Inovacije u biometriji

Desović, Anja

VELEUČILIŠTE U RIJECI

Anja Desović

INOVACIJE U BIOMETRIJI

(završni rad)

Rijeka, 2020.

VELEUČILIŠTE U RIJECI
Odjel Sigurnost na radu
Stručni studij Sigurnosti na radu

INOVACIJE U BIOMETRIJI

(završni rad)

MENTOR

Ivan Grakalić, viši predavač

STUDENT

Anja Desović

MBS: 2426000016/15

Rijeka, listopad 2020.

VELEUČILIŠTE U RIJECI
Odjel sigurnosti na radu

Rijeka, 1.7.2020.

ZADATAK
za završni rad

Pristupnica: Anja Desović MBS 2426000016/15

Studentici stručnog studija Sigurnosti na radu izdaje se zadatak za završni rad – tema završnog rada pod nazivom:

INOVACIJE U BIOMETRIJI

Sadržaj zadatka:

Opisati pojam biometrije u kontekstu kontrole pristupa. Opisati povijesni pregled te različite biometrijske metode prisutne na tržištu. Obraditi inovacije u biometrijskim tehnologijama i tržištu unazad 5 godina. Osvrnuti se na GDPR i sigurnost biometrije.

Preporuka:

Koristiti podatke s tržišta i mrežne izvore

Rad obraditi sukladno odredbama Pravilnika o završnom radu Veleučilišta u Rijeci.

Zadano: 1.7.2020.

Predati do: 15.9.2020.

Mentor:
Ivan Grakalić, v. pred

Pročelnica odjela:
Erika Gržin, v. pred.

Zadatak primio dana: 1.7.2020.

Anja Desović

IZJAVA

Izjavljujem da sam završni rad pod naslovom INOVACIJE U BIOMETRIJI izradio samostalno pod nadzorom i uz stručnu pomoć mentora IVANA GRAKALIĆA.

Ime i prezime

(potpis studenta)

SAŽETAK

Ovaj rad bazira se na traženju i praćenju novih tehnologija i inovacija u biometriji, i to od 2016. godine pa sve do sada. Uz to, u prvom dijelu rada koji služi kao svojevrstan vodič kroz biometriju i njen razvoj, ukratko se objašnjavaju pojmovi vezani uz biometrijske metode i tehnologije te poveznica između identiteta i mjerenja ljudskog života kako bi se utvrdio pojedini identitet osobe. Također se navode najnoviji trendovi i razvoj tehnologije u biometriji koji se dijele na sustave za video nadzor, razne senzore za otiske prstiju i lica i multimodalnu biometriju za koju se smatra da je puno bolja u identificiranju od unimodalne. Na kraju se razglaba o samoj sigurnosti u biometriji na način da se uspoređuje svrha biometrije i neke kontroverze u svezi sa biometrijom pri čemu se zaključuje da biometrija kao dio kontrole pristupa dodaje dodatni sloj zaštite naspram uobičajenih tipkovnica i lozinki te je puno sigurnija metoda.

KLJUČNE RIJEČI: biometrijska identifikacija, kontrola pristupa, biometrija, identitet

SADRŽAJ

1. UVOD 1
2. BIOMETRIJA 2
2.1. Učestalost korištenja biometrijske tehnologije i autentifikacije na tržištu 3
3. BIOMETRIJSKE METODE 5
3.1. Fiziološke biometrijske metode 5
3.2. Ponašajne biometrijske metode 7
3.3. Multimodalna biometrija 8
4. IDENTITET I BIOMETRIJA 11
4.1. Biometrijski podaci i GDPR 13
4.2. Primjena biometrijske tehnologije u suvremenom svijetu 14
4.3. Civilni identitet i registracija stanovništva 17
5. INOVACIJE U BIOMETRIJI 25
5.1. Inovacije u video nadzoru 26
5.2. CES 2019. 27
5.3. Inovacije u svijetu 29
6. BIOMETRIJSKA SIGURNOST 37
7. ZAKLJUČAK 39
POPIS LITERATURE 40
POPIS SLIKA I GRAFIKONA 42

1. UVOD

Biometrija je jedno od najvažnijih sredstava identifikacije i autentifikacije pojedinaca na pouzdan i brz način pomoću jedinstvenih bioloških karakteristika. Biometrija je znanost koja se koristi od davnih vremena i prati razvoj ljudskog znanja, tehnologije te znanosti.

U ovom radu obradit će se povijest biometrije, primjena biometrije u sigurnosti pojedinaca i kompanija, inovacije u biometriji i njihova primjena u budućnosti, problemi sigurnosti biometrije i voljnost ljudi da pristanu na biometrijsko identificiranje .

Drugo poglavlje „Biometrija“ , treće poglavlje „Biometrijske metode“ i četvrto poglavlje „Identitet i biometrija“ pobliže će opisati biometriju kao znanost i podjelu biometrije na ponašajne, odnosno bihevioralne biometrijske metode, fiziološke biometrijske metode i multimodalnu metodu povezanost identiteta i biometrije, biometriju i GDPR te primjenu biometrijske tehnologije u suvremenom svijetu te civilni identitet i registraciju stanovništva.

U petom poglavlju „Inovacije u biometriji “ obradit će se inovacije i trenutačni trendovi u svijetu biometrije, inovacije u video nadzoru, novi trendovi i inovacije sa CES-a 2019 te općenite svjetske inovacije u biometriji.

U šestom poglavlju „Biometrijska sigurnost“ ukratko će biti obrađena biometrijska sigurnost i kontroverze koje ju prate.

U sedmom poglavlju „Zaključak“ navedene su osnovne značajke ovog završnog rada te je ukratko opisano mišljenje autora.

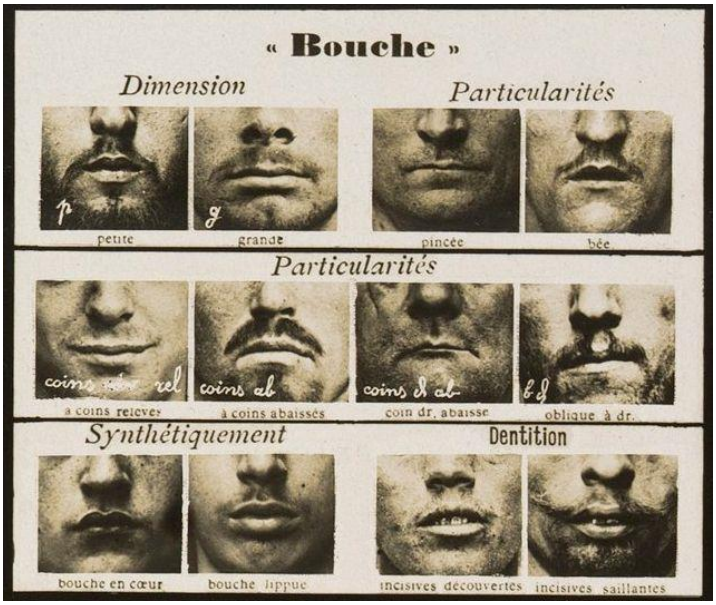
2. BIOMETRIJA

Biometrija je znanost analize fizičkih ili ponašajnih karakteristika specifičnih za svakog pojedinca kako bi se moglo potvrditi njihov identitet. Kada bismo definirali biometriju u najužem smislu, rekli bismo da je biometrija „mjerenje ljudskog tijela“ ili „mjerenje života“ kao što proizlazi iz značenja riječi biometrija (grč. bios = život i metron = mjera).[8]

Biometrija se bavi dugogodišnjom problemom dokazivanja nečijeg identiteta, nepovratno, koristeći se onim što razlikuje. Još u prapovijesti, već se osjećalo da su pojedine karakteristike poput traga prsta dovoljne za njegovo prepoznavanje, pa se "potpisivalo" prstom.

U drugom stoljeću prije Krista, kineski car Ts'In Ona je verificirao određene pečate otiskom prsta. Prepoznavanje dlana prvi je put iskoristio u komercijalnom okruženju 1858. William James Herschel, britanski časnik. Nakon što je zadužen za izgradnju cesta u Bengalu, dao je svojim kooperantima da rukama potpišu ugovore. Krajem 19. stoljeća Bertillon, francuski policajac, poduzeo je prve korake u znanstvenoj policiji. Koristio je tjelesna mjerenja bazirana na specifičnim anatomskim karakteristikama kako bi identificirao zločince koji bi ponavljali nedjela kao što i vidimo dalje na Slici 1. Tehnika koja se često pokazala uspješnom.

Slika 1: Sinoptička tablica fizionomskih obilježlja



Izvor: https://i.pinimg.com/736x/75/af/d5/75afd55002ab12493b274fe688a2c813.jpg

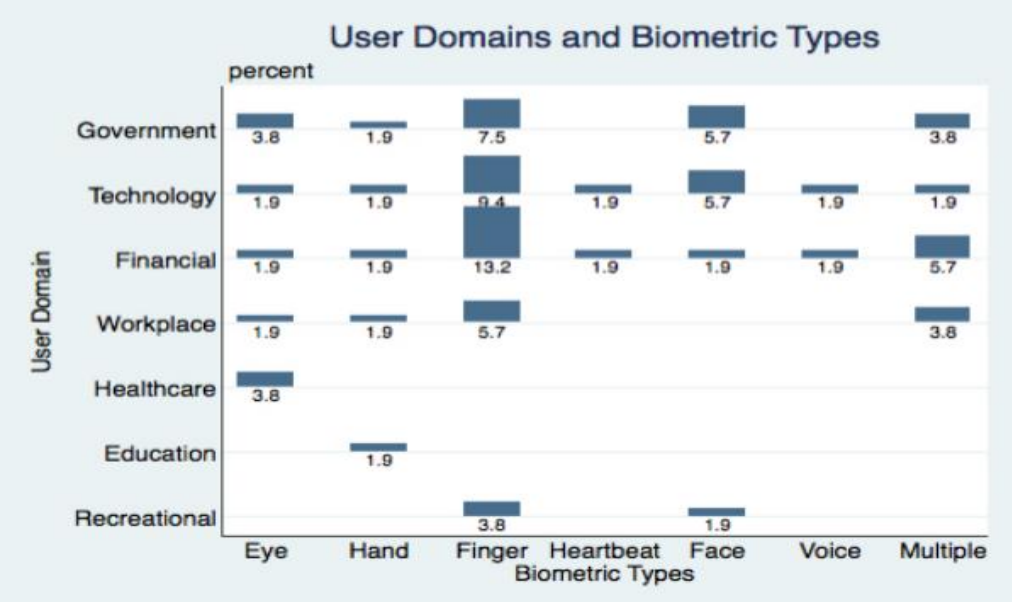
Taj antropometrijski sustav, poznat kasnije kao Bertillonage bio je prvi precizni, znanstveni sustav koji je našao široku primjenu u identifikaciji kriminalaca. Bio je zaslužan za uvrštavanje biometrije kao jedne od grana znanosti.

Biometrija brzo raste, posebno na području identifikacijskih dokumenata. Obično kombinira druge sigurnosne tehnologije poput pametnih kartica. Upotreba biometrije je, općenito, u porastu sve od jednostavnih identifikacija do verifikacija koje se koriste u važnim sigurnosnim sustavima.

2.1. Učestalost korištenja biometrijske tehnologije i autentifikacije na tržištu

U privatnom i javnom sektoru koriste se različite vrste biometrijskih metoda za autentifikaciju kao što će biti prikazano na Grafu 1 na kojem se također uspoređuje širenje različitih biometrijskih vrsta preko raznih poslovnih domena. U ovoj vrsti grafa nazvanoj „tabplot“ visina stupca predstavlja frekvenciju opažanja u toj kategoriji.

Graf 1: Usporedba korištenja biometrije na raznim korisničkim domenama



Izvor: https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf

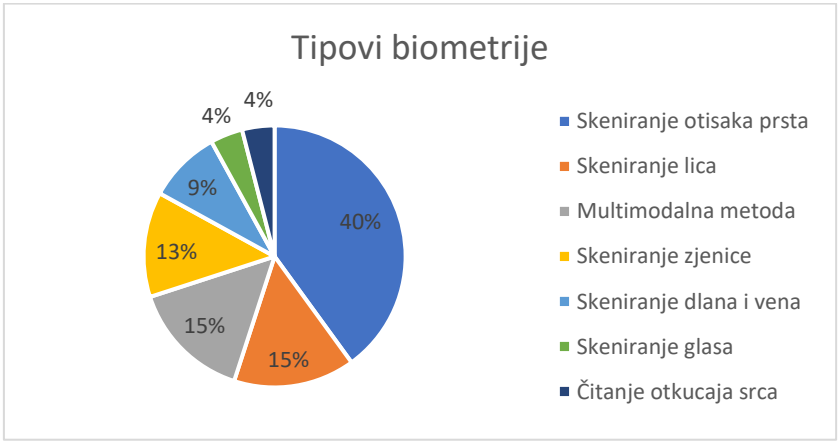
Ono što se može zaključiti iz grafa jest da je skeniranje otisaka prstiju najrasprostranjenija tehnologija za identifikaciju u skoro svakom području osim u zdravstvu (eng. *healthcare*) i obrazovanju (eng. *education*) gdje je najviše korišteno skeniranje zjenice. Financijska domena i tehnologija su najviše prigrlili ekspanziju biometrijske tehnologije tako što koriste svaki ispitani tip biometrije.

Ispitani tipovi biometrijske tehnologije u ovom istraživanju provedenog na instituciji *The University of Texas at Austin – Center for Identity* provedenog u rujnu 2017. godine jesu:

- Skeniranje otiska prsta
- Skeniranje lica
- Multimodalna metoda
- Skeniranje zjenice
- Skeniranje dlana i vena
- Skeniranje glasa
- Skeniranje otkucaja srca

Ove tipove vidimo i u idućem grafu iz kojeg proizlazi da je tehnologija skeniranja otiska prstiju i dalje najučestalija dok su čitači dlanova i vena, prepoznavanje glasa i čitači otkucaja srca najmanje iskorišteni u ovom trenutku.

Graf 2: Učestalost korištenja biometrijske tehnologije



Izvor: https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf

3. BIOMETRIJSKE METODE

3.1. Fiziološke biometrijske metode

„*Fizička biometrija je dio biometrije koja se bavi uzorkovanjem fizionomije ljudskoga tijela i njegovim jedinstvenim karakteristikama*.“[8]

Temelj fiziološke biometrije je ljudska fizička jedinstvenost koja omogućuje raspoznavanje ljudi te se prepoznati uzorci mogu koristiti u kombinaciji sa ostalim zapisima koji jedinstveno opisuju te osobe.

Fiziološka biometrija može biti morfološka i biološka. Uglavnom se sastoje od otisaka prstiju, oblika ruke, prsta, uzoraka vena, oka (šarenice i mrežnice) i oblika lica za morfološku analizu. Za biološku analizu mogu se koristiti DNK, krv, slina ili urin.

Jedna od najpoznatijih metoda identifikacije na temelju otiska prstiju koriste se automatiziranim sustavom identifikacije i klasifikacije, tzv. AFIS (eng. *Automated fingerprint identification system*). AFIS je moderni računalni sustav koji se koristi za brzu identifikaciju skeniranih otisaka papilarnih linija prstiju i dlanova, a u svojoj bazi sadrži otiske iz opće deseteroprstne zbirke, otiske dlanova i sporne tragove papilarnih linija, uključujući i fragmente otisaka. Uporabom ovog automatiziranog sustava skraćuje se vrijeme potrebno za unos podataka, a dobivaju se veće mogućnosti za provjeru cijele baze podataka. AFIS radi na sljedeći način: prvo se otisci digitaliziraju, unose se u bazu podataka skeniranjem otisaka na mjestu događaja u rezoluciji od 500 dpi radi kompatibilnosti sa čitačima otisaka prstiju, uspoređivačima otisaka i algoritmima kompresije otisaka. Nakon unosa slike u bazu podataka ona se analizira tako da se analiziraju mjesta spajanja i završetka zavijutaka papilarnih linija ili se analizira cjelokupni pravac svake pojedine linije.

Nadalje biometrijska metoda očitavanja lica jedna je od jeftinijih i nenametljivih metoda. Obično se koristi tako da se osoba fotografira u određenom mjerilu, zatim se fotografija unosi u bazu podataka i računalo te se metodama linearnih i kutnih mjerenja uspoređuju razmaci između konstantnih točaka na pojedinim dijelovima lica. Da bi prepoznavanje bilo na razini identifikacije potrebno je utvrditi dovoljan broj podudarnosti, između 15 i 20 obilježja. Važno

je napomenuti da su odabrana obilježja konstanta i relativno nepromjenjiva što znači da se većinom osoba može prepoznati i nakon kirurških korekcija lica, promjena frizure, boje kose i slično. Ono što čini ovu metodu relativno jeftinom jest to što fotografije lica ne zauzimaju puno memorije pa sustav može obraditi više milijuna fotografija u minuti. To je od velike važnosti u prostorima koji imaju veliku fluktuaciju ljudi, na primjer zračne luke.[2]

Geometrija dlana i prstiju kao biometrijska metoda utvrđivanja identiteta gotovo je podudarna prethodno opisanoj metodi identifikacije na temelju proporcija i izgleda lica. Također se provodi snimanjem ruku te automatskom usporedbom obilježja poput rasporeda, oblika i duljine kostiju. Metoda je relativno nepouzdana s obzirom da nema zadovoljavajuće razine jedinstvenosti kod svake osobe te se obično koristi u kombinaciji s drugim metodama. Jedna od pouzdanijih metoda identifikacije pomoću ruku jest metoda usporede položaja vena na šaci prilikom čega se traže mjesta spajanja krvnih žila koja čine karakterističnu šaru. [2]

Metoda snimanja spleta krvnih žila u licu i tijelu pomoću infracrvene kamere jedan je od sigurnijih metoda identifikacije osobe. Nedostatak ove metode je osjetljivost na promjene temperature i termogrami, snimke nastale ovim postupkom, koji zauzimaju značajnu količinu memorije čime ova metoda nije podobna za velike digitalne baze podataka. [2]

Jedna od zanimljivijih metoda koja se koristi u kriminalistici, odnosno odorologiji, jest izoliranje i usporedba tjelesnih mirisa korištenjem plinske kromatografije i spektrometrijom masa. Individualnost mirisa čovjeka predstavlja neku vrstu mikrotraga kojeg je moguće prikupiti te analizirati kako bi se mogao odrediti identitet osobe. Metode prikladne za prikupljanje i obradu uzoraka za stvaranje baze podataka danas se intenzivno istražuju. [2]

Analiza DNK (deoksiribonukleinske kiseline) je od svih navedenih biometrijskih metoda identifikacije zasigurno jedna od najznačajnijih i najpouzdanijih. Koristi se u mnogim područjima istraživanja, za utvrđivanje identiteta primjenjuje se u području kriminalistike i sudske medicine te za dokazivanje roditeljstva, posmrtnu identifikaciju ostatka mrtvih tijela, traseološku identifikaciju kojom se smatra „*identifikacija osoba koje su u svezi s kaznenim djelom analiziranjem tragova biološkog podrijetla pronađenih na mjestu događaja*.“ Sama identifikacija temelji se na utvrđivanju dužine i broja ponavljanja kratkih ponavljajućih sljedova

ili STR (engl. *short tandem repeats*). STR su kratke sekvence parova baza koje se pojavljuju u DNK svake osobe no broj ponavljanja sekvenci jako se razlikuje od osobe do osobe. Kako bi se STR u DNK mogao analizirati koriste se unaprijed određeni lokusi za koje je poznato da sadrže određene parove baza koje se uzastopno ponavljaju, a istovremeno pokrivaju veliku varijabilnost u ljudskoj populaciji, dakle sadržavaju VNTR ili varijabilne (polimorfne) ponavljajuće sljedove (engl. *variable number tandem repeats*). VNTR su visoko polimorfni sljedovi koji su određeni brojem repetitivnih DNK sekvenci. [2]

U idućem poglavlju ukratko će se analizirati ponašajne biometrijske metode koje opisuju fizikalne karakteristike ljudskog tijela koje su dijelom jedinstvene za svaku osobu. One se opisuju krivuljama koje se koriste za opis karakterističnih uzorka, odnosno ponašanja, u čijoj osnovi je moguće raspoznati različite ljude.

3.2. Ponašajne biometrijske metode

Najčešće ponašajne biometrijske metode su prepoznavanje glasa, dinamika potpisa (brzina kretanja olovke, ubrzanja, pritisak pod pritiskom, nagib), dinamika pritiska tipke, način na koji koristimo predmete, hod, zvuk koraka, geste itd. Različite korištene tehnike predmet su stalnog istraživanja i razvoja i, naravno, kontinuirano se poboljšavaju.

Međutim, različite vrste mjerenja nemaju sve iste razine pouzdanosti. Fiziološka mjerenja obično nude blagodati postojanja stabilnijeg tijekom života pojedinca. Na primjer, oni nisu podložni učincima stresa, za razliku od identifikacije pojedinca mjerenjem ponašanja.

U svrhu autentifikacije različitih osoba na temelju njihovih jedinstvenih glasovnih karakteristika koristi se prepoznavanje glasa ili fonoskopska identifikacija. Temelj vjerodostojne identifikacije zasnovana je na karakteristikama poput boje glasa, modulacije, frekvencije, specifičnostima izgovora određenih glasova, govornim manama i drugo. Postupak identifikacije putem glasa provodi se sa snimljenim glasovima u kojem slučaju se glas osobe snimi i zajedno sa snimkom spornog glasa obradi u električne signale koji se onda vizualiziraju kroz grafikone čije se amplitude uspoređuju. Zaključivanje o podudarnosti ili nepodudarnosti glasa određene osobe sa spornim glasom određuje se temeljem poklapanja ili odstupanja grafičkih prikaza. Takvo mjerenje identifikacije poduzima se u kriminalistici. [2]

Tehnologija prepoznavanja rukopisa ili potpisa koristi dinamičku analizu potpisa kako bi autentificirala osobu. Temeljena je općim i posebnim obilježjima rukopisa. Opća obilježja su opći izgled rukopisa, stupanj ispisanosti, raspored teksta, odnos prema liniji pisanja, veličina rukopisa, razmaci, vezanost i nevezanost slova, rastavljanje riječi, brzina pisanja, pritisak i nagib rukopisa na papir. Posebna obilježja individualna su od osobe do osobe te se baziraju na mjerenju nagiba, brzine, jačine pritiska, duljine poteza ruke. Prednost ovakve identifikacije je jednostavnost, unatoč mogućnostima automatske obrade, metoda ipak traži izuzetnu stručnost eksperta jer se radi o psihološko-grafičkoj ekspertizi. Ova metoda najčešće se koristi u *e-bussine*ss aplikacijama i e-bankingu. [2]

Tipkanje po tipkovnici se također može mjeriti sa individualnim karakteristikama osobe. Tehnika mjerenja je nenametljiva jer je potrebna samo zvučna kartica i/ ili specijalni program koji bi na razini operacijskog sustava pratio korisnikovo tipkanje. Ova tehnika se bazira na vremenskom razmaku između korisnikovog pritiska na tipkovnicu i duljine samog pritiska na tipku, dakle na korisnikovoj dinamici tipkanja.

Ljudski hod predstavlja kompleksnu prostorno-vremensku biometriju ponašanja čija karakteristika nije jedinstvenost, ali može biti uzrok identifikacije s obzirom na karakter osobe, situaciju u kojoj se nalazi i zdravstveno stanje. Ljudski hod snima se videokamerom te se provjera tog uzorka temelji na karakterizaciji nekoliko različitih pokreta svakog od artikuliranih zglobova prilikom izvođenja određene radnje.

U idućem poglavlju opisat će se multimodalna metoda koja objedinjuje kombinaciju svih biometrijskih osobina koje su dosad navedene. Ona također podrazumijeva bolju sigurnost u provjeri identiteta osobe što znači da se može izgraditi jedan sigurni informacijski sustav ukoliko se u praksi koristi veći broj prethodno nabrojenih tehnika.

3.3. Multimodalna biometrija

Multimodalna biometrija u praksi je većinom kombinacija fizioloških i ponašajnih biometrija koje podrazumijevaju provjeru i identifikaciju. Najpoznatije tehnike uključuju otiske prstiju, prepoznavanje lica, šarenice, dlana i prepoznavanje na bazi DNK.

Multimodalna biometrija kombinira nekoliko biometrijskih izvora kako bi se povećala sigurnost i točnost. Multimodalni biometrijski sustavi za identifikaciju obično traže dve biometrijske vjerodajnice, poput verifikacije lica i otisaka prstiju umjesto jednog. Oni mogu prevladati ograničenja koja se često susreću u unimodalnim sustavima.

Već nekoliko godina upotreba nekoliko biometrijskih značajki u kombinaciji, na primjer, lica i šarenice ili šarenice i otisaka prstiju, omogućuje znatno smanjenje stope pogreške. Biometrija također može poboljšati multifaktorsku provjeru autentičnosti. Geolokacija, IP adrese i obrasci unosa mogu stvoriti moćnu kombinaciju za sigurnu provjeru autentičnosti korisnika pri online provjeri identiteta. Većinom se koristi u graničnim prijelazima za kontrolu ulaska i izlaska, za kontrolu pristupa nekom prostoru, civilnoj identifikaciji i kao što je prije opisano mrežnoj sigurnosti.

Unutar multimodalnog biometrijskog sustava može postojati raznolikost u broju osobina i komponenti. Oni mogu biti kako slijedi :

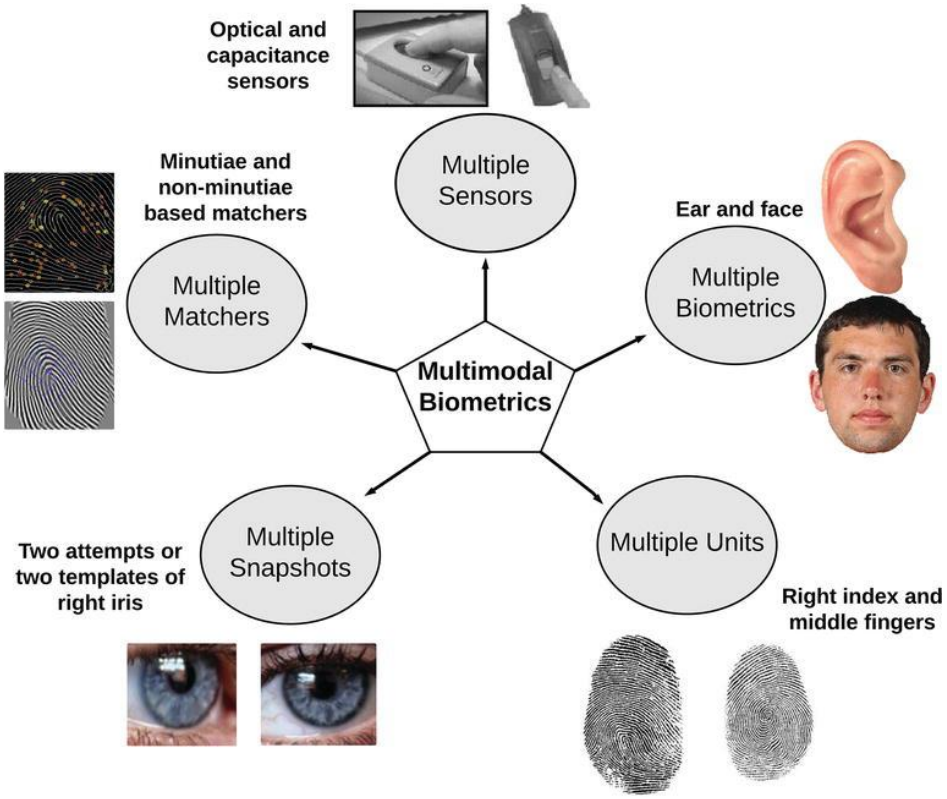
- Pojedinačna biometrijska osobina, više senzora.
- Pojedinačna biometrijska osobina, više klasifikatora
- Jedna biometrijska osobina, više jedinica (recimo, više prstiju).
- Višestruke biometrijske osobine pojedinca (recimo zjenica, otisak prsta itd.), tzv. multimodalnost

Te se osobine aktiviraju radi potvrđivanja identiteta korisnika.

Ono što je bitno za multimodalnu biometriju jest mogućnost da nadiđe nesigurnost samo jedne metode biometrijske identifikacije, ne-univerzalnost uzoraka, opseg korisničke udobnosti i slobode pri radu sa sustavom. Multimodalni biometrijski sustav povećava sigurnost i tajnost korisničkih podataka, pouzdaniji je, precizniji i može pružiti određenu sigurnost ako ikoji identifikator u sustavu prestane raditi iz poznatih ili nepoznatih razloga. Povećanje diskriminirajućih informacija i ograničenja vodi do smanjenja pogreške u procesu prepoznavanja. Više informacija može se dobiti ako se istovremeno koriste različiti izvori

informacija, a izvori informacija mogu biti u više vrsta, kao što su višestruke biometrijske osobine, algoritmi, instance, uzorci i senzori. Različiti scenariji u multimodalnom biometrijskom sustavu prikazani su na Slici 2.

Slika 2: Multimodalni biometrijski sustav



Izvor: https://www.intechopen.com/media/chapter/57552/media/F9.png

Dakle, prilikom korištenja unimodalne biometrije postoji velika mogućnost da će doći do brojnih izazova kao što su nedostatak sigurnosti, ne-univerzalnost uzoraka, opseg korisnikove udobnosti i slobode pri radu sa sustavom. To se sve može riješiti primjenom multimodalnog sustava biometrije iz razloga što je sustav pouzdaniji. Gubitak jednog od identifikatora bilo iz poznatih ili nepoznatih razloga i dalje omogućava identifikaciju na zadovoljavajućoj razini, upravo zbog primjene više modova. S druge strane unimodalni biometrijski sustavi jeftiniji su i zahtijevaju manje vremena za prepoznavanje u usporedbi sa multimodalnim sustavom. Stoga je izuzetno važno pažljivo analizirati kompromis između dodanih troškova i koristi ostvarenih prilikom poslovne primjene multibiometrije u određene svrhe kao što su komercijalna, forenzička i biometrijski sustavi koji uključuju veliko stanovništvo.

4. IDENTITET I BIOMETRIJA

Svaki entitet (čovjek, životinja ili predmet) istovjetan je sam sa sobom, neponovljiv i jedinstven. Identitet predstavlja ukupnost nepromjenjivih obilježja koja čine određenu osobu ili predmet, a prema kojima se ta osoba može razlikovati od svih drugih. Ta obilježja se nazivaju individualnost. Identifikacija se provodi utvrđivanjem nepoznatog s otprije poznatim na temelju određenih identifikacijskih obilježja, pritom se uspoređuje određen broj identifikacijskih obilježja pomoću kojih se ustanovljava podudarnost ili različitost između uspoređivanih objekata. Identifikacijska obilježja koja bi se mogla koristiti u procesu identifikacije moraju zadovoljavati iduće kriterije:

- Univerzalnost (je li ova karakteristika uobičajena kod svake osobe)
- Individualnost ili originalnost (karakteristika je različita za svakog pojedinca)
- Trajnost i nepromjenjivost (karakteristika mora biti permanentna, dakle ne smije se moći mijenjati)
- Mogućnost izdvajanja iz ukupnosti obilježja (mora se moći izdvojiti kako bi se mogla stvoriti baza podataka tog obilježja radi mogućih komparacija za utvrđivanje identiteta)
- Jednostavno prikupljanje i korištenje (karakteristika se može jednostavno prikupiti i lako kvantificirati)
- Prihvatljivost (spremnost ljudi na korištenje ove značajke za biometrijsku autorizaciju)
- Mogućnost prijevare (odnosi se na mogućnost falsificiranja uzoraka radi prevare sustava za identifikaciju) [2]

Uz sva ova obilježja, tjelesna koja se još nazivaju stvarnim ili faktičkim obilježjima, prilikom utvrđivanja i provjere identiteta osobe, koriste se pravna obilježja. Ona podrazumijevaju činjenice koje svaki čovjek dobije temeljem pravnih popisa, poput imena, prezimena, državljanstva, prebivališta i drugo. Pri utvrđivanju istovjetnosti kod predmeta, također se koriste pravna obilježja (predmeti više vrijednosti dobivaju niz podataka, od tvorničkog ili serijskog broja, modela, tipa, registarskih oznaka i slično), ali i fizičko-faktička obilježja, dakle izgled predmeta.

Suvremena biometrijska identifikacija temelji se na jedinstvenim fiziološkim osobinama i osobitostima ponašanja ispitivanog pojedinca, prepoznavanju određenih biometrijskih karakteristika te usporedbi istih s uzorkom prije pohranjenim u obliku podataka unutar baze podataka određenog sustava. Osnovni uvjet za provedbu biometrijske identifikacije je mogućnost da se tjelesne i bihevioralne karakteristike mogu koristiti u postupku automatske identifikacije.

Biometrijski sustav sastoji se od četiri osnovna dijela:

1. Ulazne jedinice: ona služi za mjerenje i registraciju određenog biometrijskog obilježja,
2. Ekstraktora: jedinice za izdvajanje obilježja iz cjeline,
3. Baze: u njoj se provodi evidencija identifikacijski obilježja te
4. Jedinice za verifikaciju i komparaciju: ona provodi provjeru kvantitete i kvalitete spornih obilježja koje potom uspoređuje s ranije pohranjenim[2]

Biometrijski sustav većinom radi u dvije faze, a to su: faza prijave i faza autorizacije. Faza prijave označava prvu prijavu korisnika u sustav, dakle prvu prijavu sa svojim biometrijskim značajkama u sustav koje se potom uspoređuju s onima pohranjenim u bazi sustava. Faza autorizacije je faza u kojoj korisnika od sustava zahtijeva identifikaciju i/ili verifikaciju pri čemu se izlučene značajke uspoređuju s onima pohranjenima u bazi biometrijskog sustava prilikom prijave te biometrijski sustav na temelju ove usporedbe donosi odluku o rezultatu identifikacije ili verifikacije.

Fiziološke karakteristike osobe obično zadovoljavaju kriterije potrebne za neupitnu biometrijsku identifikaciju osobe, dok se ponašajne karakteristike koriste kao određeni indicij koji upućuje na neku osobu. Obično se koriste prilikom skupne identifikacije, odnosno u kriminalističkom istraživanju.

Brojni sigurnosni sustavi temelje se na identifikaciji osoba sa biometrijskim metodama da bi se utvrdio identitet te osobe, takva provjera većinom se temeljila na fiziološkim metodama identifikacije te je morala biti brza, jeftina, pouzdana te ne smije narušavati privatnost osobe. Danas se većinom identitet utvrđuje verifikacijom, odnosno korisnik prilikom prve prijave u

sustav dobiva oznaku svog identiteta (lozinku, PIN, korisničko ime i slično), te je zadaća sustava, prilikom identifikacije, na temelju biometrijske karakteristike provjeriti radi li se zaista o danom identitetu. Biometrijski sustavi također imaju identifikaciju u zatvorenom skupu i identifikaciju u otvorenom skupu. Biometrijska identifikacija u zatvorenom skupu odnosi se na identifikaciju pojedinaca već prijavljenih u sustav te je njena zadaća tad samo odrediti identitet osobe. Kod otvorenog skupa osoba ne mora biti poznata sustavu te bi sustav za identifikaciju u otvorenom skupu trebao prijaviti i ispravno detektirati pokušaj identifikacije osobe koja nije dosad prijavljena u sustav.

4.1. Biometrijski podaci i GDPR

EU zakon o privatnosti podataka definira biometrijske podatke kao „posebne kategorije osobnih podataka“ i zabranjuje njihovu „obradu“. Preciznije, biometrijski podaci su „osobni podaci koji proizlaze iz specifične tehničke obrade koja se odnosi na fizičke, fiziološke ili ponašanje karakteristike fizičke osobe, što omogućuje ili potvrđuje jedinstvenu identifikaciju te fizičke osobe, poput slika lica ili podataka o otiscima prstiju“. Biografski podaci ili podaci o osobnoj povijesti kao što su datum rođenja, bračni status, spol, ime ili adresa također su zaštićeni GDPR-om, naravno. Uredba štiti građane EU-a i dugotrajne stanovnike od dijeljenja njihovih podataka s trećim stranama bez njihovog pristanka. Njihova obrada za „jedinstveno identificiranje fizičke osobe“ je zabranjena. Međutim, sadrži neke iznimke:

- Ako je suglasnost dana izričito
- Ako su biometrijski podaci potrebni za izvršavanje obveza voditelja obrade ili nositelja podataka u području zakona o zapošljavanju, socijalnoj sigurnosti i socijalnoj zaštiti
- Ako je neophodno zaštititi vitalne interese pojedinca i on / ona nije u stanju dati pristanak
- Ako je to kritično za bilo kakve pravne zahtjeve
- Ako je to potrebno iz razloga javnog interesa u području javnog zdravstva.

Štoviše, Uredba dopušta državama članicama da uvedu druga ograničenja u pogledu obrade biometrijskih podataka.

4.2. Primjena biometrijske tehnologije u suvremenom svijetu

Povijesno gledano, prijave korištenjem biometrije uglavnom su inicirale vlasti za vojnu kontrolu pristupa, kriminalnu ili civilnu identifikaciju pod strogo uređenim pravnim i tehničkim okvirom. Danas sektori, uključujući bankarstvo, maloprodaju i mobilnu trgovinu, pokazuju pravi apetit prema prednostima biometrije. Što je najvažnije, svijest i prihvaćanje povećani su u posljednjih sedam godina, jer milijuni korisnika pametnih telefona otključavaju svoje telefone otiskom prsta ili licem.

Primjena biometrijskih tehnologija najčešće se koristi u:

- Provođenju zakona i javnoj sigurnosti (identifikacija kriminalca / osumnjičenika)
- Vojsci (identifikacija neprijatelja / saveznika)
- Kontroli granica, putovanja i migracija (identifikacija putnika / migranta)
- Civilnoj identifikaciji (identifikacija građana / stanovnika / birača)
- Zdravstvu i subvencijama (identifikacija pacijenta / korisnika / zdravstvene zaštite)
- Fizičkim i logičkim pristupom (identifikacija vlasnika / korisnika / zaposlenika / izvođača / partnera)
- Komercijalnim aplikacijama (identifikacija potrošača / kupca).

Biometrija u provođenju zakona odnosi se na primjenu biometrijskih sustava koji podržavaju agencije za provođenje zakona. Ova kategorija može uključivati rješenja za identifikaciju kažnjenika poput Automatiziranih sustava za identifikaciju otiska prsta i otiska dlana (AFIS). On pohranjuje, pretražuje i dohvaća slike otisaka prstiju i podatke okrivljenika. Danas Automatizirani sustavi za biometrijsku identifikaciju (ABIS) mogu stvarati i pohranjivati biometrijske informacije koje odgovaraju biometrijskim predlošcima za lice (pomoću takozvanih „*mugshot*“ sustava), prsta i šarenice. Prepoznavanje lica uživo odnosno sposobnost izvođenja identifikacije lica u masi ljudi u stvarnom vremenu ili nakon događaja također dobiva interes za javnu sigurnost u gradovima, zračnim lukama, na granicama ili drugim većim okupljalištima poput stadiona ili sakralnim objektima.

Nepoznato je kako obrambene agencije širom svijeta koriste biometrijske podatke. Činjenica je da je do informacija teško doći i podijeliti ih jer nisu javne. Američka vojska prikupljala je lica, šarenice, otiske prstiju i DNK podatke u sustavu biometrijske identifikacije od siječnja 2009. Biometrijski program započeo je već 2004. i u početku je sakupljao otiske prstiju. Agencija za forenziku i biometriju obrane (DFBA - *Defense Forensics and Biometrics Agency*) upravlja sustavom, poznatim kao DoD automatizirani biometrijski informacijski sustav (engl. *Automated Biometric Information System*). Prema OneZero (6. studenoga 2019.), 7,4 milijuna identiteta u bazi podataka u velikoj većini potječu iz vojnih operacija u Iraku i Afganistanu. U razdoblju od 2008. do 2017. godine, Ministarstvo obrane uhitilo je ili ubilo 1.700 osoba na temelju biometrijskih i forenzičkih podudaranja (web mjesto Ureda američke vlade za odgovornost – stranica 2/59). U prvoj polovici 2019. godine biometrijska identifikacija korištena je tisućama puta za identifikaciju ne-američkih građana na bojnom polju.

Elektronička putovnica (e-putovnica) poznata je biometrijska putna isprava. Druga generacija takvih dokumenata, poznata i kao biometrijske putovnice, uključuje dva pohranjena otiska prsta i fotografiju putovnice. Prijelaz sa običnih papirnatih putovnica na elektroničke putovnice u opticaju je od 2005. godine, a sredinom 2019. godine. Više od 150 zemalja je počelo izdavati ovaj novi tip putnog dokumenta.

Slika 3: Elektronička putovnica

Izvor: https://www.thalesgroup.com/sites/default/files/gemalto/multi-passports.jpg

Preko 1,2 milijarde e-putovnica u optjecaju je 2020. godine. To znači da preko 1,2 milijarde putnika ima standardizirani digitalni portret u sigurnom dokumentu. To je neočekivana sreća za automatske sustave granične kontrole (zvane e-vrata), ali i za samoposlužne kioske.

Fotografija ubrzava prelazak granice kroz skenere koji koriste princip prepoznavanja usporedbom lica ili otisaka prstiju. Rješenja za prijavu i ispuštanje prtljage također povećavaju brzinu i učinkovitost zadržavajući visoku razinu sigurnosti.

Nepotrebno je reći da je za zračne luke i zrakoplovne tvrtke pružanje putniku jedinstveno i ugodno putničko iskustvo poslovni prioritet. Biometrija ovdje pruža nepobitne dokaze o vezi između putovnice i njezinog vlasnika.

Biometrijska provjera autentičnosti vrši se usporedbom lica ili otisaka prstiju koji su viđeni ili očitani na granici s licem ili otiscima prstiju u mikrokontroleru putovnice. Ako se oba biometrijska podatka podudaraju, potvrđuje se autentičnost. Ako je potrebno, identifikacija se vrši s biografskim podacima u čipu i ispisuje se.

Osim toga, mnoge su zemlje postavile biometrijske infrastrukture za kontrolu migracijskih tokova pri ulasku i izlasku s njihovih teritorija. Skeneri otiska prsta i kamere na graničnim prijelazima bilježe informacije koje pomažu identificiranju putnika koji ulaze u zemlju na precizniji i pouzdaniji način. U nekim državama isto se odnosi na konzulate za zahtjeve za vize i obnove.

Slijedi potanak opis tri primjera biometrijskih baza podataka:

- Biometrijski sustav IDENT-a (engl. *Automated Biometric Identification System*) američkog Ministarstva domovinske sigurnosti, najveći takve vrste
- EURODAC (engl. *European Dactyloscopy System*) Europske unije, koji opslužuje 32 europske države (biometrija za tražitelje azila)
- Ambiciozni europski sustav ulaska / izlaska (EES – engl. *Entry/Exit System*) koji će se uspostaviti 2022. godine.

Postoje i druge prijave, uglavnom nacionalne osobne iskaznice, raširene u europskim i zemljama Bliskog istoka ili Afrike za osobne iskaznice i programe zdravstvenog osiguranja, kao u Gabonu. Ovim biometrijskim osobnim iskaznicama otisci prstiju koriste se za potvrdu identiteta nositelja kartice prije nego što on ili ona može pristupiti državnim službama ili zdravstvenoj zaštiti.

Zašto je to tako? Na primjer, u Gabonu je i prije nego što je program započeo, svima bilo jasno da se trebaju implementirati svi resursi kako bi se izbjeglo da se program zdravstvenog osiguranja pretvori u središte pozornosti građana susjednih zemalja. Ova je značajka bila presudna kako bi se osiguralo da velikodušnost programa neće dovesti do njegovog kraha prevarantskom uporabom prava. Stoga se korisnici pojedinačno identificiraju kako bi im se mogao rezervirati pristup skrbi. Vlasti su odlučile da će identifikacija osiguranika biti nominativna primjenom gabonskog pojedinačnog broja zdravstvenog osiguranja.

Civilni podaci, fotografija osobe i dva otiska prsta digitalizirani su u mikroprocesoru, osiguravajući šifriranje i zaštitu tih podataka. Bolnice, ljekarne i klinike koriste karticu zdravstvenog osiguranja za provjeru prava iz socijalnog osiguranja, istovremeno štiteći povjerljivost osobnih podataka. Terminali vrše provjere senzorima otiska prsta.

AFIS baze podataka (Automatski sustav za identifikaciju otiska prsta), često povezane s bazom podataka iz matičnih knjiga, osiguravaju identitet i jedinstvenost građanina ostatku populacije na pouzdan, brz i automatiziran način. Za veću pouzdanost mogu kombinirati digitalne otiske prstiju, fotografiju i skeniranje šarenice.

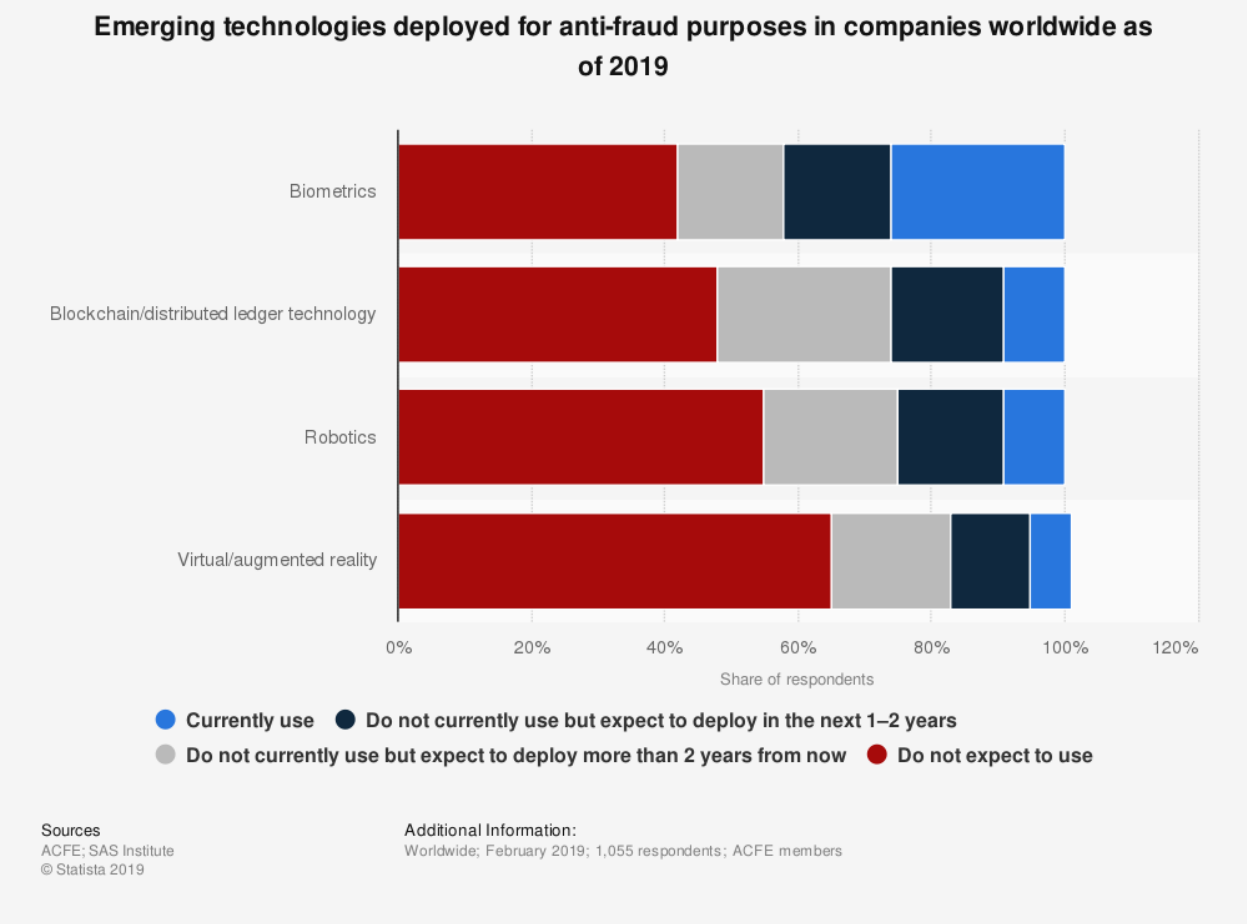
4.3. CIVILNI IDENTITET I REGISTRACIJA STANOVNIŠTVA

Indijski projekt Aadhaar simbol je biometrijske registracije. To je daleko najveći svjetski sustav biometrijske identifikacije i temelj pouzdane identifikacije i autentifikacije u Indiji. Aadhaar broj je 12-znamenkasti jedinstveni identifikacijski broj koji se izdaje svim stanovnicima Indije. Ovaj se broj temelji na njihovim biografskim i biometrijskim podacima (fotografija, deset otisaka prstiju, dva snimka šarenice). 1.262.505.064 ljudi ima Aadhaar broj,

a od 10. rujna 2020. godine, pokrivati će više od 99% odrasle indijske populacije U početku projekt je bio povezan s javnim shemama subvencija i naknada za nezaposlene, ali sada uključuje shemu plaćanja. Prema ministru financija Arunu Jaitleyu u svom govoru od 1. veljače 2018., Aahaar pruža identitet svakom Indijcu te je mnoge usluge učinio dostupnijim ljudima. Smanjio je korupciju, troškove isporuke javnih usluga i posrednike.

Prema globalnom istraživanju 2019. godine, biometrija je tehnologija koja se najčešće koristi u svrhe borbe protiv prijevara u organizacijama. Četrdeset i dvoje ispitanika reklo je da njihova organizacija ili trenutno koristi biometriju u tu svrhu ili je to planirala učiniti za jednu ili dvije godine kao što je prikazano na idućem grafu.

Graf 3: Nove tehnologije primijenjene u svrhe borbe protiv prijevara u tvrtkama širom svijeta od 2019



Izvor: https://www.statista.com/statistics/1043568/worldwide-emerging-fight-emerging-technologies/

Uz registraciju stanovništva biometrija se također koristi kako bi se verificirali glasači kao što je prikazano na Slici 4.

Slika 4: Biometrijska identifikacija glasača na dijelu

Izvor:https://www.thalesgroup.com/sites/default/files/gemalto/biometric%20voter%20registration.jpg

Na Slici 4 je prikazan prvo proces identifikacije pomoću barkoda, zatim verifikacija identiteta glasača otiskom prsta. U Hrvatskoj je također bilo govora o uvođenju online izbora, odnosno glasanja preko sustava e-Građani i to pomoću novih elektroničkih osobnih identifikacijskih iskaznica koje sadržavaju elektronički nosač podataka, tzv. čip na koji se mogu pohraniti:

- identifikacijski certifikat koji se koristi za elektroničku potvrdu identiteta i autentikaciju prilikom pristupa elektroničkim uslugama
- potpisni certifikat koji se koristi kao podrška naprednom elektroničkom potpisu i zamjenjuje vlastoručni potpis, sukladno zakonu kojim je reguliran elektronički potpis

te tako elektronička osobna iskaznica s aktivnim identifikacijskim certifikatom služi za prijavu u sustav e-Građani na internetskoj stranici https://pretinac.go.hr i druge e-usluge. Uz potpisni certifikat, elektronička osobna iskaznica služi za obavljanje aktivnosti vezanih uz ovjeru dokumenata elektroničkim potpisom, kao valjanom zamjenom za vlastoručni potpis.

Biometrijski sustavi kontrole pristupa pomažu spriječiti neovlaštenim osobama pristup:

- objektima (fizička kontrola pristupa)

- računalnim sustavima i mrežama (logička kontrola pristupa) na temelju biometrijske provjere autentičnosti.

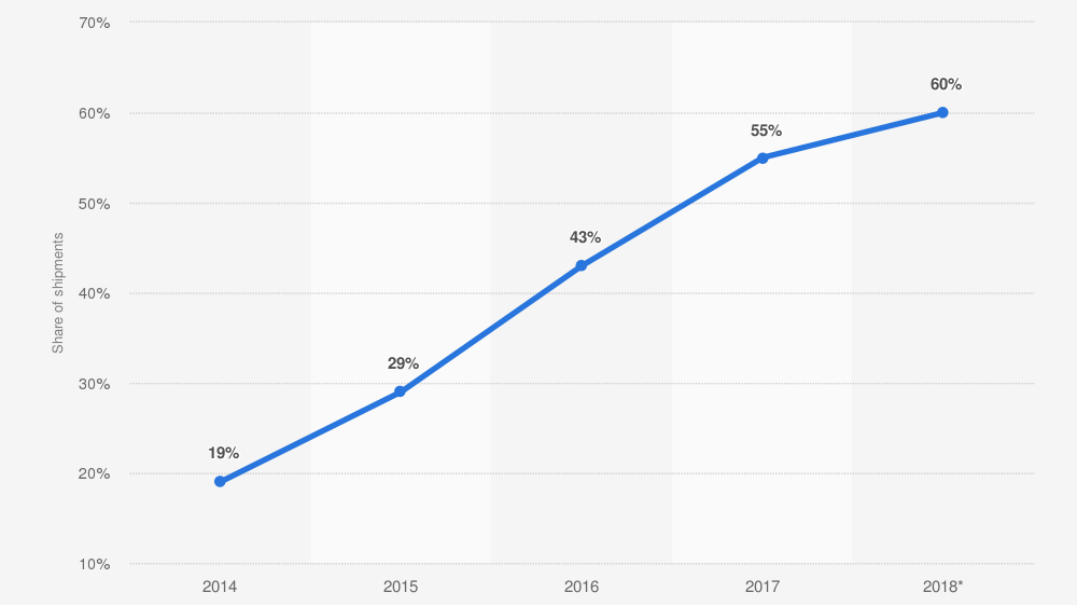
U IT-u biometrijska kontrola pristupa može biti komplementarni faktor autentifikacije korisnika i podržava organizacijske politike upravljanja identitetom i pristupom (IAM- Identity and Access Management). Za razliku od kodova, statičnih lozinki, jednokratnih lozinki ili pristupnih kartica koje se oslanjaju na podatke koji se mogu zaboraviti ili izgubiti, biometrijska provjera autentičnosti temelji se na tome tko su ljudi (a ne onome što imaju).

U mobilnom svijetu pametni telefoni (oblik IT sustava) obično uključuju značajke prepoznavanja otiska prsta i lica. IPhone 5 prvi je uveo prepoznavanje otiska prsta 2013. godine (s TOUCH ID-om), a prepoznavanje lica postalo je popularno s iPhoneom X predstavljenim u studenom 2017. (s FACE ID-om). Primjerice, kada neznanac pokupi iPhone X, taj neznanac ima jednu od milijun šansi da uspije prevariti kameru što je ogroman napredak u odnosu na onaj u 50.000 šansi s Touch ID-om, kojeg je Schiller opisao kao "zlatni standard" biometrijske provjere autentičnosti. Izgledi za prevaru postaju niži kada ljudi poput članova obitelji dijele osobine s vlasnikom telefona, iako iPhone X ima zaštitu od otključavanja lica usnulog korisnika ili njegove fotografije. Kamera TrueDepth na iPhoneu snima točne podatke o licu projicirajući i analizirajući preko 30 000 nevidljivih točaka kako bi stvorila dubinsku kartu lica korisnika, a također snima i infracrvenu sliku lica korisnika. Dio neuronskog motora čipa A11, A12 Bionic, A12X Bionic i A13 Bionic - zaštićenih unutar Secure Enclave – transformira dubinsku kartu i infracrvenu sliku u matematički prikaz i uspoređuje taj prikaz s upisanim podacima o licu. Face ID automatski se prilagođava promjenama izgleda, poput nošenja kozmetičke šminke ili rastuće dlake na licu. Ako dođe do značajnijih promjena u izgledu korisnika, poput brijanja čitave brade, Face ID potvrđuje identitet korisniak upotrebom zaporke prije nego što ažurira podatke o licu. Face ID dizajniran je za rad sa šeširima, šalovima, naočalama, kontaktnim lećama i mnogim sunčanim naočalama. Nadalje, dizajniran je za rad u zatvorenom, na otvorenom, pa čak i u potpunoj tami.

Statistički podaci na Grafu 4 pokazuju udio isporuka pametnih telefona sa senzorom otiska prsta u cijelom svijetu od 2014. do 2018. 55 posto pametnih telefona isporučenih

globalno u 2017. godini imalo je senzor otiska prsta, a u 2018. 60% što znači da je trend otključavanja i osiguravanja mobitela pomoću senzora otiska prstiju u porastu.

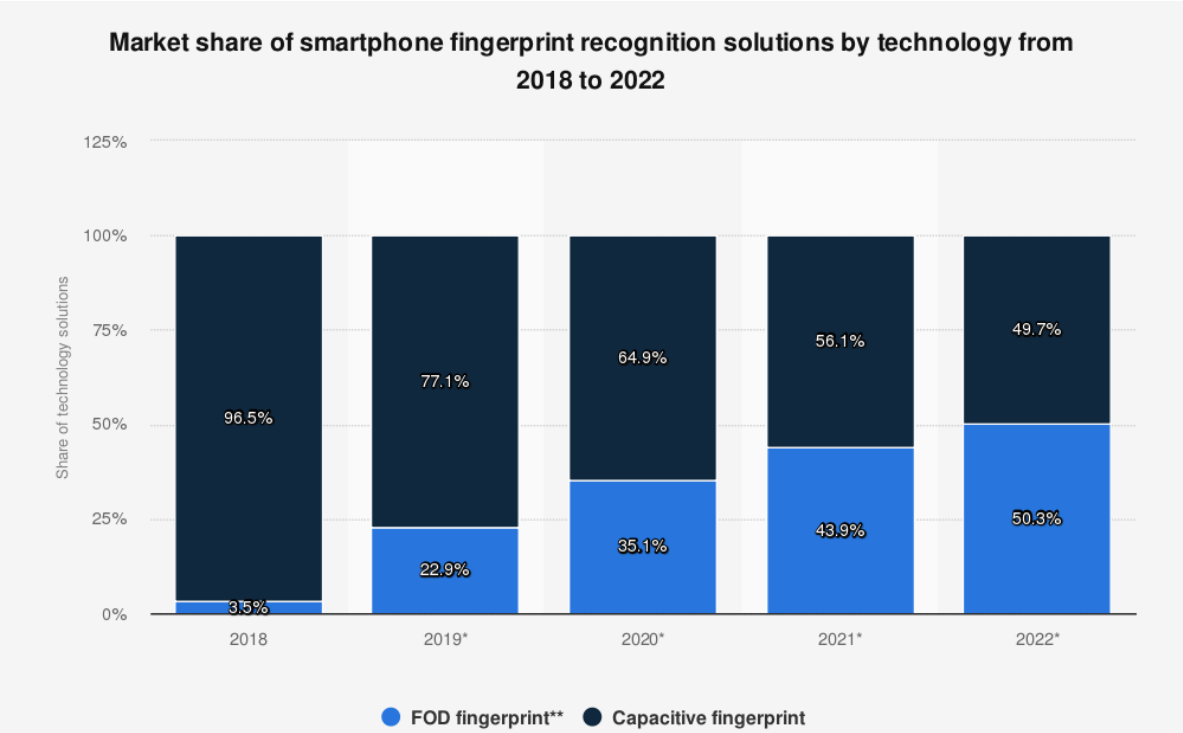
Graf 4: Udio isporuka pametnih telefona sa senzorom otiska prsta širom svijeta od 2014. do 2018. godine



Izvor: https://www.statista.com/statistics/804269/global-smartphone-fingerprint-sensor-penetration-rate/

Također, postotak implementacije senzora za otiske prstiju ispod samog ekrana pametnih mobitela se povećava, odnosno trebalo bi se povećati u odnosu prema kapacitivnom senzoru koji se obično nalazi na poleđini mobitela kao što je prikazano na idućem grafu.

Graf 5: Udio tehnologije prepoznavanja otiska prsta na pametnom telefonu 2018. - 2022



Izvor: https://www.statista.com/statistics/1003600/smartphone-fingerprint-recognition-technology-share/

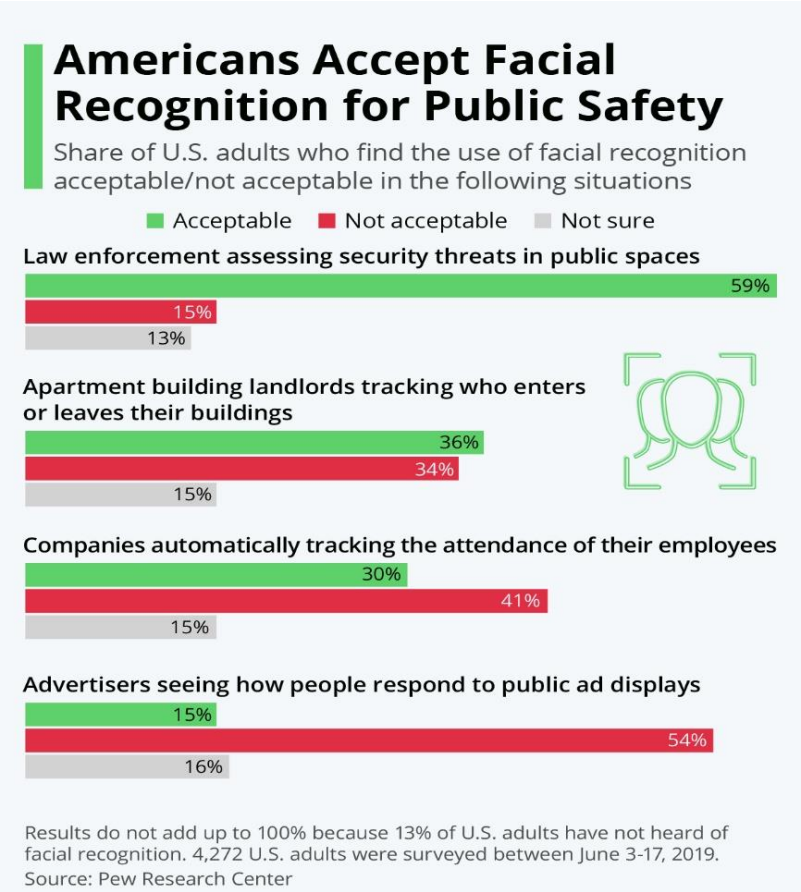
Danas mnogi Android telefoni također imaju ovu značajku (u kombinaciji sa skeniranjem šarenice). Prema Counterpointu, više od milijarde pametnih telefona s senzorima otiska prstiju isporučeno je u 2018. godini, a ta milijarda pametnih telefoni dolazit će s nekim oblikom rješenja za otključavanje licem 2020. godine.

KYC (engl. *Know Your Customer* - upoznajte svog kupca) ili KYC provjera obvezni je postupak identificiranja i provjere identiteta klijenta prilikom otvaranja računa i periodički tijekom vremena. Ova provjera se obično sprovodi u bankama jer banke moraju biti sigurne da su njihovi klijenti upravo oni. Danas je to važan element u borbi protiv financijskog kriminala i pranja novca. Korištenjem biometrije, banke, fintech organizacije ili čak telekom operateri mogu brže i učinkovitije učiniti obvezne KYC provjere. U Indiji je odobrena uporaba Aadhaar – ovog KYC-a za mobilne veze i bankovne račune (Prema Aadhaarovom amandmanski zakon iz srpnja 2019.). Trgovci mogu iskoristiti prepoznavanje lica kako bi identificirali najboljeg kupca ili bivšeg kradljivca čim dođu u trgovinu. Ako ga sustav prepozna, šalje upozorenje upravitelju trgovine.

„*Tehnologija je snažan marketinški pokretač ili se može primijeniti na policiju*.“

Barem tako tvrdi britanski The Guardian (04. kolovoza 2019.) jer navodi da je postalo besmisleno prijavljivati krađu policiji. Trgovci moraju pronaći rješenja za procijenjeni gubitak od 700 milijuna funti. Okreću se rješenjima za prepoznavanje lica. Dok prema web mjestu NYmag (listopad 2018.), američki trgovci također koriste prepoznavanje lica. Gotovo sve vodeće američke tvrtke imaju u svom programu prepoznavanje lica ili su barem istražile njegov potencijal. Wallmart ga ne koristi, Target niti, Lowe's i Saks Fifth Avenue u Kanadi koriste tu tehnologiju. Međutim, zakoni o privatnosti u Illinoisu, Teksasu, Washingtonu i Kaliforniji (od siječnja 2020.) i SHIELD-u države New York (od ožujka 2020.) predstavljat će ozbiljan izazov tim naporima. Skupine za građanske slobode u Americi žele embargo na tehnologiju i preciznu demokratsku raspravu o mjestu koje bi biometrija lica trebala zauzeti u našem životu. Iako po istraživanju o tome prihvaćaju li Amerikanci tehnologiju prepoznavanja lica u službi javne sigurnosti gotovo 60% odraslog američkog stanovništva smatraju da je prihvatljivo za izvršitelje zakona da primjenjuju tehnologiju prepoznavanja lica u javnim prostorima. Preko polovice odraslih osoba u SAD-u smatra neprihvatljivim da oglašavači prate odgovor ljudi na prikazivanje oglasa koristeći biometrijsku tehnologiju. Slično tome, otprilike četiri od deset ispitanika ne vjeruje da bi tvrtke trebale biti u mogućnosti pratiti prisustvo zaposlenih pomoću ove tehnologije kao što je prikazano na idućem grafu.

Graf 6: Prihvaćanje biometrijske tehnologije u primjeni javne sigurnosti



Izvor: https://www.statista.com/chart/19321/facial-recognition-public-opinion/

5. INOVACIJE U BIOMETRIJI

Kao što je prije bilo navedeno biometrijska identifikacija većinom se koristi u sustavima kontrole pristupa kako bi se lakše identificirala osoba koja prilazi određenom objektu ili pristupa štićenoj imovini ili osobi, a u današnje doba ima primjenu u slučajevima korištenja koji se šire i izvan upravljanja granicama.

U 2017. godini dogodile su se neke od evolucijskih promjena doživljenih na polju biometrije. Izvješće članice NAFTA-e (Sjevernoameričkog sporazuma o slobodnoj trgovini – engl. *The North American Free Trade Agreement*) napominje da su banke također ovlaštene koristiti tehnologije prepoznavanja lica i glasa za internetsku provjeru identiteta. Slična je shema u tijeku u Meksiku gdje je Nacionalno povjerenstvo za bankarstvo i sigurnost donijelo pravilo koje zahtijeva da svaka banka u zemlji uvede skenere otiska prsta za klijente u sljedećih dvanaest mjeseci.

U 2017. indijska vlada najavila je da će indijski građani u budućnosti trebati povezati Aadhaar s PAN (engl . *Permanent Account Numbers,* odnosno brojevi stalnih računa - koje je izdao Središnji odbor za izravne poreze), bankovnim računima. Ista se obveza odnosi na raznolik spektar štednih i investicijskih shema. Jedna od glavnih Aadharovih promjena je i pokretanje autentifikacije lica u srpnju 2018. S obzirom na to da je broj Aadhaar neraskidivo povezan s jedinstvenim biometrijskim podacima vlasnika, njegovo udruživanje s ključnim financijskim računima predstavlja moćno sredstvo za ispunjavanje obveza KYC-a, kao i za suočavanje s modernim prijetnjama poput pranja novca i utaje poreza. Oko 558 milijuna bankovnih računa već je povezano s Aadhaarom. Ukupan broj bankovnih računa u zemlji, prema procjenama, iznosi oko 1,1 milijardu.

U Rusiji je središnja banka u ljeto 2017. započela s izvođenjem velikog biometrijskog programa nazvanog "Unified Biometrics System" (UBS). Državna tvrtka Rostelecom vodit će bazu podataka koja će prikupljati lice, glas, šarenicu i podatke o otiscima prstiju u cijeloj zemlji. U veljači 2018. godine Rostelecom je zajedno s Tinkoff bankom, VTB bankom i Pochta bankom predstavio beta verziju svoje "UBS", digitalne platforme razvijene na zahtjev Ministarstva komunikacija i masovnih medija i Banke Rusije.

Lokalni čimbenici oblikuju globalnu budućnost biometrije. Primjerice, u Južnoj Americi borba protiv prijevara jasan je prioritet: ne samo u domeni financijskih usluga, već i drugih potencijalno ranjivih poduzeća poput iznajmljivanja automobila. Naročito je Brazil odlučio krenuti naprijed. Prije toga, Brazilski vrhovni izborni sud (TSE) dobio je pravo prikupljanja biometrijskih podataka za identifikaciju birača kao sredstva za sprečavanje prijevara. Početkom 2017. vlada je najavila da želi da TSE do 2020. prikupi biometrijske podatke od 140 milijuna građana s konačnim ciljem stvaranja jedinstvene baze podataka građana i jedinstvene osobne iskaznice. U zemljama u razvoju potreba da se građanima pruže neoborivi dokazi o identitetu presudna je u smislu širenja pristupa bankovnim računima, državnim službama i još mnogo toga.

Sve u svemu, biometrija ne predstavlja magično rješenje za sve sigurnosne probleme, drugim riječima, koliko god bila primamljiva tehnologija, godine koje su pred nama zahtijevat će od dionika da se prema biometriji odnose prema jednom od elementa mnogo šireg, višeslojnog alata za identifikaciju i provjeru.

5.1. Inovacije u video nadzoru

Koncept tehnologije bespilotnih letjelica čini se futurističkim, ali posljednjih godina primjenjuje se u vojsci, filmskoj produkciji i, relativno, u sigurnosnoj industriji. Implementacija CCTV rješenja koja koriste tehnologiju dronova može poboljšati brojne sigurnosne procese jer su otporniji, trajniji i isplatljiviji. Drone CCTV može pokriti više područja, jer nije ograničen na snimanje nadzornih snimaka s jednog određenog mjesta. Može se ručno kontrolirati prelazak određenog područja preko web lokacije ili slijediti unaprijed programirani put. Ako se aktivira alarma za neovlašten pristup području koji se kontrolira, dron se može koristiti za početnu istragu i prikazivanje snimki uživo; ovo može dobar način da stražar ili osoblje procijene rizik situacije s uljezom ili utvrde je li riječ o lažnoj uzbuni. Dronovi mogu biti neprocjenjiva vrijednost koja povećava sigurnost osoblja i javnosti.

Primjena umjetne inteligencije (AI) i strojno učenje idu ruku pod ruku sa sigurnosnim mjerama poput kontrole pristupa i video nadzora. Sa sve više i više sustava za kontrolu pristupa

koji sada koriste biometrijske podatke i prepoznavanje lica za kontrolu pristupa, AI im pomaže jer poboljšava upravljanje identitetom kontinuiranim prilagođavanjem i prepoznavanjem osobina i značajki osobe čak i u različitim svjetlima, vremenskim uvjetima i okruženju. Ova dva tehnološka elementa također se mogu integrirati u tehnologiju bespilotnih letjelica postavljanjem bespilotne letjelice na vlastiti put i namještanjem vlastitih alarma letjelice, ukoliko uoči bilo kakvo kretanje u ograničenom području kojeg drži pod nadzorom. Dronovi mogu inspekcije zaštite učiniti učinkovitijima, a upotreba AI zajedno s tehnologijom dronova može omogućiti manje ljudske intervencije - osim ako nije potrebno.

5.2. CES 2019.

CES 2019. započeo je uvod u inovacije u sigurnosnoj tehnici sa automatizacijom kuća i njegovom eventualnom integracijom sa sigurnosnim sustavima za stanovanje koje danas poznajemo kao Pametni dom. Također nudi uvid u druge značajne tehnološke trendove - umjetnu inteligenciju (AI), strojno učenje, Internet stvari (IoT), itd. - koji sada utječu na razne druge sektore sigurnosnog tržišta, najviše na video nadzor i kontrolu pristupa. Od većine kompanija potanko će se opisati par njih koje imaju mogućnost da njihova tehnologija stvori utjecaj na sigurnosnu industriju.

Uvođenje neuronske mreže, CV2 procesor podržan od umjetne inteligencije s CVFlowom od popularnog proizvođača System-on-Chip (SoC) Ambarella najnovije je otkriće Kompanije Ambarella koja je poznata na tržištu kamera za video nadzor. Ključni diferencijal je Ambarellina niža potrošnja energije, koja praktički eliminira mogućnost loših performansi zbog toplinskog okruženja čipa. Razlika u usporedbi Ambarellove identifikacije vozila na više prometnih trakova i obrade temeljene na ANPR / LPR AI-u pokazuje njihov video tok kontinuiranim i neprekinutim, dok se procesor njihovog konkurenta trudi održati korak, prikazujući isprekidani video isječak koji prikazuje snimku brzinom kadrova od 5 slika u sekundi. Njihov procesor ugrađen u nadzornu videokameru provodi jako dobre rezultate, a nadalje će se navesti što su najbolje značajke ovog čipa ugrađenog u video kameru.

- Prepoznavanje predmeta u stvarnom vremenu s visokom razinom prepoznavanja.
- Prepoznavanje ID vozila u stvarnom vremenu na višetračnim prometnicama + ANPR / LPR (engl. *automatic number plate recognition* - software koji obrađuje input od LPR kamere i prepoznaje alfanumeričke oznake na tablici te ih sprema u bazu podataka / *license plate recognition* - posebne CCTV kamere za snimanje registracijskih tablica u raznim okolišnim uvjetima) , a sposobno je prepoznati čak i kamione sa više tablica.
- 3D prikaz predmeta koji prikazuje vizualne razlike u bojama.
- Višebojni pogledi na ulice, promet, zgrade s prepoznavanjem objekata.
- Prepoznaje i identificira sva pojedinačna vozila čak i na gustom raskrižju.

Security and Safety Things (SAST) – od Boscha tvrtka nudi jednu od najperspektivnijih inovacija u sigurnosnom ekosustavu stvaranjem četiri ključne usluge:

- Prva "standardizirana" OS platforma koja podržava gotovo svaku kameru za video nadzor s transparentnim nadogradnjama, slično načinu na koji Google Play i App Store obrađuju ažuriranja.
- Portal integratora dizajniran za pružanje video usluga.
- App Store svjetske klase za kupnju video menadžmenta, analitike i srodnih aplikacija.
- Okruženje za programere dizajnirano za poticanje suradnje na novoj platformi i promicanje SAST zajednice.

Resideo je osnovan kako bi pružio HVAC, udobnost, sigurnost i potpuno integriranu automatizaciju kuće u stambeno i malo komercijalno okruženje. Najzanimljiviji je proizvod mali početni komplet za automatizaciju kuće predstavljen u paketu koji sadrži visokotehnološki cilindar s detekcijom područja, kontrolom zaključavanja ulaza, video nadzorom i zvukom.

Alarm.com poznata po svojoj sveobuhvatnoj platformi mobilnih usluga, tvrtka je na CES 2019 predstavila dvije nove značajke. Prva je nova značajka "Smart Signal" pri čijem korištenju pretplatnik može otkazati kućni alarm ili ga potvrditi, pri čemu će središnja stanica

nastaviti s dispečerskim ovlastima, što će stvoriti priliku za značajno smanjenje lažnih alarma. Druga je wellness usluga koja pruža članovima obitelji i prijateljima priliku da starije osobe zaštite, a pritom održavaju njihovu neovisnost kroz personaliziranu skrb za starije osobe. Wellness koristi diskretne bežične senzore u čitavom dnevnom prostoru, prati aktivnosti i moguće padove starijih osoba, pružajući tako njegovateljima uvid u trenutne uvjete u stvarnom vremenu , kao i potencijalne nove probleme.

UVeye je odgovor na bržu obradu pregleda vozila kroz skeniranje podnog dijela vozila. UVeye je ili će biti raspoređen u širokom rasponu vertikalnih industrija, uključujući granične prijelaze, proizvođače vozila, zračne luke i stadione. Bombe, oružje i droga skriveni u komponentama donjeg dijela vozila poput spremnika za gorivo otkrivaju se uočavanjem sitnih promjena u izgledu dijela vozila. UVeye je neprestano prikupljao uspješne skene kako bi te komponente trebale izgledati, a time poboljšava postupak prepoznavanja kroz algoritme strojnog učenja.

Kwikset je dizajnirao dvije nove pametne brave "Halo" s omogućenom Wi-Fi mrežom i Bluetoothom kojes se povezuju s postojećim usmjerivačima, nije potreban hub, a putem mobilne aplikacije za pametni telefon ili tablet Kwikset podržava 250 jedinstvenih korisničkih kodova i funkcije daljinskog zaključavanja ili otključavanja.

5.3. Inovacije u svijetu

Jedna od zanimljivijih inovacija svakako je Intelligent Fingerprinting koji koristi prijenosni uređaj za analizu sitnih tragova znoja s otisaka prstiju, a u roku od deset minuta precizno otkriva upotrebu droga u rasponu od marihuane do heroina i više, što bi moglo biti moguće samo uzimanjem uzorka mokraće ili sline. Naprava za ispitivanje droge tvrtke Intelligent Fingerprinting sadrži mali uložak za provjeru droge na koji se korisnikovi otisci prstiju prikupljaju u procesu koji traje manje od minute kao što i vidimo na Slici 5.

Slika 5: Prikupljanje otiska prstiju na ulošku

Izvor: https://i.ytimg.com/vi/h05-O_V0Z68/maxresdefault.jpg

Zatim prijenosna jedinica za analizu (Intelligent Fingerprinting DSR-Plus) očitava uložak i na zaslonu daje pozitivan ili negativan rezultat za kokain, opijate, kanabis i metamfetamin u deset minuta. Patrone su kompaktne, lagane i isporučuju se u pojedinačnim vrećicama sa zatvorenom folijom, spremne za upotrebu kad god i gdje god su potrebne. Nakon što se otisci prstiju prikupe na podlozi za nanošenje uzorka, uzorak je zaštićen od neovlaštenog otvaranja zaštitnim poklopcem koja klizi preko spremnika i zaključava se na svoje mjesto. Patrone koriste tehnologiju bočnog protoka - slično testu trudnoće - za otkrivanje određenih opojnih sredstava ili njihovih metabolita u znoju prikupljenom iz otisaka prstiju.

Nadalje će se navesti još par novijih ideja koje se testiraju sa mnogo raznih oblika biometrijske autentifikacije.

U tekućoj potrazi za zamjenom PIN-a i lozinki, Mastercard je predstavio komplet koji omogućava potrošačima da kod kuće registriraju vlastiti otisak prsta na biometrijskoj kartici, zaobilazeći potrebu da posjete banku. Kad potrošači od svog izdavača dobiju EMV karticu opremljenu Mastercardovom tehnologijom prepoznavanja otiska prsta, mogu upisati svoje

biometrijske podatke na karticu pomoću prsta i posebnog utora za karticu na baterije. Primjerak te kartice uočavamo na Slici 6.

Slika 6: Mastercardova biometrijska kartica

Izvor: https://arizent.brightspotcdn.com/dims4/default/5863229/2147483647/strip/true/crop/3264x2448+0+0/resize/733x550!/quality/90/?url=https%3A%2F%2Fsource-media-brightspot.s3.amazonaws.com%2F36%2Fc0%2F3331c3c34ba69b96cdd1a841a737%2Fbiometric.sleeve.jpg

Pojednostavljeni postupak upisa posljednji je pokušaj Mastercarda da poboljša biometrijske pristupe autentifikaciji korisnika kartica. Njegova druga biometrijska rješenja za provjeru autentičnosti uključuju "selfie pay" i skeniranje šarenice na bazi pametnih telefona.

BBVA je započela testiranje aplikacije za plaćanje prepoznavanja lica koju zaposlenici mogu koristiti u kafeterijama i restoranima u uredima Ciudad BBVA i poslovnom konferencijskom kompleksu u Madridu. Više od 1.000 zaposlenika u Ciudadu koristi aplikaciju za plaćanja, koja pruža mogućnost rezerviranja stolova i objedovanja bez izdavanja fizičkog računa. Kupci obavještavaju konobara da su spremni za odlazak, a konobar potvrđuje

registraciju u sustav i račun koji je povezan skeniranjem lica. Trošak obroka prikazan je putem aplikacije. BBVA procjenjuje da korisnici aplikacija uštede do 10 minuta u restoranima, što također donosi korist povećanom naplatom od prometa stolova. Sljedeći korak za aplikaciju za plaćanja, kaže BBVA, jest smještavanje prepoznavanja lica u praktičnu upotrebu s postavkama maloprodajnih trgovina. Aplikacija također ima person-to-person značajku koja registriranom korisniku s povezanom kreditnom karticom omogućuje slanje sredstava drugima i to slanjem poruka izravno iz aplikacije, nešto slično kao KEKS pay.

Počevši od travnja 2019., Mastercard kaže da će Mastercard Identity Check – poznatiji kao "selfie pay" - omogućiti korisnicima da odobravaju transakcije putem otisaka prstiju, šarenice ili prepoznavanja lica prilikom "checkouta" iz e-trgovine kroz plaćanja Mastercard karticom. Mastercard provjera identiteta već je dostupna u 37 zemalja, a Mastercard kaže da novi regulatorni zahtjevi Europske unije za provjeru autentičnosti koji stupaju na snagu putem PSD2 navode da banke diljem kontinenta moraju ponuditi biometrijsku opciju do početka 2019. godine.

Potrošači upisani u dansku shemu domaćih plaćanja Dankort mogu se prijaviti za plaćanje koristeći samo svoj prst u projektu koji platna kompanija Nets provodi u Kopenhagenu. Inovativni ogranak Netsa, Smart Payments, udružio se s Fingopayem i poslovnom školom u Kopenhagenu kako bi omogućio plaćanja provjerom autentičnosti vena prstiju u školskoj blagovaonici u kojoj studenti, fakultetsko osoblje i drugi kupuju bez bilo kojeg fizičkog instrumenta plaćanja. Skeneri prstiju instalirani su na svim naplatnim mjestima u školskoj blagovaonici, a svi koji su već upisani u Dankort mogu sudjelovati bez potrebnog PIN-a. Tehnologija skeniranja vena na prstima sigurnija je od provjere autentičnosti otiska prsta na pametnim telefonima jer je uzorke vena na prstima gotovo nemoguće replicirati, a za provjeru autentičnosti plaćanja potrebna je cirkulacija krvi, dakle potreban je živi prst. Korisnici također mogu u bilo kojem trenutku prekinuti funkciju skeniranja prstiju sa svojeg Dankort računa.

I vlade i privatna industrija okreću se mobilnoj biometriji kako bi ubrzale obradu identifikacije ljudi. Mobilna biometrija jednostavno znači postizanje individualne biometrijske identifikacije na mobilnom uređaju koja se lako premješta ili prebacuje s jednog mjesta na drugo. Biometrijska funkcionalnost može se postići na mobilnom uređaju bilo ugrađenim

biometrijskim senzorima ili pričvršćivanjem prijenosnog biometrijskog hardvera na njega putem USB kabela ili putem Wi-Fi veze. Ovaj trend pokreće činjenica da se biometrijska identifikacija ljudi ne može uvijek izvoditi u kontroliranom uredskom okruženju. Ponekad će biometrijska identifikacija biti potrebna tamo gdje ljudi idu i gdje se nalaze, možda na javnim mjestima. U tim situacijama mobilna biometrija može biti učinkovita i ubrzati postupak identifikacije. Sjajan primjer za to može biti irački automatizirani sustav kontrole granice. Trenutno imaju više od 100 mobilnih biometrijskih kontrolnih točaka, gdje su preko milijun podnositelja registracije koji se trenutno svakodnevno provjeravaju sustavom biometrijske identifikacije ABIS, koji je skalabilan je i prilagodljiv automatizirani sustav identifikacije otiska prsta (AFIS), kako bi zaštitili svoje granice od pobunjenika i terorista.

Sljedeći trend u biometriji je uporaba više biometrijskih sustava za provjeru autentičnosti za ljudsku identifikaciju. Multimodalni biometrijski sustavi za provjeru autentičnosti uzimaju podatke jednog ili više biometrijskih uređaja za mjerenje dviju ili više različitih biometrijskih karakteristika kako bi osigurali točnost provjere autentičnosti. Posjedovanje jednog oblika biometrije za provjeru autentičnosti više nije učinkovita opcija za mnoge tvrtke. Na primjer, tvrtka Mass Contracting Co. WLL sa sjedištem u Bahreinu je proizvodna i građevinska tvrtka. Željeli su nadzirati prisustvo svojih građevinskih radnika i odlučili su primijeniti multimodalno rješenje Bio-Plugin s modalitetom otiska prsta i vena prsta. Odluku su donijeli nakon što su razmotrili prirodu posla koji su obavljali njihovi građevinski radnici. Očekuje se da će građevinski radnici imati suhe, posječene ili oštećene prste. Imati samo unimodalno rješenje temeljeno na otisku prsta nije bilo idealno za hvatanje većine pojedinačnih biometrijskih podataka. Unimodalni biometrijski sustav bilježi i podudara se samo s jednim biometrijskim svojstvom što rezultira nedostatkom održivih načina rješavanja ograničenja poput iskrivljenih podataka, varijacija unutar klase i neuniverzalnosti. Očekuje se da će multimodalni biometrijski sustavi za provjeru autentičnosti biti pouzdaniji protiv ovih problema zbog prisutnosti višestrukih, neovisnih biometrijskih svojstava. Očekuje se da će se u budućnosti više koristiti multimodalni biometrijski sustavi za provjeru autentičnosti zbog svoje učinkovitosti u pružanju točnijih rezultata i jače sigurnosti.

Biometrijska rješenja zasnovana na cloud tehnologiji uglavnom pokreće mobilna biometrijska tehnologija. Kad razmišljate o mobilnoj biometrijskoj tehnologiji, uparivanje tog

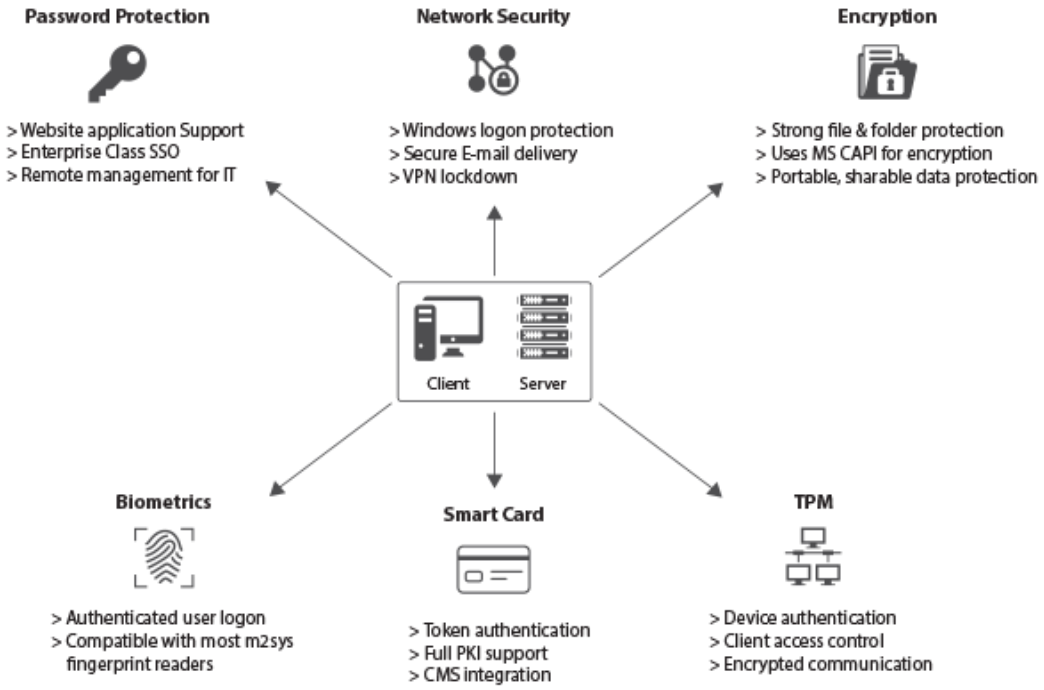
mobilnog biometrijskog uređaja s biometrijskim rješenjem temeljenim na oblaku može još više ubrzati postupak identifikacije. Umjesto lokalnog spremanja biometrijskih podataka, sigurnije je rješenje slanje u oblak. Iako i ono ima sigurnosne propuste. Uz to, kada vlada i poduzeća izračunavaju opće troškove koje moraju snositi za održavanje fizičkog poslužitelja, prelazak na oblak čini se mudrim izborom. Sljedeća činjenica iza porasta trenda korištenja biometrijskih rješenja temeljenih na oblaku je skalabilnost oblaka. Računarstvo u oblaku omogućuje poslovanju da lako poveća ili smanji svoj IT zahtjev prema potrebi. Na primjer, mogu brzo povećati svoje postojeće resurse kako bi udovoljili povećanim poslovnim potrebama ili promjenama. To im omogućuje prilagodbu poslovnom rastu bez skupih promjena postojećih IT sustava.

Imati vertikalno specijalizirano biometrijsko rješenje za upravljanje identitetima postaje popularan izbor za mnoge industrije. Ovakve vrste rješenja dizajnirane su da udovolje jedinstvenoj potražnji njihovih industrija. Također su prilagođena imajući na umu lokalne i međunarodne industrijske zakone i standarde. Na primjer, ako se pogleda vertikalno specijalizirano biometrijsko rješenje CertisID za industriju financijskih usluga, osmišljeno je kako bi pružilo sigurnost i smanjilo prevare i otpad, pružajući cjelovit revizijski trag za aktivnosti kupaca i zaposlenika. Za zdravstvenu industriju postoji pametna zdravstvena platforma RightPatient koja omogućuje višu razinu preciznosti za identifikaciju pacijenta i objedinjuje velike podatke i kliničko znanje u zdravstvu da pogoni upravljanje personaliziranim zdravljem, podrškom u donošenju odluka i prediktivnom analitikom. Kada traže rješenja za upravljanje biometrijskom identifikacijom, tvrtke su vrlo svjesne svojih jedinstvenih zahtjeva i odlučuju se za primjenu prilagođenog rješenja dizajniranog posebno za njihove vertikale. Ta rješenja ne samo da pružaju veću učinkovitost i kontrolu, već ponekad pružaju konkurentsku prednost u odnosu na tvrtke koje ih još ne usvajaju.

Jedna od najpopularnijih rasprava u ovom trenutku je hoće li biometrija zamijeniti lozinke. Ova je rasprava izašla na vidjelo zbog činjenice da mnoge tvrtke usvajaju biometrijski jedinstveni znak (SSO – engl. *single sign-on*) preko tradicionalnih lozinki kako bi zaštitile svoje mreže od kršenja podataka i smanjile troškove upravljanja lozinkama. Lozinke su slabe i to iz više razloga: mogu se pogoditi, zaboraviti, podijeliti ili zamijeniti. Suprotno tome, biometrija je jedinstvena, teško ju je obmanuti i ne može se izgubiti ili podijeliti. U nekim

slučajevima kada se zaposlenici moraju prijaviti u više baza podataka i imati različite lozinke za svaku od njih, to može biti vrlo frustrirajuće. Tvrtka za integraciju ICT-ovih sustava Digital Alliance Limited sa sjedištem u Ugandi suočila se s pomalo sličnim problemom. To nije samo frustriralo zaposlenike već i smanjilo produktivnost. Zbog toga su odlučili implementirati Enterprise Biometric Suite, cjeloviti biometrijski pojedinačni SSO. SSO je kontrola pristupa u kojem korisnik mora predstaviti svoje vjerodajnice u obliku nekog biometrijskog obilježja samo jednom da bi se prijavio na usluge, a može se neometano prebaciti na druge povezane usluge bez potrebe za davanjem vjerodajnica identiteta dok sesija traje. Ovaj pristup dramatično poboljšava korisničko iskustvo i štedi znatno vrijeme i napore na pružanju vjerodajnica svaki put kada se korisnik prebaci na drugu uslugu. Na idućoj slici je prikazan proces rada SSO-a.

Slika 7:Proces rada SSO-a



Izvor: https://www.m2sys.com/wp-content/uploads/2015/05/M2SYS-single-sign-on-working-process.png

Njihovi zaposlenici više se ne moraju sjećati lozinki, a njihove mreže su također bile zaštićene.

Tehnologija prepoznavanja šarenice na biometrijskoj osnovi za identifikaciju goveda jedna je od velikih inovacija godine. Koristeći najsuvremeniju biometrijsku IRIS tehnologiju, osiguravajuća društva mogu točno utvrditi pravu stoku vlasnika prije namire zahtjeva. Prepoznavanje lica ili šarenice također može pomoći u preciznom prepoznavanju ugroženih vrsta kako bi ih se brojalo. Jedna od vodećih indijskih biometrijskih tvrtki - Mantra Softech ima sposobnosti dizajniranja i razvoja takvog inovativnog i naprednog IRIS sustava prepoznavanja na temelju biometrije za identifikaciju goveda.

Kombinacija biometrije i tehnologije virtualne stvarnosti (VR) sljedeće generacije postala je tema tehnološke industrije. Biometrijska identifikacija, kombinirana s VR-om, može donijeti krajnje korisničko iskustvo i povjerenje u CRM (engl. *Customer Relationship Management*) dodavanjem rigoroznih sigurnosnih protokola za provjeru autentičnosti uređaja i identifikaciju potrošača. U digitalnom okruženju koje se brzo mijenja, neke e-trgovine i bankarske tvrtke omogućuju značajke virtualnog obilaska / virtualnog isprobavanja temeljene na biometriji kako bi poboljšali korisničko iskustvo.

Od početka 2019. godine novi revolucionarni ultrazvučni skeneri otiska prsta stječu veliku popularnost. Ova tehnologija koristi ultrazvučne valove za mapiranje 3D grebena i dolina otiska prsta pojedinca kako bi se postigla veća brzina i preciznost biometrijske identifikacije. Nova značajka otkrivanja otiska prsta na zaslonu modernih pametnih telefona koristi najmodernije ultrazvučne senzore otiska prsta kako bi korisnicima pružila krajnju brzinu i udobnost. Ultrazvučna tehnologija otiska prsta djeluje vrlo različito od kapacitivnih skenera otiska prsta koji mogu reproducirati samo 2D slike. 3D detalje je puno teže krivotvoriti ili prevariti od 2D slike, što ultrazvučni sustav čini mnogo sigurnijim. Podrazumijeva se da je ultrazvuk također mnogo sigurniji od optičkih skenera otiska prsta, koji su gotovo pali u nemilost.

6. BIOMETRIJSKA SIGURNOST

Biometrija može ispuniti dvije različite funkcije, autentifikaciju i identifikaciju, kao što je prije bilo navedeno.

Identifikacija odgovara na pitanje: "Tko ste vi?". U ovom slučaju, osoba je identificirana kao jedna, između ostalih. Osobni podaci osobe koju treba identificirati uspoređuju se s podacima drugih osoba pohranjenih u istoj bazi podataka ili eventualno drugim povezanim bazama podataka.

Autentifikacija odgovara na pitanje: „Jeste li stvarno ono za što kažete da jeste?“. U ovom slučaju, biometrija omogućuje potvrđivanje identiteta osobe uspoređivanjem podataka koje pružaju s unaprijed snimljenim podacima za osobu za koju tvrde da jest.

Ove dvije funkcije pozivaju se na različite tehnike. Općenito, za identifikaciju je potrebna centralizirana biometrijska baza podataka koja omogućuje usporedbu biometrijskih podataka nekoliko osoba. Autentifikacija može bez takve centralizirane baze podataka. Podaci se jednostavno mogu pohraniti na decentraliziranom uređaju, poput jedne od pametnih kartica.

Za zaštitu podataka poželjan je postupak provjere autentičnosti s decentraliziranim uređajem. Takav pristup uključuje manji rizik. Token (osobna iskaznica, vojna iskaznica, zdravstvena iskaznica) čuva se u posjedu korisnika i njihovi podaci ne moraju biti pohranjeni u bilo kojoj bazi podataka. Suprotno tome, ako se koristi postupak identifikacije koji zahtijeva vanjsku bazu podataka, korisnik nema fizičku kontrolu nad svojim podacima sa svim rizicima koje to uključuje.

Biometrijska sigurnost nudi brojne prednosti (za snažnu autentifikaciju i identifikaciju), ali nije bez kontroverzi. Ovaj je izazov povezan s privatnošću i sposobnošću građana da kontroliraju podatke o sebi.

Mogu se identificirati dvije vrste rizika:

1) Korištenje biometrijskih podataka u druge svrhe (tzv. puzanje funkcija) od onih za koje se građanin složio kod davatelja usluga. Čim su biometrijski podaci u rukama

treće strane, postoji rizik da se takvi podaci mogu koristiti u svrhe različite od onih na koje je dotična osoba dala svoj pristanak. Stoga se mogu dogoditi slučajevi neželjene krajnje upotrebe ako su takvi podaci međusobno povezani s drugim datotekama ili ako se koriste za druge vrste obrade osim onih kojima su u početku bili namijenjeni.

2) Rizik ponovne upotrebe podataka predstavljenih za biometrijske provjere. Podaci se mogu prikupiti tijekom njihovog prijenosa u središnju bazu podataka i na prijevaran način kopirati u drugoj transakciji.

Rezultat je to što osoba gubi kontrolu nad svojim podacima, što predstavlja rizik za privatnost. Čini se da u praksi tijela za zaštitu podataka daju prednost rješenjima koja sadrže decentralizirane podatkovne uređaje.

7. ZAKLJUČAK

Sve u svemu, biometrijska identifikacija danas ima velik utjecaj na život i poslovanje ljudi i velikih industrija općenito. U današnje doba u razvijenom svijetu ponekad je velika prednost imati biometrijsku kontrolu pristupa jer većinom označava naprednu, brzorastuću tvrtku i smanjuje troškove održavanja servera, ako se koristi pohrana u oblaku, pogotovo ako se biometrija koristi umjesto PIN-ova i lozinki. Biometrijske tehnologije većinom su sigurne, postojane, univerzalne, mjerljive i otporne na krivotvorenje, a većina je građana danas dobro upoznata sa pogodnostima biometrije, kao na primjer, skeneri otiska prsta i prepoznavanje lica na pametnim mobitelima ili biometrijske pametne kartice ili putovnice te osobne iskaznice.

Sustavi biometrijske identifikacije većinom su precizni, brzi i s malom mogućnošću pogreške. U današnje doba bolje je koristiti multimodalne sustave od unimodalnih jer pružaju veću sigurnost, precizniji su, osoba se može bolje identificirati preko njih jer koriste više senzora. Ono što se istražuje i evoluira u biometrijskoj identifikaciji definitivno je služba umjetne inteligencije i strojnog učenja koja poboljšava raspoznavanje biometrijskih uzoraka, ubrzava automatiziran proces identifikacije te kvalitetniji čipovi u nadzorni video kamerama koje služe primarno za identifikaciju registarskih tablica vozila na višetračnim prometnicama.

Ljudi i dan danas prema istraživanju nisu voljni davati svoje podatke ili dopustiti biometrijsku identifikaciju zbog straha o zlouporabi tih podataka. Danas ima mnogo različitih proizvoda za biometrijsku identifikaciju te se u zadnje vrijeme radi na tome da se svi ti sustavi unificiraju što bi dovelo do boljeg povezivanja i još brže identifikacije na svjetskoj razini.

Smatram da primjena biometrijske identifikacije skupa sa ostalim načinima osiguravanja imovine i ljudi uz kontrolu pristupa može samo poboljšati sveopću sigurnost.

POPIS LITERATURE

Knjige:

1. Bača, M., Biometrija između sigurnosti i privatnosti
2. Radmilović, Ž., Biometrijska identifikacija
3. Sigurnosni sustavi, Predavanje 3 , 24. slajd, Veleučilište u Rijeci, Stručni studij sigurnosti

Internetski izvori:

4. About Face ID advanced technology, 26.2.2020. https://support.apple.com/en-us/HT208108(6.9.2020.)
5. Arjun Singh, 25.12.2019., The Most Iconic Biometric Innovations of 2019 https://blog.mantratec.com/top-biometric-technology-innovations-2019 (11.9.2020.)
6. Biometric data and data protection regulations (GDPR and CCPA) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data (11.9.2020.)
7. Biometrics: definition, trends, use cases, laws and latest news, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (28.8.2020.)
8. Biometrija, CCERT-PUBDOC-2006-09-167, https://www.cert.hr/wp-content/uploads/2006/09/CCERT-PUBDOC-2006-09-167.pdf (26.8.2020.)
9. Daniel Wolfe, 6 new innovations in biometric authentication, https://www.paymentssource.com/list/6-new-innovations-in-biometric-authentication (11.9.2020.)
10. Fingerprint Drug Test Technology Developed, https://www.securitymagazine.com/articles/90471-fingerprint-drug-test-technology-developed(10.9.2020.)
11. Mike Haldas, 13.12.2010., What is the difference between LPR and ANPR surveillance? https://videos.cctvcamerapros.com/support/topic/what-is-the-difference-between-lpr-and-anpr-surveillance(7.9.2020.)
12. Latest innovations in security technology, https://www.millenniumsecurity.co.uk/2020/02/03/innovations-security-technology (10.9.2020.)
13. Multimodal Biometric Systems https://www.tutorialspoint.com/biometrics/multimodal_biometric_systems.htm (26.8.2020.)
14. New trends in biometrics with Isabelle Moeller from the Biometrics Institute, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/trends-in-biometrics (27.8.2020.)
15. Nick Tabor, 20.10.2020., FACIAL RECOGNITION OCT. 20, 2018 Smile! The Secretive Business of Facial-Recognition Software in Retail Stores https://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html (10.9.2020.)

16. Önsen Toygar, Esraa Alqaralleh and Ayman Afaneh, Person Identification Using Multimodal Biometrics under Different Challenges, 20.12.2017. https://www.intechopen.com/books/human-robot-interaction-theory-and-application/person-identification-using-multimodal-biometrics-under-different-challenges (7.9.2020.)
17. Osobna iskaznica (eOI) https://mup.gov.hr/osobna-iskaznica-eoi/328 (22.8.2020.)
18. Rachel German, K. Suzanne Barber, Current Biometric Adoption and TrendsUT CID Report #18-02, rujan 2017. https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf (20.8.2020.)
19. Shanhong Liu, 11. rujna, 2020, Biometric technologies - Statistics & Facts , https://www.statista.com/topics/4989/biometric-technologies/ (26.8.2020.)
20. Shaon Shahnewaz , 5 Recent Trends in Biometric Technology https://www.m2sys.com/blog/mobile-biometrics-2/5-recent-trends-in-biometric-technology/ (5.9.2020.)
21. Steve Surfaro, 11.1.2019., Innovations in security tech from CES 2019 https://www.securityinfowatch.com/video-surveillance/video-analytics/article/21040959/innovations-in-security-tech-from-ces-2019 (10.9.2020.)
22. Tom Chivers, 4.8.2019., Facial recognition… coming to a supermarket near you https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties (10.9.2020.)
23.

POPIS SLIKA I GRAFIKONA

Slika 1: Sinoptička tablica fizionomskih obilježlja 2
Slika 2: Multimodalni biometrijski sustav 10
Slika 3: Elektronička putovnica 15
Slika 4: Biometrijska identifikacija glasača na dijelu 19
Slika 5: Prikupljanje otiska prstiju na ulošku 30
Slika 6: Mastercardova biometrijska kartica 31
Slika 7:Proces rada SSO-a 35

Graf 1: Usporedba korištenja biometrije na raznim korisničkim domenama 3
Graf 2: Učestalost korištenja biometrijske tehnologije 4
Graf 3: Nove tehnologije primijenjene u svrhe borbe protiv prijevara u tvrtkama širom svijeta od 2019 18
Graf 4: Udio isporuka pametnih telefona sa senzorom otiska prsta širom svijeta od 2014. do 2018. godine 21
Graf 5: Udio tehnologije prepoznavanja otiska prsta na pametnom telefonu 2018. - 2022 22
Graf 6: Prihvaćanje biometrijske tehnologije u primjeni javne sigurnosti 24