УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

БИОМЕТРИЈСКИ ЛИЧНИ ПОДАЦИ

(мастер рад)

Ментор:
проф. др Милош Прица

Студент:
Бојана Антанасијевић
М004/22-ИТ

Ниш, 2024. године

Садржај:

I Увод

Подаци о личности представљају опредмећени део самог човековог идентитета. Једна од значајних последица развоја информационих технологија у последњих двадесет година јесте енормно повећање количине података. Логично је да, са повећањем броја података, расте и могућност њихове злоупотребе како од стране самих појединаца тако и компанија и државних институција. Слободан проток информација данас представља нужност али и велику претњу за приватност, независност и индивидуалност података. У Универзалној декларацији о људским правима из 1948. године, Европској конвенцији о људским правима из 1950. године и Пакту о грађанским и политичким правима из 1966. године права нису била ограничавајућег карактера, па је примена и остваривање заштите појединих универзалних права показала да се у оквиру права на поштовање приватног живота мора штитити и право на заштиту података о личности. Након тога, право заштите података се одвојило из права на поштовање приватног живота и настало као посебно фундаментално људско право. Као и са већином других земаља и Република Србија је зајамчила уставом највредније човеково богатство-његову личност а подаци су неодвојиви од саме личности.[1] Одређење појма податка можемо пронаћи у Закону о заштити података о личности [2]који је почео да важи 2019. године и усаглашен је са најважнијим документом којим се регулише ова област Општом уредбом о заштити података – GDPR.[3] Основни принципи којима се законодавац водио приликом регулисања имплементације GDPR у Србији редстављају следећа начела:

- Законитости, поштења и транспарентности;
- Ограничења у односу на сврху обраде;
- Минимизације података;

[1] Устав обезбеђује људско достојанство, као саставни елемент човека и његове личности. Као такво, оно је неприкосновено и сви су дужни да га поштују и штите. На овај начин људско достојанство ужива исти степен заштите као сам људски живот, који је неприкосновен. Чл. 23, Устава РС, „Сл. гласник РС“, бр. 98/2006.

[2] Закон о заштити података о личности, „Сл. гласник РС“, бр. 87/2018.

[3] https://www.poverenik.rs/sr-yu/%D0%BC%D0%B5%D1%92%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8-%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B86/%D0%B5%D0%B2%D1%80%D0%BE%D0%BF%D1%81k%D0%B0-%D1%83%D0%BD%D0%B8%D1%98%D0%B0/3443-%D0%BE%D0%BF%D1%88%D1%82%D0%B0-%D1%83%D1%80%D0%B5%D0%B4%D0%B1%D0%B0-%D0%BE-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B8-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BE-%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8.html

- Тачности података;
- Ограничења чувања података;
- Интегритета и поверљивости података;
- Одговорности за поступање.

Наведена начела суштински осликавају и основне принципе Уредбе Европске уније о заштити података о личности. Тумачење и спровођење GDPR у Србији подржава искључиво законито и тачно прикупљање и обраду података о личности, односно његово временско ограничење и прописивање одговорности лица које врше обраду личних података. Податак о личности представља податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.[4] Имајући у виду значај, пре свега самих података, њиховог складиштења и заштите али и са друге стране њихову правилну анализу, не би ли њихов потенцијал остао сачуван и употребљен највише у сврху очувања човекове личности, овај истраживачки рад је и усмерен што бољем и лакшем разумевању истог. Најпре ћемо се осврнути на преглед саме дефиниције и схватања појма личних података, упознавање са новим изазовом данашњице – постојањем биометрије, биометријским личим подацима, биометријским системима и начином такве идентификације. Кроз рад ћемо се детаљније фокусирати на конкретне врсте биометријских података, начине њиховог прикупљања, складиштења и чувања те на крају њихове заштите, примене и целокупне будућности и значаја у успостављању равнотеже између државног интервенционизма и субјективних права. Сваки допринос овој теми је од велике важности јер нам је виртуелна будућност на прагу, а са њом и огроман задатак на нама, да очувамо оно што се још од памтивека чува те и правни систем мора да испрати те кораке.

[4] Ibid чл. 4, ст. 1, тач.

1.1. Одређивање појма личних података

Право на поштовање приватног живота и право на заштиту података о личности, иако уско повезана, различита су права која су се развила из права приватности. Право на приватност једно је од универзалних права човека установљених у Универзалној декларацији о људским правима (УДЉП), усвојеном 1948. године. Ово право у Европи је потврђено Европском конвенцијом о људским правима 1950. године. ЕКЉП предвиђа да свако има право на поштовање приватности и породични живот, дом и преписку. Мешање у то право властима је забрањено, осим ако је мешање у складу са законом, ако постоји важан и легитимни јавни интерес и неопходно је у демократском друштву. УДЉП и ЕКЉП су усвојени знатно пре почетка компјутерске ере, интернета и информатичког друштва. Нове информационе технологије побољшале су квалитет живота сваког појединца, али су и створиле нове ризике по право на поштовање приватног живота. Као одговор на потребу за стварањем правила која регулишу прикупљање и коришћење личних података. Ово је довело до развоја посебног права заштите личних података. Право на заштиту података о личности није таксативно наведено као једно од основних људских права у међународним правним актима који су представљали темељ универзалних људских права.

Како се убрзано развијају информационе технологије као одговор на исте суочавамо се са великом злоупотребом података о личности. Јавила се потреба за детаљнијим и опсежнијом обрадом података те је у неким државама добила измењени концепт као што је право на информациону приватност (САД, УК, Јапан...) или право на информационо самоодређење (Немачка)[5]. Право на заштиту личних података и право на поштовање приватног живота уско су повезана права која штите међусобно повезане вредности: слободу, људско достојанство и аутономију појединца, омогућавајући му да развија своју посебну сферу личности. Оба права су суштински предуслов за остваривање других фундаменталних људских права, као што су слобода изражавања, слобода удруживања, слобода вероисповести, итд. Разлика између права на поштовање приватног живота и

[5] J. Slemmons, J.Стрaford, Data Protection and Privacy in the United States and Europe, IASSIST QUARTERLY January 1999.,Vol.223. https://pdfs.semanticscholar.org/b943/61448c2772cfaab7ad3ffcb66b60e058acac.pdf;
Y. Orito, K. Murarta, Rethinking the Concept of Information Privacy: A Japanese Perspective; This study was supported by an Academic Frontier project for private universities entitled “Global Business and IT Management: Global e-SCM”: a matching fund subsidy was provided by MEXT (the Ministry of Education, Culture, Sports, Science and Technology), 2002-2006. http://www.isc.meiji.ac.jp/~ethicj/Orito.pdf

права на заштиту података о личности је у њиховом обухвату и формулацији. Док је право на поштовање приватног живота формулисана као забрана мешања која је подложна изузецима на основу јавног интереса, право заштите података о личности је формулисано као право да се подаци о личности не обрађују без нашег знања и пристанка нити у сврхе које нису изричито наведене, а такође садржи и активно право провере од стране независних органа и појединаца[6]. За податке се данас каже да су они "нафта 21. века" што са сигурношћу и можемо да потврдимо с обзиром на то колика је њихова вредност. Подаци о личности ће постојати док год постоји човека самим тим не постоји крајња граница у искоришћавању истих. Подаци о личности представљају карактеристичну особину одређеног лица. Они се користе у свакодневним животним ситуацијама, служећи као средство конкретизације и остваривања правних односа. Међутим, подаци о личности не представљају само средство идентификације. Заправо, они представљају појавни облик одређене личности у правном животу који служи за остваривање различитих права и интереса. Да би један податак представљао податак о личности он мора да се односи на физичко лице, што искључује правна лица из обима заштите. Није важан начин и средство путем кога се сазнају, као ни која врста података је у питању. На крају, податак о личности мора се односити на посебну карактеристику физичког лица која га чини јединственим, при чему је неопходно да се ради о конкретном лицу или о лицу које може бити одређено (одредиво) на основу чињеница конкретног случаја.

Ово одређење разликује се од дефиниције која је садржана у претходном Закону о заштити података о личности (2008). Претходни закон одређивао је податак о личности као „сваку информацију која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и слично), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања, начин сазнавања информације (непосредно, путем слушања, гледања, односно посредно, путем увида у документ у којем је информација садржана) или без обзира на друго својство информације"[7]. Претходни закон изједначавао је податак о личности са конкретизованом информацијом. Такво решење није било адекватно будући да се мора правити разлика између информације и податка, па је боље

[6] Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2018.
[7] Чл. 3 ст. 1 тач. 1, Закона о заштити података о личности „Сл. гласник РС" бр.97/2008.

податак о личности одредити по својој правној природи, него га одређивати у односу са информацијом. Појам податак о личности у прописима права у Србији изједначен је са појмом података о личности у прописима европског права. Лични податак је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена (папир, трака, филм, електронски медиј). Постоје две категорије личних података. Прва категорија обухвата податке који чине физички део саме личности. Реч је о биометријским подацима (својеручни потпис, отисак прстију, дигитализована слика лица, скен очне рожњаче и др.) који, као непроменљиви и неодвојиви од личности, представљају личне податке у ужем смислу. Другој категорији личних података припадају типови података који говоре о личности, али нису њен физички део (име, национална припадност, пол, језик, вероисповест и сл.). Будући одвојиви од личности, те и потенцијално заменљиви, ови типови података представљају личне податке у ширем смислу, за које ћемо из разлога јасног предочавања и разликовања употребити израз „подаци о лицу“.[8]

1.2. На које све начине остављамо личне податке

[8] О. Суботић, Биометријски системи идентификације, Београд 2007. године, стр. 20-21.

Наше личне информације се налазе у огромним базама података широм интернета којима се лако може приступити. Свака државна или привредна организација, удружење или институција, која је у законској обавези да нам утврди идентитет пре него што нам испоручи услугу, било да је реч о школи, болници, електродистрибуцији, банци, интернет провајдеру, прикупља разне наше податке. Продавци новина или ципела, на пример, немају ову обавезу, али им уговори и дозволе могу омогућити да прикупљају податке о личности, како би нам доставили робу на кућну адресу или послали рекламну поруку. Без обзира да ли податке узимају уз наш пристанак или по другом правном основу, да ли поступају као државни органи или приватне организације, сви актери који обрађују личне податке обавезни су да ускладе своје пословање са Законом о заштити података о личности. Сви лични подаци на интернету се могу поделити у три категорије:

- Активни дигитални трагови - подаци (о себи или другима) које сами корисници остављају приликом коришћења интернета, обично свесно, мада не нужно и намерно (нпр. приликом куповине неких производа, преузимања нечега са интернета, постављања фотографија, отварања профила на некој друштвеној мрежи);
- Пасивни дигитални трагови – подаци које корисници остављају на интернету приликом његовог коришћења, углавном несвесно (нпр. путем колачића[9] , отиска прстију, података о локацији, коришћења паметних ствари и паметних играчака);
- Подаци добијени анализом првих двеју категорија података, помоћу алгоритама (кроз процес профилисања), евентуално у комбинацији са другим изворима података.[10]

Интернет је донео нове начине на које се може са погубнијим последицама повредити нечија приватност (неовлашћено праћење, складиштење и обрада информација о активностима корисника интернета). Најопаснији вид података – МЕТАПОДАЦИ – високоризичне категорије информација по приватност човека. Метаподатке треба евидентирати приликом прикупљања личних података и потребно их је ажурирати када се подаци мењају. Односно, важније радње над личним подацима треба забележити кроз

[9] Eng. Cookies- комадићи података које интернет сајтови размењују са корисничким уређајем за краткорочно памћење активности корисника на сајту.
[10] https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat

метаподатке. Метаподаци дају одговоре на питања повезана с изворoм података као што су: Ко је створио извор податка? Шта је садржај извора? Када је створен извор података? Које подручје обухватају подаци? Зашто су прикупљани? Како су подаци прикупљани?[11] У теорији и пракси, најраспрострањенија дефиниција је да метаподаци представљају податке о подацима. Свакако велики обрађивачи метаподатака јесу државне односно службе које брину о јавној безбедности, којима закон даје могућности да податке прикупљају и обрађују и без сагласности физичких лица, али уз поштовање унапред одређених сврха и у случају поштовања легитимних интереса за ту обраду. Такође, данашње највеће светске компаније попут Google-a или Facebook-a модел свог пословања заснивају управо на прикупљању и коришћењу метаподататка корисника. Исти случај је и са многим другим платформама за бесплатну размену порука, блоговање, размену слика, видеа итд. Иако, наизглед бесплатни сервиси, своје услуге наплаћују управо приватним подацима. Примера ради, у mail комуникацији метаподатком би се сматрала адреса пошиљаоца, адреса примаоца, наслов mail-a, mail сервис који је коришћен за размену mail-a, али не и сама садржина mail-a. Метаподаци нам такође говоре о датуму креирања податка, намени, значењу, аутору односно креатору, локацији рачунара на ком је креиран податак, коришћеним стандардима, величини фајла, квалитета, извора податка и процеса и метода коришћених код његове производње. Данашњи софтверски системи уз помоћ алгоритама лако повезују податке и на основу њих генеришу слику о оствареним контактима, интересовањима и другим склоностима лица на које се односе те на тај начин прате његово кретање и предвиђају понашање. Не мора увек бити случај транспарентности података широј друштвеној заједници већ само одређеним лицима којима је намењено, с тим да то не искључује чињеницу да такви подаци могу лако да дођу у руке оних који ће то учинити доступним и на тај начин угрозити приватност.

1.3. Дигитална сигурност и подаци о личности

[11] Ж. Хећимовић, Метаподаци, Свеучилиште у Сплиту, Факултет грађевинарства, архитектуре и геодезије, Катедра за геодезију и геоинформатику, Сплит 2016. године, стр.7.

Према речима Хелен Нисенбаум, професорке информатике на Универзитету Корнел, „Приватност није право на тајност, нити на контролу, већ право на одговарајући проток личних података.” Тек са раним хришћанством и пропагирањем молитви у тишини, права и потребе за осамљеношћу и изолацијом, приватност у пуном смислу речи добија на значају. Ако узмемо у обзир и чин исповести, а нарочито праксу у западноевропском хиршћанству, где су исповедаонице пројектоване на начин да обезбеде визуелну приватност исповеданог, можемо закључити колико је чин приватности унутар друштва и односа људи међусобно значајан у хришћанској вери. Међутим, у односу према Богу, према хришћанским веровањима и обичајима, приватности нема, јер је односу између човека и Бога, непосредан и транспарентан.[12] Интернет је донео нове начине на које се може повредити нечија приватност са много погубнијим и далекосежнијим последицама по оштећеног. Кроз податке личности који се тим путем могу прикупити, може се заћи у најдубље сфере личности, а људски интегритет се може непоправљиво угрозити на најтеже начине.[13]Свако од нас је мање или више свестан свог дигиталног окружења и сам може лично одлучити са ким ће га делити. Потребно је упознати се како и у које сврхе се користе наши лични подаци, ко их складишти и чува и како се исправљају и бришу уколико имају неких неправилности. Велики број сајтова и апликација (видео игрице, друштвене мреже, web-сајтови за клађење...) тражи од новопријављених да упишу свој узраст. Углавном је уписана граница година старости испод које се не може регистровати нови корисник. Садржај оваквих страница, њихова намена или што се прикупљају подаци старијих особа није намењен деци или особама испод одређеног узраста. Према америчком Закону о заштити приватности деце на интернету (The Children’s Online Privacy Protection Act – COPPA), ниједна организација нити особа која користи услуге на интернету (укључујући и власнике друштвених мрежа) не сме да прикупља личне податке особа млађих од 13 година без одобрења њихових родитеља или старатеља.[14] Такви услови се налазе у Условима за коришћење одређене странице или сервиса и могуће их је потврдити уписом погрешних броја година него ли оних које су прописане. Типични примери су данашње популарне друштвене мреже као што су Facebook, Instagram, Tiktok, Snapchat...

[12] Д. Поповић, М. Јовановић, Право Интернета – одабране теме, Правни факултет у Београду, 2017. године, стр. 123.
[13] Ibid.
[14] https://www.ftc.gov/system/files/2012-31341.pdf

Родитељи се суочавају са изазовом да ли да своју децу региструју у узрастима млађим од наведених, те се на тај начин укључе у дигитално окружење у којем се могу суочити са садржајем који није њима прилагођен (узнемирујући, експлицитни или насилни...) или види нешто што не жели, или да његов профил буде обрисан с обзиром да нису испуњени услови за његово коришћење.

Са развојем информационих технологија дигитална сигурност је неизбежни део сваког разговора. Аутоматизована обрада личних података, у односу на конвенционалну, у крајњем исходу значи повећану ефикасност за онога ко се служи таквом обрадом и већи ризик угрожавања приватности појединца, посреди је неоправдано (нелигитимно) ограничавање приватности. У таквим случајевима конвенционални (традиционални) захвати државне власти у приватну сферу појединца (у зависности од облика и интезитета примене информационих технологија) мењају своју природу и сврху. Информационим друштвом можемо сматрати оно друштво које функционише претежно помоћу информационих технологија, које као снага напретка служи и интересима грађана. Његова супротност јесте тзв "информационо контролисано друштво" (друштво информатичке репресије), када центри моћи користе информационе технологије ради надзора над понашањем грађана.[15] Усложњавањем разних функција многе радње олакшава употреба интернета а са њим и потреба остављања личних података. Данас је могуће извршити различите уплате широм света само једним кликом, купити, послати пакет, те у свакодневној дигиталној комуникацији остављамо безброј наших личних података на које треба пазити. Велики број истих лозинки користи се за различите мреже или се кликће на линкове који су несигурни. Врло је корисно инсталирати различите програме и антивирусе који би, на неки начин, заштитили отпуст личних података у нежељеном правцу. У правним поретцима савремених држава, типове неоправданог ограничавања приватности појединца, применом савремених информационих технологија, постоје код издавања биометријских личних докумената, као и код појединих видова надзора електронске комуникације грађана.

[15] О. Суботић, op.cit.,стр. 20-21.

II Биометријски системи

Појам „биометрија“ може имати различита значења зависно од контекста у коме се користи. Етимологија речи говори да је у питању мерење биолошких особина одређеног организма (од грч. имен. ὁ βίος – живот и гл. μετρέω (поимен. ἡ μέτρησις) – мерити (поимен. мерење)).[16] Биометрија је скуп метода за идентификовање појединаца на основу физичких карактеристика и/или карактеристика понашања. Биометријски системи обухватају различите технологије које помоћу биолошких карактеристика човека врши његову идентификацију. Да би се биолошке мере могле класификовати као биометријске морају задовољити услове:

Универзалност: Она се односи на то да свака особа треба да има то својство (карактеристику). На пример, готово сви у некој организацији ће имати барем један прст за отисак прста, али биометрија скенирања хода може бити неизводљива ако имате неку особу са инвалидитетом (у инвалидским колицима).

Јединственост: Односи се на то да свака особа мора имати јединствену вредност одређене карактеристике, то значи да не смеју бити две особе са истим вредностима. Када су у питању близанци, неке особине су јединствене а неке не, тако да треба бити пажљив при одабиру.

Трајност: Добра биометријска особина се не мења у току животне доби човека, или барем у периоду од важности. ДНК и отисак прста у потпуности задовољавају овај услов, док потпис и гласовно препознавање нису баш најбољи избор на дужи период.

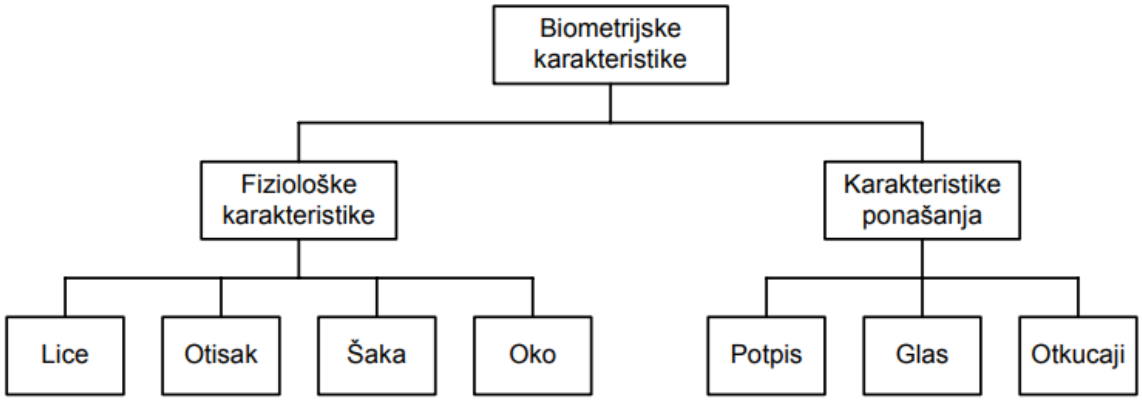
Прикупљивост: Ово подразумева лакоћу са којом можемо узети биометријски узорак неке особе. Вредности неких карактеристика се може прикупити без знања дате особе и без икаквог физичког контакта, док одређене особине захтевају пуну сарадњу. ДНК скор ове особине је веома низак док отисак прста и потпис бележе врло високе резултате.

Могућност обмане: Ово се односи на то колико лако фалсификатор може преварати биометријски систем (на пример, старији уређаји за узимање отиска прста, могу се

[16] J. Ashbourn, The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management, Background paper for the Euroscience Open Forum ESOF 2006, Minhen 2006.

заварати коришћењем такозваног „лепљивог прста"). Али ова особина се такође односи на могућност напада на биометријски систем на друге начине, као што је напад преко мреже.

Примери биометријских карактеристика које се данас користе у аутоматским системима (лице, шака, око, отисак прста, потпис, глас, образац куцања) приказани су на слици 1.[17]



Слика 1 - Подела биометријских система по пореклу карактеристика

Након одабира биометријског система који се користи за утврђивање идентитета мора се водити рачуна и о следећим факторима:

• **поузданост** – односи се на тачност, брзину, као и на факторе који могу утицати на рад система;

• **прихватљивост** – означава степен спремности људи да прихвате коришћење овог система у свакодневном раду;

• **отпорност** – колико је систем отпоран на потенцијално кривотворење и нападе.

У табели 1. дата је перцепција испуњавања горе побројаних услова код различитих биометријских система при чему су В, С и Н ознаке за високо, средње и ниско испуњавање појединачног фактора (услова) респективно.[18]

[17] B. Miller, Vital signs of identity, IEEE Spectrum, February 1994, Vol. 31, No. 2, pp. 22-30.
[18] S. Prabhakar, S. Pankanti, K. Jain, IEEE Security & Privacy Magazine, 1(2), 2003., pp. 33-42.

Табела1. Компарација различитих биометрија

biometrika	univerzalnost	jedinstvenost	nepromenljivost	kolektibilnost	pozdanost	prihvatljivost	otpornost
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	S
Geometrija šake	S	S	S	V	S	S	S
Iris	V	V	V	S	V	N	V
Retina	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N

А. Верификација – врши се када нека особа тврди да има неки идентитет (у традиционалним системима то се радило уз помоћ лозинке, ИД картице и сл.); систем потврђује или одбија идентитет упоређивањем биометријских карактеристика са шаблоном (template) претходно сачуваним у бази и изводи се поређење један–према–један (one-to-one-comparison). Ово је такозвано ‘позитивно препознавање’ чији је циљ да се спречи да више људи користи исти идентитет.

Б. Идентификација – систем мора да изврши препознавање особе тако што ће упоредити њене биометријске карактеристике са свим шаблонима сачуваним у бази да би нашао највеће поклапање. Том приликом се изводи један–према–много (one-to-many) поређења и ово се назива ‘негативно препознавање’ где систем може утврдити да ли је особа оно што имплицитно тврди да није. Циљ је да се спречи да једна особа користи више идентитета.

За разлику од система базираних на лозинкама, где је потребно савршено (100%) поклапање између две вредности како би се потврдио идентитет корисника, биометријски систем ретко сусреће два узорка биометријских особина чије се карактеристике тачно поклапају. То је због несавршених услова очитавања (нпр. лошег отиска прста због неправилног функционисања сензора), промене у корисничким биометријским карактеристикама (нпр. респираторне болести утичу на гласовно препознавање), промене у условима окружења (нпр. неправилан ниво осветљење при препознавању лица) и варијације у интеракцији корисника са сензором (нпр. Оклузија ириса или делимични отисак прста). Биометријски системи функционишу преко уписа корисника мерењем и чувањем њихове одређене биометрије, а касније упоређивањем сачуваних биометријских

података са подацима непроверених субјеката како би се утврдило да ли им се смије дозволити приступ систему или локацији. Погледајмо целокупан процес у више детаља:

Упис: Пре него што корисник може да почне да користи биометријски систем, он мора да попуни (заврши) уписни процес. Овде он даје почетне (уводне) биометријске податке, који се могу састојати од нпр. стављања прста на читач отисака прстију (за биометрију отисака прстију), гледања у објектив дигиталног фотоапарата (за биометрију шаренице ока) или понављања неких речи или израза (за гласовну биометрију).

Употреба: Када корисник жели да приступи систему са уграђеном заштитом на принципу биометрије, корисник потврђује веродостојност по поступку, што би могло значити стављање прстију на читач отиска прста, стављање руке (шаке) на скенер за руку, давање ручног потписа или окретање лица према камери ради скенирања.

Ажурирање: За тип биометрије који се споро мења током времена (као што је рукопис или препознавање лица) биометријски систем ће можда морати да ажурира податке који су првобитно дати на упису. Ово ажурирање се може обавити са сваким наредним мерењем, чиме се повећава број узорака, са нагласком на новијим, или се може користити засебан процес ажурирања. Биометријски системи су генерално прилично једноставни за кориштење. У већини случајева, чак и упис траје само минут или два, и за свакодневну употребу потребно је само неколико секунди.

2.1. Биометријска идентификација и приватност

У контексту тако одређеног идентитета, информације о личности се често разлажу на три компоненте: атрибутивну (име и презиме, датум и место рођења, место пребивалишта...), биографску (детаљи везани за запослење, школску спрему, финансијске трансакције...) и биометријску (лични биометријски подаци попут слике, потписа, отисака прстију...). По питању наведених података, могла би се увести и другачија класификација, у смислу података о личности и личних података, која се често користи када се прави разлика између биометрије (која је лична особеност, тј. лични податак) и других типова података (који говоре о личности, али нису физички део ње саме).[19] У том контексту, идентификација представља процес у коме се помоћу одређеног броја мање или више дистинктивних података једнозначно утврђује идентитет одређене особе у конкретном друштву (тј. ко је та особа). Аутентификација (потврда аутентичности) представља процес у коме се успоставља одређени степен сигурности у складу са тврђењем одређене особе зарад постизања различитих циљева.

Препознавање личности изгледа једноставно због тога што га људи свакодневно врше напослу, улици, кући, на било ком другом месту где долазе у контакт са другим људима. Међутим, у модерном свету, оно није тако лако као што се чини. Технолошки развој, постојање глобалне рачунарске мреже која се сваким даном све више шири, повећање броја путника на глобалном нивоу, као и аутоматизација разних послова и услуга захтева поуздане методе за утврђивање и проверу идентитета. Наиме просечна особа се дневно идентификује више од 10 пута приликом коришћења рачунара, телефона, кредитних и платних картица, аутоматских терминала за исплату новца, примања социјалне помоћи, коришћења здравствених услуга[20]. Идентификација личности треба да буде брза, поуздана, тешка за превару, јефтина, и у великом броју случајева друштвено прихватљива за особу која треба да се идентификује.

У области сигурности позната су 3 различита начина за проверу идентитета:

• Нешто што знаш (knowledge) – шифра, ПИН (лични идентификациони број), нека лична

[19] R. Clarke, Biometrics and privacy, Department of Computer Science, Australian National University,Canberra, 2001., p. 45.
[20] B. Miller, op.cit.,Vol.31,No.2, pp.22-30.

информација (нпр. име маминог пса и сл.);

• Нешто што имаш (possesion) – картицу (нпр. “паметне” или сличне);

• Нешто што јеси – биометрија.

Биометрија користи неке карактеристичне податке (познате и под називом биометријски потпис или кључ) о особи, који омогућавају да се утврди идентитет особе. Биометрија може да позитивно идентификује особу и тиме спречи читав низ превара везаних за идентитет, али она може и да, без дозволе субјекта, прати његове поступке и повеже личне информације из различитих извора, што је велики напад на приватност. Њено коришћење је моћно средство у рукама јаких корпорација (зашто не и влада и њених агенција), да вежбају контролу над појединцем, али и друштвом у целини. Све ово баца ново светло на могућност коришћења али и злоупотребе биометрије.

Биометријска идентификација подразумева настарији вид идентификације. Још у време Сумераца и Египћана су се потврђивали и потписивали уговори на глиненим плочицама остављањем отисака прстију. Временом су се методе идентификације све више усавршавале па је преко тетоважа, жигосања животиња како би се показало чије су власништво, дошло до начина идентификације какав је данас. Развојем технологија успешно је направљен биометријски податак као дигитални али уз могућност да једном украден више не може да се замени, као и то да су као дигитални трагови склони копирању те и на тај начин обмани и крађи. То не представља проблем када су у питању мање мреже али за велике интернет удаљености свакако представљају мету коју чекају пресрети.

Најновији експерименти везани за биометријску идентификацију грађана, који се изводе у неким британским и америчким градовима, интерактивно комбинују сигнал камера високе резолуције које су постављене на јавним местима (тзв. CCTV- Closed Circuit TV) са алгоритмима за препознавање лица, специфичних покрета и динамике кретања. Циљ је, према речима владиних службеника, да се једног дана добије систем за интерактивно препознавање сваког пролазника и сузбијање потенцијалних криминалних активности.[21]

[21] K. Ball, D. Lyon, D. Murakami Wood, C. Norris, C. Raab, A Report on the Surveillance Society, Full Report, 2006., p. 24.

Биометријска идентификација подразумева технике мерења и статистичке анализе људских карактеристика и ослања се на две методе идентификације:

-статистичка биометријска идентификација- проверава физичке карактеристике појединца (отисак прста, облик лица, дужина ока...)

-динамичка биометријска идентификација- проверава различита понашања тог појединца и као таква идентификација узима се глас или рукопис корисника.

У зависности од броја метода која се користе у идентификацији постоји и пропорционалан број погрешних идентификација који се решава на разне начине.

Све технике биометријске идентификације садрже у себи основни модел пословања. Модел се састоји од два одвојена дела. У првом делу је узимање биометријских података њихова компресија и складиштење у базу података. Овим се обезбеђује да када се корисник појави и затражи идентификацију постоји податак о њему са којим се може упоредити. Овде су могуће две варијанте: Једна варијанта је да приликом узимања биометријског отиска, систем проналази у бази података одговарајуци запис и упоређује га са узетим отиском. Логика овог система је питање "Да ли систем зна ко је власник узетог биометријског податка", а то се постиже упоређивањем скинутог податка и податка у бази. Друга варијанта је да приликом узимања биометријских података исти се упоређују са подацима који се налазе на смарт картици или неком другом носиоцу података који се локално убацује у читач како би подаци били упоредени. Логика ове варијанте је "Да ли је власник биометријског отиска стварно тај за кога се издаје.

Резултати упоређивања се прослеђују апликацији на даље пословно процесирање. Коначни упис догађаја са свим пратећим подацима.

Биометрија има неколико предности у односу на остале методе провере идентитета:

-Биометријски узорци се тешко краду, деле и репродукују. Чак и ако неко покуша да приложи лажни узорак, системи су опремљени такозваним “liveness” детектором, који проверава да ли је узорак заиста жив или се ради о такозваном “гуменом отиску прста”.

-Биометријски системи су веома толерантни на нападе грубом силом. На пример, на основу узорака ириса, могуће је произвести кључ за шифровање дужине 256 бита, што значајно отежава нападе грубом силом у односу на лозинке дужине 6-7 карактера састављене од малих слова и, евентуално, бројева.

-Биометријски системи намећу идентични ниво сигурности свим корисницима. За разлику од лозинки, не постоје краћи, дужи, једноставнији или сложенији узорци.

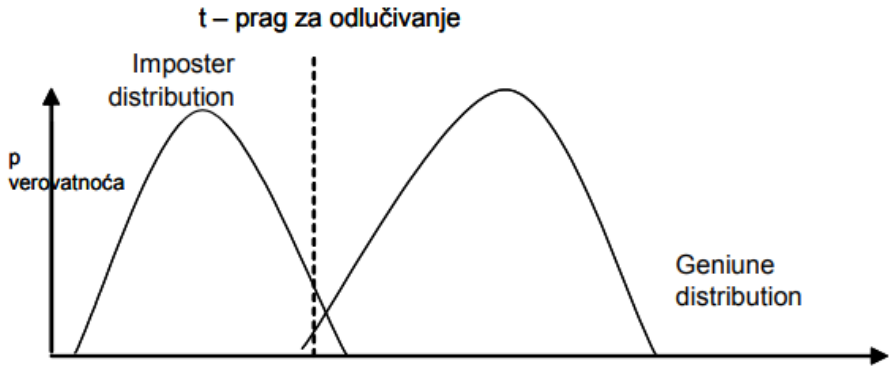
-Биометријски системи пружају сигурносну услугу непорецивости. На пример, уколико се за контролу провере радног времена на послу користи идентификациона картица, запослени је једноставно може дати колеги и на тај начин "допунити" радне сате. Слично, надређени може рећи да га је неко "уписао", чак и ако то није урађено. У случају да се провера врши помоћу биометријских система, нико не може да поништи чињеницу да се одређени корисник пријавио на систем а активности верификованог корисника се не могу оповргнути. Проблеми који прате биометријску идентификацију:

- Уређаји који се користе за идентификацију као и одговарајућа софтверска решења су јако скупи;
- Биометријски системи идентификације су наметљиви;
- Трајно се искључују особе са одређеним хендикепом (оштећење коже немогуће за очитавање, губитак ока...);
- Трајност уређаја још увек није испитана јер су уређаји релативно нови;
- Непоузданост појединих уређаја (причање неистина...);
- Потреба обуке корисника са радом на оваквим уређајима;
- Проблеми са приватношћу;
- Из тог проблема јавља се и проблем стварања централне базе података;
- Базе података погодују онима који краду „ идентитет";
- Недостатак стандарда ; сваки од произвођача има неко своје решење за уређаје за идентификацију;
- Слање биометријских података путем интернета ствара додатни ризик. [22]
-

[22] Др.В. Васковић, Примена биометријских метода идентификације у банкама, Београдски Универзитет ТФ Бор, 2008. године, стр. 99.

2.2.Тачност биометријских система идентификације

Биометријски системи као излазни резултат дају степен подударања (matching score) улазног податка са шаблоном сачуваним у бази. Два узорка исте биометрије од исте особе могу да се разликују у зависности од услова и времена њиховог узимања, па се не може очекивати њихово апсолутно поклапање. Што је степен подударања већи то је систем сигурнији да два биометријска узорка долазе од исте особе. Ипак одлуку система дефинише нека граница (праг) коју корисник поставља у складу са апликацијом за коју се биометријски систем користи. Резултати добијени од поређења парова узорака различитих особа, као и они добијени од поређења узорака исте особе дају нам расподеле које се зову 'impostor distribution' и 'genuine distribution', и приказане су на слици 2. Видимо да се у једном делу преклапају. Приликом пројектовања биометријског система граница (prag) одлучивања се пројектује у складу са специфичним захтевима апликације. [23]



Слика 2. Утицај прага на перформансе (тачност) биометријског система

Тачност биометријских система може се одредити преко две специфичне променљиве а то су:

f FAR (false accept rate) – лажно прихватање, где се биометријске карактеристике од две различите особе прихватају као да су исте;

[23] R. M. Bolle, J. H. Connell, N. K. Ratha, Biometric perils and patches, Pattern Recognition, 2002., Vol. 35, pp. 2727-2738.

FRR (false reject rate) - лажно одбијање, где се биометријске карактеристике од исте особе не прихватају тј. сматрају се узорцима различитих особа. Смањивањем једног фактора (грешке) повећавамо други. Како успоставити најбољи однос зависи од конкретне примене система и од тога где ћемо поставити праг за одлучивање. Наиме ако се жели максимална сигурност да само стварно ауторизовани корисници пролазе кроз систем, чак и по цену да се понекад и одбије ауторизовани корисник онда се смањује FAR по цену повећања FRR. Ово је у случајевима заштите разних сигурносних система. Са друге стране за неке комерцијалне апликације одбијање ауторизованог корисника може нанети велике штете, па се ту смањује FRR на рачун повећања FAR.

III Биометријски идентификациони документи

Резултат оправданог задирања у приватност сваког појединца јесте његово идентификовање пред различитим институцијама, органима и појединцима, те у у ту сврху ради остваривања зајамчених права као и несметаног одвијања друштвеног живота, постоје идентификациона документа у свом конвенционалном (папирном) облику. Како информационе технологије својим убзаним развојем успевају да обгрле све области друштвеног интервенционализма, полако се са већ упознатим дугогодишњим коришћењем папирних докумената прелази на електронске идентификационе документе, баш као што је случај и код, полаког али сигурног, преласка на употребу платних картица а све мање долажење у посед папирног новца као таквог. Електронски идентификациони документи могу бити биометријски и небиометријски. Знамо да биометријско идентификовање подразумева мерење одређених својства сваког појединца у циљу његовог откривања идентитета на основу сопствених карактеристика, имајући то у виду, биометријским називамо оне правно-информационе системе који користе различита физио-биолошка својства и/или мерења понашања људског тела која се могу користити за конкретну идентификацију дате особе. И коначно, биометријски идентификациони документи су само они електронски документи који садрже биометријске податке њеног имаоца.[24]Временом се дијапазон биометријских личних података ширио и усложњавао као и сами биометријски системи идентификације па кренувши још од традиционалних података као што су отисци прстију, својеручни потпис данас постоје генерисање тродимензионалног модела лица, препознавања распореда вена, анализе ДНК структуре, детекцију мириса и специфичних хемијских својстава коже за сваког човека.[25]

Биометријски системи идентификације уз помоћ идентификационих докумената оправдано задиру у приватност сваког појединца али и носе нове изазове и ризике са собом. Уз помоћ биометријских личних података ствара се централна база биометријских података из које произилази тоталитарни потенцијал. Иако звучи много безбедније да је сам ималац података једини власник и да биометријски лични подаци не напуштају идентификациони документ али су они идеалан алат у рукама државе за контролу појединаца, оправдано када је у борби против организованог криминала и модернизације

[24] О. Суботић, op.cit., стр. 50.
[25] Ibid.

државне управе, али да ли стварно њен домашај може бити савршен за оне који су изнад оквира да сачува безбедност и приватност личних података?

3.1. Биометријски пасош

Биометријски пасош представља путну исправу која садржи биометријске личне податке који олакшавају идентификацију лица које прелази границу. Наиме, њихово увођење дошло је као резултат политике Сједињених Америчких Држава након напада који су се догодили 11. септембра 2011. године.[26] Сједињене Америчке Државе најпре су (USA Patriot Act - потписан 26. октобра 2001. и Законом о повећаној безбедности границе и реформи визног система из 2002.) поседовање биометријског пасоша поставиле као услов уласка на њихову територију, а затим је Међународна организација за цивилно ваздухопловство Уједињених Нација године 2003. прописала стандард (ICAO 9303) о електронским пасошима који ће садржати биометријске личне податке. Стандард (ICAO 9303) предвиђа дигитализовану слику лица, не захтевајући притом образовање централне базе података. Предочени стандард прихваћен је од стране Европске уније и Савета Европе, с том разликом што биометријски пасоши европских држава чланица дотичних организација, поред дигитализоване слике лица садрже и дигитализоване отиске прстију, чиме су европске државе предвиделе више биометријских података, него што је случај у Сједињеним Америчким Државама. На основу одговарајућег стандарда утврђен је изглед и садржина пасоша док личне карте зависе од националних законодавстава. Земље Европе (на првом месту Visa Waiver земље, чијим грађанима не треба виза за улазак у САД)[27] су биле принуђене да удовоље захтевима САД које су од њих захтевале израду биометријских пасоша у одређеном року. Око биометријских пасоша у односима ЕУ и САД је било пуно неспоразума. Наиме, иако је 18. фебруара 2004. године Европска комисија дала предлог да само дигитализована слика лица буде обавезан део нових пасоша ЕУ, 13. децембра исте године је донета регулатива по којој су за нове пасоше (или замену старих који су ис-

[26] 11. септембра 2001. дошло је до координисаних напада на Сједињене Америчке Државе. Напади су извршени авионима, који су претходно отети. Два авиона су ударила у зграду Светског трговинског центра, трећи је ударио у зграду Пентагона у Вашингтону, док се четврти срушио у области саставне државе Пенсилваније.

[27] Андора, Аустралија, Аустрија, Белгија, Брунеји, Данска, Финска, Француска, Немачка, Исланд, Ирска, Италија, Лихтенштајн, Луксембург, Монако, Холандија, Нови Зеланд, Норвешка, Португал, Сан Марино, Сингапур, Словенија, Шпанија, Швајцарска, Шведска и Велика Британија.

текли) обавезна и два отиска прста.[28] То је уједно постала и регулатива за земље потписнице Шенгенског споразума (с обзиром да Норвешка и Исланд нису чланице ЕУ),[29] које у своје нове пасоше треба да укључе исте податке (поред дигиталне слике лица и два отиска прстију),[30] као и да морају имати додатне механизме за заштиту података. Крајњи рок наведен да земље Шенгенске зоне уведу биометријске пасоше био је 28. јун 2009. године. Пошто се путовање по шенгенској зони обично изводи преко личних карти (уколико се оне користе као путничка исправа), постојала је могућност да се од земаља те зоне тражи да у личне карте такође угради биометријске податке који се налазе у новом пасошу, мада је то напослетку остављено на опционој основи као аутономно питање националних законодавстава. Информације на биометријском пасошу су заштићене помоћу приватног кључа, а сертификат за дигитални потпис и пар кључева ће се добијати преко сертификационих тела у земљама које ће израђивати ICAO компатибилне пасоше, што и јесте у складу са условом ICAO да информације на пасошу буду везане електронским потписом.[31] Прве земље које су кренуле са увођењем бесконтактних пасоша базираних на RFID (Radio Frequency Identification – бесконтактна идентификација на бази радио таласа) биометријских пасоша су Белгија, Немачка, Шведска и Норвешка.

Република Србија спада у земље које су увеле најсавременији вид пасоша. Подаци који се налазе у пасошу, поред тога што се налазе на папиру самог документа, чувају се и на чипу. Управо у том чипу се чувају информације попут препознавања лица, отисака прстију и изгледа мрежњаче. Овакав пасош је готово немогуће фалсификовати и злоупотребити јер подаци који се чувају на чипу су заштићени немогућношћу уништења чипа. Први биометријски пасош у Србији је издат 2008. године. Пасош се издаје за неограничен број

[28] P. E. Schmitz, R. Tavano, J. Lodge, Ronald Huijgens & al., Biometrics in Europe - Trend Report (BETR), Brisel, 2006., p.54.

[29] У месту Шенген (војводство Луксембург) је 14. јуна 1985. године донет споразум, од стране пет земаља (Немачка, Француска, Белгија, Холандија и Луксембург), који је за циљ имао слободно кретање грађана и роба у оквиру граница земаља потписница (дакле, без пасоша и пратећих формалности). За борбу против организованог криминала на основу тог споразума (члан 93) створен је Шенген информациони систем, гигантска база података у којој се чувају подаци о грађанима земаља потписница. Овај споразум је неколико година чуван у тајности, да би јуна 1990. земље учеснице приступиле његовом остварењу. Касније су се придружиле Италија (1990), Шпанија и Португал (1991), Грчка (1992), Аустрија и Данска (1994). Енглеска и Ирска су одбиле да се придруже, позивајући се на чињеницу да је то највећа регистрација грађана у историји људског рода и да је тај систем антидемократски. Данас се под том зоном налази 15 чланица ЕУ и две које су ван ЕУ (Норвешка и Исланд).

[30] HCICT, p. 14. – Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[31] K. Woodward, „Directory Holds The Key To E-Passport Authentication ", Card Technology, 2006., p.26.

путовања на период од десет година. Он служи за путовање, боравак у иностранству као и повратак у земљу те се на тај начин утврђује идентитет једног лица и доказује српско држављанство. На корицама које су „царско" црвене боје налази се назив „Пасош" исписан ћирилицом у златној боји као и ознака да је пасош биометријски. На унутрашњој страни корица исписано је „Србија", наизменично ћирилицом и латиницом које је видљиво само под ултраљубичастим светлом. Како данашњи пасош има седам нивоа заштите,што је основна разлика у односу на претходни, представља најмодернији пасош у Европи. У дну друге стране налазе се лични подаци имаоца пасоша. Врло је важно да се ова страница заштити како би се спречило фалсификовање. Она има кинеграм[32] и оптички варијабилне боје, у процесу ламинације[33] уносе се мат и сјајни елементи и састоји се од више слојева пластике. Подаци се уносе ласером али не на први слој него на доње слојеве поликарбоната што би значило да уколико неко жели да фалсификује документ мора да оштети површински слој.

Први корак у процесу издавања личног документа је подношење захтева. Подношење захтева подразумева прикупљање текстуалних демографских података подносиоца захтева, затим скенирање папирних докумената, биометријски подаци (отисак прста, слика лица, скен зенице ока….). Након успешног прикупљања података и креирања захтева, даље процесирање захтева повлачи целокупан сет предефинисаних корака. Најпре се спроводе провере над предатим подацима, као и провере самог лица које је поднело захтев, а затим се врши одобравање захтева од стране оператера. Оператер који је задужен за одобравање захтева прво спроводи увид у резултате провера, а затим одлучује по сваком појединачном захтеву. Одобрени захтеви се шаљу на персонализацију како би се за њих

[32] Кинеграм је заштитни елемент који се користи на различитим врстама идентификационих и сигурносних докумената, као што су новчанице, пасоши, личне карте и слично. То је специјални холограмски елемент који се састоји од микроструктуре која ствара визуелне ефекте када се промени угао гледања. Кинеграми се дизајнирају тако да буду тешко копирани и имају за циљ да обезбеде аутентичност и заштиту докумената од фалсификовања. Они могу садржати различите елементе, као што су слике, текст или друге графике, које се мењају када се мења угао гледања.

[33] Ламинација је процес којим се који се затим загрева и стапа са површином материјала. Овај процес ствара заштитни слој који штити од влаге, прљавштине, хабања и других оштећења.

Ламинација се често користи за заштиту и продужење трајности докумената као што су идентификационе картице, возне карте, радне дозволе, као и заштита фотографија, мапа, постера и других штампаних материјала. Такође се користи у производњи амбалаже, етикета и других производа како би се побољшала издржљивост и естетика штити и ојачава папир, картон, фотографије или други материјали. Уобичајени поступак ламинације укључује прекривање материјала транспарентним пластичним филмом.

креирали идентификациони документи. Персонализација докумената је процес у оквиру кога се на бланко документ утискују подаци из одобреног захтева за документ. Персонализовани документи се затим пакују у кутије које садрже баркод пошиљке, након чега се транспортују у одговарајуће испоставе ради уручења. Процес уручења документа започиње утврђивањем идентитета или надлежности особе да преузме документ, након чега се спроводи и само преузимање документа. Уколико документ садржи биометријске податке подносиоца захтева, онда се пре самог уручења спроводи биометријска провера особе која преузима документ спрам биометријских података који се налазе у документу (пример: провера отиска прста спрам отиска који је смештен у чип пасоша)

.

3.2.Биометријска лична карта

Биометријска лична карта представља тип националног идентификационог документа који садржи биометријске податке у електронском облику. Данас, веома мали број земаља има електронске личне карте на националном нивоу у обавезујућем виду. То, пре свега, избегавају јер се возачка дозвола и пасош могу користити за идентификацију а и на тај начин ће избећи формирање централне базе података која представља опасност по приватност појединца. Не постоји неки заједнички став о томе да ли да се уводе биометријске личне карте или не, али се земље Европске уније противе њиховој употреби док их користе за потребе миграната, апликанте за азил или визу. Тако можемо препознати неколико решења, прво се односи на англо-америчко право где се возачке дозволе користе за идентификацију; друго решење негује постојање личних карти у виду папирном (пластифицираном) облику где спадају Француска, Немачка и Грчка. Код трећег решења разликујемо електронске личне карте које могу биометријске и небиометријске. Небиомметријске се пак деле на обавезне (Белгија, Естонија) и необазне (Норвешка, Финска). Биометријске могу почивати на принципу облигаторности (Шпанија, државе "трећег света") или по принципу добровољности где спада и наша држава. Земље у којима је употреба личне карте обавезна могу користити папирну, пластифицирану, електронску са биометријом и без биометрије. Када су у питању личне карте националним законодавствима је дата аутономија. Неке земље Европске Уније као што су Данска и Ирска чак не познају идентификационе документе а неке тек сад почињу да раде на плану

њиховог увођења. У земљама са већинским православним становништвом далеко је актуелнија израда биометријских пасоша због визног услова САД, што је потпуно одвојено питање од биометријских личних карти. Тако Грчка, рецимо, нема планове за увођење електронских личних карти, иако је кренула са пројектом израде биометријских пасоша за своје грађане.

Биометријске личне карте уведене су код нас Законом о личној карти[34] из 2006. године. Њиме је установљено обавезно издавање биометријских личних карти, као и образовање централне базе биометријских података (дигитализованих отисака прстију, дигитализоване слике лица са фацијалним особеностима и дигитализованим потписом). На предњој страни личне карте штампају се следећи подаци:

1. Презиме;
2. Име;
3. Датум рођења;
4. Пол;
5. Регистарски број;
6. Датум издавања;
7. Важи до;
8. Документ издаје.

На полеђини личне карте штампају следећи подаци:

1. Јединствени матични број грађана;
2. Држава рођења;
3. Место и општина рођења;
4. Пребивалиште и адреса стана;
5. Машински читљива зона.

Приликом промене личних података, као што су име, презиме и адресе, као и у случају губитка личне карте, мора се издати друга. Лична карта на старом обрасцу је важила на рок издавања наведеном на личној карти, најкасније до 31. децембра 2016.године.

[34] Закон о личној карти "Сл. гласник СР", бр. 62/2006, 36/2011 и 53/2021.

Држављанин који нема пријављено пребивалиште у Србији, сходно члану 5 Закона о личној карти, може имати личну карту са роком важења од две године. Уколико особа одбије да покаже личну карту полицији или не поседује личну карту добија новчану казну у висини од 50 хиљада динара или 30 дана затвора. Лична карта не поседује RFID, те не испуњава ICAO9303 стандард путних исправа али се може користити као путна исправа у неколико земаља: Босна и Херцеговина, Црна Гора, Македонија, Албанија и Турска (али само у случајевима путовања авионом и то у изузетним случајевима).

Задња страна личне карте са чипом

Задња страна личне карте без чипа

Слика 3. Изглед задње стране личне карте са и без чипа

3.3.Биометријска возачка дозвола

Биометријска возачка дозвола је врста идентификационог документа који користи биометријске технологије за верификацију идентитета возача. Биометријска возачка дозвола има неколико кључних карактеристика и предности:

1.Јединственост идентификације: Биометријске возачке дозволе користе биометријске податке који су јединствени за сваку особу. Отисци прстију, фотографија лица или скенирање шаренице ока омогућавају прецизну идентификацију возача.

2.Сигурност: Биометријски подаци су тешко подложни фалсификовању, што чини биометријску возачку дозволу сигурнијом од традиционалних дозвола. Висок ниво сигурности смањује могућност злоупотребе и фалсификовања идентитета.

3. Брза и ефикасна верификација идентитета: Употреба биометријских података омогућава брзу и ефикасну верификацију идентитета возача. Ово је посебно корисно у ситуацијама попут rent-a-car услуга, граничних прелаза или полицијских контрола.

4. Једноставно очитавање података: Биометријске возачке дозволе често садрже RFID[35] чипове који омогућавају брзо и једноставно очитавање података о возачу. Ово смањује време потребно за проверу идентитета и олакшава административне процедуре.

5. Додатне сигурносне функције: Биометријске возачке дозволе често имају и додатне сигурносне функције као што су холограми, QR кодови или други заштитни елементи. Ови елементи отежавају фалсификовање дозвола и повећавају њихову сигурност.

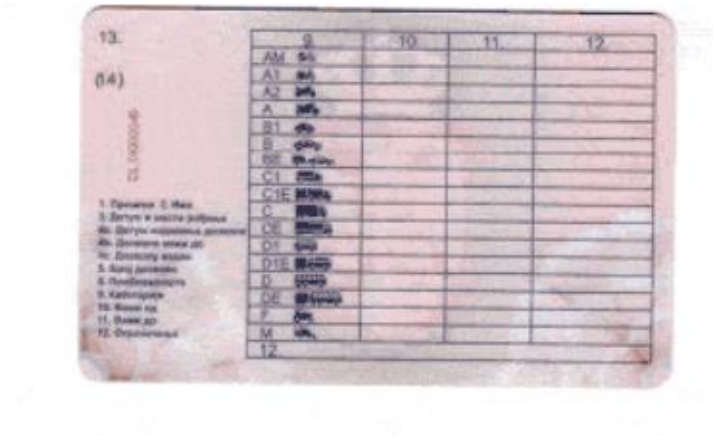
6. Међународна прихватљивост: Биометријске возачке дозволе обично су препознате и прихваћене на међународном нивоу. То олакшава путовање и вожњу у иностранству, јер возачи не морају носити више различитих идентификационих докумената.

Разлика између обичне и биометријске возачке дозволе лежи у начину идентификације возача и сигурносним функцијама које су имплементиране у сам документ. Обична возачка дозвола се обично идентификује на основу информација наведених на самом

[35] **RFID** је скраћеница од **Radio frequency identification** (у слободном преводу — *Идентификација путем радио фреквенције*). RFID је систем даљинског слања и пријема података помоћу RFID плочица/одашиљача. RFID плочица је изузетно мали објекат који се може залепити или уградити у жељени производ. RFID плочице садрже у себи антену која им омогућава пријем и слање радио-таласа од RFID примопредајника.

документу, као што су име, фотографија и број дозволе. Биометријска возачка дозвола користи биометријске податке, као што су отисци прстију, фотографија лица или скенирање шаренице ока, како би се верификовала аутентичност возача.

Слика 4. Предња страна возачке дозволе



Слика 5. Полеђина возачке дозволе

Биометријске возачке дозволе доносе неколико додатних бенефита и могућности:

1. Брже и ефикасније трансакције: Биометријске возачке дозволе могу се користити за брже и ефикасније трансакције, као што су плаћање путем мобилних уређаја или приступ одређеним услугама. Биометријски подаци возача могу се повезати са другим системима како би се омогућило једноставно и сигурно извршавање различитих трансакција.

2. Дигитална верзија: Биометријске возачке дозволе могу бити доступне у дигиталном формату, што омогућава возачима да их носе на својим паметним телефонима или другим

електронским уређајима. Ово олакшава ношење и приступ дозволи, а такође помаже у смањењу ризика од губитка или крађе физичког документа.

3. Повезивање са другим идентификационим системима: Биометријске возачке дозволе могу бити повезане са другим идентификационим системима, као што су база података о криминалним евиденцијама или системима за препознавање лица. Ово омогућава брзу и ефикасну проверу идентитета возача у различитим ситуацијама, као што су полицијске контроле или провере безбедности на аеродромима.

4. Универзална компатибилност: Биометријске возачке дозволе могу бити дизајниране да буду универзално компатибилне, што значи да могу бити прихваћене у различитим земљама и регионима. Ово олакшава путовање и вожњу у иностранству, јер возачи не морају носити више различитих идентификационих докумената.

5. Побољшана сигурност саобраћаја: Коришћење биометријских возачких дозвола може допринети побољшању сигурности саобраћаја. Биометријски подаци возача омогућавају прецизну идентификацију и проверу возача, смањујући могућност превара или вожње под туђим идентитетом.

Технологија биометријског идентификовања возача почела је да се користи почетком 2000-их година са својом првом употребом у Финској 1999. године. У неким земљама она може представљати идентификациони документ уместо пасоша. У Републици Србији је нова биометријска возачка дозвола као и саобраћајна почела да се издаје 3. јануара 2011. године.

У чип саобраћајне дозволе подаци се уносе на начин који омогућава читање података читачима идентификационих картица. Саобраћајна дозвола садржи следеће податке видљиве оком, и то[36] : на предњој страни, у левом, мањем делу, на врху, садржи међународну ознаку Републике Србије „СРБ“ исписану латиничним писмом беле боје на правоугаоном пољу плаве боје, испод које се налази чип, на чијој левој страни се налази словна и бројчана ознака и стрелица, која означава правац убацивања картице у читач картица. Испод чипа је графичкии симбол управљача возила, а испод њега речи: „Ова

[36] https://ltablice.com/novosti-za-vozace/saobracajna-dozvola-srbije

исправа мора се показати на захтев сваког овлашћеног лица“. У десном, већем делу картице (картица је подељена вертикалном линијом на леви и десни део), на врху је натпис: „РЕПУБЛИКА СРБИЈА“ исписан ћирилицом, испод кога је превод тог натписа на енглеском језику, испод кога су исписане речи: „САОБРАЋАЈНА ДОЗВОЛА“ на ћирилици и на енглеском језику. Десно од наведених речи је мали грб Републике Србије, а испод се исписује назив органа надлежног за регистрацију возила. Ниже доле налазе се следећи кодирани (убачени у чип дозволе) подаци:

А – регистарска ознака возила

Б – датум прве регистрације

И – датум издавања саобраћајне дозволе

Ц.1.1 – презиме власника (фирма односно назив за правна лица)

Ц.1.2 – име власника

Ц1.3 – пребивалиште (седиште) и адреса власника возила

Ц.3.1 – презиме корисника возила (фирма односно назив за правна лица)

Ц.3.2 – име корисника возила

Ц.3.3 – пребивалиште (седиште) и адреса корисника возила

Слика 6. Предњи изглед саобраћајне дозволе

Испод горе наведених података је број под којим је возило уписано у регистар и у доњем десном углу је серијски број саобраћајне дозволе.

У позадини се налази шара комплексне структуре са мотивом вотивних колица. На полеђини саобраћајне дозволе налазе се кодирани подаци и то редом на доле:

Д.1 – марка возила

Д.2 – тип возила

Д.3 – комерцијална ознака (модел)

Е – број шасије

Ф.1 – највећа дозвољена маса (овде убаци линк ка појмовима)

Г – маса

Х – важење регистрације (уписује се датум када се замењују регистарске таблице)

К – хомологацијска ознака

П.1 – радна запремина мотора

П.2 – снага мотора у kW

П.3 – врста горива или погона

Q – однос снага/маса у kW/кг (само за мотоцикле)

С.1 – број места за седење укључујући и место возача

С.2 – број места за стајање

У чип саобраћајне дозволе, поред видљивих података из саобраћајне дозволе, уписују се и следећи кодирани подаци (налазе се само у чипу):

J – врста возила

П5 – број мотора

Л – број осовина

Р – боја возила

забрана отуђења возила до (датум)

ЈМБГ, односно матични број власника возила

ЈМБГ, односно матични број корисника возила

носивост возила

На полеђини саобраћајне дозволе, у позадини се налази шара комплексне структуре и грб Републике Србије.

Алфанумерички подаци, који се односе на кодиране податке у видљивом делу саобраћајне дозволе и у невидљивом делу – чипу, уносе се латиничним писмом и арапским бројевима. Подаци о власнику и кориснику возила уписују се на начин како су уписани у исправи која је приложена као доказ о њиховом идентитету.

Слика 7. Полеђина саобраћајне дозволе

Identity Document Management System (IDMS) платформа представља обједињено решење које нуди целокупан процес обраде захтева за идентификационим документом, производњу документа и његово издавање. Платформу чини више модула који управљају процесом биометријске аквизиције, провером прикупљених података, биометријском дедупликацијом особа, логистиком бланко докумената, персонализацијом и контролом квалитета, затим физичким транспортом докумената на њихово одредиште и самим издавањем документа грађанину. Поред поменутих процеса који директно учествују у обради захтева за лични документ, платформа подржава и целокупан сет административних процеса, као што су креирање извештаја и управљање правима приступа оператера.[37]

[37] https://www.netsetglobal.rs/nacionalni-sistemi-za-izdavanje-i-upravljanje-identifikacionim-dokumentima/

IV Врсте биометријских личних података

4.1. Појам биоментријских личних података

У горенаведеном тексту упознали смо се са појмом биометријских личних података. Биометријски податак је податак о личности добијен посебном техничком обрадом у вези са физичким обележјима; податак о личности добијен посебном техничком обрадом у вези са физиолошким обележјима; податак о личности добијен посебном техничком обрадом у вези са понашањем физичког лица. То су подаци који си могу дефинисати као одређене карактеристике појединца помоћу којих се врши његова идентификација. Ови подаци су јединствени идентификатор једне особе. Биометријски подаци се обично користе у биометријским системима као што су отисци прстију, скенирање шаренице ока, препознавање лица, препознавање гласа, геометрија шаке или потписи.

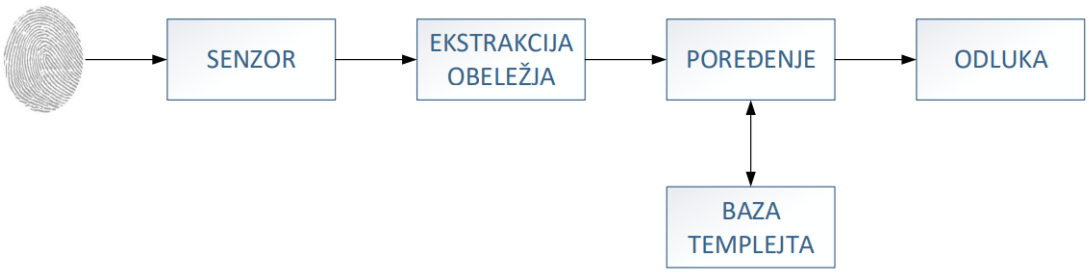
4.2. Отисак прста

Отисак прста јесте један од најчешће коришћених врста биометријских података али и најверодостојнији и најпоузданији јер се формира још у пренаталном периоду, у осмом месецу трудноће. Отисак прста чине папиларне бразде(шаре) на јагодицама прстију и оне су јединствене за сваког појединца. Они су детаљни, издржљиви током живота и готово је немогуће изменити их и фалсификовати. Још су старе цивилизације знале њихову улогу и значај па су веродостојност појединих правних односа потврђивали отисцима прстију утиснутим у глиненим плочицама. Овај биометријски податак се није одувек могао наћи као доказ пред судовима, године 1901. Scotland Jand [38] је формирао први Биро за отиске да би се исте године почели користити као доказ пред снглеским судовима. Са појавом савремених информационих технологија настају компјутеризоване базе података а од аналогних постају дигиталне те је поступак верификације отиском прста постао тачнији и веродостојнији. Постоје четири врста скенера: оптички, капацитивни, ултразвучни и термички скенер. Сви они се ослањају на снимање јединствених папиларних линија које чине отиске прстију и упоређују их са подацима који постоје у базама података с циљем проналаска оних са којима се подударају. Отисак прста је најприступачнији биометријски

[38] https://www.netsetglobal.rs/biometrijska-autentikacija/

лични податак и његово коришћење се креће од свакодневне употребе кроз аутентификацију на паметним телефонима, преко потврде идентитета у банкама до преласка граничног прелаза. Највеће базе података и најбољи алгоритми за претраживање формирани су управо овим податком, рангирају се према нивоу осетљивости (броју скенираних тачака) а у зависности од траженог нивоа заштите где су почетак свог коришћења нашле у полицијским установама а касније се њихова употреба шири. Отисак прста уз друге биометријске податке може да олакша контролу приступа одређеним информацијама, могућност верификације како би се извршила електронска плаћања и слично. За свако мерење и упоређивање код генеричког система биометрије постоје неколико компоненти без којих није могуће доћи до аутентификације и идентификације корисника:

- ✓ Сензор (sensor);
- ✓ Модул за екстракцију обележја (feature extractor);
- ✓ Модул за поређење (matcher);
- ✓ База података о идентитетима корисника и одговарајућим биометријским темплејтима[39](stored templates);



Слика 8. Генерички систем за биометријску контролу

[39] Биометријски шаблон, или биометријски темплејт, је дигитални запис који садржи карактеристичне особине биометријског податка појединца. Овај шаблон се користи за идентификацију или верификацију идентитета особе у биометријским системима.
Биометријски темплејт је резултат процесирања и анализе биометријских података како би се издвојиле кључне карактеристике и креирао јединствени дигитални запис. На пример, за отисак прста, биометријски темплејт ће садржати информације о распореду вртложних линија, тачака и других карактеристика отиска прста.
Биометријски темплејт се обично чува у сигурној бази података или на сигурном уређају, где се користи за упоређивање са новим биометријским узорцима приликом идентификације или верификације идентитета. Приликом упоређивања, систем тражи подударање између новог узорка и постојећег биометријског темплејта.

Корисник прво прилаже свој узорак, што је у овом случају отисак прста којег очитава сензор. Модул за екстракцију обележја издваја карактеристична обележја и генерише темплејт (шаблон) који се чува у бази података. Темплејт настаје као резултат сложених математичких операција и алгоритама које је модул за екстракцију извео над снимком узорка.

Циљ је да се на основу одговарајућег биометријског податка (узорка) постигне верификација и идентификација имаоца узорка. Верификација корисника биометријског систем функционише на следећи начин:

1. Корисник који жели да приступи одређеним ресурсима наводи свој идентитет;

2. Сензор прикупља биометријски узорак корисника;

3. Из узорка се издвајају атрибути и формира вектор обележја;

4. Рачуна сличност између генерисаног темплејта и темплејта смештеног у бази података који одговара наведеном идентитету;

5. На основу дозвољене границе грешке систем доноси одлуку, тј. одређује да ли је то заиста тај корисник и сходно одлуци дозвољава или блокира приступ ресурсима. У случају биометријске верификације генерисани темплејт се пореди са тачно једним темплејтом у бази!

Поступак идентификације корисника је сличан али нешто скупљи по питању процесорског времена. Приликом идентификације корисника, биометријски систем функционише на следећи начин:

1. Корисник који жели да приступи одређеним ресурсима прилаже своје биометријски узорак сензору;

2. Из узорка се издвајају атрибути и формира вектор обележја;

3. Рачуна сличност између генерисаног темплејта и СВИХ темплејта смештених у бази података. У случају биометријске идентификације генерисани темплејт се пореди са СВИМ темплејтима у бази!

Биометријски узорци, а самим тим и генерисани темплејт никада нису исти.

• Систем мора да квантификује и процени сличност између њих и да на основу одређених параметара донесе одлуку о прихватању или одбијању.

• Резултат поређења (matching score) $s \in [0,1]$.

• Дефинише се праг прихватања (threshold) t.

• Системске одлуке се доносе на основу прага прихватања.

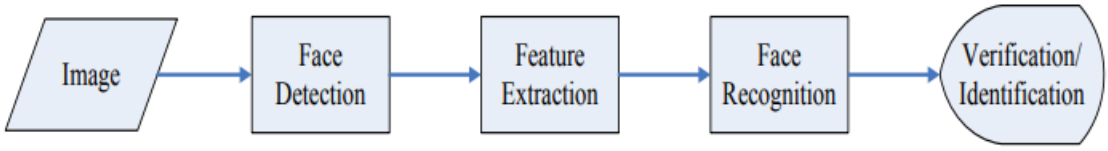
• Ако је $s > t$, резултат је прихватљив а препознавање успешно.

• Ако је $s < t$, резултат је неприхватљив а препознавање неуспешно.

4.3.Препознавање лица

Технике препознавања лица у последњих двадесет година добијају на значају и све више се истражују, на западу је јако привлачно владиним агенцијама као и великим банкарским компанијама за повећање метода идентификације па данас своју велику примену остварује у повећању сигурности, надзора, управљању запосленима...Ове методе се користе за верификацију (аутентификацију) и идентификацију појединца на основу карактеристика лица. Систем аутоматске верификације има два модула: Face detection и Face recognition. На одређеној слици се прво препознаје постојање лица, издвајање својстава, упоређивање особина са ониима у базама података што нас доводи до препознавња лица и верификације и идентификације корисника. Верификација представља

тзв. затворени систем где се остали биометријски подаци, у овом случају црте лица, упоређују са подацима у бази података.



Слика 9. Структура аутоматског face verification система

Рад на софтверима за препознавање лица започео је још 1960. године. Прва генерација софтвера је била полуаутоматска, што значи да се прво одређивао положај појединих карактеристичних црта лица на фотографији – као што су очи, нос, уста, уши – а потом су се вршила математичка мерења ради поређења. У њихов рад је морао бити укључен и сам корисник софтвера, који је ручно вршио математичка мерења, што је уједно био највећи недостатак прве генерације софтвера а 1987. године развили нови алгоритам за препознавање лица заснован на увођењу главних компоненти лица (**eigenface**).

Изазов са којим се суочава оваква метода идентификације је проблем осветљења који може да утиче на тачност резултата.[40] „Употреба DCT 1 (Discrete Cosine Transform) за неутралисање варијација у осветљењу први пут је представљена у W. Chen, M. Er, S. Wu; "Illumination compensation and normalization for robust face recognition using discrete cosine transform in logarithm domain", IEEE Trans. on Systems, Man and Cybernetics (2006) Аутори су користили DCT коефицијенте ниске фреквенције на слику у логаритмском домену као апроксимацију за регулисање осветљења (цомпенсатион терм), подешавајући их на нулу и реконструишући нормализовану слику на тај начин. Овај метод надмашио је многе постојеће методе који се баве варијацијама осветљења када су тестиране на Yale B бази података лица. Неке методе засноване на DCT-у су представљене на локални начин, полазиле су од идеје да се локални приступи боље носи са проблемима осветљења од глобалних. Подјелом слике лица на правоугаоне регионе и постављање истих на нулте ниско-фреквентне DCT коефицијенте сваког региона, постигнуте су боље перформансе. Uniform Local Binary Pattern (LBN) хистограм су прорачунавани за сваки регион и коришћени при класификацији. Примећено је да је иста регионска подела коришћена за

[40] Y. Leung, Knowledge Discovery in Spatial Data, Berlin Heidelberg, Springer Verlag, 2010., pp.143-221.

претпроцесирање помоћу DCT-а и за класификацијски корак користећи LBN, па је у овом случају фотометријска нормализација чврсто везана за структуру слике која је коришћена за издвајање карактеристика и класификацију."[41] IDIAP, Швајцарска компанија – креатор Torch3vision решења, је предложио три различита класификатора, уз два различита корака претпроцесирања, што је резултирало са укупно шест система за проверу аутентичности лица. Кораци претпроцесирања настоје побољшати слику или смањити утицај промене осветљења. Torch3vision[42] је машинска визиона библиотека заснована на C++ језику и Torch библиотеци која је формирана као софтверска платформа у области за препознавање лица и гестикулације. Google portrait је демонстрација система IDIAP технологије за детекцију лица.

Постоје три методе за препознавање лица:

1) Геометријски метод верификације лица се врши на основу кључних карактеристика лица**.** У кључне детаље лица спадају: Карактеристични детаљи лица, површине између карактеристичних детаља лица, удаљеност између карактеристичних детаља, растојање између очију, ширина носа, вилична линија...

Поступак препознавања спроводи се кроз 5 фаза и то:

- фазе детекције лица,

- фазе подешавања,

- фазе нормализације,

- фазе екстракције карактеристика и

- фазе компарације.

2) Фотометријски метод се врши на основу целокупног изгледа лица. Слика лица се пореди са својственим сликама (eigenface). Људско лице може да се подели на градивне јединице (128 градивних јединица). У систему постоји велики број лица које служе за

[41] M. Villegas, R. Paredes, Comparison of illumination normalization methods for face recognition, presented at the Third COST 275 Workshop on Biometric on the Internet 2005.
[42] Д. Томић, Биометријска метода скенирања лица, Универзитет у Београду, Факултет Организационих Наука, март 2012. године, стр.1169.

тренира. Из лица са фотографија се издвајају одређене градивне јединице које се складиште и помажу при каснијим поређењима. Дводимензионална слика сваке градивне јединице се назива својствено лице (eigenface) и свака од њих потенцира неку карактеристику.

Слика 10. Дводимензионална својствена лица

Слике се пореде тако што се нормализују, постављају се карактеристике на карактеристике (очи на очи, брада на браду...) јер морају бити исте величине, па се упоређујући формира скор подударности. Скор подударности је отисак лица (faceprint) у фотометријским системима што представља листу вредности, по једну за свако својствено лице.

3) Тродизимензионални метод - Ова техника користи 3-Д сензоре како би придобила информације о облику лица. Подаци који се добијају овим методом независни су од угла посматрања и осветљења. Поступак препознавање лица у 3Д системима састоји се из сљедећих корака:

1. детекција- лице се издваја из текстуре слике;

2. поравнавање-одређује се позиција и величина;

3. мерење-мере се линије лица и ствара се шаблон;

4. кодирање-шаблон ствара јединствени код што је 3Д код лица;

5. компатибилност- ова фаза постоји само ако се упоређује са 2Д подацима;

6. верификација или идентификација- поређење кода са кодовима из базе података.

4.4. Глас

Препознавање гласа јесте софтвер који је научен да декодира, разликује и аутентификује глас особе приликом идентификовања корисника. Овај програм процењује биометрију гласа скенирају говор и усклађује га са потребом гласовне команде. Постоје две скроз различите техонологије, прва испитује карактеристике гласа (Ко говори?) а друга препознаје говор (Шта се говори?). У првом случају се врши идентификација говорника на основу карактеристика његовог гласа док се у другом случају препознају изговорене речи ради задавања команди гласом. Овакав вид идентификације почео је брзо и нагло да се развија због лакоће његове примене те је наишао на потврду од стране друштва. Лични асистенти на паметним телефонима као што су Amazon Echo, Google Assistant, Apple Siri i Microsoft Cortana функционису без употребе руку и тастатуре приликом задавања команди, писања белешки, управљањем уређајима и сл. Генерисање гласа почиње у гласним жицама све до вокалног тракта који модификује садржај гласа. Аналогни звук (изговорени) претвара се у дигиталне сигнале (дигиталне податке који имају опис гласа) и који се назива „voice print" или профил гласа. Алгоритми који се користе имају за основу комбинације већег броја фактора, тј. једна иста реч се понавља више пута како би се избегло опонашање гласова. Дигитализацијом се свака реч дели на сегменте који садржи неколико формата и сви они заједно представљају профил гласа. Системи за препознавање гласа могу да функционишу по принципу независних речи, зависних речи или комбинацијом ова два принципа. Када је реч о систему независног текста препознају се карактеристике гласа а не онога што је речено. Нису унапред дефинисане речи за идентификацију већ зависи од дужине говора као и од јачине, тоналитета, стреса, нагласка говорника. Текст зависни системи могу да идентификују глас корисника само уколико се изговарају већ деифинисане реченице које се упоређују са онима који се налазе у бази података.

Препознавање гласа се углавном користи за биометријску аутентификацију корисника јер се лозинке, пинови, кодови могу изгубити или заборавити, међутим препознавање гласа је много веродостојније и сигуније у поређењу са тим а и знатно брже од куцања на тастатури. Његова примена је могућа у форензици, приликом обављања финансијских услуга, за перосанилизовани садржај корисника, за здравство... Једини проблем је што се глас може променити са годинама те га систем не може препознати па је пожељно имати неке друге алтернативе.

4.5. ДНК

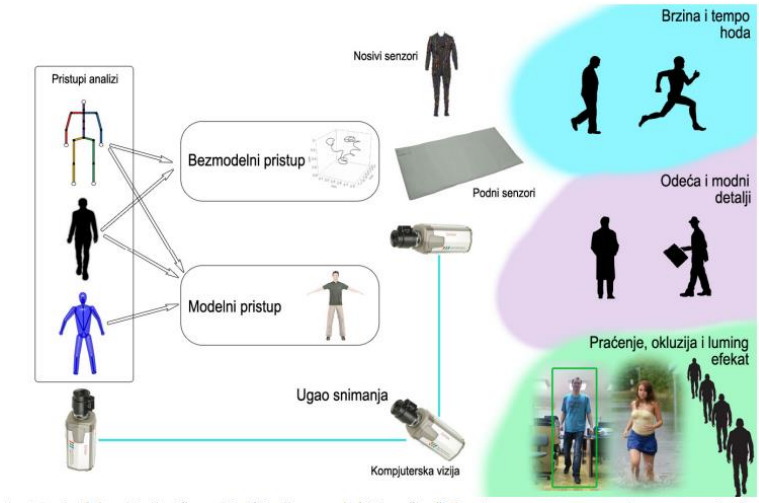
О методама попут вађења крви или ДНК постоје јако поверљиве информације тако да се о њима јако мало зна. Иако се ради о тајним подацима, они су свакако најпоузданији и најтачнији за биометријску идентификацију. Користе се у различитим подручјима где се анализа ДНК користи за утврђивање идентитета особе, утврђивање родитељства, одређење пола, утврђивање идентитета на посмртним остацима... Развојем молекуларне биологије дошло се до спознаје о индивидуалности и непоновљивости ДНК молекула. ДНК или дезоксирибонуклеинска киселина [43] се састоји од пара молекула у облику спирале које су повезане паровима. Сваки молекул садржи око три милиона парова база. Његова структура чини основу наслеђивања. Око 99,5% молекула ДНК је исто свим људима и то је некодирајући део, док је преосталих 0,5% јединствено за сваког човека и баш тај узорак се користи за биометријску идентификацију. Поред нуклеусне (ону на коју мислимо када каземо ДНК) ДНК постоји и митохонфријска ДНК, која се за разлику од претходне,која се налази у језгру, налази у цитоплазми и која се користи за биометријску идентификацију. Митохондријска ДНК се разликује од нуклеусне по томе што има око 10000 пута мање парова база али има више стотина копија језгра и она се наслеђује по мајци. Чак и у случају малог биолошког материјала овакву ДНК је лако узети у довољној количини потребној за анализу. Генерални недостаци ДНК анализе је што је то дуг и скуп процес који подразумева анализу од стране стручно оспособљене особе, пошто је рад са њима јако осетљив, какве су и оне те се лако могу оштетити или изгубити.

4.6. Шетање

Ход је једна од најизучаванијих биометријских података која се заснива на моторним способностима човека. Још пре него су кренули са истраживањима, некадашње цивилизације су знале да се на основу хода може идентификовати нека особа. Временом је постигнут споразум да људски ход карактерише довољан степен јединствености да се може користити за биометријско познавање. Велики број фактора је ту укључен: специфичан темпо хода, нагињање главе, померање торзоа, померање руку и ногу... У односу на друге биометријске податке приликом идентификације сензор се може

[43] https://sh.wikipedia.org/wiki/DNK

поставити на већој удаљености, потребно је да снимци буду високих резолуција јер се касније појединац може идентификовати помоћу одређених делова тела као што су очи, положај главе, шаке... Већа удаљеност камере за снимање омогућује праћење више људи истовремено што олакшава разликовање појединца од неког другог јер и свако од њих има специфичан ход и када не размишља о томе како се креће. Због тога се овај биометријски податак тешко прикрива него ли када је случај са гласом, лицем које може да се прекрије качкетом, капом или шминком јер је за промену хода потребно много више концентрације која, ако нестане на кратко, поново доприноси уобичајеном ходу. Постоје многи приступи у анализи препознавања хода и кретања који зависе од бројних карактеристика.



Слика 11. Разни фактори који утичу на разне приступе у анализи препознавања хода

4.7. Потпис

Од давнина је позната вредност потписа и рукописа. Како је рукопис попут отиска прста и биометријски потпис има могућност идентификације особе. Графологија[44] је вештина темељне анализе препознавања рукописа ради идентификовања особе. Код разних правних односа као што су плаћање картицом, потписивање уговора или давање изјава потребно је потписати се, а да би произвео правно дејство карактеристике потписа одређују идентитет особе која гарантује за ставке на документу који се потписује.

[44] https://sr.wikipedia.org/sr-ec/%D0%93%D1%80%D0%B0%D1%84%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%98%D0%B0

Верификацијом потписа се идентификује начин на који се одређена особа потписује тј. сама особа. Начин потписивања обележен је одређеним крактеристикама као што су брзина потписивања, отисак предмета којим се потписује, дебљина и облик слова што све заједно чини оригиналност потписа. Иако многи тврде да је, нарочито када је реч о биометријским потписима, могућност кривотворења јако велика ипак одређена обележја остају јединствена и непромењена. Сваки потпис има своја општа и посебна обележја. Општа обележја су изглед, распоред текста, величина рукописа, размаци, везаност и независност слова, растављање речи, брзина писања, нагиб, притисак на папир, украшавање. Посебна обележја су јединствена за сваку особу као што су брзина, дужина потеза руке, нагиб и управо се на овим карактеристикама темељи биометријска идентификација појединца. Приликом верификације потписа могу се користит две методе: статичка и динамичка. Статичком методом се испитују величина слова, дебљина, генерално његов облик и геометријске карактеристике док се динамичком методом утврђује брзина и путања приликом ове радње. Захваљујући савременим технологија данас, не само да је порасла потреба и већ је повећана сигурност биометријског потписа па се користи стилус[45] и таблет који су објединили статички и динамички метод верификације. На тај начин је кривотворење потписа постало готово немогуће јер је потребно прекопирати све наведене карактеристике.

Слика 12. Стилус и таблет.

[45] Стилус је врста модерне хемијске оловке која се користи да помогне у навигацији и писању приликом tachscreen опције. То је алат који помаже у раду са телефонима, таблетима и мониторима осетљивим на додир.

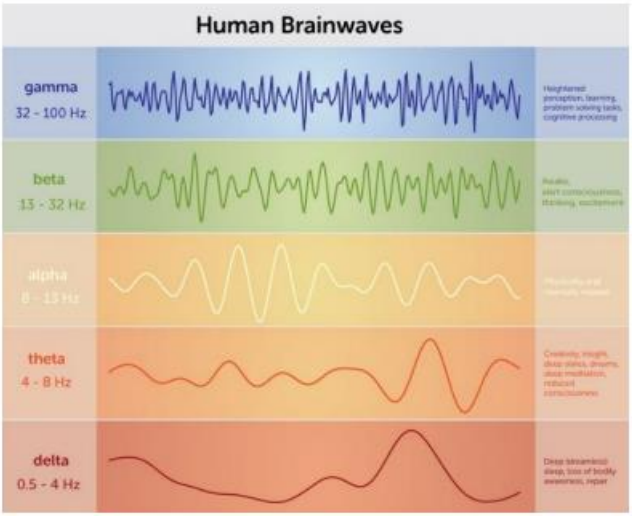
4.8. ЕЕГ

ЕЕГ (електроенцефалографија) је техника снимања електричне активности мозга. Користи се за мерење и бележење електричних сигнала који се генеришу у мозгу путем електрода постављених на скалпу. Електрична активност мозга је резултат комуникације између милијарди нервних ћелија, познатих као неурони. Ови неурони емитују електричне импулсе који се могу детектовати и снимити помоћу електрода постављених на површини скалпа. Када се безбедоносно осетљиви подаци налазе на различитим информационим системима потребно је да се они и заштите одређеном контролом приступа. На тај начин је немогуће приступити од неовлашћене особе у циљу злоупотребе података. Да би се дошло до идентификације корисника потребно је да биометријски сензори прикупе податке које ће упоређивати са постојећим у самом систему[46]. Аквизиција представља прикупљање података из спољашње средине у одређени електрични уређај, то јест сензор. Када се говори о биометријском податку, онда је потребан биометријски уређај за аквизицију такве врсте података[47]. ЕЕГ аутентификација користи електрофизиолошки систем за праћење активности мозга. Ова технологија је врло популарна и може се користити без икаквих споредних ефеката на мозак. До сада је извршено неколико истраживања о могућности примене ЕЕГ сигнала за аутентификацију корисника[48]. Постоји неколико комерцијалних уређаја са различитим бројем електрода које се користе за прикупљање ЕЕГ података. Неки од сензора користе суве електроде, а неки сензори користе мокре електроде. Мождани режњеви емитују ЕЕГ сигнале као одговор на различите стимулансе и ментална стања. Претпоставља се да постоји променљива разлика узорака ЕЕГ таласа док се визуелизује лозинку у мирним условима у односу на принуду, због различитих менталних стања, мозак производи различите обрасце аналогног ЕЕГ таласа.

[46] J. Isuru, M. Cohen, S. Amarakeerthi, BrainID: Development of an EEG-Based Biometric Authentication System, IEMCON: Proc. Information Technology Electronics and Mobile Communication Conf., 2016., pp. 1-6.
[47] A. K. Jain, A. A. Ross, K. Nandakumar, Introduction to Biometrics, Springer, USA, 2011., pp. 1-23.
[48] Y. S. Soni, S. B. Somani, V. V. Shete, Biometric user authentication using brain waves, International Conference on Inventive Computation Technologies (ICICT), India, 2016., pp 1-6, И Ala Abdulhakim Alariki, Abdul Wasi Ibrahimi, Mohammad Wardak, John Wall, A Review Study of Brian Activity-Based Biometric Authentication, Journal of Computer Science, 2018., pp.1-3.

Слика 13. Neuro Sky Mind Wave 2-EEG као биометријски уређај

Уређајем се сакупљају одређене врсте таласа у мозгу (алфа, бета, гама и тета мождани таласи) и тренутно стање усредређености (фокуса) и стање опуштености.



Слика 14. Значење можданих таласа[49]

Тип теста може бити:

1. Опуштено – субјекат се потпуно опусти и затвори очи;

2. Читање – субјекат добија текст који треба да чита у себи;

3. Лепе слике – субјекат посматра слике које у њему буде лепе емоције;

4. Математика – субјекат добија математички задатак који треба да реши;

[49] M. McDowell, Brainwaves: The Nature Of Brain Waves & Their Frequencies, Kindle edition, 2015., p.23.

5. Узнемиравајуће слике – субјекат посматра слике које треба да изазову ружне емоције (слике ратних злочина, искасапљених животиња и слично).

У овој фази истраживања предвиђено је да се ради до 5 мерења свих наведених тестова у различите дане. Основни циљ је да се испитају мождани таласи на одговарајући тип теста за сваког субјекта не би ли се извршила идентификација. Упоређују се подаци добијени тренутним снимањем и подацима који постоје у бази података, њиховим поклапањем поступак аутентификације је завршен.

4.9. Мирис

Мирис је јединствен за сваку особу и може се користити за идентификацију или верификацију идентитета. Ова техника се назива биометријско препознавање мириса или олфактометрија. Свака особа има свој јединствени мирисни профил који је резултат комбинације различитих хемијских једињења које се ослобађају путем знојења или излучивања из тела. Ови мириси могу бити специфични за сваку особу и остају релативно константни током времена. Биометријско препознавање мириса укључује снимање и анализу мирисних узорака ради идентификације или верификације идентитета. Ови узорци се могу прикупити са тела, као што су отисци прстију, или из ваздуха који окружује особу. Биометријско препознавање мириса може се постићи кроз различите методе мерења и анализе мирисних узорака. Ове технике омогућавају идентификацију и квантификацију специфичних мирисних једињења како би се створио јединствени мирисни профил особе. Ево неколико метода које се користе у овом процесу:

1. Гасна хроматографија (ГЦ): Ово је једна од најчешћих техника за анализу мирисних узорака. Узорак се инјектује у гасни хроматограф, где се компоненте раздвајају према њиховим физичким и хемијским карактеристикама. Након тога, детектор региструје и мери концентрације појединачних мирисних једињења. Ова техника омогућава добијање детаљног профила мирисних компоненти узорка.[50]
2. Масена спектрометрија (МС): Масена спектрометрија се често користи у комбинацији са гасном хроматографијом. Након раздвајања компоненти узорка гасном

[50] https://sh.wikipedia.org/wiki/Gasna_hromatografija

хроматографијом, мирисне компоненте се јонизују и идентификују на основу њихове масе и начина фрагментације. Ова техника омогућава прецизно одређивање структура мирисних једињења.[51]

3. Електронски нос (енг. Electronic nose): Електронски нос је уређај који опонаша способност детекције мириса људског носа. Састоји се од сензора који реагују на мирисне молекуле и претварају их у електричне сигнале. Ови сигнали се затим анализирају и користе за генерисање јединственог мирисног профила. Електронски нос може бити користан у брзом и аутоматском препознавању мириса, али има ограничену способност разликовања и идентификације специфичних мирисних компоненти.

4. Машинско учење: Машинско учење се често користи за анализу и обраду података добијених из мирисних узорака. Ове технике се користе за идентификацију и класификацију мирисних профила, као и за проналажење карактеристичних образаца и веза између мирисних компоненти и идентитета особе.

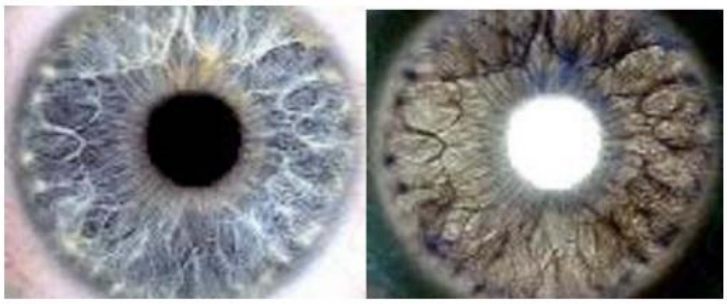
Након прикупљања узорака зноја или неких других излучевина које садрже мирисни молекул врши се анализа неком од наведених метода, а затим и упоређивање узорака са постојећом базом података што доводи до верификације и идентификације корисника.

Биометријско препознавање мириса има потенцијалну примену у областима као што су безбедност, форензика, медицина и маркетинг. Међутим, постоји неколико изазова у примени ове технике, укључујући стандардизацију поступака, осетљивост на спољне факторе (попут мириса околине) и заштиту приватности података.

4.10. Зеница (скенирање ока)

Приликом скенирања ока које се користи у поступку иденфиковања и верификације одређене особе користе се две методе: скенирање дужице ока (iris) и скенирање мрежњаче. Iris је мишић ока који контролише величину зенице јер на тај начин регулише колика количина светлости ће ући у око. То је обојено ткиво које окружује зеницу. Дужица ока поседује много каратеристика помоћу којих је могуће извршити идентификацију и верификацију неког лица, те ту спадају пегице, бразде и прстенови.

[51] https://sr.wikipedia.org/sr-ec/Masena_spektrometrija



Слика 15. Дужица ока и његов негатив

Овај биометријски податак одликује се високом прецизношћу јер је током живота непроменљив. Како је ово унутрашњи орган заштићен је од утицаја спољашње средине. [52] За снимање дужице ока може се користити обична камера. Потребно је да се очита испред скенера са раздаљине од неколико центиметара па чак и до пола метра, притом се може користити и скенирање преко наочара. Време верификације обично траје и мање од 5 секунди. Како би сам скенер избегао верификовање вештачког ока, систем врши осветљење да види да ли долази до скупљања зенице, проверава у циљу детекције дилатације зенице што је природна особина зенице која се не може фалсификовати те из тог разлога јесте реч о природном оку. Прилико скенирања прецизно се лоцирају унутрашња и спољашња граница дужице. Након одређивања граница спроводи се анализа карактеристика који се налазе на површини дужице. Др Даугманов алгоритам обезбеђује 3-4 бита података по квадратном милиметру.[53] На крају анализе, видљиве карактеристике дужице се конвертују у 256/512B IrisCode профил где се у добијени профил смешта у базу података и даље користи за верификацију док се, у случају идентификације профил пореди са расположивим профилима.

Скенирање мрежњаче је један од најпоузданијих метода идентификације лица. Као подаци који се користе приликом ове врсте идентификовања узимају се крвни судови који се налазе у дну ока. Све до данас није пронађен начин да се фалсификују такви подаци. Они су непроменљиви током целог живота и након смрти човека се брзо распадају те је немогуће да се злоупотре у том периоду. За разлику од скенирања дужице ока овде је немогуће скенирање преко наочара и траје око 10-15 секунди. Скенери ове врсте обично се

[52] R. Volner, P. Boreš, Multi-Biometrics Techniques, Standards Activities and Experimenting, Elecrtronics and Elektrical Engineering No 8., Czech Technical University in Prague, 2006., p.96.

[53] Др John Daugman, професор на Харварду, 1989. године почео је да развија алгоритам за препознавање дужице. Патенти су данас власништво Indian Technologies, Inc.

користе за аутентификацију и идентификацију. Скенирање мрежњаче практикује више организација као што су FBI, CIA и NASA. Међутим, последњих година скенирање мрежњаче постало је популарно у комерцијалне сврхе. Скенирање мрежњаче користи се и у затворима, приликом верификације код коришћења банкомата и ради превенције злоупотребе социјалне новчане помоћи. Скенирање мрежњаче има своју примену и у медицини. Преносива обољења као што су сида, сифилис, маларија и богиње, као и наследна обољења као што је леукемија, одражавају се на очи. Трудноћа такође утиче на очи. Сходно томе, показатељи хроничних здравствених стања, као што су срчане мане, артеросклероза и проблеми с холестеролом прво се примећују у очима.

Предности ове биометријске технике су:

-Мала вероватноћа лажних позитивних резултата;

-Екстемно мала вероватноћа (скоро 0%) лажних негативних резултата;

-Висок ниво поузданости, јер две особе немају исти облик мрежњаче;

-Брзи резултати: идентитет особе утврђује се веома брзо.

Мане ове биометријске технике су:

-Прецизност мерења може бити смањена услед болести као што су катаракта;

-Прецизност мерења такође може бити смањена услед тешког облика астигматизма;

-Метод није баш једноставан за коришћење;

-Особа која се скенира мора бити веома близу оптике камере те се не може користити без знања те особе;

-Висока цена опреме.

4.11. Остале врсте биометријских података

Поред горепоменутих биометријских података који се користе за идентификацију користе се и облик ушне шкољке, распоред крвних жила, динамика типкања, пулсирање крвотока, термограф лица и тела, биометрија длана (мери се биометрија сваког прста, дужина, ширина, дубина као и све те карактеристике сваког дела длана понаособ тако и длана као целине). Релативно нова врста података који се користе је препознавање распореда вена чиме се мери кретање крви у шакама и проверава да ли се врши идентификација живе или мртве особе. Ради повећања поузданости многи од ових података се комбинују те се користе мултимодалне технологије. У следећој табели можемо видети преглед биометријских личних података, њихову универзалност, трајност, јединственост, прикупљивост, перформансе, прихватљивост и могућност фалсификовања и подвале.

Sistem	Univerz a-lnost	Jedinstve-nost	Trajnost	Prikuplji-vost	Performa-nse	Prihvatlji-vost	Mogućnost podvale
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	V
Geometrija dlana	S	S	S	V	S	S	S
Dinamika kucanja	N	N	N	S	N	S	S
Raspored vena dlana	S	S	S	S	S	S	V
Dužica	V	V	V	S	V	N	V
Mrežnjača	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N
Miris	V	V	V	S	V	N	N
Oblik uha	S	S	V	S	S	V	S
Način hodanja	S	N	N	V	N	V	S
Termogram lica	V	V	N	V	S	V	V
DNK	V	V	V	S	V	N	N
V-visok; S-srednji; N-nizak							

Слика 16. Поређење биометријских личних података

V Методологија

5.1. Опис метода и техника прикупљања биометријских података

Септембра месеца 2003. године тадашњи министар полиције Републике Србије, Душан Михајловић, се преко средстава јавног информисања обратио јавности, наводећи да је са фирмом Motorola склопљен уговор вредан 20 милиона евра, „чија ће примена побољшати имовинску и личну сигурност грађана, остваривање њихових права и безбедност државне границе“. Притом је наведено да је у питању најсавременији биометријски систем идентификације и да су средства за тај пројекат обезбеђена из републичког буџета. Како се временом све више развијао тај систем, пролазио кроз негодовања и одобравања, унапређивао је разне методе и технике прикупљања података. За корисника чији подаци се још увек не налазе у базама података први сусрет управо обухвата прикупљање и упис у базу података чиме се, касније, олакшава иденификација и верификација корисника.

Слика 17. Прикупљање биометријских података

Прикупљање података има веома важну улогу у будућем успешном функционисању биометријског система. Зато је веома важно пажљиво одабрати сензоре за снимање, начин организације података, формат у којем ће се чувати исти као и услови у којима се чувају. Различите методе прикупљања остављају могућност различитих квалитета података, прудужење или смањење потребног времена те је важно да сви ти факори буду повољни за сваки узорак. Овај општи поступак обухвата неколико фаза. У првој фази се прикупља корисников биометријски узорак на уређају за очитавање. Узорак мора да буде одређеног квалитета јер је кључан за даљу аутентификацију. Уколико се, пак ипак не добије адекватан узорак, он улази у скуп неуспелих регистрација(енг. fail to enroll - FTE). У другој фази врши се анализа

прикупљених података, где се извлачењем одређених параметара добијају карактеристике одређеног појединца. Добијени подаци могу у себи да садрже велики број узорака у зависности од тога која биометријска метода се користи. Трећу фазу обележава складиштење у базу података. Постоје три класична приступа складиштења података:

- Локално складиштење на уређај је сигуран и брз начин аутентификације.
- Складиштење података на удаљеној локацији при чему подаци морају да се размењују преко сигурне везе. Овај начин је добар зато што омогућава аутентификацију са различитих локација.
- Складиштење података на преносивим медијима као што су паметне картице, решава проблеме у претходно наведеним примерима. Подаци се не чувају у централној бази и не путују мрежом, већ их корисник сам носи на жељене локације.

Које ће се методе користити приликом прикупљања биометријских личних података зависи од природе самог узорка који се узима. Сваки биометријски систем има четири модула [54] :

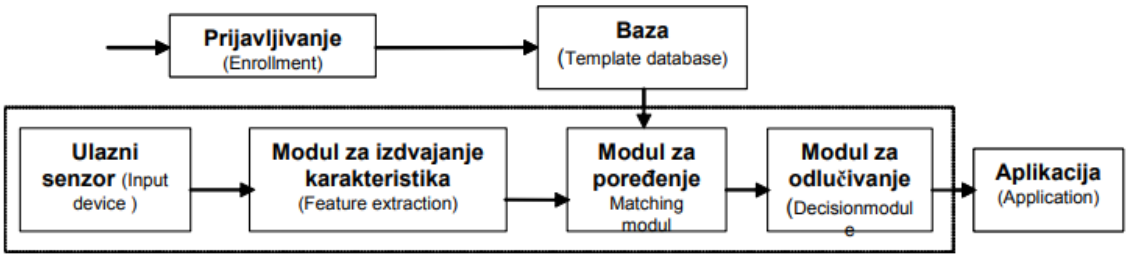
1. улазни уређај-сензор (sensor module) – који узима и дигитализује биометријску карактеристику (нпр. скенер за отиске прстију);

2. модул за издвајање карактеристика (feature extraction module) – који обрађује дигитализован податак ради издвајања карактеристика које га чине јединственим и које се могу сместити у шаблон (темплате) (нпр. издвајање минуција из слике отиска);

3. модул за поређење (matching module) – где се пореде издвојене карактеристике са подацима из шаблона сачуваног у бази;

4. модул за доношење одлуке (decision-making module) – где се идентитет прихвата или одбија (верификација), или утврђује на основу скора поређења (идентификација).

[54] A. Ross, A. K. Jain, Information fusion in biometrics, Pattern Recognition Letters, 2003., Vol. 24, pp. 2115-2125.



Слика 18. Блок дијаграм биометријског система

Мора се додати и пети модул тј. база (template database) где се чувају шаблони узети од особе у поступку пријављивања (регистрација-enrollment). Поступак пријављивања подразумева узимање биометријске карактеристике од особе, прављење шаблона и његово даље чување. База може бити централна; локална у односу на место где се користи (нпр. зграда где се ради); или може бити на уређају који корисник носи са собом (smartcad и сл.). Наравно може бити и комбинација било које две или чак све три. Такође се ти подаци могу чувати тако да се могу користити само за ту апликацију и организацију, или за више њих.

Biometrika	FAR	FRR	Komentar
Lice	1%	10%	Promenljivo osvetlje-nje, unutra/spolja
Otisak prsta	2%	2%	Rotacija i preterana distorzija kože
Geometrija šake	2%	0.1%	Sa prstenjem i nepri-kladnim postavljanjem
Iris	0.94%	0.99%	Unutrašnje okruženje
Retina	0.0001%	0.2%	Najbolji uslovi
Glas	2%	10%	Text independent, multilingual

Слика 19. Преглед технологија са стањем тачности

5.2. Преглед уређаја и система за прикупљање б.п. података

Уређаји којима се врши прикупљање биометријских личних података зависе од врсте узорка који се прикупља. Временом су се развијали новији и савременији читачи узорака којима се повећавао квалитет истих јер и смањила се могућност неуспелих регистрација а самим тим и подвала и превара коју многи желе да постигну како би злоупотребили те податке. Како смо у претходним двема главама навели врсте биометријских података и поступак њиховог прикупљања, сада ћемо направити преглед уређаја којима се узимају одговарајући узорци, претварају у одговарајуће карактеристике помоћу одређених алгоритама а онда и пореде са другим у одговарајућој бази података.

Данас постоји много биометријских техника за идентификацију и могу се поделити на две велике целине: биометријски ситеми према физичким карактеристикама и они који су засновани на препознавању понашања.

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

Слика 20. Табеле заступњених система идентификације

Отисак прста као један од најстаријих и најчешћих врста биометријског податка који се прикупља узима се на неколико начина. Без обзира који се начин користи за све је заједничко постојање скенера којим се преко сензора узима одговарајући узорак. Управо такви сензори могу да буду различити. Постоје:

- Капацитивни сензори који се састоје од низа кондензатора који мере проводљивост и генеришу слику отиска прста у зависности од различитих делова на прсту. Овде је потребан прави отисак прста који ствара 2Д слику отиска прста у црно белој боји. Проблем постоји када је прст мокар и сув јер ствара светлу или тамну слику која може пореметити праве карактеристике отиска прста. Притиском на сензор

додирују се ћелије чији се транзитори активирају тако да сваки сензор снима тачан део који је испод њега. Ту постоје разни произвођачи (Fidelica Microsystem, Fingerprints cards…) који се разликују према удаљености прста од сензора.

- Оптички сензори су најчешће коришћени сензори отиска прста. Они садрже оптичку призму са извором светлости (LED диода) који осветљава бразде на прсту и камеру (CCD сензор) која прихвата ту светлост и ствара слику отиска прста. Проблем који постоји код ове врсте технике јесте што се отисак прста може задржати као на било ком предмету и тиме пореметити скенирање идућег прста или пак крађу постојећег на сензору.
- Ултразвучни сензори користе звучне таласе али су они још увек у развоју.
- Термоелектрични сензори мере разлику у температури на бразди прста и долини када је прст прислоњен на сензор чиме се добија слику високе резолуције. Овакво скенирање се врло ретко користи.
- E-field сензори садрже електрично поље испод горњег слоја коже, тамо где отисак почиње. Ретко се користи јер се добија слаба резолуција слике.
- Сензори осетљиви на притисак користе пиезоелектричне кристале који под притиском генеришу струју.
- Сензори осетљиви на отпорност садрже одређене електроде које мере отпорност коју има површина коже[55].

Данас је уобичајено уграђивање читача са сензором на мобилним телефонима, банкоматима, вратима, уређајима за контролу приступа...

Скенирање лица је други најчешће коришћени начин идентификовања особе. На почетку се вршио уз помоћ специјализованих камера којима се очитава лице мада је сада могуће уз обичне камере (на мобилном телефону, лаптопу, другим уређајима којима је могуће преко камере приступити и контролисати...) под одређеним углом особе чије се лице скенира и са одређеним софтвером који је инсталиран унутар уређаја. Да би се добили квалитетни резултати постоје инфрацрвене камере, рефлектор инфрацрвене светлости, термалне камере на које мањи утицај има осветљење сензор удаљености тј. дубине и рефлектор точка. Проблеми који могу да се јаве у виду непрегледне слике

[55] M. Kakona, Drawbacks of Biometric Methods, Prague, 2001., pp. 4-6.

превазилазе се различитим неуронским мрежама. Прикупљање узорака се врши уз помоћ сензора којима може да се обезбеди дводимензионална слика, тродимензионалне моделе лица (на основу ласера или стереографије[56]).

Након горепоменутог Torch3vision филтера развиле су се неке новине по питању скенирања лица:

- artificialLight.cc – чита pgm (Portable Gray Map) слику и прави вештачко осветљење на њој;
- enhancepgm.cc – програм чита pgm слику изједначавањем хистрограма;
- diffusionVcycle.cc – чита pgm слику и нормализује услове осветљења помоћу Gross & Brajovic алгоритма.[57]

Скенирање гласа се најчешће користи када није потребно коришћење руку. Данас је то изражено код handsfree уређаја у аутомобилима али и код куће приликом управљања разним апаратима. Ту постоје два модела. ,,Скривени Марковљев модел се може најјасније приказати као генерализација проблема урни: Дух се налази у једној соби која није видљива за посматрача. У тој скривеној соби постоје урне X1, X2, X3,... Свака од тих урни у себи садржи познату комбинацију кугли, а свака кугла је обележена са y1, y2, y3,… Дух бира урну и насумично извлачи кугле из ње. Дух затим кугле ставља на покретну траку на којој посматрач може да види изабрану секвенцу кугли, али не и секвенцу урни из које су изабране. Дух има неку своју процедуру којом бира урне. Избор урне за n-ту куглу зависи само од насумичног броја и извора урне за (n-1)-ту куглу. Избор урне није директно зависан од урни изабраних пре једне предходно изабране урне, стога се ово назива Марковљевим процесом. Сам Марковљев процес се не може видети, једино је секвенца кугли видна зато се он и назива скривеним Марковљевим моделом. Кугле y1, y2, y3, y4 могу да буду извучене у сваком стању. Чак и ако посматрач зна садржај урни и треба да посматра само секвенцу од три кугле y1, y2 и y3 на покретној траци, посматрач још увек не може да буде сигуран из које урне је дух изабрао трећу куглу. Међутим посматрач може да одреди друге детаље, као што је идентитет урне из које је дух највероватније изабрао

[56] Стереографија је тело у равни.
[57] K. Messer, J. Kittler, S. Marcel, Y. Rodriguez, Performance Characterisation of Face Recognition Algorithms and Their Sensitivity to Severe Illumination Changes, Institute of Computing Technology, Chinese Academy of Sciences, China, 2006., Vol.1, pp.1-11.

трећу куглу.,,[58] Други метод најчешће коришћен за преопознавање на основу биометрије гласа је Гаусова Мешавина модела (енг. Gaussian Mixture Model). Овај метод је јако сличан скривеном Марковљевом моделу, али се он више користи код неограничених система који не зависе од текста (енг. text independent). Он функционише тако што користи глас од којег прави векторска стања која заступају разне звучне форме које су карактеристичне за понашање различитих појединаца. Оваквим начином рада, ове методе упоређују сличности и разлике улазног гласа са оним који се чувају у бази података и одлучују о томе да ли та особа јесте она за коју се представља. Након уписа у базу података, током фазе препознавања, квалитет, трајање и јачина звука се издвајају из узорка, па се потом шаљу на упоређивање са већ снимљеним подацима свих говорника. Када се заврши фаза препознавања, добија се однос вероватноћа о томе ко је од упоређених говорника највише вероватан на основу претходно изведених карактеристика.[59]

ДНК се узима преко крви уз специјализовану опрему и уз вешто обучене кадрове.

Скенирање хода. Временом је начин препознавања хода постао сложенији. Ту постоји неколико система. У прву групу спадају системи који користе видео камере за снимање човековог хода. Ово је најстарија и уједно највећа група. Друга група подразумева методу где се сензори притиска постављају у под по ком , лице чији се подаци узимају, хода. Ту се идентификација врши на основу брзине, темпа и снаге притиска. CBIR (Content Based Image Retrieval) је технологија која се користи за претраживање слика покрета из великих база података. Ту се у обзир узимају боје, текстура, облик и објекат на основу којих се врши иденнтификација. Трећа група обухвата различите сензоре где су најпознатији засновани на технологији акцелерометар[60]. [61]За препознавање хода користе се и моделни и безмоделни принцип. Код моделног приступа постоји структурни и модел покрета. Структурним моделом се описује физиономија људског тела (цилиндри, купе или затворене криве, штапне фигуре или посебни облици који описују ивице делова тела).

[58] R. J. Elliot, J. B. Morre, Laghdar Aggoun , Hidden Markov Models Estimation and control, Springer London, 2008., p. 269.
[59] D. A. Reynolds, T. F. Quatieri, R. B. Dunn, Speaker Verification Using Adapted Gaussian Mixture Models, Lexington, Massachusetts, 2000., pp. 19-41.
[60] **Акцелерометар** је направа за мерење убрзања (акцелерације) тела у покрету. Користи се за разне намене, индикацију оптерећења, мерење пређеног пута, навођење ваздухоплова и пројектила и друге.
[61]D. Gafurov, A Survey of Biometric Gait Recognition: Approaches, Security and Challenges. Norwegian Symposium on Informatics 2007 (NIK 2007) (pp. 119-132). Oslo, Norway: Curran Associates, Inc.

Потребно је да се дводимензионални снимак пребаци у тродимезионални како би слика била реалнија а самим тим могла да се изврши идентификација. Код безмоделног приступа није неопходно никакво претходно знање о људској фигури или ходу, користи се силуета особе добијена на основу сенке, те се проналазе неке структурне или динамичке карактеристике које служе за препознавање. Занимљивост у вези препознавања покрета која не служи конкретно за идентификацију је Microsoft Kinetis технологија којом се, држећи контролер у руци, управља аватаром у игрици.

Скенирање потписа се врши помоћу одређених лаптопова или таблета који имају сензитивну плочу за писање и одговарајуће оловке (стилуса) за писање по таквој површини.

ЕЕГ или препознавање на основу електроенцефалографије користи се за препознавање рада мозга. Подаци се прикупљају преко електрода на одговарајућим местима на којима се налазе сензори који бележе одређено кретање неурона и стварају слику можданих таласа.

Препознавање мириса данас није толико истражено. Свака јединка има свој посебан мирис те и сензори морају бити осетљиви за одређену групу ароматских смеса. Сензор је потребно нормализовати јер велики утицај могу имати хемијске супстанце као што је дезодоранс, парфем, креме...

Скенирање ока је једно од најпоузданијих биометријских система који се користе за идентификацију. Традиционалне методе користе сензоре на уређајима који се базирају на NIR (near infrared) технологији где је потребно да око буде у близини сензора. За снимање дужице ока довољна је и обична камера (нпр. препознавање на телефону) где даљина или коришћење наочара нема утицај. Када је реч о снимању мрежњаче, користе се посебне камере са сензорима којима је потребно прићи ближе, концентрисати поглед на једну тачку као и скинути наочаре.

Што се тиче осталих врста биометријских личних података, уређаји којима се прикупљају њихови узорци узимају се преко инфрацрвених камера када су у питању снимање крвних жила када је реч о скенирању вена. Користе се и оптички и капацитивни сензори за скенирање дланова, камере високе резолуције, 3D камере и сл.

5.3. Валидација и квалитет биометријских личних података

Перформансе биометријских система зависе од много услова. Оне се мере, квантификују и пореде једна са другом а све у циљу њихове веће успешности. Прецизност биометријских система се мери преко три основна параметра: 1) да се биометријски податак једног човека повеже са биометријским податком другог човека; 2) да се не препозна садашњи биометријски податак узет од човека са податком узетим од раније; 3) да систем не може прецизно да одреди резултат због слабог квалитета улазних података. Наиме, на читав поступак који се финализира идентификацијом корисника, утичу многе карактеристике које могу да поремете квалитет узорака а самим тим и смање проценат поклапања потребан за аутентификацију. На узорке могу да утичу услови окружења, промене биометријском параметру и други фактори па само биометријски системи функционишу на принципу оцене поклапања којима се изражава одређена сличност. Врло је важно, нарочито приликом узимања података по први пут, да све буде спроведено на најквалитетнијим сензорима, пажњиво и стрпљиво јер од првог узорка зависи које ће се карактеристике одвојити као јединствене како би у сваком другом случају могло да дође до поклапања. Такав начин фунцкионисања доводи до могућности постојања грешака које их прате. Те грешке се могу јавити у процесу уписа, процесу верификације али и неизоставно у процесу идентификације.

Приликом уписа података неке особе, може доћи до тешкоћа. Те тешкоће се јављају у виду FTA (Failure to Acquire – грешка код узимања података) и FTE (Failure to Enroll-грешка приликом уписа).

FTA представља проценат корисника за које систем не може да прикаже корисне биометријске узорке приликом њиховог уписа.

FTE представља проценат корисника за које систем не може да да направи квалитетан биометријски узорак (шаблон) због недостатка технологије.

За процес уписа је важно и TTE (Time to Enroll) што показује време које је потребно од узимања узорка до креирања самог шаблона што значајно утиче на квалитет биометријских узорака.

Код поступка верификације потребно је да се биометријски узорци поклапају са одговарајућим шаблонима који су пре тога направљени и који се складиште у бази података. Како постоје многе околности које утичу на тренутни узорак систем треба да квантификује и процени пре него добије оцену о прихватању тј. неприхватању. Резултат поређења означава се са s и он иде у интервалу [0,1] док се системске одлуке изражавају с вредношћу t, тако да су вредности изнад t прихватљивије. Током одлучивања система могу да се јаве две врсте грешака: FRR (False rejection rate- грешка одбијања) и FAR(False acceptance rate- грешка прихватања) и обе би требале бити што мање.

EER (Equal error rate) је тачка пресека претходне две грешке и она одређује вредност системске одлуке у тачки где су ове две грешке еквивалентне.

У делу о тачности биометријских система идентификације говорили смо о двема важним грешкама које се јављају FAR- лажно прихватање и FMR- лажно одбијање. И оне знатно утичу на квалитет података у поступку верификације.

И поступак идентификације прате одређени проблеми. Ту се јављају:

FPIR (False positive identification error rate- стопа лажне позитивне идентификације) када се прослеђује одлука о идентитету а корисник чак није ни уписан у систем. Формира се од стопе лажног поклапања и неуспелог сакупљања.

FNIR (False negative identification error rate- стопа лажне негативне идентификације) када систем не прослеђује тачну одлуку о идентитету а корисник је уписан у систем.

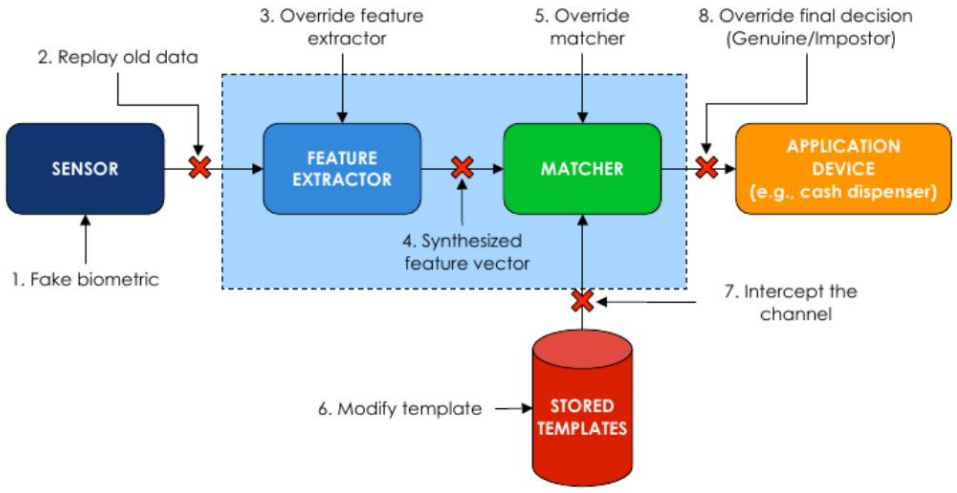
CIR (Correct identification rate- стопа тачне идентификације) показује када систем прослеђује тачне податке о идентитету кориснику који је уписан у систем.

Разни графички прикази помоћу крива олакшавају тачност резултата јер се њиховим пресеком лакше може уочити та одлука.

VI Сигурност и заштита биометријских личних података

6.1. Напади и претње биометријским системима

Данас се сусрећемо са различитим изазовима којима се угрожава или повређује сигурност биометријских система. Како су различите врсте сензора задужене за прикупљање података, они су први изложени претњама и први на удару различитих напада. Међутим, напади не морају бити нужно само на сензору, они се јављају и на комуникационим каналима, модулима и базама података. Напади се могу груписати у три велике групе: напади на улазном ниову, на нивоу обраде и преноса података и напади на нивоу чувања података.



Слика 21. Напади на биометријске системе[62]

На наредној слици се може видети преглед напада.

[62] B. Biggio, Adversarial Pattern Classification, Doctoral Dissertation, Electrical and Electronic Engineering University of Cagliari, 2010., p.15.

Tačka	Pretnje	Kontra-mere
1 Prikupljanje podataka	Obmana	Provera živosti
	Upotreba uređaja bez poverenja	Obostrana autentifikacija uređaja i servera
	Preopterećenje	Upotreba snažnih uređaja
2 Prenos originalnih podataka	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
3 Obrada signala	Umetanje lažnih podataka	Upotreba snažnih algoritama
4 Prenos obrađenih podataka	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
5 Poređenje	Umetanje lažnih podataka	Upotreba snažnih algoritama
6 Uzimanje šablona	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
	Povratni napad	Digitalno potpisivanje podataka, upotreba TTL taga.
	Čovek u sredini	Povezati biometriju i PKI
	Napad čistom silom	Upotreba Time out/lock out polisa
7 Čuvanje	Kompromitacija baze podataka	Snažnija zaštita šifrovanjem servera za smeštanje šablona. Smeštanje šablona na pametne kartice ili slične uređaje..
8 Prikaz rezultata poređenja	„Hill climbing“ napad	Inkrementalna povratna sprega
9 Odlučivanje	„Hill climbing“ napad	Inkrementalna povratna sprega
10 Komuniciranje sa aplikacijom	Prisluškivanje	Šifrovani prenos podataka, obostrana autentifikacija, upotreba simetričnog ključa
11 Aplikacija	Maliciozni kôd	Poštovati standarde (BioAPI, CBEFF)

Сваки систем, као и биометријски, има своје слабе тачке. Када је реч о њима, можемо прикази најчешће:

1) Прву претњу представља лажна биометрија која има неколико видова испољавања:

- Лажно представљање када неовлашћени корисник жели да се представи као легитимни које може бити случајно, уколико се не мења биометријски параметар али може бити и циљано уколико се намерно опонаша туђи биометријски узорак.
- Обфускација која мењањем параметара биометријског узорка онемогућује систему да донесе такву одлуку по питању идентификације корисника.
- Фалсификовање којим се прикупља неовлашћени узорак од другог корисника у нади да ће да се завара систем. (Replay напади)

2) Друга врста претње јесте Тројански коњ који има два вида испољавања:

- Систем може бити тако нападнут да произведе унапред одређени сет карактеристика и тако замени карактеристике улазног сигнала.
- Напад којим се производи лажан низак ниво поређења што утиче на систем за доношење одлука и постиже се она којој се стреми.

3) Трећа врста су напади на комуникационе канале чиме се добија увид у податке, врши њихово прикупљање и манипулише њима.

- Неовлашћено прикупљање које се постиже пресретањем комуникационих канала чиме се долази до информација о биометријским параметрима;
- ,,Човек у средини,, где се неовлашћени корисник неприметно убацује у комуникациони канал и преузима котролу над протоком података и самим подацима чиме се постиже утисак да постоји директна комуникација у којој и он учествује;
- Напад исцрпном претрагом (brute force) где неовлашћени корисник презентује велики број података с циљем да ће један од њих бити довољно сличан корисниковом и чиме ће се навести систем да донесе одређену одлуку;
- ,,Пењање уз брдо,, који је сличан као претходном нападу с тим да нападач има увид у оцену одлука система;
- Напад понављањем где се неовлашћено прикупљају подаци и поново шаљу у одговарајућем моменту, без мењања;
- Напад на оцене поклапања где се директно мењању подаци који утичу на доношење одлуке;

- Напад на финалну одлуку чиме се мењањем података који се односе на доношење одлуке прослеђују даље;

4) Четврта врста напада су напади на базе података где се добија увид у податке, мењају се шаблони те се на тај начин постиже лажно представљање или пак се ускраћују права која је корисник имао или нарушава функционисање система.

5) Пета врста претњи су напади на модуле система чиме се издвајају одређене карактеристике и поређења, директно се нападају хардвер и софтвер уз директне измене на њима чиме се постиже неправилно функционисање система или путем малициозних програма преузима конрола над системом.

6) Шеста врста претњи је приликом поступка регистрације где се мењају подаци и региструје лажни корисник.

Данас се у системима често користе knowledge&possesion metode као замена компромитоване биометрије. Ако се деси да неко украде картицу, лозинку, биометрија ће се поништити и добити друга али уколико је компромитована то је заувек. Напади не морају да буду нужни од стране појединца, то је могуће од корпорација како бивши радници не би имали права, од стране владиних агенција за ускраћивање права онима којима је то потребно (терористи...).

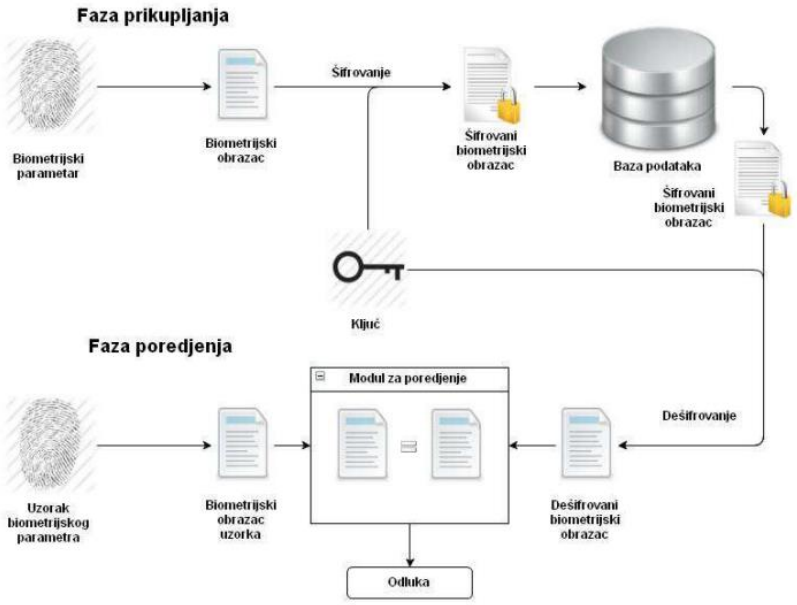
6.2. Криптографија у заштити биометријских података

Биометријска криптографија може да се дефинише, у основи, као процес који користи ПИН, лозинку или криптолошки кључ у комбинацији са биометријским подацима, на такав начин да оригинални биометријски подаци, нити кључ не могу бити откривени или регенерисани на основу референтног податка који је предвиђен за складиштење. Криптографијом се шифрују подаци и на тај начин се штите одређене информације. Два биометријска обрасца не морају да буду идентична. Важно је да оба обрасца потичу од истог биометријског извора да би било могуће регенерисати кључ. Коришћењем ове технике могуће је направити одређен компромис између биометријске варијабилности и

захтеване криптографске прецизности.[63] Биометријска криптографија омогућава вишеструку употребу биометријских образаца па уколико један од њих буде откривен, мање су могућности да се то учини другим налозима за приступ другим сервисима. Постоји могућност генерисања на основу оригиналне биометрије што је обележје модерних биометријских система. Криптографијом се обезбеђује јача веза између аутентификатора (корисника) и корисничког налога, обежбеђена је заштита лозинки и кључева креирањем референтних података. Нападач нема могућност да добије кључ на основу рефенетних података али ни информацију о биометрији корисника сервиса. Биометријска криптографија повећава безбедност личних података и саму комуникацију.

Када је реч о безбедности биометријских личних података, они се најбоље штите када се шифрују. Проблем који се јавља када су у питању биометријски параметри јесте немогућност одступања од устаљеног обрасца који се шифрује. Наиме, како знамо да биометријски систем приликом доношења одлуке функционише по принцпипу поређења и најсличнијих поклапања јер нису исте ни околности, а некад исти биометријски узорак може бити оштећен, уништен... док у случају шифровања он не може препознати и вршити поређење. Примена криптографских алгоритама врши шифровање над прикупљеним и обрађеним подацима а касније у фази дешифровања врши поређење над отвореним биометријских подацима. Ово је јако сложен систем па је поступак идентификације тежак за реализацију због великог броја криптографских операција и то све захтева боље перформансе система али и самог хардвера.

[63] https://sr.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%98%D1%81%D0%BA%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%98%D0%B0



Слика 22. Заштита биометријских образаца криптографским алгоритмом

Постоји нов концепт, хомоформно шифровање где се над шифрованим подацима спроводе математичке операције па се у случају дешифровања добија исти резултат математичких операција као и када су у питању нешифровани подаци. Подаци могу да се пореде у шифрованом облику. Јављају се неке врсте напретка у тој области. Компанија Fujitsu развила је систем аутентификације који користи хомоформно шифровање где се ствара одређени редослед и подаци се шифрују у блоковима.[64] Један од метода који се користи је да се лозинке не чувају уопште већ њихове хеш вредности али једносмерна криптографија ипак не може да обезбеди вредности које могу да се пореде и којима се врши аутентификација.

Један од видова шифровања јесте стеганографија што је техника скривања поруке коју сем пошиљаоца нико не зна, чак ни да је порука послата. У односу на криптографију постоји предност јер не привлачи неког да поремети комуникацију не би ли неовлашћено преузео податке, смањује се вероватноћа пресретања како нико не зна да порука постоји.

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

6.3. Заштита биометријских података

Основни циљ сваког система јесте његово несметано функционисање што се постиже када су сви захтеви испуњени. Један од главних јесте обезбеђивање безбедности. Безбедност може да угрози нормалан рад система поред грешки које се јављају а које смо у гореведеном тексту споменули, те је потребно више пажње томе посветити. На првом месту је потребно користити адекватни хардвер, способно техничко особље и омогућити, пре свега, добро физичко обезбеђење. Безбедоносни проблеми са којима се суочава систем могу бити: заобилажење чиме се користе пропусти на софтверу, харфдверу и у систему да би се дошло до неовлашћеног прикупљања података; порицање када корисник не испуњава захтеве система; неовлашћено прикупљање података и лажно презентовање за постизањење исто циља као и претходно; дослух којим лице које има одређена овлашћења у договору са трећим лицем дозволи злоупотребу података; принуда којом се наводи лице да омогући приступ неовлашћеном лицу...[65]

Заштита биометријских података у општем смислу може да се постигне коришћењем криптрографских алгоритама, енкрипцијом биометријски подаци треба да буду енкриптовани приликом преноса и чувања како би се обезбедила додатна сигурност и спречило неовлашћено читање или манипулација подацим. Енкрипција помаже у заштити биометријских информација од хакера и злонамерних напада. Организације које користе биометријске системе треба да успоставе јасне сигурносне политике и процедуре за заштиту личних података. Ово укључује правила о приступу подацима, управљању правима приступа, праћењу активности и обуци запослених о безбедном руковању биометријским информацијама. Двоструком аутентификацијом користи се комбинација биометријских података и додатних фактора као што су лозинке или ПИН кодови, може додатно ојачати сигурност система. Ова додатна сигурносна мера повећава тежину за неовлашћене особе да приступе подацима. Псеудонимизација биометријских података је процес који замењује идентификационе информације са псеудонимима или кодовима ради смањења ризика од идентификације појединаца. Ово је корисна техника за заштиту приватности и спречавање директног повезивања биометријских података са конкретним особама. Редовне провере безбедности биометријских система и података су кључне за

[65]S. Prabhakar, D. Maltoni, D. Maio, A. K. Jain, Handbook of fingerprint recognition, Springer London, 2003., pp.234-240.

откривање потенцијалних рањивости и брзу реакцију на могуће претње. Континуирано ажурирање система, тестирање сигурносних мера и реаговање на инциденте су важни кораци у заштити биометријских личних података. Поред ових постоје и други видови заштите система попут дигиталног потписа због повећања аутентичности; коришћење временских ознака; коришћење специфичних техника (challenge/response) где је потребно одговорити на одређене упите пре него ли се спречило слање биометријских података; могу се ограничити покушаји где се након неколико њих више не може приступити; заокруживање оцена поклапања да би се смањила могућност напада ,,пењање уз брдо,,; коришћење стеганографије и воденог жига[66] да се обезбеди јединственост и немењање података.[67]

Постоје и друге мере којима се обезбеђује сигурност:

1) Чување података у централној бази где се поређење података врши у централном серверу. Шаблон података се чува на централном серверу где је заштићен од спољњих утицаја. Администратор има пуну контролу над сервером и може да детектује нападе. За пренос шаблона од сензора где се узима па све до сервера користи се криптрографија јер се уз одговарајуће алгоритме подаци шифрују и избегава њихово мењање.

2) Чување на паметној картици је један од најбезбеднијих начина заштите података. Смарт картица је пластична картица у коју се интегришу подаци, складиште и процесуирају чиме се постиже лака преносивост. Сама повезаност са биометријским системом може постојати на неколико начина:

- Издвајањем биометријског обрасца на картицу који уз небиометријске податке на њој помажу у аутентификацији;
- Када се на картици налази биометријски образац и модул за поређење где се од картице серверу шаље коначна одлука;
- Када се уз претходни начин подаци на картици процесуирају, одлазе у сервер и враћају се на картици и пореде ради доношења коначне одлуке;

[66] Водени жиг се користи за означавање једног скупа података. Интегрисањем воденог жига спречава се могућност да се подаци , на којима се налази, промене.
[67] A. K. Jain, U. Uludag, Hiding biometric data, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003.,Vol, 25, pp.1494-1498.

- Издвајање комплетног биометријског система на картици а једино се одлука доноси тамо где је област примене што је најзахтевније решење.

3) Чување у локалној бази где се шаблон налази у хард диску на којем се врши и поређење. Како се локални рачунар не налази у зони сигурног окружења постоји велика шанса да шаблон или лозинка дођу у руке неовлашћеног лица. Проблем такође може бити то што се корисник може пријавити само на компјутеру где се налази шаблон.

4) Чување на паметној картици у локалној бази. Корисник може приступити само ако унесе одређени ПИН правилно и он и шаблон се пореде у локалној бази што може да буде на мети напада.

5) Чување у сензору омогућује поређење података у самом сензору што је с једне стране безбедно али сам корисник не може приступити шаблону.

6) Чување на паметној картици али где се поређење врши на сензору. Овде се поређење врши на сензору али се ПИН и лозинка враћају на картицу како би се омогућио приступ.

7) Чување на паметној картици где се и поређење врши на паметној картици. Ово је најсигурнији начин заштите биометријских података јер нема ПИНА, лозинки који могу да се украду.

Заштита биометријских личних података је од велике важности због осетљиве природе ових информација и потенцијалних ризика у вези са њиховим неовлашћеним приступом или злоупотребом.

Биометријски лични подаци имају неприкосновену вредност за сваког појединца па је потребно да се изаберу најприлагођенији начини за њихову заштиту. У широкој примени биометријских података у практичним ситуацијама, биометријски подаци долазе у руке лица који могу да их злоупотребе, униште или користе у комерцијалне сврхе. Из тих разлога се препоручује одабир једног од горенаведених начина заштите али и повећање свести сваког појединца да бар их бар физички заштити али и предузме све коракаке да приликом свакодневног коришћења они остану безбедни.

V II Примена биометријских личних података у информационим системима

7.1. E-commerce, e-governement и биометрија

У свету данас преовлађује online трговина која олакшава обављање разних трансакција, куповину производа и повећава животни стандард. Да би се платни промет одвијао несметано потребно је да постоје одређени механизми за препознавање којима се спречава могућност трошења истог дигиталног новца два пута. Како се подаци чувају на картици постоје организоване криминалне групе чији је рад усмерен на прављење дупликата картица, снимање корисника док користе банкомате како би се дошло до лозинки, прављење лажних докумената... Без гаранције самим корисницима да њихови биометријски подаци неће бити откривени нема ни куповине преко интернета што захтева комплексије уређаје и целокупан систем. Несметано одвијање трговине мора да поштује одређена правила:

- Да се обезбеди приватност корисника, сачувају њихови подаци од намерног или ненамерног откривања;

- Провера да ли одређене информације нису процуриле током комуникационог канала и на тај начин биле измењене;

- Да се изврши аутентификација клијената и самих сервера;

- Ауторизација којом се провера платежна способност корисника, као и то да ли је то лице овлашћено да добије таква права.

Различити системи којима се врши криптовање података, генератор случајних бројева, лозинки и сл доприносе сигурнијем систему. Временом рачунари постају бржи и јефтинији, расте продуктивност самог система јер се повећава и дужина кључа која је потребна за дешифровање података како би се обавила трговина а са најсавременијом опремом смањује се могућност откривања кључа у реалном времену и извршење обавеза из правног односа се постиже само уколико у томе учествује корисник, носилац података и познавалац кључа.

Online трговина и биометрија су области које су све више повезане како би се унапредила сигурност и практичност процеса куповине путем интернета. Биометрија се користи за идентификацију и аутентификацију корисника путем физичких карактеристика, попут отиска прста, препознавања лица или скенирања шаренице ока. Интеграција биометрије у онлине трговину омогућава корисницима да сигурно приступе својим налозима, обаве куповину и изврше плаћање без потребе за традиционалним корисничким именом и шифром. Коришћење биометрије у online трговини такође пружа додатни слој сигурности, јер је теже за преваранте да фалсификују или преузму биометријске податке корисника у поређењу са традиционалним методама аутентификације. Ово доприноси смањењу ризика од превара и неовлашћеног приступа налозима, пружајући корисницима веће поверење у online куповину. Биометрија може бити коришћена и за персонализацију корисничког искуства у онлине трговини. На пример, препознавање лица може омогућити персонализоване препоруке производа или прилагођене маркетиншке кампање засноване на претходним куповинама или интересовањима корисника. Ово може побољшати корисничко искуство, чинећи онлине куповину ефикаснијом и пријатнијом.

Ево неколико практичних примера како се биометрија може користити у онлине трговини:

1. Биометријско скенирање отиска прста за плаћање: Купци могу користити своје отиске прста уместо традиционалних метода плаћања попут картица или е-новчаника приликом обављања трансакција у онлине трговини. Ово убрзава процес плаћања и пружа додатни сигурносни слој.

2. Препознавање лица за пријављивање: Уместо уношења корисничког имена и шифре, корисници могу користити технологију препознавања лица за брзо и сигурно пријављивање на своје налоге приликом куповине online. Ово чини процес пријављивања једноставнијим и безбеднијим. Ово је доста заступљено приликом куповине апликација у виду дигиталног проузвода чија се могућност инсталирања одобрава управо препознавањем лица мада постоје и многи други случајеви у којима се њихова сврха остварује.

3.Биометријско скенирање шаренице ока за потврду идентитета: Када се обавља трансакција високе вредности, корисници могу користити биометријско скенирање

шаренице ока као додатну потврду идентитета. Ова технологија пружа врхунску сигурност и спречава неовлашћени приступ налозима.

4.Биометријско скенирање гласа за аутентификацију: Купци могу користити технологију биометријског скенирања гласа за потврду идентитета приликом обављања телефонских наруџбина или корисничке подршке у online трговини. Ово омогућава брзу и сигурну аутентификацију без потребе за традиционалним методама верификације.

5.Персонализоване препоруке производа на основу препознавања лица: Када се корисник пријави на свој налог путем технологије препознавања лица, онлине трговина може користити ове информације да би пружила персонализоване препоруке производа које су релевантне за њихове претходне куповине или интересовања. Ово побољшава корисничко искуство и повећава шансе за успешну продају.

E-government(електронска управа) је концепт који се односи на коришћење информационо-комуникационих технологија (ИКТ) за пружање услуга и информација грађанима, предузећима и другим ентитетима од стране владе. Интеграција биометрије у e-government може донети бројне бенефите у погледу сигурности, ефикасности и персонализације услуга. Ова технологија може помоћи владама да изграде ефикасније и транспарентније системе електронске управе који боље служе потребама грађана и предузећа.

Можемо навести неке примере примене у пракси:

1.Биометријска аутентификација за приступ порталима и апликацијама: Грађани могу користити биометријске податке, попут отиска прста или препознавања лица, за сигуран приступ владиним порталима и апликацијама. Ово осигурава да само овлашћене особе имају приступ осетљивим информацијама и услугама.

2.Биометријска идентификација за електронску легитимацију: Биометријски подаци могу се користити за електронску легитимацију грађана приликом обављања различитих административних процедура online. На пример, биометрија може бити коришћена за потврду идентитета приликом подношења захтева за документа или услуге.

3.Биометријска верификација за потписивање докумената: Биометрија може бити коришћена за верификацију идентитета приликом електронског потписивања докумената или образаца. Ово пружа додатни ниво сигурности и гарантује да су електронски потписи валидни и повезани са правим особама.

4. Биометријско скенирање за безбедније и ефикасније услуге: Интеграција биометрије омогућава владама да пруже персонализоване услуге грађанима на ефикаснији начин. На пример, препознавање лица може омогућити аутоматско попуњавање формулара или приступ персонализованим информацијама без потребе за додатним корацима аутентификације.

5. Биометријски системи за безбедност грађана: Биометријски системи могу се користити у безбедносне сврхе, као што су праћење присуства на јавним местима или идентификација криминалаца. Ово може побољшати сигурност грађана и помоћи владама у борби против криминала и тероризма.

Интеграција биометрије у e-government има потенцијал да трансформише начин на који се пружају услуге и комуницира са грађанима. Ево неколико додатних информација о томе како биометрија може унапредити e-governement:

1.Побољшана сигурност података: Биометријски системи пружају висок ниво сигурности јер се физичке карактеристике, попут отиска прста или препознавања лица, користе за аутентификацију идентитета. Ово помаже у заштити осетљивих информација и спречавању неовлашћеног приступа подацима грађана.

2. Смањење административних трошкова: Коришћење биометрије за аутентификацију и идентификацију може смањити потребу за традиционалним методама, попут папирних докумената или физичких идентификационих картица. Ово може резултирати ефикаснијим процесима и смањењем административних трошкова за владу и грађане.

3.Персонализоване услуге за грађане: Биометрија омогућава владама да пруже персонализоване услуге грађанима на основу њихових биометријских података. На пример, препознавање лица може омогућити персонализоване информације или препоруке услуга које су релевантне за сваког појединачног грађанина.

4. Ефикасније решавање административних процедура: Интеграција биометрије у e-government може убрзати процесе попут подношења захтева, регистрације или потписивања докумената. Коришћење биометрије за идентификацију и аутентификацију може елиминисати потребу за ручним проверама идентитета и омогућити брже и ефикасније решавање административних процедура.

5.Повећање поверења грађана: Имплементација биометрије у e-government може повећати поверење грађана у владине институције, јер пружа додатни ниво сигурности и гарантује да су њихови подаци заштићени. Ово може допринети бољој сарадњи између грађана и владе и побољшати транспарентност и одговорност у пружању услуга.

Укупно, интеграција биометрије у е-говернмент доноси бројне предности, укључујући већу сигурност, ефикасност, персонализацију услуга и поверење грађана. Ова технологија има потенцијал да трансформише начин на који владе комуницирају са грађанима и пружају услуге, стварајући ефикасније и транспарентније административне процесе.

Модернизација државне управе у виду e-governement промовише концепт електронске управе који штити приватност корисника и безбедно је када се користе небиометријски обрасци. То је већ уведено у неким општинама у Србији. У свету велики број e-governement апликација функционише коришћењем небиометријских метода ради бружања одређених интерактивних услуга. Овај вид се може успоставити помоћу смарт картица које нису биометријски идентификоване и јесу најпоузданији носиоци дигиталног сертификата (електронског уверења о веродостојности скупа података) и приватног кључа који је потребан за дешифровање података како би касније могли да се поред и донесе коначна одлука. Потребно је да постоји аутентификације корисника али да се очува анонимност као на пример у случају електронског гласања. Док код електронске трговине није потребно биометријско идентификовање, само обична аутентификација код електронке управе је то другачије. Уколико се на пример купује алкохол, потребно је да особа има више од 18 година па је потпуно небитно њено име и презиме или датум рођења. Много се потенцира постојање електронског потписа али је много практичније постојање смарт картице без биометрије и још боље за откључавање података са картице потребно непостојање биометрије већ коришћење пина.

7.2 Биометрија у online банкарству

Методе за биометријско препознавање имају све већи успех, брзо се шире и уводе у систем плаћања као и сам сектор банкарског финансијског пословања. Иако су данас пуно распрострањене, претпоставка је да ће већ за коју годину бити водеће у чијем учествовању ће биометријски подаци имати велику улогу. У новије време велику улогу у заштити текућих рачуна и трансакција користе се технологије за препознавање лица. У циљу заштите клијената банке, како картица може бити изгубљена, пин заборављен, на неким банкоматима се инсталира одређени софтвер за препознавање лица. Уколико сам систем препозна клијента банке одобрава одређену услугу без проблема.[68] Једна од компанија која је започела поступак инсталирања софтвера за препознавање лица али за трансакције које се извршавају преко телефона је MasterCard. Велика количина новца је последњих година уложена управо у те свхре, као додатни вид заштите а не самостални, како би се што брже и лакше разоткриле могуће злоупотребе. Ова компанија је предвидела могућност плаћања преко мобилних телефона и поред препознавања лица ангажовала и системе за препознавање отиска прста. Најпре је потребно да се преузимање апликације са одређене продавнице на интернету а потом и попунити податке о картици, што је и уобичајено када је у питању овакво плаћање. Ова врста плаћања путем selfi-a (selfie pay) захтева да се пре употребе верификују подаци (лице) када се упали камера, да корисник трепне не би ли се избегао случај верификовања фотографије. Након тога је могуће вршити плаћања. Постоји и посебан вид плаћања који се зове „Pay by touch" која се заснива на систему препознавања отиска прста. Ова новина која је почела да се користе јесте плаћање е-чековима. Како чекови представљају осовни начин безготовинског плаћања у свету и код нас, велика промена је уследила због спознаје да се папирни чек може заменити електронским а потпис извршити скенирањем отиска прста. Најпре се врши регистровање корисника који има активан чековни рачун у банци. Добија се електронски чек који ималац чека треба да попуни а остали подаци се попуњавају аутоматски а подаци се чувају на серверу провајдера. Провајдери само формирају документа којима се врши плаћање и поравнање али не примају средства од самих власника чекова већ шаљу криптованим комуниокационим каналима банкама. Овакво

[68] С. Р. Пауновић, Примена мултимодалне биометрије у системима за утврђивање идентитета, Докторски рад, Београд, Факултет организационих наука, 2014. године, стр. 177-181.

плаћање се може извршити само код трговаца који су регистровани за такав вид плаћања. Уз отисак прста се прилаже и празан чек како би се трговац уверио да корисник има рачун у банци. Уз одговарајући број (који је јаван а не тајан) омогућује се брже претраживање базе података отисака прстију. Када се нађе одговарајуће поклапање врши се плаћање скидањем одређених средства са рачуна. Поред броја који се може користити постоји и шифра али само како би се активирао новчаник (wallet) који врши криптовање података и слање на сервер за проверу. Уколико је све у реду трансакција се извршава и добија се број под којим је она заведена (нарочито када је реч о blockchain технологији). Трговац мора да има уређај за скенирање отиска прста повезан са касом, као и скенер за и-чекове за нове кориснике. Овакав вид плаћања је бржи и јефтинији од стандардних платних картица али је проблем уколико корисник на било који начин оштети површински слој прста на ком се врши скенирање.

Слика 23. Pay by touch систем плаћања

Плаћање је могуће извршити и помоћу технологије препознавања зенице. Овде постоје два система: у једном се чувају подаци о скенираној зеници а у другом стања на рачунима корисника који су регистровани и чији се подаци о зеници налазе у бази података. Поступак је сличан као и претходни поступци. Регистрација, постојање банковног рачуна, камера која скенира зеницу и шаље информације серверу након чије потврде се врши

пренос средстава са рачуна корисника на рачун продавца услуге или робе где се добијају повратне информације о извршеној трансакцији и њеном успешном окончању.

Потпис се већ одавно користи за идентификацију корисника приликом плаћања путем картица где се на одређеним уређајима потписивање одобрава и потврђује одређена трансакција.

Један систем плаћања још увек се испитује. То је Limiguard систем где се врши спектроскопска анализа коже на прсту, шаци или ручном зглобу. Одређени сноп светлости обасјава површину коже и тај зрак специфичних особина се анализира. Ово се користи, пре свега, за иденфтикацију корисника а остали поступак плаћања би био стандардан. Мада овакав вид плаћања није заживео не значи да у неком будућем периоду неће с обзиром да се пуно ради на његовом усавршавању.

7.3. Биометрија у правосуђу и криминалистичким истрагама

Биометрија као нова и савремена техонологија налази своју примену у правосуђу и разним криминалистичким истрагама за идентификовање осумњичених, сведока и других лица који учествују у овим поступцима. Иако се ради о јако осетљивим подацима који могу бити злоупотребљени, ипак се на овоме доста ставља акценат с обзиром да се на овај начин брже решавају случајеви, повећава се тачност идентификације, повећава сигурност али и смањује могућности за преваре.

Предност технологије за препознавање лица у оваквим случајевима корисна је из много разлога. Софтвери којима се врши скенирање и препознавање садрже базе података са лицима осумњичених или осуђених те их лакше лоцирају на местима где се они налазе. На овај начин се људи одговарају од неприхваћеног понашања, делује превентивно на оне који су планирали да изврше неко кривично дело али и репресивно на оне које су то учинили. Превентивни утицај се види у немогућности сакривања идентитета приликом извршења неког кривичног дела где ће на тај начин сигурно проћи кажњено него ли избећи такве последице. Када је у питању репресивни утицај, он се огледа у томе да се брже и лакше проналазе починиоци и пре него што успеју да сакрију своје радње. У оваквим случајевима особе нису ни свесне да се над њиховим лицем врши скенирање јер

није потребно идентификовање ока, прстију или слично. До биометријских података се највише долази у контролисаним условима под вештачким осветљењем чиме се над малом групом људи постиже жељени резултат. Корисно је код лица чији се подаци налазе у бази података због неког претходног извршеног кривичног дела. Захваљујући биометријским подацима води се евиденција несталих особа али и жртава криминалних радњи и повезивања са њиховим породица или идентификовања у општем смислу. Висок ниво прецизности у раду може да се постигне комбиновањем овог биометријског података са другим биометријским методама као што су отисци прстију, скенирање мрежњаче, препознавање гласа...[69]

Стално праћење затвореника у установама омогућава систему да брзо реагује уколико неко од њих планира свој бег. То се постиже технологијом препознавања гласа у исто време сваког дана. Наиме, затвореник је дужан да у тачно одређено време приступи уређају којим се скенира његов глас и након повратних инрофмација система може наставити даље активности.[70]

Многим преварама покушава да се обмане систем као и сам поступак пред судом. Из тих разлога се користе биометријски подаци како би особе које учествују у поступку могле да се идентификују. Један од метода којим се врши препознавање жртве јесте употреба ДНК особе али неизоставно и ДНК лица са којим је било у контакту, које је руковало оружјем или да на други начин учествовало у убиству, крађи, принуди... Захваљујући томе превазилази се могућност преваре система и подметања туђих отисака прстију, лица које имају физичке карактеристике као и онај који се треба наћи пред судом, туђих дигиталних потписа или злоупотреба туђих биометријских података да би се избегао негативан исход. Отисцима прстију и идентификовање препознавањем лица омогућује се верификација лица које није сведок и избегава могућност лажног сведочења. Изузетан значај биометријски подаци налазе у форензичким анализама (анализа отисака прстију, ДНК узорка...) који представљају доказе на суду без којих није ни могуће решити случај. На овај начин се врши и контрола приступа лицима којима је улаз забрањен као што је улаз у суднице када је поступку искључена јавност и сл. Биометријом у овим областима пружају

[69] S. Z. Li, A. K. Jain, Handbook of face recognition (2nd Edition), New York, Springer, 2011., Vol. 6, pp.377-453.

се моћни алати за прецизне и ефикасне процесе који помажу у борби против криминала или обезбеђивању сигурности грађана.

VIII Будућност биометријске идентификације и изазови

8.1. Предности и недостаци биометрије у поређењу са традиционалним методама идентификације

У односу на традиционалне методе идентификације биометријским методама се брже и лакше постиже исти циљ. Они су замена на компликоване системе јер се њима подиже безбедност, прецизност и поједностављује поступак утврђивања идентитета и верификовања. Како се овакав поступак све више прихвата од стране корисника ради се на његовом усавршавању и још већој ефикасности. Постоје многе предности узимајући сваки биометријски метод понаособ али је за све њих нешто карактеристично а то су неке најзначајније карактеристике на основу којих су биометријски подаци у далекој предности. Најважнија од њих је свакако **јединственост** која је припада сваком човеку што систем чини знатно поузданијим јер су се, код традиционалних метода, подаци могли лажирати. Повећана је сигурност идентификације захваљујући **немогућности фалсификовања** као што је постојала код лозинки и картица. Најчешће је потребно идентификовати велики број људи на одређеним местима, омогућити или онемогућити приступ одређеним местима или просторијама што се постиже великом **брзином и практичношћу** коју имају овакви видови идентификације. Захваљујући биометрији **елиминишу се могућности губитка картица и заборављања лозинки** чиме се постиже општеприхваћени поступак ком се увек прибегава. Мала је вероватноћа лажних позитивних резултата, екстремно мала вероватноћа лажних негативних резултата и велика поузданост успред гореспоменуте јединствености биометријских података сваког појединца. **Флексибилност** обезбеђује примену у различитим сегментима приликом контроле приступа, идентификацију на мрежи, управљање идентитетом, праћење присуства... На почетку су била потребна већа финансијска улагања али на дугорочном плану, биометрија може да **смањи трошкове** кроз разне олакшице попут непотребних издавања картица, докумената и саме процедуре око истих. Пошто су биометријски подаци трајни и не мењају се током времена и сама употреба биометрије је **дугорочна** јер се једном узети подаци чувају и користе за сваку идућу идентификацију и верификацију корисника. Међутим, биометрија се суочава и са одређеним изазовима:

1) шум у улазним подацима може се јавити из неколико разлога. Може постојати као последица неодржавања самих сензора, прашина на њима или физичких оштећења али и због промене самих биометријских модалитета као што су прехлада која утиче на боју и висину гласа, повреда површинских делова коже код отисака прстију или фалсификовање отиска прста пошто се тек ради на усавршавању сензора да препознају прави од вештачког прста мерењем температуре, проводљивост прста...; обољења очију код препознавања ока, удаљеност од камере, лоше осветљење..;

2) варијације у класи се јављају услед временских промена самих биометријских модалитета или у разлици приликом коришћења сензора у различитим периодима од стране исте особе (немогућност плаћања због недостатака на површини коже прста, болест код гласа...);

3) јединственост биометријских карактеристика може представљати проблем када сензор не може систему да пошаље адекватну информацију о улазним подацима чиме се повећава могућност да се две особе идентификују као исте;

4) универзалност такође може представљати проблем уколико неке особе не задовољавају одређени ниво квалитета биометријског узорка или се они током времена промене (као што је то код старијих особа...);

5) проблеми који постоје услед лажних података да би се покушало са преварама и добили жељени резултати;

6) проблеми приватности што утиче на смањену слободу од наметања, могућности да контролишемо податке, слободу од назирања, крађа информација, коришћење информација у јавном и приватном сектору али не од стране особа чији су подаци, ненамерно одавање информација, неовлашћена употреба...;

Постоје многа решења за елиминацију оваквих врста проблема због чега се непрестано ради на усавршавању биометријских система. Могу се користити и системи који користе више сензора у оквиру једног типа сензора (идентификовање лица на паметним телефонима); системи који користе више алгоритама који се користе за екстракцију и поређење; системи који користе више инстанци једног биометријског података или више

узорака истог податка (отисци прстију обе руке, ириса и мрежњаче...); мултимодални биометријски системи чиме се узимају узорци већег броја биометријских података (лице и глас, отисак прста и потпис...); хибридни системи који комбинују неке од претходних модела како би се постигла већа флексибилност, ефикасност и смањила могућност превара и злоупотреба.

8.2. Напредак технологије биометрије

Да би један систем несметано функционисао, потребно је да све његове компоненте функционишу тако да једна другу допуњују и формирају јединствену целину која ради како је и планирано. Непрестана комуникација делова система омогућује бржу, лакшу, безбедну и ефикасну примену самог система. Интероперабилношћу[71] се постиже тај циљ, како на нивоу самих података тако и у самом процесу и поступцима који се користе у самом систему за добијање жељеног резултата. Временом су предлагана многа решења у погледу евалуације биометријских система. Постоје многи приступи који конкретизују програмске језике који су потребни за прикупљање података; фокус се ставља на виши ниво апстракције не би ли се постигла нека стандардизација података за разлику од традиционалног начина прикупљања података и складиштење који се концентрише на конкретне формате складиштења података. Иако су ово неки напредци, ипак још увек нису савршени, фокусирани су на само један део биометријског система или су слабо прихваћени одређени стандарди. Уочена су нова достигнућа у погледу коришћења машинског учења, софтверског инжењеринга, интеракције човек-рачунар и администрације рачунарских система. Што се тиче сваког биометријског податка понаособ уочене су новине, иновације и побољшања. Алгоритми за препознавање лица постају прецизнији и софистицираније. Укључују се у рад вештачка интелигенција и машинско учење ради повећања поузданости узимања, складиштења и препознавања биометријских узорака. Види се напредак у односу на претходне године, у погледу превазилажења проблема слабог осветљења или препознавања са слике на којој се налазе више особа. Када је реч о сензорима за препознавање отисака прстију, постају сложенији по питању детектовања и анализе дубљих слојева коже, чишћења плочица сензора како би одолевале

[71] Интероперабилност је способност система или компоненти да размењују информације као и да користе информације које су разменили.

временским условима, оштећењима или уништењу појединих делова, чиме се смањује могућност лажног идентификовања. Како се скенирање ока узима као једна од најпоузданијих биометријских метода идентификовања, временом се постигла већа брзина препознавања уз коришћење инфрацрвених светала и камера високих резолуција и на тај начин се постиже прецизност у очитавању јединствених карактеристика ока. Приликом препознавања гласа почеле су да се користе технике фреквенције, тоналитета и ритма за употребу у различитим окружењима. Мобилни телефони све више користе биометријске технологије за идентификовање корисника кроз отисак прста, препознавање лица или скенирања ока чиме се обезбеђује сигуран приступ телефону и подацима али се и интеграцијом биометрије у мобилне телефоне омогућује сигурна ауторизација приликом плаћања или обављања других трансакција. Ниво поузданости се повећава и кроз мултимодалне биометрије применом више података у односу на једну биометријску карактеристику. Посебну популарност представља „cloud окружење" које постоји као вирутелна библиотека података, слика или докумената којима се може приступити са различитих уређаја и локација. На овакав начин се потхрањују и обрађују биометријски подаци у сигурном окружењу и на тај начин се несметано имплементирају у различите апликације. Употребом биометријских података узорци се анонимизују и омогућује се сигурно чување. Технике као што су хомоморфна енкрипција[72] и multi-party[73] рачунање обухвата обраду самих података а да се не дира у приватност корисника.

[72] Хомоморфна енкрипција је техника енкрипције која омогућава обављање математичких операција над шифрованим подацима, без потребе за дешифровањем тих података. Другим речима, омогућава извршавање операција над шифрованим подацима, а резултат тих операција ће бити тачан када се подаци дешифрују. Ова техника је важна јер омогућава обраду осетљивих података (попут биометријских података) на сигуран начин, без откривања самих података. На пример, ако су биометријски подаци енкриптовани хомоморфно, систем може извршавати операције над тим подацима (нпр. поређење отиска прста) без потребе да се подаци дешифрују, чиме се штити приватност корисника.

[73] Мулти-парту рачунање (МПК) је област криптографије која се бави израчунавањем функција над приватним подацима који су подељени међу више учесника, при чему ниједан учесник не открива своје приватне податке другима. Ова техника омогућава извођење заједничких операција и анализа над подељеним подацима без откривања самих података.

У мулти-парту рачунању, сваки учесник има своје приватне податке које жели да задржи тајнима, али жели да допринесе заједничком израчунавању одређене функције или анализе. Кроз сигурне протоколе и алгоритме, учесници могу сарађивати и израчунавати резултате без откривања својих приватних података. Ова техника је посебно корисна у ситуацијама где је потребно извршити анализе над осетљивим подацима, као што су медицински подаци, финансијски подаци, или биометријски подаци, а истовремено очувати приватност и поверљивост тих података. Мулти-парту рачунање се све више користи у областима као што су здравство, финансије, истраживање и развој, као и у cloud рачунарству, како би се омогућила сигурна и приватна анализа података између више страна.

IX Закључак

Примена биометријских података приликом идентификовања корисника али ,и онда када се не користи само за идентификацију, је данас у експанзији. У те сврхе се користе различити биометријски модалитети али и алгоритми за рад са истим. За заштиту података сваког корисника од изузетне важности је правилан одабир биометријских модалитета, процедура за процесирање биометријских података, формирање база података за чување и алгоритама који се користе за аутентификацију. Како се увелико користе у великој су предности у односу на традиционалне методе индентификације пошто се ради о својствима који се тешко могу опонашати или копирати. Пронашле су примену у различитим областима, свакодневно се користе пинови, лозинке те се потврђује идентитет лица и управо ту наступа биометрија која омогућује приступ захваљујући физичким карактеристикама. Да би се повећала сигурност потребно је да се повећа одговорност и транспарентност где се подвргњују надзору и контроли употребе технологије и креирања база података, повећања казни због могућих злоупотреба, брисање старих података како би се избегла могућност њихове злоупотребе и унапред одређена сврха употребе одређене технологије. Иако се осигурава сигурност, заштита и приватност као релативно нови начин идентификације и он има неке недостатке као што су скупа опрема, немогућност уноса података у базе због величине датотеке и постојање могућности лажне идентификације али и упркос изазовима са којима се сусреће, напредне технологије биометрије дају важан корак ка развоју савршенијих метода идентификације. Живот без савремених технологија се данас не може ни замислити, оне олакшавају поједине радње, повећавају животни стандард али и штеде време сваког појединца које ће у конкретном случају користити за неке административне послове, плаћања, приступу одређеним установама или компликованим поступцима за идентификацију па је потребно да све то право испрати и технологије придобије на својој страни и омогући најбоље, најбезбедније и сигурно решење за права сваког човека. Држава мора да обезбеди одговарајуће уређаје који се користе у те сврхе, да се обезбеди несметано функционисање али и пажња самих грађана приликом откривања података за разне намене. Повећати казне, превентивно деловати на руковаоце подацима, ефикасношћу уређаја за узимање биометријских узорака, сигурношћу сервера који доносе одлуку и адекватним праћењем рада биометријских система обезбеђује се правовремено регулисање области биометријских личних података и

саме идентификације за коју се такви подаци и користе јер у супротном може бити кобно за сваког појединца чији би се подаци нашли на „ пијаци” база података који лако могу допрети у руке оних који ће их злоупотребити.

X Сажетак и кључне речи

Биометријски подаци су резултат савремених информационих технологија. Развој интернета допринео је стварању различитих начина којима се угрожава безбедност личних података, нарочито биометријских узорака сваког појединца. Апликације које су широко распрострањене у својој енормној примени свакојаких телефона или других уређаја раде по принципу уношења података приликом њиховог коришћења. Овакав начин функционисања доноси многе ризике за очување података. Кључну улогу у целом раду имају биометријски лични подаци који се провлаче у свакој од тема. Најпре се упознајемо са личним подацима уопштено, на које све начине ми остављамо своје податке и колико је то сигурно, с обзиром да са дигиталним окружењем многе од њих дајемо несвесно или пак више од онога што је потребно. Други део рада обухвата сам појам биометријских система, биометријске идентификације као и тачност самих система све у циљу заштите приватности. Значај овог рада огледа се у конкретном појединачном објашњењу најпознатијих врста биометријских личних података, докумената у којима се налазе као и начину њиховог прикупљања, како на општем нивоу тако и на специјалном. Током обраде ове материје обухватили смо и области заштите кроз разне физичке компоненте али и неизоставно кроз шифровање које користи разне криптографске алгоритме у ту сврху. Како је примена биометријских система велика, многе се тек развијају а постојеће се усложњавају па се кроз рад могу видети и практични случајеви у појединим областима. Упркос многим изазовима и ризицима који прате биометрију, предности у односу на конвенционалне методе су огромни а сигурно ће и допринос остварењу многих права постати већи јер, иако је пракса међународних судова многобројнија, и домаћи судови прате тај развој да би створили добру домаћу судску праксу у овој области. На крају рада су изнета закључна разматрања са опажањем да је потребно подробније подизање свести ималаца личних података на њихову заштиту, али не само њих већ и руковаоце подацима и обрађиваче као и трећих лица која долазе у контакт са њима те да се активно ради на прилагођавању државе и права које треба да испрате све те кораке.

Кључне речи: лични подаци, приватност, биометрија, биометријска идентификација, врсте биометријских личних података.

Summary and key words

Biometric personal data

Biometric data is the result of modern information technologies. The development of the internet has contributed to the creation of various ways in which the security of personal data, especially biometric patterns of each individual, is compromised. Widely used application on various devices require data input upon usage, a process fraughtwith risks for data integrity. Central role to this work is biometric personal data, which intersect with each topic.We begin by examing personal data broadly- how it is collected, its security in digital environments and the often unconscious or excessive sharing by individuals. The second part of the work covers the concept of biometric systems, biometric identification, and the accuracy of the systems themselves, all aimed at protecting privacy. The significance of this work is reflected in a specific individual explanation of the most well-known types of biometric personal data, the documents in which they are found, and the methods of their collection, both at a general level and a specialized level. During the processing of this material, we also explore areas of protection through various physical components but also inevitably through encryption that uses various cryptographic algorithms for that purpose. As the use of biometric systems is extensive, many are still being developed, and existing ones are becoming more complex. Through the work, practical cases can be seen in specific areas. Despite the many challenges and risks associated with biometrics, the advantages compared to conventional methods are enormous, and it will certainly contribute to the realization of many rights, as the practice among international courts is more common and domestic courts are following this development to create a good domestic judicial practice in this area. Final considerations are presented with the observation that there is a need for a more detailed raising of awareness among data subjects for their protection, as well as data controllers and processors, and third parties who come into contact with them, and that active work is needed to adapt the state and law that should support all these steps.

Keywords: personal data, privacy, biometrics, biometric identification, types of biometric personal data.

XI Литература:

1. Андоновић С., Прља Д., Основи права заштите података о личности, Институт за упоредно право, Београд, 2020. године;
2. APF, „National ID scheme; Elsewhere in the World“. Чланак је преузет са адресе: http://www. privacy.org.au/Campaigns/ID_cards/Resources.html#NatIDSchemes.
3. Ashbourn J., The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management, Background paper for the Euroscience Open Forum ESOF 2006, Minhen 2006.
4. Ball K., Lyon D., Murakami D. W., Norris C., Raab C., A Report on the Surveillance Society, Full Report, 2006.
5. Biggio B., Adversarial Pattern Classification, Doctoral Dissertation, Electrical and Electronic Engineering University of Cagliari, 2010.
6. EBP, „Biometric passports introduced in Sweden and Norway“. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=31.
7. Bolle R.M., Connell J.H., Ratha N.K., Biometric perils and patches, Pattern Recognition, 2002. (чланак)
8. Clarke R., Biometrics and privacy, Department of Computer Science, Australian National University,Canberra, 2001.
9. Council od the European Union, 15801/06, Press Release, 2768th Council Meeting, Justice and Home Affairs.
10. Elliot R. J., Morre J. B., Aggoun Laghdar, Hidden Markov Models Estimation and control, Springer London, 2008.
11. Gafurov D., A Survey of Biometric Gait Recognition: Approaches, Security and Challenges. Norwegian Symposium on Informatics 2007 (NIK 2007). Oslo, Norway: Curran Associates, Inc.
12. EBP, „Greece set for ePassports“. Вест је преузета са адресе: http://www. europeanbiometrics.info/news/newsdetail.php?Id_news=157.
13. Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2018. (prirucnik zakona u skladu sa GDPR-om)
14. Хећимовић Ж., Метаподаци, Свеучилиште у Сплиту, Факултет грађевинарства, архитектуре и геодезије, Катедра за геодезију и геоинформатику, Сплит, 2016. године.
15. Isuru J., Cohen M., Amarakeerthi S., “BrainID: Development of an EEG-Based Biometric Authentication System“,IEEE 7th Annual Information Technology and Mobile Communication Conf., 2016.
16. Jain A. K., Uludag U., Hiding biometric data, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003.
17. Jain A.K., Ross A.A., Nandakumar K., Introduction to Biometrics, Springer, USA, 2011.
18. Kakona M., Drawbacks of Biometric Methods, Praque, 2001.
19. Leung Y., Knowledge Discovery in Spatial Data, Springer Verlag, Berlin Heidelberg 2010.
20. Li, S. Z., Jain, A. K., Handbook of face recognition (2nd Edition), New York, Springer, 2011.

21. McDowell M., Brainwaves: The Nature Of Brain Waves & Their Frequencies,Kindle edition, 2015.
22. Messer K., Kittler J., Marcel S., Rodriguez Y., Performance Characterisation of Face Recognition Algorithms and Their Sensitivity to Severe Illumination Changes, Institute of Computing Technology, Chinese Academy of Sciences, China, 2006.
23. Miller B., Vital signs of identity, IEEE Spectrum, February 1994.
24. Танјуг, „MUP-Mihajlovic: Novi informacioni sistem poboljsace sigurnost gradjana “, 11. септембар 2003. Вест је преузета са адресе: http://www.mfa.gov.yu/Srpski/Bilteni/Srpski/b120903_s.html#N25.
25. Пауновић С.Р., Примена мултимодалне биометрије у системима за утврђивање идентитета, Докторски рад, Београд, Факултет организационих наука, 2014. године.
26. EBP, „Pilot project for biometric passports in Switzerland “. Вест је преузета са адресе http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=258.
27. Поповић Д., Јовановић М., Право Интернета – одабране теме, Правни факултет у Београду, 2017.године.
28. Prabhakar S., Pankanti S., Jain K., IEEE Security & Privacy Magazine, 1(2), 2003.
29. Prabhakar S., Maltoni D., Maio D., Jain A. K., Handbook of fingerprint recognition, Springer London, 2003.
30. Reynolds D.A., Quatieri T.F., Dunn R.B., Speaker Verification Using Adapted Gaussian Mixture Models, Lexington, Massachusetts, 2000.
31. Ross A., Jain A.K, Information fusion in biometrics, Pattern Recognition Letters, Department of Computer Science and Engineering, Michigan State University, 2003.
32. Schmitz P.E., Tavano R., Lodge J., Huijgens R. & al., Biometrics in Europe - Trend Report (BETR), Brisel, 2006. (извештај)
33. Slemmons J., Straford J., Data Protection and Privacy in the United States and Europe, IASSIST QUARTERLY, 1999.; Orito Y, Murarta K., Rethinking the Concept of Information Privacy: A Japanese Perspective; This study was supported by an Academic Frontier project for private universities entitled “Global Business and IT Management: Global e-SCM”: a mathching fund subsidy was provided by MEXT(the Ministry of Education, Culture, Sports, Science and Technology) (чланак)
34. Soni Y.S., Somani S.B., Shete V.V., Biometric user authentication using brain waves, International Conference on Inventive Computation Technologies (ICICT), India 2016., И Ala Abdulhakim Alariki, Abdul Wasi Ibrahimi, Mohammad Wardak, John Wall, „A Review Study of Brian Activity-Based Biometric Authentication“, Journal of Computer Science, 2018.
35. Суботић О., Биометријски системи идентификације, Београд, 2007. године
36. Томић Д., Биометријска метода скенирања лица, Универзитет у Београду, Факултет Организационих Наука, март 2012. године.
37. 4 EBP, „UK: Liberal Democrats urge citizens to renew their passports“. Вест је преузета са адресе: http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=181.
38. Upmanyu M., Namboodiri A.M., Srinathan K., Jawahar C.V. Efficient biometric verification in encrypted domain. In Advances in Biometrics, Springer Berlin Heidelberg, 2009.
39. Др.Васковић В., Примена биометријских метода идентификације у банкама, Београдски Универзитет ТФ Бор, 2008.

40. Villegas M., Paredes R., Comparison of illumination normalization methods for face recognition, presented at the Third COST 275 Workshop-Biometric on the Internet 2005.

41. Volner R., Boreš P., Multi-Biometrics Techniques, Standards Activities and Experimenting, Elecrtronics and Elektrical Engineering No 8., Czech Technical University in Prague, 2006.
42. Woodward K., Directory Holds The Key To E-Passport Authentication , Card Technology, 2006.
43. Зуковић С., Слијепчевић С., Родитељска контрола понашања деце на интернету и социјалним мрежама, Педагошко друштво Србије и Институт за педагогију и андрагогију Филозофског факултета Универзитета у Београд, Београд, 2015.године;
44. Yam C.H., Nixon M. S., Gait Recognition, Model-Based, University of Southampton, Science+Business Media, LLC. 2009.

XII Остала истраживачка грађа

1. Закон о личној карти "Сл. гласник СР", бр. 62/2006.

2. Закон о путним исправама, „Сл. гласник РС." бр. 90/2007.

3. Закон о раду, „Сл. гласник РС." бр.24/2004

4. Устав Републике Србије, „Сл. гласник РС." бр.98//2006

5. Закон о заштити података о личности „Сл. гласник РС" бр.97/2008

6. Закон о заштити података о личности, „Сл. гласник РС." бр. 87/2018

7. HCICT– Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. (direktiva)

8. https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat

9. https://ltablice.com/novosti-za-vozace/saobracajna-dozvola-srbije

10.https://www.netsetglobal.rs/nacionalni-sistemi-za-izdavanje-i-upravljanje-identifikacionim-dokumentima/

11. https://www.netsetglobal.rs/biometrijska-autentikacija/

12. https://sh.wikipedia.org/wiki/DNK

13.https://sr.wikipedia.org/sr-ec/%D0%93%D1%80%D0%B0%D1%84%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%98%D0%B0

14. https://sh.wikipedia.org/wiki/Gasna_hromatografija

15. https://sr.wikipedia.org/sr-ec/Masena_spektrometrija

https://sr.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%98%D1%81%D0%BA%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%98%D0%B0

16. https://sr.wikipedia.org/sr-ec/RFID

17. https://w.wiki/9Jqa

18. https://www.milic.rs/zastita-podataka-o-licnosti/

19.https://www.poverenik.rs/sr-yu/%D0%BC%D0%B5%D1%92%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8-%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B86/%D0%B5%D0%B2%D1%80%D0%BE%D0%BF%D1%81k%D0%B0-%D1%83%D0%BD%D0%B8%D1%98%D0%B0/3443-%D0%BE%D0%BF%D1%88%D1%82%D0%B0-

%D1%83%D1%80%D0%B5%D0%B4%D0%B1%D0%B0-%D0%BE-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B8-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BE-%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8.html

XIII Биографија студента

Антанасијевић Бојана рођена је 26.03.1998. године у Врању. Основну школу "Доситеј Обрадовић" у Врању завршила је 2013. године као носилац Вукове дипломе. Гимназију Бора Станковић- језички смер у Врању завршила је 2017. године, такође, као носилац Вукове дипломе и исте године уписала Правни факултет у Нишу на ком је дипломирала 27. септембра 2022. године са просечном оценом 9.27. На трећој години студија освојила је друго место на такмичењу у писају есеја на тему "Вештачка интелигенција и људска права " у организацији Else. Школске 2022/2023. године уписала је мастер студије на Правном факултету у Нишу, смер информационе технологије. Током студирања обавила је потребне стручне праксе, најпре у Основном суду у Врању а онда и у адвокатској канцеларији у Нишу.

Ауторка је била корисница стипендије из буџета Републике Србије и као један од најбољих студената, добијала је награде града Врања за успех остварен током студирања.

Од 2021. године постала је стипендиста Фонда за младе таленте Републике Србије- "Доситеја", Министарства омладине и спорта за основне академске студије и мастер академске студије.

Марта 2023. године је уписала курс "Увод у Јава програмирање" са циљем специјализовања у тој области.

Студенткиња је оспособљена за рад на рачунару, познаје енглески и служи се француским језиком док поседује и усмено познавање турског и шпанског језика за личне потребе.

ИЗЈАВА О ИСТОВЕТНОСТИ ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора: Бојана Антанасијевић

Наслов мастер рада: ,,Биометријски лични подаци“

Ментор: проф. др. Милош Прица

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом : „Биометријски лични подаци“

пријављен и одбрањен на Правном факултету Универзитета у Нишу:

• резултат сопственог истраживачког рада;

• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;

• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Бојана Антанасијевић

У Нишу, _____

Потпис аутора

_____