Biometrijska identifikacija putnika u zaštiti zračnog prometa

Prlenda, Matej

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Matej Prlenda

BIOMETRIJSKA IDENTIFIKACIJA PUTNIKA U ZAŠTITI ZRAČNOG PROMETA

ZAVRŠNI RAD

Zagreb, 2018.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 16. ožujka 2018.

Zavod: **Zavod za zračni promet**
Predmet: **Zaštita u zračnom prometu**

ZAVRŠNI ZADATAK br. 4487

Pristupnik: **Matej Prlenda (0135242020)**
Studij: Promet
Smjer: Zračni promet

Zadatak: **Biometrijska identifikacija putnika u zaštiti zračnog prometa**

Opis zadatka:

U uvodnim postavkama potrebno je opisati predmet istraživanja, objasniti svrhu i cilj istraživanja te dati kratak pregled strukture završnog rada. Protumačiti povijest biometrijske identifikacije osoba. Objasniti principe rada biometrijskih tehnika i opisati vrste metoda i tehnika koje se koriste u svrhu prepoznavanja fizičkih i ponašajnih karakteristika osoba. Preispitati i raspraviti etička pitanja povezana s primjenom biometrijskih metoda prepoznavanja osoba te razinu sigurnosti dobivenih podataka. Specificirati i analizirati zakonske okvire primjene biometrije. Izdvojiti i opisati primjere upotrebe biometrijskih metoda u zračnim lukama. Izvesti zaključke i interpretirati dobivene rezultate.

Mentor:

Arijana Modić

Arijana Modić, mag. ing. traff.

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

BIOMETRIJSKA IDENTIFIKACIJA PUTNIKA U ZAŠTITI ZRAČNOG PROMETA

BIOMETRIC PASSENGER IDENTIFICATION IN AIR TRAFFIC SECURITY

MENTOR: Arijana Modić, mag.ing.traff.

STUDENT: Matej Prlenda

JMBAG: 0135242020

Zagreb, rujan 2018.

SAŽETAK

Suvremena biometrijska identifikacija temelji se na prepoznavanju određenih biometrijskih značajki te uspoređivanju s pohranjenim uzorkom u podatkovnom obliku unutar baze podatka određenog sustava. Biometrijska identifikacija sve se više primjenjuje u zaštiti zračnog prometa, pri čemu je nužno osigurati sigurnost informacijskih sustava unutar koji se biometrijski podaci pohranjuju, kao i prihvatljivost biometrijskih metoda korisnicima. U radu je dan pregled dostupnih biometrijskih tehnika, objašnjeni njihovi principi rada te prednosti i nedostaci kao i najčešći tipovi pogrešaka biometrijskih sustava. Prikazani su načini korištenja biometrije u zaštiti zračnog prometa te zakonski okviri primjene biometrije u SAD-u i Europi. Korištenje biometrijskih metoda značajno ubrzava zaštitne procedure u zračnim lukama, smanjuje mogućnosti krađe identiteta, a omogućuje i pravovremeno prepoznavanje sumnjivih putnika koji se zatim mogu podvrgnuti dodatnih kontrolama.

Ključne riječi: biometrijska identifikacija; zaštita zračnog prometa; biometrijske metode; sigurnost

SUMMARY

Modern biometric identification is based on recognizing of certain biometric characteristics which are then compared to previously stored sample in digital form in the system's database. Application of biometric identification in air traffic security is increasing, whereat it is necessary to ensure the safety of information systems in which biometric data is stored, as well as acceptability of biometric methods to users. A review of available biometric techniques, along with their working principles and advantages and disadvantages and most common types of errors is given in this paper. Modes in which biometrics is used in air traffic security are shown and legal framework for use of biometrics in USA and Europe is discussed. Utilization of biometric methods speeds up security procedures at airports significantly, lowers the possibility for identity theft and enables recognition of suspects among passengers that can then be subjected to additional checks.

Key words: biometric identification; air traffic security; biometric methods; safety

SADRŽAJ

1. UVOD

Riječ biometrija dolazi od starogrčkih riječi *bios* = „život“ i *metron* = „mjera“. Biometrija se definira kao znanost o postupcima za jedinstveno prepoznavanje ljudi, na temelju uspoređivanja jednog ili više urođenih tjelesnih obilježja, ili obilježja čovjekovog ponašanja, odnosno biometrija predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi temeljeno na jednoj ili većem broju njihovih fizičkih i ponašajnih karakteristika.

Razvojem tehnologije, računalne biometrijske metode počinju se naveliko koristiti. Suvremena biometrijska identifikacija temelji se na prepoznavanju određenih biometrijskih značajki te uspoređivanjem s pohranjenim uzorkom u podatkovnom obliku unutar baze podatka određenog sustava. Biometrijska identifikacija svoju je primjenu pronašla i u zaštiti zračnog prometa.

Cilj je ovog završnog rada dati pregled dostupnih biometrijskih tehnika, objasniti njihove principe rada i proučiti na koje je sve načine biometrija primijenjena u zaštiti zračnog prometa. Rad je podijeljen u 8 cjelina:

1. Uvod
2. Povijest biometrije
3. Principi rada biometrijskih tehnika
4. Vrste biometrijskih tehnika
5. Sigurnost podataka i etička pitanja vezana uz biometrijske metode
6. Zakonski okviri primjene biometrije
7. Primjeri korištenja biometrijskih metoda na zračnim lukama
8. Zaključak

U drugom poglavlju dan je povijesni pregled razvoja biometrije.

U trećem poglavlju objašnjeni su glavni pojmovi vezani uz principe rada biometrijskih tehnika, kao što su digitalizacija, upisivanja korisnika u sustav, identifikacija, verifikacija, multimodalna biometrija te su navedeni i objašnjeni najčešći tipovi pogrešaka u radu biometrijskih sustava.

Četvrto poglavlje obuhvaća vrste biometrijskih tehnika, načine njihova korištenja te prednosti i nedostatke njihove uporabe.

U petom poglavlju razmatra se sigurnost informacijskih sustava unutar kojih se biometrijski podaci pohranjuju te prihvatljivost korištenja biometrije korisnicima.

U šestom poglavlju dan je osvrt na zakonske okvire primjene biometrije, točnije *General Data Protection Regulation (GDPR) for European Member States* i *US legal landscape for biometric data protection*.

Sedmo poglavlje obuhvaća primjere primjene biometrijskih metoda u zaštiti zračnog prometa na zračnim lukama.

U posljednjem je poglavlju, na temelju interpretiranih podataka, izveden zaključak.

2. POVIJEST BIOMETRIJSKE IDENTIFIKACIJE

Automatizirani biometrijski sustavi postali su dostupni tek unazad nekoliko desetljeća zbog značajnih napredaka koji su nastali u području procesiranja podataka korištenjem računala. No, mnoge od tih novih automatiziranih tehnologija zasnivaju se na idejama koje su nastale stoljećima, pa čak i tisućljećima prije današnjeg modernog doba.

2.1. Biometrijski sustavi prije 20. stoljeća

Jedan od najstarijih i najjednostavnijih primjera karakteristika koje se koriste za prepoznavanje je lice. Od početaka civilizacije, ljudi su prema licu raspoznavali poznate od nepoznatih osoba. Također, ljudi prepoznaju jedni druge prema tonu glasa i načinu govorenja i takvi načini djelomično nesvjesnog prepoznavanja drugih osoba događaju se svakodnevno.

Još su stari Egipćani vršili različita mjerenja tijela za identifikaciju, dok se u Babilonu otisak prsta na pločici od gline koristio za poslovne transakcije. Kineski trgovci su u 14. stoljeću uz pomoć tinte i papira radili otiske dlanova i stopala u svrhu razlikovanja male djece.

U Europi je francuski policijski službenik i znanstvenik Alphonse Bertillon prvi razvio antropometrijski sustav kasnije nazvan Bertillonageov sustav koji je našao široku primjenu u identifikaciji kriminalaca. Sustav se temeljio na preciznom mjerenju dimenzija tijela, dužine i širine glave te bilježenju osobnih obilježja osobe kao što su razne tetovaže, ožiljci i deformacije tijela. Bertillonageov sustav bio je u upotrebi sve dok njegovi propusti u radu nisu postali očigledni. Problemi koji su se javljali, najčešće su bili vezani uz neujednačene postupke mjerenja, nedovoljnu preciznost mjerenja i veliku promjenjivost ljudskog tijela tijekom godina. Sustav je sužavao broj počinitelja, ali nije davao točan rezultat.

Drugi sustav koji se razvio u 19. stoljeću bio je zasnovan na upotrebi otiska prsta. Prvi takav robustan sustav koji je obuhvaćao klasifikaciju i pohranu prikupljenih podataka razvijen je u Indiji za policijske potrebe. Sustav je nazvan Henryev sustav prema imenu glavnog inspektora policije u Bengalu, a varijacije tog sustava i danas su u upotrebi [1].

2.2. Razvoj biometrije kroz 20. stoljeće do danas

Šezdesetih godina 20. stoljeća nastao je prvi polu-automatizirani sustav temeljen na prepoznavanju lica. Navedeni sustav koristio je fotografije lica na kojima su se mjerile udaljenosti i omjeri veličina u odnosu na zajedničke referentne točke, a rezultati mjerenja uspoređivani su sa referentnim podacima. U to je vrijeme razvijen i prvi model temeljen na akustičnoj govornoj produkciji. Godine 1965., Sjevernoameričko zrakoplovstvo (*North American Aviation*) razvilo je prvi sustav koji se temeljio na prepoznavanju karakteristika potpisa.

Sedamdesetih godina 20. stoljeća prvi sustav temeljen na geometriji šake postao je komercijalno dostupan, a istih godina je i FBI razvio algoritme za poboljšanje biometrijskog sustava temeljenog na otiscima prsta. Godine 1976. razvijen je prvi prototip sustava koji koristi prepoznavanje glasa, a koji je testiran u Američkim zračnim snagama (*US Air Force*).

U osamdesetim godinama prošlog stoljeća odobren je patent za koncept upotrebe šarenice oka za identifikaciju te je razvijen algoritam za automatizirano prepoznavanja ljudskih šarenica.

Procvat pravih biometrijskih sustava dogodio se u drugoj polovici 20. stoljeća, usporedno s razvojem kompjuterskih sustava. Najviše razvojnih aktivnosti dogodilo se u 90.-im godinama prošlog stoljeća što je rezultiralo svakodnevnom upotrebom biometrije već u ranim 2000.-im godinama.

Devedesetih godina započela je s radom Tehnologija prepoznavanja lica (*FacE REcogntion Technology* - FERET) te je time sustav temeljen na prepoznavanju lica postao komercijalno dostupan. Godine 1994. implementiran je biometrijski sustav pomoću kojeg su putnici mogli zaobići čekanje na prolazak na imigracijskim šalterima na odabranim zračnim lukama u SAD-u, tj. Ubrzani servisni sustav za imigraciju i naturalizaciju putnika (*Immigration and Naturalization Service Passenger Accelerated Service System* - INSPASS). Autorizirani putnici dobili su karticu u kojoj su bile kodirani informacije o njihovoj geometriji šake. Umjesto prijema kod imigracijskog inspektora, INSPASS putnici pokazali bi svoje kartice s kodiranim informacijama i svoje ruke na biometrijskom uređaju. Nakon verifikacije identiteta, putnici su mogli nastaviti s carinskim pregledom i tako je njihov ulazak u SAD bio ubrzan i povećana je efikasnost rada.

West Virginia University je 2000. godine osnovao program za dobivanje diplome u području biometrije čime je dokazano da je važnost biometrije prepoznata, a tako i potreba da se u tom području specijalizirano educira buduće stručnjake. Godine 2002. Međunarodna organizacija za standardizaciju (*The International Organization for Standardization* - ISO) uspostavila je ISO/IEC JTC1 podkomisiju 37 (JTC1 /SC37) kako bi podržala standardizaciju generičkih biometrijskih tehnologija. Navedena podkomisija razvija standarde koji promiču interopreabilnost i izmjenu podataka između različitih sustava. Organizacija međunarodnog civilnog zrakoplovstva (*The International Civil Aviation Organization* - ICAO) 2003. godine usvojila je globalni, harmonizirani program za integraciju biometrijskih identifikacijskih podataka u putovnice i druge putničke dokumente koji se mogu strojno očitavati. Prepoznavanje lica odabrano je kao tehnika za globalno biometrijsko strojno prepoznavanje identiteta. Godine 2003. osnovan je Europski biometrijski forum pri Europskoj komisiji koji potiče suradnju, podržava rad i osnažuje nacionalna tijela koja se bave biometrijom diljem Europe.

Dalje je u 2000.-ima nastavljena primjena biometrijskih sustava – s radom je započela Tehnologija prikaza posjetiteljskog i imigrantskog statusa SAD-a (*The United States Visitor and*

Immigrant Status Indication Technology - US-VISIT) program čiji je cilj povećanje sigurnosti i kontrole ulaza stranaca u SAD, a temelji se na kombinaciji biometrijskih tehnika. Također, razvijene su baze biometrijskih podataka, unaprijeđeni postojeći sustavi, a 2013. Apple je prvi primijenio biometrijske sustave u svojim mobilnim telefonima te drugim uređajima i aplikacijama razvijenima u toj tvrtki čime je moderna biometrija postala dostupna širokoj populaciji [1].

3. PRINCIPI RADA BIOMETRIJSKIH TEHNIKA

3.1. Biometrijska karakteristika

Prema ISO/IEC TR 24741:2018, biometrijska tehnika je automatizirano prepoznavanje individualaca bazirano na njihovim biološkim i ponašajnim karakteristikama.Pojam biometrijska karakteristika stoga označava biološku ili ponašajnu karakteristiku osobe od koje se mogu izdvojiti razlikovni elementi u svrhu biometrijskog prepoznavanja, pri čemu je te elemente moguće ponovljivo mjeriti[2].

Idealna biometrijska karakteristika zadovoljavala bi sljedeće uvjete:

- univerzalnost (svaka osoba posjeduje tu karakteristiku),
- specifičnost (karakteristika je jedinstvena za određenog korisnika),
- postojanost (karakteristika mora biti stalna tijekom vremena kao, npr. šarenica oka, dok se lice osobe ili glas mijenjaju starenjem osobe),
- mjerljivost(karakteristika se može lako izmjeriti i kvantitativno izraziti, npr.potpisi i prepoznavanje lica)
- prihvatljivost (ispitivanoj osobi je prihvatljiv način biometrijskog prepoznavanja)[2], [3].

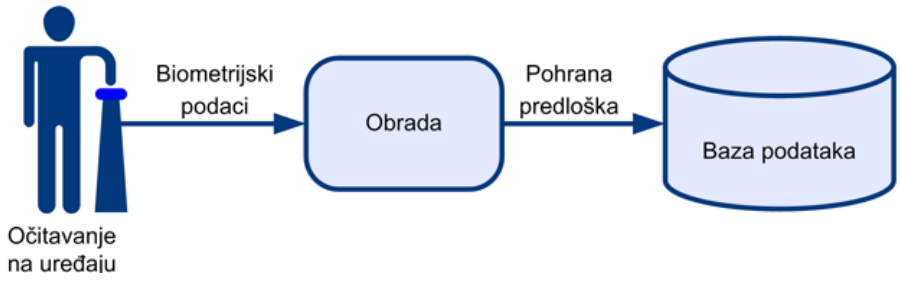
Nažalost, ni jedna biometrijska karakteristika nema sve navedene osobine – u nekim karakteristikama postoje značajne sličnosti kod različitih osoba, biometrijske karakteristike mogu se promijeniti s vremenom, prihvatljivost je ovisna o pojedincu koji je podložen biometrijskoj identifikaciji itd. Pri razvoju biometrijske tehnike potrebno je stoga napraviti određene kompromise i razviti robusne sisteme koji mogu nadvladati varijabilnost ljudi [2], [3].

3.2. Temeljni procesi u biometrijskoj identifikaciji

Kada se odaberu temeljne biometrijske karakteristike koje će se koristiti u biometrijskoj metodi, osnovni elementi za primjenu modernih računalnih biometrijskih metoda su digitalizacija, tj. pretvaranje analognog u digitalne signale te umjetna inteligencija.

Glavni segment u procesu prepoznavanja uzoraka je **digitalizacija**. Za potrebe računalne obrade podatke dobivene skeniranjem i sl. potrebno je prevesti u digitalni format s kojim računalo može raditi. To je proces u kojem se analogni signal pretvara u digitalni te prepoznaje programskom opremom. Što je kvalitetnija oprema, to su veće šanse za prepoznavanje uzorka. Analogni signal se pretvara u digitalni korištenjem elektroničkog digitalnog audio-video konvertera (*digital audio-video converter* - DAC) [4]. Pri prvom susretu osobe s biometrijskim sustavom, vrši se registracija njegovih biometrijskih podataka (eng. *enrollment*) i upis u bazu podataka (prikaz procesa na slici 1.). Najprije se prikupljaju biometrijski podatci pomoću uređaja

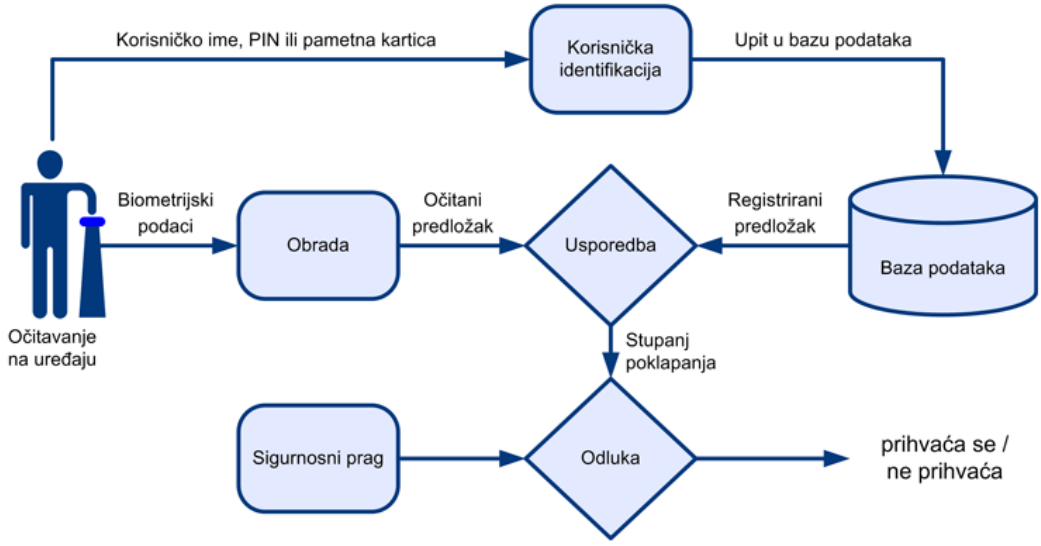
za očitavanje. Taj prvi korak uzimanja uzorka ključan je za daljnju autentifikaciju zbog čega je potrebno posvetiti osobitu pozornost kvaliteti uzetog uzorka. Zatim se u drugoj fazi analiziraju dobiveni neobrađeni podaci na način da se iz njih izdvajaju podaci koji karakteriziraju korisnika pomoću specifičnog algoritma te im se pripisuje brojčana vrijednost. Izdvojeni podaci čine biometrijski predložak (eng. *biometric template*). Predlošci se potom spremaju, što se može raditi na dva načina: decentralizirano (na čip karticu ili računalo) i centralizirano (u bazu podataka, odnosno arhivu predložaka).



Slika 1. Registracija biometrijskih podataka

Izvor: [5]

Pri ponovnom susretu korisnika s biometrijskim sustavom, vrše se procesi identifikacije i verifikacije (prikaz na slici 2.)



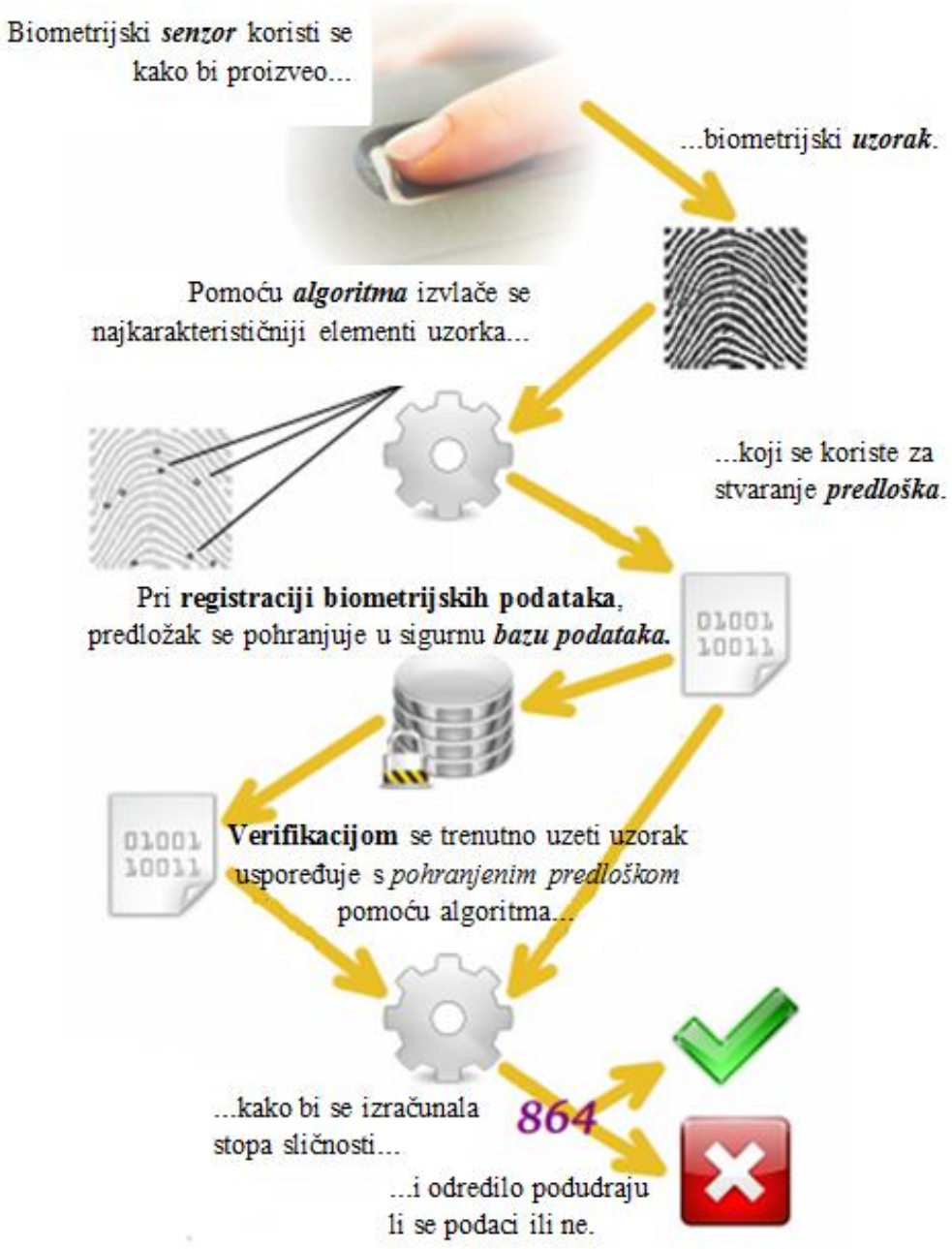
Slika 2. Identifikacija i verifikacija korisnika

Izvor: [5]

Proces **verifikacije** sastoji se od usporedbe upravo očitanih podataka s onima iz korisnikovog predloška. Korisnik mora priložiti identifikacijski podatak pomoću kojeg sustav pronalazi odgovarajući predložak. Taj se podatak može isporučiti u vidu korisničkog imena, PIN-a ili pametne kartice [5]. Sustav za verifikaciju zaprima biometrijski uzorak te temeljem njega kreira probni predložak baziran na algoritmu sustava identifikacije. Nakon toga vrši se usporedba na principu 1:1 gdje sustav uspoređuje probni predložak s prije spremljenim podacima korisnika i traži podudaranje, odnosno računa stopu sličnosti (*s*) – što je stopa sličnosti veća, to sustav s većom sigurnosti tvrdi da se radi o istoj osobi (prikaz na slici 3). Na taj je način onemogućeno da više osoba koristi isti identitet. Verifikacijski biometrijski sigurnosni sustav može sadržavati od nekoliko desetaka, pa sve do nekoliko milijuna registriranih identifikacijskih podataka [6].

Nasuprot tome, **identifikacijski** proces počinje s trenutnim prezentiranjem biometrijske karakteristike na za to predviđenom uređaju, snimanja, procesiranja, izvlačenja potrebnih podataka (najkarakterističnijih elemenata uzorka) pomoću algoritama i generiranja predloška. Ispitivani predložak se nakon toga uspoređuje sa svim referentnim predlošcima u bazi podataka i ponovno se računa stopa sličnosti, kao i u sustavu verifikacije. Ovakav način usporedbe jednog uzorka sa mnogo predložaka pohranjenih u bazi, umjesto verifikacijskog procesa kod kojeg je usporedba po principu 1:1, sprječava da jedna osoba koristi više identiteta.

Osim stope sličnosti, važna je i granična vrijednost, eng. *threshold* (*t*). Biometrijski sustav generira vrijednost *s* i ako je ona veća ili jednaka *t* zaključuje da se pohranjeni predložak i očitani uzorak podudaraju, odnosno da se radi o istoj osobi. Nadalje, ako je dobivena vrijednost *s* manja od *t*, sustav zaključuje da se uzorci ne podudaraju i da potječu od 2 različite osobe [7], [8].



Slika 3. Pojednostavljeni prikaz osnovnih procesa rada biometrijske tehnike koja se temelji na verifikaciji

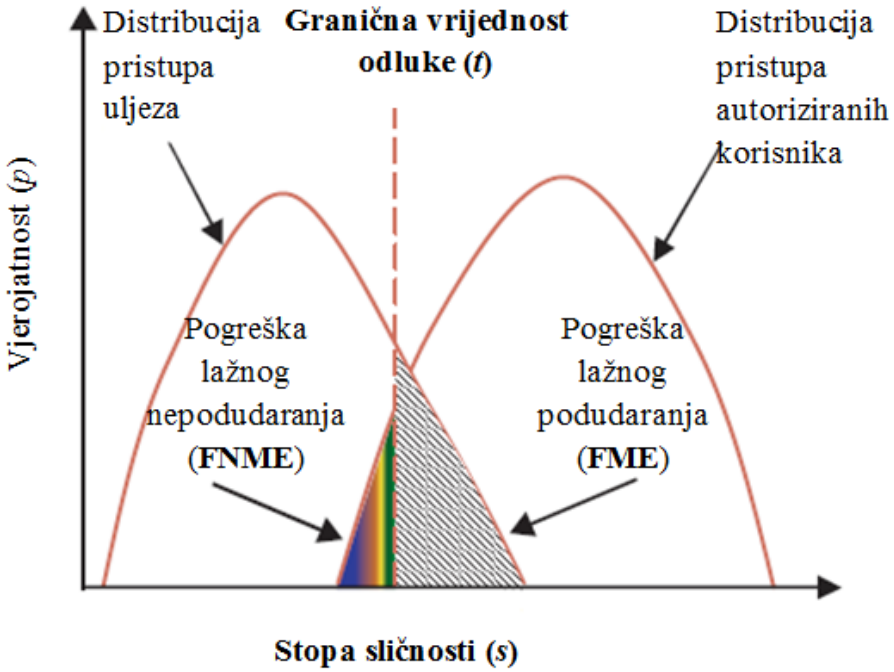
Izvor:[10]

Umjetna inteligencija je dio računalne znanosti koja se bavi zahtjevima za obavljanje poslova iz domene percepcije, shvaćanja i učenja uzoraka. Umjetna inteligencija je dosad objasnila prirodu problema shvaćanja, i postavila osnovne pretpostavke inteligentnih sustava, a trenutno se radi na razvoju kognitivnih modela koji bi trebali objasniti ljudsku kogniciju.

Umjetna inteligencija kao podloga za biometriju je potrebna zbog dijela zvanog „neuronske mreže“ koji se primjenjuje u analizi signala i slika. Teorijsko ishodište i inspiracija neuronskih mreža je u ljudskom mozgu. Cilj je spajanje sposobnosti ljudi da dobro prepoznaju oblike, lica i glasove i sposobnost računala da izvršava numeričke proračune i radi s velikom količinom podataka na osnovu izračunatih proračuna [4].

3.3. Tipovi pogrešaka u radu biometrijskih tehnika

Dva biometrijska uzorka prikupljena od iste osobe (npr. snimka glasa, tj. govora) u različitim vremenskim točkama ne mogu biti identična zbog razlikovanja okolnosti tijekom prikupljanja uzorka (npr. vjetar, pozadinska buka, suho grlo korisnika), promjena u biometrijskoj karakteristici od interesa (npr. promuklost, visoki tonovi govora u stanju uzbuđenosti) i promjenjivoj interakciji između korisnika i senzora (položaj i blizina usta mikrofonu). Posljedično, biometrijski sustavi mogu stvoriti 2 tipa pogrešaka pri verifikaciji. Prvi tip je pogreška lažnog podudaranja (*False Match Error* - FME) koja se događa kada algoritam pogrešno klasificira uljeza kao autoriziranog korisnika. Drugi tip pogreške je pogreška lažnog nepodudaranja (*False Non-match Error* - FNME) koja se događa kada sustav ne prepozna autoriziranog korisnika, odnosno klasificira ga kao uljeza (prikaz na slici 4). Stopa pogrešaka lažnog podudaranja (*False Match Rate* – FMR) je postotak nepodudarajućih parova uzoraka za koje je sustav generirao vrijednost *s* veću ili jednaku *t*, dok je stopa pogrešaka lažnog nepodudaranja (*False Non-match Rate* – FNMR) postotak podudarajućih parova uzoraka za koje je sustav generirao s manju ili jednaku *t*. Redukcija jednog tipa pogrešaka povećava vjerojatnost za drugi tip pogrešaka pa postavljanje granica prihvatljivosti ovisi o zahtjevima i prirodi specifične primjene – niža stopa FNME rezultira u većoj upotrebljivosti, dok je niža stopa FME nužna za primjene u sustavima visoke sigurnosti. Američka Uprava za sigurnost prometa (*Transportation Security Administration* - TSA) kao kvalifikacijske zahtjeve za primjenu biometrijskih tehnika postavila je stopu FME i FNME < 1.0% [8].



Slika 4. Prikaz zastupljenosti FMR i FNMR za danu graničnu vrijednost odluke (t) preko krivulja koje prikazuju pokušaje pristupa biometrijskom sustavu od strane uljeza te od strane autoriziranih korisnika

Izvor:[7]

I druge se pogreške mogu dogoditi u biometrijskim sustavima, kako u modulima koji uključuju verifikaciju, tako i u modulima koji uključuju identifikaciju. Pogreška prikupljanja podataka (*Failure to Acquire* - FTA) događa se kad korisnici nisu u mogućnosti dati upotrebljiv biometrijski uzoraka, ili zbog toga što ne posjeduju biometrijsku karakteristiku od interesa (npr. nijemi ljudi) ili zbog toga što ju nije moguće izmjeriti (npr. zbog jake promuklosti). Pogreška pri registraciji podataka(*Failure to Enroll*- FTE) događa se kad je nemoguće izvući podatke iz prethodno uspješno prikupljene karakteristike, što se događa zbog ograničenja korištene tehnologije.

Kako bi se unaprijedila osobna identifikacija u biometrijskim sustavima, multimodalni pristup u kojem se istovremeno koristi 2 ili više biometrijskih karakteristika, sve je češće u primjeni [8].

3.4. Procjena točnosti rada biometrijskih tehnika i pouzdanosti rezultata dobivenih biometrijskom identifikacijom

Procjena učinkovitosti biometrijske tehnike provodi se izvođenjem velikog broja usporedbi uzoraka dobivenih od autoriziranih korisnika te uzoraka uljeza i analizom dobivenih rezultata podudarnosti. Stope pojavljivanja pogrešaka računaju se kao omjer broja uzoraka uljeza koji su lažno prihvaćeni kao podudarajući (*False Acceptance Rate* - FAR) i broja uzoraka autoriziranih korisnika koji su lažno odbijeni kao nepodudarajući (*False Rejection Rate* - FRR). Kako bi se izbjegle FRR pogreške, biometrijski uređaj treba biti što manje osjetljiv na razne periferne faktore (npr. prljavost prsta u sustavima koji se temelje na prepoznavanju otiska prsta) i biti sposoban snimiti biometrijski predložak visoke kvalitete kako bi se osiguralo slaganje sa sljedećim biometrijskim snimkama. Javljanje FAR pogreški ovisi o više faktora, među kojima su, kao i u slučaju FRR, sposobnost sustava da ispravno snimi biometrijski predložak, da ga ispravno spari s originalnim zapisom pri ponovnom mjerenju, a najvažnije za izbjegavanje FAR pogreški je da je odabrana biometrijska karakteristika što je više moguće jedinstvena za svakog korisnika. U tom pogledu je biometrijska identifikacija pomoću šarenice oka idealna jer je visok stupanj kompleksnosti takvog uzorka pa je stoga i različitost vrlo velika između različitih ljudi [9].

Za usporedbu jednog biometrijskog sustava s drugim koristi se vrijednost FRR, uz uvjet da je razina FAR fiksna, a na isti se način može procijeniti je li neki sustav dovoljno točan za određenu namjenu.

Karakteristike baze podataka imaju veliki utjecaj na postignutu učinkovitost biometrijskog sustava. Upravo zbog tog razloga je nemoguće uspoređivati rezultate dobivene korištenjem različitih baza podataka. Što više prikupljeni uzorci oponašaju ciljane uvjete pri uzimanju uzorka u smislu korištenog senzora (tip i kvaliteta), tipa dobrovoljaca (dob, spol, etnička/rasna pripadnost...) čiji su uzorci pohranjeni u bazi i njihovog tjelesnog stanja, to će pouzdaniji biti rezultati dobiveni biometrijskim mjerenjem [10].

4. VRSTE BIOMETRIJSKIH TEHNIKA

Biometrija se bavi identifikacijom pojedinaca, temeljenoj na njihovim biološkim karakteristikama ili karakteristikama ponašanja. U početku korištenja biometrijskih sustava, prednost je davana fizičkim karakteristikama u odnosu na ponašajne karakteristike. Smatralo se da su fizičke karakteristike pouzdanije od ponašajnih, jer one imaju tendenciju manjih razlika unutar grupa od ponašajnih karakteristika. U nastavku je dan pregled glavnih biometrijske metode temeljenih na fizičkim i ponašajnim karakteristikama.

4.1. Fizičke biometrijske tehnike

Fizička biometrija je dio biometrije koja se bavi uzorkovanjem fizionomije ljudskoga tijela i njegovim jedinstvenim karakteristikama. Temelj fizičke biometrije je ljudska fizička jedinstvenost koja omogućuje raspoznavanje ljudi [4].

4.1.1. Otisak prsta

Za otisak prsta (slika 5) može se reći da je najstarija i najpoznatija korištena metoda autentifikacije. Metodom analize pojedinosti analiziraju se relativni položaji individualnih karakteristika otiska prsta kao što su: završeci grebena, bifurkacije (mjesta na kojima se dvije linije spajaju u jednu), uzorak izbočina i udubljenja na površini jagodice prsta, a nastaje sakupljanjem mrtvih, otvrdnulih stanica, koje se neprekidno u slojevima ljušte sa površine prsta.

Oblik i formacija otiska ovise o prvotnim uvjetima razvoja embrija. Otisci prstiju su jedinstveni za svaki prst osobe, uključujući i jednojajčane blizance.

Otisak prsta u primjeni je jedna od najdostupnijih i najčešće korištenih biometrijskih metoda. Glavni nedostatak je mogućnost korištenja umjetno napravljenih otisaka prstiju neke osobe (pomoću voska, gela i sl.), a nedostaci se nastoje izbjeći korištenjem metode uzimanja otiska više prstiju. Također, najnoviji ultrazvučni čitači trebali bi doskočiti ovome problemu, a radi se i na razvoju uređaja koji uz skeniranje otiska prstiju registriraju i protok krvi.

Postoje tri tehnike za skeniranje otisaka prstiju: optički čitač, silicijski čitač i ultrazvučni čitač.

Optički čitač otiska prsta reagira na promjene u refleksiji svjetla na mjestima gdje papilarni grebeni dodiruju površinu. Optički senzori su relativno jeftini, rade pouzdano i generiraju sliku zadovoljavajuće kvalitete. Njihov glavni nedostatak su prašina i nečistoća koja se nakuplja na dodirnoj površini. Ako se radi o ekstremnoj površinskoj nečistoći ona može poprimiti oblik pravog otiska prsta i uzrokovati pogrešno prihvaćanje. Zato ovakav uređaj ima kratak vijek

trajanja i treba ga redovito održavati. Optički čitač reagira na pritisak i može se lako zavarati korištenjem trodimenzionalnog modela prsta, stoga se u njih često ugrađuje posebni detektor.

Silicijski čitač otiska prsta zasniva se na kapacitivnosti prsta. Sastoji se od mrežne površine malih kapaciteta, gdje je njegova površina jedna, a prst druga ploča. Čitač registrira grebene prsta koji prelaze iznad uređaja zbog većeg kapaciteta od udubljenih dijelova. Ovakvi čitači su mali, jeftini i brzi, a nedostatak im je preosjetljivost kapacitivnosti na vlagu i znoj [11].

Ultrazvučni čitač predstavlja najnoviju tehnologiju, a sastoji se od odašiljača i prijemnika ultrazvučnih valova. Ultrazvučni puls se usmjerava prema prstu kada je prst naslonjen na skener uređaja. Dio ultrazvučnih valova pritom se apsorbira, a dio se odbija ovisno o porama i grebenima otiska prsta te vraća prema senzoru. Senzor detektira mehanički stres koji se koristi za izračun intenziteta povratnog ultrazvučnog pulsa na različitim dijelovima skenera pomoću kojih stvara 3D sliku otiska prsta koja je puno preciznija i pouzdanija od 2D slika [12].

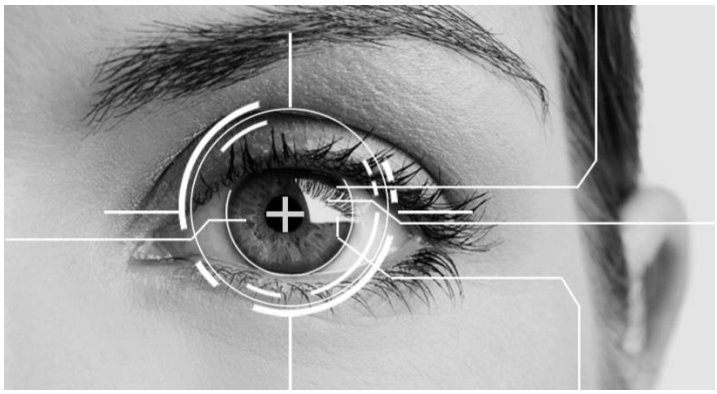
Slika 5. Otisak prsta

Izvor: [3]

4.1.2. Šarenica oka

Šarenica (eng. *iris*) je obojeni dio oka koji okružuje zjenicu, a sastoji se od prstena, brazdi i pjega u različitim bojama, koji čine jedinstveni vremenski nepromjenjiv kompleks boja i šara kod svakog pojedinca. Šarenica je univerzalna, trajna (izgled poprima u najranijem djetinjstvu i ne mijenja se tijekom vremena) ine može se promijeniti bez velikog rizika od gubitka vida pa je zbog toga veoma korisna za identifikaciju. Sustav za identifikaciju na temelju šarenice nije

moguće zavarati lećama, staklenim ili pravim okom odstranjenim s mrtvog čovjeka. Naime, kad je riječ o lećama postoje algoritmi koji registriraju leće, a kod staklenog oka ili oka mrtve osobe nema očekivane kontrakcije ili širenja zjenice pri obasjavanju oka. Ova tehnika identifikacije vrlo je jednostavna i pouzdana, neinvazivna je jer nije potreban fizički kontakt osobe sa skenerom. Može se obaviti i snimanjem šarenice oka s običnom kamerom s udaljenosti i do pola metra. Za pregled baze potrebno je par sekundi. Prepoznavanje osoba skeniranjem šarenice (irisologija) jedna je od najpouzdanijih biometrijskih metoda, ponajviše zbog prirodnih karakteristika šarenice (prikaz na slici 6). Metoda je veoma korisna za potvrdu i utvrđivanje identiteta [13].



Slika 6. Biometrijsko skeniranje šarenice oka

Izvor: [9]

4.1.3. Mrežnica oka

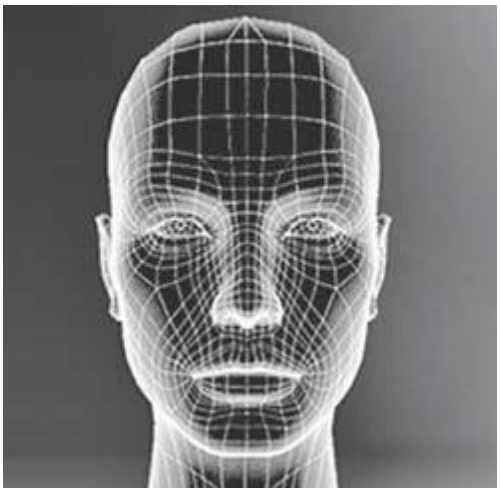
Mrežnica (lat. retina) je unutarnja ovojnica oka. Smještena je na stražnjem dijelu očne jabučice i njezin je najvažniji dio. Sadrži vidne stanice, štapiće i čunjiće koji pomažu u osjetu svjetla i raspoznavanju boja, a povezane su sa živčanim vlaknima koja se udružuju u vidni živac [13]. Jedinstvena je svaku osobu zbog mreže krvnih kapilara kojima je prožeta, ne mijenja se tijekom života osim u slučajevima glaukoma i dijabetesa. Slika mrežnice dobiva na način da se laserska infracrvena svjetlost usmjeri u unutrašnjost oka. Reflektirana svjetlost sadrži podatke o položaju kapilara.

Ova biometrijska metoda daje najveću točnost prepoznavanja, ali je i najskuplja. Skeniranje mrežnice traje 10-15 sekundi. Nedostatak metode je nelagodnost koju izaziva kod korisnika jer zahtijeva prodiranje laserske svjetlosti u oko osobe [11].

4.1.4. Prepoznavanje lica

Izgled lica, poput čela, očiju, usta i nosa uvjetovan je i građom kostura glave, lica, rasporedom muskulature. Na licu je moguće mjeriti i uspoređivati preko 80 obilježja koje se ne mijenjaju tijekom godina, kao što su razmak očiju, širina nosa, dubina očnih udubljenja, jagodice, vilica, brada itd. Navedeni ključni detalji se mjere (najčešće samo njih 20-ak), te se formira numerički digitalni kod koji predstavlja lice u bazi podataka (slika 7).

Postoje dvodimenzionalni i trodimenzionalni algoritmi za prepoznavanje lica. Kada se koriste dvodimenzionalni algoritmi za usporedbu lica, najpoznatije su metode: algoritam svojstvenih lica, metoda kojom se uspoređuje lice osobe s unaprijed unesenimi pohranjenim slikama ljudskih lica. Druga poznata metoda je algoritam facijalne metrike, metoda kojom se analizira položaj i relativna udaljenosti između dijelova korisnikova lica (nosa, usta i očiju) te informacije o njima zapisuju se u predložak. Dvodimenzionalni algoritmi se lako mogu zavarati podmetanjem slike legitimnog korisnika. Kvaliteta prepoznavanja ovisi o kutu upada svjetlosti na lice korisnika i promjeni kuta gledanja u kameru. Problem predstavlja i promjenjivost lica starenjem, različite osobe mogu imati vrlo slična lica, mijenjanjem frizure, načina šminkanja, izraza lica i brade ili nošenjem naočala. Zbog nepouzdanosti i nepreciznosti dvodimenzionalne metode se malo koriste u identifikaciji. Trodimenzionalni algoritmi analiziraju i pohranjuju 3D karakteristike i veličine dijelova lica. Na taj način se izbjegavaju problemi koji karakteriziraju dvodimenzionalne metode jer svojstva trodimenzionalnog modela ne zavise o izrazu lica, trenutnom psihičkom stanju, načinu šminkanja, zakrenutosti glave i sl. [11].



Slika 7. Prepoznavanje lica

Izvor: [11]

4.1.5. Termogram lica

Termogram lica je nova i perspektivna biometrijska metoda koja još nije našla komercijalnu primjenu zbog visokih cijena opreme potrebne za snimanje. Lice svakog čovjeka prožeto je razgranatim mrežama krvnih žila. Snimke dobivene infracrvenom kamerom govore o položajima krvnih žila koji su jedinstveni za svakog čovjeka. Za razliku od metode prepoznavanja lica, slike se mogu prikupljati bez obzira na osvjetljenje u okolini. Prednost je nenametljivost prema korisniku. Prepoznavanje funkcionira neovisno o dobi, izrazu lica i estetskim modifikacijama. Zbog visoke točnosti i brzine metoda je pogodna za identifikaciju [13].

4.1.6. Analiza DNK

Analiza DNK (deoksiribonukleinske kiseline) jedna od najznačajnijih i najpouzdanijih biometrijskih metoda identifikacije. Ljudski geni građeni su od lanaca DNK. Postotak od 99,5% DNK molekule je zajednički svim ljudima i to područje DNK naziva se nekodirajuće područje, dok preostalih 0,5% predstavlja kodirajuća područja koja su visoko varijabilna i čine svaku osobu jedinstvenom.

Analiza DNK koristi se u mnogim područjima istraživanja, a najzanimljivija primjena je u području kriminalistike i sudske medicine gdje se analiza DNK koristi za utvrđivanje identiteta nepoznate osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tijela itd. Nedostaci DNA metode se ogleda u tome što je to dugotrajan i skup proces analize koji uključuje stručno osposobljene osobe [11].

4.2. Biometrija ponašanja

Biometrija ponašanja opisuje fizikalne karakteristike (kao što su kretanje u prostoru, glas, izgled…) čovječjeg tijela koje su dijelom jedinstvene za svaku osobu. Dobiveni uzorci se opisuju krivuljama koje se koriste za opis ponašanja pa je na osnovu njih moguće raspoznavati različite ljude. Navedene tehnike se koriste u kombinaciji s tradicionalnim načinima jednoznačnog opisivanja ljudi [4].

4.2.1. Glas

Prepoznavanje glasa koristi se za identifikaciju korisnika na temelju njegovih jedinstvenih glasovnih karakteristika. Korisnik mora izgovoriti neki tekst koji je prethodno izgovorio i koji je spremljen u bazu podataka kako bi se identificirao. Tu postoji visoka jedinstvenost pošto ljudi uglavnom različito izgovaraju iste rečenice (tonalitet, brzina, prekidi). No, mogućnost zlouporabe je velika jer je moguće snimiti zvučni zapis identifikacije neke osobe. Stoga se ovu metodu mora koristiti u kombinaciji s drugim metodama [4].

Prednost ovakvih sustava je što koriste uobičajenu, jeftinu i lako nabavljivu hardversku opremu. Sustav je vrlo prihvatljiv i nenametljiv za korisnike. Nažalost, učinkovitostnije tako dobra i mogućnostzavaravanja sustavaje relativno velika. Sustav je osjetljiv na pozadinsku buku, a glas varira ovisno o dobi i raspoloženju korisnika [5].

4.2.2. Dinamika potpisa

Prepoznavanje dinamike potpisa zasniva se na načinu na koji nastaje potpis i obično ne uzima u obzir izgled samog potpisa. Analizira se smjer, akceleracija, pritisak, duljina, trajanje i broj poteza ruke. Postoje dva načina da se dohvate ti podaci:

- ploča osjetljiva na dodir (eng. *tablet*) registrira pokrete i pritisak olovke na površinu,
- pametna olovka funkcionira kao svaka druga olovka- ima tintni uložak kojim se korisnik potpisuje na papir. U pametnoj olovci se bilježe pokreti u sve tri dimenzije kao i pritisak na površinu [5].

Prednost ispitivanja dinamike potpisa je što se ne može krivotvoriti proučavajući zapisani potpis korisnika. Krivotvorenje može uspjeti samo ako zlonamjerna osoba proučava način na koji se korisnik potpisuje, međutim u praksi se pokazalo da je čak i to izvedivo pa se metoda ne smatra sasvim pouzdanom [13].

4.2.3. Dinamika tipkanja

Ova tehnika se razvila tijekom drugog svjetskog rata u primjeni kod radiotelegrafista jer je uočeno da se po brzini tipkanja mogu razlikovati pošiljatelji poruka. Ako se danas govori o dinamici tipkanja onda se podrazumijeva dinamika tipkanja po tipkovnici. Kao tehnika je vrlo nenametljiva jer 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. Glavna karakteristika na kojoj se ova tehnika bazira je vremenski razmak između korisnikovog pritiskanja na tipkovnicu [4].

4.2.4. Dinamika hodanja

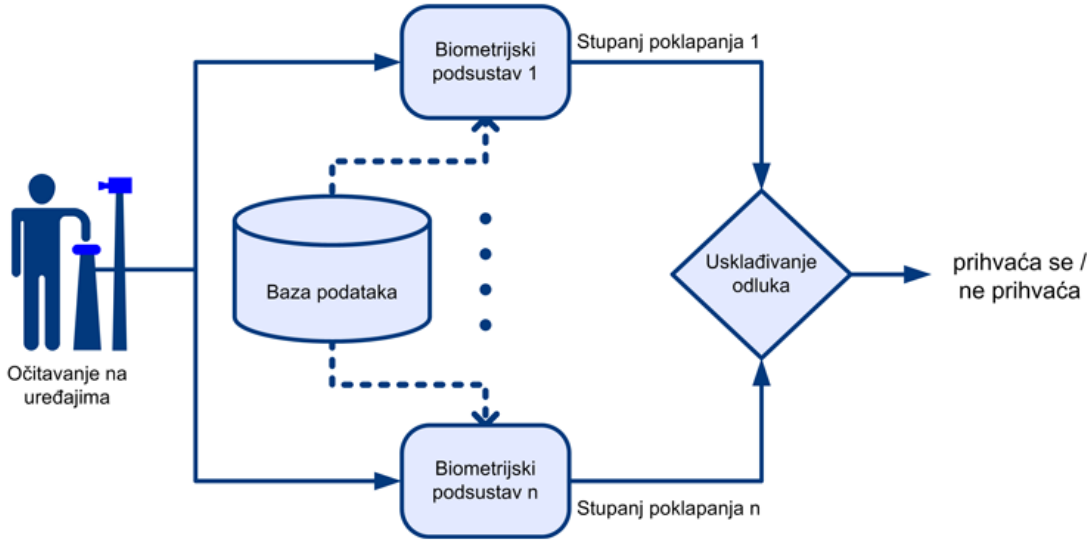
Ljudsko hodanje predstavlja kompleksnu prostorno-vremensku biometriju ponašanja. Njegova karakteristika je to što nije jedinstven za svakog od pojedinaca, ali je po svojim karakteristikama karakterističan u svrhu provjere identiteta s obzirom na karakter, situaciju u kojoj se nalazi osoba i na njeno zdravstveno stanje. Hod nije nepromjenjiv, pogotovo kod dužeg vremenskog perioda jer se osoba umara. 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].

4.2.5. Dinamika mirisa

Svaki objekt u prirodi ima svoj miris koji je karakterističan za njegov kemijski sastav. Biometrijski sustavi koji detektiraju mirise rade na principu upuhivanja zraka preko kemijskih senzora od kojih je svaki osjetljiv na određenu grupu mirisa, tj. na njegova kemijska svojstva. Miris se opisuje mjerenjima obuhvaćenom od senzora i u njegovom intenzitetu na svakome od njih. 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 od sporedne. Posebno je važno razlikovati miris osobe od parfema na njoj pa je u tom polju potrebno još istraživanja kako bi se odijelili mirisi [4].

4.3. Multimodalna biometrija

Multimodalni sustavi (slika 8) upotrebljavaju dvije ili više biometrijskih metoda za identifikaciju. Svaka metoda svojim algoritmom izračunava stupanj poklapanja. Dobiveni stupnjevi se usklađuju i donosi se konačna odluka. Veći broj upotrebljenih metoda znači veću točnost, ali i veći trošak. Ne postoji jednostavan način odabira biometrijskih metoda koje ćemo upotrijebiti u multimodalnom sustavu. Izabrane metode zavise o njegovoj primjeni, međutim u većini slučajeva najbolje rezultate daju kombinacije biometrijskih metoda velike i srednje točnosti. Među najčešće korištene metode ubrajaju se otisak prsta, prepoznavanje lica i šarenica oka [5].



Slika 8. Multimodalni biometrijski sustav

Izvor: [5]

5. SIGURNOST PODATAKA I ETIČKA PITANJA VEZANA UZ BIOMETRIJSKE METODE

Sigurnost cijelog sustava je dobra koliko najslabija njegova karika - zaporka. U tradicionalnim sustavima koji se temelje na lozinkama koje su kombinacije brojeva ili brojeva i slovanemoguće je utvrditi je li osoba koja je zaporku upisala uistinu njezin vlasnik ili je zaporka ukradena. Također, postoje brojni problemi sa ključevima i karticama za identifikaciju. Na primjer, ključevi i kartice mogu se dijeliti, umnožavati, izgubiti ili biti ukradeni, a i napadač može napraviti „master“ ključ koji može otvoriti mnoga vrata. Značajno je kompliciranije kopirati i dijeliti biometrijske karakteristike.

Biometrijska karakteristika ne može biti izgubljena ili zaboravljena, osoba u trenutku identifikacije mora biti osobno prisutna, a teško ih je i krivotvoriti. Osim toga, svi korisnici sustava imaju relativno jednak stupanj sigurnosti i jedan račun nije lakše probiti nego bilo koji drugi. Biometrija je također puno pogodnija za korisnike koji više ne moraju pamtiti dugačke i kompleksne lozinke niti ih učestalo mijenjati, a pritom se zadržava dovoljno visok stupanj sigurnosti.

Za napad na biometrijske sustave, treba generirati velik broj biometrijskih uzoraka (npr. otisaka prstiju), što je puno teže nego što je generirati veliki broj pinova/zaporki. Multimodalnom biometrijom se dodatno povećava sigurnost pristupa sustavu jer je potrebno sustavu prezentirati dvijeili više biometrijskih značajki čime je dodatno otežano dešifriranje i provala u sustav.

Nedostatak je biometrijskih sustava što jednom kompromitirani biometrijski uzorak, zauvijek ostaje kompromitiran i ne može se obnoviti kao što je u tradicionalnih sustavima sigurnosti moguće zatražiti i kreirati novu lozinku. Korisnik ima samo jedno lice, 10 otisaka prstiju itd. i teško je iznova kreirati njegov biometrijski predložak kad se jednom ugrozi. Taj se nedostatak nastoji riješiti ugradnjom kriptografskih tehnologija u biometrijske sustave. Primjerice, umjesto pohranjivanja originalnog biometrijskog signala nakon očitavanja senzorom, sistemska baza podataka može tijekom registracije korisnika pospremiti samo transformiranu verziju signala koju ju nemoguće „preokrenuti“ u originalnu verziju. Tijekom prepoznavanja, biometrijski senzor ponovo kreira transformirani signal koji se zatim uspoređuje s pohranjenim transformiranim signalom u biometrijskom predlošku. Različiti biometrijski sustavi mogu koristiti različite kriptografske tehnike pa je time stvoreni predložak upotrebljiv samo u sustavu koji ga je stvorio i izbjegnuta je mogućnost da se haker, koji je u jednom sustavu uspio dešifrirati biometrijski uzorak, može istim uzorkom koristiti u drugim sustavima. Nedostatak ovih sustava je smanjenje točnosti jer je sustavu otežano raditi sa svim varijacija biometrijskog signala iste

osobe u transformiranoj bazi podataka. Jednostavan i efikasan način kreiranja biometrijskih predložaka koje je u slučaju provale u sustav moguće poništiti je povezivanje biometrijskog predloška koji je kriptiran s korisničkom lozinkom [7].

Kad su u pitanju stavovi korisnika prema biometriji, pitanje koje korisnici najčešće postavljaju i koje ih najviše brine jest ugrožava li biometrija njihovu privatnost. Kako bi se osigurala privatnost biometrijskih podataka, samih biometrijskih sustava te na taj način privatnost krajnjih korisnika prvo je neophodna zaštita biometrijskih podataka. Također, dizajn i način korištenja biometrijskih sustava uvijek trebaju poštivati strogo propisane smjernice. Za ostvarenje privatnosti moraju se zadovoljiti četiri glavne smjernice, a to su: opseg i mogućnosti biometrijskog sustava; zaštita podataka; korisnička kontrola osobnih podataka te objavljivanje, revizija i odgovornost biometrijskih sustava. Prva smjernica odnosi se na opseg i mogućnosti sustava. Opseg i funkcionalnost sustava ne bi trebali biti prošireni bez izričitog dopuštenja i obavještavanja svih korisnika. Zadržavanje biometrijskih podataka mora biti minimalno, što znači da se verifikacijski podaci trebaju uvijek brisati, a biometrijski predlošci čuvati. Osim toga, korisnik treba biti obaviješten o brisanju verifikacijskih podataka. Prikupljanje bilo kakvih drugih podataka osim onih za koje je korisnik dao informirani pristanak je apsolutno nedozvoljeno i treba biti onemogućeno. Zaštita podataka je druga točka osiguravanja privatnosti. Prije svega vrlo je važna uporaba odgovarajućih tehnologija za zaštitu podataka. Biometrijski sustavi trebaju se koristiti u kontroliranim i sigurnim uvjetima. Uz to je važno istaknuti da samo ograničen broj operatera treba imati pristup bazama biometrijskih podataka. Korisnička kontrola osobnih podataka znači da korisnik mora zadržati kontrolu nad svojim biometrijskim podacima, da korisnici biometrijski sustav moraju koristi dobrovoljno i nikako drugačije te da korisnik ima mogućnost mijenjanja i brisanja svojih osobnih podataka. Zadnja točka je područje vezano uz odgovornost za biometrijske podatke. Svaki operater mora biti upoznat sa svrhom biometrijskog sustava. Važno je znati kada se koristi biometrijski sustav, pogotovo kada se provodi verifikacijska ili identifikacijska faza. Operateri moraju preuzeti odgovornost za eventualno počinjene pogreške tijekom provođenja nekog od biometrijskih postupaka [14].

Udruga za korisničku tehnologiju (*Consumer Technology Association* - CTA) provela je 2016. godine u SAD-u istraživanje o biometrijskim tehnologijama i njihovoj prihvaćenosti od strane korisnika. Pokazalo se da je manje od polovine odraslih osoba prihvatilo ili koristilo neku od vrsta biometrijske tehnologije. Otisak prsta i prepoznavanje glasa dvije su najviše korištene i prihvaćene biometrijske metode identifikacije. Većina ispitanika osjeća se sigurno s biometrijskim tehnologijama na mjestima koja su visoko zaštićena, kao što su zračne luke ili koja trebaju veću zaštitu, primjerice područja s visokom stopom kriminala. Više od polovice (63%) odraslih ispitanika su otvoreni i spremni na korištenje biometrijskih tehnologija za potrebe kao što su npr. medicinska istraživanja (58%). No, ispitanici smatraju da organizacije trebaju educirati korisnike o prednostima biometrije i njihove uporabe. Istraživanje koje je 2015. godine provela kompanija Gigya pokazalo je da 41 % stanovnika SAD-a ima veliku razinu povjerenja u

prijavljivanje na web stranice i mobilne aplikacije koristeći svoje otiske prstiju. No, više od 90% USA i UK korisnika su na neki način zabrinuti za privatnost njihovih podataka i na način koji ustanove koriste njihove podatke. Treće istraživanje provedeno 2014. godine među stanovnicima Ujedinjenog Kraljevstva dokazalo je da 79% ispitanika i ujedno korisnika biometrijskih tehnologija je spremno odbaciti lozinke i zamijeniti ih skenerima otisaka prstiju, a 53% ispitanika bi voljeli kada bi njihove banke implementirale skenere za otiske prstiju u svoje digitalne usluge [15].

Istraživanje provedeno 2015. godine u razdoblju od travnja do lipnja obuhvaćalo je područje biometrijske identifikacije u uređajima najbližim krajnjem korisniku kao što su pametni telefoni. Istraživanjem se htjelo uvidjeti kakva je korisnička percepcija o sigurnosti biometrijske identifikacije na pametnim telefonima, kako oni percipiraju korisnost i pouzdanost identificiranja šarenice oka te se htjelo vidjeti utječu li demografski čimbenici kao što je dob na percepcije korisnika. Anketa je bila u online obliku i sastojala od dva dijela, prvi dio se odnosio na percepciju korisnika o sigurnosti i privatnosti biometrijske identifikacije na pametnim telefonima, a drugi dio se odnosio na percepciju korisnika o korištenju identifikacije putem šarenice oka na pametnim telefonima. Većina ispitanika koja je sudjelovala u istraživanju je bila u dobi između 25 i 44 godine. Ispitanici se slažu s potrebom zaštite podataka i sigurnosti na njihovim pametnim telefonima (šifriranje podataka, zaštita telefona od krađe, zloupotrebljavanja, hakiranja i sl.). Vrlo važnim smatraju i zaštitu svojih osobnih podataka kao što su ime, prezime, lokacija, zanimanje i sl. Kod starijih ispitanika važnost zaštite i sigurnost informacija na pametnim telefonima bila je veća nego kod mlađih ispitanika. 85% ispitanika u dobi između 25 i 44 godine iskazali su visok značaj zaštite njihovih informacija na pametnim telefonima, a samo 67% u dobi između 15 i 24 godine složilo se s istim. Istraživanjem je i dokazano da ispitanici više preferiraju moderne tehnologije te su pokazali veliku zainteresiranost za identifikaciju putem šarenice oka. Najveći broj ispitanika za idealnu kombinaciju za zaštitu i dodatnu sigurnost izabralo je lozinku i otisak prsta, a njih 21% odgovorilo je da im nije bitno sve dok nije kompliciranо. Zaključeno je da ispitanici smatraju da je sigurnost podataka i privatnost na pametnim telefonima jako važna. Ispitanici ne vjeruju tehnologijama koje nisu toliko popularne i dovoljno promovirane kao što su prepoznavanje lica. Kada se radi o prepoznavanju šarenice oka mnogim korisnicima nije problem prilagoditi se ograničenjima poput toga da se tijekom identifikacije oko ne smije micati kao ni telefon te da se moraju skinuti dioptrijske naočale, no neki ispitanici su izrazili nezadovoljstvo što su trebali pronaći savršeno osvjetljenje kako bi identifikacija bila moguća. Vrlo je važno istaknuti da se 90% ispitanika znalo služiti svim biometrijskim metodama identifikacije dovoljno dobro da bi se osigurao biometrijski uzorak koji zadovoljava njihove kriterije kvalitete [15].

6. ZAKONSKI OKVIRI PRIMJENE BIOMETRIJE

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka - Opća uredba o zaštiti podataka (u daljnjem tekstu Uredba, eng. *General Data Protection Regulation* - GDPR) izravno se primjenjuje u Republici Hrvatskoj od 25. svibnja 2018. godine. Uredba predstavlja bitan napredak u području zaštite osobnih podataka.

Tehnološkim razvojem i novim načinima obrade osobnih podataka, postalo je nužno donošenje novog instrumenta koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka. Također, Općom uredbom se osigurava ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka, što će imati za posljedicu jednostavniju i jednaku zaštitu prava svih pojedinaca u Europskoj uniji.

Općom uredbom o zaštiti podataka uvode se nove i pojednostavljuju se neke već postojeće definicije, određuju biometrijski i genetski podaci, preciznije opisuju postojeći pojmovi, jačaju prava ispitanika te se smanjuju i pojednostavljuju pojedine administrativne obveze voditelja zbirke osobnih podataka, jačaju nadzorne ovlasti te mogućnost izricanja kazni od strane tijela za zaštitu osobnih podataka.

Prema Uredbi, osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Dakle, jako je širok spektar što su osobni podaci, no jednostavnije rečeno to su: ime i prezime, identifikacijski broj, slika, glas, adresa, broj telefona, IP adresa, povijest bolesti, popis najdraže literature ili pjesama, ako takvi podaci mogu dovesti do izravnog ili neizravnog identificiranja pojedinca. Za zakonitu obradu osobnih podataka nužan je uvjet da je ispitanik dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha - privola je dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose, a osim toga je uvjet da je obrada podataka nužna iz pravnih ili drugih razloga.

Pojam biometrijski podaci, prema Uredbi, označava osobne podatke dobivene posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.

U članku 9. Obrada posebnih kategorija osobnih podataka Uredbe stoji da je u osnovi zabranjena obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja itd. te obrada genetskih podataka i biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, osim u specifično definiranim slučajevima. Za takve posebne slučajeve u kojima se dozvoljava obrada podataka potrebna je izričita privola

osobe čiji se podaci obrađuju ili kad je obrada nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu. Smatra se da je, uz posebne uvjete, dozvoljeno podatke obrađivati za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti te kad je obrada nužna iz drugih pravnih razloga. Također, poseban slučaj je obrada podataka koja je potrebna u svrhu preventivne medicine ili medicine rada, kao i za praćenje javnog zdravlja kako bi se osigurala zdravstvena zaštita i visoki standardi zdravstvene skrbi, u što se ubraja i dostupnostpotrebnih lijekova i medicinskih proizvoda. U članku 9. navodi se i da države članice Europske unije mogu zadržati ili uvesti dodatne uvjete, uključujući ograničenja s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje [16].

U SAD-u ne postoji jedinstveni, sveobuhvatni zakon koji bi regulirao prikupljanje, obradu i upotrebu osobnih podataka općenito, kao niti specifično biometrijskih podataka. Postoje razni zakoni i regulative za pojedinačne zemlje koji se djelomično preklapaju, a u nekim su segmentima čak i kontradiktorni. Državne agencije i industrijske grupacije samostalno su razvile vlastite smjernice za reguliranje obrade podataka utemeljene na praksi. Apple, Facebook, Google i Microsoft primjeri su takvih kompanija koje provode samokontrolu, a imaju značajna ulaganja u kreiranje tehnologija prepoznavanja lica. Primjerice, DeepFace, Facebookov sustav prepoznavanja lica ima 97%-tnu točnost.

Od srpnja 2017. godine u 47 država SAD-a legalno je da softver identificira osobu prema fotografijama koje su snimljene dok je osoba u javnosti, bez njezinog pristanka. Washington je, poslije Illinoisa i Texasa, tek treća država koja je usvojila zakon o privatnosti biometrijskih podataka, eng. *Biometric Information Privacy Act* koji postavlja zakonske zahtjeve za tvrtke koje koriste biometrijsku identifikaciju za komercijalne svrhe.

Pitanje privole za obradu podataka i načina postupanja s biometrijskim podacima proteže se kroz nekoliko različitih zakonskih akata izdanih od strane različitih agencija. Tako National Institute of Standards and Technology postavlja zahtjeve za evaluaciju biometrijskih tehnologija dok je Federal Trade Commission izdala akt u kojem se štiti korisnike zabranom nepoštenih i zavaravajućih sustava što se odnosi kako na izvanmrežnu, tako i na mrežnu, eng. *online* privatnost i postupke vezane za sigurnost podataka. The Department of Health and Human Services izdao je Health Insurance Portability and Accountability Act u kojem se postavljaju zahtjevi za zaštitu medinskih podataka.

Sa sve jačim razvojem biometrije i njenom sve većom primjenom, sigurno je da će i SAD morati donijeti specifičan zakon koji će regulirati prikupljanje, obradu i zaštitu biometrijskih podataka, što je u zemljama Europske unije već regulirano na puno većem stupnju [17], [18].

7. PRIMJERI KORIŠTENJA BIOMETRIJSKIH METODA NA ZRAČNIM LUKAMA

Cilj korištenja biometrijskih metoda na zračnim lukama je povećanje sigurnosti uz istovremeno značajno smanjenje čekanja putnika pri zaštitnim pregledima, kontrolama ukrcajnih propusnica, predaji prtljage itd.

Jedan od primjera korištenja biometrije u svakodnevnom životu, kao i na zračnim lukama su biometrijske putovnice. Organizacija međunarodnog civilnog zrakoplovstva(*International Civil Aviation Organization* - ICAO) izdala je dokument Doc 9303 posvećen putnoj dokumentaciji koja se može strojno očitavati. Dokument detaljno opisuje potrebne tehničke specifikacije i ISO standarde koji se tiču biometrijskih putovnica [19]. Biometrijska putovnica je javna isprava koja u svojoj strukturi sadrži elektronički „nosač" podataka – čip, koji je skriven unutar putovnice. Unutar čipa putovnice pohranjuju se: osobni podaci nositelja putovnice (ime, prezime, državljanstvo, datum rođenja, podatak o spolu, oznaka za vrstu putne isprave, oznaka države, broj putovnice, osobni identifikacijski broj, datum izdavanja i datum isteka valjanosti putovnice i tijelo koje je putovnicu izdalo) i biometrijski podaci nositelja putovnice (u RH digitalizirana slika lica i otisci dva kažiprsta). Biometrijsku putovnicu RH-a je uvela zbog usklađivanja s međunarodnim standardima sigurnosti putnih dokumenata, kao elementa sigurnosti granica i putovanja. Biometrijska putovnica ima značajne prednosti nad dosadašnjom hrvatskom putovnicom: pruža još veću zaštitu od prijevarne zlouporabe i neovlaštenih izmjena; smanjuje rizik od „krađe identiteta"; pospješuje zaštitu hrvatske granice putem brze provjere nositelja hrvatskih putovnica koji ulaze u zemlju [11].

Svaka zemlja samostalno odlučuje hoće li se bazirati na verifikaciji, identifikaciji ili oba modula u sklopu elektronskog sustava za kontrolu graničnih prijelaza. Na primjer, mnoge zračne luke odabrale su automatizirane sigurnosne provjere (identifikaciju), dok je tradicionalni način u kojem djelatnik vizualno uspoređuje putnika i njegovu fotografiju na identifikacijskoj ispravi još uvijek zastupljen kao verifikacijski modul. U posljednjih nekoliko godina, automatizirani sustavi kontrole putovnica sve su više zamijenili tradicionalne šaltere za provjeru putovnica na međunarodnim zračnim lukama u SAD-u, Kanadi, Nizozemskoj, Estoniji, Australiji, Novom Zelandu, Japanu itd. što je značajno ubrzalo vrijeme potrebno za identifikaciju putnika [8].

Biometrijska identifikacija također je značajan doprinos za olakšavanje procesa i ubrzavanje prolaska niskorizičnih putnika koji su u kategoriji čestih putnika, eng. *frequent flyer*. Takav je program pod nazivom Privium dostupan na nizozemskoj zračnoj luci Schiphol. Korisnici Priviuma prolaze kroz kontrolne točke zračne luke skeniranjem šarenice oka [20].

U.S. Customs and Border Protection od 2013. intenzivno radi na razvoju optimalnog biometrijskog postupka kojim bi se verificirao identitet osoba koje na zračnim lukama ulaze u

SAD i onih koji iz SAD-a odlaze u usporedbi s identifikacijskim dokumentom kojeg putnici prilažu. Program biometrijske kontrole putnika koji iz SAD-a odlaze zove se *Biometric Air Exit*, a njegova je primjena počela u lipnju 2016. godine na zračnoj luci Hartfield-Jackson Atlanta International Airport. Radi se o biometrijskom sustavu koji se temelji na prepoznavanju lica kao biometrijskoj karakteristici, a s obzirom na uspjeh prvotne primjene, razvijen je Servis za verifikaciju putnika (*Traveler Verification Service* -TVS) koji kreće u primjenu na više zračnih luka [21].

Sita, kompanija koja nudi komunikacijske i IT infrastrukture za zrakoplovnu industriju testirala je nekoliko različitih biometrijskih sistema diljem svijeta. U 2017. napravili su probnu primjenu na zračnoj luci u Birsbaneu u trajanju od 6 mjeseci u kojem su putnici na check-in šalteru pokazali svoju putovnicu i ukrcajnu propusnicu, a pritom je napravljena i slika njihova lica. Nakon toga su sve ostale preglede na zračnoj luci prolazili jednostavnim pogledom u kameru bez ponovne kontrole dokumenata što je značajno ubrzalo procese i povećalo zadovoljstvo putnika [22].

U svibnju 2017. Finnair je ponudio 1000 svojih redovnih korisnika da prije leta učitaju 3 *selfija* i podatke sa svoje kartice vjernosti u testni biometrijski sustav. Dolaskom na zračnu luku u Helsinkiju putnici su došli do samostalnog check-in šaltera koji je upotrebljavao tehnologiju prepoznavanja lica i time je njihov check-in bio izvršen bez potrebe prikazivanja identifikacijskih dokumenata ili čekanja na check-in šalterima [22].

Delta Air Lines u lipnju 2017. predstavio je prvi biometrijski sustav samostalne predaje prtljage na zračnoj luci Minneapolis-St Paul s ciljem značajnog ubrzanja procesa, a sustav se temelji na prepoznavanju lica. Prednost ovog sustava je dvostruka – osim uštede vremena, postoji vizualni trag putnika koji je predao prtljagu čime je značajno povećana sigurnost [22].

Prepoznavanje lica kao biometrijska metoda kontrole na *boarding gateovima* uveden je i na Boston Logan International Airport u suradnji s kompanijom JetBlue, zračnoj luci Schiphol u Amsterdamu u suradnji s prijevoznikom KLM te na terminalu 5 zračne luke Heathrow u Velikoj Britaniji u suradnji s British Airwaysom [22].

Neke zračne luke primijenile su biometrijska rješenja kao dio imigracijske procedure. Ujedinjeni Arapski Emirati (UAE) pokrenuli su još 2003. program nazvan *Iris Expellees Tracking and Border Control System* kako bi smanjili broj ilegalnih imigranata. Sustav funkcionira na način da se u deportacijskom centru, prije izbacivanja osobe iz zemlje, skenira njegova šarenica i podaci se pohranjuju u centralnu bazu podataka koju vodi policija Abu Dhabija. Šarenice svih stranaca koji ulaze u zemlju s novim vizama također se skeniraju i uspoređuju s bazom podataka koja je ujedno najveća baza na svijetu s pohranjenim biometrijskih predlošcima baziranim na šarenici oka. Na taj način je moguće unutar dvije sekunde primijetiti

osobu koja je pokušala ponovo ući u zemlju nakon deportacije korištenjem lažnih dokumenata. U periodu od 8 godina korištenja programa, gotovo 350 tisuća deportiranih osoba je identificirano [23].

U brojnim područjima zračnih luka nužno je osigurati pristup isključivo autoriziranom osoblju pri čemu se biometrijske tehnike iznova pokazuju kao izvrsno rješenje. U zračnoj luci Los Angelesa u kojoj se godišnje izda oko 60 tisuća zaposleničkih iskaznica, umjesto broja iskaznice kao mjera sigurnosti počeli su se primjenjivati otisci prstiju, a radi se i na snimanju šarenica zaposlenika kako bi u budućnosti primijenili multimodalni biometrijski pristup koji će uključivati i geometriju šake kako bi se mogućnost pogreški svela na minimum. S istim ciljem je u Švicarskoj razvijen multimodalni sustav koji se temelji na prepoznavanju lica i načinu hoda za autentifikaciju zaposlenika koji je probno testiran na Euroairportu u Švicarskoj, kao dio znanstvenog projekta Promatranje i autentifikacija ljudi korištenjem biometrijskih indikatora i ponašajne analize (*Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis* - HUMABIO) [8].

O primjeni biometrije na zračnim lukama sve se više govori i u pogledu profiliranja osoba za koje se sumnja da imaju zle namjere. Izraelska kompanija WeCU Technologies Ltd. razvila je sustav u kojem su zvučni ili video podražaji specifično dizajnirani za relevantne ciljane grupe za koje se očekuje da će kod njih izazvati biometrijski odgovor, odnosno svjesnu ili podsvjesnu tjelesnu ili ponašajnu reakciju. Te reakcije moguće je snimiti skrivenim kamerama ili skrivenim senzorima. Na primjer, ako terorist promatra ekran s rasporedom letenja, a na zaslonu se pojavi simbol njegove terorističke grupe, to će kod njega izazvati nesvjesnu reakciju kao što je ubrzan rad srca, brže disanje, fiksacija pogleda itd. Iz kompanije tvrde da u roku 35 sekundi njihov sustav može izmjeriti do 14 varijabli i da je uspješnost testiranja približno 95%. WeCU Technologies Ltd. nije jedina kompanija koja je razvila takav sustav, primjerice sustav za detekciju sumnjivaca *Cogito* testiran je na američkim i izraelskim zračnim lukama, a zamišljen je kao kabina u kojoj osoba odgovara na pitanja pri čemu se snimaju njene reakcije i zabilježava biometrijski odgovor [8].

Nakon nesreće Germanwingsa na letu 9525 2015. godine kada je kopilot Andreas Lubitz, nakon izlaska pilota iz kokpita, zaključao kokpit te namjerno srušio zrakoplov u planinu što je uzrokovalo pogibiju svih 144 putnika i 6 članova posade, sve se više govori o potrebama osiguravanja sigurnosti i tijekom leta, a ne samo na zračnim lukama. Posljedično je Europska agencija za sigurnost zračnog prometa (*European Aviation Safety Agency* - EASA) izdala preporuku da se osigura da su minimalno dvačlana posade, uključujući barem jednog pilota prisutna u kokpitu tijekom cijelog leta. No, kreirana su i biometrijska rješenja da se osigura siguran kokpit u smislu ograničavanja ulaska u kokpit isključivo autoriziranom osoblju. Jedno od rješenja koje donosi SAFEE program je da se u kokpit može ući isključivo prezentiranjem otiska prsta koji se onda uspoređuje s bazom podatka u kojoj su biometrijski predlošci posade za svaki

pojedinačni let. Također, postavljaju se i kamere koje su povezane s video prikazom u kokpitu što omogućava pilotu ili kopilotu da provjere želi li u kokpit ući član posade ili potencijalni uljez [8].

8. ZAKLJUČAK

Biometrijske metode već se naveliko koriste u našem svakodnevnom životu – svoje pametne telefone otključavamo pomoću otiska prsta ili glasom (Siri na iPhone-ima), a na svoja računala ulogiravamo se pomoću prepoznavanja lica (sustav Windows 10).

Može se reći da je primjena biometrijskih metoda na zračnim lukama još u svojim začecima, ali posljednjih je godina primjetan porast njihove primjene i povećan interes kako zračnih luka, tako i aviokompanija, a sve s ciljem postizanja što boljeg korisničkog iskustva i privlačenja korisnika korištenjem najnovijih tehnologija koje ubrzavaju procese kontrole i smanjuju broj dokumenata koje korisnici trebaju prilagati. U vrijeme brojnih terorističkih napada koji se događaju diljem svijeta, sigurnost postaje od presudne važnosti zbog čega je također primjena biometrije veoma bitna. Korištenje biometrijskih metoda značajno smanjuje mogućnosti krađe identiteta, a omogućuje i pravovremeno prepoznavanje sumnjivih putnika koji se zatim mogu podvrgnuti dodatnih kontrolama.

Sigurno je da će pokusni biometrijski sustavi koji su trenutno u primjeni ukazati na potrebna poboljšanja koja je potrebno provesti, ali uz napredak tehnologije to će biti dostižan cilj. Realno je za očekivati da će se u sljedećim godinama biometrijski sustavi kontrole, barem u nekom obliku, uvesti na sve zračne luke svijeta. Galopirajući razvoj biometrije morat će pratiti i zakonodavstvo od kojeg se očekuje da definira pravne okvire korištenja biometrijskih tehnologija s naglaskom na zaštitu biometrijskih podataka kako bi se osigurala privatnost korisnika i sigurnost biometrijskih sustava od zlouporabe.

Popis kratica

CTA	(Consumer Technology Association) Udruga za korisničku tehnologiju
DAC	(Digital Audio-Video Converter) elektronički digitalni audio-video konverter
EASA	(European Aviation Safety Agency) Europska agencija za sigurnost zračnog prometa
FAR	(False Acceptance Rate) stopa pojavljivanja pogrešaka lažnog prihvaćanja
FERET	(FacE REcognition Technology) tehnologija prepoznavanja lica
FME	(False Match Error) pogreška lažnog podudaranja
FMR	(False Match Rate) stopa pogrešaka lažnog podudaranja
FNME	(False Non-match Error) pogreška lažnog nepodudaranja
FNMR	(False Non-match Rate) stopa pogrešaka lažnog nepodudaranja
FRR	(False Rejection Rate) stopa pojavljivanja pogrešaka lažnog odbijanja
FTA	(Failure to Acquire) pogreška prikupljanja podataka
FTE	(Failure to Enroll) pogreška pri registraciji podataka
GDPR	(General Data Protection Regulation) Opća uredba o zaštiti podataka
HUMABIO	(Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis) promatranje i autentifikacija ljudi korištenjem biometrijskih indikatora i ponašajne analize
ICAO	(International Civil Aviation Organization) Organizacija međunarodnog civilnog zrakoplovstva
INSPASS	(Immigration and Naturalization Service Passenger Accelerated Service System) ubrzani servisni sustav za imigraciju i izdavanje državljanstva putniku
ISO	(International Organization for Standardization) Međunarodna organizacija za standardizaciju
TSA	(Transportation Security Administration) Uprava za sigurnost prometa
US-VISIT	(United States Visitor and Immigrant Status Indication Technology) tehnologija prikaza posjetiteljskog i imigrantskog statusa SAD-a

Literatura

1. Biometric Update.com.
   URL: https://www.biometricupdate.com/201802/history-of-biometrics-2 (pristupljeno: lipanj 2018.) [1]
2. ISO/IEC TR 24741:2018 (en) Information technology — Biometrics — Overview and application.
   URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en (pristupljeno: lipanj 2018.) [2]
3. Stanilović, P. Zaštita zemaljske strane u zračnim lukama, završni rad, FPZ, Zagreb 2017. [3]
4. CARNet (Croatian Academic and Research Network): Biometrija, CCERT-PUBDOC-2006-09-167. [4]
5. Nimac, L. Pregled biometrijskih metoda autentifikacije, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, završni rad, Zagreb 2013. [5]
6. Project Management Institute: A Guide to the Project Management Body of Knowledge, 3rd Ed., Project Management Institute, Newtown Square, Pennsylvania USA, 2004. [6]
7. Prabhakar S, Pankanti S, Jain A.K. Biometric recognition: security and privacy concerns. IEEE Security & Privacy 2003;99(2):33-42. [7]
   URL: https://ieeexplore.ieee.org/document/1193209/?part=1 (pristupljeno: srpanj 2018.).
8. Teodorović, S. The role of biometric applications in air transport security. NBP Journal of Criminalistics and Law. 2016; 2:139-158. [8]
9. Iritech Inc. How to evaluate the accuracy of a biometric modality?
   URL: http://www.iritech.com/blog/biometric-accuracy-evaluation/ (pristupljeno: srpanj 2018.) [9]
10. Precise Biometrics. Understanding biometric performance evaluation.
    URL: https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf (pristupljeno: srpanj 2018.) [10]
11. Boban, M; Perišić, M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava, pregledni rad. Zbornik radova Veleučilišta u Šibeniku, Vol. , No. 1-2/2015, 2015.[11]
12. Android authority. URL: https://www.androidauthority.com/how-do-ultrasonic-fingerprint-scanners-work-666053/ (pristupljeno: srpanj 2018.) [12]
13. Huđek, D. Primjena biometrijske zaštite u inteligentnim transportnim sustavima; završni rad, FPZ, Zagreb 2015. [13]
14. Cimato S, Gamassi M, Piuri V, Sassi R, Scotti F. Privacy in biometrics. University of Milan, Department of Information Technologies. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.649&rep=rep1&type=pdf (pristupljeno: kolovoz 2018.) [14]

15. International Biometrics Identity Association. Recent Opinion Surveys on Public Perceptions of Biometrics.
URL: https://www.ibia.org/download/datasets/3372/Public-Perceptions-of-Biometrics-opinion-surveys%20.pdf (pristupljeno: kolovoz 2018.) [15]
16. Uredba (EU) 2016/679 Europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). URL: http://azop.hr/images/dokumenti/626/opca-uredba.pdf (pristupljeno: kolovoz 2018.) [16]
17. Thomson Reuters Practical Law. Data protection in the United States: overview.
URL:https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1&comp=pluk (pristupljeno: kolovoz 2018.) [17]
18. International Comparative Legal Guides. Data Protection 2018, USA.
URL:https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#chaptercontent18 (pristupljeno: kolovoz 2018.) [18]
19. ICAO. Machine Readable Travel Documents, Seventh Edition, 2015.
URL:https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf (pristupljeno: kolovoz 2018.) [19]
20. Schiphol. URL: https://www.schiphol.nl/en/privium/ (pristupljeno: kolovoz 2018.) [20]
21. U.S. Customs and Border Protection. URL:https://www.cbp.gov/travel/biometrics/air-exit (pristupljeno: kolovoz 2018.) [21]
22. Independent.
URL:http://www.independent.co.uk/travel/news-and-advice/airport-biometrics-trial-face-recognition-klm-brisbane-sita-a7813271.html (pristupljeno: kolovoz 2018.) [22]
23. Emirates Identity Authority.
URL: https://www.ica.gov.ae/en/media-centre/news/2012/11/4/iris-scan-prevented-entry-of-20000-deportees-into-uae-director-general-of-abu-dhabi-police-central.aspx (pristupljeno: kolovoz 2018.) [23]

Popis slika

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

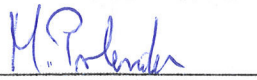
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Biometrijska identifikacija putnika u zaštiti zračnog prometa**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 3.9.2018



(potpis)