

Biometrijske metode identifikacije

Skoko, Lea

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:131:842601>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2023-03-23**



Repository / Repozitorij:

[ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences](#)



SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020./2021.

Lea Skoko

Biometrijske metode identifikacije

Završni rad

Mentor: dr. sc. Vedran Juričić, doc.

Zagreb, rujan 2021.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

SADRŽAJ:

1. UVOD.....	1
2. POJAM IDENTIFIKACIJE I BIOMETRIJE	2
2.1. Identitet i identifikacija	2
2.2. Općenito o biometriji	3
3. BIOMETRIJSKI SUSTAVI PREPOZNAVANJA.....	4
3.1. FIZIČKA BIOMETRIJA	4
3.1.1. Analiza DNK zapisa	4
3.1.2. Skeniranje oka (šarenica i mrežnica oka).....	5
3.1.3. Prepoznavanje crta lica	6
3.1.4. Geometrija dlana i raspored vena	8
3.1.5. Odontologija.....	9
3.1.6. Otisak prsta.....	10
3.1.7. Termogram lica i tijela	11
3.2. BIOMETRIJA PONAŠANJA	12
3.2.1. Prepoznavanje glasa.....	12
3.2.2. Prepoznavanje rukopisa ili potpisa	13
3.2.3. Dinamika tipkanja.....	14
3.2.4. Dinamika hoda.....	14
3.2.5. Dinamika mirisa.....	15
4. MULTIMODALNA BIOMETRIJA	17
5. POUZDANOST I PRECIZNOST BIOMETRIJSKIH SUSTAVA.....	18
5.1. Zaštita privatnosti.....	19
6. ZAKLJUČAK	21
LITERATURA	22
SAŽETAK.....	25
SUMMARY	26

1. UVOD

Još od početka ljudske civilizacije poznate su različite metode prepoznavanja osoba u zemljama širom svijeta. Kroz povijest se identificiranje provodilo u različitim situacijama u svrhu prepoznavanja osoba u poslovnim transakcijama, pisci kao dokaz autorstva na dokumentu ili plemena kako bi označila prognanika. Provodilo se pomoću otisaka prstiju i dlanova, mjerenjem tijela, sakaćenjem, žigosanjem i sličnim metodama.

Ljudsko tijelo još od rođenja nosi informacije koje se koriste za identifikaciju. Svakodnevno se identificiramo i to nekoliko puta na dan, bilo da se radi o jednostavnoj identifikaciji poznanika pogledom na lice, pa sve do identifikacije preko kreditnih kartica, računala, telefona, aplikacija, društvenih mreža itd. Razvojem tehnologije povećava se potreba za sigurnijim i preciznijim načinima identifikacije koju danas nazivamo biometrijskom identifikacijom.

Biometrija je znanost koja predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi postupkom uspoređivanja uzoraka u svrhu identifikacije. Postoje dvije osnovne metode biometrijske identifikacije, a to su fizička metoda i metoda koja se bazira na ponašanju pojedinca. Fizička biometrija se bavi identificiranjem fizionomije ljudskog tijela. Neke od fizičkih metoda bile bi analiza otisaka prstiju, otisaka dlanova, DNK analiza, prepoznavanje crta lica, skeniranje oka i slično. Biometrija ponašanja opisuje fizikalne karakteristike kao što su kretanje u prostoru, izgled, glas itd.

Svrha rada je prikazati koliko je važna identifikacija, prepoznavanje i razlikovanje osoba, ali i ukazati na pouzdanost, preciznost te moguće greške biometrijskih sustava. Danas je gotovo nemoguće ne koristiti zaporke, koje se vrlo lako mogu izgubiti ili zaboraviti ili pak zloupotrijebiti od strane napadača. Upravo iz tog razloga biometrija omogućuje ljudima pristup određenoj mreži, odnosno identificiraju se pomoću svojih jedinstvenih karakteristika.

2. POJAM IDENTIFIKACIJE I BIOMETRIJE

2.1. Identitet i identifikacija

Pojam identiteta označava subjekt koji sebe određuje u odnosu na objekt, tj. u odnosu na sve druge koji ga okružuju ili na koje može misliti [1]. Svaki pojedinac posjeduje osobine koje ga čine jedinstvenim, prepoznatljivim i neponovljivim. Te osobine nam omogućavaju potvrdu našeg identiteta i onemogućavaju nekog drugog da ga koristi. Ponekad su obilježja pojedinca očita, pa je identitet lako utvrditi. No, često su objekti iste vrste slični i ne mogu se razlikovati bez primjene određenih metoda, pomoću kojih se detektiraju i u postupku identifikacije koriste detalji po kojima se objekti ipak razlikuju. Identitet predstavlja ukupnost nepromjenjivih obilježja koja čine određenu osobu ili predmet, a prema kojima se ta osoba ili predmet može razlikovati od svih drugih. Taj skup obilježja, odnosno individualnih karakteristika predstavlja individualnost [2].

Na temelju određenih identifikacijskih obilježja utvrđuje se istovjetnost nepoznatog s otprije poznatim, a taj proces utvrđivanja zove se identifikacija osoba. Budući da je svaki čovjek, životinja ili predmet jedinstven, neponovljiv i identičan samo sam sa sobom, podrazumijeva se da se razlikuje od svih drugih ljudi, životinja ili predmeta. Stoga identifikacija predstavlja postupak uspoređivanja određenog broja identifikacijskih obilježja kako bi se utvrdila podudarnost ili različitost objekata koji se uspoređuju. Da bi se ta identifikacijska obilježja mogla koristiti u procesu identifikacije, potrebno je zadovoljiti sljedeće uvjete:

1. univerzalnost - da ga posjeduje svaki pojedinac,
2. individualnost ili originalnost – podrazumijeva se da je različito kod svake osobe,
3. trajnost i nepromjenjivost,
4. mogućnost izdvajanja iz ukupnosti obilježja te
5. jednostavno prikupljanje i korištenje.

Kada govorimo o postupku utvrđivanja i provjere identiteta osobe koriste se tjelesna i pravna obilježja. Tjelesna obilježja se još nazivaju i stvarnim ili faktičkim obilježjima. Ona su definirana sama po sebi. Pravna obilježja podrazumijevaju činjenice koje svaki čovjek dobiva temeljem određenih pravnih propisa, kao npr. ime, prezime, državljanstvo, prebivalište i drugi [2].

Identitet određene osobe dijeli se na *osobni identitet* (koji je temeljen na podacima stečenim samim rođenjem, a uključuje ime, prezime, datum i mjesto rođenja te podatke o roditeljima), *biografski identitet* (koji osoba stječe kroz život, koji se prati preko službenih dokumenata i uvjerenja, kao što su škola, posao, banka, liječnički karton i sl.) i *biometrijski identitet* (koji je zasnovan na jedinstvenim fizičkim ili ponašajnim karakteristikama, kao što je otisak dlana, analiza lica, DNK analiza itd.) [3].

2.2. Općenito o biometriji

Biometrija potječe od grčkih riječi *bios* (život) i *metron* (mjera). Predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi temeljeno na jednoj ili većem broju njihovih fizičkih i ponašajnih karakteristika [4].

Kao tehnika identifikacije, biometrija je poznata još od davnina, ali na malo drugačiji način. Stari Egipćani su u svrhu identifikacije vršili različita mjerenja tijela, u Babilonu se otisak prsta na glinenoj ploči koristio za poslovne transakcije, a u Kini su trgovci uz pomoć tinte i papira radili otiske dlanova i stopala kako bi razlikovali malu djecu [5].

Prvi antropometrijski sustav, kasnije nazvan Bertillonageov sustav, razvio je francuski policijski službenik i znanstvenik Alphonse Bertillon. Sustav je imao široku primjenu u identifikaciji kriminalaca i prijestupnika, a temeljio se na preciznom mjerenju dimenzija tijela, dužine i širine glave te evidentiranjem osobnih obilježja osobe kao što su razne tetovaže, ožiljci i deformacije tijela. Sustav Bertillon se koristio sve dok se nisu pojavili problemi vezani uz neujednačene postupke mjerenja, nedovoljnoj preciznosti kod mjerenja i velikoj promjenjivosti ljudskog tijela tijekom godina. Sustav je sužavao broj počinitelja, ali nije davao točan rezultat [5].

Ravoj tehnologije povećava i potrebu za sigurnijim načinima identifikacije osoba pa su biometrijske metode postale znatno složenije i preciznije.

3. BIOMETRIJSKI SUSTAVI PREPOZNAVANJA

Biometrijska identifikacija se odnosi na tehnologije koje mjere i analiziraju fizičke i ponašajne karakteristike čovjeka. Iako se prvenstveno koristi za potrebe identifikacije, primjenjuje se i u drugim područjima kao što je prepoznavanje korisnikovog govora u svrhu bržeg pisanja. Biometrija objedinjuje korištenje specijalnih uređaja koji prate određene fizičke ili ponašajne karakteristike te programa koji analiziraju dobivene informacije.

Sastavni elementi biometrije su uzorkovanje, odnosno pretvaranje analognog signala u digitalni i umjetna inteligencija. Dobivene informacije se obrađuju u računalu, stvara se umjetna inteligencija, računalo prepoznaje uzorke i uspoređuje se sistem učenja računala s ljudskim mozgom. Cilj je korištenje računala kao posrednika u uzorkovanju, dok programski paket preuzima odluku što će poduzeti s digitaliziranim uzorcima. To obuhvaća sveukupan proces digitalizacije, prepoznavanja uzoraka, umjetne inteligencije, a sve sa ciljem kako bi se računalo unaprijedilo u procesu učenja i kako bi samostalno bilo u stanju upamtiti i koristiti uzorke [4].

3.1. FIZIČKA BIOMETRIJA

Fizička biometrija je dio biometrije koja se bavi uzorkovanjem fizionomije ljudskog tijela i njegovim jedinstvenim karakteristikama. Temelj fizičke biometrije je ljudska fizička jedinstvenost koja omogućuje raspoznavanje ljudi na osnovi iste i korištenje pripadajućih opisa uzoraka za njihovo prepoznavanje. Prepoznati uzorci mogu se koristiti u kombinaciji s ostalim klasičnim zapisima kojima se jedinstveno opisuju osobe. Pod fizičku biometrijsku metodu prepoznavanja spadaju: analiza DNK zapisa, skeniranje oka, prepoznavanje crta lica, geometrija dlana i raspored vena, odontologija, otisak prsta te termogram lica i tijela.

3.1.1. Analiza DNK zapisa

Ljudska identifikacija ima veoma važnu ulogu u mnogim poljima u svijetu kao što su forenzika, vladine institucije, medicinske primjene i slično. Konkretno korištenje DNK analize smatra se jednim od najpouzdanijih i najznačajnijih metoda biometrijske identifikacije. DNK (deoksiribonukleinska kiselina) je dvolančana nukleinska kiselina, sastavljena od šećera deoksiriboze, fosfatne skupine i pridruženih dušičnih baza. Ona se uvija

višestruko i zajedno s proteinima jezgre tvori kromosome. Kromosomi i geni na njima su nositelji nasljednih svojstava svakog čovjeka koji se mogu biometrijski identificirati.

Britanski znanstevnik sir Alec Jeffreys prvi je primijenio činjenicu o jednostavnosti građe molekule DNK na identifikaciju, odnosno otkrivanje kriminalaca. „Ova metoda temelji se na činjenici da je ljudski organizam sastavljen od oko 100 trilijuna živih stanica. Svaka stanica građena je od jezgre kao središnjeg dijela i citoplazme koja okružuje jezgru, a koja je s vanjske strane obavijena membranom koja stanicu odvaja od drugih stanica. U kromosomima je smještena jezgrina ili nuklearna DNK, dok se u citoplazmi nalaze brojne stanične strukture među kojima i mitohondriji, u kojima se nalazi mitohondrijska DNK. Cjelokupni genetički profil organizma zove se genom.“ [2]

DNK je jedinstvena je za svaku osobu s iznimkom jednojajčanih blizanaca čija je struktura DNK ista. Čak oko 99,5% molekule DNK je zajedničko svim ljudima, dok preostalih 0,5% čini kodirajuća područja koja su polimorfna te tako čine svaku osobu jedinstvenom [2].

Analiza DNK zapisa funkcionira tako da se DNK neke jedinice nakon očitavanja uspoređuje s pohranjenim zapisom u bazi podataka. Na taj je način moguće provoditi identifikaciju korisnika prilikom pristupa nekom sustavu ili prostoru. Ova tehnika se koristi u mnogim područjima istraživanja, neke od zanimljivih primjena su u području kriminalistike i sudske medicine gdje se analiza DNK koristi za utvrđivanje identiteta nepoznate osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tijela, određivanje spola osoba, te kriminalistička istraživanja kaznenih djela.

3.1.2. Skeniranje oka (šarenica i mrežnica oka)

Ljudsko oko je jedan od najkompleksnijih parnih organa. Ono je ujedno i najvažnije ljudsko osjetilo jer njime primamo preko 80% svih informacija iz okoline. To je senzorni organ koji se nalazi u orbiti lubanje. Sastoji se od unutarnje, srednje i vanjske ovojnice. Vanjsku očnu ovojnicu čine bjeloočnica (sklera) i rožnica (kornea). Srednja očna ovojnica sastoji se od šarenice (iris), cilijarnog tijela, leće, staklastog tijela i žilnice (koroidea). Unutarnu očnu ovojnicu čini mrežnica (retina) i očni živac. Oko sadrži mnogo individualnih karakteristika koje ga čine izuzetno pogodnim za postupak identifikacije osoba. Postoje dvije metode određivanja identiteta pomoću oka, a to su: skeniranje šarenice i skeniranje mrežnice oka.

Identifikacija ljudskog bića pomoću šarenice oka jedna je od najsigurnijih biometrijskih metoda. Šarenica je obojeni dio oka koji okružuje zjenicu, a sastoji se od mnoštva brazdi, prstena i pjega u različitim bojama. Na šarenici se nalazi oko 200 karakteristika pogodnih za samu identifikaciju osobe. Svaki pojedinac ima svoj neponovljivi i jedinstveni kompleks boja i šara koje su pogodne za identifikaciju. Izgled šarenice se definira u ranom djetinjstvu i starenjem se ne mijenja. Nemoguće ju je promijeniti bez velikog rizika od gubitka vida. Osim toga, šarenicu je nemoguće krivotvoriti ili prevariti lećama, staklenim ili pravim okom koje je odstranjeno s mrtvaca. Postoje algoritmi koji registriraju promjene na živom oku, a kod staklenog oka ili oka mrtve osobe nema ekspanzije ili kontrakcije zjenice kad je oko osvijetljeno svjetlošću. Ova metoda identifikacije je vrlo jednostavna i pouzdana te ne zahtijeva fizički kontakt oka i skenera. Snimanje se može obaviti i s običnom kamerom na udaljenosti i do pola metra, a za pregled baze je potrebno par sekundi. Metodu prepoznavanja osoba skeniranjem šarenice nazivamo i irisologija [6].

S druge strane, mrežnica je tanki sloj stanica s obiljem krvnih žila smještenih u stražnjem dijelu oka. Njena je struktura individualna i jedinstvena za svaku osobu. Ono što mrežnicu čini jedinstvenom jest složenost mreže krvnih žila. Ova biometrijska metoda pruža najveću točnost prepoznavanja, ali je ujedno i najskuplja metoda identifikacije jer je oprema koja se koristi za skeniranje mrežnice vrlo skupa. Zbog visoke cijene, ali i visoke pouzdanosti ova metoda koristi se u područjima i objektima visokog stupnja sigurnosti gdje cijena opreme nije odlučujući čimbenik. Za uspješno skeniranje mrežnice oka potrebno je skinuti naočale i oko približiti skeneru, te fokusirati pogled na određenu točku. Proces skeniranja traje 10-15 sekundi i oko se za vrijeme skeniranja osvjetljava blagim snopom svjetlosti, zbog čega ova metoda spada u neugodnije biometrijske metode [6].

Također, ovu metodu nije moguće promijeniti ili replicirati unutarnju strukturu oka, jer se niti ona ne mijenja tijekom čitavog života, a mrežnica mrtve osobe toliko brzo propada da nisu neophodne dodatne mjere utvrđivanja znakova smrti [2].

3.1.3. Prepoznavanje crta lica

U svakodnevnom životu ljudi prepoznaju jedni druge prema izgledu lica. Uz ostale tjelesne i ponašajne karakteristike, lice definira ono što primarno doživljavamo izgledom neke osobe. Lice svakog pojedinog čovjeka je individualno, po svom izgledu i građi se razlikuje od lica svih drugih osoba, primjerice fizionomijom lubanje, rasporedom miškulature, položajem i izgledom dijelova lica poput čela, nosa, očiju, usta i slično. No,

budući da se identifikacija prepoznavanjem temelji na vidu čovjeka koji prepoznaje, psihološkim procesima vezanim za percepciju, pamćenjem i slično, može se reći da je ova vrsta identifikacije vrlo subjektivna, pa se u postupku prepoznavanja mogu dobiti nepouzdana podaci. Identifikacija temeljem rasporeda crta lica, odnosno skeniranje lica je jedno od najzanimljivijih i najistraživanijih područja biometrije.

Sustav za prepoznavanje lica može se koristiti na dva načina, verifikacijom ili autentikacijom i identifikacijom. Verifikacija ili provjera autentičnosti potvrđuje ili negira identitet određene osobe, dok sustav identifikacije lica pokušava uspostaviti identitet određene osobe iz nekog skupa ljudi [7].

U klasičnoj identifikaciji poznata je identifikacija osoba putem fotografije, pri čemu se osoba, čiji je identitet potrebno utvrditi, fotografira u istom mjerilu u kojem je fotografija osobe s kojom je želimo usporediti. Metodama linearnih i kutnih mjerenja uspoređuju se razmaci između pojedinih dijelova lica. Kroz povijest se dosta primjenjivala i tzv. metoda superpozicije, odnosno preklapanja spornog i nespornog negativa filma ili dijapozitiva jednog preko drugog te se provjerom poklapanja određenih točaka i detalja utvrđivala istovjetnost [2].

Što se tiče računalnog, biometrijskog prepoznavanja lica, uglavnom se radi o usporedbi na temelju fotografije ili videosnimke. Budući da se lice dijeli na oko 80 karakteristika, kao što su razmak između očiju, dimenzije nosa, položaj i razmak između jagodičnih kostiju, dimenzije i oblik brade itd., potrebno je ispuniti uvjete tražene za identifikacijska obilježja. Potrebno je preklapanje od 15 do 20 karakteristika, tako da se osoba može identificirati i nakon estetskih korekcija izgleda lica, promjene frizure, nošenja naočala i slično. Uzimajući u obzir da fotografija zauzima malo memorije, sustav može uspoređivati više milijuna fotografija u minuti, što daje veliku prednost u pronalaženju i potvrđivanju identiteta [2].

Danas se prepoznavanje lica koristi gotovo svakodnevno i može se reći da je to najčešće korišten način identifikacije. Pametni mobilni uređaji nude mogućnost prepoznavanja svojih korisnika prema izgledu i građi njihovog lica. Prepoznavanje lica na taj način zamjenjuje kratke zaporke, crtanje po ekranu, čak i prepoznavanje otiska prsta prilikom otključavanja mobilnog uređaja. Tako primjerice Apple mobilni uređaji koriste novu tehnologiju za otključavanje mobilnih uređajaja koja se naziva Face ID. Face ID koristi precizne kamere za snimanje lica kako bi se izradila detaljna karta i infracrvena slika na temelju više od trideset tisuća točaka na korisnikovom licu [8]. Dugoročno se prilagođava

korisnikovom licu te bi trebao prepoznati strukturu lica i slučaju da korisnik počne nositi naočale, dobije ili izgubi na kilaži, ostari ili promijeni bilo koju drugu fizičku karakteristiku. Pored otključavanja mobilnih uređaja, prepoznavanje lica se koristi i za upravljanje fotografijama. Tako neki mobilni uređaji imaju mogućnost grupiranja fotografija na kojima se nalazi ista osoba.

3.1.4. Geometrija dlana i raspored vena

Identifikacija na temelju izgleda i geometrije dlana, odnosno šake, je proces u kojem se analizira dužina prstiju i oblik dlana. Provedba ove metode je gotovo podudarna s ranije opisanom identifikacijom na temelju izgleda i proporcija lica. Provodi se snimanjem ruku, te automatskom usporedbom oko 90 obilježja kao što su oblik, raspored i duljina kostiju. S obzirom da geometrija dlana nije dovoljno jedinstvena kod svake osobe, radi se o relativno nepouzdanom metodi koja se uglavnom koristi u postupcima provjere identiteta, odnosno za autentikaciju.

Mnoge karakteristike dlana se mogu koristiti za identifikaciju, a neke od osnovnih značajki dlana su glavne linije, nabori, grebeni, singularne točke i detaljne točke. Ova metoda može biti, ali i ne mora biti vidljiva golim okom. Identifikacija se postiže pomoću algoritama koji mogu razlučiti razlike između dvije osobe prema značajkama dlana. Te značajke se mogu prikupiti uzimanjem otiska dlana. Otisak je utisak na nekoj površini pritiskom, a čini ga obrazac kože na dlanu sastavljen od svojih jedinstvenih karakteristika kao što su linije, točke i tekstura. Zbog znojenja, otiske dlana možemo naći na površinama raznih objekata. Ako je dlan suši, to su otisci manje vidljivi. Može se prikazati sa i bez tinte [9].

Osim identifikacije pomoću geometrije dlana, pojavljuje se i jedna od novijih metoda identifikacije na temelju ruku, a to je identifikacija bazirana na usporedbi rasporeda vena na šaci, prilikom koje se traže mjesta spajanja krvnih žila koje imaju svoje jedinstvene šare. Ova metoda se bazira na suvremenim tehnologijama i spada u neinvazivne metode. Vrlo je primjenjiva u sustavima gdje je potrebno u kratko vrijeme usporediti veliki broj objekata, bez visokih zahtjeva pouzdanosti [2]. Pretpostavlja se da će ova metoda u budućnosti primjenu pronaći i kod proizvodnji brava koje se automatski otključavaju ili kod oružja koje može opaliti samo ukoliko se nalazi u ruci vlasnika.

Sve metode imaju svoje prednosti i mane te niti jedna nije savršena za svaku situaciju. Prednosti ove metode su manji troškovi, budući da se mogu koristiti slike niske rezolucije, društveno je prihvatljiva, jeftiniji su prikladni senzori te ima stabilne strukturalne značajke

koje su nepromjenjive tijekom života. Osim toga, otisak dlana ima veliku površinu pa se može izučiti mnogo linijskih značajki koje se ne mijenjaju tijekom života, na dlanu ima manje prljavštine ili masti nego na prstu. Vremenske neprilike ili oštećena koža nemaju nikakvog utjecaja na točnost prilikom autentifikacije. No veliki utjecaj ima nakit na ruci, nedostatak dijela prstiju ili pak izostanak prstiju s ruke [9].

3.1.5. Odontologija

Utvrđivanje identiteta temeljem statusa zubala zove se odontologija. Primjena dentalne identifikacije posebno je bitna u okolnostima kada stradaju velike skupine ljudi, kao što su prirodne katastrofe: požari, potresi, poplave, prometne nesreće. Odontologija se pokazala nužnom i u ratnim i poslijeratnim prilikama. Ovom vrstom identifikacije moguće je odrediti pravi identitet nepoznate osobe uz pomoć poznatih premortalnih obilježja, a poznavanjem dentoantropoloških parametara također je moguće utvrditi pripadnost rasi, dobi i spolu [10].

Zubna identifikacija preuzima glavnu ulogu u identifikaciji posmrtnih ostataka kada postmortalne promjene, traumatična ozljeda tkiva ili nedostatak zapisa otiska prsta onemogućuje upotrebu vizualnih metoda ili metoda otiska prsta. Identifikacija zubnih ostataka od primarne je važnosti kada je preminula osoba skeletonizirana, razgrađena, spaljena ili raskomadana. Glavna prednost dentalnih dokaza je što se, kao i ostala tvrda tkiva, dugo čuvaju nakon smrti. Čak se i status zuba osobe mijenja tijekom života, a kombinacija pokvarenih, ispalih ili izvađenih i ispunjenih zuba mjerljiva je i usporediva u bilo kojem trenutku. Temeljni principi dentalne identifikacije su usporedivi i isključivi. Na primjer, odontologija se koristi kada su dostupni premortalni zapisi za navodno preminulu osobu i posredni dokazi sugeriraju identitet preminuloga. Koristi se i za isključivanje identiteta drugih neidentificiranih osoba čiji su podatci prije smrti poznati. Identifikacija zahtijeva popis mogućih uključenih osoba kako bi se mogle pronaći odgovarajuće zabilješke. Dostupnost i točnost ovih zapisa određuju uspjeh identifikacije. Nažalost, stomatolozi često vode lošu evidenciju, što rezultira zbrkom koja onemogućava identifikaciju zubala [11].

Osim utvrđivanja identiteta mrtve osobe može se raditi i o identifikaciji počinitelja i/ili žrtve koji je ostavio tragove zubi na drugoj osobi ili predmetima. U postupku klasične identifikacije gleda se broj zubi, njihov položaj i raspored, veličina, razmak, a zatim i osobitosti zuba i zubala. Mogu se koristiti i tragovi stomatoloških zahvata poput popravaka, plombi, kruna, mostova, proteza i dr. Dakle više se uspoređuje vizualno, dok se u području

biometrijske identifikacije najviše koristi dentalna radiologija, odnosno rendgenske snimke [2].

3.1.6. Otisak prsta

Koža se dijeli na vanjski sloj, epidermis, i unutarnji sloj koji se sastoji od dermisa i potkožnog vezivnog tkiva. Prsti, dlanovi i donji dijelovi epidermisa na stopalima ispresijecani su mnogobrojnim uleknućima i uzdignućima koji tvore papilarne linije. One se počinju stvarati u maternici, tijekom prvih tjedana razvoja embrija. Identifikacija otisaka papilarnih linija prstiju i dlanova predstavlja biometrijsku metodu koja se temelji na jedinstvenom rasporedu udubljenja i ispupčenja kože. Otisak papilarnih linija se koristi za identifikaciju jer su njegove glavne karakteristike vremenski nepromjenjive i jedinstven je za svakog pojedinca.

Karakteristike slike otiska se mogu podijeliti na lokalne i globalne. Globalne obuhvaćaju tok papilarnih linija koje tvore neki od prepoznatljivih oblika po kojima se otisci svrstavaju na pet klasa: lijeva i desna petlja, luk i šatorski luk te spirala. Globalne karakteristike nisu dovoljne za pouzdanu identifikaciju. Papilarne linije su ponekad vrlo kratke ili iz jedne nastaju dvije, odnosno obiluju raznim detaljima koje se nazivaju minucije, što spada u lokalne karakteristike. One jesu dovoljne za pouzdanu identifikaciju, ali sustavi za prepoznavanje, temeljeni samo na njima, zanemaruju ostale jedinstvenosti otiska kao što je primjerice lokalna orijentacija papilarnih linija. Procjena lokalne dominantne orijentacije je jedna od najvažnijih operacija u sustavima za automatsko prepoznavanje otisaka prstiju [12].

Identifikacija pomoću otiska prsta najrasprostranjenija je u kriminalistici, a jedan od prvih sustava za kriminalističku identifikaciju razvio je Ivan Vičetić, policijski službenik hrvatskog podrijetla, 1891. godine u Argentini. Ovaj način identificiranja osoba danas je poznat pod nazivom daktiloskopija. Klasična daktiloskopija u digitalnom okruženju dobiva novi oblik te se ne koristi samo u kriminalistici, već i u području privatne zaštite sustava za autorizaciju i autentikaciju, odnosno za kontrolu ulaska i kretanja po zaštićenom prostoru [2].

U području policijske djelatnosti implementiran je sustav za automatsku obradu otisaka papilarnih linija koji je poznat pod nazivom AFIS (*Automated fingerprint identification system* - Sustav automatizirane identifikacije otisaka prstiju). AFIS je moderni računalni sustav za automatiziranu obradu otisaka papilarnih linija prstiju i dlanova, a u svojoj bazi podataka sadrži otiske iz opće deseteroprstne DKT zbirke, otiske dlanova i sporne tragove papilarnih linija. Sustav se pokazao odličnim prije svega zbog brzine uspoređivanja

otisaka u bazi podataka. Princip rada AFIS-a je vrlo jednostavan, otisci se digitaliziraju skeniranjem traga, odnosno otiska s mjesta događaja, izuzetog na foliji ili fotografiranog te se unose u bazu podataka. Nakon unosa u bazu podataka započinje proces analize gdje se uspoređuju uneseni otisci s postojećima iz baze podataka [2].

Postoje brojne tehnologije za evidentiranje otisaka prstiju i njihovu usporedbu. Najpoznatije su: *optička* - za očitavanje papilarnih linija prsta koriste digitalne kamere, *kapacitivna* - temelji se na razlikama napona između ispupčenja i zraka u udubinama, *radijska* - bazira se na radiovalovima niskog intenziteta kojima se ozrači prst, *tehnologija tlaka* - čitač je sastavljen od mnoštva točki koje su osjetljive na tlak i evidentiraju uzorak grebena kad se na njega položi prst, *mikro-elektro-mehanička metoda* - temelji se na mnoštvu mikro-mehaničkih tipki koje raspoznaju grebene i doline otiska prsta i *toplotna* - temelji se na piroelektričnim materijalima koji mogu razliku u temperaturi pretvoriti u određeni napon. Nažalost, većina ovih tehnika ima brojne nedostatke te je nemoguće razlikovanje živog prsta od imitacije. Postoje razne aplikacije i računalni programi koji se baziraju na temeljnom postupku za prepoznavanje otisaka prstiju. Prvi korak je prikupljanje otisaka prstiju osoba u zbirku, a taj uzeti otisak prsta se naziva predložak osobe. Nakon toga se snimaju otisci prstiju osoba. Takvi podaci se zovu uzorci. Naposljetku se u automatskom postupku uspoređuju predložak i uzorak. Za usporedbu predložka i uzorka koristi se usporedni algoritam koji provjerava i uspoređuje različita usmjerenja slike i stupanj sukladnosti te ih izražava u brojčanoj vrijednosti poklapanja. Podudarnost koja je iznad određene razine potvrđuje istovjetnost ili bliskost [2].

3.1.7. Termogram lica i tijela

Prema Hrvatskoj enciklopediji, termografija predstavlja postupak snimanja objekata koji zrače infracrveno zračenje. Provodi se termografskim kamerama koje registriraju emitiranu energiju zračenja objekata, s primarnim ciljem određivanja temperature njihove površine. U tim kamerama zračenje prolazi kroz optički sustav za izoštravanje te pada na senzor koji energiju zračenja pretvara u naponski signal. Signal se nakon pojačavanja i obrade sprovodi na zaslone, na kojim se prikazuje termogram. To je zapis trenutačne razdiobe temperature na promatranoj površini objekta prikazane različitim tonovima [13]. Dakle, termogram je snimka koja se dobiva snimanjem infracrvenom kamerom koja omogućuje registriranje toplinskih zračenja koje krvne žile emitiraju kroz kožu.

Splet krvnih žila kojima je prožeto ljudsko tijelo, a posebno njegov potkožni dio, predstavlja jedinstveno obilježje i individualan je kod svakog pojedinog čovjeka. Termogrami lica i tijela ispunjavaju gotovo sve uvjete za identifikaciju jer su univerzalni, individualni i konstantni, ali kao i kod većine biometrijskih metoda identifikacije, tako i kod ove metode postoje određeni nedostaci. Jedan od nedostataka je taj što postoji mogućnost manipulacije promjenama u termogramu pod utjecajem različitih unutarnjih i vanjskih čimbenika, npr. izjednačavanjem temperature okoline i tijela, pod utjecajem opojnih sredstava i sl. Osim toga, cijena opreme je izrazito visoka i slike dobivene ovom metodom zauzimaju puno memorijskog prostora, pa iz toga razloga nije primjerena za velike digitalne baze podataka. Zanimljiva je činjenica da je identifikaciju moguće obaviti pod raznim svjetlosnim uvjetima, kao i u potpunom mraku. Osim toga, ova metoda omogućuje prepoznavanje i bez suradnje osobe [2].

3.2. BIOMETRIJA PONAŠANJA

Biometrija ponašanja opisuje fizikalne karakteristike čovjekovog tijela koje su dijelom jedinstvene za svaku osobu. Dobiveni uzorci se opisuju krivuljama koje se koriste za opis ponašanja pa je na osnovi istih moguće raspoznavati različite ljude. Navedene tehnike se koriste u kombinaciji s tradicionalnim načinima jednoznačnog opisivanja ljudi. Pod ponašajnu biometrijsku metodu prepoznavanja spadaju: prepoznavanje glasa, prepoznavanje rukopisa ili potpisa, dinamika tipkanja, hod i tjelesni mirisi.

3.2.1. Prepoznavanje glasa

Glas osobe predstavlja jedinstveno i individualno obilježje, pa se zbog toga može, poput npr. otisaka prstiju, koristiti za identifikaciju ljudi. Budući da veoma lagano prepoznamo glas, odnosno govor osoba koje poznamo, jasno je da se radi o subjektivnom doživljaju baziranom na subjektivnim karakteristikama slušatelja.

Kad je riječ o identifikaciji osobe temeljem glasa, radi se o karakteristikama glasa poput boje glasa, modulacije, frekvencije, specifičnostima izgovora određenih glasova, govornim manama i drugo, a to područje identifikacije zove se fonoskopska identifikacija. Postupak identifikacije na temelju glasa obavlja se na način da se glas osobe snimi, što čini nesporni uzorak, i zajedno sa snimkom spornog glasa dostavi na vještačenje. Eksperti posebnim uređajem glas pretvaraju u električne signale i vizualiziraju kroz grafikone čije se

amplitude uspoređuju. Preklapanjem ili odstupanjem grafičkog prikaza glasa određene osobe s grafičkim prikazom sporne osobe dobivamo rezultate identifikacije [2]. Rezultati ovakve metode ovise o kvaliteti snimaka, lokaciji mjesta na kojem je govornik stajao za vrijeme snimanja, promjeni boje glasa godinama ili bolešću, akustici prostorije u kojoj se glas snima, položaju i udaljenosti od mikrofona i slično. Ova metoda identifikacije je pogodna jer je oprema za izvođenje jeftina i lako dostupna, a pouzdana je ukoliko se kombinira s drugim metodama.

Identifikacijom govornika mogu se baviti stručnjaci koji imaju primarno akademsko obrazovanje u području fonetike, lingvistike, patologije glasa i govora (logopedije) i/ili akustike [14].

3.2.2. Prepoznavanje rukopisa ili potpisa

Iako u današnjem vremenu tipkovnica sve više zamjenjuje standardno pisanje pomoću olovke i papira, još uvijek postoji mnogo zadataka koje ljudi više preferiraju unositi rukom nego tipkovnicom, npr. bilješke s predavanja, izrada nacrtanih skica itd. Rukopis je osobna vještina svakog pojedinca, sastoji se od umjetnih grafičkih oznaka kojima je svrha prenijeti poruku [15]. Budući da svaka osoba ima svoj jedinstven rukopis i potpis, također ih možemo koristiti u svrhu identificiranja. Prepoznavanje se bazira na brzini pisanja, pritisku prilikom potpisivanja, veličini rukopisa, dužini poteza, rasporedu teksta, vezanosti i nevezanosti slova, nagibu rukopisa, ukrašavanju i slično.

U klasičnoj identifikaciji rukopisa i potpisa provodi se grafološka analiza koja se uglavnom temelji na grafičkim, ali i nekim psihološkim i biheaviorističkim premisama skriptora, odnosno osobe kojoj pripada rukopis ili potpis. Međutim, kada je riječ o biometrijskoj metodi analize potpisa i rukopisa, treba naglasiti da je metoda prihvatljiva, ali i da postoji mogućnost krivotvorenja. Ipak, određena obilježja rukopisa, odnosno potpisa mogu se grafički determinirati i klasificirati, jer ostaju nepromijenjena unatoč pokušajima namjernog pokušaja promjene rukopisa [2]. Velika prednost ove metode identifikacije je to što za dobijanje statične slike potpisa nije potrebna nikakva posebna oprema, dovoljan je potpis na papiru, skener ili digitalni fotoaparatus. Važna je činjenica da se rukopis mijenja vremenom te je zbog toga potrebno povremeno ažurirati podatke u bazi podataka kako bi identifikacija bila što pouzdanija.

3.2.3. Dinamika tipkanja

Tijekom Drugog svjetskog rata, kada su obavještajne službe pokušavale saznati tko je pošiljatelj telegrama na osnovu načina slanja telegrafskih poruka, uočeno je da se pošiljatelji poruka mogu razlikovati po brzini, ritmu i dinamici tipkanja. Identificiranje pošiljatelja poruke moglo je pridonijeti prepoznavanju korištenog koda i dešifriranju poruke. Danas dinamika tipkanja podrazumijeva tipkanje na tipkovnici računala, odnosno vremenskom razmaku između pritiskanja dvije tipke, dinamici otipkavanja PIN koda na uređajima za autentikaciju i slično.

Radi se o perspektivnoj i značajnoj metodi identifikacije, čije korištenje može biti vrlo jednostavno i jeftino. Nije potrebno uvoditi nikakve dodatne uređaje za detektiranje, osim zvučne kartice. Eventualno je moguće posjedovati i specijalizirani program koji bi na razini operacijskog sustava pratio korisnikovo tipkanje [4]. Dinamika tipkanja je postupak analize načina na koji korisnik tipka na uređaju. Izvodi se praćenjem obrasca pritiskanja tipki na tipkovnici i pokušajem identificiranja korisnika na temelju uobičajenih ritmičkih uzoraka u stilu po kojem tipkaju. Postupak prepoznavanja mjeri ritam tipkanja korisnika i generira jedinstveni biometrijski predložak za obrazac tipkanja određenog korisnika. Mjere koje se mogu snimiti uključuju vrijeme zadržavanja (vrijeme pritiska i otpuštanja jedne tipke) i vrijeme između dva uzastopna pritiska tipki. Snimljeno vrijeme se zatim obrađuje pomoću novog algoritma, koji određuje primarni obrazac za podatke o tipkanju [16]. Posebno je značajno područje identifikacije korisnika računala po dinamici tipkanja pri tzv. *On-line* tipkanju na tipkovnici računala, zbog poznatih oblika kaznenih djela vezanih uz internet.

Problem s prepoznavanjem dinamike tipkanja je taj što za razliku od drugih nestatičnih biometrijskih metoda (poput prepoznavanja glasa) ne postoje poznata obilježja ili značajke koje su namijenjene isključivo za nošenje diskriminirajućih podataka. Srećom, u posljednjih nekoliko godina istraživači su predstavili empirijska otkrića koja pokazuju da različiti pojedinci imaju različita svojstva u svome ritmu tipkanja, koji su izrazito individualni i da se te karakteristike mogu uspješno upotrebljavati u svrhu identifikacije [16].

3.2.4. Dinamika hoda

Ljudsko hodaње je složeno djelovanje kretanja koje uključuje sinkronizirane integrirane pokrete dijelova tijela, zglobova i interakciju među njima. Različite varijacije između svojstava tjelesnih struktura, težine udova i djelovanja različitih subjekata mogu pružiti jedinstveni znak za prepoznavanje identiteta. Dinamika hoda je novonastala

biometrijska metoda koja nudi mogućnost prepoznavanja ljudi na daljinu. Dok većina metoda identifikacije obično zahtijeva fizički dodir ili proksimalni senzor, identifikacija pomoću hoda ne zahtijeva korisnikovu interakciju.

Mnogo je svojstava hoda koji mogu poslužiti kao prepoznatljiva obilježja čovjeka. Mogu se karakterizirati kao statičke i dinamičke značajke, pri čemu prvi obično odražavaju mjerenja temeljena na geometriji, poput visine tijela i građe, dok se drugi baziraju na putanje glavnih udova u zglobovima. Prepoznavanje hoda, kao kombinacija ljudske analize kretanja i biometrije, u osnovi ima za cilj diferencirati ljude načinom na koji hodaju [17]. Ovaj način identifikacije uvelike ovisi o tome kako se oblik statične siluete mijenja s vremenom, primjerice starenjem. Osim toga, uvjetovan je brojnim tjelesnim i drugim karakteristikama.

Uzorak hoda se dobiva iz video zapisa učinjenog video kamerom. Sve provjere dinamike hoda se temelje na karakterizaciji nekoliko različitih pokreta svakog od zglobova prilikom izvođenja određene radnje [4].

3.2.5. Dinamika mirisa

Svako biće u prirodi ima svoj miris koji je karakterističan za njegov kemijski sastav. Miris je skup izlučevina ljudskog tijela koji je individualan za svaku osobu te se iz tog razloga ljudski mirisi koriste u svrhu identifikacije u kriminalističkom istraživanju.

Budući da u današnjem vremenu kriminalci pokazuju sve veći nivo svog kriminalističkog obrazovanja kroz detaljnije planiranje, načine izvršenja, ali i načine uklanjanja vidljivih tragova, raste veća potreba za mogućnošću pronalaska onih nevidljivih tragova koji ostaju na licu mjesta kaznenog djela. Odorologija je posebna grana kriminalistike koja se bavi tjelesnim mirisima [18]. Većina mirisa luči se iz površine tijela, kože i potkožnog tkiva, ali velik dio potječe iz pluća i gastrointestinalnog trakta. Mirisi tog podrijetla imaju vrlo veliku diferencijalnu vrijednost, nastalu specifičnom prehranom, životnim stilom i brojnim dodatnim specifičnostima određene osobe. Ljudski miris predstavlja posebnu vrstu mikrotraga, jer čovjek prilikom kretanja iza sebe u zraku ostavlja molekule mirisa koje se sastoje od individualnog mirisa osobe i raznovrsnih mirisa sredine u kojima boravi. Za detektiranje mirisa postoje biometrijski sustavi koji rade na principu upuhivanja zraka preko kemijskih senzora od kojih je svaki osjetljiv na određenu grupu mirisa, tj. na njegova kemijska svojstva. Zatim se opisuju miris i njegov intenzitet obuhvaćeni sensorima mjerenja. Pretpostavljajući da svaka osoba sadrži karakterističan miris, moguće je po parametrima svakog od senzora odrediti o kojoj se osobi radi i odrediti glavnu notu mirisa.

Važno je odijeliti mirise, posebno razlikovati miris osobe od mirisa parfema te je zbog toga potrebno još istraživanja kako bi metoda pokazala što točnije rezultate. Danas se intenzivno radi na pronalasku metoda prikladnih za prikupljanje i pohranu uzoraka, kako bi se omogućilo stvaranje baza podataka mirisa [2].

4. MULTIMODALNA BIOMETRIJA

Biometrijski sustavi se koriste za provjeru i identifikaciju pojedinaca koristeći njihove fiziološke ili ponašajne značajke. Te značajke se mogu kategorizirati u unimodalne i multimodalne sustave, u kojima prvi imaju nekoliko nedostataka koji smanjuju točnost sustava, poput sličnosti među klasama, varijacija unutar klase, neuniverzalnosti i slično. Unimodalni biometrijski sustavi vrše provjeru posmatrajući samo jednu ulaznu osobinu, primjerice otisak prsta. Ovi sustavi nisu potpuno pouzdani jer su stope pogrešaka prilično visoke.

Multimodalni biometrijski sustav se može definirati kao sustav koji kombinira ishod dobiven iz više biometrijskih značajki u svrhu identifikacije. Za razliku od unimodalnog biometrijskog sustava koji može rezultirati neuniverzalnošću, multimodalni sustav koristi više značajki koje rezultiraju vrlo preciznim i sigurnim sustavom biometrijske identifikacije [19]. Multimodalna biometrija podrazumijeva kombiniranje nekoliko prethodno navedenih biometrijskih metoda, a ukoliko se koristi veći broj metoda, može se izgraditi jedan sigurni informacijski sustav. Koristi se u graničnim prijelazima za kontrolu ulaska ili izlaska, za kontrolu pristupa nekom prostoru, civilnoj identifikaciji, mrežnoj sigurnosti itd. Osim toga, koristi se i ukoliko iz izvornih dokumenata i zapisa nije moguće dobiti dovoljan broj podataka kojima bi se opisala neka osoba [4].

Uvijek postoji mogućnost zloupotrebe identiteta, stoga se preporučuje kombinacija standardnih sigurnosnih mehanizama i biometrijskih metoda. Jedan od primjera je lažni predložak otiska prstiju. Ukoliko se koristi samo jedna tehnika, npr. prepoznavanje otiska prsta, moguća je situacija u kojoj treća osoba posjeduje lažni otisak prsta s kojim obavlja autentikaciju u ime neke osobe. Dok npr. korištenjem metode verifikacije lica ili raspoznavanjem rožnice i provjerom rasporeda vena postoji veća mogućnost utvrđivanja identiteta ili razotkrivanja krađe identiteta.

5. POUZDANOST I PRECIZNOST BIOMETRIJSKIH SUSTAVA

Razvojem tehnologije raste i potreba za sigurnijim okruženjem, pouzdanim sustavima za osiguranje osoba i imovine. Identifikacija osobe je značajan čimbenik pri postizanju sigurnosti. Provjera identiteta pomoću zaporki, pinova, potpisa i slično polako zastarijeva te njeno mjesto preuzima biometrija kao sve češći i sigurniji oblik autentikacije. Biometrijski sustavi identifikacije su daleko više pouzdani nego tradicionalne tehnologije prepoznavanja koje se temelje na znanju korisnika (PIN, lozinka) ili na onome što korisnik fizički posjeduje (ključ, kartica). Razlog tome su česta gubljenja, zaboravljanja, dijeljenja i kopiranja lozinki, ključeva, kartica i slično. S druge strane, biometrija ne može biti izgubljena te ju je puno teže dijeliti ili kopirati.

Svi korisnici sustava imaju relativno jednak stupanj sigurnosti i jedan račun nije lakše probiti nego bilo koji drugi. Svakako treba uzeti u obzir da i navedeni biometrijski sustavi imaju svoje nedostatke, slabosti i ograničenja te je zbog toga vrlo važno voditi računa o pouzdanosti prilikom odabira biometrijskih sustava identifikacije. Pouzdanost predstavlja sposobnost funkcionalne jedinice sustava za izvršavanje određene funkcije i rad sustava bez otkaza, što čini pouzdanost jednim od ključnih elemenata kada se radi o kvaliteti izvedbe biometrijskog sustava [20].

Preciznost biometrijskih sustava identifikacije ovisi o opsegu i tipu podataka koji se uzimaju, kvaliteti opreme potrebne za analizu biometrijskih uzoraka, ali i stanja ulaznog biometrijskog podatka. Danas nijedan biometrijski sustav identifikacije nije u potpunosti precizan. Biometrijske značajke uzete od iste osobe mogu se razlikovati ovisno o uvjetima i vremenu uzimanja pa se ne može očekivati njihova apsolutna podudarnost. Što je veći stupanj podudaranja, to je sustav sigurniji da dva biometrijska uzorka potječu od iste osobe. Preciznost biometrijskih sustava se mjeri kroz tri osnovna pokazatelja: mjera u kojoj su biometrijski podaci jedne osobe povezani s biometrijskim podacima druge osobe, mjera nepriznavanja trenutnih biometrijskih podataka osobe s prethodno uzetim podacima te osobe i mjera nemogućnosti preciznog određivanja rezultata zbog loše kvalitete ulaznih podataka [21].

Prije korištenja biometrijskih sustava identifikacije potrebno je detaljno proučiti njihove karakteristike, izvedbe i ograničenja. Prilikom korištenja biometrijskih sustava mogu se pojaviti i sljedeće greške: pogrešno prihvaćanje i pogrešno odbijanje. Pogrešno prihvaćanje predstavlja situaciju u kojoj sustav prihvaća lažnog korisnika kao odgovarajuću

osobu, imajući u vidu da je u bazi podataka pronašao biometrijske podatke slične ulaznim podacima. Ova greška se najčešće pojavljuje u slučaju velikog stupnja sličnosti između biometrijskih karakteristika različitih pojedinaca. Pogrešno odbijanje predstavlja situaciju u kojoj biometrijski sustav ne prepoznaje odgovarajućeg korisnika zbog nedovoljnog podudaranja ulaznih podataka s onim podacima u bazi te zbog toga odbija identifikaciju. Ova vrsta ograničenja sustava je prihvatljivija od prve jer korisnik može ponoviti postupak identifikacije nekoliko puta [21].

Za bolju analizu utjecaja ovih grešaka na rad sustava potrebno je izračunati odnos između broja pogrešnih prihvaćanja i broja neovlaštenih pristupa, odnosno postotak pogrešnog prihvaćanja (*FAR – False Acceptance Rate*). Također je potrebno pronaći vezu između broja pogrešnih odbijanja i broja odobrenih pristupa, odnosno postotak pogrešnog odbijanja (*FRR – False Rejection Rate*). Prihvatljive vrijednosti za *FAR* i *FRR* ovise o sigurnosnom pragu sustava. Za sustave koji zahtijevaju višu razinu sigurnosti, sustav će imati strože mjere usporedbi trenutno unesenih biometrijskih podataka s podacima u bazi podataka. Na taj način će se smanjiti neusklađenosti, ali će proporcionalno povećati broj pogrešnih odbijanja. Može se zaključiti da su *FAR* i *FRR* obrnuto proporcionalne funkcije ovisno o razini sigurnosti sustava, koja ovisi o namjeni biometrijskog sustava i predstavlja kompromis između upotrebljivosti i sigurnosti rada. Osim ovih grešaka, pojavljuju se još neka ograničenja koja otežavaju primjenu biometrijskih sustava, poput skupe opreme, nedovoljne testiranosti uređaja u praksi jer je tehnologija još uvijek relativno nova i nepouzdanosti pojedinih sustava. Pojavljuje se i pitanje privatnosti jer postoje protivnici biometrijskih sustava koji smatraju da se takvim sustavima zadire u privatnost korisnika [21].

5.1. Zaštita privatnosti

Privatnost je sposobnost samostalnog vođenja života i kontroliranje pristupa svojim osobnim podacima. Budući da se biometrija i biometrijski sustavi danas koriste u svim sferama života npr. u medicini, financijama, osiguranjima, forenzici te osobnim dokumentima pojedinaca kao što je putovnica, javlja se problem zaštite privatnosti.

Kod biometrije se javljaju tri glavna problema privatnosti. Prvi problem je taj što su biometrijske karakteristike biološkog podrijetla te bi ljudi koji prikupljaju te podatke mogli prikupiti i dodatne osobne podatke iz skeniranih biometrijskih mjerenja. Izvedene medicinske informacije kao npr. deformirani prsti koji mogu biti povezani s određenim genskim poremećajima, često postaju osnova za diskriminaciju. Drugi problem privatnosti je što su

neke metode biometrijske identifikacije dovoljno jake da omogućuju i neželjenu identifikaciju. Na primjer, osobe koje iz sigurnosnih razloga imaju pseudonime, dakle drugo ili tajno ime, mogu biti identificirane prema svom otisku prsta. Treći problem prihvatnosti je što biometrijske karakteristike nisu tajne te je često moguće dobiti biometrijski uzorak osobe bez njenog znanja, dakle osoba ne može biti anonimna [22]. Kako bi se dobila što veća privatnost pojedinca, biometrijski sustavi se ograničavaju na prikupljanje podataka, svrha prikupljanja mora biti definirana te se dobiveni podaci mogu koristiti samo u svrhe za koje su i predviđeni.

Za zaštitu podataka su predlagane razne sigurnosne mjere i strategije kako bi se biometrijski podaci sigurno pohranili u bazu podataka u takvom obliku da ih je gotovo nemoguće dobiti u originalu i kako bi se podaci zaštitili u slučaju da baza više nije sigurna. Koristi se i opozvana biometrija i obnovljivost te kripto-biometrija. Opozvana biometrija ima cilj zaštite podataka nakon krađe, a funkcionira sastavljanjem neupotrebljivih navoda na biometrijski predložak s čime se podiže razina privatnosti. Kripto-biometrija je jedna od najpoznatijih tehnika za zaštitu biometrijskih podataka koja se bazira na ključevima, a koristi kriptografske algoritme za šifriranje i dešifriranje. PIN, lozinke i alfanumeričke veze će biti potvrđene samo ako je točan biometrijski uzorak, koji se nakon svakog završenog procesa uništava. Prednosti ove metode su manje zadržavanje biometrijske slike ili pohranjenog predloška, mogućnost korištenja anonimnih modela baze podataka te veća usklađenost sa zakonima o privatnosti. No, nedostaci kripto-biometrije su nizak postotak točnosti za korištene algoritme i postojanje opasnosti od povećanih napada na biometrijski predložak ili sam komunikacijskih kanal [23].

6. ZAKLJUČAK

Primjena biometrije i biometrijskih metoda identifikacije dobiva sve više na važnosti zbog razvijenijih sustava identifikacije koji nude kvalitetnije i pouzdanije identificiranje. Automatizirani sustavi koji prepoznaju identitet osobe na osnovu fizičkih ili ponašajnih karakteristika već su odavno postali dio naše svakodnevnice.

Biometrijske metode identifikacije su pronašle primjenu u mnogim poljima i pokazale svoje ogromne prednosti. Svakodnevno smo primorani koristiti zaporke, pinove i lozinke, bilo da se radi o prijavama na društvene mreže ili pak na neke ozbiljnije sustave. Nedostatak identifikacije pomoću zaporki je mogućnost gubljenja, zaboravljanja ili zlouporabe istih od strane napadača. Upravo tu nastupa biometrija, koja ljudima omogućuje pristup određenoj mreži ili sustavu, tj. identificiranju pomoću svojih fizičkih ili ponašajnih karakteristika. Biometrija omogućuje identificiranje pomoću različitih metoda, a najbolji rezultati se dobivaju kombiniranjem različitih metoda, odnosno multimodalnom biometrijom.

Ovaj način identifikacije je još uvijek relativno mlad, ali pronalazi svoju primjenu u mnogim sustavima. Iako osigurava privatnost, pouzdanost i zaštitu identiteta korisnika, biometrija ima i nekoliko nedostataka. Najčešći su skupa oprema, nemogućnost unosa podataka u baze zbog veličine datoteka i mogućnost lažne autentikacije.

Unatoč nedostacima, progresivna digitalizacija društva, čiji smo dio, daje poticaj ljudima za razvoj što savršenije metode identifikacije. Od žigosanja i sakaćenja, do suvremenih sofisticiranih načina prepoznavanja humanih karakteristika, prošlo je dosta vremena. Kroz tu evoluciju, čovjek je još jednom pokazao vidljivi kognitivni napredak o kojemu će ovisiti kako će digitalna budućnost izgledati.

LITERATURA

- [1] Altaras Penda, Ivor. Identitet kao osobno pitanje. // Revija za sociologiju 36, 1-2(2005). URL: <https://hrcak.srce.hr/13684>
- [2] Radmilović, Želimir. Biometrijska identifikacija. // Policija i sigurnost 17, 3-4 (2009). URL: <https://hrcak.srce.hr/79284>
- [3] Dimić, Marina. Biometrijski sustavi identifikacije. Završni rad. Filozofski fakultet Sveučilišta u Osijeku. 2016. URL: <https://zir.nsk.hr/islandora/object/ffos:2344/preview>
- [4] Biometrija. URL: <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-167.pdf>
- [5] Boban, Marija; Perišić, Mirjana. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. // Zbornik radova Veleučilišta u Šibeniku / uredio Dragan Zlatović. Šibenik: Veleučilište u Šibeniku, 2015. URL: <http://hrcak.srce.hr/142285>
- [6] Marinović, Dunja; Čoklo, Miran; Njirić, Sanja; Mužić, Vedrana. Personal Identification by Eyes. // Collegium antropologicum 35, 2 (2011). URL: <https://hrcak.srce.hr/file/107598>
- [7] Tomić, Dragan. Biometrijska metoda skeniranja lica. // InfoTeh-Jahorina 11 (2012). URL: <https://infotech.etf.ues.rs.ba/zbornik/2012/radovi/STS/STS-28.pdf>
- [8] Šokec, Tajana. Prepoznavanje lica primjenom SVD dekompozicije. Diplomski rad. Fakultet organizacije i informatike u Zagrebu. 2019. URL: <https://urn.nsk.hr/urn:nbn:hr:211:352891>
- [9] Hrastinski, Davor. Korištenje geometrije dlana za identifikaciju osoba. Završni rad. Fakultet organizacije i informatike Sveučilišta u Zagrebu. 2018. URL: <https://urn.nsk.hr/urn:nbn:hr:211:885423>
- [10] Galić, Jelena; Brkić Hrvoje; Kaić Zvonimir; Čadež Josip. Postmortalna identifikacija dobi postignuta zubalom. // Acta stomatologica Croatica 29, 3 (1995). URL: <https://hrcak.srce.hr/99254>
- [11] Avon, Sylvie Louise. Forensic odontology: the roles and responsibilities of the dentist. // Journal-Canadian Dental Association 70, 7 (2004). URL: <http://www.cda-adc.ca/jcda/vol-70/issue-7/453.pdf>
- [12] Borković, Goran; Miroslav Vrankić; Viktor Sučić. Usmjereni digitalni filtri za prepoznavanje otisaka prstiju. // Engineering Review 28, 1 (2008). URL: <https://urn.nsk.hr/urn:nbn:hr:190:980941>

- [13] Leksikografski zavod Miroslav Krleža. Hrvatska enciklopedija, mrežno izdanje. 2021. URL: <https://www.enciklopedija.hr/>
- [14] Kovač, Zlatko. Prepoznavanje osobe u forenzici na temelju glasa. // Policijska i sigurnost 21, 2 (2012). URL: <https://hrcak.srce.hr/87241>
- [15] Plamondon, Rejean; Srihari, Sargur N. Online and off-line handwriting recognition: a comprehensive survey. // IEEE Transactions on pattern analysis and machine intelligence 22, 1 (2000). URL: <http://ivizlab.sfu.ca/arya/Papers/IEEE/PAMI/2000/January/Handwriting%20Recognition.pdf>
- [16] Jin, Zhe; Teoh, Andrew Beng Jin; Ong, Thian Song; Tee, Connie. Typing dynamics biometric authentication through fuzzy logic. // International Symposium on Information Technology 3, 2008. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4631978>
- [17] Wang, Liang; Ning, Huazhong; Tan, Tieniu; Hu, Weiming. Fusion of static and dynamic body biometrics for gait recognition. // IEEE Transactions on Circuits and Systems for Video Technology 14, 2 (2004). URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1269749>
- [18] Milosavljević, Mladen; Milosavljević, Dušica; Milosavljević, Sunčica. Forenzička odorologija. // Kriminalističke teme 9, 3-4 (2009). URL: <http://krimteme.fkn.unsa.ba/index.php/kt/article/view/286/293>
- [19] Oloyede, Muhtahir O.; Hancke, Gerhard P. Unimodal and Multimodal Biometric Sensing Systems: A Review. // IEEE Access 4. 2016. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7580649>
- [20] Ćosić, Zoran. Metoda evaluacije pouzdanosti biometrijskih sustava. Doktorski rad. Fakultet organizacije i informatike Sveučilišta u Zagrebu. 2015. URL: <https://urn.nsk.hr/urn:nbn:hr:211:269147>
- [21] Paunović, Saša; Starčević, Dušan. Biometrijski sistemi za utvrđivanje identiteta. // Primena multimodalne biometrije u menadžmentu identiteta. URL: <http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/081.pdf>
- [22] Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf

- [23] Konjevod, Mihaela. Biometrija i zaštita privatnosti. Završni rad. Filozofski fakultet Sveučilišta u Osijeku. 2016. URL: <https://urn.nsk.hr/urn:nbn:hr:142:787558>
- [24] Jojić, Jovana; Babić, Zdenka; Đurović, Željko. Klasifikacija i prepoznavanje otisaka prstiju. // Infoteh-Jahorina 13, 2014. URL: <http://www.advancedsourcecode.com/RSS-2-7.pdf>
- [25] Joksović, Maja; Minović Miroslav. Primena rešenja otvorenog koda u prepoznavanju osobe putem rukopisa. // InfoM - časopis za informacijsku tehnologiju i multimedijske sustave 42, 2012. URL: <https://infom.fon.bg.ac.rs/index.php/infom/article/view/1051/1023>
- [26] Khudhur, Saja Dheyaa.; Croock, Muayad Sadik. Biometrics System based Human Identification using STR DNA Marker. // International Journal of Computer Applications 138, 2016. URL: https://www.researchgate.net/publication/298801578_Biometrics_System_based_Human_Identification_using_STR_DNA_Marker
- [27] Kolar-Gregorić, Tatjana. Kriminalistička identifikacija osoba // Krimarak 9, Zagreb: MUP RH, 2002.
- [28] Peroš, Jasminka; Mršić, Gordan; Škavić, Nevenka. Uvođenje biometrije u putne isprave. // Policija i sigurnost 21, 2 (2012). URL: <https://hrcak.srce.hr/87239>

SAŽETAK

Razvojem tehnologije i društva raste potreba za što preciznijim i pouzdanijim načinom identifikacije. Biometrija predstavlja skup automatiziranih metoda koje služe u svrhu identificiranja. Zastupljena je u različitim znanstvenim područjima i danas je gotovo nezaobilazna. U radu su definirani identitet i identifikacija te su opisane metode provođenja identifikacije kroz povijest. Pojašnjen je pojam biometrije kao znanosti i opisana potreba današnjih informacijskih sustava za sigurnijim i preciznijim načinima identifikacije. Analizirane su metode biometrijske identifikacije, pri čemu se posebno fokusiralo na fizičke i ponašajne metode. U radu su detaljno obrađene metode navedenih vrsta identifikacije i opisane njihove karakteristike obzirom na način djelovanja, provođenja i primjene. Također su navedene prednosti i mane biometrijskih metoda identifikacije. Definiran je i pojam unimodalnog, odnosno multimodalnog biometrijskog sustava i način kombiniranja više biometrijskih značajki u takvom sustavu. Osim navedenog, u radu je prikazana važnost i potreba za što većom pouzdanosti i preciznosti biometrijskih sustava. Na kraju se osvrće na moguće greške sustava i probleme kod zaštite privatnosti podataka.

Ključne riječi: *identifikacija, biometrija, biometrijske metode identifikacije, identitet, biometrijski sustavi*

SUMMARY

With the development of technology and society, the need for the most accurate and reliable way of identification is growing. Biometrics is a set of automated methods used for identification. It is represented in various scientific fields and is almost unavoidable today. The paper defines identity and identification and describes methods of performing identification through history. The notion of biometrics as a science is explained and the need of today's information systems for more secure and accurate identification methods is described. Biometric identification methods have been analyzed, with particular focus on physical and behavioral methods. The paper deals in detail with the methods of these identification types and describes their characteristics in terms of operation, implementation and application. The advantages and disadvantages of biometric identification methods are also listed. The concept of unimodal or multimodal biometric system and the way of combining several biometric features in such a system are also defined. In addition, the paper presents the importance and need for greater reliability and accuracy of biometric systems. Finally, it addresses potential system failures and privacy issues.

Keywords: *identification, biometrics, biometric identification methods, identity, biometric systems*