



B&B
VIŠJA STROKOVNA ŠOLA

Diplomsko delo višješolskega strokovnega študija
Program: Logistično inženirstvo
Modul: Vojaška logistika

BIOMETRIČNA TEHNOLOGIJA KOT ELEMENT VARNOSTI V LETALSKEM PROMETU

Mentor: Dr. Gregor Garb
Lektorica: Ana Peklenik, prof. slov.

Kandidatka: Nina Pogačnik

Kranj, september 2013

ZAHVALA

Hvala dr. Garbu za pomoč in nasvete pri izdelavi te naloge.

Zahvaljujem se tudi lektorici Ani Peklenik, ki je mojo diplomsko nalogo jezikovno in slovnično pregledala.

IZJAVA

»Študentka Nina Pogačnik izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom dr. Gregorja Garba.«

»Skladno s 1. odstavkom 21. člena Zakona o avtorski in sorodnih pravicah dovoljujem objavo tega diplomskega dela na spletni strani šole.«

Dne _____

Podpis: _____

POVZETEK

Diplomska naloga predstavlja biometrično tehnologijo, ki je namenjena in se uporablja za zagotavljanje varnosti v letalskem prometu.

Z rastjo potreb po zagotavljanju varnosti ter napredkom in razvojem biometrične tehnologije postajata ta dva pojma nerazdružljiva. Implementacija biometrične tehnologije je na letališčih po svetu različno intenzivna in uspešna. Vezana je predvsem na razvoj tehnologije in biološka odkritja unikatnosti človeških lastnosti. Tehnološki napredek biometrične tehnologije zagotavlja večjo gotovost pri varnostnih odobritvah na kontrolnih točkah in zmanjšuje možnosti prevar, kot je na primer prehajanje meje z ukradenimi potnim listom. Biometrična tehnologija, uporablja obširne baze podatkov z odvzetimi biometričnimi vzorci, v nekaj sekundah preveri, primerja in ne dopušča odstopanj. To jo določa kot element varnosti.

V nalogi je predstavljena različna biometrična tehnologija, razloženo je njeno delovanje in uporaba. Predstavili smo tudi praktične primere uporabe na večjih letališčih po Evropi, ki to tehnologijo s pridom uporabljajo.

KLJUČNE BESEDE

- biometrična tehnologija
- varnost
- letalski promet
- uporaba biometrične tehnologije
- letališča

ABSTRACT

Our diploma thesis presents biometric technology which is intended and used for ensuring safety in air traffic. With the growth of need in ensuring safety and on the other side achievements and evolution of biometric technology, these two concepts are becoming inseparable. Implementation of biometric technology on airports around the world is diverse with different intensity and success. It is bounded mostly on development of technology and biological discoveries of uniqueness in human features. Technological development guarantees greater certainty when it comes to security improvements in access controls. It also decreases possibilities of deception, for instance border crossing with stolen passport. Biometric technology uses wide bases of information with taken biometric samples compares the data in few seconds and does not allow exceptions and deviation. That defines biometric technology as element of safety.

We presented different biometric technology, explained operation and usage. We described practical usage on larger airports that use this technology on daily basis.

KEY WORDS

- Biometric technology
- Safety
- Air traffic
- Biometric technology usage
- Airports

KAZALO

1	UVOD	1
1.1	Predstavitev problema.....	1
1.2	Cilji naloge	1
1.3	Predstavitev okolja	1
1.4	Predpostavke in omejitve	2
1.5	Metode dela	2
2	BIOMETRIČNA TEHNOLOGIJA	3
2.1	Zgodovina biometrije.....	4
2.2	Identifikacija, verifikacija, avtentikacija	6
2.3	Algoritem.....	6
2.4	Točnost delovanja (FAR, FRR, EER)	7
3	LETALSKI PROMET	8
3.1	Zgodovina letalskega prometa	8
3.2	Letalski promet kot kritična infrastruktura v RS.....	9
3.3	Letalski promet v Republiki Sloveniji	10
4	PRSTNI ODTISI	13
4.1	Razvoj.....	13
4.2	Klasifikacija	14
5	OBRAZNA PREPOZNAVA	19
5.1	Razvoj.....	19
5.2	Lastnosti	20
6	PREPOZNAVA ŠARENICE	25
6.1	Razvoj.....	25
6.2	Lastnosti	26
7	BIOMETRIČNI POTNI LIST	28
7.1	Razvoj.....	28
7.2	Lastnosti	29
8	VAROVANJE OSEBNIH PODATKOV	32
8.1	Identifikacija kot grožnja zasebnosti in varnosti	34
8.2	Zakonska ureditev	35
9	UPORABA BIOMETRIČNE TEHNOLOGIJE NA LETALIŠČIH	38
9.1	IRIS na letališču Heatrow	39
9.2	Vrata Easypass na letališču Frankfurt	41
9.3	PARAFE na letališču Charles de Gaulle.....	44
10	ZAKLJUČEK	46
11	BIBLIOGRAFIJA	49

1 UVOD

1.1 Predstavitev problema

Letalski promet je pomemben za dobrobit državljanov v smislu prevoza dobrin in hitrega ter varnega transporta ljudi na zelene destinacije s poslovnim ali turističnim namenom. Letalska infrastruktura se uvršča med kritično, saj bi lahko koncentracije ljudi, ki so vsakodnevno zbrane na letališčih, in medijska odmevnost letalskih nesreč privabila napadalce. V letalskem prometu zato deluje tesno povezan sistem varnosti, katerega element je tudi biometrična tehnologija. Ta zagotavlja dokaj zanesljive rezultate identifikacij oseb, saj je avtomatizirana, faktor človeške napake je izključen. Problem biometrične tehnologije se pojavlja predvsem v varovanju osebnih podatkov, ki jo je v informacijski dobi težko zagotavljati, odrazi se lahko tudi v kraji identitete.

1.2 Cilji naloge

Cilj naloge je predstaviti letalski promet in zagotavljanje nemotenosti njegove infrastrukture. Predstavili bomo biometrično tehnologijo, ki se uporablja kot poglobitveni element za opravljanje pregledov, za selekcioniranje, komu je odobren vstop na varovana območja letališč, na splošno za zagotavljanje varnosti in kontrole. Opisati želimo nekaj konkretnih primerov uporabe biometrične tehnologije na letališčih, med katerimi bodo predvsem večja evropska letališča, ki so nam blizu, imajo dovolj sredstev in potrebo po uporabi biometrične tehnologije.

Cilji naloge so predstaviti, kaj pomeni varnost v letalskem prometu, ki predstavlja enega od dejavnikov kritične infrastrukture. Kaj je biometrična tehnologija? Katera biometrična tehnologija se uporablja za zagotavljanje varnosti v letalskem prometu? Katera biometrična tehnologija se uporablja na izbranem letališču? Kako je urejeno varovanje osebnih podatkov?

1.3 Predstavitev okolja

Raziskovano okolje predstavljajo letališča kot sestavni del letalskega prometa. Pod drobnogled smo vzeli predvsem večja letališča, ki potrebujejo, imajo in dnevno uporabljajo biometrično tehnologijo. To so letališča v Frankfurtu, Londonu, Parizu, ki se vsako leto uvrščajo v sam vrh po številu potnikov v letalskem prometu.

Letališča so zaprta območja, dostopna zaposlenim in varnostno preverjenim osebam, ki jim je bil odobren vstop. Vsi potniki v letalskem prometu so varnostno pregledani, poostreni nadzori na letališčih pa so le posledica tega, da se letališča in celoten letalski promet uvrščajo v kritično infrastrukturo.

1.4 Predpostavke in omejitve

Predpostavili smo, da se z razvojem biometrične tehnologije izboljšuje in poenostavlja izvajanje varnostnih pregledov in ukrepov v letalskem prometu.

Omejitve: biometrična tehnologija se uporablja na veliko področjih. Osredotočili se bomo predvsem na njeno uporabo v letalskem prometu. Omejitve predstavlja tudi dostopnost podatkov s področja varnosti, saj bi odprtost podatkov predstavljala luknjo v varovanju letalskega prometa. Omejitve predstavljajo tudi zbiranje, analiziranje in hranjenje osebnih podatkov.

1.5 Metode dela

Deskriptivna: opisali bomo obstoječe pojave, ki nam bodo služili kot teoretično izhodišče.

Primerjalna: na podlagi dostopne literature in osebnih opazovanj bomo praktično primerjali letališča in njihovo uporabo biometrične tehnologije za zagotavljanje varnosti v letalskem prometu.

Metoda združevanja: tematsko bomo združili izsledke različnih avtorjev.

Analitična metoda: podrobneje bomo preučili različne biometrične sisteme, nastanek, razvoj in uporabo.

Sekundarna interpretacija statističnih podatkov: zbrane statistične podatke bomo ponazorili z grafi.

Induktivno-deduktivna metoda: iz uporabe biometrične tehnologije v praksi na določenem letališču bomo sklepali o splošni uporabi.

2 BIOMETRIČNA TEHNOLOGIJA

Beseda biometrija je v uporabi od začetka 20. stol in se nanaša na področje razvoja statističnih in matematičnih metod analize problemov v biološki znanosti. Biometrija obdeluje podatke v bioloških vedah, v nalogi pa se bomo osredotočili predvsem na biometrijo kot vedo, ki posameznikove telesne in vedenjske lastnosti opazuje, preučuje in shranjuje za namene identifikacije.

»Sama beseda biometrija izhaja iz starogrške besede »Bios« (življenje) in »metron« (meritev). Poenostavljeno bi lahko rekli, da je biometrija ali biometrika, kot včasih tudi zasledimo, veda o načinih prepoznave ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnosti, ki jih imajo vsi posamezniki, so edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, DNK ter značilne drže.« (IPRS, 2013)

»Biometrija je veda o uporabi edinstvenih fizioloških značilnosti, s katerimi se lahko verificira identiteta posameznikov. Nanaša se na uporabo matematično-statističnih analiz bioloških karakteristik. Namen preiskovanja v biometriji, kot tudi drugih tovrstnih identifikacijskih postopkov, je torej najti individualnost znotraj splošnega. Vsak človek ima obraz, roke, prste. Raziskovanje teh splošnih človeških lastnosti pa je pot k medsebojnemu ločevanju oseb.« (Trapečar & Robek, 2003)

»Biometrija je veda o uporabi edinstvenih fizioloških in ali edinstvenih vedenjskih značilnosti, s pomočjo katerih se prepoznavna identiteta posameznikov. Nanaša se na uporabo matematično-statističnih analiz značilnosti.« (Anžič, 2003)

Biometrija je torej veda, ki se ukvarja s prepoznavo oseb na podlagi njihovih osebnih lastnosti. Te lastnosti so lahko fiziološke: višina in oblika postave, obrazne značilnosti (struktura obraznih kosti, razdalja med posameznimi deli obraza, npr. med očmi, med usti in nosom), odtisi papilarnih linij na prstih, dlaneh, stopalih, DNK, individualne karakteristike mrežnice in šarenice v očesu ali razlike v oblikah ušesnih školjk. Med fiziološke značilnosti lahko štejemo tudi prepoznavo na podlagi vonja, s katero se ukvarja odorologija. Vsi ljudje imamo vonj, ki je lahko bolj ali manj izrazit, posledica različnih življenjskih navad, rase, jemanje zdravil. Druge vrste lastnosti so vedenjske: gibanje, hoja, rokopis, glas. Za osebne lastnosti je značilno, da so razmeroma trajne, nespremenljive, nekatere pa tudi neponovljive in unikatne. Zapis DNK ni enak niti pri enojajčnih dvojčkih.

Prednosti biometričnih značilnosti so (IPRS, 2013):

- unikatne,
- neprenosljive na drugo osebo,

- ni jih mogoče pozabiti ali izgubiti,
- težko jih je kopirati ali ponarediti,
- lahko se uporabijo z vednostjo ali brez vednosti posameznika,
- posamezniku jih je težko spremeniti ali skriti.

Zbiranje podatkov za biometrično bazo podatkov ima svojo zgodovino.

2.1 Zgodovina biometrije

Pri ugotavljanju in umeščanju biometričnih metod v zgodovino si avtorji niso enotni, zagotovo pa so stare več tisoč let. Iz novejšega obdobja zgodovine je z vidika prepoznavne nedvomno zelo pomemben Alphonse Bertillon. Uradnik v pariški policiji je začel meriti telesne mere zapornikov in ugotovil, da se nikoli ne pojavljajo v enakih kombinacijah. Leta 1883 je sistem merjenja predstavil policijsko-varnostni javnosti in sprva doživel velik posmeh, kasneje pa je metodo uspešno uporabil v praksi. Fizična merjenja v njegovem sistemu prepoznave so vključevala mere lobanj, dolžine rok, prstov, podlakti idr. Policija je sprejela njegov sistem prepoznave, imenovali so jo »antropometrija« ali »bertijonaža« kot uradno metodo registracije storilcev kaznivih dejanj. Uvedel je tudi kriminalistično fotografijo (slikanje od spredaj in s profila) in opisni portret, kar je prispevalo k boljši identifikaciji oseb. Slabost antropometričnega postopka je v dolgotrajnosti in v površnosti uslužbencev (meritve so izvajali nenatančno).

Antropometrija predstavlja nekakšen uvod v iskanje vedno novih načinov identifikacije oseb in le nekaj let kasneje je v veljavo stopila daktiloskopija¹. Začetniki daktiloskopije so doživljalo podobno kot Bertillon posmeh in zavračanje. Prelomno delo na tem področju je izdal Sir Francis Galton, Fingerprints, pomembno pa je tudi odkritje Henryja Fauldsa, da je prstni odtis edinstven in opravi identifikacijo s primerjavo papilarnih² linij. Juan Vucetich, v Argentini živeči Hrvat, pri nas bolj poznan kot Ivan Vučetić, je prvi raziskal umor s pomočjo prstnega odtisa, izumil učinkovitejši sistem klasifikacije prstnih odtisov in ga opisal v knjigi Dactiloscopia Comparada. Ker je bila antropometrija sprejeta in poznana po vsem svetu, so se je dolgo oklepali in zavračali daktiloskopijo.

»Prstne odtise so poznali že v prazgodovinski dobi, vendar še do danes ni znano, ali so služili le za okras ali pa tudi kot podpis oziroma pečat na različnih, zlasti glinenih izdelkih.« (Maver, 2004)

¹ Daktiloskopija je veda, ki se ukvarja s kožnimi reliefi prstov (Maver 2004)

² Papila je brazdičasta vboklina, kapilarna linija, izboklina na povrhnjici prstov, dlani ali podplatov (Maver, 2004).

Identifikacijska vrednost daktiloskopije je zasnovana na dveh znanstveno in mednarodno priznanih dejstvih, to je, da ni dveh oseb s popolnoma enakimi prstnimi odtisi in da se ti ne spremenijo (razen po velikosti) od rojstva do razpada trupla.

Naslednja velika prelomnica na področju biometrične metode prstnih odtisov je bil razvoj in vpeljava sistema avtomatske identifikacije prstnih odtisov – AFIS. Računalniški sistem AFIS je uredil daktiloskopsko zbirko, olajšal primerjavo in shranjevanje. Izdelan in razvit je bil leta 1974 v podjetju Printrak, prvi pa ga je začel aktivno uporabljati FBI. Omogoča daktiloskopske primerjave odtisov papilarnih linij z daktiloskopsko zbirko.

»Na področju obrazne prepoznave je zarisal temelje Francoz Eugene Francois Vidocq. Vidocq je bil kriminallec, ki je najprej ponudil policiji svoje usluge kot vohun. Z dobrim poznavanjem kriminalnega podzemlja Francije je leta 1811 prevzel vodenje »Brigade de Surete«, prve kriminalistične policije na svetu. Uvedel je posebne metode delovanja policije, tajne sodelavce, z vidika biometričnih metod pa je pomembna njegova parada prepoznavanja. Njegovi policisti so obiskovali jetnišnice in opazovali zapornike, da bi si jih zapomnili.« (Geringer, 2003)

»Prava biometrična tehnologija se je začela pojavljati v drugi polovici 20. stol in sovpada s pojavom računalniških sistemov. Razvijajoče področje je doživelo eksplozijo aktivnosti leta 1990 in se začela odražati v vsakodnevni uporabi aplikacij leta 2000.« (Biometrics history, 2006)

»Prvi polavtomatski program obrazne prepoznave so ustvarili Woody Bledsoe, Helen Chan Wolf in Charles Bisson 1960. leta. Njihov program je zahteval administratorja za lociranje oči, nosa, ušes, ust na fotografiji. Potem je izračunal razdaljo in razmerja skupne referenčne točke in jo primerjal z referenčnimi podatki.« (DuVal)

Biometrična obrazna prepoznavna je vezana na razvoj računalniške tehnologije in je dokaj nova biometrična metoda. Računalniki dandanes že ponujajo slike obrazov visoke ločljivosti, 3D-skeniranje in izris obraza, ki so vsako leto neprimerno natančnejši.

Koncept in uporaba biometričnih metod imata svojo zgodovino. Znanstveno raziskovanje se pojavi v začetku 17. stoletja, se z avtomatizacijo v 20. stoletju eksplozivno razmahne in vstopi v vsakodnevno uporabo.

2.2 Identifikacija, verifikacija, avtentikacija

Termini so medsebojno povezani, vendar imajo različne pomene in večkrat se zgodi, da jih uporabljamo na napačne načine. Identifikacija pomeni določanje osebe na podlagi njenih biometričnih podatkov. Identifikacijo lahko opravimo, ko imamo zbrano bazo biometričnih podatkov in jo primerjamo s trenutno zajetimi podatki. Sprašujemo se, kdo je ta oseba. Identične podatke iščemo med mnogo osebami v bazi, torej opravljamo primerjavo 1 : N oziroma »ena proti mnogo« (angl. one to many). Biometrične vzorce primerjamo z vsemi vzorci v bazi. V kolikor odvzet vzorec sovпада s katerim izmed vzorcev v bazi, dobimo identiteto, ime osebe, v nasprotnem primeru pa iskanje spodleti. Sistem identifikacije vedno vključuje centralno zbirko biometričnih podatkov, sistem avtentikacije pa ne nujno. Tipičen primer sistema identifikacije je iskanje storilcev kaznivih dejanj na podlagi npr. prstnih odtisov. Podatke o prstnem odtisu, najdenem na kraju zločina, vnesejo v sistem, ki jih nato primerja z vsemi že prej shranjenimi podatki. Če najde par, je oseba identificirana.

Pri verifikaciji se sprašujemo, ali je oseba res tista, za katero se predstavlja. Tu iščemo samo eno primerjavo, 1 : 1 – »ena proti ena« (angl. one to one). Ker že poznamo podatke osebe, le primerjamo odvzete vzorce s shranjenimi biometričnimi lastnostmi osebe v sistemu. Kot rezultat dobimo potrditev avtentičnosti osebe. Avtentikacija pomeni določanje osebe na podlagi njenih biometričnih podatkov in potrditev identitete, za katero se izdaja.

2.3 Algoritem

»Algoritem je navodilo, s katerim rešujemo nek problem. Običajno je zapisan kot seznam korakov, ki nas pripeljejo do rešitve problema. Kako podrobno razdelamo korake, je odvisno od tega, kdo izvaja algoritem (človek, računalnik). Če ga izvaja računalnik, potem govorimo o računalniškem programu.« (Wikipedija)

»V biometrični tehnologiji se opravlja odzemanje vzorcev in identifikacija strojno oziroma računalniško. Algoritem je določeno zaporedje navodil ali ukrepov, ki pove računalniškemu sistemu, kako rešiti določen problem. Biometrični sistemi imajo veliko algoritmov, npr. procesiranje slik, obdelave, primerjave.« (Biometrics history, 2006)

»Biometrični algoritem je torej zaporedje navodil, ki biometričnemu sistemu dajejo navodilo, kako po zaporedju korakov rešiti določen problem. Značilno je, da biometrični sistemi uporabljajo zaporedja pravil za razlago podatkov, ki so bili pridobljeni z danega vira. Npr. namesto da preučujejo celoten odvzet vzorec, biometrični sistemi vzamejo iz vzorca najbolj tipične lastnosti, ki najbolj diferencirajo lastnosti med dvema vzorcema. Algoritem ima določeno število

korakov in se uporablja v biometrični tehnologiji za določanje, ali se odvzeti vzorec in predloga ujemata.» (www.tecnovelgy.com)

2.4 Točnost delovanja (FAR, FRR, EER)

V nasprotju s klasičnimi metodami moramo pri biometričnih metodah upoštevati tudi verjetnost. Vsi senzorji, ki so v uporabi, so podvrženi šumom in napakam. Še večji problem pa predstavlja dober in robusten algoritem. Biometrične metode niso eksaktne. Na koncu se te omejitve stekajo k dvema pojmom: FRR – število lažnih zavrnitev (angl. false rejection rate) ter FAR – število napačne odobritve (angl. false acceptance rate).

»FAR predstavlja uspešno registracijo neavtoriziranega oz. neobstoječega uporabnika v sistemu. FRR pa pomeni neuspešno registracijo uporabnika z obstoječo avtorizacijo. Potrebno je narediti kompromis pri občutljivosti sistema. Če je sistem visoko občutljiv, dobimo majhne FAR vrednosti, zato pa toliko večje FRR. Za slabo občutljiv sistem pa obratno, takšen sistem sprejme skoraj vsakogar (FAR > FRR). Občutljivost lahko izberemo tako, da sta vrednosti FAR in FRR enaki, tej skupni vrednosti pravimo EER (angl. equal error rate). Manjša kot je vrednost EER, večja je točnost sistema. Pri aplikacijah, kjer dajemo prednost uporabnosti pred varnostjo (npr. hotelske sobe), se moramo sprijazniti z visoko FAR vrednostjo.« (Mraovič, 2006)

»Merilo verjetnosti, da bodo biometrični sistemi nepravilno zavrnili dostop pooblaščenega uporabnika. FRR število je navedeno kot razmerje med številom lažnih zavrnitev, deljeno s številom identifikacijskih poskusov.« (Bayometric inc., 2012)

3 LETALSKI PROMET

Letalski promet je najmlajša transportna panoga, saj se je dodobra razvila šele konec 20. stoletja. Predstavlja obliko prometne veje, ki zagotavlja eno temeljnih oblik prevoza ljudi in blaga.

Dandanes je osredotočeno predvsem na prevoze ljudi, prevoz blaga se opravlja istočasno ali pa z za transport namenjenimi letali. Zelo priročen je v dostopanju na bolj odročne kraje, ki so zaradi geografskih posebnosti težje dostopni. Letalski promet je postal zelo priljubljen v obdobju množičnega turizma, saj je s tovrstnim potovanjem mogoče hitro obiskati različne lokacije, in kar je najpomembneje, obenem prihraniti čas.

3.1 Zgodovina letalskega prometa

Zgodovina letalskega prometa se po vsej verjetnosti začne z mitološko zgodbo o Dedalu in njegovemu sinu Ikaru, ki sta z lastnoročno izdelanimi krili poskušala poleteti in pobegniti iz zapora. Do naslednje pomembnejše prelomnice v zgodovini letalstva je preteklo precej časa, pisalo se je leto 1903, ko je decembra bratoma Wright uspel polet z letalom na bencinski motor. Prvi let je trajal 12 sekund in je meril 36,5 metrov. Polet je bil prvi kontroliran polet z motorno napravo, težjo od zraka. V dokaz, da uspeh ni bil naključen, sta brata opravila še tri leta. Zadnji, četrti let, je trajal 59 sekund in je bil dolg 259,7 metrov. Njune iznajdbe so omogočile bliskovit razvoj zrakoplovov s fiksnimi krili, težjimi od zraka, čemur pravimo letala.

Naslednja pomembnejša prelomnica se je zgodila leta 1909, ko je Blériot s svojim letalom preletel Rokavski preliv in pristal v Angliji. Le nekaj let kasneje je bila ustanovljena prva letalska redna linija med Sankt-Peterburgom in Tampa na Floridi, z nastopom prve svetovne vojne pa so letala dobila praktično vlogo izvidništva.

Vojna je močno spodbudila razvoj letalske industrije, začela se je prava bitka za prevlado v zraku, izdelovali so vse več različnih modelov, med njimi so bili nekateri tudi primerni za prevoz vojakov. Vojake so po vojni zamenjali civilni potniki.

Letalski promet se je med vojnama bliskovito razvijal, letala so postajala zmogljivejša, omogočala so hiter prevoz tovora na daljše razdalje in postajala komercialno privlačna za potovanja. Do začetka druge svetovne vojne so imela skoraj vsa večja mesta svoja letališča, po koncu, leta 1945, pa je bilo prepeljanih že 9 milijonov potnikov. Med tem časom je zanimanje za letalski promet zaradi številnih nesreč nekoliko upadel, po drugi strani pa so v javnosti odmevali dogodki, kot je Lindberghov polet brez postanka čez atlantski ocean 1927, Smithov prvi polet čez Tihi ocean, leto kasneje prvi polet čez južni tečaj, kar je bilo letalstvu in celotni javnosti v ponos.

V petdesetih letih je letalska industrija doživela premierni let prvega reaktivnega potniškega letala De Havilland Comet. Kljub občutnemu skrajšanju časa potovanja, ki ga je doprineslo novo reaktivno letalo, so ga Britanci kaj kmalu umaknili iz prometa, saj so po dveh strmoglavljenih ugotovili pomanjkljivosti v konstrukciji. Američani so se iz njihove zgodbe veliko naučili in rezultat je bil Boing 707, ki je uspešno povezoval celine.

V šestdesetih letih se je letalstvo usmerilo v udobnejša in cenovno ugodna potovanja, kar je prekinila naftna kriza 1973. Letalske družbe so strategije usmerile v zniževanje stroškov in vpeljavo varčnih letalskih motorjev.

V zadnjih dvajsetih letih smo bili priča velikim spremembam v letalstvu, ki pa niso bile tehnične narave, saj so današnja letala precej podobna tistim izpred 30 let, bistveno pa se je spremenila sama storitev. Z uveljavljanjem nizkocenovnih prevoznikov so se potovanja z letalom začela približevati vožnji z avtobusom, temu primerne so tudi cene. Na trg zračnega prometa je začelo prihajati gibanje nizkocenovnih prevoznikov, ki v svojem poslovanju zajemajo le najnujnejše stroške in z nižjimi cenami vozovnic ponujajo svet na dlani tudi potnikom z nizkimi finančnimi prihodki. Nudijo osnovno storitev, to je prevoz s točke a na točko b. Letalske družbe rednih prevoznikov, največkrat nacionalnih, ki so uživali zlate čase trga brez konkurence in monopolne položaje, so bili prisiljeni v zniževanje cen vozovnic, kar vodi v zmanjšanje kakovosti storitve, za nekatere prevoznike pa je bila adaptacija celo neuspešna in so svoje poslovanje zaključili.

Nizkocenovni prevozniki ponujajo zgolj prevoz na določeno destinacijo, kakršne koli druge storitve je potrebno dodatno plačati. Plačati je potrebno npr. dodatno oddano prtljago, kakršnokoli pijačo in hrano, ki vam jo proti plačilu ponudijo člani kabinskega osebja med letom. Poleg tega stroškovna politika nizkocenovnih prevoznikov nudi časovnice samih poletov, ki niso najbolj po meri, pa še letališča, na katerih pristajajo nizkocenovni prevozniki, so običajno odročna oz. bolj oddaljena od mestnih središč. Morda bi nekateri letalski zanesenjaki dejali, da so nizko cenovne letalske družbe odvzele letalstvu del čara, ampak dejstvo je, da so letenje približali najširšim množicam, kar je verjetno njihov največji prispevek človeštvu.

3.2 Letalski promet kot kritična infrastruktura v RS

»Kritična infrastruktura predstavlja razvejano mrežo neodvisnih, večinoma v zasebni lasti, sistemov, zmogljivosti in procesov, ki s sinergijskim delovanjem zagotavljajo neprekinjeno proizvodnjo in distribucijo osnovnih dobrin in storitev in katerih uničenje ali okvara lahko povzroči hude posledice na javno zdravstvo, varnost, gospodarsko stanje, socialno blaginjo prebivalcev ali delovanje javnega sektorja.« (Garb, 2009)

»Kritična infrastruktura pomeni infrastrukturno zmogljivost, sistem ali njun del, ki se nahaja v državah članicah EU in je bistven za vzdrževanje ključnih družbenih funkcij zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij. Komisija kot kritično infrastrukturo določa tudi številne sektorje gospodarstva, tudi bančništvo in finance, promet, infrastrukturo, zdravstveno oskrbo, prehransko oskrbo, komunikacije in tudi državne službe. Našteti elementi kritične infrastrukture pomenijo omrežja in dobavne verige, ki podpirajo oskrbo s ključnimi proizvodi in tudi samo delovanje sektorjev.« (Direktiva sveta, 2008)

»Kritična infrastruktura je hrbtenica našega narodnega gospodarstva, varnosti in zdravja. Poznamo jo kot elektriko v naših domovih, vodo, ki jo pijemo, transport, ki nas premika, in komunikacijski sistem, na katerega se zanašamo, da ostajamo v kontaktu s prijatelji in družino. Kritične infrastrukture so sredstva, sistemi in mreže, bodisi fizično ali virtualno, tako vitalnega pomena, da bi njihova onesposobitev ali uničenje imelo izčrpavajoč vpliv na varnost, nacionalno gospodarsko varnost, javno zdravstvo in varnost oziroma katero koli njihovo kombinacijo.« (Homeland security)

»Kritično infrastrukturo si lahko predstavljamo kot mrežo neodvisnih, večinoma zasebnih, antropogenih sistemov in procesov, ki delujejo skupaj in s sinergijskimi učinki z namenom ustvarjanja in usmerjanja stalnega toka pomembnih dobrin in storitev. Torej gre za sisteme in sredstva, fizična ali navidezna, katerih onesposobitev ali uničenje bi imela določen učinek na nacionalno varnost v vseh njenih prvinah. Izhajajoč iz tega gre poleg same infrastrukture oziroma objekta tudi za storitve, ki jih infrastruktura nudi oziroma zagotavlja.« (Wiger & Dunn, 2004)

3.3 Letalski promet v Republiki Sloveniji

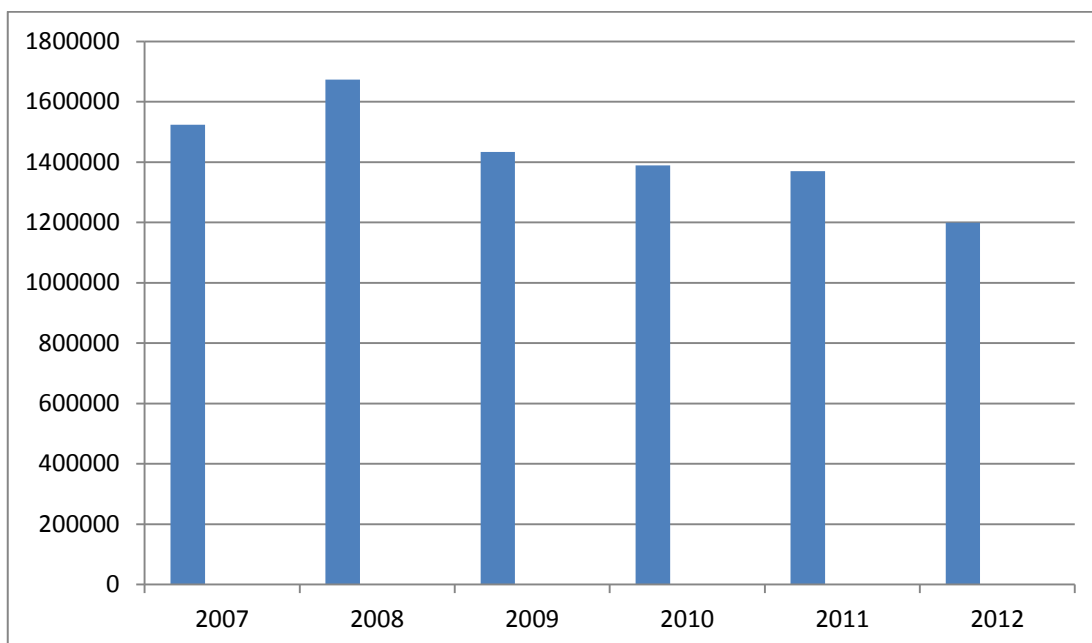
»Če umestimo Slovenijo kot članico EU, lahko povzamemo, da je majhna država z malo prebivalci in posledično malo letalskega prometa. Na ravni EU začasno zaprtje letališča Jožeta Pučnika ne bi imelo velikega vpliva. Vsekakor pa zaradi majhne količine objektov, ki lahko prenesejo večjo obremenitev letalskega transporta, pomen na ravni države ni majhen. Ti objekti namreč edini zagotavljajo nemoten letalski promet v Republiki Sloveniji.« (Pengal, 2008)

»Mednarodno civilno letališče Jožeta Pučnika Ljubljana je kritično zato, ker je edino veliko letališče v RS, kjer lahko pristajajo tudi največja letala. Je najboljše opremljeno tako za prevoz potnikov kot tovora in predstavlja glavno referenčno točko za večino letalskega transporta v Republiki Sloveniji. Njegova morebitna onesposobitev bi pomenila veliko neposredno in posredno gospodarsko škodo in šok za slovenski zračni promet ter edinega nacionalnega prevoznika Adrio Airways.« (Pengal, 2008)

Letalski promet in mreža objektov za njegovo izvajanje je v Sloveniji kljub njeni majhnosti dobro razvit. Imamo 2 večji civilni letališči, Letališče Jožeta Pučnika Ljubljana in Letališče Edvarda Rusjana Maribor. Poleg njiju so še manjše letališče v Portorožu, vojaško v Cerkljah ob Krki in še mnogo drugih, namenjenih privatnemu letalskemu prometu.

Letališče Ljubljana je s svojim obratovanjem začelo 24. decembra 1963, redni promet pa je stekel 9. januarja 1964. Vlada RS je junija 2007 sprejela sklep o preimenovanju letališča v Letališče Jožeta Pučnika po enem izmed akterjev osamosvojitve RS. Danes je eno izmed treh, vendar glavno in največje mednarodno letališče v Republiki Sloveniji. Ima strateško lego v središču Slovenije, saj je le 25 km oddaljeno od prestolnice in največjega mesta Ljubljane, do katerega nudi avtobusne povezave. Geografsko je dobro umeščeno med Alpami in Sredozemskim morjem, vmesna postaja med Balkanom in preostalo Evropo. Vsak dan odpravijo različne prevoznike, kot so Air France, Finnair, Turkish Airlines, nizkocenovne Easyjet, Wizzair, največ letov pa opravi slovenski nacionalni prevoznik Adria Airways. Adria je leta 2012 od 1,2 milijona prepeljanih potnikov prepeljala približno milijon.

Na potniškem terminalu najdemo več prijavnih okenc za potnike, kjer oddajo tudi prtljago. Potniki prečkajo varnostno kontrolo, kjer stopijo skozi detektorje kovin, njihova ročna prtljaga pa potuje skozi rentgen za natančnejši pregled. Ko prestanejo varnostno kontrolo, potniki lahko nakupujejo v brezcarinskih prodajalnah ali pa čakajo na izhodih na vkrcanje na njihov let. Poleg prostorov, namenjenih potnikom, so na terminalu tudi poslovni prostori za različne službe, ki delujejo na letališču, kot so predstavništva letalskih družb, turističnih agencij, banka, pošta, zdravniška služba. Na letališču deluje gasilska služba, zadolžena za intervencije v primeru nesreč, v zimskem času pa za očiščenost stez, platforme in letal. Za varnost na letališču skrbijo letališka policija in varnostne službe. Na letališču Jožeta Pučnika je tudi kontrola zračnega prometa, ki nadzoruje celoten slovenski zračni prostor, deluje pa tudi meteorološka služba.



Slika 1: Število prepeljanih potnikov v 1000 na letališču Jožeta Pučnika

(Vir: http://www.lju-airport.si/pripona/1121/AL_brosura_284x185mm-SLO-1.pdf)

Slika 1 prikazuje promet potnikov na letališču Jožeta Pučnika od leta 2007 do 2012. Največ prepeljanih potnikov so imeli leta 2008, v letu 2009 pa so doživeli občuten padec, kar je posledica predvsem splošne gospodarske krize v svetu, ki se občuti še danes. Po podatkih statističnega urada je letališče Jožeta Pučnika že v prvem polletju leta 2013 zaznalo 6-odstoten porast v številu prepeljanih potnikov v primerjavi z istim obdobjem leta 2012. Strateški plan do leta 2020 pričakuje porast prometa potnikov na več kot 2 milijona, čemur naj bi botrovala predvsem izgradnja novega potniškega terminala v bližnji prihodnosti.

Novi terminal bo povečal kapaciteto pretoka, postavljenih naj bi bilo 40 okenc za prijavo na let in trije trakovi za prevzem prtljage. Na terminalu bo tudi prostor za prevoznike, turistične agencije, restavracije in trgovine, predvideni pa so tudi poslovni saloni in dodatna ponudba za dobro počutje potnikov, obljublajo na spletni strani letališča (www.lju-airport).

4 PRSTNI ODTISI

Koža je največji organ v telesu. Organ ji lahko rečemo, ker je sestavljena iz več tkiv, milijone senzoričnih receptorjev in obsežno mrežo ožilja, ki medsebojno povezani opravljajo njeno najpomembnejšo vlogo – zaščito vitalnih organov. Koža je povečini gladka, sestavljena iz vrhnjice in debelejše usnjice. Usnjica ima brazde in gube, ki se jim povrhnjica tesno prilega, kar je vidno na površini. Koža na teh mestih ni gladka, ampak nagubana, sestavljena iz ukrivljenih linij. Ljudje imamo na blazinicah prstov, dlaneh in podplatoev nešteto ukrivljenih izbočenih linij, ki potekajo bolj ali manj vzporedno in tvorijo različne vzorce. Črte, ki tako tvorijo različne vzorce, se imenujejo papilarne linije, prstni odtis pa je odtis blazinice človeškega prsta.

Prstni odtisi imajo tri temeljne značilnosti (Maver, 2004):

- **Edinstvenost** – vsak prstni odtis je edinstven, niti dva človeka nimata enakih, prav tako se razlikujejo tudi vsi prsti iste osebe.
- **Trajnost** – prstni odtisi so nespremenljivi od tretjega meseca zarodka do razkroja trupla. Brazgotine odstopajo od tega pravila, pa še to le, če so trajne.
- **Vzorčnost** – vsi prstni odtisi so lahko razvrščeni v vzorčne tipe.

Zaradi teh lastnosti so prstni odtisi temeljni v uporabi biometrike. Edinstvenost velja le za empirično ugotovitev, čeprav še vedno niso odkrili dveh oseb, ki bi imela popolnoma enake prstne odtise, zgolj veliko podobnost. Problem ugotavljanja istovetnosti je v napravah, saj niso popolnoma odporne na napake in lahko zaznajo ujemanje dveh različnih oseb.

4.1 Razvoj

Dogodki in obdobja, ki pomenijo napredek v poznavanju klasifikacije prstnih odtisov in identifikacije, so (Maver, 2004):

- 1955–1913 pr. n. št. – vladavina Hamurabija v Babilonu – prstni odtisi na pečatih pogodb;
- drugo ali tretje stoletje pr. n. št. – lončeni pečatni grbi s prstnimi odtisi na Kitajskem;
- dvanajsto stoletje – kitajski romanopisec opozori na zvezo med prstnimi odtisi in identifikacijo kriminalcev;
- 1684 – Nehemiah Grew opiše pore in njihovo funkcijo na koži rok in nog;
- 1686 – Marcello Malpighi opravi prve preiskave papilarnih linij z uporabo novoizumljene naprave – mikroskopa;
- 1788 – J. Mayer prepričuje o edinstvenosti prstnih odtisov;
- 1823 – Johannes Purkinje klasificira vzorce prstnih odtisov, vendar jim ne pripisuje identifikacijske vrednosti;

- 1860 – William Herchel odvzema prstne odtise za izplačevanje pokojnin v Indiji, prav tako poudari, da se prstni odtisi v življenju ne spremenijo;
- 1880 – Henry Faulds zaključi, da je prstni odtis edinstven, in opravi identifikacijo s primerjavo sledi papilarnih linij in poznanih primerkov;
- 1891 – Juan Vucetic razvije uporaben identifikacijski sistem;
- 1892 – Francis Galton izda knjigo z naslovom Fingerprints;
- 1892 – Juan Vucetic na podlagi prstnih odtisov reši prvi primer umora;
- 1896 – Argentina ustvari prvo kriminalno zbirko prstnih odtisov;
- 1896 – Edward Henry izumi sistem desetprstne klasifikacije, ki ga poimenujejo po njem;
- 1901 – prvi klasifikacijski sistem prstnih odtisov v Scotland Yardu;
- 1912 – Edmond Locard govori o poroskopiji, identifikaciji s pomočjo pozicije in strukture por;
- 1930 – Battley razvije prvi enoprstni sistem prstnih odtisov;
- 1974 – V podjetju Printrak razvijejo prvi sistem avtomatske identifikacije prstnih odtisov AFIS.

AFIS omogoča daktiloskopske primerjave prstnih odtisov z bazo podatkov. Stopnjo ujemanja določa na skladnosti detajlov v določenih točkah.

Sistemi za avtomatsko obdelavo prstnih odtisov deluje po fazah (Maver, 2004):

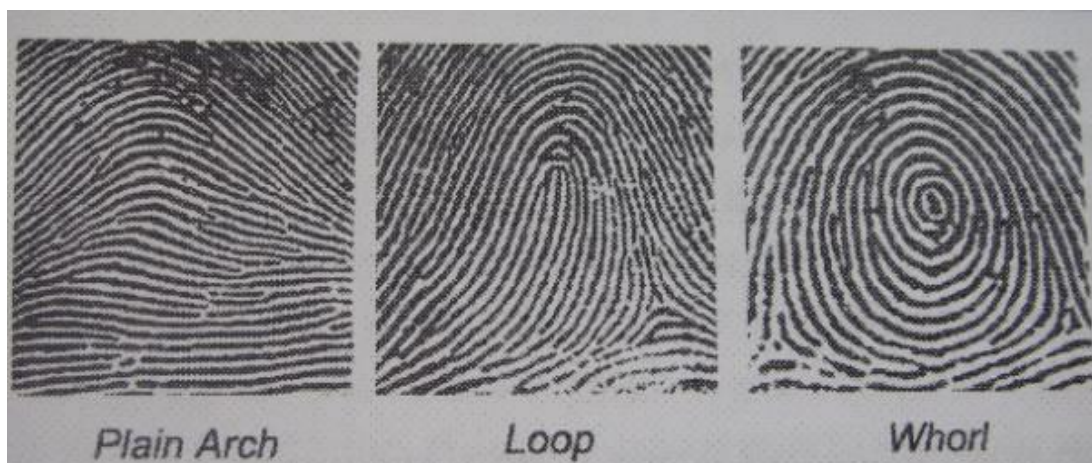
- **Ustanovitev baze** – vnos daktiloskopiranih kartonov prek skenerjev v bazo daktiloskopiranih kartonov, sprejemanje in shranjevanje t. i. vstopnikov s podatki, kot so ime, priimek, rojstni datum in drugi. Pri skeniranju prstne odtise natančno povečajo in izostrijo, nato pa sistem avtomatsko klasificira vseh deset prstnih odtisov. Sledi primerjava z bazo osumljencev in bazo vnesenih prstnih sledi ter povratna informacija.
- **Zajem vzorca** – vnos prstnih odtisov oziroma prstnih sledi v sistem prek skenerja in kamere.
- **Vzorčenje** – izdelana je šablona individualnih značilnosti, kjer lahko sistem avtomatsko označi individualne značilnosti ter opravi kvalifikacijo. Možno pa je tudi, predvsem pri sledih papilarnih linij, ročno označevanje individualnih značilnosti in osnovnega vzorca.
- **Primerjava zajetega vzorca z vzorci v bazi.**
- **Rezultat.**

4.2 Klasifikacija

Ali bi se dalo identificirati osebo s prstnimi odtisi, ko pri sebi nima dokumentov? Odgovor na to vprašanje je iskal že Francis Galton, njegovo delo pa nadaljeval in dopolnil Edvard Henry. Tako je nastal Galton-Henryjev klasifikacijski sistem prstnih odtisov.

Ta sistem razvršča prstne odtise v štiri osnovne vzorce (Maver, 2004):

- vrtinčasti ali krožni vzorci (Whorl),
- enostavni ali čisti loki (Arcus),
- radialne in ulnarne zanke (Loop),
- jelkovi loki (Tented Arches).



Slika 2: Vzorce prstnih odtisov

(Vir: http://www.nutrigenomika.info/epigenetika/prstni_odtisi_2.html)

Poznamo še sestavljene vzorce, npr. iz zanke in kakšnega krožnega vzorca ali pa iz dveh zank (double loop, twins, accidental), ter naključne vzorce, ki jih ne moremo razporediti v nobeno izmed opisanih skupin.



Slika 3: Dvojna zanka

(Vir: http://www.sfis.ca.gov/pattern_types.html)

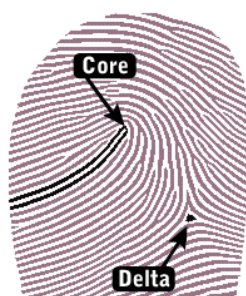


ACCIDENTAL

Slika 4: Naključna razporeditev

(Vir: http://www.sfis.ca.gov/pattern_types.html)

Prstni odtisi torej tvorijo različne vzorce. Vzorce pa določajo točke, okoli katerih so ovite linije. Točki sta poglobitvi sestavini individualnosti vsakega prstnega odtisa, imenujemo ju jedro (angl. core) vzorca in delta. Jedro se pojavlja v krožnih, zankastih vzorcih v obliki kroga, delta pa je področje odtisa, kjer linije oblikujejo trikotno strukturo.

**Slika 5: Jedro in delta**

(Vir: <http://www.ezfingerprints.com/fingerprinting-faqs.htm>)

Identifikacija s prstnimi odtisi temelji na ujemanju vzorca, kateremu sledi zaznava značilnosti grebenov, ki jih poznamo pod imenom Galtonovi detajli oz. minucije (angl. minutiae). Posamezen prstni odtis ima več kot sto minucij, ki se s primerjavo lahko uporabijo v identifikacijske namene.

Nekaj primerov minucij prikazuje slika 6.



Slika 6: Primeri minucij

(Vir: <http://old.policensw.com/info/fingerprints/finger08.html>)

»Morfologija (oblika) prstnega odtisa je povezana s specifičnimi električnimi in toplotnimi značilnostmi kože. To pomeni, da svetlobo, toploto ali električno napetost (ali kombinacijo vseh) lahko uporabimo za zajem podobe prstnega odtisa. Za zajem značilnosti vzorca prstnega odtisa obstaja več algoritemskih metod. Najbolj razširjene metode temeljijo na prepoznavanju vzorca ali izvlečku minucij. V primeru algoritmov, ki temeljijo na minucijah, je prstni odtis sestavljen iz grobih značilnosti, kot so loki, zanke in zasuki, ter drobnih značilnosti (minucije), kot so predvsem bifurkacije (razdelitve), delte (združevanja v obliki črke Y) in zaključki grebenov. Prstni odtis ima med 30 in 40 minucij. Značilnost vsake od njih je položaj (koordinate), tip (bifurkacija, delta ali zaključek) in usmerjenost (orientacija). Skupek značilnosti minucij lahko da predlogo za prstni odtis. Če so značilnosti natančno zajete, je možnost, da bi imela dva prstna odtisa enake značilnosti, izjemno nizka.« (Prstni odtis)

Zajemanje prstnih odtisov se je najbolj uveljavilo v kriminalistično preiskovalne namene, danes pa nam pomeni najbolj zanesljivo metodo identifikacije in služi kot element zagotavljanja varnosti. Metoda dajanja prstnega odtisa se ni veliko spreminjala, vendar se je z razvojem tehnologije bistveno olajšala primerjava odtisov z bazo podatkov. Za zajetje prstnega odtisa ne potrebujemo več črnila in lista papirja. Blazinico prsta položimo na napravo, ki jim rečemo skenerji (angl. live scan). Skenerji so elektronski čitalci, ki odčitajo prstni odtis. Poznamo več različnih čitalcev, ki delujejo na različnih principih.

Optični čitalci

»Optična metoda zajemanja prstnih odtisov ima najdaljšo zgodovino izmed Live scan čitalcev. Deluje tako, da prst v celoti položimo na prizmo, na katero usmerimo svetlobo. Tam, kjer se grebeni dotikajo prizme, se svetloba razprši, kar se odraža na

sliki kot črna barva. Pri dolinah pa se žarki zaradi pojava interne refleksije v večini odbijejo nazaj na tipalo, kar se odraža na sliki kot bela barva.« (Klopčič, 2009)

Termični čitalci

»Ti čitalci so ponavadi narejeni iz piroelektričnih materialov (angl. Pyro-electric). Piro izhaja iz grške abecede in pomeni ogenj, toplota. Čitalci namreč ob stiku s prstom zaradi toplote slednjega proizvedejo majhen električni tok. Preko tega lahko razberemo strukturo prstnega odtisa, saj je temperaturna razlika med grebeni prstnega odtisa, ki so v stiku s površino čitalca, in zračnih žepov v dolinah, dovolj velika.« (Klopčič, 2009)

Ultrazvočni čitalci

»Temeljijo na pošiljanju ultrazvočnih signalov proti prstu in sprejemanju odbojnih signalov. Preko teh se nato izračuna oddaljenost posamezne točke in posledično prstni odtis. Ultrazvočni signali lahko prodrejo tudi skozi umazanijo in oljne madeže, kar je njihova velika prednost. Zato ponavadi z ultrazvočnimi čitalci pridobimo slike prstnih odtisov dobre kvalitete.« (Klopčič, 2009)

Kapacitivni čitalci

»Čitalec je občutljiv na spremembe električne napetosti, ki se zapišejo kot črno-bela slika. Ko se s prstom dotaknemo površine sensorja, se med površino kože ter sensorji vzpostavi majhen električni naboj. Jakost tega je na področjih, kjer so prisotni grebeni, manjša kakor na področjih, kjer so prisotne doline. Slabost kapacitivnih čitalcev je, da naboj med prstom in sensorjem zelo hitro upade, zato mora biti zaščitna plast čim bolj tanka. Posledica tega je tudi občutljivost na statično elektriko, kar lahko privede do napak. Čitalci se slabo obnesejo na vlažnih in mastnih prstih, vendar pa so zelo dobri pri prepoznavanju ponarejenih prstnih odtisov. Zaradi majhne velikosti večina elektronskih naprav za identifikacijo preko prstnega odtisa uporablja kapacitivne čitalce.« (Klopčič, 2009)

5 OBRAZNA PREPOZNAVA

Prepoznati neko osebo pomeni ugotoviti njeno istovetnost z lastnim zaznavanjem (Maver, 2004). Zgodovina uporabe obrazne prepoznavne se je začela z identifikacijo osumljencev v kriminalistično-preiskovalne namene v začetku 19. stoletja. Z razvojem računalniške tehnologije je obrazna prepoznavna dobila povsem nov pomen. Zbiranje, primerjanje in identifikacijo oseb je poenostavila, izločila pa je tudi človeški faktor in z njim povezane napake ob različnih zaznavah.

5.1 Razvoj

Razvoj obrazne prepoznavne je vezan na tehnologijo, razvoj vse več in vse boljših programov za obrazno prepoznavo pa je vezan na različne dogodke, ki so opozorili na varnostne pomanjkljivosti oziroma pripeljali do želje po večjem nadzoru.

Razvoj po letnicah kot ga navaja literatura DuVal:

- 1960 – Bledsoe, Chan Wolf, Bisson ustvarijo prvi polavtomatski sistem obrazne prepoznavne. Njihov program je omogočal lociranje oči, ušes, nosu, ust na fotografiji. Izračunal je razdaljo med posameznimi elementi in jih primerjal z referenčnimi podatki.
- 1970 – Goldstein, Harmon, Lesk so uporabljali 21 specifičnih subjektivnih pokazateljev, kot so barva las, debelina ustnic, da bi avtomatizirali potrditev identitete. Meritve je bilo potrebno vnašati in računati ročno, kar je vzelo precej dela in časa.
- 1988 – Kirby in Sirovich sta vnesla standardno algebrsko tehniko v obrazno prepoznavo. Postavila sta mejnik, saj se je pokazalo, da so bile prepoznavne zelo natančne.
- 1991 – Turk in Pentland sta odkrila tehniko, ki je omogočala zaznavo obrazov na slikah. Tehnika je postala znana širši javnosti, ko so jo januarja 2001 uporabili na ameriškem Super Bowlu. Posnetke varnostnih kamer so primerjali z bazo aretiranih oseb. Našli so 19 ljudi z nerešenimi nalogi za prijetje.
- 1993 – FERET (Facial Recognition Technology Evaluation) je spodbudila razvoj algoritmov in tehnologije za obrazno prepoznavo in jo postavila na trg komercialnih izdelkov.
- 2002 – FRVT (Face Recognition Vendor Tests). Testi prodaje tehnologije obrazne prepoznavne so bili opravljeni v letih 2000, 2002, 2006 s ciljem ocenjevanja zmogljivosti komercialno dostopnih sistemov obrazne prepoznavne in izobraževanjem javnosti, kako pravilno predstaviti in analizirati rezultate.
- 2006 – FRGC (Face Recognition Grand Challenge). Tekmovanje tehnologije obrazne prepoznavne je ocenila zadnje algoritme obrazne prepoznavne: visoke

ločljivosti slik obrazov, 3D-skeniranje obraza ipd. Rezultati so pokazali, da so novi algoritmi veliko natančnejši kot pred leti, nekateri sistemi so celo presegli človeško prepoznavo obrazov ter razločili in identificirali enojajčne dvojčke.

5.2 Lastnosti

Eno izmed petih čutil, ki jih človek ima, je vid. Z vidom zaznavamo svetlobo, podobe, jih interpretiramo in povezujemo v nam znane podatke. To je proces, ki ga dnevno opravljamo, nezavedno, rutinirano in brez posebnega truda. Sem spada tudi obrazna prepoznavna in identifikacija oseb.

»Obrazna prepoznavna oseb je človeški naravni proces, izvajan vsakodnevno. Le bežen pogled na obraz in že smo zmožni prepoznati obraz in imenovati osebo. Ta proces se izvaja tako hitro, da nikoli ne razmišljamo, kaj na obrazu smo pravzaprav gledali. Nekateri izmed nas potrebujemo nekaj časa, da imenujemo osebo, medtem ko je prepoznavna instantna. Kompleksnost človeškega obraza izhaja iz nenehnih sprememb, ki potekajo skozi čas življenja. Tem spremembam navkljub smo ljudje še vedno sposobni prepoznati obraz in identificirati osebo. Naša naravna zmožnost prepoznavne pa sega preko obrazne prepoznavne, saj vzporedno zaznavamo tudi različne vzorce, zvoke in vonje in vse skupaj povežemo v celoto. Na žalost to naravno sposobnost najdemo le pri ljudeh in ne obstaja pri strojih, čeprav jo bolj ali manj uspešno poskušajo simulirati. Obrazna prepoznavna s strojem pa je lahko neprecenljiva in ima različne pomembne vloge v življenju, kot so elektronski in fizični nadzor dostopa ter nacionalna in mednarodna obramba in varnost. Simulacija človeške obrazne prepoznavne na strojno-računalniškem področju je zahtevna naloga, ampak ne nemogoča. Skozi življenje v spomin shranimo veliko obrazov in ustvarimo nekakšno bazo podatkov. Strojno prepoznavanje prav tako uporablja bazo podatkov, ki je sestavljena iz različnih obrazov, v obzir pa so vzete tudi variacije obraznih lastnosti. Najbolj poznani metodi obrazne prepoznavne temeljijo na zaznavi obraznih lastnosti in njihovi uporabi v identifikacijske namene oziroma celotno analizo obraza kot celote. Prvi pristop uporablja dele obraza kot so nos, oči, usta, da jih poveže z obrazom osebe. Drugi pristop pa uporablja cel obraz za identifikacijo.« (Delač & Grgič, 2007)

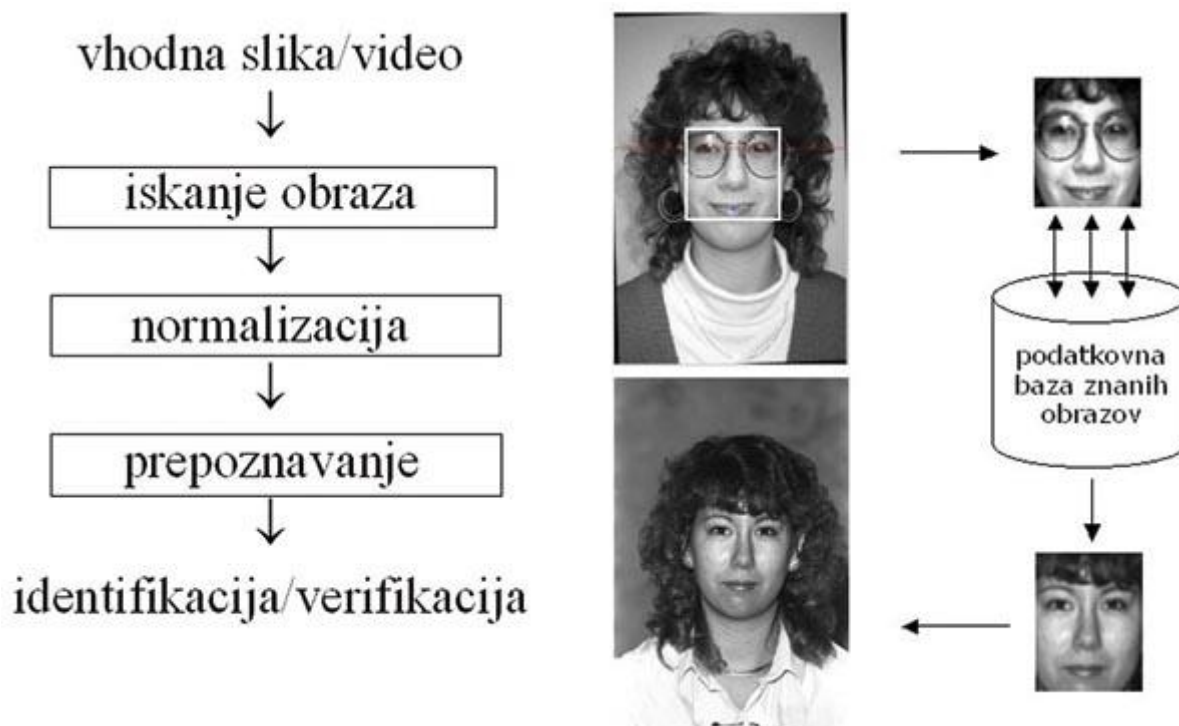
Sistem baze podatkov temelji na podobah človeških obrazov, zajetih, procesiranih in pripravljenih na primerjavo. Težave nastanejo pri različnih zajetjih podobe obraza, zato je potrebno biti pazljiv na nekatere stvari pri detekciji obraza, kot navajata avtorja (Delač & Grgič, 2007):

- Obraz ne sme biti zakrit s predmeti, lasmi, pokrivali. Pozorni moramo biti na prisotnost ali odsotnost strukturnih elementov, kot so brada, brki, očala, obrazni izraz. Poza mora biti frontalna, pod kotom 45 stopinj.

Prepoznavanje obrazov je naloga, ki jo ljudje opravljajo izredno hitro in uspešno. Izkazalo se je, da je ta očitna preprostost nevarno zavajajoča, saj se samodejno prepoznavanje obrazov zdi kot problem, ki je še vedno daleč od rešen. Kljub več kot 20 let trajajočim obsežnim raziskavam veliko število člankov, objavljenih v revijah in konferencah, namenjenih temu področju, še vedno ne moremo trditi, da umetni sistemi lahko merijo podobno kot človek. Samodejno prepoznavanje obrazov je zapleteno predvsem zaradi težkih pogojev slikanja (razsvetljava in vidik sprememb, ki jih povzroča gibanje telesa) in zaradi različnih drugih vplivov, kot so staranje, obrazna mimika, zapor itd. Raziskovalci iz računalniškega vida, s slikovno analizo in obdelavo podatkov, razpoznavanjem vzorcev, strojnim učenjem in drugimi področji skupaj delajo, motivirani predvsem zaradi številnih možnih praktičnih aplikacij.

Kot taka je postala ena od treh identifikacijskih metod na področju e-potnih listov in biometrične izbire za mnoge druge varnostne aplikacije. Kognitivni in modeli dojetanja predstavljajo pomembno podlago za interdisciplinarne raziskave, ki povezujejo znanstvenike iz na videz nezdržljivih področjih in izmenjujejo tako metodologijo kot rezultate. Dokazi iz nevrobioloških, psiholoških, zaznavnih in spoznavnih strok poskušajo zagotoviti potencialno koristen vpogled v to, kako so vizualne kode sistema povezane.

Obrazna prepoznavna je bistveno napredovala od predstavitve metode Eigneface. V nadzorovanih okoliščinah, npr. ob svetlobi, pozi, obraznem izrazu lahko računalniška prepoznavna zlahka preseže človeško, še posebej če ima obsežno zbirko podatkov. Verifikacija obraza poteka pri e-potnih listih, ko se primerja skeniran obraz z evidentiranim, obrazna identifikacija pa poteka na principu primerjave enega proti mnogim, da bi povezala skeniran obraz z zabeleženimi v podatkovni bazi. Sistem obrazne prepoznavne je v veliki meri odvisen od različnih faktorjev, kot so ambientalna osvetlitev, izraz na obrazu, pričeska ... Na temelju teh faktorjev lahko obrazno prepoznavo razdelimo v dve kategoriji: prvo, v kateri osebe v postopku identifikacije sodelujejo, in drugo, ko ne sodelujejo. Med sodelujoče spada preverjanje e-potnega lista, ko oseba predstavi svoj obraz v namene identifikacije na pravilen način (npr. direkten pogled z odprtimi očmi) z namenom, da se mu odobri vstop. Druga kategorija je tipična za metode nadzora; uporabnik se ne zaveda, da ga snemajo, zato seveda povzroča največ problemov. Za optimalen posnetek mora biti razdala manjša od 1 m.



Slika 7: Potek obrazne prepoznave

(Vir: http://www.monitor.si/images/clanki/slika/slika3_006.jpg)

»Obrazna prepoznavna v grobem poteka po več stopnjah. Generalno je sestavljena iz štirih modulov, ki so prikazani na sliki 7: Lociranje obraza, normalizacija, ekstrakcija značilnosti in ujemanje. Zaznavanje obraza (ang. face detection) je namenjeno izločitvi obraza iz podlage oziroma odzadja. Lociranje obraza (angl. face landmarking) poišče obrazne značilnosti, kot so nos, usta, oči, oblika obraza. Normalizacija obraza (angl. face normalization) geometrično normalizira obraz, kar pomeni, da različne izraze, poze obraza in osvetlitev postavi v standarden okvir, kar mu omogoči prepoznavo. Na normalizirani sliki obraza se naredi ekstrakcija obraznih posebnosti (angl. face feature extraction), da se pridobi zanesljive informacije, s katerimi se obraze razlikuje med osebami in jih uporabi za iskanje pravilnega ujemanja. V preverjanju ujemanja (angl. face matching) se uporabijo pridobljene značilnosti in se primerjajo z eno (verifikacija) ali mnogo (identifikacija) obrazov v podatkovni bazi. Rezultat pri verifikaciji je pozitiven ali negativen, pri identifikaciji pa pri veliki gotovosti ujemanja objavi rezultat identifikacije, v nasprotnem primeru pa objavi vzorec kot neznan.« (Li & Jain, 2011)

Obstaja več tipov tehnologij obrazne prepoznavne, od katerih lahko vsaka deluje bolje v določenih okoliščinah. Nekatere so zelo občutljive na svetlobne pogoje, nekatere na temperaturne, ene pa imajo celo sposobnost učenja. Vsaka predstavlja svojo rešitev v dani situaciji. Glede na to se danes uporablja pet različnih načinov kot navajata avtorja Chirillo in Blau (2003).

Toplotni (thermal)

»Obstajata dve obliki toplotne obrazne prepoznavne. Prva uporablja toplotne kamere za zaznavo vzorcev krvnih žil, ki se nahajajo pod kožo, na podlagi česar se naredi šablona. To je način, po katerem se loči celo identične dvojčke. Druga oblika pa za zaznavo vzorca toplote uporablja infrardečo kamero. Ta oblika je občutljiva na spremembe v stanju človeka in okolice.« (Chirillo & Blau, 2003)

Avtomatsko obdelovanje obraza (automatic face processing)

»Ta način uporablja razdalje in razmerja razdalj med glavnimi obraznimi značilnostmi, kot so oči, nos in usta ter velja za najšibkejšo možnost, lahko pa deluje bolje v okoliščinah pri majhni osvetlitvi s frontalnim zajemom.« (Chirillo & Blau, 2003)

Analiza lokalnih značilnosti (local feature analysis)

»Pri obrazni prepoznavi deluje sistem na principu lokaliziranja značilnosti znotraj mreže, npr. položaja oči, nosu, ušes, ust, brazgotin ipd. Po končanem postopku oz. procesu lahko na osnovi vsote številnih karakteristik, ki so vpletene v mrežni sistem, istovetnost potrdi ali zavrže. Večina sistemov uporablja črno-belo video kamero, s katero se posname osebo.« (Chirillo & Blau, 2003)

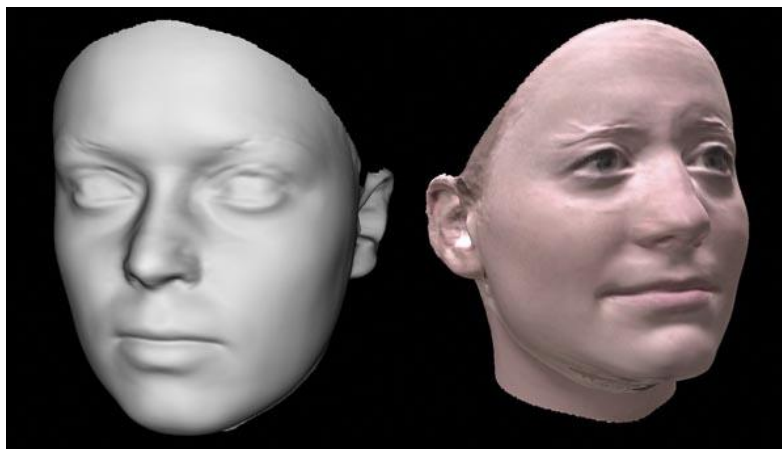
Eigenface

»Eigenface je metoda, razvita na inštitutu MIT (Massachusetts Institute of Technology), pomeni pa »lasten, svoj obraz«. Metoda temelji na 2D-slikah, ki vsebujejo podatke o različnih obraznih lastnostih. Eigenface aproksimiramo iz slik, na katerih z algoritmom poiščemo določene lastnosti. Ponavadi se za aproksimacijo uporabijo slike več obraznih izrazov iste osebe, slike z in brez očal, brade, brkov ter različnih pričesk. Vsakemu Eigenfaceu pa je potrebno določiti še spol, raso, ime, starost in ostale potrebne lastnosti. Uporabna je tako za verifikacijo kot avtentikacijo prepoznavne, potrebno pa je zagotoviti dobro osvetljen prostor in kvalitetne slike prednje strani obraza.« (Mraovič, 2006)

Nevronske mreže (angl. Neural network)

»Nevronske mreže veliko obetajo v prihodnosti. Pri nastavljanju (učenju) mreži predstavimo sliko, ki jo ta primerja s sliko v svojem spominu. Mreža nato nastavlja uteži, dokler ne dobimo zelenega rezultata. Teoretično se lahko mreže naučijo prepoznati vse obraze na tem planetu tudi pri zelo slabih pogojih zajemanja slike. Mreža analizira celotno sliko, na kateri išče kontrastne elemente (oči, obrvi, eno stran nosa, usta, ličnice ...). Uporabna je pri avtentikaciji ali verifikaciji.« (Mraovič, 2006)

3D-obrazna prepoznava



Slika 8: 3D-posnetek obraza

(Vir: http://www.monitor.si/images/clanki/slika/slika5_006.jpg)

Tridimenzionalna prepoznavna obrazov je dokaj nov trend, ki na nek način prekinja dolgo tradicijo 2D-naprav, ki temeljijo na posnemanju človeške zaznave in prepoznavne. 2D-tehnologija obrazne prepoznavne je občutljiva na svetlobne pogoje, usmeritev glave, pogleda, obrazno mimiko in ličila, kar izhaja iz omejenih pridobljenih informacij o 2D-sliki.

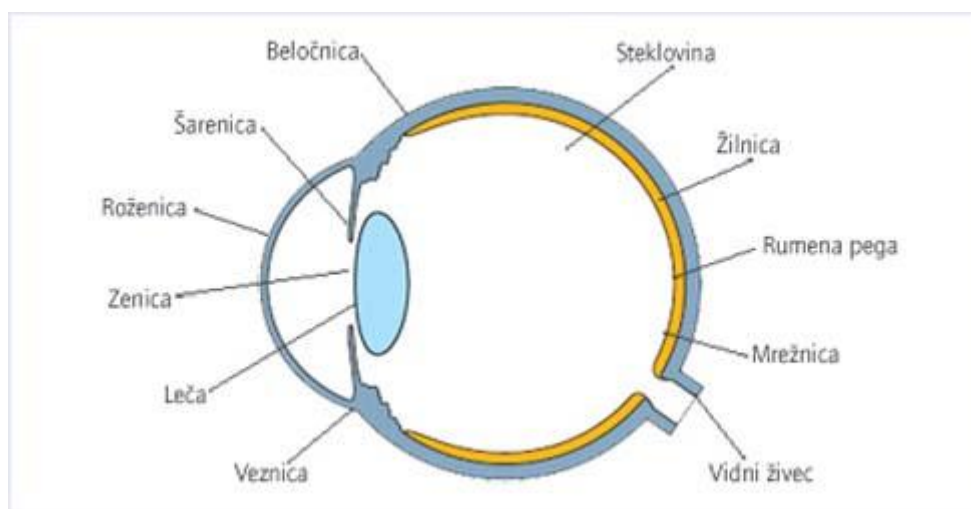
Glavna ideja novih algoritmov je predstavitev obrazne površine, ki se ne spreminja oz. je neobčutljiva na deformacije, ki nastanejo npr. z obraznimi izrazi.

6 PREPOZNAVA ŠARENICE

Oko je organ, ki nam omogoča delovanje enega najpomembnejših čutil, vid. Z njim zaznavamo oblike in barve, vendar le na podlagi svetlobe, ki jo sprejme. V popolni temi ljudi ne vidimo. Oko pretvori zaznane oblike in jih po vidnem živcu pošlje v možgane, ki zapis preberejo in pretvorijo v vidne podobe. Oko je sestavljeno iz več delov, kot je razvidno iz slike 9.

Šarenica je obarvani del, ki temelji na količini pigmenta melatonina v mišici. Čeprav je barva in struktura šarenice genetsko povezana, podrobni podatki o vzorcih niso. Šarenica se razvije v prednatalnem obdobju rasti skozi proces oblikovanja membrane. Čeprav so genski zapisi lahko identični, so šarenice ljudi edinstvene in strukturalno različne, kar omogoča njeno uporabo v namene prepoznave.

Šarenica je mišica v očesu, ki se nahaja med roženico in lečo. Deluje refleksno in brez našega zavedanja ali vpliva, njena glavna naloga pa je urejanje velikosti zenice in s tem kontroliranje koliko svetlobe lahko vstopi v oko. V mraku se šarenica razširi in tako izboljša zaznavanje šibke svetlobe. Pri močni svetlobi se šarenica zoži in omeji količino svetlobe, ki vstopi v oko.



Slika 9: Oko

(Vir: <http://www.morelaokulisti.si/diagnostika/refraktivne-napake-ocesa/anatomija-ocesa>)

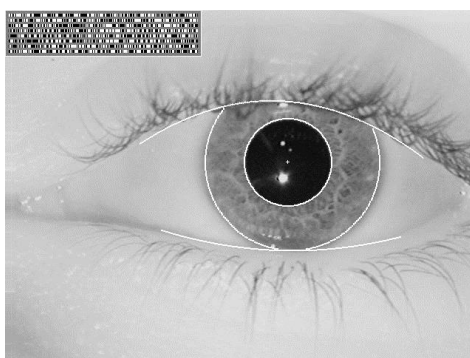
6.1 Razvoj

Oblika in barva oči sta prepoznavni znak osebe. Po letih raziskovanj so odkrili še unikatnost vzorca šarenice, kar je samo po sebi narekovalo razvoj za namene identifikacije. Prelomnice razvoja smo povzeli po Biometrics, 2006.

- 1936 – oftalmolog³ Frank Burch predlaga koncept z uporabo vzorcev šarenice kot metodo prepoznavne posameznika.
- 1985 – okulista dr. Leonard Flom in dr. Aran Safir predstavita koncept unikatnosti šarenice, podeljen jima je patent za koncept identifikacije šarenice.
- 1987 – dr. Floam in Dr. John Daugman združita moči v razvijanju algoritma za avtomatizirano prepoznavo šarenice.
- 1993 – Agencija za jedrsko obrambo (angl. the Defense Nuclear Agency) začne preizkušati prototip naprave, preizkusi so se uspešno zaključili leta 1995 s pomočjo Drs. Floam, Safir, Daugman.
- 1995 – Prvi komercialni produkti postanejo dostopni na trgu.
- 2005 – širok patent, ki je zajemal prepoznavo šarenice, je potekel, kar je odprlo možnosti za druga podjetja, ki so razvila svoje algoritme za prepoznavo šarenice.

6.2 Lastnosti

Prepoznavna šarenice je proces prepoznavanja osebe z analizo vzorca šarenice. Avtomatizirana metoda je relativno mlada, obstaja kot patent od leta 1994. Pred prepoznavo se šarenico lokalizira na podlagi njenih značilnosti (določi se zunanje in notranje meje). Te značilnosti in različna oblika šarenice omogočajo slikanje, določitev značilnosti in ekstrakcijo. Lociranje šarenice je zelo pomembno za nadaljnje korake, saj s pravilnim lociranjem izločimo motnje, kot so trepalnice, odsevi, zenice in veke.



Slika 10: Lociranje šarenice

(Vir: http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html)

Slikanje šarenice zahteva uporabo visoko kakovostne digitalne kamere. Kamere uporabijo infrardečo svetlobo za osvetlitev šarenice, ne da bi poškodovale ali povzročale nelagodje očesu.

³ Oftalmologija ali okulistika je veja medicine, ki se ukvarja z zdravljenjem očesnih bolezni.

Posnamejo čisto sliko visoke ločljivosti, obenem pa analizirajo vzorce šarenice in jih prevedejo v kodo, ki omogoča nadaljnjo obravnavo.

Avtentikacija oseb na podlagi skeniranja šarenice je ena izmed najzanesljivejših biometričnih tehnologij prepoznave. Sistem preprosto vzame sliko šarenice in jo uporabi za preverjanje pristnosti. Uporaba šarenice za namene identifikacije oseb omogoča njena nespremenjenost skozi celo življenje, unikatnost in zanesljivost v smislu, da vzorec šarenice ni dovzeten za krajo, izgubo ali ponarejanje. Tudi sama tehnologija se je pokazala za uporabno, saj so sistemi za skeniranje šarenice nevsiljivi, neškodljivi, omogočajo pa hitro in zanesljivo identifikacijo. Uporabna je praktično za identifikacijo vseh ljudi, vsi imamo vsaj eno oko, izjema pa niso niti slepi, saj za sliko šarenice ni nujno, da oseba vidi. Potrebuje le malo sodelovanja skenirane osebe, ki pristavi oko k skenerju na razdaljo, ki jo predpisuje vsak sistem posebej. Za odvzem vzorca ne potrebuje veliko svetlobe, kamera se samodejno aktivira in prilagodi ter posname digitalno sliko šarenice. Odvzet vzorec se primerja z vrednostmi, shranjenimi v bazi podatkov, in potrdi ujemanje (Iris ID).

Dandanes je najpogostejša uporaba sistemov za skeniranje šarenice fizični nadzor dostopa z varnostnim namenom, vsestranskost tehnologije pa bo vodila do vse večje uporabe v velikih gospodarskih sektorjih, kot so promet, zdravstvo, nacionalni programi identifikacije.

7 BIOMETRIČNI POTNI LIST

Potni list je javna listina, ki slovenskemu državljanu služi za prehod državne meje ter dokazovanje njegove istovetnosti in državljanstva. Do potne listine je upravičen vsak državljan Republike Slovenije. Zanj lahko zaprosi ob predložitvi osebnega dokumenta in fotografije predpisane velikosti.

7.1 Razvoj

Od običajnih potnih listov za identifikacijo so dokumenti napredovali zaradi zahtev po večji varnosti, omejitvi prevar in izboljšanju uporabniške izkušnje s strani lastnikov potnih listov in uradnikov, zadolženih za pregledovanje.

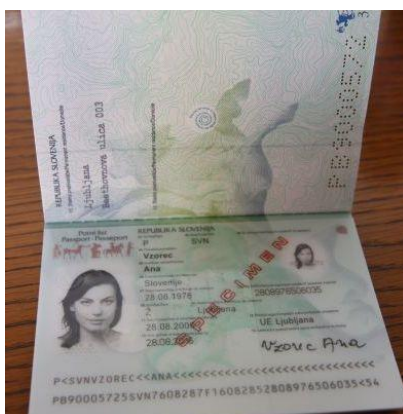
- Standarde za biometrične potne liste je začela razvijati skupina ekspertov pri ICAO (International Civil Aviation Organization) že leta 1986.
- Ministrstvo za domovinsko varnost ZDA izvaja program za nadzor meje, ki predvideva zbiranje biometričnih podatkov vseh tujcev, ki za vstop v ZDA potrebujejo vizum. Ameriški kongres je leta 2002 skupini privilegiranih držav VWP (Visa Waiver Program), med katerimi je tudi Slovenija, omogočil, da njihovi državljani za poslovni ali turistični obisk ZDA do 9 dni ne potrebujejo vizuma, postavil pa je tudi zahtevo ter določil rok 26. 10. 2006, do katerega morajo članice začeti izdajati potne liste z biometričnimi identifikacijskimi podatki, sicer bodo njihovi državljani ob vstopu v ZDA obravnavani tako kot državljani držav, ki za vstop potrebujejo vizum.
- 18. 1. 2005 je stopila v veljavo Uredba Sveta EU o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice. Določa, da morajo imeti potni listi vgrajen shranjevalni medij – čip z zadostno kapaciteto, na katerem bosta shranjena zapisa dveh vrst biometričnih podatkov, podoba obraza in prstni odtisi v interoperabilni⁴ obliki (Upravne enote).
- Republika Slovenija je 28. 8. 2006 pričela z izdajo novih, biometričnih potnih listov. Biometrični potni listi vsebujejo nove zaščitne elemente, med katerimi je tudi brezkontakten čip, na katerem je bila sprva shranjena le fotografija imetnika potnega lista in podatki, ki so tudi sicer vidno zapisani v potnem listu, po letu 2009 pa tudi prstni odtis dveh prstov. Novost novega potnega lista so še zapisi določenih podatkov v vseh uradnih jezikih Evropske unije (E-uprava, 2012).

⁴ Interoperabilnost je zmožnost različnih sistemov in organizacij, da sodelujejo. Izraz se pogosto uporablja v tehničnem smislu systemske tehnike, ali pa v širšem smislu, ob upoštevanju družbenih, političnih in organizacijskih dejavnikov, ki vplivajo na sistem za delovanje sistema (NCOIC).

7.2 Lastnosti

Na prvi pogled se biometrični potni listi od starih ne razlikujejo dosti. Na platnico sprednje strani je dodan napis »Evropska unija« in manjši mednarodno dogovorjen znak, ki sporoča, da potni list vsebuje čip. Čip je vgrajen v polikarbonatni strani potnega lista, ki je posledično nekoliko debelejša. Oblikovna podoba potnih listov se od stare razlikuje predvsem po barvnem odtenku strani potnega lista. Nova modrozelena barva nadomešča stare rdeče odtenke, izbor motivov, ki predstavljajo osnovne kulturne in zgodovinske informacije oziroma značilnosti Slovenije od prazgodovine preko spomenikov rimske dobe, srednjega veka, romantike, gotike, baroka, secesije, moderne in najnovejšega časa, ostaja enak. Na obrazcih potnega lista so določeni podatki prav tako napisani v vseh uradnih jezikih Evropske unije (Upravne enote).

Biometrični potni listi morajo biti interoperabilni, kar pomeni, da morajo biti podatki na čipu zapisani tako, da jih lahko prebere mejni organ katere koli tuje države, ne glede na to, kakšno strojno in programsko opremo uporablja na svojem mejnem prehodu. Za zagotovitev interoperabilnosti je vsebina podatkov na čipu točno določena. Na čipu so zapisani le tisti podatki, ki so tudi sicer vidno zapisani v potnem listu (osebno ime, državljanstvo, datum rojstva, spol, država izdaje, številka potnega lista in datum poteka) in fotografija, ki je na potnem listu. Ob mejni kontroli se s primerjavo na licu mesta zajete podobe osebe in podobe, shranjene na čipu v biometrični obliki, ugotavlja le, ali je oseba, ki z dokumentom prehaja mejo, res oseba, ki ji je bil dokument izdan. Fotografij na čipu se ne uporablja za primerjavo z evidenco npr. iskanih oseb, prav tako je odveč bojazen državljanov, da bodo njihove podatke, shranjene na čipu, prebrale neavtorizirane osebe. Čip je »zaklenjen« in prebere ga lahko le avtorizirana oseba na mejnem prehodu s položitvijo biografske strani potnega lista na čitalec zapisa (Upravne enote).



Slika 11: Vzorec potnega lista

(Vir: <http://radio.ognjisce.si/sl/126/slovenija/6621/>)

»Običajni potni list ima vpisane podatke o lastniku, vsebuje njegovo sliko in dve vrstici strojno berljivih podatkov (MRZ – Machine Readable Zone) in mora ustrezati nekaterim fizičnim varnostnim standardom (poseben papir, vodni tisk ...). Če odprete svoj potni list, boste MRZ našli na levem robu – to sta dve strojno berljivi vrstici po 44 znakov, ki vsebujeta med drugim ime in priimek lastnika, njegov rojstni datum in številko potnega lista. Čip pa vsebuje MRZ, biometrične podatke in elemente za digitalno zaščito podatkov na njem. Po specifikaciji ICAO, iz katere je vzeta slika na desni, so podatki na čipu razvrščeni v 16 skupin.« (Lah, 2007)

ISSUING STATE or ORGANIZATION RECORDED DATA			
Detail(s) Recorded in MRZ	DG1	Document Type	
		Issuing State or organization	
		Name (of Holder)	
		Document Number	
		Check Digit - Doc Number	
		Nationality	
		Date of Birth	
		Check Digit - DOB	
		Sex	
		Date of Expiry or Valid Until Date	
		Check Digit - DOE/VUD	
		Optional Data	
		Check Digit - Optional Data Field	
		Composite Check Digit	
Encoded Identification Feature(s)	GLOBAL INTERCHANGEABLE FEATURE	DG2	Encoded Face
	Additional Feature(s)	DG3	Encoded Finger(s)
		DG4	Encoded Eye(s)
Displayed Identification Feature(s)	DG5	Displayed Portrait	
	DG6	Reserved for Future Use	
	DG7	Displayed Signature or Usual Mark	
Encoded Security Feature(s)	DG8	Data Feature(s)	
	DG9	Structure Feature(s)	
	DG10	Substance Feature(s)	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	Optional Detail(s)	
	DG14	Reserved for Future Use	
	DG15	Active Authentication Public Key Info	
	DG16	Person(s) to Notify	

Slika 12: Podatki na čipu potnega lista

(Vir: <http://www.si-ca.si/kripto/kr-potnilist.html>)

»Kot vidimo, prvo skupino (DG1) predstavlja MRZ. V drugo skupino (DG2) spada slika obraza v formatu jpeg, v tretjo (DG3) prstni odtis in v četrto (DG4) slika šarenice. Zaenkrat se na potnih listih še ne uporablja slik šarenice.« (Lah, 2007)

Kako pa naj bi bili podatki na čipu zaščiteni? Navedene so naslednje možnosti zaščite, od katerih se pri sedaj izdanih potnih listih uporabljata samo prvi dve, kot navaja Lah (2007):

- **Osnovni nadzor dostopa (Basic Access Control – BAC).** Ta kontrola je obvezna po odločbi Evropske komisije. Kontrolor odpre potni list in ga položi na optični čitalec, da ta prebere MRZ in ga sporoči nadzornemu sistemu (terminalu). Ta iz MRZ izračuna ključ za simetrični algoritem. Čip in terminal potem oba poznata ključ in vzpostavita šifrirano povezavo po predpisanem

postopku. Če čip ugotovi, da terminal ne pozna ključa, ne dovoli dostopa do podatkov. Čitalec mora torej poznati ključ, če hoče prebrati podatke na čipu, zato naj bi to preprečilo, da poljuben čitalec posname podatke iz čipa (skimming). Ker MRZ ne moremo prebrati, če je potni list zaprt, sklepamo, da je lastnik prostovoljno izročil svoj potni list v pregled. Ta kontrola pa ne more preprečiti, da bi čip kopirali.

- **Pasivna avtentikacija (Passive Authentication).** Ta kontrola je obvezna po dokumentu ICAO, torej za vse biometrične potne liste. Terminal preveri digitalni podpis, tako da uporabi javni ključ podpisnika, ki je na čipu. Če bi nekdo hotel spremeniti podatke na čipu, bi moral poznati zasebni ključ podpisnika (izdelovalca potnih listov). Ta čip dokazuje, da podatki na čipu niso bili spremenjeni. Ne prepreči pa, da bi čip kopirali ali nadomestili z drugim.
- **Aktivna avtentikacija (Active Authentication).** Po specifikaciji ICAO ni obvezna, prav tako ne po specifikaciji EU. Vsak čip vsebuje poseben par asimetričnih ključev za aktivno avtentikacijo, in sicer javni ključ in zasebni ključ v zaščitenem delu spomina. Zasebni ključ lahko uporabi le čip v internih operacijah, ne da pa se ga prebrati. Terminal pošlje čipu v podpis naključno generirano število in z uporabo ključa preveri, da je odgovor res podpisan z zasebnim ključem čipa. To dokazuje, da čip ni bil kopiran ali nadomeščen z drugim. Ker pa bi se ta sistem lahko zlorabilo za sledenje osebam in predstavlja grožnjo zasebnosti, kaže, da bodo države EU namesto njega uporabile "avtentikacijo čipa".
- **Razširjeni nadzor dostopa (Extended Access Control – EAC).** Sestavljata dve kontroli, ki sta za potne liste držav EU obvezni, ker so na čipu prstni odtisi.
- **Avtentikacija čipa (Chip Authentication).** Čip vsebuje par asimetričnih ključev za avtentikacijo, in sicer javni ključ in zasebni ključ v zaščitenem delu spomina. Zasebni ključ lahko uporabi le čip v internih operacijah, ne da pa se ga prebrati. Čip in nadzorni sistem se z uporabo asimetričnega algoritma dogovorita za skupni simetrični ključ za nadaljnji dostop do občutljivih podatkov. Ker je povzetek javnega ključa vključen, bi zamenjavo tega para ključev odkrili pri pasivni avtentikaciji. To dokazuje, da čip ni bil zamenjan in da je prebran z verodostojnega čipa. Nadomešča "aktivno avtentikacijo", je pa ta sistem boljši, ker čip pri vzpostavitvi komunikacije z nadzornim sistemom ne podpiše poslanega sporočila, poleg tega pa se zagotovi močno enkripcijo za dostop do občutljivih podatkov na čipu.

»Prve tri stopnje zagotavljajo, da čip ni bil kopiran ali zamenjan, da podatki na njem niso bili spremenjeni, poleg tega je prisluškovanje onemogočeno zaradi šifriranja povezave, ki se vzpostavi ob avtentikaciji čipa. Dostop do občutljivih podatkov je omogočen samo pooblaščenim nadzornim sistemom.« (Lah, 2007)

Biometrični potni listi nudijo veliko tehničnih novosti, poleg tega pa je tudi njihovo pridobivanje preprostejše. Fotografijo dobimo pri fotografu, ki jo v elektronski obliki pošlje na strežnik upravne enote. Na upravni enoti fotografijo pridobijo s strežnika, jo dodajo v potni list, potem pa se še podpišemo na elektronsko tablico, ki potnemu listu digitalno doda podpis. Evropska unija zahteva skeniranje 2 prstov, kazalcev leve in desne roke. Če sta kakorkoli poškodovana ali neberljive kakovosti, se lahko uporabi odtise tudi sredincev ali palcev. Ti odtisi se hranijo zgolj za namene istovetnosti imetnika potnega lista pri prehajanju meje, torej primerjavo 1 : 1.

8 VAROVANJE OSEBNIH PODATKOV

»Varnost etimološko izhaja iz besede »securitas« – varen, odsotnost nevarnosti. Varnost je vrednota vseh treh nivojev človekovega bivanja, delovanja in povezovanja, sestavljena iz elementov in komponent sistema ter njihovih medsebojnih relacij tako, da je zagotovljena določena stabilnost in fleksibilnost sistema v razmerju do ogrožanj iz družbenega in naravnega okolja.« (Anžič, 2010)

Potreben je sistemski pristop k varnosti:

- varnost posameznika,
- varnost družbe,
- varnost mednarodne skupnosti,
- varnost enega nivoja je nujen pogoj za varnost ostalih nivojev.

»Grožnje varnosti moramo razumeti v kontekstu razmerja do varnosti. Razmerje je deterministično v obe smeri: razumevanje varnosti referenčnega objekta vpliva na identificiranje groženj varnosti tega objekta in obratno. Brez ogrožanja varnosti pojem varnosti sploh ne bi bil spoznaven in torej ne bi obstajal. Sam koncept varnosti je torej mogoče opredeliti z njegovim nasprotjem, podobno kot ne bi mogli označiti nečesa za svetlo ali veliko, ne da bi to razumeli v zvezi s temnim in majhnim.« (Prezelj, 2001)

Varnost je kompleksen pojem, razsežen na nacionalni, nadnacionalni in mednarodni ravni. Najpomembnejše pa je dojetje varnosti na osebni ravni. Ljudje imamo različne predstave, kriterije in meje, do katerih se še počutimo varno.

»Povečanje varnosti, ki jo lahko prinesejo biometrične metode, je precej široko področje in je hkrati povezano s področji uporabe biometričnih metod. Povečanje varnosti gre tako predvsem na račun dostopa do varovanih (zaščitenih, občutljivih) območij, zanesljivejšega ugotavljanja identitete in kontrole vstopa in izstopa iz države ter prepoznave (znanih) teroristov.« (Anžič, 2003)

V slovenski Ustavi⁵ je pravica do zasebnosti natančno definirana, nedotakljivost človekove telesne in duševno celovitosti se uvršča v klasično ustavno svoboščino. Večina držav Evropske unije (v nadaljevanju EU) ima pravico do zasebnosti definirano v svoji ustavi. Torej to zasebnost uvršča v skupino temeljnih človekovih pravic. V večini evropskih držav je zasebnost ustavna kategorija, razen v Avstriji, Franciji, Norveški in San Marinu, kjer je v veljavi poseben zakon o varstvu podatkov (v Avstriji) ali pa je pravica do zasebnosti omenjena v ustavi implicitno (v Franciji). Velika Britanija, ki nima pisne ustave, je leta 1998 zaradi skladnosti z Evropsko konvencijo o človekovih pravicah, ki so jo sprejele praktično vse evropske države, sprejela Human Rights Act, v katerem je omenjena tudi pravica do zasebnosti. Evropske države, članice Sveta Evrope, razen San Marina, so sprejele tudi Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. To pomeni, da imajo večinoma tudi poseben zakon o varstvu osebnih podatkov in vzpostavljen nadzorni organ, ki bdi nad varstvom informacijske zasebnosti.

»Osebni podatek je katerikoli podatek, ki se nanaša na točno določeno ali vsaj določljivo osebo, ne glede na obliko, v kateri je izražen. Biometrične značilnosti se lahko štejejo za občutljive osebne podatke, vendar le, če je z njihovo uporabo mogoče določiti posameznika v zvezi s tistimi lastnostmi, ki jih zakon našteva kot občutljive osebne podatke (predvsem podatki o rasnem, narodnem ali narodnostnem poreklu ali zdravstvenem stanju). Kar velja za biometrične značilnosti kot take, velja tudi za digitalen zapis teh značilnosti, ki so sestavljeni na podlagi unikatnih značilnosti, ne glede na to, kolikokrat in kako je ta zapis kasneje spremenjen. Na podlagi tega lahko rečemo, da biometrični podatki, četudi shranjeni v reducirani, digitalizirani obliki, so vedno osebni podatki, saj se nanašajo na določeno ali vsaj določljivo osebo.« (IPRS, 2013)

Države Evropske unije imajo urejene zakonodaje o varovanju osebnih podatkov, saj so osebni podatki dokaj delikatno področje. Vsak poseg v namene identifikacije lahko predstavlja hud vdor v zasebnost in s tem kršenje demokratičnih vrednot. Z razvojem biometrične tehnologije je posegla tudi na to področje, da bi uredila pogoje uporabe in preprečila zlorabe. Zakon o varstvu osebnih podatkov (ZVOP-1) iz leta 2007 prvič omeni biometrične značilnosti in jih označi kot občutljive osebne podatke

⁵35. člen Ustave RS (varstvo pravic zasebnosti in osebnostnih pravic). Zagotovljena je nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti in osebnostnih pravic.

38. člen Ustave RS (varstvo osebnih podatkov). Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi (Ustava RS).

v kontekstu uporabe za namene identifikacije osebe. Biometrične značilnosti določijo kot telesne, fiziološke in vedenjske značilnosti, ki jih imajo vsi posamezniki. Zakonodaja na tem področju je dokaj stroga in informacijska pooblaščenka jo striktno izvaja, saj je prav ona tista, ki presodi potrebo in upravičenost uporabe biometrične tehnologije. Na eni strani imamo torej strogo izvajanje zakonodaje o uporabi, na drugi strani pa dostopnost sistemov in opreme s področja biometrične tehnologije. Dostopna je kompleksna oprema za širšo uporabo, kot tudi razni čitalci prstnih odtisov za vstop v stanovanje, za dostop do računalnika, ki so bolj namenjeni domači uporabi.

Letališče in celotni letalski promet spadata med kritično infrastrukturo in kot tako je varnostno preverjanje zelo pomembno.

8.1 Identifikacija kot grožnja zasebnosti in varnosti

Biometrična tehnologija je s svojim razvojem omogočila veliko prednosti. Vsaka stvar pa je dobra le, če se uporablja v dobre namene. Dobra stran je zanesljiva in učinkovita identifikacija, ki omogoča dostop do varnostno omejenih prostorov. Slaba stran je možnost ponarejanja in kraje identitete, s katero nas strašijo akcijski filmi. Biometrične lastnosti kot edinstvene in neponovljive predstavljajo veliko oviro za ponarejevalce. Kraja identitete pa ni edina skrb, ki jo imajo ljudje. Identifikacija sama predstavlja velik poseg v zasebnost in ni jih malo, ki so že ob oddaji vloge za pridobitev biometričnega potnega lista imeli pomisleke ob skeniranju prstnih odtisov. Dajanje prstnih odtisov ima že samo po sebi negativen priokus zaradi njihovega zbiranja v policijsko-kriminalistične namene. Še večji vdor v zasebnost predstavljajo procesi obrazne prepoznave oziroma vseh identifikacij, ki se lahko opravljajo brez vednosti tistega, ki se ga identificira. Zasedili smo tudi zaskrbljenost ljudi s področja uporabe biometričnih tehnologij, povezanih predvsem s higieno naprav. Čitalci prstnih odtisov so potencialni prenašalec raznih okužb, ko ljudje polagajo prste nanj, ne da bi ga primerno dezinficirali. S skeniranjem biometričnih podatkov iz oči, npr. šarenice, se pojavlja skrb o vplivu na vid.

Najpomembnejše pa se nam zdi vprašanje, kako varni so pravzaprav naši odvzeti biometrični vzorci pred krajo. Biometrični osebni podatki so odvzeti s pomočjo različnih tehnologij, vendar so vsi shranjeni v elektronski obliki, v bazah podatkov ali na strežnikih. Vsestransko vcepljanje strahu s strani medijev ali varnostnih podjetij, kako ranljivi znajo biti tudi najbolj varovani strežniki s podatki, pa zaupanja, da naši osebni podatki ne bodo zlorabljeni, ne zvišuje.

Biometrija po našem mnenju prinaša več dobrih stvari, pomeni zanesljivejše povezovanje osebe z njeno pravo identiteto, poleg tega je biometrične

identifikacijske vzorce težko ponarediti, kar po našem mnenju celo zmanjšuje možnosti kraje identitete.

8.2 Zakonska ureditev

Prstni odtisi, vzorci šarenice, obraz so biometrični podatki in nedvomno tudi osebni podatki. Ker so še toliko bolj občutljivi, saj so v nasprotju z imenom, priimkom, naslovom, edinstveni in lastni le posamezniku, so še občutljivejši. Za biometrične podatke velja ZVOP-1 (Zakon o varstvu osebnih podatkov, 2007), kjer je urejena splošna uporaba, obdelava in nadzor osebnih podatkov, biometrija pa je urejena v posebnem poglavju (78.–81. člen).

Splošna določba

Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitve posameznika. Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.⁶

Zavarovanje osebnih podatkov

Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov tako, da se:

- varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.⁷

⁶ 8. člen ZVOP-1

⁷ 24. člen ZVOP-1

Pogodbena obdelava

Upravljavca osebni podatki lahko posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe iz 24. člena tega zakona.

Pogodbeni obdelovalec sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih iz 24. člena tega zakona. Upravljavca osebni podatki nadzoruje izvajanje postopkov in ukrepov iz 24. člena tega zakona.

V primeru spora med upravljavcem osebnih podatkov in pogodbenim obdelovalcem je dolžan pogodbeni obdelovalec na podlagi zahteve upravljavca osebne podatke, ki jih je pogodbeno obdeloval, nemudoma vrniti upravljavcu. Morebitne kopije teh podatkov mora takoj uničiti ali jih posredovati državnemu organu, ki je v skladu z zakonom pristojen za odkrivanje ali pregon kaznivih dejanj, sodišču ali drugemu državnemu organu, če tako določa zakon.⁸

Namen zbiranja in nadaljnja obdelava

Osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.⁹

Neposredno opravljanje inšpekcijskega nadzora

Inšpekcijski nadzor neposredno opravlja nadzornik v mejah pristojnosti državnega nadzornega organa.¹⁰

Pristojnosti nadzornika

Pri opravljanju inšpekcijskega nadzora je nadzornik upravičen:¹¹

- pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter iznos osebnih podatkov v tretjo državo in posredovanje tujim uporabnikom osebnih podatkov,
- pregledovati vsebino zbirk osebnih podatkov ne glede na njihovo zaupnost ali tajnost in katalogov zbirk osebnih podatkov;
- pregledovati dokumentacijo in akte, ki urejajo zavarovanje osebnih podatkov;

⁸ 11. člen ZVOP-1

⁹ 16. člen ZVOP-1

¹⁰ 52. člen ZVOP-1

¹¹ 53. člen ZVOP-1

- pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;
- preverjati ukrepe in postopke za zavarovanje osebnih podatkov ter njihovo izvajanje;
- izvajati druge pristojnosti, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek;
- opravljati druge zadeve, določene z zakonom.

Biometrija

Z obdelavo biometričnih značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija oziroma preveri njegova identiteta pod pogoji, ki jih določa zakon.¹²

Zakon dovoljuje uporabo biometrije le v naslednjih primerih (IPRS, 2013).

Javni sektor: kadar tako določa zakon (npr. Zakon o potnih listinah državljanov Republike Slovenije), če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Izjemoma na podlagi posebnih zakonskih določil tudi za vstop v stavbo ali dele stavb in evidentiranje zaposlenih na delu.

Zasebni sektor lahko uporablja biometrijske ukrepe, če so nujno potrebni za:

- opravljanje dejavnosti,
- varnost ljudi ali premoženja,
- varovanje tajnih podatkov ali
- varovanje poslovne skrivnosti.

Zasebni sektor lahko biometrijske ukrepe izvaja le nad svojimi zaposlenimi, če so bili ti o tem predhodno pisno obveščeni. Če izvajanje biometrijskih ukrepov v zasebnem sektorju ni določeno z zakonom, mora tisti, ki želi uvesti biometrijske ukrepe, pridobiti odločbo Informacijskega pooblaščenca. Izvajanje biometrijskih ukrepov brez pozitivne odločbe Pooblaščenca je prekršek.

ZVOP-1 pod pojmom »biometrijskih ukrepov« zajema dva različna načina (postopka) prepoznave posameznika (IPRS, 2013):

- postopek, s katerim se ugotavljajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija;
- postopek, s katerim se primerjajo lastnosti posameznika, tako da se lahko preveri njegova identiteta oziroma istovetnost

¹² 78. člen ZVOP-1

Iz tega je razvidno, da zakon sicer loči med izvrševanjem identifikacije (prepoznavo) in preverjanjem identitete posameznika (istovetnost ali avtentikacijo), vendar za oba postopka uporablja enoten termin – biometrijski ukrep.

Zakonodajalec je uredil izdajo in uporabo potnih listih v posebnem zakonu o potnih listinah, s katerega povzemamo njihovo uporabo (Zakon o potnih listinah, 2011).

Evidence

Podatke iz evidence lahko uporabljajo delavci pristojnega organa, ministrstva, pristojnega za notranje zadeve, in ministrstva, pristojnega za zunanje zadeve, za opravljanje nalog s svojega delovnega področja, uporabljajo pa jih lahko tudi policisti, če gre za izvrševanje z zakonom določenih nalog /../.

Podoba obraza imetnika potne listine, shranjena kot biometrični podatek, in prstni odtisi oziroma prstni odtis, shranjen kot biometrični podatek na pomnilniškem mediju, se lahko uporabljajo le za preverjanje verodostojnosti potne listine in istovetnosti imetnika potne listine pri prehajanju državne meje.¹³

9 UPORABA BIOMETRIČNE TEHNOLOGIJE NA LETALIŠČIH

Zakon o letalstvu – Zlet (2010) opredeljuje letališče kot določeno kopensko ali vodno površino, vključno z objekti, napravami in opremo, ki je v celoti ali deloma namenjena za pristajanje, vzletanje in gibanje zrakoplovov. Cona letališča je določen kontroliran del zračnega prostora nad letališčem in okrog njega, namenjen varovanju letališkega prometa. Deli letališča so površine na letališču, ki funkcionalno služijo ali so prostorsko namenjene izvajanju dejavnosti obratovanja letališča ali dejavnostim uporabnikov letališča in drugim aktivnostim v zračnem prometu. Letališča so civilna, vojaška in mešana. Civilna letališča so javna ali se uporabljajo le za lastne potrebe. Letališča se razvrščajo glede na referenčno kodo, kategorijo in namen letališča ter obseg zračnega prometa.¹⁴ Letališče ima svojo infrastrukturo, v katero spadajo vzletno-pristajalne steze, svetlobni, navigacijski sistemi, potniški terminali, objekti in naprave varovanja in drugi objekti in naprave, namenjeni varnemu zračnemu prometu in obratovanju letališča.¹⁵ Na letališču delujejo tudi različne službe. Med obvezne spadajo reševalna in gasilska, služba za vzdrževanje, nadzor in upravljanje ploščadi, med drugimi tudi služba varovanja¹⁶ (Zakon o letalstvu, 2010).

¹³ 31. člen Zakona o potnih listinah 29/2011

¹⁴ 85. člen Zlet (letališča in vzletišča, splošne določbe)

¹⁵ 88. člen Zlet (letališka infrastruktura)

¹⁶ 89. člen Zlet (službe na letališču)

Službe varovanja so skrbijo za nadzor, varnostne preglede in varovanje na letališču. Varnostni službi morajo biti zagotovljene ustrezne površine, prostori in oprema za varnostne preglede zrakoplovov, potnikov, prtljage, letalskega tovora in stvari.¹⁷ Oprema se po letališčih razlikuje glede na potrebe, promet, finančno ozadje in biometrična tehnologija ni implementirana na vseh. V nadaljevanju smo predstavili nekaj primerov uporabe.

9.1 IRIS na letališču Heathrow

Leta 1930 je britanski inženir in letalski konstruktor Richard Fairey kupil zemljišče, da bi zgradil zasebno letališče in testiral letala. Ustvaril je travnato vzletno pristajalno stezo in nekaj stavb, kar je bilo le skromen predhodnik na svetu najbolj prometnega letališča Heathrow. Danes ima Heathrow (koda letališča LHR) 5 terminalov in 2 vzletno-pristajalni stezi. Z letališča leti 84 letalskih družb, ki pokrivajo destinacije v 80 državah. Leta 2012 so zaznali okoli 70 milijonov premikov potnikov. Osvojili so že veliko nagrad po izboru potnikov in strokovnih komisij, letošnje leto jim je bila podeljena tudi nagrada za najboljše letališče¹⁸ (Heathrow airport).

IRIS (iris recognition immigration system) je avtomatski sistem prepoznavne šarenice za namene identifikacije v sistemu priseljevanja. Uporabljajo ga na letališčih za vstop v državo. Sistem naj bi omogočal hiter vstop za registrirane uporabnike preko avtomatskih postaj, v katere vstopimo. Svoj obraz približamo napravi, ki s sofisticirano kamero prebere unikatni zapis naše šarenice in ga primerja z vzorci v shranjeni podatkovni bazi. Če vzorec ustreza shranjenemu zapisu v bazi, se vstop v državo odobri in avtomatizirana vrata se odprejo. IRIS je bil prvi sistem biometrične avtomatizirane mejne kontrole v Veliki Britaniji. Predstavljen je bil leta 2004 v Londonu. Po mnenju britanske vlade naj bi skrajšal čakalne vrste in zmanjšal možnosti vstopa s ponarejenimi listinami.

Uporaba (UK Boarder agency):

V sistem IRIS prijava ni več mogoča, ko pa je bila, so se lahko prijavile osebe:

- državljani in osebe, ki imajo stalno prebivališče v Veliki Britaniji,
- prebivalci držav EU,
- osebe z delovnim dovoljenjem v Veliki Britaniji in njihovi družinski člani,
- osebe, ki pogosto potujejo iz Velike Britanije in vanjo vstopajo.

Prijavili so se lahko na prijavnih terminalih ob odhodu iz Velike Britanije. Prijavo so opravili z veljavnim potnim listom, predložiti pa so morali tudi letalsko vozovnico kot potrdilo o odhodu in destinaciji. Celoten postopek ni trajal več kot 15 minut, na kontaktni naslov pa so poslali tudi natančna navodila o uporabi avtomatskih mejnih

¹⁷ 127. člen Zlet (varnostni preglede in varovanje)

¹⁸ Nagrada za najboljše letališče v kategoriji letališč z več kot 25 milijonov potnikov po izboru ACI EUROPE awards (Airport Council International)

kontrol ob prihodu oziroma vrnitvi v Veliko Britanijo. Migracijska služba je preverila pristnost in lastništvo potnega lista. V sistem je vnesla njegove osebne podatke, podatke o potnem listu in bivalnem statusu (državljan, tujec, bivanje). Glede na te podatke je odvisna tudi doba veljavnosti; osebe s stalnim prebivališčem v Veliki Britaniji so v sistemu vnesene 2 leti, če pa je ta doba že potekla, so napoteni na klasično kontrolo. Ko so bili vsi podatki vneseni, so potniki približali obraz kameri, da je posnela fotografijo obraza in skenirala vzorec šarenice vsakega očesa posebej. Vzorec šarenice se je nato prevedel v kodo, ki jo je sistem shranil v svojo bazo podatkov.

Potek:

Sistemi IRIS so postavljeni kot postaje, kabine, v katerih poteka preverjanje. Potnik pristopi h kabini in ko ga senzor zazna, se odprejo avtomatska vrata za vstop v kabino. Potnik vstopi in se približa kameram, ki so višinsko razporejene glede na višino potnikov. S seboj lahko vzame vso prtljago, da le ne zastira kamer. Potnika vodi posnet glas, ki ga usmerja na pravilen položaj do ene izmed treh kamer, ki so vgrajene, da lahko posnamejo najbolj optimalno sliko šarenic. Priporočljivo je, da se ne premikamo, da senzori hitreje nastavijo kamere v pravilen položaj. Če je sistem uspešno povezal odvzet vzorec z registrirano osebo, se izhodna vrata avtomatsko odprejo in s tem odobrijo vstop. Namesto žiga v potni list se natisne listič, ki nadomešča žig. Če ne pride do odobritve vstopa v prvem poizkusu, lahko potnik večkrat poizkusi, dokler ne doseže odobritve. V nasprotnem primeru se ponovno odprejo vstopna vrata, skozi katera lahko potnik, pri katerem so nastali problemi pri skeniranju, zapusti kabino in uredi vstopne dokumente na klasični kontroli ali ponovno poizkusi. Pred skeniranjem je potrebno odstraniti obarvane kontaktne leče, medtem ko uporaba brezbarvnih kontaktnih leč ali korekcijskih očal ne povzroča problemov.

Tehnologija se je sčasoma izkazala za nezanesljivo. Kamere velikokrat niso prepoznale vzorca in odprle vrat, ljudje so ostajali ujeti, poleg tega so sistemi zaradi človeške dinamike potrebovali za skeniranje veliko več kot le 12 sekund, kot je bilo sprva predvideno. Naprave so že umaknili z večine britanskih letališč, ostaja le še na letališču Heatrow na dveh terminalih za že registrirane uporabnike, novih vpisov pa ne izvajajo več. Poleg problemov z delovanjem so mejne kontrole IRIS pričeli zamenjevati veliko bolj učinkoviti sistemi, ki delujejo z uporabo biometričnih potnih listov.



Slika 13: Iris recognition system

(Vir: <http://www.dailymail.co.uk/news/article-2102076/Millions-drain-airports-SCRAP-iris-passport-scanners.html>)

9.2 Vrata Easypass na letališču Frankfurt

Frankfurtsko letališča (koda letališča FRA) je s svojimi letalskimi operacijami pričelo leta 1936. Je najbolj obremenjeno nemško komercialno letališče. Ima 2 terminala in 2 vzletno-pristajalni stezi. Delovno območje letališča se razprostira čez približno 21 kvadratnih metrov in zagotavlja objekte za letalske prevoznike in druge najemnike, pa tudi širok spekter letaliških storitev. V svetu zaseda 9. mesto po merilu prometa, beležijo dokaj konstantno rast prometa potnikov, v letu 2012 so jih odpravili in sprejeli rekordno število 57,5 milijonov (Frankfurt airport).

Easypass (lahek prehod) temelji na e-potnih listih in tehnologiji obrazne prepoznave. Sistem je v pristojnosti nemške Zvezne policije (Bundespoleizei), Zvezni urad za informacijsko varnost (BSI – Bundesamt für Sicherheit in der Informationstechnik) in uprave letališča Frankfurt – Fraport. Z uporabo so začeli avgusta 2009 s štirimi avtomatskimi kabinami in eno nadzorno postajo. Po poizkusnem obdobju so začeli z rednim izvajanjem.

Postopek Easypass uporablja podatke, shranjene na elektronskem čipu potnega lista. Sestavljen je iz sistema senzorjev, kamer in avtomatskih vrat, vse skupaj je narejeno kot kabina. Easypass je varna in priročna alternativa postopkom mejne kontrole, ki lajša in pospešuje mejne kontrole na letališču Frankfurt. Sistem uporablja tehnologije prepoznave obraza, skeniran obraz primerja z obrazom na fotografiji, shranjeni na čipu potnega lista. Ko sistem opravi prepoznavo, se vrata avtomatsko odprejo in lahko gredo skozi. Za uporabo vrat ne potrebujemo

nobene registracije ali predhodnega vpisa v sistem. Uporabljamo jih lahko le z veljavnim potnim listom držav članic Evropske unije, Norveške, Islandije, Liechtensteina in Švice. Po vsaki uporabi, ko je vstop odobren, se podatki takoj izbrišejo iz sistema, kar zagotavlja maksimalno varnost. Vse skupaj je pod video nadzorom, da lahko mejni uradniki izvajajo nadzor nad celotnim postopkom. Veliko potnikov ni seznanjenih, da imajo e-potni list in kako ga uporabiti, na splošno pa so uporabniki elektronske mejne kontrole predvsem zaradi hitrosti uporabe zelo zadovoljni. Za uporabo velja le starostna omejitev 18 let. Število do zdaj znanih napak, ko je sistem napačno zavrnil potnika, je zanemarljivo.

Potek:

Ko prispemo do vrat Easypass, nas uslužbenec, ki nadzoruje, da postopek teče, usmeri h kabinam glede na naše potne liste. Torej če že imamo potne liste z elektronskim čipom, kar je označeno na platnici, lahko stopimo do prazne kabine in pripravimo svoj potni list. Odpremo ga na strani s fotografijo in trdno položimo na skener, ki je postavljen ob vstopu. Potni list s fotografijo mora biti obrnjen navzdol. Ko skener potrdi, da je prebral naš potni list, ga lahko odstranimo in vstopimo v kabino. Odstraniti moramo vse objekte, ki bi lahko zakrivali naš obraz, kot so klobuk, očala in drugo. Stopimo na točno določene oznake na tleh in pogledamo naravnost v kamero. Senzorji, nameščeni ob strani kabine, zaznajo telo, ki mora biti v določenem položaju, in višini primerno prilagodijo kamero, da zajame optimalno sliko obraza. Sistem primerja zajet obraz z obrazom na fotografiji in potrdi ujemanje. Po pozitivni prepoznavi se vrata avtomatsko odprejo in lahko zapustimo kabino, saj nam je bil odobren vstop v državo. Vse skupaj poteka zelo hitro, avtomatizirano in ni nam potrebno čakati v dolgih vrstah pred mejnim uradnikom. Do mejnega uradnika moramo le, če bi nas sistem zavrnil.



Slika 14: Potek Easypassa

(Vir:

<http://ec.europa.eu/avservices/photo/photoByMediaGroup.cfm?sitelang=en&mgid=630>)

Celoten proces poteka zelo hitro, izračunali so, da traja 18 sekund (Marzahn, 2011).

- 5–6 sekund potrebuje optični ali elektronski skener za preverjanje e-potnega lista.
- 5–6 sekund, da potnik vstopi v kabino.
- 1 sekunda za odvzem slike obraza in primerjavo.
- 5–6 sekund, da potnik zapusti kabino.

Po tem postopku se je sistem takoj pripravljen sprejeti novega potnika. Očem nevidno pa v postopku potekajo številni varnostni sistemi. Usklajeni evropski predpisi za nadzor meja zahtevajo preverjanje, ali potnik sploh ima dovoljenje za

prehod meje. S tem namenom sistem v prvem koraku preveri veljavnost in verodostojnost e-potne listine na podlagi digitalnih certifikatov, ki smo jih že omenili v poglavju o biometričnih potnih listih. V naslednjem koraku se osebni podatki primerjajo z iskanimi osebami v policijskem omrežju. V policijskem omrežju se preveri tudi certifikat izdanega potnega lista, kar omogoča zanesljivo odkrivanje ukradenih ali prirejenih potnih listov. Če sistem odkrije kakršnokoli napako, se vse informacije izpišejo na nadzornikovem monitorju v nadzorni postaji, ki izvede nadaljnje ukrepe. Drug scenarij je kraja in zloraba potnega lista osebe, ki izgleda podobno. V takih primerih biometrična obrazna prepoznavna z algoritmi, ki so skoraj 100-odstotno zanesljivi, opozori na prevaro (Gate case study, maj 2010).

9.3 PARAFE na letališču Charles de Gaulle

Letališče Charles de Gaulle (koda letališča CDG) je drugo najprometnejše evropsko drugo najprometnejše letališče, takoj za londonskim Heathrowom. Imenuje se po francoskem predsedniku, ki je predsedoval v času druge svetovne vojne. Odprlo se je leta 1974. Trenutno ima 3 terminale, 1. terminal je namenjen mednarodnim potnikom, 2. uporablja Air France in druge evropske letalske družbe, terminal 3 pa je namenjen izključno čarterskim letom. V svetu se z 61,6 milijoni potnikov v letu 2012 uvršča na 7 mesto po prometu.

PARAFE – Le Passage Automatisé Rapide aux Frontières Extérieures je kratica, ki pomeni avtomatiziran hiter prehod zunanjih schengenskih meja. Uporaba sistema je bila odobrena z odlokom Evropske unije avgusta 2007. Z njegovo uporabo lahko potniki, če želijo, samostojno, enostavno in hitro prečkajo mejo z avtomatsko kontrolo potnih listov. Sistem uporablja tehnologijo biometričnega preverjanja identitete s skeniranjem prstnih odtisov. Uporaba sistema je brezplačna in prostovoljna. Dovoljena je polnoletnim državljanom Evropske unije, Evropskega gospodarskega prostora (EGP) ali švicarske konfederacije, ki imajo biometrične potne liste oziroma potne liste, ki so elektronsko berljivi (kar so bili že potni listi pred 2005). Registracijo dovoljujejo tudi državljanom držav nečlanicam prej omenjenih držav, ki imajo dovoljenje za prebivanje oziroma so družinski člani državljana Evropske unije. Potniki s francoskim biometričnim potnim listom registracije ne potrebujejo, vsi ostali potniki pa se morajo registrirati v sistem. Registracijo lahko potnik na letališču Charles de Gaulle opravi vsak delovni dan, če potuje iz odhodnih terminalov 1 ali 2, pri mejnih uradnikih. Za registracijo potrebuje elektronsko berljiv potni list, veljaven še vsaj 6 mesecev, odvzamejo pa mu prstne odtise osmih prstov razen palcev. Prstni odtisi se uporabljajo le v namene identifikacije in za nikakršna druga preverjanja. Po registraciji potnik preizkusi uspešnost registracije in se seznanji z uporabo na testnem terminalu PARAFE. Registracija je veljavna 5 let na letališčih, ki so opremljeni s sistemom PARAFE. Poleg letališča Charles de Gaulle je to še pariško letališče Orly (Aéroport de Paris).

Potek:

Ko je potnik registriran v sistem, lahko mejo prečka hitreje tako ob odhodu kot ob prihodu. Kabine so sestavljene podobno kot pri sistemu Easypass. Nahajajo se poleg mejnih kontrol, ki jih kontrolirajo mejni uradniki. Ob prihodu se postavimo v vrsto in počakamo, da je kabina prosta. Pristopimo do čitalca potnih listov, ki je nameščen ob vstopu v kabino. Ko je potni list preverjen, se odprejo avtomatska vrata, skozi katera vstopimo v kabino. Poiščemo skener prstnih odtisov in nanj položimo enega izmed skeniranih prstov, najpogosteje kazalec. Ko sistem potrdi avtentikacijo, se odprejo avtomatska izhodna vrata, skozi katera izstopimo. Vse skupaj traja približno 30 sekund (Parafe, 2012).



Slika 15: Sistem PARAFE na pariškem letališču

(Vir: <http://corporate.airfrance.com/en/press/media-library/photos/latest-news/hub-2012/image/parafe-at-paris-charles-de-gaulle-page15a/>)

10 ZAKLJUČEK

V nalogi smo spoznali prstne odtise, ki so lastni vsakemu človeku, od zarodka do razkroja, njihova unikatnost pa jih dela uporabne za namene identifikacije. Prstne odtise so sprva in poglavitno uporabljali z odvzemom s kraja zločina in jih uporabili za iskanje storilcev. Za odvzem prstnih odtisov s kraja zločina se uporabljajo različne tehnike, v avtomatizirani identifikaciji pa se odvzemi opravljajo z različnimi čitalci, kot so optični, termični in najbolj uporabljeni kapacitativni.

Obrazna prepoznavna ima dolgo zgodovino, temelji na človekovem nezavednem, vsakodnevnem opazovanju oseb in povezovanju opazovančevih lastnosti, potez in videza z že znanimi osebami. Tudi za obrazno prepoznavo obstajajo različni sistemi, najnovejši pa je trenutno sistem s 3D-obdelavo.

Oko je organ, ki nam omogoča najpomembnejše čutilo, vid. Šarenica je mišica v očesu, ki ga vidimo kot obarvani del, pri vsakem človeku je drugačna in edinstvena, kar omogoča trenutno najzanesljivejšo metodo prepoznave ljudi.

V nalogi smo predstavili tudi biometrične potne liste. Na prvi pogled se ne razlikujejo od dosedanjih, imajo pa čipe, na katere se lahko spravi različne podatke, od običajnih osebnih, kot so ime, naslov, do biometričnih, kot so prstni odtis.

Biometrija in z njo biometrična tehnologija v zadnjih desetih letih doživljata svoj razcvet. K pospešenemu razvoju metod so pripomogli različni varnostni vdori in nesrečni dogodki 2001 v ZDA. ZDA so pospešile in zahtevale uvedbo biometrije, da bi se obvarovale pred morebitnimi podobnimi napadi in nadzorovale promet potnikov ne le na notranjih letih znotraj Amerike, temveč tudi na medcelinskih, ko potniki prihajajo v ZDA z različnih destinacij. Amerika je na področju razvoja in uporabe biometrične tehnologije še vedno vodilna, vendar Evropa ne zaostaja veliko za njo. To smo dokazali s praktičnimi primeri uporabe različne biometrične opreme na večjih letališčih v Evropi. Predstavljeni sistemi biometričnih avtomatskih mejnih kontrol so prvi delujoči in uporabni sistemi. Imeli so nekaj poporodnih težav, ki pa jih uspešno odpravlja tehnološki napredek. Evropa je uvedla biometrične potne liste, ki so popolnoma podobni dosedanjim, vendar vsebujejo različne osebne podatke lastnika, ki so v pomoč predvsem mejnim kontrolorjem, za identifikacijo in nadzor varnostnim odobritvam osebam za prečkanje meje. Na letališču Frankfurt so mejno kontrolo potnih listov uspešno avtomatizirali z avtomatskimi vrati Easypass, ki je hiter in zanesljiv sistem, predvsem pa prijazen uporabnikom in ima največ potenciala, da ga uvedejo tudi na druga letališča.

V uporabi je tudi sistem obrazne prepoznavne in celo skeniranje šarenice za namene identifikacije. Sistemi identifikacije šarenice so se v praksi izkazali za najbolj zanesljive, čeprav so pri ljudeh zbužali največ skepse in strahu, kar se tiče varne

uporabe žarkov skenerja, kar tudi botruje k počasnemu ukinjanju sistema IRIS na letališču Heathrow. Obrazna prepoznavna kljub svojemu opaznemu napredku še vedno potrebuje dovolj robustne algoritme, ki bodo odporni na spremembe videza, kot so obrazne dlake, lasje, očala in morebitne plastične operacije. Vsi ti sistemi so le začetna postaja na poti uvajanja in izpopolnjevanja novih tehnologij in sistemov ter vodijo k popolni avtomatizaciji mejnih kontrol, ki bo zagotovo zanesljivejša in hitrejša.

Biometrična tehnologija je velik skok v prihodnost, ki jo je povzročil razvoj tehnologije in potreba po učinkovitih in zanesljivih sistemih identifikacije. Pomembno je, da jo sprejemamo kot del napredka in pot k zagotavljanju večje varnosti. Ne moremo mimo vprašanja, kako in v kolikšni meri bo biometrična tehnologija vplivala na zasebnost posameznika. Sistemi prepoznave uporabljajo unikatne človeške lastnosti, ki jih hranijo v posebnih zbirkah, bazah podatkov. Kraja tako delikatnih podatkov bi lahko imela nepopravljive posledice. Kljub vsem akcijskim filmom, ki nas strašijo s krajo identitete, je biometrične podatke težko ponarediti, kar po našem mnenju vseeno zagotavlja veliko mero zaupanja v sisteme.

V nalogi smo predstavili zakonske omejitve poseganja v zasebnost z biometričnimi sistemi in ugotovili, da je področje samo še dokaj slabo raziskano in zakonski okvirji le bežno določeni oziroma strožji, kot bi bilo potrebno. S povečevanjem uporabe biometrične tehnologije, ne le na letališčih, temveč tudi v zasebni rabi, lahko pričakujemo ureditev konkretnjših pravnih podlag. Urad informacijske pooblaščenke prejme največ prošenj delodajalcev, ki želijo uporabljati biometrično tehnologijo za evidentiranje prisotnosti na delu. Urad več prošenj zavrne kot odobri, saj se te evidence lahko vodijo tudi z milejšimi ukrepi. To je le potrditev, da se pridobivanje biometričnih podatkov uvršča med hude posege v zasebnost in ne le kot običajne osebne podatke. Biometrični podatki so le osebni podatki in izvajanje zakona bi morala prevzeti sodišča in inšpekcije, umakniti pa bi morali tudi pridobivanje dovoljenj pri informacijski pooblaščenki in dovoliti, da se delodajalci in zaposleni oziroma vsi polnoletni državljani sami dogovorijo o uporabi biometrične tehnologije.

Letalski promet je dokaj mlada prevozna panoga, ki se je v tehnološkem smislu hitro razvila, sedaj pa se razvoj nadaljuje le v smislu ponudbe in dostopnosti. Letalski prevozniki želijo polete cenovno čim bolj približati širšim množicam, kar jim predvsem na področju turizma dobro uspeva. V letalskem prometu se varnostni standardi konstantno dvigajo, čemur na žalost botrujejo tudi letalske nesreče in teroristični napadi. Uporaba biometrične tehnologije v letalski promet je pomenila predvsem skrajšanje čakalnih vrst z avtomatiziranimi prehodi mej, vendar tudi vpeljala nove standarde na področju varnosti, s tem da je vstop odobren le identificiranim osebam.

Dotaknili smo se tudi letališč kot sestavnega dela letalskega prometa. Letališča so zaprti sistemi s specifičnim delovanjem in ureditvijo. Pomembna so za pretok dobrin in ljudi, njihova funkcionalnost raste vzporedno z letalskim prometom. Slovenija je kljub svoji majhnosti, ne le po ozemlju, predvsem po številu prebivalcev, letalsko dobro razvita. Ima tri mednarodna letališča, ki so strateško postavljena na različne dele Slovenije: v Ljubljano, Maribor, Portorož. S tremi letališči, izmed katerih je večjim letalom in potniškemu prometu namenjeno le ljubljansko, v svetu nima velike vloge, vsa letališča pa predstavljajo kritično infrastrukturo za Republiko Slovenijo in njene prebivalce. Pod kritično infrastrukturo se uvrščajo, ker bi prekinitev ali onemogočenje njihovega delovanja pomenila izpad pretoka dobrin in ogrozila blaginjo ljudi.

11 Bibliografija

- Biometrics.* (7. avgust 2006). Pridobljeno 31. 7. 2013 z naslova Biometrics.gov: <http://www.biometrics.gov/Documents/irisrec.pdf>.
- Biometrics history.* (2006). Pridobljeno 31. 7. 2013 z naslova <http://www.biometrics.gov/documents/biohistory.pdf>.
- Zakon o varstvu osebnih podatkov.* (16. oktober 2007). Pridobljeno 17. 7. 2013 z naslova zakonodaja.gov.si.
- Direktiva sveta.* (8. december 2008). Pridobljeno 16. 6. 2013 z naslova: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SL:PDF>.
- Zakon o letalstvu.* (15. oktober 2010). Pridobljeno 17. 7. 2013 z naslova <http://www.uradni-list.si/1/objava.jsp?urlid=201081&stevilka=4332>.
- Zakon o potnih listinah.* (18. april 2011). Pridobljeno 17. 7. 2013 z naslova zakonodaja.gov.si.
- Bayometric inc.* (18. 6 2012). Pridobljeno 8. 4. 2013 z naslova False Acceptance Rate (FAR) & False Recognition Rate (FRR): <http://www.bayometric.com/blog/index.php/biometric-security-systems/false-acceptance-rate-far-false-ecognition-rate-frr/>.
- E-uprava.* (23. 3 2012). Pridobljeno 2. 4. 2013 z naslova <http://e-uprava.gov.si/e-uprava/dogodkiPrebivalci.euprava?zdid=1213&sid=119>.
- Parafe.* (2012). Pridobljeno 8. 4. 2013 z naslova <http://www.parafe.gouv.fr/wp-content/uploads/2012/06/Fiche-FAQ-PARAFES-GB.pdf>.
- Aéroport de Paris.* Pridobljeno 9. 4. 2013 z naslova PARAFE: <http://www.aeroportsdeparis.fr/ADP/en-GB/Passagers/Procedure-practical-information/Crossing-Borders-Easily/>.
- Anžič, M. (2003). *Vloga biometričnih metod v boju proti terorizmu*. Ljubljana: Fakulteta za družbene vede.
- Chirillo, & Blau. (2003). *Glossary of biometric terms*.
- Delač, K., & Grgič, M. (2007). *Face-rec*. Pridobljeno 9. 4. 2013 z naslova http://www.face-rec.org/journals-books/Delac_Grgic_Face_Recognition.pdf.
- DuVal, A. *Forensic psychology*. Pridobljeno 8. 4. 2013 z naslova <http://forensicpsych.umwblogs.org/research/criminal-justice/face-recognition-software/>.
- Frankfurt airport.* Pridobljeno 17. 7. 2013 z naslova http://www.frankfurt-airport.com/content/frankfurt_airport/en/misc/container/facts-and-figures-2011/jcr:content.file/zadafa-2012_e_lowres.pdf.
- Garb, G. (2009). *Varnostno upravljanje kritične infrastrukture*. Magistrska naloga, Celje: Fakulteta za logistiko. Pridobljeno 16. 6. 2013 z naslova <http://dkum.uni-mb.si/Dokument.php?id=10068>.
- Geringer, J. (2003). *Vidocq: Convict Turned Detective Magnifique*. Pridobljeno 17. 7. 2013 z naslova http://www.trutv.com/library/crime/gangsters_outlaws/cops_others/vidocq/4.html: Crime library.
- Heathrow airport.* Pridobljeno 17. 7. 2013 z naslova <http://www.heathrowairport.com/about-us/>.

- Homeland security*. Pridobljeno 2. 7. 2013 z naslova <http://www.dhs.gov/what-critical-infrastructure>.
- IPRS. (2013). Pridobljeno 2. 7. 2013 z naslova <https://www.ip-rs.si/varstvo-osebni-podatki/informacijske-tehnologije-in-osebni-podatki/biometrija/>.
- Iris ID*. Pridobljeno 8. 4. 2013 z naslova How it works: <http://www.irisid.com/howitworks>.
- Klopčič, U. (2009). *Sistem za verifikacijo osebe na podlagi prstnega odtisa*. Diplomsko delo, Ljubljana: Fakulteta za računalništvo in informatiko.
- Lah, P. (2007). *Kripto*. Pridobljeno 2. 4. 2013 z naslova <http://www.si-ca.si/kripto/krpotnilist.htm>.
- Li, S. Z., & Jain, A. K. (2011). *Handbook of face recognition*. London: Springer.
- Aerodrom Ljubljana. Pridobljeno 9. 4. 2013 z naslova <http://www.lju-airport.si/o-podjetju/gradimo-za-prihodnost/?url=/o-podjetju/gradimo-za-prihodnost/&ID=&fName=vsebina.asp&IDM=171>.
- Marzahn, B. (7. 9. 2011). *ICAO*. Pridobljeno 8. 4. 2013 z naslova e-gate case study: http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-20/TagMrtd-20_Pres_Marzahn.pdf.
- Maver, D. (2004). *Kriminalistika*. Ljubljana: Uradni list Republike Slovenije.
- Mraovič, M. (29. 9. 2006). *Biometrične metode v sistemu pristopne kode*. Pridobljeno 8. 4. 2013 z naslova <http://dat.si/publikacije/Article/Biometri--269-nemetode-v-sistemu-pristopne-kode/44>.
- NCOIC. Pridobljeno 9. 4. 2013 z naslova [ncoic.org: https://www.ncoic.org/technology/what_is_interoperability/](https://www.ncoic.org/technology/what_is_interoperability/).
- Pengal, B. (2008). *Kritična transportna infrastruktura v Republiki Sloveniji*. Magistrska naloga, Ljubljana: Fakulteta za družbene vede.
- Prezelj, I. (2001). Grožnje varnosti, varnostna tveganja in izivi v sodobni družbi. *Teorija in praksa*, 130.
- Prstni odtis*. Pridobljeno 9. 4. 2013 z naslova <http://www.prstni-odtis.si/si/lastnosti>.
- Tecnovelgy*. Pridobljeno 9. 6. 2013 z naslova <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=72>.
- Trapečar, M., & Robek, A. (2003). Sodobne biometrične metode pri verifikaciji identitet posameznikov ter njihova uporabnost v letalskem prometu. *Varstvoslovje*, 49.
- UK Boarder agency*. Pridobljeno 9. 4. 2013 z naslova <http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/>.
- Upravne enote*. Pridobljeno 2. 4. 2013 z naslova [Upravneenote.org: http://www.upravneenote.gov.si/fileadmin/pageuploads/ueljutomer/pdf/Novice/biometricni_potni_listi.pdf](http://www.upravneenote.gov.si/fileadmin/pageuploads/ueljutomer/pdf/Novice/biometricni_potni_listi.pdf).
- Ustava RS*. Pridobljeno 17. 7. 2013 z naslova <http://www.us-rs.si/media/ustava.republike.slovenije.pdf>.
- Wiger, I., & Dunn, M. (2004). *An Inventory And Analysis Of Protection Policies in Fourteen Countries*. Pridobljeno 16. 6. 2013 z naslova <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.195.4030>.

Wikipedija. *Wikipedija*. Pridobljeno 9. 6. 2013 z naslova <http://sl.wikipedia.org/wiki/Algoritem>.

KAZALO SLIK

Slika 1: Število prepeljanih potnikov v 1000 na letališču Jožeta Pučnika	12
Slika 2: Vzorci prstnih odtisov	15
Slika 3: Dvojna zanka	15
Slika 4: Naključna razporeditev	16
Slika 5: Jedro in delta	16
Slika 6: Primeri minucij	17
Slika 7: Potek obrazne prepoznave	22
Slika 8: 3D-posnetek obraza	24
Slika 9: Oko	25
Slika 10: Lociranje šarenice	26
Slika 11: Vzorec potnega lista	29
Slika 12: Podatki na čipu potnega lista	30
Slika 13: Iris recognition system	41
Slika 14: Potek Easypassa	43
Slika 15: Sistem PARAFE na pariškem letališču	45

KRATICE

- **DNK:** Deoksiribonukleinska kislina
- **AFIS:** Automatic Fingerprint Identification system (sistem za avtomatsko identifikacijo prstnih odtisov)
- **FBI:** Federal Bureau of Investigation (ameriška zvezna agencija za preiskovanje)
- **3D:** Tridimenizionalno
- **FAR:** False Acceptance Rate (število lažnih sprejemov)
- **FRR:** False Rejection Rate (število lažnih zavrnitev)
- **EER:** Equal Error Rate (enaka skupna vrednost FAR in FRR)
- **RS:** Republika Slovenija
- **EU:** Evropska unija
- **NATO:** North Atlantic Threat Organization (Organizacija severnoatlantskega sporazuma)
- **ZDA:** Združene države Amerike
- **FERET:** Facial Recognition Technology Evaluation (ocena uporabnosti tehnologije)
- **FRVT:** Face recognition Vendor Test (testi prodaje tehnologije obrazne prepoznave)

- **FRGC:** Face Recognition Grand Challenge (tekmovanje tehnologije obrazne prepoznavne)
- **2D:** Dvodimenzionalno
- **ICAO:** International Civil Aviation Organization (mednarodna organizacija civilnega letalstva)
- **VWP:** Visa Waiver Program (program, ki omogoča prebivalcem določenih držav, da potujejo v ZDA za 90 dni, ne da bi potrebovali vizo)
- **MRZ:** Machine readable zone (strojno berljivi podatki)
- **BAC:** Basic access control (osnovna kontrola dostopa)
- **EAC:** Extended access control (razširjena kontrola dostopa)
- **ZVOP:** Zakon o varstvu osebnih podatkov
- **IPRS:** Urad Informacijskega pooblaščenca Republike Slovenije
- **Zlet:** Zakon o letalstvu Republike Slovenije
- **IRIS:** Iris Recognition Immigration System (avtomatski sistem prepoznave šarenice, za namene identifikacije v sistemu priseljevanja)
- **UK:** United Kingdom (Združeno kraljestvo Velike Britanije)
- **BSI:** Bundesamt für Sicherheit in der Informationstechnik (Zvezni urad za informacijsko varnost v Nemčiji)
- **PARAFE:** le Passage Automatisé Rapide aux Frontières Extérieures
- **EGP:** Evropski gospodarski prostor