипохидроза или анхидроза⁴⁸ или смањена функција знојних жлезда, (представља стање које се карактерише потпуним престанком излучивања зноја (обзиром да је знојење физиолошки процес неопходан за нормалну терморегулацију организма,



⁴⁶ <http://tholath.files.wordpress.com/2009/10/lateral-pocket-loop1.jpg?w=450>

⁴⁷ http://news.xinhuanet.com/tw/2008-02/01/xinsrc_2320205010720359265506.jpg

⁴⁸ **Хипохидроза** или **анхидроза** представља стање које се карактерише потпуним престанком излучивања зноја.

овај поремећај може бити опасан по живот), нетолеранција на топлоту, дистрофија⁴⁹ ноктију, умерена задебљања (*лат. hyperkeratosis*) дланова и табана, ретикуларна хиперпигментација (препигментација одређених делова тела, позната као „тамне тачке болести“, која почиње да се развија од друге године живота, без фазе запаљења) као и абнормална зубна глеђ која за последицу има релативно рано испадање зуба.

До данас је забележено више породица са оболелим особама кроз неколико генерација (и мушкараца и жена), а учесталост обољења се процењује на једног оболелог од три милиона људи. (ITIN, 2009)

Дијагноза је клиничка и може бити потврђена генетском анализом, а случај пренаталне дијагнозе за сада још није забележен. Узрок болести је мутација фенотипа (грешка на протеину званом Кретин 14 (*Cretin 14*), која се преноси наследно. На слици 2-40 видимо Кинеза Хуан Тианга⁵⁰ са сином и унуком без отисака прстију.



Слика 2-40 Хуан Тианг (黄振添) са сином и унуком без отисака прстију

2.1.14 Биометријски отисци код животиња

Отисци прстију нису јединственост која постоји само код људи. Отиске имају и друге врсте примата, шимпанзе, орангутани (Слика 2-42)⁵¹, гориле...

⁴⁹ **Дистрофија** не дегенерација ткива узрокована болешћу или потхрањеношћу

⁵⁰ http://news.xinhuanet.com/tw/2008-02/01/xinsrc_222020501072078177804.jpg

⁵¹ <http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm>



Слика 2-42 Папиларне шаре на прстима орангутана

Коале (Слика 2-41)⁵² такође имају отиске прстију и стопала иако се сматрају потпуно различитом подкласом сисара.⁵³



Слика 2-41 Стопало коале



Слика 2-43 Зебре – биометријска различитост

Многе друге животиње као на пример зебре (Слика 2-43)⁵⁴ или многе врсте риба (Слика 2 – 44,45)⁵⁵, имају шаре које



Слика 2-44 Ctenochaetus strigosus

неодољиво подсећају на људске отиске прстију.



Слика 2-45 Ctenochaetus Hawaiiensis

⁵²<http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm>

⁵³<http://echidnawalkabout.files.wordpress.com/2013/11/rainirightfoot290208p1.jpg>

⁵⁴<http://www.peoplepets.com/people/pets/article/0,,20544504,00.html>

⁵⁵<http://www.bromba.com/knowhow/BiometricAnimals.htm>

2.2 ПРИВАТНОСТ

2.2.1 Појам приватности

Не може се озбиљно сагледати ни једна друштвена појава или појам без сагледавања њене историјско-правне позадине.

Дефиниција приватности добија свој класичан израз кроз чувени чланак под именом „Право на приватност“ (енгл. *The Right To Privacy*), аутора двојице америчких правника Семјуела Ворена⁵⁶ (*Samuel Dennis Warren*) и Луиса Брендиса⁵⁷ (*Louis Dembitz Brandeis*) који је публикован у харвардском правном журналу „Харвард Лоу Ривју“ (*Harvard Law Review*), децембра 1890. У том чланку приватност се једноставно описује као „право да будете остављени на миру“ (енгл. „...the right to be let alone...”)



Слика 2-47 Д.Ворен



Слика 2-46Слика 2-5– Кинески документ „потписан“ Д. Бр

Да је приватност много сложенији појам наговештавају размишљања многих. Право на приватност се у оквиру грађанско-правне науке данас сврстава у домен тзв. личних права (Станковић О., Водинелић В., 1996.) и брани се како државним, тако и универзалним правним механизмима.

Неки приватност посматрају као „фундаментално право“ и као пример истоветних се наводе право на живот и слободу, а неки полазе од приватности као начелне друштвене вредности. Приватност је обухваћена кроз бројне правне оквире.

Међународна конвенција о грађанским и политичким правима (*International Covenant on Civil and Political Rights*) чланом 17. брани приватност грађана прописујући да „нико не може бити изложен произвољном или незаконитом мешању у приватност, породицу, кућу или преписку, нити незаконитом атаку на достојанство и углед“.

Општа декларација о правима човека (*Universal Declaration of Human Rights*) у члану 12. захтева да „нико не сме бити изложен произвољном мешању у

⁵⁶http://upload.wikimedia.org/wikipedia/commons/c/ca/Samuel_Dennis_Warren_by_William_Notman%2C_c1875.jpg

⁵⁷<http://en.wikipedia.org/wiki/File:Brandeisl.jpg>

приватни живот, породицу, стан или преписку нити нападима на част и углед“ и да свако има право на законску заштиту против оваког мешања или напада.

Европска конвенција о људским правима (*Convention for the Protection of Human Rights and Fundamental Freedoms*) уплив држави у приватност грађана дозвољава само у оној мери која је реално потребна. (Суботић, 2011).

Забрана неовлашћеног приступа над личним подацима или заштита контроле над личним подацима се сматра најчешће коришћеним описом приватности. Аналогно томе, повредом приватности се сматра нарушавање нечије интиме, осамљености или приватних послова, јавно обелодањивање приватних чињеница о некој особи, лажно излагање неке личности погледу јавности и преузимање нечијег имена и лика зарад одређене користи, и др.

2.2.2 Информациона приватност

Разматрајући питање приватности неминовно смо дошли до питања информационе приватности и у оквиру ње морамо разликовати заштиту података од заштите приватности, зато што је заштита података само део заштите приватности.

Такође, када говоримо о заштити приватности у информационом добу, важно је нагласити да је веома битан **концепт анонимности**.

У савременом свету постаје веома тешко одредити потребан баланс између анонимности и недвосмисленом аутентификацијом, па је сукоб интереса чест.

Агресивна пропаганда **„културе безбедности“** од стране америчке власти, посебно после Патриотског закона (*Patriotic Act*⁵⁸) из 2001. године, који је усвојен од америчког Конгреса, а као последица терористичког напада 11. септембра 2001. г. Овим концептом грађанима је наметнута „трампа“, приватност за безбедност и грађани САД су углавном прихватили тај концепт.

Презвитер, Оливер др Суботић разматрајући ову проблематику користи појам **„Информационо контролисано друштво (ИКД)“**. Држава својим институционалним овлашћењима све више заузима простор који је био резервисан за приватност, и ако се тај тренд не заустави, постоји реална опасност од тоталитаристичког концепта друштва где нема тајни за мали број властодржаца и који знају све о свима који нису део тзв. елите. Скандали „Викиликса“ и Џулиана Асанжа, као и Едварда Сноудена у новије време показује да су одређене отуђене службе спремне на тоталну информациону контролу свих, укључујући и председнике страних држава.

2.2.3 Релативизација и добровољно одрицање од приватности

Творци и спроводиоци парадигме „културе безбедности“, израдили су читав низ техника којима утичу на понашање грађана. Уочавају се два главна паралелна смера са истим циљем, где је циљ промена понашања грађана.

Грађани који изразе одређену бојазан по питању угрожавања његових права везаних за приватност, подржаваоци концепта „културе безбедности“ излажу подсмеху говорећи о „теорији завере“ и на тај начин покушавају да дискредитују било какву (оправдану или заиста параноичну) полемику.

С друге стране постоје грађани који напросто из неспремности за борбу, пристају на надгледање зарад безбедности, изговарајући се „ја немам шта да кријем“.

⁵⁸<http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>

То и јесте један од урбаних митова. **Питање приватности није питање тајности већ – контроле.**

Понашање грађана у ИКД-у узрокује нове феномене као што су **феномен самоконтроле** који је везан за начин понашања под видео надзором, или **феномен самоцензуре** у говору или писаној речи.

У сведочењу пред специјалним одбором британског парламента професор Клајв Норис, један од најпознатијих светских истраживача из области утицаја видео надзора на друштво, наводи да постоји неколико кључних проблема у погледу ефеката државног надзора, међу којима је први и основни **феномен неповерења**, које се ствара у друштву у коме се подаци масовно скупљају, чиме се шаље порука да се грађанима не сме веровати, а коју прати стварање дистанце између полиције и грађанства (Суботић, 2011).

2.2.4 Критички поглед на технологију

Аустралијанац, Роџер Кларк⁵⁹ (*Roger Clarke*), један од водећих стручњака који се бави проблемима везаним за информационе системе и приватност, људска права и слободе, каже: „**Биометрија је једна од најозбиљнијих од много технологија за надзирање које прете слободи појединаца и друштва**“.

На другом месту, а везано за технологије које су данас водеће у процесу аутентификације, каже: „Смарткард апликације треба користити само онда када постоји јасна сагласност јавности за овај тип аутентификације, где је сигурност биометријских система убедљива, и где нема наговештаја о формирању централног регистра биометријских информација“.

Због свих наведених (и ненаведених) разлога, важно је критички сагледавати употребу технологије у савременом друштву и чинити крајње напоре у очувању људских права и слобода. **Најбоље је када је технологију могуће употребити не против, већ у корист очувања поменутих права.**

2.2.5 Духовност и философија vs. биометрија

Поводом учесталих полемика 2006. године о Закону о личној карти, (подстакнутих недоумицама верника и једног дела епископата), Свети Архијерејски Синод СПЦ је јуна месеца 2006. године затражио стручно мишљење од Оливера Суботића, тадашњег дипломираног инжењера и теолога, службеника Информационо-документационог центра Православног богословског факултета.

На основу тог захтева, др Суботић је изradio стручну студију, која је послужила као почетна основа за креирање далеко опсежнијег дела од стране истог аутора, под називом „Биометријски системи идентификације: критичка студија“, публикованог марта 2007. године. (Б.Нешић, 2007)

Закључујући своје ставове, након опсежних истраживања, о потреби



Слика 2-48 Роџер Кларк

⁵⁹<http://www.rogerclarke.com/Photos/ISTAS-Jun10-Med.jpg>

холистичког приступа сагледавању, заузимању ставова и доношењу одлука по питању биометријских система, свештеник др Суботић између осталог, упозорава:

Биометријске системе идентификације превасходно треба проучавати у контексту њихових друштвених импликација, а не само кроз питања техничке изводљивости и применљивости. То подразумева мултидисциплинаран приступ који пре свега обухвата етичке, информатичке, правне и социолошке дисциплине. Сваки редукционизам и свођење ове проблематике на само један од наведених аспеката не доноси добре резултате и води ка погрешним закључцима који могу имати далекосежне последице.

Имплементација биометријских система идентификације на бази политичког волунтаризма, без критичког става и ванакадемске расправе је недопустива. Политичке структуре најчешће имају мало знања из ове области и ослањају се углавном на проспекте биометријских корпорација, притом често улазећи и у конфликт интереса. Ниједно слободно друштво себи не сме дозволити да се питања идентификационог менаџмента решавају превасходно у политичким и/или интересним круговима, већ иницијатива и предложена решења првенствено морају долазити од стране стручних и научних институција из релевантних области. Поред стручних и научних препорука, потребно је уважити и став грађана, јер уколико не постоји шира подршка грађана биометријском систему идентификације, исти не треба ни имплементирати.



Слика 2-49 Др Оливер Суботић

Технологија сама по себи не сме бити циљ, већ искључиво средство и мора бити одмеравана општеприхваћеним етичким постулатима. У случају колизије технолошких решења и правно-цивилизацијских норми, предност увек треба да је на страни ових других, што је принцип који треба применити и на биометријске системе идентификације.

Не сме се допустити укидање концепта анонимности у случајевима где га је могуће очувати.

Будуће итерације некритичких имплементација биометријских система идентификације конвергирају ка друштву тоталног надзора и контроли свих трансакција. Проблематични аспект токен-а, тј. уређаја на коме је смештена биометрија, није везан за његову садашњу имплементацију у виду једнонаменских смарт карти, већ за концепт вишенаменског документа и евентуалну будућу имплементацију у виду биочипа (имплантата), што је огромном броју људи данас апсолутно неприхватљиво. Концепт биочипа је посебно неприхватљив у срединама са већински хришћанским становништвом, због конотација које такав развој догађаја доноси у поређењу са Јовановим Откровењем и чињеницом да би неслагања по том питању интересне групе могле да искористе за увођење раскола и немира међу неистомишљенике. (Суботић Д. О., 2007)

2.3 БИОМЕТРИЈА ПРИВАТНОСТИ

2.3.1 Аутентификација – опште информације

Постоји више дефиниција аутентификације. Неке од њих су:

Аутентификација (грч. *αυθεντικός* - прави или оригиналан, од грч. *αυθεντης* аутентис - аутор) је чин којим се потврђује истинитост атрибута једног податка или ентитета.

За разлику од идентификације која се односи на чин тврдње која наводно потврђује идентитет лица или ствари, аутентификација је процес који заправо потврђује идентитет.

То може да подразумева потврђивање идентитета уз лична документа, проверу валидности сајта са дигиталним сертификатом, потврду старости артефакта методом датирања угљеника, или да гарантује да је производ оно што његово паковање и етикетирање тврде. Другим речима, аутентификација често укључује проверу валидности најмање једног облика идентификације. (Authentication, 2014)

Аутентификација је, најкраће речено, провера (потврђивање) идентитета.

То је процес којим се учесник у комуникацији уверава о идентитету другог. У свакодневном животу, аутентификацији се прибегава када се две стране „не познају лично“, а имају потребу да размене или потврде неке важне информације. Познато је да се аутентификација (путем рачунара) извршава на три основна начина који се могу користити самостално или у комбинацији са другима, то су:

- **знање** (имамо неку важну информацију, лозинку и сл.)
- **поседовање** (имамо кључ, токен, паметну картицу или нешто што гарантује наш идентитет)
- **биометрија** (онога што јесмо, што гарантују јединствене карактеристике сваког појединца).

Такође је јасно да знање може бити компромитовано - забором, поседовање – губитком или крађом, док биометријска обележја, која су јединствена за сваког човека на планети, човек носи са собом, јер се ради о самој супстанци онога који се аутентификује.

2.3.3 Биометријска аутентификација

Биометријска аутентификација представља процес аутентификације у коме учествују биометријска читавања. Генерално, се дели на две фазе:

- **фазу уписа** (која подразумева читавање биометријских података појединца, и израду шаблона за складиштење (у случају опозиве биометрије), и
- **аутентификацију** (или верификацију), која подразумева поновно читавање (поновну израду шаблона) и поређење тог шаблона са оним које се налази у бази података.

Биометријска читавања су ретко идентична и зависна су од услова читавања и технологије која се користи (самог уређаја). Шаблон је апроксимативни приказ биометријских података (трансформисан неким неповратним алгоритмом), а успешност верификације зависи од тога колико је претходно уписани, референтни образац сличан контролном.

Имајући у виду да аутентификација која је заснована на биометрији може дати неоторив доказ о идентитету корисника, као и чињеница да се током живота јединке ти подаци не мењају, веома је важно те податке сачувати. (Ang, R., Safavi-Naini, R. & McAven, L. F. , (2005).)

Може се чак рећи да је случај отуђивања тих података који чине идентитет, заправо случај „електронског убиства“, после чега јединка не може да се опорави. У доба аналогije, појединац који је изгубио лични документ, огласио га је неважећим у штампи и затражио од одговарајућег органа (који му је и издао претходни документ) издавање новог документа. Нови документ би добио свој нови јединствени идентификатор и проблем је био решен. Познати су случајеви крађе идентитета када је појединац компромитацијом својих биометријских података западао у велике проблеме, јер су ти подаци послужили криминалцима да се обогате на терет „власника“ биометријских читавања. Сајбер-криминалци су поседовали оно што неко други јесте и на тај начин „доказали“ електронски идентитет.

Поседовање изворних биометријских података од стране државних органа, медицинских и других установа, чак и без конкретног нарушавања безбедности база података, поседује потенцијал за њихову злоупотребу. Подаци могу да се повежу са другим базама података и да се затим профилишу (*eng. profiling*) у циљу упознавања навика, потреба и особина човека, начина вођења живота и политичког става, што у потенцијалу звучи као увод у тоталитарно, информационо-контролисано друштво.

Др Оливер Суботић о опасности прикупљања и груписања података о грађанима, пише: „Концепт централне базе биометријских и њима придружених података има потенцијал за актуелизацију информационо контролисаног друштва. Иако у перцепцији просечног грађанина проблематичан може бити само уређај на коме се биометрија налази (смарт картица или нешто друго), у етичком, правном и информационом смислу највећи проблем представља централна база биометријских података, која временом може да прерасте у тоталитарни паноптички супстрат уколико постоји могућност укрштања са осталим базама. Укрштање разнородних база података је могуће на више начина, али у пракси се своди на коришћење универзалног алфанумеричког идентификатора. Због повећања концентрације моћи полицијског апарата, рањивости централне базе споља и изнутра и њене потентности за развој информационо контролисаног друштва, концепт централ(изов)ане базе биометријских и укрштањем придружених података представља насртај на концепт слободног друштва и треба га законом забранити.“ (Суботић Д. О., 2007)

2.3.2 Опозива биометрија

Трагом заштите приватности, а у потрази за обновљивим извором биометријских читавања родила се **опозива биометрија** (*eng. cancelable biometrics*). (Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, Ruud M. Bolle, april 2007)

Опозива биометрија подразумева неповратно трансформисање и чување биометријских података у неком „обрасцу“ (*eng. template*) и ако би евентуално дошло до компромитовања базе података трансформисаних верзија, не би дошло до

угрожавања приватности тј. електронског идентитета корисника. Трансформација је један од начина који омогућава да поседовање информације о трансформисаној биометрији не одаје информације о стварним биометријски подацима.

Опозива биометрија такође, пружа виши ниво приватности омогућавајући израду много различитих образаца са истим изворним биометријским подацима и самим тим немогућност повезивања корисничких података који су смештени у више различитих база података. (Ang, R., Safavi-Naini, R. & McAven, L. F. , (2005).)

2.3.3 Системи биометријског шифровања

Биометријско шифровање (*eng. Biometric Encryption - (BE)*) је група нових технологија које:

- *везују дигитални кључ за биометрију* или
- *генеришу дигитални кључ из биометријских читавања*, тако да нема сачуване слике биометрије или шаблона.

У систему биометријског шифровања (СБШ), оно што се складишти је шаблон СБШ, другачије познат као " **биометрички шифрован кључ**" (*eng. biometrically encrypted key*) или „**помоћни подаци**“ (*eng. helper data*). Последица тога је да нити дигитални кључ, нити оригинални биометријски подаци не могу бити издвојени из депонованог шаблона БШ.

Систем биометријског шифровања (СБШ) се концептуално разликује од других система који шифрују биометријске слике или шаблоне користећи конвенционално шифровање, чувањем криптографског кључа и његовим уништавањем након успешне аутентификације. СБШ подразумева да се дигитални кључ поново обнавља само уколико је исправан биометријски узорак присутан. Резултат верификације СБШ је или дигитални кључ или порука о неуспешној операцији. Овај процес шифровања и дешифровања је расплут (*eng. fuzzy*) због природног варирања биометријских узорака.

Концепт система биометријског шифровања (СБШ) је први пут представљен у средином 90-тих од стране Џорџа Томка, Колина Соутара и Грегори Шмита (*George J. Tomko, Colin Soutar, Gregory J. Schmidt*).

СБШ је процес који безбедно везује дигитални кључ са биометријским или генерише кључ из биометрије.

Може се рећи да је кључ „шифрован“ биометријским читавањем. Резултујући **биометријски-кодиран кључ**, се још назива и „СБШ шаблом“ или „помоћним подацима“. Овако добијени шаблон се депонује на неке меморијске јединице. Дигитални кључ може бити "дешифрован" у процесу верификације, ако се приложи тачан биометријски узорак.

Овај процес шифровања/дешифровање је расплут (*eng. fuzzy*) по својој природи, јер биометријски узорак је другачији сваки пут, за разлику од кључа за шифровање у конвенционалној криптографији.

Главни технолошки изазов је имати поново исти дигитални кључ, упркос природним варијацијама на улазној биометрији. Након успешне верификације и поновног формирања кључа, дигитални кључ може да се користи као основа за било какву физичку или логичку примену. Најочигледнија и најчешћа примена је у

конвенционалном криптосистему где кључ служи као лозинка и може генерисати, на пример, пар јавних и приватних кључева.

Оно што треба напоменути је да само биометријско шифровање није криптографски алгоритам. (Ann Cavoukian and Alex Stoianov, 2009)⁶⁰

Улога Система биометријског шифровања (СБШ) је да рањиве системе засноване на лозинкама замени или ојача сигурнијим и комформнијим за примену, биометријски управљаним кључевима.

СБШ не треба мешати са другим системима који шифрују биометријске слике или шаблоне користећи конвенционалну енкрипцију или смештају криптографски кључ на токен или на други уређај, а затим га се ослобађају након позитивне биометријске провере.

Биометријско шифровање припада другој породици технологија, оних које унапређују приватност, а названо је **опозива биометрија**. (Ann Cavoukian and Alex Stoianov, 2009)⁶¹



Слика 2-50 Др Ен Кавокијан

Постоје дакле, два приступа СБШ:

- **везивањем кључа**, када је произвољни кључ (случајно генерисан), чврсто везан за биометријски, и
- **генерисањем кључа**, када се кључ изводи из биометрије.

Подаци се у оба случаја складиште у обрасце (или помоћне податке) који су од биометрије зависни.

Неки шеме БШ система (нпр. привржене расплинутој логици (*eng. Fuzzy Commitment*)), расплинутом своду (*eng. Fuzzy Vault*) могу да раде подједнако и у моду генерисањем кључа и у моду везивањем кључа. Режим рада „генерисањем кључа“ је такође познат као „Сигуран цртеж“ (*eng. Secure Sketch*), он подразумева да ће се уписани биометријског шаблон опоравити на верификацији када свеж биометријски узорак приступи помоћним подацима (тј. цео шаблон или стринг изведен из њега, као на пример, хешована вредност шаблона, која служи као дигитални кључ).

Треба нагласити, да овај „кључ“ није трајна или апсолутна вредност (за неку конкретну биометрију), већ се та вредност мења при сваком поновном упису.

Величина простора за кључ, код „сигурног цртежа“ је дефинисана од стране унутар класних варијација биометрије, насупрот приступа везивањем кључа.

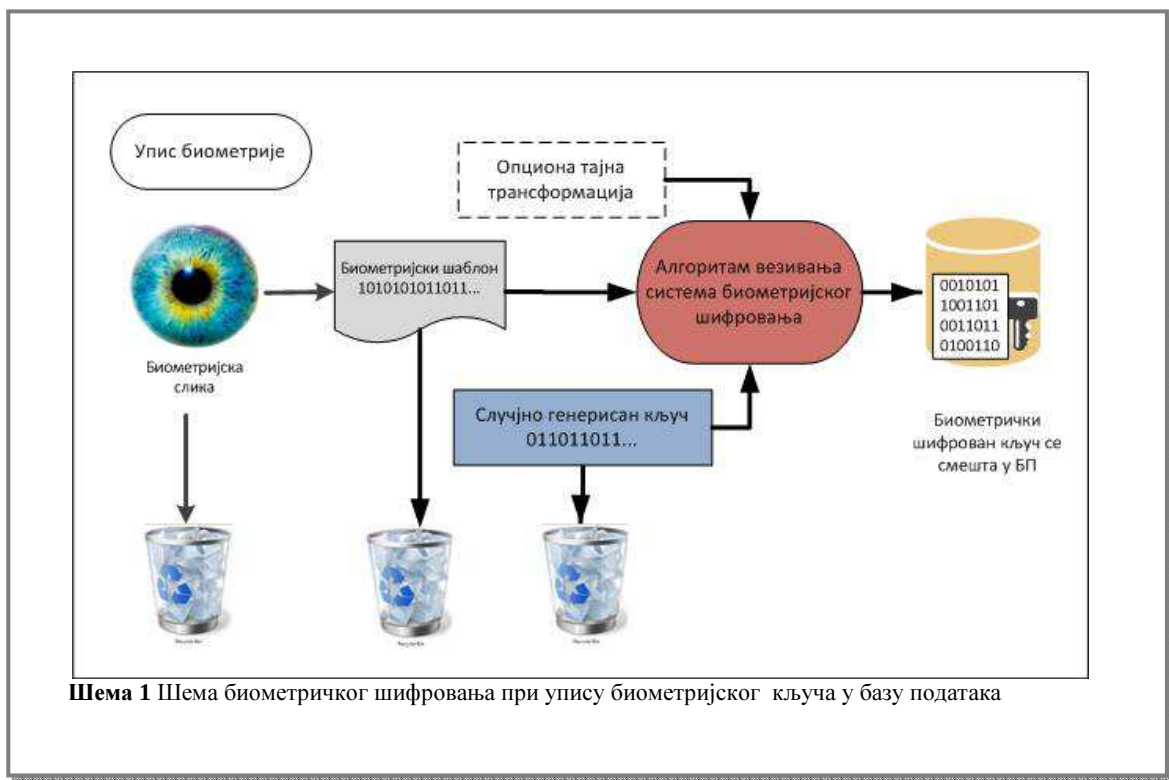
СБШ врши трансформацију (пожељно, иреверзибилну) у биометријску слику или шаблон и пореди га са већ трансформисаним шаблонима. Ова трансформација се обично држи у тајности. За разлику од система биометријског шифровања, систем опозиве биометрије не везује нити генерише кључ.

Опозива биометрија остаје суштински рањива на „напад убацивањем“ (да/не одговор) и на „напад супституције“.

⁶⁰ Др Ен Кавокијан је бивши комесар за информације и приватност Онтарија у Канади, једна од водећих заштитника приватности у свету. Припадник је идеје „Приватности по дизајну“ (*eng. Privacy by Design*), да је идеју приватности неопходно уткати у дизајн информационог система, проактивно, а не „лечити“ последице безбедносних пробоја.

⁶¹ http://www.privacybydesign.ca/content/uploads/2012/11/Commissioner_2008_sq.jpg

У режиму **везивањем кључа**, дигитални кључ се случајно генерише на упису, тако да ни корисник нити било ко други то не зна. Сам кључ је потпуно независан од биометрије, и стога, увек може увек бити промењен. (Шема 1 Шема биометричког шифровања при упису биометријског кључа у базу података Шема верификација биометријског кључа из базе података и реконструкције кључа)⁶² После читавања биометрије, алгоритам чврсто и доследно везује кључ за биометрију да би створио **биометрички шифрован кључ**.



Шема 1 Шема биометричког шифровања при упису биометријског кључа у базу података

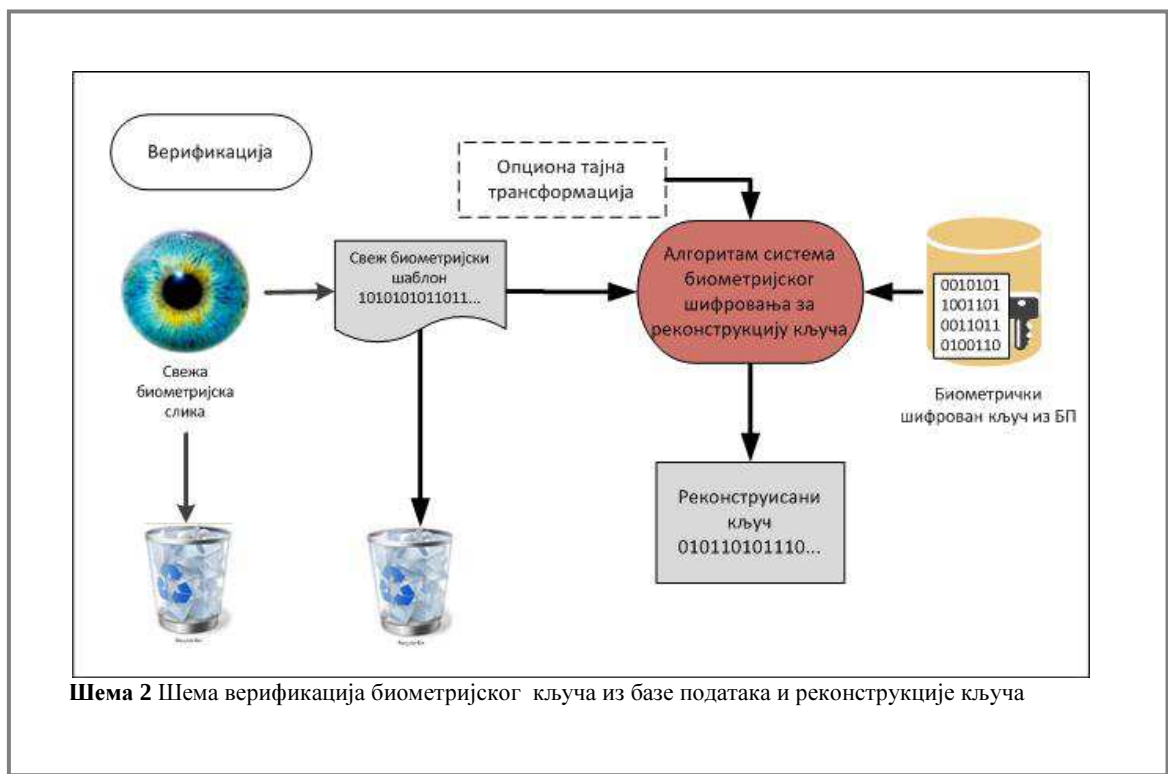
СБШ шаблон обезбеђује заштиту приватности и може бити депонован у базу података или локално (на паметну картицу, токен, лаптоп, мобилни телефон, итд). На крају уписа, и кључ и оригинални биометријски подаци се бришу.

У процесу верификације, корисник читава свој свеж биометријски узорак, који, када се примени на легитимни СБШ шаблон, омогућава СБШ алгоритму да поново врати почетни кључ. На крају провере, биометријски узорак се поново брише. (Шема 2 Шема верификација биометријског кључа из базе података и реконструкције кључа

СБШ алгоритам је дизајниран тако да израчуна прихватљиве разлике у улазној биометрији. С друге стране, нападач чија биометрија је довољно различита, неће моћи да поново креира кључ. Многи системи биометријског шифровања похрањују хеш вредност кључа, тако да се тачан кључ ослобађа из система СБШ само ако је хеширана вредност добијена на верификацији - потпуно иста. Постоји пракса је да се кључ ни не ослобађа, већ уместо кључа, се прави још једна хеширана верзија кључа, за било коју апликацију. Ова хеширана верзија може послужити као криптографски кључ. Са овом архитектуром, нападач не би био у

⁶² Шема је прилагођена у изгледу и преведена на српски језик. Оригинална шема се налази у раду: (Ann Cavoukian and Alex Stoianov, 2009)

стању да добије оригинални кључ изван система СБШ. Такође, биометријску слику/шаблон, не би требало слати на сервер. Провера система СБШ треба да се ради локално у већини сценарија. (Ann Cavoukian and Alex Stoianov, 2009)



Важан део већине алгоритама система биометријског шифровања (СБШ) је „Код за исправљање грешака – КИГ“ (*eng. Error Correcting Code (ECC)*).

КИГ (*eng. ECC*) се користи у комуникацији, за складиштење података и у другим системима где се јављају грешке. Биометријско шифровање је нова област за примену КИГ-а (*eng. ECC*).

На пример, бинарни блок КИГ-а (*eng. ECC*), који је означен (n, k, d), кодира k бита са $n > k$ бита додавањем неке редунаданце. Ти n -битни стрингови названи су **кодним речима** (*eng. Code Words*). Постоји их 2.000 укупно, где је k дужина кључа. Минимална раздаљина (обично је Хамингова дистанца подразумевана) између кодних речи је d . Ако се у каснијој фази (у случају биометријског шифровања СБШ, на верификацији), јави грешка, КИГ (*eng. ECC*) је гарантовано исправља до $(d-1)/2$ - битне грешке међу n бита. У идеалном случају, легитимни корисници ће имати низ грешака у оквиру граница тако да ће КИГ (*eng. ECC*) декодирати оригиналну кодну реч, и самим тим, дигитални кључ. С друге стране, нападач ће произвести непоправљив број грешака, а КИГ (*eng. ECC*) и систем биометријског шифровања ће објавити неуспешно откључавање. У пракси, систем биометријског шифровања СБШ, као и било који биометријски систем, има и стопу **лажних одбацивања** и **стопу лажних прихватања** (*eng. false rejection and false acceptance rates (FRR and FAR)*). (Ann Cavoukian and Alex Stoianov, 2009)

Постоје и друге технике поређења и методи препознавања, а поред наведених поменућемо и **Стварну стопу прихватања** (*eng. Genuine Accept Rate - GAR*), која се рачуна формулом $GAR = 1 - FRR$. (Mankame, 2013)

Треба имати на уму да систем биометријског шифровања СБШ не користи никаква поређења резултата. Уместо тога, ФРР/ФАР компромис се може постићи у неким случајевима варирањем параметара шеме система биометријског шифровања СБШ. Неки кодови за исправљање грешака – КИГ (*eng. ECC*) могу да раде у „меком“ режиму декодирања, тј. излаз са декодера је увек најближа кодна реч, чак и ако је то изван граница КИГ-а (*eng. ECC*). Ово омогућава постизање веће корекције грешака. (Ann Cavoukian and Alex Stoianov, 2009)

Један од начина би било коришћење технике рандомизације, као што је **биохешинг** или „сољење“. (Ong Thian Song, Andrew Teoh Beng Jin, Tee Connie, 2007)

Трансформација може бити контролисана лозинком корисника или може бити одвојена од осталих помоћних података чувањем на токenu или серверу.

2.3.4 Неке слабости биометријских система

Поред безбедносних претњи које подривају поузданост биометријских система, постоји одређени број проблема везаних за приватност, а у вези са овим технологијама:

- **притајена (латентна) функција** (тј. неовлашћена секундарна употреба биометријских података)
- **проширен надзор**, праћење, профилисање, и потенцијална дискриминација (биометријски подаци могу бити упарени са прикупљеним узорцима, сачувани на другом месту и кориштени при доношењу одлука везаним за посматране појединце)
- **злоупотреба података** (повреда приватности података, крађа идентитета, превара)
- **негативне последице на личност** засноване на погрешним идентификацијама (као некога другог), непотврђивању исправног личног идентитета, грешака у систему, и неуспеха (последице системских аномалија, нарочито у великим системима, често падају несразмерно на појединце, у облику непријатности, трошкова и стигматизације појединца)
- **недовољна одговорност**, надзор, и отвореност над системима биометријских података.
- **потенцијал за прикупљање и коришћење биометријских података без знања**, сагласности, или личне контроле. Ове врсте ризика угрожавају поверење корисника, што доводи до неприхватања и одбацивања биометријских система.

2.3.5 Предлози шема „биометрије приватности“

Аутентификација представља почетак процедуре коју органи државног апарата свакодневно чине у односу на грађане, при вршењу функција државног администраирања. Тај процес се одвија углавном пред службеним лицима, на шалтерима, при легитимисању возача од стране саобраћајне полиције, при гласању на изборима... Негде, улогу „сведочења да сте то заиста ви“ преузима лична карта, возачка дозвола, банковна картица...Како оне са контактним као и оне са (безконтактним) радио-фреквенцијским чипом.

Подаци којима се приступа често спадају у категорију „осетљивих“, па је и њихова заштита неопходна. Медицински картони садрже податке о болестима, пореска докумената - податке о личној имовини, студентски индекс - податке о полагању испита, возачка дозвола - о казним поенима и сл. Сви они могу бити третираны заштитним мерама. Дистрибуција база података је једна о таквих мера.

Државни органи, не би смели да поседују биометријске податке, сем оних за које није потребна сарадња, попут потографије, мада би и то требало да буде предмет законске регулативе.

Ипак, неки небиометријски подаци као што су име, презиме, улица и број, место и датум рођења, положене возачке категорије, казни поени и сл. представљају неопходне информације државним службеницима – саобраћајцима, на које се односи шема која се предлаже овим радом и о којој ће бити речи у наставку.

Посматрајући до сада изнесено и сагледавајући проблематику са аспекта приватности, овај рад предлаже модел функционисања, кроз три варијације, које уклапају савремена достигнућа из области опозиве биометрије и система биометријског шифровања, коју је аутор овога рада назвао **биометријом приватности**.

2.3.5.1 Услови функционисања система биометрије приватности

При разматрању функционисања поменутих шема полази се од следећих претпоставки:

- безбедност бежичне везе између мобилног биометријског читача и удаљене базе података је - неупитна. Користи се нпр. ИПСЕК (*eng. IPSEC*) интернет протокол који размењује шифроване податке.
- физичка безбедност како мобилних уређаја, тако и база података је – такође неупитна. Уређај чува наоружан полицајац који тај уређај дужи, а базе података су у објектима под надзором и са ограниченим приступом.
- Одбацује се могућност напада на биометријске системе „силиконским прстом“. Биометријско читавање се врши пред полицајцем који пре читавања врши контролу (прста).
- Очитани отисак је „идеалан“. Очитавање може да се понови неограничен број пута, у случају одбијања система.

2.3.5.2 Предложена шема 1

Ситуација 1 (Шема бр.3):

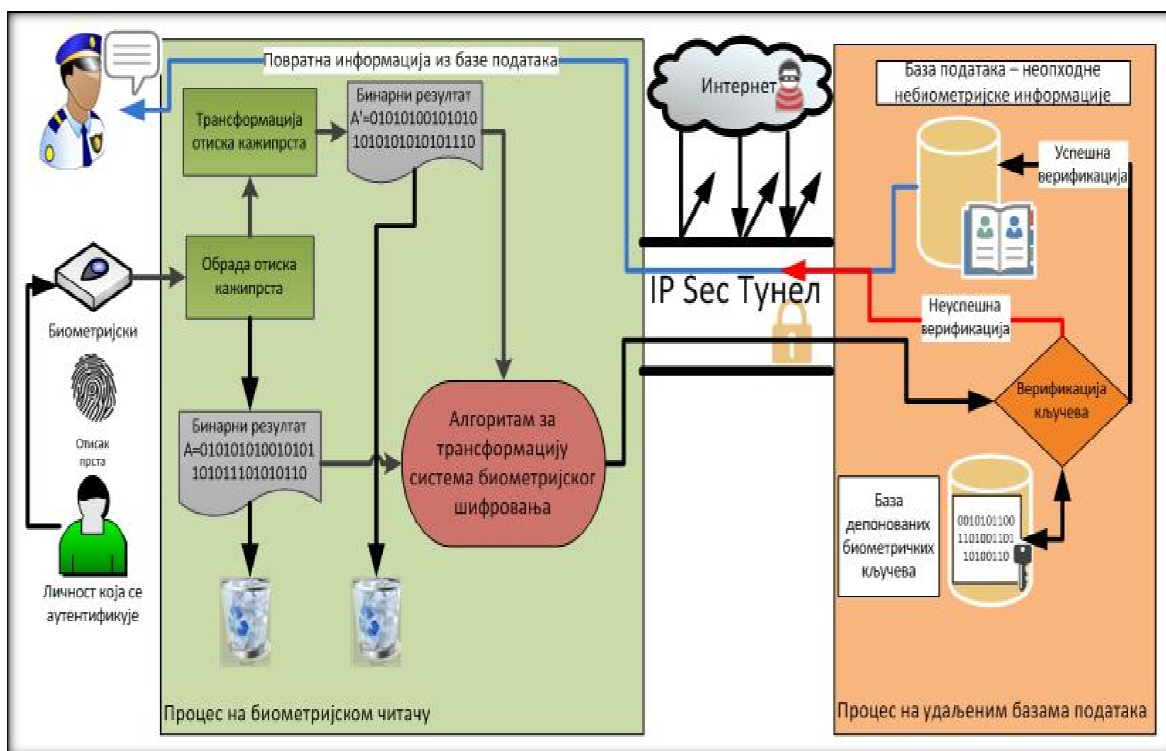
Саобраћајни полицајац поседује уређај који је у сигурној бежичној вези са базом података. У склопу обављања регулације и контроле саобраћаја, зауставља возило и започиње процес аутентификације.

Након службеног поздрава, љубазно али ауторитативно захтева да се возач представи (да каже име и презиме), и да пружи (нпр. кажипрст десне руке), и наслони на мобилни биометријски читач, на за то предвиђено место.

Тада се започиње процедура скенирања и обраде отиска прста, углавном заснованих на кључним тачкама минуција врха прста. Тако се добија образац отиска прста или шаблон, који се алгоритамски шаље на две адресе. Над једним примерком шаблона се врши трансформација и добија неки бинарни резултат **A'**. Други примерак шаблона нетрансформисан такође представља неки бинарни резултат **A**. Оба бинарна израза улазе у алгоритам за трансформацију отиска прста везивањем и постају нереверзибилно измењени.

(Може се рећи да долази до закључавања трансформисаног биометријског обрасца – нетрансформисаним биометријским обрасцем.)

Након тога, бежичним рачунарским системом, тунеловањем, шифрат (**A'**, **A**) који је уствари биометријски кључ, стиже до удаљеног рачунарског система који врши проверу тог кључа, поредећи га са депонованим биометријским кључевима. Уколико је верификација успешна, систем „откључава“ одговарајући досије са неопходним подацима и шаље их на умрежени бежични биометријски читач. Уколико је верификација негативна, полицајац добија поруку система и понавља поступак.



Шема 3

Оно што је изузетно важно нагласити је, да се после трансформисања оба бинарна резултата (на мобилном читачу), они бришу из меморије.

Евентуални нападач који „снифује“ тј. прислушкује саобраћај, снима њему потпуно неразумљиве податке.

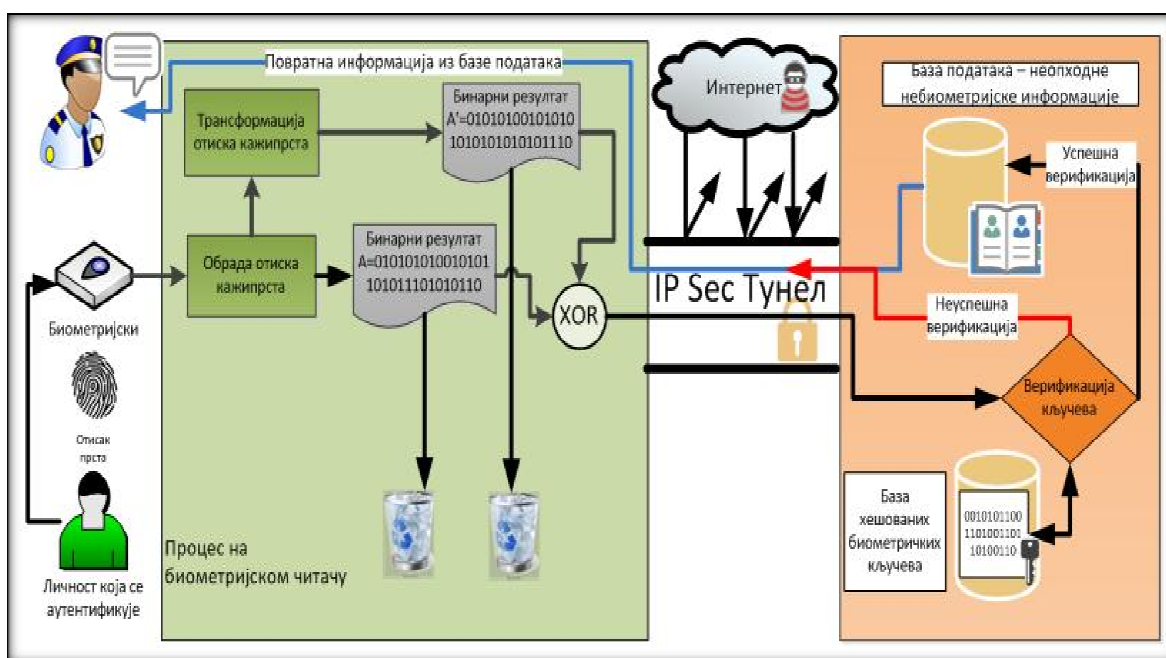
Лоша страна ове шеме била би могућност честог одбацавања резултата, која је природно условљена варијацијама у читавањима.

Треба напоменути да већ данас постоје алгоритми са изузетно високом стопом тачног прихватања са 99, 83%, који теже нултој стопи лажног прихватања FAR (*eng. FAR*), и са стопом лажног одбијања од 0,17% (*eng. FRR*). (Ong Thian Song, Andrew Teoh Beng Jin, Tee Connie, 2007)

2.3.5.3 Предложена шема 2

Ситуација 2 (Шема бр.4):

Први део ситуације 2 је идентичан ситуацији 1, до момента где се два бинарна резултата хешују, уместо њихове алгоритамске трансформације. Хеш вредност се шаље тунеловањем, а уместо биометријских кључева, у базама података се чувају хеш вредности које су уствари хеш кључеви. Они се пореде и уколико је вредност одговарајућа, систем поступа као и у претходном случају.



Шема 4

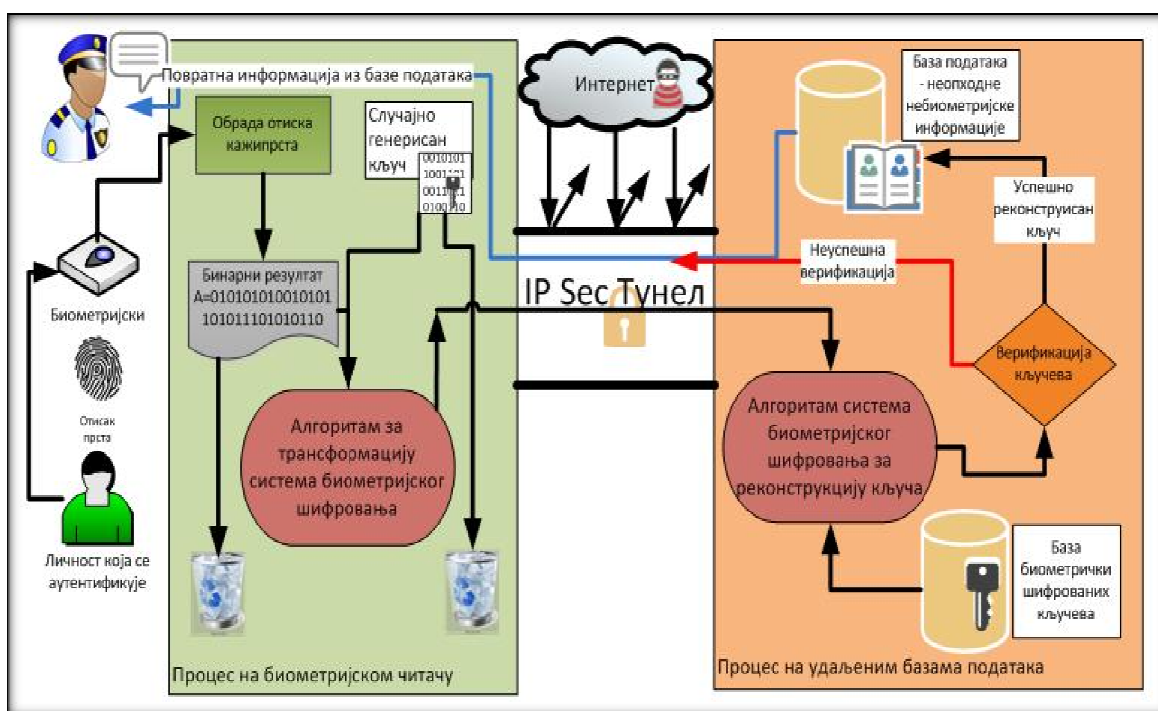
2.3.5.4 Предложена шема 3

Ситуација 3 (Шема бр.5):

Ситуација 3 се технички разликује од прве две. Она подразумева постојање генератора кључева (ПРНГ)⁶³ који генерише псеудо-случајни кључ и после биометријског читавања и добијања биометријског шаблона, везује га кроз алгоритам трансформације система биометријског шифровања. Тако трансформисан образац одлази до удаљеног система где пролази кроз алгоритам за реконструкцију кључа. Сервер реконструисани кључ користи (а образац брише) и откључава потребне податке.

Овакав модел може имати потенцијално високу стопу лажно прихваћених кључева, али то у сваком случају зависи од квалитета алгоритма.

Философија ових система мора бити расплнута (*eng. fuzzy*), како би се стопа тачности повећала, а усклађивање Хамингове дистанце на праве вредности може бити кључно.



Шема 5

Оно што би свакако било интересантно је да саобраћани полицајац на терену, не би имао приступ базама података на серверу (не би могао „да разгледа базе“) без биометрије појединца која откључава САМО његов досије.

Након провере, полицајац утврђује да ли особа има возачку дозволу, да ли има забрану и сл. На почетку је речено да полицајац захтева и име и презиме возача. То је секундарна провера тачности биометријских података. Наиме, постоји (изузетно мала) могућност да систем погрешно, да пошаље туђ досије, а да и возач и изглед особе на фотографији буду слични. Име и презиме, тада, могу упозорити саобраћајца на грешку система.

⁶³ Псеудо-рандом генератор, генератор псеудо-случајних бројева

3 Закључак

Имплементација овако замишљеног система, имала би несумњиво велике економске, социјалне, друштвене и политичке последице. Навешћемо само неке.

- **На првом месту се намеће могућност укидање законске обавезе ношења личних докумената, као и њихово постојање.**

Зашто би човек уопште био присиљаван да носи некаква документа са собом? (Свако за себе зна ко је). Документи су нам потребни само приликом аутентификације, а видимо да ни они више нису потребни. Можемо се идентификовати преко „онога што јесмо“.

Већина држава развијеног Запада уопште нема личне карте. У САД де факто идентификациони документ је возачка дозвола (и то изборно биометријска, у зависности од државе до државе). Лична карта не постоји.

Парламент Велике Британије је Законом о идентификационим документима (*eng. The Identity Cards Act*”, 21.јануара 2011), укинуо Закон о Личним картама из 2006, и биометријске личне карте у УК су укинуте, сем за стране држављане.

Канада. После темељног истраживања, које је обухватило и обилазак земаља које имају биометријске исправе, комисија је 8. октобра 2003. готово једногласно усвојила извештај (*eng. Report of the Standing committee on citizenship and immigration*) да предложени пројекат израде биометријских личних карти представља беспотребно губљење времена и ресурса.

Аустралија и Нови Зеланд су одбацили увођење биометријских докумената.

У Јапану, технолошки најразвијенијој земљи, не постоје обавезне личне карте. Постоји само систем под именом Јуки-Нет, који представља електронски систем идентификације, али на добровољној бази и који има мали број корисника у односу на број становника. Међутим, и поред тога што је пројекат на добровољној бази, неколико префектура је донело судске одлуке да је пројекат неуставан, јер се коси са чланом 13 Устава те земље који гарантује приватност грађана. 73% грађана Јапана нема Јуки-Нет личне карте.

Слично се десило и у Тајвану, само на нивоу Врховног суда, јер је 22. јуна 2005. године тај суд стопирао биометријски пројекат који је развила тајванска Влада, јер је оценио да би пројекат прикупљања дигиталних отиска прстију и стварања националне базе истих могао бити неуставан, што би довело до беспотребног трошења новца за опрему. (Суботић О. , 2011)

Једина земља која се супротставља овом тренду је Индија, која је сваком од својих 1,2 милијарде становника издала биометријске личне карте. Куриозитет је у томе што милиони Индијаца живе у удаљеним селима и никада нису имали никакав документ којим се званично потврђује њихово постојање.

- **Недвосмислена аутентификација пред службеним лицем**

Уколико би се унапредили алгоритми и постигли жељених 100% тачности аутентификације.

- **Буџетске уштеде државе, као и уштеде грађана на (не) издавању личних карата би биле енормне.**

Треба само замислити колико личних докумената типа биометријске личне карте, возачке дозволе, саобраћајне дозволе има... Ради се о милионима документа. Треба замислити колико пратеће документације се користи у том процесу, папири, оловке, штампачи, таксе, време које се проводи у чекању...

Велики број бирократа, више не би био потребан. Многи би остали без посла, али би држава смањила непотребну администрацију и буџетска расипања.

- **Утицај на приватност, такође, био би огroman.**

Уместо да се гомилају и централизују подаци, а грађани профилишу, имали би почетак супротних трендова. Саобраћајцу није неопходно да зна да је неко платио порез или за кога навија возач. Није му потребно ни сазнање о нечијој болести или брачном стању.

Ако замислимо понижење (које аутор овог рада сваки пут осети) када изађете на биралишта, када вас неко „обележи“ чувеним невидљивим спрејовима, уместо аутентификације попут оне које су наведене у објашњењу предложених шема, без „прскања“.

- **Политичке последице би такође постојале.**

Могле би бити укинуте манипулације око вишеструког гласања, могло би се гласати било где на територији Србије, сваког тренутка би се знао тачан број изашлих на биралишта. Коначно би се средили и бирачки спискови. Тренутно добијање масовних података могло би бити корисно у друштвеним и политичким анализама.



Слика 3-1 Веричип имплант, 12 mm дуг, а 2,1 mm широк

- **Повећање комфора, слободе и осећаја среће због немања обавезе ношења докумената.**
- **Могла би бити отклоњена опасност чиповања**

Некритички заговорници коришћења информационих технологија иду до тога да због могућности губитка токена или електронског идентификационог документа чип, треба да се имплантира у људско тело како нико други не би могао да га употреби уместо вас. На мала и велика врата се говори о тим технологијама, а компанија Веричип (*engl. Verichip*) ⁶⁴ је савладала ту технологију.

Рад на биометрији приватности показује да је могуће, не само не размишљати о имплантима, већ и да је могуће размишљати чак и о непотребности личних документа. Већина ствари у животу могу да се употребе, али и злоупотребе. Аутор овога рада позива на коришћење и технологија и достигнућа на добробит, како појединачна, тако и целокупног људског друштва. Остаје само нада да ће осећај посебности човека, свест, а што не и уверења, зауставити киборгизацију која је започела свој пут.

На крају, као закључак се намеће мисао да се биометрија засигурно не може зауставити. Треба је искористити за очување приватности и унапређење људских слобода.

⁶⁴ http://1.bp.blogspot.com/_NIdOvK-wjYc/SX5zO7qZhZI/AAAAAAAAA0/UXfuMT1J0ZY/s320/chip+and+rice.jpg

Литература

- [1] Станковић О., Вединелић В., **Увод у грађанско право**, Номос, Београд 1996.
- [2] Оливер Суботић, **Информационо контролисано друштво**, Бернар, Стари Бановци 2011.
- [3] Ang, R., Safavi-Naini, R. & McAven, L. F. (2005). *Cancelable key-based fingerprint templates*. In C. Boyd & J. Gonzalez Nieto (Eds.), *Australasian Conference on Information Security and Privacy* (pp. 242-252). Germany: Springer.
- [4]

Списак слика

Слика 2-1- Отисак длана праисторијског човека на зиду пећине Шавé, јужна Француска	- 6 -
Слика 2-2 - Отисак длана праисторијског човека на зиду пећине Ел Кастиљо, Шпанија.	- 7 -
Слика 2-3- Отисак прста у глини кориштен од Вавилонаца.	- 7 -
Слика 2-4 - Пример буле (печата), Римљана (са отиском прста).	- 8 -
Слика 2-5– Кинески документ „потписан“	- 8 -
Слика 2-6- Статуа Рашида Ал Дин Хамаданија у Ирану	- 9 -
Слика 2-7 Аутопортрет (фотографија) Алфонса Бертилиона	- 10 -
Слика 2-8 Хенри Фолдс (<i>engl. Henry Faulds</i>)	- 11 -
Слика 2-9 Аутентична историјска фотографија из криминалистичке евиденције српске полиције	- 13 -
Слика 2-10 Др Арчибалд Рајс	- 14 -
Слика 2-11 Др Арчибалд Рајс: „Чујте Срби“	- 14 -
Слика 2-12 Урна Др Арчибалда	- 14 -
Слика 2-13 Криминално-техничка лабораторија Србије између два светска рата -	15 -
Слика 2-14 Криминално-техничка лабораторија Србије	- 16 -
Слика 2-15 Бушена картица, ИБМ картица, или Холерит картица	- 18 -
Слика 2-16 Рач. интерфејс за приступ ИАФИС-у, фирме Фори технолоџис (<i>Foray Technologies</i>)	- 19 -
Слика 2-17 Рач. интерфејс за приступ ИАФИС-у, фирме Папилон Системс (<i>Papillon Systems</i>)	- 21 -
Слика 2-18 Лого Интерпола	- 22 -
Слика 2-19 3Д биометрија	- 23 -
Слика 2-20 3Д биометрија шаке	- 23 -
Слика 2-21 Хитачи систем за видео назор (<i>Hitachi Kokusai Electric surveillance system</i>)	- 24 -
Слика 2-22 Демонстрација функционисања система Гугл-гоглс	- 25 -
Слика 2-23 Учесталост коришћења биометријских технологија	- 26 -
Слика 2-24 Папиле на врховима прстију	- 28 -
Слика 2-25 Ручица бебе 51 дана у материци	- 28 -
Слика 2-26 Основни облици минуција	- 29 -
Слика 2-27 Оби чан лүк	- 31 -
Слика 2-28 Шаторски лүк	- 31 -
Слика 2-29 Кости десне руке (поглед спреда и од позади)	- 32 -
Слика 2-30 Лакатна петља	- 33 -
Слика 2-31 Радијална петља	- 33 -
Слика 2-32 Лакатна петља (леве руке)	- 34 -
Слика 2-33 Радијална петља (леве руке)	- 34 -
Слика 2-34 Обична спирала	- 35 -
Слика 2-35 Спирала са средишњом петљом	- 35 -
Слика 2-36 Спирала са двоструком петљом	- 35 -
Слика 2-37 Спирала случајности	- 36 -
Слика 2-38 Спирала са бочним џепом	- 36 -
Слика 2-39 Хуангов прст без отисака	- 36 -
Слика 2-40 Хуан Тианг (黄振添) са сином и унуком без отисака прстију	- 37 -
Слика 2-41 Стопало коале	- 38 -

Слика 2-42 Папиларне шаре на прстима орангутана	- 38 -
Слика 2-43 Зебре – биометријска различитост	- 38 -
Слика 2-44 <i>Stenochaetus strigosus</i>	- 38 -
Слика 2-45 <i>Stenochaetus Hawaiiensis</i>	- 38 -
Слика 2-46 Д. Брендис	- 39 -
Слика 2-47 Д.Ворен	- 39 -
Слика 2-48 Роџер Кларк.....	- 41 -
Слика 2-49 Др Оливер Суботић	- 42 -
Слика 2-50 Др Ен Кавокијан.....	- 46 -
Слика 3-1 Веричип имплант, 12 mm дуг, а 2,1 mm широк.....	- 55 -

Списак табела

Табела 1	- 30 -
----------------	--------

Списак шема

Шема 1 Шема биометричког шифровања при упису биометријског кључа у базу података	- 47 -
Шема 2 Шема верификација биометријског кључа из базе података и реконструкције кључа	- 48 -
Шема 3	- 51 -
Шема 4	- 52 -
Шема 5	- 53 -