Jadranka Stojanović[1]

UDK 351.755.62:57.087.1
DOI 10.7251/ERB2214138S
Originalni naučni rad

BIOMETRIJSKE METODE IDENTIFIKACIJE OSOBA PREKO OTISKA PRSTA, LICA I DUŽICE OKA

Sažetak

Opšte je poznato da ljudsko tijelo od rođenja nosi informacije koje su jedinstvene i specifične za svakog pojedinca. Takve informacije su: otisak prsta, geometrija šake, dužica ili mrežnjača oka, raspored vena ili glas te nekih obilježja čovjekovog ponašanja npr, hoda, potpisa, dinamike kucanja na tastaturi. Biometrija je nauka koja se bavi ispitivanjem tih karakteristika i osobina sa ciljem potvrde identiteta neke osobe i polako postaje vodeća tehnologija određivanja identiteta. Ali i pored svojih brojnih prednosti, biometrija sa sobom nosi mnoga ograničenja i probleme vezane za bezbjednost kao i privatnost pojedinaca.

Ovim radom, autor je nastojao da predstavi osnovne tehnike za identifikaciju korisnika koje su zasnovane na karakteristikama, otiska prsta, lica i dužice. Opisan je proces registacije biometrijskih podataka, objašnjena je njihova identifikacija koja se koristi i u elektronskom poslovanju. Definisana je uspješnost identifikacije na osnovu grešaka. Pri tom je ukazano na moguće probleme prilikom kreiranja takvih baza biometrijskih podataka.

Ključne riječi: biometrija, identifikacija, verifikacija, otisak prsta, lice, dužica.

BIOMETRIC METHODS OF IDENTIFICATION OF PEOPLE THROUGH FINGERPRINT, FACE AND IRIS OF THE EYE

Abstract

It is common knowledge that the human body from birth carries information that is unique and specific to each individual. Such information is: fingerprint, geometry of the hand, retina or retina of the eye,

[1] e-mail: s.jadranka70@gmail.com, master opšte bezbjednosti, Doboj.

arrangement of veins or voice, or some features of human behavior such as walking, signature, typing dynamics. Biometrics is the science that examines these characteristics and properties for the purpose of verifying a person's identity, and is slowly becoming the leading technology in determining identity. But despite its many advantages, biometrics brings with it many limitations and problems related to the security and privacy of individuals.

With this work, the author sought to present basic techniques for identifying users based on characteristics, fingerprint, face, and plume. The process of registering biometric data is described, their identification, which is also used in e-commerce, is explained. Error-based identification success is defined. It pointed out possible problems when creating such biometric databases.

Keywords: biometrics, identification, verification, fingerprint, face, iris.

UVOD

Pitanje svih mogućih aspekata razlikovanja, prepoznavanja i identifikacije javlja se još u dalekoj istoriji. U plemenskom sistemu prvobitne zajednice, nepodobne članove plemena koji su se ogriješili o plemenska pravila uz progon kao mjeru s vrlo izvjesnom smrtnošću (nije se moglo preživjeti sam, bez vatre hrane, i lovačke opreme), određivalo se i označavanje istih sakaćenjem, ožiljcima ili žigosanjem, kako bi svi znali da se radi o prognaniku, pa ga obično nakon što je prepoznat kao takav, nije prihvaćalo i drugo pleme. Poznati su i slični načini označavanja ubojica, lopova i nemoralnih u srednjevjekovnoj Evropi, ali i širom svijeta.

Pojedine metode identifikacije koristile su se i u *humanije* svrhe, pa je poznato da su u pisanim dokumentima Asiraca i Babilonaca kao znak pisca i dokaz autorstva na dokument otiskivani otisci papilarnih linija prsta (tzv. Supur), a još stari Kinezi datiloskopirali su novorođenčad kako bi izbjegli zamjenu djece. U novom vijeku a posebno razvojem humanističkih i prirodnih nauka došlo je do procvata brojnih metoda koje su trebale pridonijeti identifikaciji, prepoznavanju i razlikovanju određenih osoba. Prije svega radi se o apliciranju medicinskih nauka u području kriminalističke identifikacije osoba traseološkoj identifikaciji[2].

[2] Subotić, O., (2007), *Biometrijski sisitemi identifikacije,* (kritička studija), Institut za političke studije, Beograd.

Savremeni kriminalitet, međunarodni terorizam, takođe je u znatnoj mjeri determiniran naučno-tehnološkom savremenošću, jer učinioci pri činjenju krivičnih dijela, međunarodni teroristi, sve češće pribjegavaju sofisticiranim metodama i tehnikama rada, te pri tom primjenjuju najmodernija sredstva i pomagala. U ovoj eri, koja se može nazvati informatičkom, kompjuterskom ili digitalnom, spomenute tehnologije otvaraju potpuno novu stranicu u klasičnom poimanju nekih pojmova vezanih uz predmete krivičnog djela (sredstva činjenja, predmete na kojima je počinjeno krivično djelo, odnosno predmete nastale krivičnim djelom), materijalni dokaz *modus operandi*, kao i razne druge aspekte važne za kriminalistiku i bezbjednost.

Neke od klasičnih identifikacijskih metoda, koje su prema opštim karakteristikama biometrijske, dobivaju potpuno novo značenje i kvalitetu, doživljavaju svoje *remake* u informatičko-digitalnom okruženju. Naime primjenom modernih tehnologija iz domena elektrotehnike i računarstva, kroz savremene hardverske uređaje i softverske alate, neke svojevremeno kroz istoriju odbačene identifikacijske metode, doživljavaju svoj procvat i novu afirmaciju. To je posebno značajno u području antropološke identifikacije koja je zbog tehnološkog ograničenja tokom 20. vijeka gotovo napuštena osim u području sudsko-medicinskih ekspertiza.

1. DEFINICIJA BIOMETRIJE I PODRUČJA PRIMJENE

Biometrija se definiše kao tehnika o automatizovanim postupcima jedinstvenog prepoznavanja ljudi (autentifikacija) na temelju jednog ili više urođenih fizioloških (bioloških) obilježja ili obilježja čovjekovog ponašanja[1]. Biometrija prethodi događajima. U informacijskoj tehnologiji, biometrijska *autentifikacija* ili dokazivanje autentičnosti odnosi se na tehnologije koje mjere i analiziraju čovjekove tjelesne karakteristike, jednako kao i karakteristike ponašanja u svrhu autentfiikacije. Primjeri fizioloških karakteristika su otisci prstiju, mrežnjače i dužice oka, facijalni uzorci (uzorci lica), te mjere ruke (dlana i šake), dok primjeri karakteristika ponašanja uključuju vlastoručni potpis, te način i uzorke rukopisa. Za glas se pak smatra da je mješavina kako fizioloških tako i karakteristika ponašanja. Međutim, ostaje otvorena rasprava prema kojoj sva biometrijska obilježja dijele na fiziološki aspekt i aspekt ponašanja.

1.1.Istorijski razvoj biometrije

Dok u zemljama zapadne kulture biometrija nije bila u primjeni sve do kasnog 19-og vijeka, u Kini je bila u upotrebi još od 14-og vijeka. Poznato je da su kineski trgovci radili otiske dječjih dlanova i stopala na papiru, sa svrhom razlikovanja male djece[3]. Na zapadu, međutim, dugo vremena identifikacija se temeljila na saopštenjima svjedoka i primitivnim crtežima, što je bilo vrlo nepouzdano, sve dok 1883. godine francuski policijski službenik i antropolog Alphonse Bertillon nije razvio antropometrijski sistem (kasnije poznat kao *bertillonage*)[4]. Bio je to prvi precizni, naučni sistem koji je našao široku primjenu u identifikaciji kriminalaca i koji je zaslužan što je biometrija postala grana nauke. Sistem se bazirao na mjerenju širina i dužina glave i tijela, zapisivanju osobnih oznaka kao što su tetovaže ili ožiljci, te karakteristikama osobnosti.

Nakon uspješnog prepoznavanja 241 prestupnika 1884. godine Bertillonov sistem su odlično prihvatile policije Amerike i Britanije, sve dok njegove mane nisu postale očigledne – uglavnom problemi vezani uz različite postupke mjerenja, različite mjere dobijene mjerenjem istih karakteristika od strane različitih osoba i promjenjive mjere ljudskog tijela tokom godina. Sistem je sužavao izbor u potrazi za prestupnikom, ali nije davao tačan rezultat. Nakon toga, policije zapadnog svijeta okrenule su se postupcima koji koriste otiske prstiju, a koji su u osnovi postupci koji su u upotrebi u Kini već stotinama godina.

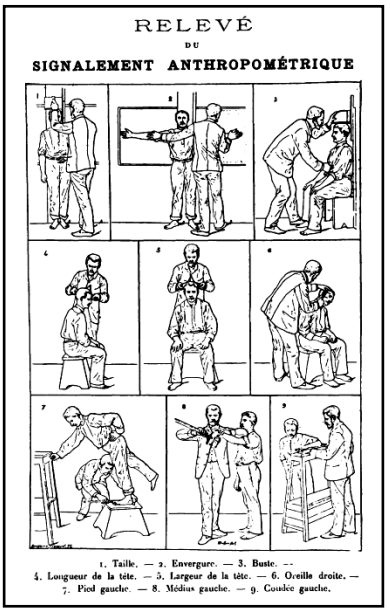
U zadnje vrijeme biometrija je poprilično odmakla od jednostavnog uzimanja otisaka prstiju. Danas se vrše mnoga različita fiziološka mjerenja i mjerenja ponašanja. Uopšte, upotreba biometrije danas je u znatnome porastu čemu je najviše zaslužan porast terorističkih aktivnosti u svijetu, a samim time i odraz na bezbjednost civila u svakodnevnim manjim ili većim migracijama.

---

[3] https://sr.wikipedia.org/Biometrija, posjećeno 23. 09. 2021. g.

[4] http:// www.forensic-evidence.com/site/ID/ID_bertillion.html. posjećeno 23. 09. 2021. g.

Slika 1. Bertillonov antropometrijski sistem – preteča biometrije



Izvor: Bertillon – *Identification anthropometrique (1893)*

1.2.Primjena biometrije u svakodnevnom životu

U modernom svijetu, svijetu protoka informacija, globalnog kriminala i terorizma, pouzdano osiguranje je jedna od najpoželjnijih odlika. Bez kvalitetnog osiguranja ugrožene su svakodnevne aktivnosti: zaštita osobnih računara, telefona i internet radnji od neovlaštene upotrebe drugih osoba, zaštita motornih vozila, mašina i sličnih predmeta od neovlaštene upotrebe istih, sprečavanje krađa i krivotvorenja pri finansijskim transakcijama,elektronskim plaćanjem kreditnim karticama i putem interneta,omogućavanje pristupa radnim mjestima, skladištima, područjima povećane bezbjednosti, vojnim objektima i oblastima, nadzor pristupa obavljanju usluga javnog prijevoza, posebno u vazdušnom saobraćaju, provjera identiteta osobnih iskaznica, vozačkih dozvola, pasoša i sličnih dokumenata.

Značajan pokazatelj pri postizanju bezbjednosti je identifikacija osobe. Provjera mora biti brza, pouzdana, da ne zadire u tijelo osobe i primjerene cijene. Do sada provjera identiteta se vršila isključivo putem sigurnosnih kartica, lozinki, PIN-ova i vlastoručnih potpisa, međutim,

danas sve to postaje nepouzdano i vrlo ograničeno. Biometrija koja nudi jednostavno, pouzdano i povoljno rješenje pri provjeri identiteta i danas u praksi nalazi čitav niz primjena. Prva i vjerovatno i najrašireniija jest upotreba biometrijskog pasoša i lične karte, a u ovo informacijsko doba mnoge zemlje na velika vrata u službene dokumente uvode i biometrijske podatke, o čemu će govora biti pri kraju rada. Primjenu biometrijske tehnologije u bezbjednosnim sistemima nalazimo u čitavoj lepezi aplikacija i ljudskih aktivnosti kao što su: putni dokumenti (vize, pasoši/putovnice), pogranična kontrola (vazduh, kopno i more), bezbjednost vazdušnih luka (kontrola putnika, pristup zaposlenika), policijske službe (kriminalna i civilna provjera), kontrola pristupa i upravljanje raznovrsnim objektima, raznovrsni lični dokumenti, registracija glasača, elektronsko bankarstvo, investiranje i druge finansijske transakcije itd.

U uobičajenom biometrijskom sistemu osoba se registruje u sistem kada se od nje prikupi jedna ili više fizioloških osobina ili osobina ponašanja. Dobivene informacije tada se podvrgavaju obradi kroz numerički algoritam, te se na kraju kreira digitalni zapis dobijene biometrije. Ako sistemu pristupa novi korisnik njegove biometrijske osobine se tada po prvi put spremaju u bazu podataka.

Svaki slijedeći pokušaj registracije u svrhu korišćenja sistema zahtijeva ponovno očitavanje biometrije korisnika te usporedbu sa već poznatim digitalnim obrascem. Taj obrazac se tada u svrhu identifikacije uspoređuje sa već postojećima u bazi podataka[5]. Postupak pretvaranja prikupljene biometrije, u digitalni predlagač za usporedbu se vrši svaki put kada se korisnik pokušava registrovati pri ulasku u sistem. Tako na primjer, postupak usporedbe zapisa dužice obuhvata korištenje postupka određivanja *Hammingove udaljenosti*[6] dobivenih digitalnih podataka, koja je mjera sličnosti dva niza kodova dužice. Na primjer, dva identična niza kodova imaju Hammingovu udaljenost nula, dok dva potpuno različita imaju Hammingovu udaljenost jednaku jedan (matematički gledano). Prema tome, Hammingova udaljenost mjeri postotak različitosti kodova iz broja obavljenih usporedbi. U idealnom se slučaju korisnik loguje na sistem i približno sve njegove osobine se poklapaju sa onima u bazi podataka.

U slučaju da se neki drugi korisnik (koji se ne poklapa u potpunosti sa traženim osobinama) pokuša logovati na sistem, sistem neće dozvoliti

---

[5] Kolar-Gregorić T.: *Kriminalistička identifikacija osoba,* Krimark 9, Zagreb 2002, str. 3-5.

[6] Broj bitova koji se ne slažu između dva binarna vektora. Koristi se kao mjera različitosti

logovanje toj novoj osobi jer ne posjeduje biometrijske podatke potrebne za autorizaciju. Trenutno dostupne tehnologije imaju dosta različite vrijednosti greške jednakosti, koje variraju od niskih 60% do visokih 99.9%..

1.3.Registracija biometrijskih podataka[7]

Da bi se osoba mogla identifikovati, njene biometrijske karakteristike prvo se pohranjuju u bazu podataka. Pristupnik podnosi biometrijski uzorak uređaju te se, ovisno o tome koje se karakteristike traže od osobe (otisak prsta, slika lica, dužice…), prikuplja čitavi skup podataka koristeći prikladni senzor. Podaci se zatim pregledavaju, ako su nepotputni odbijaju se ili se daju daljnje instrukcije za poboljšanje kvalitete. Nakon toga se vrši ekstrakcija traženih osobina iz skupa podataka; podaci se kodiraju te se iz njih kreira referentni obrazac koji se koristi za buduću usporedbu. Veličina predloška je između 9 i 20.000 bitova, ali većinom manje od 1.000, što garantuje brzu usporedbu karakteristika.

Način prikupljanja, kodiranja i pohrane obrazaca ovisi o proizvođaču, ali danas se radi na kompatibilnosti uređaja raznih proizvođača. Obrazci se potom spremaju, što se može raditi najčešće na dva načina: decentralizovano (na čip karticu ili PC) i centralizovano (u bazu podataka, odnosno arhivu podataka/obrazaca).

Takođe, zbog promjena na tijelu nastalih tokom vremena potrebno je povremeno obnavljati obrazac da ne bi nastali problemi pri identifikaciji ili verifikaciji. Sam postupak registracije traje najviše desetak minuta, a kako kvaliteta registracije određuje i performanse autentifikacije, registracija se mora pažljivo implementirati i obaviti u pouzdanoj okolini.

1.4.Identifikacija[8]

Nakon registracije biometrijskih podataka u sistem, slijedi proces utvrđivanja identiteta osobe koja koristi biometrijski sistem pomoću ili metode identifikacije ili metode verifikacije. Za obje metode vrijedi podjela na 4 faze procesa: uzimanje uzorka, ekstrakcija obilježja, uspoređivanje i rezultat (podudaranje ili nepodudaranje). Proces identifikacije teče na slijedeći način: nakon što je obavljen proces registracije biometrijskih podataka u sistem, osoba podnosi probni uzorak sistemu na identifikaciju.

---

[7] Kolar-Gregorić T.: *Kriminalistička identifikacija osoba,* Krimark 9, Zagreb 2002, str. 3.

[8] Ibid. str. 4.

Sistem postavlja sebi pitanje: „Ko je ova osoba?“, te upoređuje uzorak sa svim pohranjenim obrascima u sistemu, odnosno vrši usporedbu na principu 1:N. Postoje dva tipa sistema za identifikaciju, **zatvoreni i otvoreni.**

Zatvoreni identifikacijski sistemi rade na principu identifikacije osobe čiji su biometrijski podaci registrovani u bazi podataka sistema, te se traži podudaranje rezultata.

Otvoreni identifikacijski sistemi su dizajnirani tako da potvrđuju nepostojanje biometrijskog referentnog obrasca osobe koja se želi identifikovati, te se traži nepodudaranje rezultata. Usporedbom biometrijskih podataka osobe sa svim referentnim obrascima iz baze podataka osigurava se, da se ta osoba ne može korištenjem lažnih dokumenata registrovati pod više vlastitih identiteta.

1.5.Verifikacija[9]

Nakon procesa registracije korisnik unosi svoj identitet u sistem (preko tipkovnice ili putem kartice). Sistem zatim uzima skenirani biometrijski uzorak, te generiše probni obrazac baziran na algoritmu proizvođača. Nakon toga vrši se uporedba na principu 1:1[10], odnosno sistem upoređuje probni obrazac, sa prije spremljenim referentnim predloškom istog korisnika, te se traži podudaranje.

Verifikacijski sistemi mogu sadržavati od nekolicine do nekoliko milijuna registrovanih obrazaca, ali zbog činjenice da uvijek utvrđuju podudarnost s referentnim obrascom jedne osobe (što čine za manje od 1 sekunde) to im daje prednost pred identifikacijskim sistemima koji su znatno sporiji, kada je broj referentnih obrazaca u bazi podataka visok.

Međutim, jedan od nedostataka ove vrste sistema je taj što korisnik prvo unosi svoj identitet u sistem prije čega može doći do zaboravljanja lozinke ili gubitka kartice.

1.6.*Prag odluke*[11]

Zbog prije spomenute unikatnosti svakog biometrijskog uzorka podudarnost nikada nije savršena, niti kod identifikacije niti kod verifikacije. Iz tog razloga se biometrijski sistemi konfigurišu tako, da donose odluke o podudarnosti ili nepodudarnosti, bazirano prema prije

[9] Ibid. str. 4
[10] Ibid. str. 4.
[11] Ibid. str. 5.

definisanom broju koji se naziva *prag odluke*, a koji ustanovljava stepen sličnosti između probnog i referentnog obrazca.

Nakon usporedbe generiše se rezultat koji predstavlja stepen sličnosti, te se taj rezultat uspoređuje s pragom za donošenje odluke o podudarnosti ili nepodudarnosti. Ovisno o spremljenom iznosu praga kod sistema za identifikaciju ponekad nekoliko referentnih obrazaca odgovara probnom, a odluka se donosi prema boljem rezultatu.

2. BIOMETRIJSKA METODA IDENTIFIKACIJE OSOBA POMOĆU OTISKA PRSTA

Identifikacija pomoću otisaka prstiju[12] počinje da se primjenjuje u 19-om vijeku, kada nekolicina naučnika publikuje radove na temu otisaka prstiju. Međutim, početak ove metode u smislu kriminalne istrage, te identifikacije sumnjivih osoba dešava se 1892. g. kada argentinski službenik hrvatskih korijena Ivan Vučetić, putem otisaka na mjestu zločina dokazuje krivnju sumnjivca u slučaju ubistva. Od tada je ova metoda napredovala, a dosadašnja istraživanja i pokusi govore da je identifikacija osoba pomoću otiska prstiju trenutno jedna od najpouzdanijih metoda identifikacije, a samim time i najrašireniji način provjere identiteta osobe.

Automatizovani sistemi su komercijalno dostupni još od 1970-ih, a još donedavno ova je metoda korišćena kao primarni dokaz na sudskim procesima u SAD-u. Fiziološki je otisak prsta konfiguracija *grebena* s porama koje dijele *doline*. Otisak prsta nastaje još pri razvoju embrija i ne mijenja se sa starošću, nego raste u svojem prvobitnom obliku i kad se završi rast osobe ostaje u svojoj veličini nepromijenjen. Još uvijek nisu pronađena dva identična otiska prsta, pa je prema tome opšte prihvaćena činjenica da je svaki otisak jedinstven za svakog pojedinca.

Danas postoje čitave baze podataka otisaka prstiju koje se koriste uglavnom u kriminalnim istragama ili u najnovije doba - za bezbjednosnu kontrolu javnih objekata i službi. Najveća svjetska baza podataka otisaka prstiju i kriminalne prošlosti je FBI-aev[13] IAFIS[14], koji je u novije doba

---

[12] Pavišić, B, Modly, D, Veić, P., (2006), *Kriminalistika 1,* Golden Marketing-Tehnička knjiga , Zagreb,
str. 159-180.

[13] FBI - Federal Bureau of Investigation - Federalni istražni biro

[14] IAFIS -Integrated Automated Fingerprint Identification System (Integrisani sistem automatske
identifikacije otiska prsta

povezan i s drugim nacionalnim i internacionalnim službama, te sadrži preko 50 milijuna otisaka prstiju i dosijea, subjekata kriminalne prošlosti i oko 1.5 milijuna otisaka prstiju civila.

2.1.Klasifikacija otisaka prstiju i tehnologija rada

Morfologija otiska prsta povezana je sa specifičnim električnim i toplinskim značajima kože. To znači da svjetlost ili električni napon možemo koristiti za evidentiranje slike otiska prsta. Tehnologija prepoznavanja otiska vrši ekstrakciju obilježja iz kopije koju su napravili pojedini grebeni na vrhovima prstiju. Otisci mogu biti **ravni i rolani.**

Ravni otisak zaprima jedino pritisak centralnog dijela, između vrha prsta i prvog zgloba, brže ga je i lakše skenirati, dok *rolani otisak* zaprima grebene s obje strane prsta i ima veću površinu za identifikaciju.

Bez obzira na vrstu otisaka uređaji za identifikaciju putem otisaka prstiju, kao i svi drugi, imaju svoj *hardware-ski* i *software-ski* dio. Dok se pod *software-skim* dijelom prije svega misli na čitav niz algoritamskih metoda za evidentiranje značaja otiska prsta, glavni dio *hardware-skog* dijela je skener. Skener zaprima sliku otiska prsta, te je pojačava i konvertuje u predložak. Ovisno o tehnologiji koja se koristi, skeneri mogu biti:

- ***optički*** - (slika sa tamnim grebenima i bijelim dolinama se konvertuje u digitalni signal)
- ***poluprovodnički kapacitivni*** - (niz piksela mjeri varijacije u kapacitivnosti između senzora i prsta, te se taj kapacitet konvertuje u osmobitnu crno-bijelu sliku),
- ***poluprovodnički temperaturni*** - (mjeri razliku u temperaturi za vrijeme kreiranja digitalnog uzorka),
- ***poluprovodnički senzori električnog polja*** - (stvaraju električno polje i pomoću niza piksela mjere varijacije u polju, kao posljedicu naboranosti kože prsta),
- ***ultrazvučni*** - (koristi zvukove visoke frekvencije, te mjerenjem akustične impedancije prsta uzima otisak).

Ultrazvučni, iako potencijalno najpreciziji, nemaju široku primjenu nego se najčešće koristi i najstarija tehnologija – *optička*. Za vrijeme konvertovanja otiska prsta u digitalnu sliku zbog prljavštine, posjekotina, ožiljaka, suvih i mokrih ruku, nastaje *šum*, u obliku šara ili tačkica koji iskrivljuje sliku. Postupkom pojačavanja šum se redukuje, a definicija grebena i dolina se pojačava. Tek mali postotak populacije (npr. neki muzičari, penjači…) imaju oštećene otiske prstiju, međutim taj

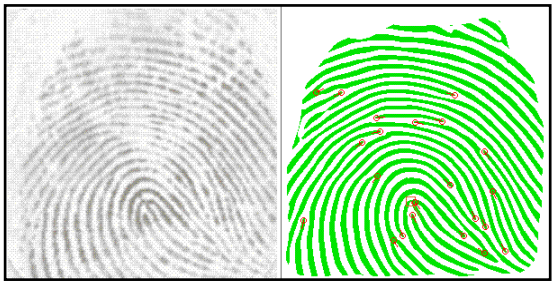
postotak je zanemariv i ne bi trebao predstavljati problem za identifikacijske sisteme u vazdušnom saobraćaju, koji koriste ovu metodu. Nakon što se dobije gotova digitalna slika otiska prsta izdvajaju se značajne karakteristike, koristeći neku od poznatih algoritamskih metoda.

Dvije su najraširenije metode identifikacije pomoću otisaka prstiju: metoda prepoznavanja *uzorka grebena* i metoda temeljena na izvodu *lokalnih karakteristika – minucija* (tačke gdje se crte otiska granaju ili završavaju).

Prva je metoda prepoznavanja otiska prsta uspoređivanjem s drugim, već poznatim otiscima, međutim, takva identifikacija nije preporučljiva jer se zbog oštećenja na prstima i uvjetima skeniranja često ne dobija tačan rezultat. Kada se govori o algoritmima koji se temelje na minucijama, treba početi od toga da je otisak prsta sastavljen od grubih karakteristika kao što su *vitice*, *krakovi* i *zavijuci*, te od sitnih karakteristika (minucija), a to su prije svega *bifurkacije* (račvanja), *delte* (spajanja u obliku slova Y) i *završetci grebena*.

Otisci, ako gledamo cijelu površinu prsta, sadrže oko 100 minucija, ali sam skenirani otisak najčešće između 30 i 40. Karakteristike koje se bilježe za svaku od njih je položaj (koordinate), tip (bifurkacija, delta ili završetak) i usmjerenost (orijentacija). Skup minucija daje uzorak za otiska prsta, a na kraju se dobija tablica sa specifičnim tačkama za svaki otisak prsta.

Slika 2. *Primjer otiska prsta sa naznačenim karakteristikama*



Izvor: National Science and Technology Council, Biometric Tehnologgy and Standards Overview

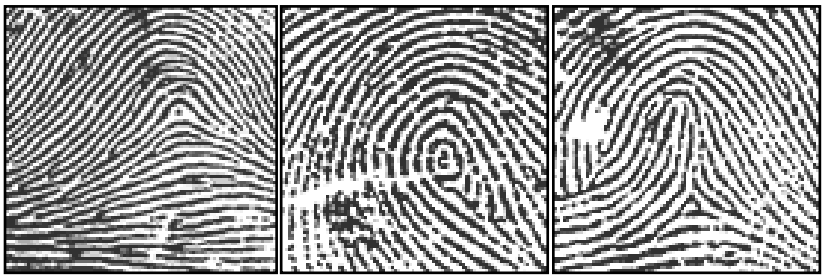
Prije kompjuterizacije, a da bi se olakšala obrada otisaka prstiju, otisci su klasifikovani prema opštim formacijama grebena, odnosno

globalnim karakteristikama otiska. Poznata su 3 sistema klasifikacije: *Roscher-ov (Njemačka i Japan), Vucetich-ev (Južna Amerika) i Henry-ev (Indija i zemlje engleskog govornog područja).* Prema *Henry-evoj* klasifikaciji (još uvijek aktuelna) postoje 3 osnovna uzorka grebena (globalne karakteristike): *luk, petlja* i *spirala* (slika 3.).

Zahvaljujući elektronskom evidentiranju slika i algoritmima za raspoznavanje uzoraka, danas je postupak obrade i pohrane u potpunosti automatizovan, a vrlo često i standardizovan (najviše korišten je standard koji propisuje američki NIST. Nakon što je izvršena grupacija i klasifikacija otisaka postupak identifikacije pojednostavljeno teče na sljedeći način:

1. pretvaranje otiska u digitalni oblik i uklanjanje šuma,
2. ekstrakcija lokalnih karakteristika koju obavlja algoritam proizvođača,
3. filtriranje uzorka,
4. klasifikacija, odnosno razvrstavanje na podgrupe radi ubrzavanja procesa,
5. usporedba (s grupom iz baze podataka ili podacima s kartice) i
6. pokretanje aktivnosti (dozvola ili zabrana prolaza).

Slika 3. *Primjeri glavnih tipova otiska: a) luk, b) spirala i c) petlja*



Izvor: www.dosi.zesoi.fer.hr

Male su razlike jedino između verifikacijskih i identifikacijskih sistema. Verifikacijski sistemi uspoređuju prvo susjednu i prvu sljedeću tačku, te ako su razlike male smatra se da se otisci podudaraju. Identifikacijski sistemi postupkom razvrstavanja, klasifikuju otiske prema njihovim globalnim karakteristikama, eliminišući tako ostale grupe, koje ne odgovaraju i zatim vrše uporedbu na principu 1:N.

2.2.Lažiranje otisaka prstiju

Jedan od potencijalno najvećih problema kada se radi o fingerprint tehnologiji[15] u bezbjednosti vazdušnog saobraćaja, je relativno laka mogućnost falsifikovanja otisaka prstiju, što bi moglo predstavljati metu za buduće napada, na ove sisteme u vazdušnim lukama. Kopija se može napraviti uz dobrovoljno sudjelovanje vlasnika ili bez nje - pomoću latentnih otisaka. Fingerprint tehnologija je, ako je uporedimo s drugim biometrijskim tehnologijama (dužica, slika lica…), podložnija mogućnosti pravljenja kopije bez znanja vlasnika.

Dobrovoljno je proces vrlo jednostavan – u toploj plastici ili vosku napravi se kalup, zatim iz njega i silikonski odljev. Bez znanja vlasnika ovaj proces je malo složeniji – otisak sa bilo koje glatke površine pokupi se, koristeći ljepljivu traku i grafitni prah. Otisak se skenira u visokoj rezoluciji, pročisti, te se zalijepi na materijal poput onog za matične ploče na kompjuteru i iz njega se izlije silikonski otisak.

Loša vijest za vazdušni saobraćaj je ta što je ova metoda, tzv. Matsumoto metoda, testirana na uređajima raznih proizvođača (Siemens, Sony, NEC…), te je zaključeno da je većinom uspješna bez obzira na vrstu senzora, te da danas nijedan od čitača nije u mogućnosti pouzdano razlikovati prst od dobro napravljene kopije, s toga proizvođači danas dosta pažnje posvećuju razvoju tehnologije bazirane na temperaturi, krvnom pritisku, pulsu ili provodljivosti kojoj to neće biti problem.

---

[15]**Fingerprint tehnologija (eng. *fingerprints*)** - Otisak prsta ili dermatoglifi je trag koji ostavljaju trenja i pritisc
površine ljudskog prsta na ravnim podlogama. Oporavak djelomičnih otisaka s mjesta zločina važan je metod
forenzičke nauke . Vlaga i masnoća na prstu rezultiraju ostavljanje otisaka prstiju na površinama poput stakla ili
metala. Namjerni prikazi cijelih otisaka prstiju mogu se dobiti tintom ili drugim tvarima koje se sa vrhova
rubova trenja na koži prenose na glatku površinu kao što je papir. Zapisi o otiscima prstiju obično sadrže otiske
s jastučića na zadnjem zglobu prstiju, mada službene kartice otiska prsta obično bilježe i dijelove donjih
zglobova prstiju. https://bs.wikipedia.org/wiki/Otisak_prsta - posjećeno 27. 09. 2021.

3. BIOMETRIJSKA METODA IDENTIFIKACIJE OSOBE POMOĆU LICA

Lice je najvažniji dio čovjekovog vanjskog izgleda pomoću kojega se ljudi međusobno razlikuju. Metoda identifikacije pomoću lica temelji se na činjenici da svako lice sadrži jedinstven skup karakteristika koje je moguće izmjeriti, te uporediti. Međutim, lice nije u toj mjeri jedinstveno kao neka druga fiziološka obilježja, (otisci prstiju, dužica…) i tokom godina se znatno mijenja, pa je i stepen pouzdanosti nešto niži, no, ako se koristi u kombinaciji s drugim tehnologijama dobija se jedan novi stepen pouzdanosti identifikacije što ovu tehnologiju čini konkurentnom u domenu bezbjednosti. Automatizovani sistem prepoznavanja lica relativno je nov koncept u biometrijskoj tehnologiji.

Rani, polu-automatizovani sistemi razvijeni su u 60-ima, a glavno obilježje im je bilo to da je administrator locirao karakteristike na licu (oči, uši, nos) koje su se zatim upoređivale sa zajedničkim referentnim podacima. U 70-ima naučnici Goldstein, Harmon i Lesk upotrijebili su 21 specifični subjektivni marker kao što su boja kose i debljina usana za automatizaciju sistema, međutim, mjerenja i lokalizacija su i dalje vršeni ručno.

Svojevrsna prekretnica se dešava 1988. g. kada naučnici Kirby i Sirovich uvode načelo analize komponenti - standardnu tehniku linearne algebre koja je pokazala da je potrebno manje od 100 vrijednosti za precizno kodiranje prikladno postavljene i normalizovne slike lica. Još jedan značajan pomak se dešava 1991. kada naučnici Turk i Pentland, s američkog MIT-a, uvode metodu tzv. svojstvenih lica, otkriće koje je omogućilo razvoj pouzdanih automatizovanih sistema prepoznavanja lica u stvarnom vremenu.

3.1.Analiza značaja lica i tehnologija rada

Tehnologija prepoznavanja lica podrazumijeva identifikaciju pomoću analize crta lica koje se ne mijenjaju tokom godina (gornje linije očnih šupljina, dijelovi oko jagodične kosti i usta…). Ova tehnologija može funkcionisati na način da upoređuje živi uzorak lica s pohranjenim uzorkom ili da uporedbu vrši pomoću digitalne fotografije iz pasoša. Inače, prepoznavanje lica koristi se i u identifikacijskim i u verifikacijskim sistemima. Kod procesa prepoznavanja lica, zahtjeva se prije svega kontakt sa skenerom tj. kamerom, za uzimanje uzoraka, stoga se prilikom implementacije ovih sistema može koristiti i već postojeća nadzorna oprema.

Ova činjenica čini ovu tehnologiju jedinstvenom budući da je ovo jedina biometrija koja se može koristiti osim za identifikaciju i za nadzor i praćenje. I ovdje vrijedi faza registracije biometrijski podataka prije identifikacije. Idealno bi bilo uzeti više fotografija iz više uglova radi bolje efikasnosti. Na ljudskom licu postoji oko 80 ključnih detalja: razmak očiju, širina nosa, dubina očnih udubljenja, jagodice,vilica, brada, itd. Ti ključni detalji se mjere (najčešće samo njih dvadesetak), te se formira numerički digitalni kod koji predstavlja lice u bazi podataka.

Proces identifikacije podijeljen je u faze:

1. **faza detekcije** (software pretragom niske rezolucije traži lice u polju vidljivosti. Kada se detektira oblik ljudske glave software prebacuje kameru na režim rada s visokom rezolucijom.),
2. **faza podešavanja** (određivanje pozicije, veličine i orijentacije glave, te pretvaranje 3D prikaza glave u 2D ne-frontalnu sliku i zatim u 2D frontalnu),
3. **faza kodiranja** (statička tehnika korekcije ili umanjivanja razlika u licu istog čovjeka na različitim slikama),
4. **faza kodiranja** (mjerenje i pretvaranje 2D frontalne slike u jedinstven digitalni kod za uporedbu.) i
5. **faza komparacije**

Dva su glavna pristupa problemu prepoznavanja lica: *geometrijski* (baziran na obilježjima) i *fotometrijski* (baziran na pogledu). Prvi, poznat i kao anliza lokalnih obilježja (LFA) koristi desetke slika za stvaranje uzoraka. Svaka slika sadrži specifične tačke, a njihovim preklapanjem dobivamo topografsku sliku lica sa udaljenostima između tačaka. Problem kod ove metode je što bilo koja promjena u izrazu lica može biti shvaćena kao specifična tačka što opet rezultuje neuspjelom identifikacijom.

Druga metoda, poznata pod nazivom *eigenface* ili svojstveno lice (slika 4.), danas je glavna metoda ove tehnologije i najviše je u upotrebi. *Eigenface sistem za prepoznavanje* sakuplja velik broj slika lica u bazu. Sistem kreira niz svojstvenih lica kombinacijom svih slika iz baze, te usporedbom zajedničkih karakteristika i različitosti među grupama slika lica pojedinaca. Svojstvena lica koje generiše sistem prikazuju se kao dvodimenzionalni niz svjetlo-tamnih područja u određenom uzorku.

Kada se lice prezentuje na identifikaciju, prvo se lociraju oči koje služe kao referentna točka da bi se locirala glava i standardizovala njena veličina. Sistem se potom usredotočuje jedino na lice, otklanjajući varijacije u svjetlosti i kontrastu koje uzrokuju okolina i kamere. Program zatim upoređuje karakteristike živog *eigenface uzorka* sa onima u bazi i određuje stepen podudaranja, te ako je isti dovoljan – sistem prepoznaje i

prihvata lice. Bilo koja osoba se može identifikovati uz pomoć 100-150 svojstvenih lica.

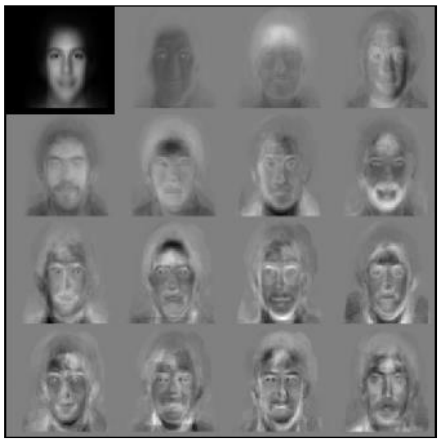
Do danas su razvijeni i mnogi algoritmi neophodni za funkcionisanje ovih sistema od kojih su tri najvažnija i najčešće spominjana:

- analiza glavnih komponenti (PCA),
- analiza linearne razlike (LDA),
- podudaranje uz pomoć elastičnog grupnog grafa (EBGM).

Kod PCA metode misli se prije svega na upotrebu svojstvenih lica, tehnika kojoj su začetnici bili *Kirby i Sirovich*. Kod ove tehnike tzv. *sondne* i *galerijske*[16] slike moraju biti iste veličine, normalizovane, što znači poravnanje očiju i usta subjekata unutar slike. PCA pristup zatim redukuje dimenzije podataka, te prikazuje najefikasniju niskodimenzionalnu strukturu facijalnih uzoraka. Ova redukcija dimenzija otklanja neupotrebljive informacije i precizno raščlanjuje facijalnu strukturu na pravokutne (nepovezane) komponente (svojstvena lica). Svaka slika se može prikazati kao vektor obilježja svojstvenih lica i koji su pohranjeni u jednodimenzionalnoj mreži. Srodna slika se uspoređuje sa slikom iz galerije mjerenjem udaljenosti između pojedinačnih vektora obilježja. PCA zahtjeva punu frontalnu prezentaciju lica, u suprotnom će rezultati identifikacije biti slabi. Prednost ove tehnike je u tome što se podaci za identifikaciju redukuju na 1/1000 prezentovanih podataka.

[16] Misli se na živi uzorak za identifikaciju i slike pohranjene u bazi za uporedbu.

Slika 4. *Standardna svojstvena lica – eigenfaces iz kojih se dobijaju vektori obilježja*



Izvor: National Science & Technology Council, *Biometrics Fundation Documents*, Biometric Overview

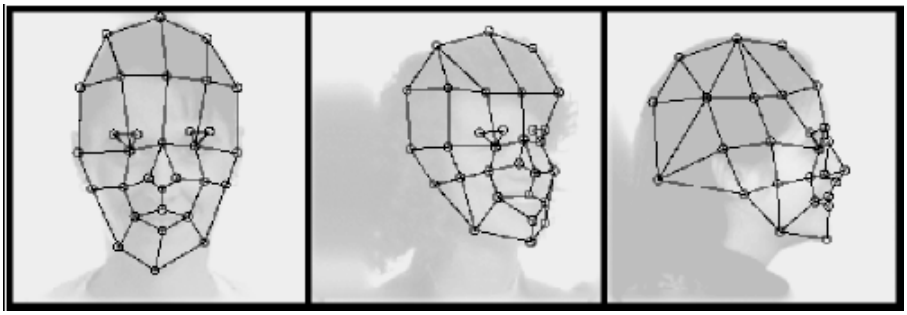
LDA je statistički pristup klasifikacije uzoraka nepoznatog razreda baziran prema *istreniranim* uzorcima poznatih razreda. Cilj ove tehnike je maksimizovati međuklasnu i minimizovati unutarklasnu različitost. Na slici 5. svaki blok slika predstavlja razred ili klasu; razlike među razredima su velike, ali unutar svakog razreda razlike su male. Problem kod ove tehnike se javlja kod analize visokodimenzionalnih facijalnih podataka – u usporedbi s dimenzionalnošću prostora relativno je mali broj istreniranih uzoraka za usporedbu.

Slika 5. *Primjer šest razreda (klasa) koristeći LDA metodu (algoritme)*

Izvor: National Science & Tehnology Council, *Biometrics Fundation Documents,* Biometric Overview

EBGM metoda oslanja se na koncept da stvarne slike lica imaju podosta nelinearnih karakteristika koje nisu zahvaćene metodama linearne analize spomenutim prije, kao što su varijacije u osvijetljenju, položaju glave ili izrazu lica. Inače, ova biološki bazirana metoda upotrebe *Gaborovih filtera* je proces koji se obavlja u vizualnom korteksu viših sisara. *Gaborova valna transformacija* kreira dinamičku arhitektonsku vezu koja projicira lice na elastičnu mrežu.

Slika 6. *Projekcija elastične mreže na lice kod EBMG metode*



Izvor: National Science & Tehnology Council, *Biometric Fundation Documents,* Biometric Overview

Gaborova amplituda je čvorište na elastičnoj mreži, označena krugovima na slici 6, koja opisuje ponašanje slike (oblika) oko zadanog piksela. Ona predstavlja savijanje slike uz pomoć Gaborovog filtera, koji se koristi za detekciju oblika i ekstrakciju obilježja za vrijeme procesuiranja slike. Prepoznavanje se bazira na sličnosti odgovora Gaborovog filtera kod svakog *Gaborovog čvora*. Problem kod ove metode je zahtjev za preciznom lokalizacijom graničnog orijentira, što se može postići kombinacijom PCA i LDA metode.

3.2.3D prepoznavanje lica

Najnoviji pravac u kojem se kreće razvoj nove generacije biometrije je 3D prepoznavanje lica. U decembru 2004. g. američko Ministarstvo obrane u saradnji sa kompanijama Unisys i A4Vision uložili su 700.000 $ u projekt 3D sistema za prepoznavanja lica. 2005. godine In-Q-Tel, grupa koju podupire CIA (**!**)u saradnji s Motorolla-om ulaže 6 milijuna $ u software i opremu za 3D prepoznavanje lica kompanije A4Vision. Najveći problemi kod 2D identifikacije, kao što je već naglašeno, prije svega se odnose na nemogućnost kompenzacije kretanja i položaja osobe, te svjetlosnih uslova u kojima se obavlja identifikacija.

3D prepoznavanje koristi se obilježjima lubanjske strukture gdje je su kruto tkivo ili kosti najvidljiviji (zakrivljenja očnih šupljina, nos, brada) i koji se ne mijenjaju tokom vremena. 3D identifikacija predstavlja metodu dubinskog mjerenja gdje se facijalne krivulje i kutovi mjere na sub-milimetarskoj razini. Na preciznost ovih sistema ne utiče svjetlo, položaj i kretanje, te se mjerenje može obavljati čak i u mraku–noću, zbog upotrebe približno infracrvenih svjetlosnih projektora. Prepoznavanje je moguće gotovo i pod 90° i nije potrebna saradnja osobe, koja se želi identifikovati.

Problem se javlja kod usporedbe 3D uzoraka s 2D slikama iz baza podataka, međutim, A4Vision je razvio algoritme za prekrivanje 2D slika, otklanjajući nedostatke 2D baza podataka, stvarajući 3D predloške. Budući da se za uzimanje uzoraka, koriste raspoređene 3D kamere, uska je veza između njihove kvalitete i mogućnosti sistema[17]. Unatoč nespornoj kvaliteti i znatnom napretku u razvoju ove vrste biometrije ostaje otvoreno pitanje interesa tako moćnih organizacija kao što je Central Intelligence Agency-CIA[18], moralno-pravna pitanja u bližoj ili daljoj budućnosti, te moguća zloupotreba ovih sistema i ugrožavanja osnovnih ljudskih prava.

---

[17] Radmilović, Ž.., (2008), *Biometrijska identifikacija,* Zagreb, str. 172.
[18] CIA - centralna Istražna Agencija

3.3.Primjena tehnologije identifikacije pomoću lica

Iako trenutno najnepouzdanija, tehnologija identifikacje osoba pomoću lica nalazi svoju primjenu u nekima od najvažnijih svjetskih vazdušnih luka. Razlozi su kod svih isti – zbog činjenice da se osobni dokumenti, pa i kontrola ulaza u neke države već dugo vremena obavlja primarno uzimanjem fotografija, ljudi ove sisteme smatraju izrazito prihvatljivim. Vazdušna luka u Sydney-u je prva u svijetu uvela ove sisteme sa ciljem ubrzavanja kontrole pasoša i pojačavanja sigurnosti. 1.2 milijuna $ vrijedni SmartGate kiosci imaju mogućnost skeniranja fotografije na pasošu i elektronskog upoređivanja s licem osobe koja drži pasoš. SmartGate sistemi su se dokazali kao visoko precizni za vrijeme testiranja, te su zainteresovali i druge zemlje.

Berlinska vazdušna luka prva u Evropi je uvela i uvodi sisteme za prepoznavanje lica pod nazivom Zn-Face, sistemi se koriste za osiguranje osjetljivih područja vazdušne luke pohranjivanjem podataka registrovanog osoblja na smart karticu, sa već poznatim postupkom identifikacije i kontrole pristupa. Zn-Face omogućava višeslojna prava pristupa za svakog uposlenika, te nadogradnju i poboljšanje drugih sistema pri čemu sam sistem radi potpuno nezavisno i bez mana.

Osim svih standardnih prednosti koje ovi sistemi nude, još jedna od zanimljivih i korisnih pojedinosti je tzv. optička okretaljka koja pasivno broji osobe koje prolaze kroz vrata na kojima im je odobren pristup. Osoblje mora ulaziti pojedinačno, te se svaki prolaz registruje. Ovakvi sistemi se nalaze na vazdušnoj luci u Thunder Bay-u prvoj kanadskoj vazdušnoj luci koja je usvojila sisteme za prepoznavanje lica.

4. BIOMETRIJSKA METODA IDENTIFIKACIJE OSOBA POMOĆU DUŽICE

Biometrijska identifikacija osoba pomoću dužice predstavlja proces analize nasumičnih uzoraka dužice ljudskog oka, jedna je od najnovijih i najsigurnijih metoda identifikacije danas. Ovu metodu je iznimno teško prevariti, uzorak se relativno lako izuzima s fotografije, a šanse da dvije osobe imaju isti uzorak na dužici gotovo ne postoje.

1936. godine oftamolog Frank Burch predstavlja koncept korištenja uzoraka dužice za identifikaciju osobe. Ideju prepoznavanja dužice prvi su patentirali oftamolozi Alan Safir i Leonard Flom 1987. g., ali nisu znali kako tu ideju da računarski implementuju sve dok fizičar i računarski

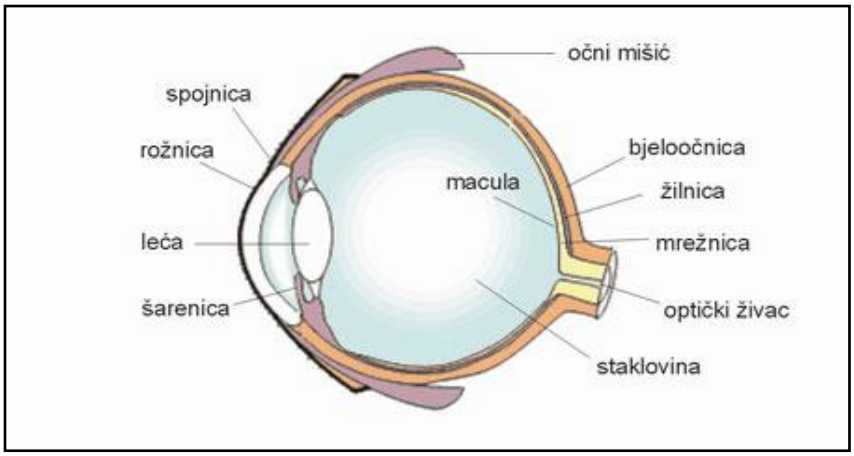
vizionar John Daugman sa sveučilišta u Cambridge-u, nije napravio prvi i najefikasniji algoritam za identifikaciju pomoću dužice.

Daugman je svoju ideju patentirao 1994. g. i danas se većina istraživanja na ovom području temelji na njegovim postavkama. Od 1995. g. su na tržištu dostupni prvi komercijalni sistemi, a Daugmanov algoritam je od 2006. g. osnova svih sistema koji se koriste metodom identifikacije osoba pomoću dužice.

4.1.Analiza karakteristika oka i tehnologija rada

Dužica je unutrašnji organ oka – najvažnijeg ljudskog osjetila, nalazi se u prednjem dijelu oka, ispred samog sočiva i jedini je unutrašnji organ kod čovjeka vidljiv izvana. Dužica je mišić unutar oka koji reguliše veličinu zjenice, odnosno količinu svjetla koje dopire u oko[19].

Slika.7. *Presjek oka*

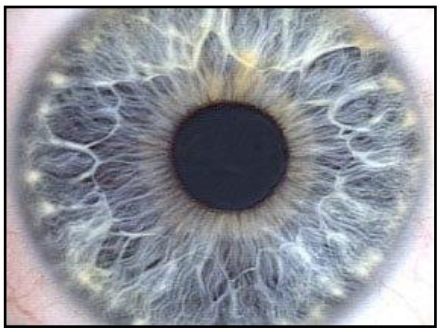


Izvor: www.optika - moni.com

Osim mišića za kontrolu širine zjenice dužica se sastoji i od *kromatofora* i *melanocita*, te pigmenta. Rezultat kombinacije svega toga je niz linija i uzoraka koji svakoj dužici daje jedinstven izgled[20].

[19] Krmpotić-Nemanić, J.: (1980), *Anatomski atlas,* Jugoslovenska medicinska naklada, Zagreb, str. 358.
[20] Ibid. str. 359.

Slika 8. *Izgled dužice ljudskog oka*



Izvor: www.accessexellence.org

Na dužici se nalazi oko 200 tačaka za identifikaciju, a uzimanje uzorka se vrši skeniranjem sa udaljenosti od 10 cm do 100 m. Razlog tome je refleksija svjetla koja nastaje kao posljedica vlažne i prozirne opne iznad dužice. Za uzimanje se koriste visokokvalitetne digitalne CCD kamere. Jedna od negativnih strana je ta, što nekim ljudima jednostavno nije ugodn bilo kakav pa i svjetlosni kontakt s okom. Uređaj najčešće glasovno navodi korisnika na pozicioniranje i u pravom trenutku uzima uzorak.

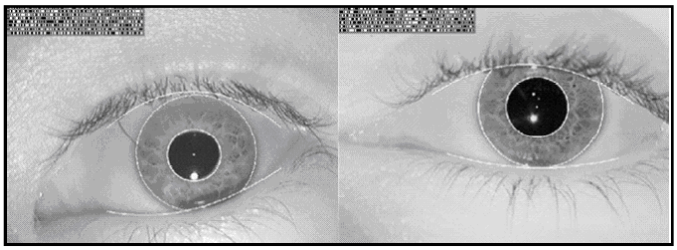
Današnji sistemi koriste prvo infracrveno svjetlo za osvjetljenje dužice i izdvajanje karakterističnih detalja dužice a da pri tome ne štete oku niti uzrokuju nelagodu subjektu na identifikaciji, a potom i vidljivu svjetlost (kako bi se osiguralo da je predstavljeno oko ono od živog subjekta). Slike ne moraju biti velike razlučivosti, otprilike 480 x 640 piksela, te imaju paletu od 256 sivih nijansi što je jedna od prednosti ove metode jer takva oprema nije skupa. Za dobro prepoznavanje, radijus dužice trebao bi iznositi oko 70 piksela. Nakon uzimanja uzorka potrebno je sa slike izdvojiti samu dužicu budući da na identifikaciju utiču kapci, trepavice i ostali strani elementi (šum). Potrebno je pronaći središte zjenice i središte dužice koji se najčešće ne nalaze na istom mjestu, te radijuse zjeničnog i vanjskog ruba dužice[21].

Za pronalaženje radijusa i središta koristi se *Daugmanov integracijsko-diferencijalni operator*. Kada se ovi elementi pronađu, sličan postupak se provodi i za pronalaženje očnih kapaka. Slike na kojima se vidi

[21] Zjenica nema stalno kružni oblik i veličina joj se mijenja, a razlika u središtima dužiice i zjenice iznosi i do
20%.

manje od 40-50 % dužice smatraju se neupotrebljivima. Nakon što se dobije slika dužice i izdvoje nepotrebna područja slika se transformiše u koordinatni sistem čime se postiže efekt da na prepoznavanje ne utiče veličina zjenice i same slike.

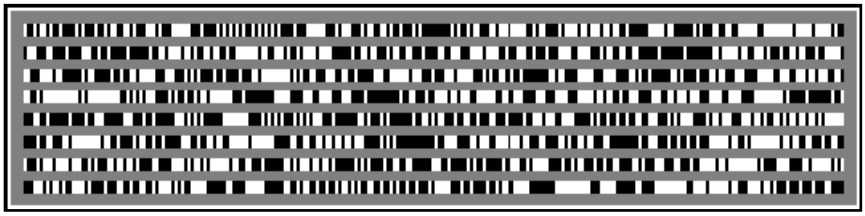
Slika 9. *Lokalizacija zjenice i dužice*



Izvor: National Science & Tehnology Council, *Biometrics Fundation Documents,* Biometric Overview

Za dobijanje tzv. *potpisa* ili *koda dužice* koriste se *dvodimenzionalni Gaborovi valni filteri* pomoću kojih se struktura dužice prikazuje kao niz vektora u kompleksnoj ravnini. Iz tih vektora se dobijaju 4 parametra: veličina, orijentacija i dvije pozicijske koordinate. Te vektorske karakteristike strukture dužice mogu se dobiti pomoću samo 256 bita, plus kontrolni bitovi (zbog mogućih smetnji ili slike lošije kvalitete). Kada se dobije potpis dužice upoređuje se s potpisima u bazi podataka i to jako velikom brzinom – do 1.000.000 uzoraka iz baze po sekundi.

Slika 10. IrisCode® - potpis dužice



Izvor: National Science & Tehnology Council, *Biometrics Fundation Documents,* Biometrric Overview

Uspoređivanje se radi tzv. *testom statističke nezavisnosti*. Svaki potpis dužice generisan iz bilo kojeg oka će proći na testu statističke nezavisnosti sa potpisom dužice bilo kog drugog oka. Za dobivanje rezultata na testu statističke nezavisnosti koristi se Hamming-ova[22] udaljenost. Ako Hamming-ova udaljenost pokaže da je manje od 1/3 bitova potpisa različito potpis pada na testu indicirajući da potpisi potječu od iste dužice. Prema tome, ključni koncept prepoznavanja dužice je, pad na testu statističke nezavisnosti.

4.2.*Nezavisna testiranja i vrijednosti grešaka*

Iz razloga što se dužica ne mijenja tokom godina i što ju je gotovo nemoguće krivotvoriti ovo je jedna od najpouzdanijih metoda identifikacije danas. Sistemi za prepoznavanje dužice ne mogu se prevariti nošenjem kontaktnih sočiva jer postoje algoritmi pomoću kojih se jasno vidi nosi li osoba sočiva ili ne. Stakleno oko ili pravo oko odstranjeno sa čovjeka, također ne mogu služiti za prevaru jer se na njima zjenica ne miče, dok je kod živog oka podložna stalnim kontrakcijama i širenju. Nemogućnost prevare ovih sistema očituje se prije svega zbog izrazito skupe opreme, ali i zbog činjenice da je potrebna saradnja osobe čiji se uzorak želi kopirati.

Godine 2005. američki NIST izvršio je prvu otvorenu nezavisnu procjenu tehnologije prepoznavanja dužice za masovnu upotrebu, pod nazivom ICE 2005[23]. Procjena je vršena prema modelu Face Recognition Vendor Test - FRVT[24] 2006. g., a sudjelovalo je 9 proizvođača iz 6 zemalja sa svojih 15 algoritama, te razne vladine i nevladine organizacije (FBI, DHS). Ciljevi ove procjene su bili omogućiti razvoj tehnologije prepoznavanja dužice i procijeniti trenutni status iste uz jednaku zastupljenost svih sudionika. Rezultati su bili najbolji što se tiče biometrije uopšte do tada. FAR odnosno FMR idu gotovo do nevjerojatnih 0% (0,0001 i manje) dok je FNMR ~ 1%. Ovako visoka pouzdanost ide u veliku korist implementaciji ove vrste biometrijske tehnologije u vazdušnom saobraćaju na svjetskoj razini.

---

[22] Hammingova udaljenost - je imenovana po Richardu Hammingu, koji ju je uveo u svom fundamentalnom radu
o kodovima detekcije i ispravljanja grešaka.

[23] https://www.nist.gov/programs-projects, posjećeno dana 02. 11. 2021. g.

[24] Face Recognition Vendor Test (FRVT) - Test dobavljača prepoznavanja lica

4.3.Primjena tehnologije prepoznavanja dužice

Svakako najbolji primjer primjene ove vrste tehnologije su Ujedinjeni Arapski Emirati. Naime, svih 17 pomorskih, kopnenih i vazdušnih luka, ulaza u zemlju od 2003. g. su osigurani sistemima prepoznavanja dužice i to je najveća takva primjena danas u svijetu. Svaki dan se izvrši oko 7.000 skeniranja, do sada ih je izvršeno preko 10 milijuna, a uhapšeno je oko 70.000 osoba s liste sumnjivih. Biometrija je postala ključni element identifikacijskih sistema policijskih i bezbjednosnih službi u cijelom svijetu, pri čemu je za istaknuti najveća baza otisaka prstiju na svijetu IAFIS. Kod sistema s velikim bazama podataka verifikacijski sistemi zbog znatno veće brzine rada imaju prednost pred identifikacijskim sistemima što je od važnosti za protočnost na terminalima koji će se u budućnosti koristiti biometrijom. Niske vrijednosti pogrešaka ovih sistema garantuju visoku pouzdanost pri identifikaciji ili verifikaciji. Vrijednosti pogrešaka i vremena potrebnog za pojedine radnje vezane uz biometrijske sisteme u stvarnim uvjetima nešto su veća nego što propisuju proizvođači ili što pokazuju nezavisna testiranja, čemu se treba posvetiti više pažnje u budućnosti. Investicije i kapitalna ulaganja u biometriju dostigli su vrtoglave cifre gotovo preko noći, pa se danas govori o multibilijunskom tržištu biometrijskom tehnologijom.

Nezavisna testiranja garantuju kvalitetno tržište biometrijskom tehnologijom. Podizanje razine pouzdanosti i efikasnosti biometrijskih sistema postiže se na nekoliko načina: kombinacijom s osobnim predmetima (smart kartice, biometrijski pasoši…) dobija se nova razina kvalitete identifikacije, biometrija sama za sebe ne može funkcionsati ni egzistirati, stoga mora biti upotpunjena kvalitetnim i osposobljenim kadrovskim sistemom i bezbjednosnim osobljem, te unapređenim sistemima kontrole putnika i prtljage (CAPPS, poboljšani rendgenski sistemi, detekcija hemijskih tragova…), internacionalna, regionalna i međusektorska kooperacija i saradnja službi, od iznimne je važnosti za efikasnost provjere putnika i izdvajanja sumnjivih i traženih osoba, razina efikasnosti biometrijskih sistema i bezbjednosnog menadžmenta mora biti kontrolisana kroz redovne i temeljite ICAO[25] programe provjere i nadzora.

[25] International Civil Aviation Organization ICAO – Organizacija međunarodnog civilnog vazduhoplovstva,
osnovana 1947 sa sjedištem u Montreal, Canada.

5. BIOMETRIJSKI PASOŠI

Biometrijski podaci pohranjeni u ličnim dokumentima nisu novost. Brazil, još od početka 20-og vijeka koristi lične karte/iskaznice sa biometrijskim podacima vlasnika. Podaci su pohranjeni u 2D bar kodu, na ličnoj karti/iskaznici i sastoje se od fotografije u boji, vlastoručnog potpisa, dva otiska prsta i drugih osobnih podataka. Brazil je i prva država koja je započela i s primjenom biometrijskih pasoša, koji sadrže fotografiju, potpis, i 10 otisaka prstiju. Danas većina svjetskih država primjenjuje biometrijske pasoše. Zemlje Evropske Unije (EU), su dogovor o uvođenju biometrijskih pasoša donijele 2004. godine, a od 2006. dostupne su svim članicama. Njemačka je prva zemlja u Evropi koja je uvela biometrijske pasoše za svoje građane. Pasoši pod nazivom *ePass sadrže digitalnu fotografiju i dva otiska prsta*. Osim digitalne slike za prepoznavanje lica za pohranu podataka upotrebljava se čip najčešće dovoljno velik za dodatne podatke koji bi se mogli pohraniti u budućnosti.

Neizostavno i ovdje su se javili problemi. Njemački stručnjak za elektronsku bezbjednost *Lukas Grünwald*[26] *obavijestio je sudionike jedne konferencije o bezbjednosti u Las Vegas-u da je* uspio za dva tjedna klonirati čip njemačkog pasoša, te podatke prebaciti u kopiju pri čemu se poslužio standardima koji su objavljeni na web stranici ICAO-a. Ista metoda bila bi djelotvorna i na pasošima drugih zemalja jer svi sadrže standarde ICAO-a.

Problem se javio, jer podaci pohranjeni na čipu nisu enkriptovani, pa ih može pročitati svako ko želi, a posjeduje opremu i znanje. Sami podati su ipak dobro zaštićeni i ne mogu se mijenjati, a da to pri kontroli pasoša ne bude uočeno. Mnoge zemlje izrazile su zabrinutost, a stručnjaci za razvoj biometrijskih pasoša i ICAO ovome će morati posvetiti više pažnje da se otklone nastali problemi, iz bezbjednosnih razloga.

[26] https//www.it-zoom.de//it-director - interviju - posjećeno 10. 11. 2021. g.

ZAKLJUČAK

Razvoj biometrije naročito je porastao poslije terorističkih napada u Americi, 11. septembra 2001. g. kada su pooštrene kontrole na aerodromima i kada se javila potreba da se iz mase izdvoje potencijalni teroristi. Kako raste potreba za višim nivoima bezbjednosti, tako su i biometrijski sistemi sve manji, precizniji, pouzdaniji i brži, nalaze sve veću primjenu u svim djelatnostima gdje je neophodno nedvosmisleno utvrditi ili potvrditi identitet osobe. Ljudski faktor i dalje predstavlja osnovnu „rupu“ u bezbjednosti brojnih sistema: nemaštovite lozinke u vidu datuma rođenja, lozinke zaljepljene na papiru sa donje strane tastature, PIN-ovi na ceduljicama u novčanicima i sl. Biometrija eliminiše potrebu za pamćenjem lozinki, jer smo lozinka mi sami. Ono što je nekada predstavljalo osnovni trik u naučnofantastičnim filmovima, danas postaje uobičajena slika u državnim institucijama, na aerodromima tehnološko naprednog Zapada, a odskora i kod nas.

Svaka od tri navedene vrste biometrije ima svoje prednosti i nedostatke, iako se prepoznavanje dužice pokazalo kao najefikasnije, ali i najskuplje za instalaciju, što mogu priuštiti samo najbogatiji, sistemi za prepoznavanje lica nisu još dostigli razinu pouzdanosti da bi mogli funkcionisati zasebno, stoga dok ne dostignu zrelost za kvalitetnu upotrebu egzistiraju samo kao podrška drugim biometrijskim sistemima i bezbjednosnim metodama. Ni jedna od biometrijskih tehnologija, trenutno se nije pokazala bez greške u stvarnim uslovima.

Vrijednosti grešaka i vremena potrebnog za obavljanje pojedinih radnji, nešto su veće nego što propisuju proizvođači ili što pokazuju nezavisna testiranja, zato bi te nedostatke u budućnosti trebalo otkloniti da bi se naišlo na odobravanje od strane putnika.

Budući da je biometrijska tehnologija najuže povezana interakcijom čovjek-mašina, odnosno dugoročnom pohranom najosobnijih podataka, od iznimne važnosti je usaglašavanje državno-pravnih sa sociološko-etičkim aspektima, te izučavanje samih korisnika, odnosno građanstva i upoznavanje s ukupnom problematikom i procedurama. Iz istog razloga postoji opravdani strah građana zbog interesa i izravne umiješanosti vlada i bezbjednosnih službi (CIA) u razvoj i implementaciju ove tehnologije.

Biometrija je okrenuta strogo ka budućnosti, ima potencijal promijeniti sliku društva. Na odgovornima je da odrede na koji način.

LITERATURA:

- Agree Philip Edward,(2003) *Your face is not bar code*, Uniiversity of California, Los Angeles,
- Kolar Gregorić Tatjana, (2002), *Kriminalistička identifikacija osoba*, Krimark 9, Zagreb,
- Krmpotić Nemanić Jelena, (1980), *Anatomski atlas (svezak 1),* Jugoslovenska medicinska naklada Zagreb.
- Pavišić Berislav, Modly Duško, Veić Petar, (2006), *Kriminalistika 1*, Golden Marketing – Tehnička Knjiga, Zagreb.
- Radmilović Želimir, (2008), *Biometrijska identifikacija,* Zagreb Polic. sigur. (Zagreb), godina 17. (2008), broj 3-4, str. 159-180.
- Subotić Oliver (2007), *Biometrijski sistemi identifikacije (kritička studija),*Institut za političke studije, Beograd,
- Turk, A. Matthew Pentland P.Alex, (1991), *Face recognition using-eigenfaces,* Massachussets Institute of Technology

Internetski izvori:

- https://sr.wikipedia.org Biometrija
- https//www.it-zoom.de//it-director
- https://researchers,a-star.edu.sg
- https://www nise.gov/programs-projects
- www.accessexellence.org
- www.optika - moni.com
- www.dosi.zesoi.fer.hr
- www/beingfirst.com/meet-our-team/linda
- www.forensis-evidence.com /site/ID/ID/bertillion. html

Korišćeni stručni časopisi:

- Security and safety audits", Icao Journal, br. 6, 2002.
- Biometrics National Test Center, "Collected works 1997 – 2000", San Jose State University, august 2000.
- "Biometrics for Airport Access Control" – Guidance Package, 30. 9. 2005.
- National Science and Technology Council, "Biometrics Technology and Standards Overview"X
- National Science and Technology Coucil, "Biometrics Fundation Documents"

- Rick Smith, Ph.D., CISSP, "The Biometric Dilemma", 28.10.2001.