

# Tehnologija za prepoznavanje lica

Seminarski rad u okviru kursa  
Računarstvo i društvo  
Matematički fakultet

Đorđe Mutavdžić

mi17096@alas.matf.bg.ac.rs

12. septembar 2022.

## Sažetak

Ovaj rad se bavi tehnologijom za prepoznavanje lica. Obraduje osnovne koncepte biometrije, uvodi čitaoca u tehnologiju kroz terminologiju i izazove sa kojima se susretalo i sa kojima se susreće prepoznavanje lica. Takođe govori o širokim primenama ove tehnologije i zanimljivim statistikama i činjenicama.

## Sadržaj

<b>1</b>	<b>Uvod</b>	<b>2</b>
1.1	Istorija . . . . .	2
1.1.1	Forenzički umetnici . . . . .	2
1.1.2	Razvoj tehnologije . . . . .	2
1.2	Uloga tehnogolije . . . . .	2
<b>2</b>	<b>Biometrija</b>	<b>2</b>
2.1	Osnovne osobine biometrije . . . . .	2
2.2	Identifikacija i verifikacija . . . . .	4
2.2.1	Četiri koraka identifikacije/verifikacije . . . . .	4
<b>3</b>	<b>Prepoznavanje lica</b>	<b>5</b>
3.1	Prednosti u odnosu na druge biometrijske osobine . . . . .	5
3.2	Crte lica . . . . .	5
3.3	Dizajn sistema za prepoznavanje lica . . . . .	6
3.4	Poređenje lica . . . . .	7
3.4.1	Tehnike zasnovane na modelu . . . . .	7
3.5	Najčešće primene . . . . .	9
3.5.1	Kontrola pristupa . . . . .	9
3.5.2	Obezbeđenje privatnih objekata . . . . .	9
3.5.3	Granični prelazi . . . . .	9
3.5.4	Bankovni sistemi i bankomati . . . . .	9
3.6	Statistika i zanimljive činjenice . . . . .	9
<b>4</b>	<b>Zaključak</b>	<b>10</b>

# 1 Uvod

## 1.1 Istorija

### 1.1.1 Forenzički umetnici

Jedan od prvih oblika identifikacije pre računara su bili identifikovanje kriminalaca ili nestalih osoba. Najveću ulogu u ovom procesu imali su forenzički umetnici i očevici. Glavni posao umetnika je bilo pažljivo slušanje očevica koji je opisivao glavne karakteristike lica osobe. Nakon toga crtež bi bio stavljen na flajere i predat policiji, televiziji, medijima, u nadi da će pomoći u potrazi. Jedna od najvećih mana ovog pristupa je zapravo količina potrebne edukacije svakog umetnika. Ona se sačinjavala od:

- 120 sati edukacije (80 sati kompozitnog crtanja i 40 sati povezanih kurseva).
- Minimalno 5 godina rada sa nekom agencijom za sprovođenje zakona.
- Pet uspešnih crteža (pogodaka), uključujući i zapisane detalje slučajeva i kako su crteži napravljeni.
- Tri pisma preporuke.

### 1.1.2 Razvoj tehnologije

Uspešnost prethodne discipline je bila odlična za to vreme, ali razvojem tehnologije ona je ubrzo zastarela. U 21. veku imamo računare koji su sposobni da veoma brzo i efikasno prepoznaju individualce, čak iako je broj takvih osoba ogroman upravo zbog intenzivnog razvoja procesorske moći. Nije ni čudo što interesovanje za biometrijskim tehnologijama rapidno raste u poslednjih 10 godina.

## 1.2 Uloga tehnologije

U dobu u kome se sad nalazimo, društvo je dovelo do napretka načina na koji vršimo transakcije. Svakodnevne aktivnosti dovele su da se sve više umesto olovke i papira, ili lica u lice, većina stvari izvršava digitalno. Porast u izvršavanju elektronskih transakcija dovelo je do veće potražnje u domenu preciznog izvršavanja identifikacije korisnika, samim tim i autorizacije. Ovaj rad približava čitaocima kako su se razvijali i trenutno koriste sistemi za automatsko prepoznavanje osoba. Naročito se obazire na biometriju (otisak prsta, dužica, mrežnjače i naravno lica) u kontekstu kako se i kako bi trebalo da se koriste da bi se osigurale bezbednost i privatnost svakog od nas.

# 2 Biometrija

## 2.1 Osnovne osobine biometrije

Biometrija predstavlja tehnologiju automatskog prepoznavanja ljudi, bazirana na tehnikama prepoznavanja šablona, koristeći psihološke ili karakteristike ponašanja osobe (*biometrički autentifikatori*). Neke od ljudskih osobina koje su trenutno iskorišćenje uključuju otiske prstiju, dužica, mrežnjača, lica, govor, potpis. Treba imati na umu da je glavna karakteristika ovih osobina zapravo činjenica da one ne mogu biti pomešane, duplirane ili ukradene.

Ukoliko se još malo udubimo u biometrike, prvo pitanje koje nam se postavlja je "Koji je autentifikator najbolji za rešavanje nekog specifičnog problema biometrijskog prepoznavanja?"[1]. Da bi odgovorili na ovo pitanje, moramo uvesti neke od osobina biometrija:

- **Univerzalnost:** svaka osoba bi trebala da ima izabranu osobinu.

- **Razlučivost:** bilo koje dve osobe se moraju razlikovati po izabranoj osobini.
- **Imutabilnost:** osobina mora ostati ista tokom dužeg vremenskog perioda.
- **Pribavljivost:** osobina mora biti pribavljiva i kvantitativno merljiva.
- **Performanse:** preciznost identifikacije i potrebno vreme za uspešno prepoznavanje moraju biti zadovoljavajući.
- **Prihvatljivost:** osobina se ne sme činiti napadna ili opasna kako bi ljudi bili voljni da je prihvate.

S obzirom da postoji mnogo biometrijskih sistema, to znači da ni jedan nije savršen. Svaki biometrijski modalitet ima svoje prednosti i mane s obzirom na prethodno navedene faktore, s toga ima smisla koristiti onaj koji najviše odgovara problemu. Koristeći pravi selekcion kriterijum zasnovan na različitim mogućnostima i performansama postojećih biometrijskih sistema, finalni identifikacioni sistem će biti u mogućnosti da dokaže sa razumnom tačnošću da mi jesmo ili nismo neko ko je ranije registrovan u korisničkoj bazi.

U skorijim godinama biometrijske tehnologije sve više dobijaju na popularnosti u širokom spektru aplikacija, od vladinih programa (*National ID card*, *Visa*, *borba protiv terorizma...*), komercijalne aplikacije poput nadzora, sistemi bezbednosti i kontrole pristupa (elektronska trgovina, e-banking...), sve do personalnih aplikacija poput kontrole logičkog i fizičkog pristupa (pristup računaru, internetu, paljenje automobila bez ključa...). Iako je dostupan veliki broj efektivnih rešenja, i dalje postoje brojni problemi u poboljšavanju preciznosti, efikasnosti i lakoće korišćenja biometrijskih sistema.

## 2.2 Identifikacija i verifikacija

Prepoznavanje obuhvata dve standardne metode poklapanja tek zabeleženih biometrija:

- *Identifikacija* je proces određivanja **ko je osoba**. Uključuje uzimanje izmerene karakteristike i pokušavanja pronalaska odgovarajućeg para u bazi podataka koja sadrži zapise ljudi i te karakteristike. Opštije, sistem će vratiti listu osoba koje su najslbličnije. Ovaj metod može zahtevati ogromnu količinu moći procesiranja i vremena ukoliko je baza velika. Većina ovog procesa se primenjuje za forenziku, sprovođenje zakona i obaveštajne službe.
- *Identifikacija (Autorizacija)* je proces određivanja **da li je osoba ona za koju tvrdi da jeste**. Algoritam ili potvrđuje ili odbija zahtev za pristup. Proces uključuje uzimanje izmerene karakteristike i njeno upoređivanje sa prethodno zabeleženim podacima za tu osobu. Očigledno je da ova metoda zahteva puno manje moći procesiranja i vremena od prethodne, zato što zahteva *1 na 1* upoređivanja (dok identifikacija zahteva *1 na N*, gde je N broj korisnika u bazi). Opšti autentifikatori uključuju šifre, privatne ključeve, magnetne kartice ili PIN-ove.

### 2.2.1 Četiri koraka identifikacije/verifikacije

Osnovni proces biometrijskog prepoznavanja ne zavisi od biometrijskog problema koji treba da zadovolji, niti od osobine koja je izabrana. Stoga svaki sistem se sastoji od istih koraka.

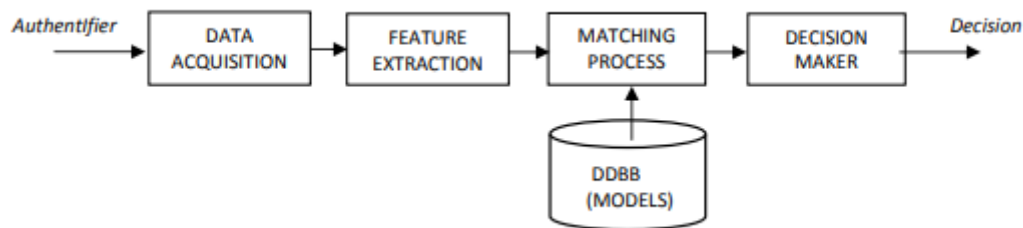


Figura 1: Generalna šema generičkog biometrijskog sistema za prepoznavanje.

1. **Uzimanje uzorka:** Pravi se uzorak uz pomoć sistema sticanja posebne namene. Ova faza je najosetljivija zbog činjenice da većina algoritama za prepoznavanje zavise od kvaliteta karakteristika uzoraka. Stoga, ako je moguće, kvalitet će se proveravati. Ako je uzorak lošeg kvaliteta, proces će se ponoviti. Takođe je bitno zabeležiti i dovoljan broj uzoraka kako bi se ostvarila visoka robusnost sistema.
2. **Ekstrakcija:** Izvlače se jedinstveni podaci koji mogu da se pronađu u uzorku i pravi se šablon.
3. **Poređenje:** Izmereni parametri iz prethodnog koraka se koriste za izgradnju modela zadatog korisnika. U slučaju identifikacije, novonastali model se upoređuje sa svim šablonima iz baze podataka, dok se prilikom verifikacije upoređuje samo sa jednim.
4. **Odluka:** Sistem odlučuje da li je skup osobina prikupljenih iz uzorka pogodak ili promašaj.

### 3 Prepoznavanje lica

Prepoznavanje lica je jedan od metoda biometrijske identifikacije koji najviše obećavaju zato što je to najprirodniji način za prepoznavanje identiteta među ljudskim bićima. Ljudska lica predstavljaju jedan od najčešćih vizuelnih šablona u našoj okolini. Stoga, uobičajeno je za ljude da identifikuju nekoga po njegovom licu, dok bi bilo nemoguće za njih da to urade po otisku prsta, dužici, mrežnjači, čak i po ličnoj karti zbog postojanja velikog broja jezika, čak sa različitim karakteristikama, širom sveta (Figura 2).

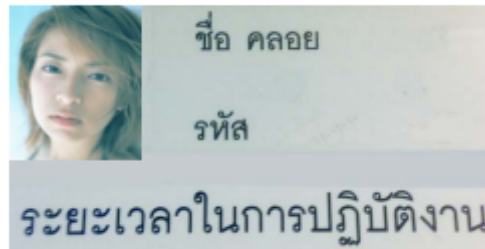


Figura 2: Lična karta neke osobe. Možemo primetiti da bi zapadnjaci mogli da identifikuju osobu na osnovu slike, ali ne i teksta.

#### 3.1 Prednosti u odnosu na druge biometrijske osobine

Jedna od najvećih prednosti je visoka društvena prihvaćenost korisnika jer ne sadrži kriminalne predrasude povezane sa drugim biometrijskim osobinama, poput otiska prstiju. Iako je ova tehnologija uglavnom adaptirana za aplikacije sa kooperativnim korisnicima, interakcija sa korisnicima nije uvek obavezna. Ovaj poslednji aspekt is veoma značajan za primenu u aplikacijama za nadzor na mestima poput aerodroma, železničkim stanicama, visoko obezbeđenim prostorima... Takođe pored identiteta lica prenosi i emocije osobe, kao i biološke informacije (pol, etničku pripadnost, starost...).

#### 3.2 Crte lica

Lice se sastoji od čela, obrva, očiju, nosa, usta, obraza i brade. Antropometrijska istraživanja su pokušala da okarakterišu dimenzije lica bazirane na skupu anatomske značajnih tačaka. Antropometrijske veličine se koriste za istraživanje rasta šablona kod ljudi kao i razumevanje kako se karakteristike lica odnose na pol i etničku pripadnost. Forenzičari su koristili ove tačke kako bi identifikovali lica sa slika. Međutim ove veličine se ne koriste previše u sistemima za automatsko prepoznavanje lica zbog njihovih nedostataka posebnosti. Štaviše, izvlačenje ovi tačaka sa slika lošeg kvaliteta može biti izazovno.

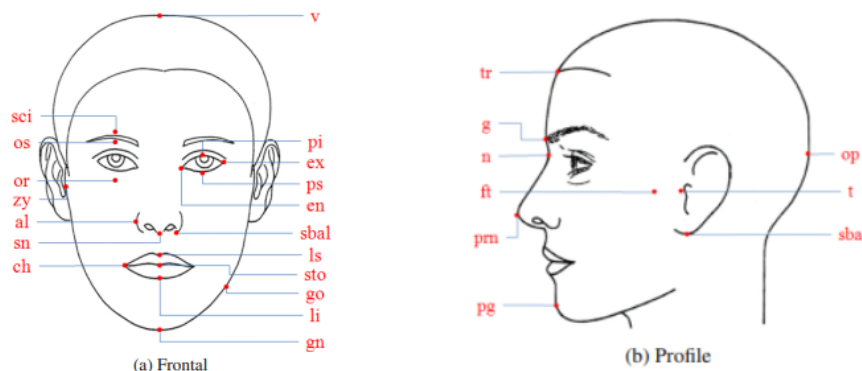


Figura 3: Skup anatomske značajnih tačaka

Karakteristike lica se mogu organizovati u tri nivoa:

- **Prvi nivo detalja** se sastoji od grubih karakteristika lica koje su lako uočljive. U njih spadaju npr. geometrija lica i boja kože. Na osnovu njih lako možemo praviti razliku između
  - Kratkih, okruglih i dugih, tankih lica
  - Muških i ženskih lica
  - Lica ljudi različitih etničkih pripadnosti

Ove karakteristike se mogu izvući čak i iz slika niskih rezolucija.

- **Drugi nivo detalja** se sastoji od lokalizovanih informacija o licu poput strukture komponenti lica, odnosa između komponenti i preciznog oblika lica. Ove karakteristike su veoma bitne za precizno prepoznavanje lica i one zahtevaju veću rezoluciju slike.
- **Treći nivo detalja** se sastoji od nestruktuiranih, sitnih detalja lica, koji uključuju ožiljke, pege, promena boje kože i mladeža. Ovaj nivo detalja je veoma koristan pri rešavanju veoma problematičnog problema *identičnih blizanaca*.

### 3.3 Dizajn sistema za prepoznavanje lica

Tipičan sistem za prepoznavanje lica se sastoji iz tri dela:

- Dobijanje slike
- Detekcija lica
- Poređenje lica

Slika lica koja se dobija od senzora može biti kategorisana po spektralnom opsegu (vidljiv golim okom, infracrveno zračenje, toplotni) korišćenom za slikanje i prirodi tehnike renderovanja slike (2D, 3D i video). Pošto je većina sistema za prepoznavanje lica koriste 2D slike koje su uslikane korišćenjem spektralnog opsega koji je vidljiv golim okom, u nastavku ćemo se fokusirati na procesiranje slika ovog tipa. *Detekcija lica* se odnosi na proces određivanja pozicije lica na slici. Ovaj korak može biti veoma težak u slučaju kada se na slici lice pomeša sa gustom pozadinom. Zbog karakterističnih osobina šablona očiju većina komercijalnih sistema za prepoznavanje lica prvo detektuju oči pa tek posle ostatak lica. Detekcija lica na 3D slikama se smatra jednostavnijem u odnosu na 2D zbog dostupnosti informacija o dubini.

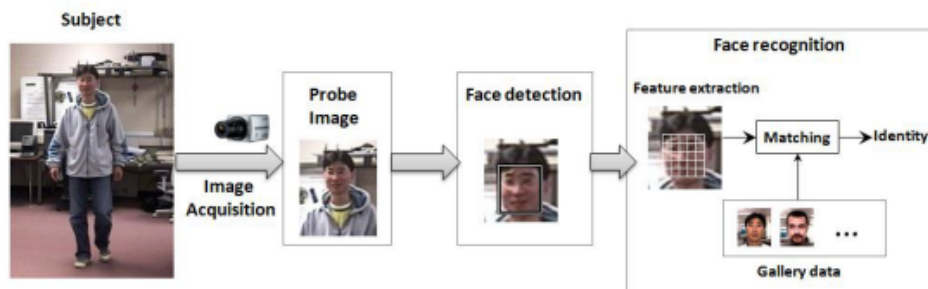


Figura 4: Šema procesa prepoznavanja lica

### 3.4 Poređenje lica

Postoje tri glavna pristupa za poređenje detektovanih lica sa slika:

- **Tehnike zasnovane na izgledu** generišu kompaktnu reprezentaciju cele regije lica u dobijenoj slici mapirajući visokodimenzionalnu sliku lica u niskodimenzionalni podprostor. Ovaj podprostor je definisan skupom reprezentativnih baznih vektora, koji su naučeni tokom treninga nad skupom slika.
- **Tehnike zasnovane na modelu** grade 2D ili 3D modele lica koji omogućavaju poklapanje lica sa slika u različitim položajima.
- **Tehnike zasnovane na teksturama** pokušavaju da nađu snažne lokalne karakteristike koje se ne menjaju u zavisnosti od položaja ili osvetljenja.

#### 3.4.1 Tehnike zasnovane na modelu

Ove tehnike pokušavaju da izvedu reprezentaciju slika lica koja ne zavisi od položaja što bi omogućilo poređenje lica u različitim položajima. Ove šeme obično zahtevaju detekciju par pouzdanih tačaka na licu (ćoškovi očiju, vrh nosa, ćoškovi usana, brada) što dovodi do povećanja kompleksnosti ovih algoritama. Neke od ovih tehnika se mogu koristiti i za generisanje realističnih animacija lica.

Šema **elastičnog poklapanja grafa grupa** predstavlja lice kao graf čiji su čvorovi pouzdane ili karakteristične tačke lica. Dok je svaki čvor grafa obeležen sa skupom Gaborovih koeficijenata koji karakterišu informacije lokalnih tekstura oko tačaka, svaka grana grafa je obeležena na osnovu rastojanja između odgovarajućih pouzdanih tačaka. Gaborov koeficijent neke tačke na slici se može dobiti uvijanjem slike uz pomoć kompleksnog 2D Gaborovog filtera centriranog na toj tački. Varijiranjem orijentacije i frekvencije Gaborovog filtera može se dobiti skup koeficijenata. Korišćenjem pouzdanih tačaka lica omogućeno je pravljenje parcijalnih grafova čak i kada je lice iskrivljeno.

Graf grupa lica (GGL) može biti konstruisan u dve faze od trening skupa slika lica u specifičnim položajima. U prvoj fazi dizajner mora ručno da izabere pouzdane tačke i definiše geometrijsku strukturu grafa slike za jednu ili više početnih slika. Grafovi slika ostalih fotografija iz trening skupa mogu se dobiti poluautomatski, poređenjem novih slika sa modelom grafova (slike koje su već obeležene) na osnovu Gaborovih koeficijenata. Tokom ovog procesa ručna intervencija je obavezna samo ako se pouzdane tačke pogrešno odrede.

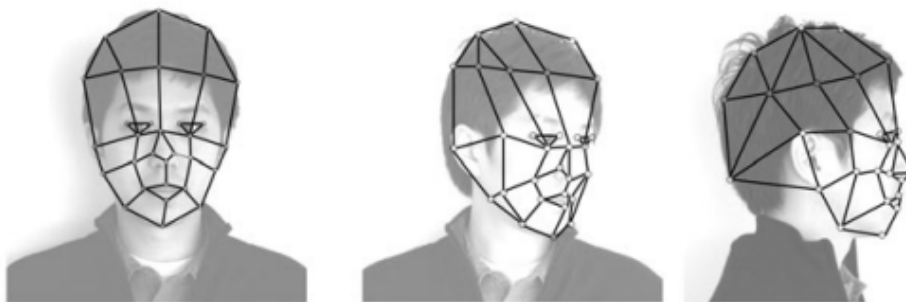


Figura 5: *Određivanje grafova slike za lice u različitim položajima. Čvorovi su pozicionirani automatski na osnovu poređenja Gaborovih koeficijenata date slike sa onim iz početnog grafa modelovanog od strane dizajnera.*

U drugoj fazi GGL se dobija kombinovanjem reprezentativnog skupa individualnih grafova slika u strukturu nalik steku. Tako je svaki čvor u grafu lica obeležen skupom Gaborovih koeficijenata koji predstavljaju lokalnu varijaciju u odgovarajućoj pouzdanoj tački. Skup Gaborovih koeficijenata koji odgovaraju istoj pouzdanoj tački se nazivaju *grupa*. Na primer, grupa oka može da sadrži koeficijente otvorenog, zatvorenog, muškog, ženskog... Grane su obeležene na osnovu prosečnog rastojanja između odgovarajućih čvorova u trening skupu. Kada imamo graf lica, pouzdane tačke za nove slike lica se mogu naći maksimizovanjem sličnosti između grafa koji odgovara datoj slici i grafa identičnog položaja. Ovaj proces se naziva *Elastično poklapanje grafa grupa* i sastoji se od sledeća tri koraka:

- Pronalaženje približne pozicije lica grubim skeniranjem slike sa zgusnutim GGL-om. Ovo se postiže određivanjem Gaborovih koeficijenata u određenim tačkama slike i njihovim upoređivanjem sa koeficijentima u zgusnutom GGL-u uzimajući u obzir geometrijsku strukturu GGL-a.
- Prečistiti poziciju i veličinu lica ponovnim pretraživanjem slike sa potpunim GGL-om, čija veličina i odnos širine i dužine sistemski variraju. Pri poređenju sličnosti između Gaborovih koeficijenata date slike i koeficijenata GGL-a, samo su razmatrani oni koeficijenti koji se najviše poklapaju.
- Precizno određivanje pouzdanih tačaka pomeranjem svih čvorova lokalno i relativno u odnosu na druge u cilju optimizovanja sličnosti grafa u daljem procesu.

Rezultat ovog algoritma je slika grafa koji najbolje predstavlja datu sliku.

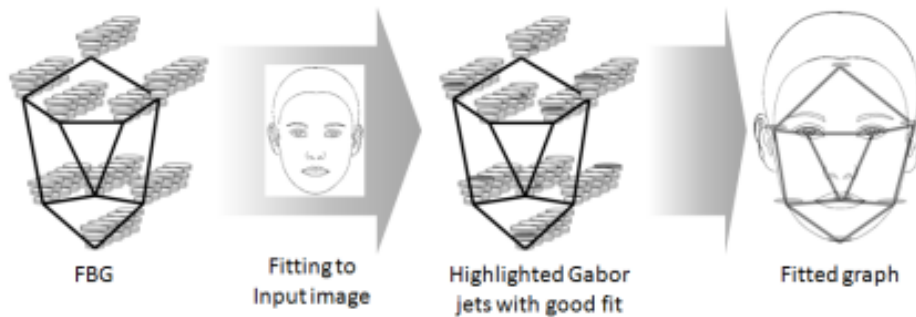


Figura 6: *Graf grupa lica*



### 3.5 Najčešće primene

#### 3.5.1 Kontrola pristupa

S obzirom da većina uređaja danas ima ugrađenu kameru korišćenje tehnologija za prepoznavanje lica je pristupačnija i zbog svoje lakoće korišćenja u odnosu na šifre predstavlja očigledan izbor. Najpoznatiji sistem za kontrolu pristupa je "Face ID" od kompanije Apple.

#### 3.5.2 Obezbeđenje privatnih objekata

Činjenica da računari danas mogu precizno da prepoznaju individualce predstavlja mnoštvo mogućnosti za sigurnosti sektor zbog mogućnosti identifikacije neovlašćenih pristupa lokacijama. Poznato je da IP kamere danas mogu biti opremljene sa softverom za prepoznavanje lica. Uz pomoć belih i crnih lista za specifične lokacije može se implementirati detekcija opasnosti i upada.

#### 3.5.3 Granični prelazi

Na graničnim prelazima sve više i više se koriste ovi sistemi za automatsko dozvoljavanje prolaza. Kontrola je povezana sa bazama podataka poput *Intepolove "Facial Identification" metode*, kako bi identifikovala potencijalno opasne individualce.

#### 3.5.4 Bankovni sistemi i bankomati

U većini banaka, njihovi korisnici mogu da omoguće prepoznavanje lica kao dodatni bezbednosni faktor za pristup njihovim nalogima ili pri izvršavanju transakcija.

### 3.6 Statistika i zanimljive činjenice

- 1. Sistem za prepoznavanje lica može postići i do 99.97% preciznosti. [3]**  
Međutim, ovo je moguće postići samo u idealnim okolnostima (osvetljenje je dobro i konstantno, osoba gleda direktno u kameru i nalazi se blizu nje...). Iz ovog razloga stopa preciznosti je obično oko 90%. Jedan od glavnih razloga ove razlike od blizu 10% je što osoba ne gleda direktno u kameru.
- 2. Šansa da neko drugi otključa vaš telefon preko Face ID je jedan u milion. [4]**  
Kada su telefoni u pitanju, statistike pokazuju da je prepoznavanje lica 20 puta sigurnije od identifikacija zasnovanih na otisku prsta.
- 3. 72% hotela će verovatno investirati u tehnologije za prepoznavanje lica do 2025. [5]**  
Verovatno nije prva industrija koja bi pala na pamet, ali nije retko da hoteli koriste tehnologije za prepoznavanje lica. Na primer, u Kini možete da se prijavite na recepciji pomoću računara koji vam skenira lice. Takođe prepoznavanje lica zamenjuje ključeve, plaćanje bez kontakta i nadzor gostiju.
- 4. Market prepoznavanja lica je proizveo 3.8 milijardi dolara samo u 2020. [6]**  
Sa sektorima za odbranu, bezbednost i sličnim organizacijama koje investiraju sve više i više, ovo i nije toliko iznenađujuće. Štaviše, eksperti očekuju da će market dostići i do 8.5 milijardi dolara do 2025, što znači da će se duplirati u odnosu na trenutnu vrednost.
- 5. U Kini možete "platiti osmehom" u KFC-u. [7]**  
Mnogi od nas su se već navikli na život bez gotovine plaćajući karticama ili čak telefonima. Ipak *Alibaba* se čini dva koraka ispred. Njihova najnovija tehnologija omogućava da 3D kamera skenira lice kupca i automatski skine svotu sa njihovog Alipay novčanika.
- 6. U Americi, tehnologija za prepoznavanje lica ima stopu odobrenja od 83%. [8]**  
Držanje opasnih ljudi van prostora škola i pronalaženje nestalih osoba su neke od glavnih

argumenata osoba koje podržavaju ovu tehnologiju. Aerodromi u Americi već uveliko koriste sisteme za prepoznavanje lica.

#### **7. Belgija i Luksemburg su zabranili korišćenje. [9]**

Ovo su jedine dve države koje su zabranile korišćenje, iako su Belgijske kriminalističke službe koristile prepoznavanje lica - ilegalno. U septembru 2021, policija je poricala optužbe, ali mesec dana kasnije ministar unutrašnjih poslova je priznao da je tehnologija korišćena 100 do 500 puta.

## **4 Zaključak**

Tehnologija prepoznavanja lica konačno dostiže zavidan napredak i brz rast u praktičnim primenama. Velika količina istraživačkog truda svuda oko sveta biva primenjena na poboljšanje preciznosti i proširenje mogućnosti u ovom biometrijskom domenu. Iako već postoji ogroman broj primena, iz dana u dan zbog novih okolnosti ljudi nalaze još više primena. U bliskoj budućnosti možemo očekivati još veći broj uređaja koji koriste ovaj vid sigurnosnih protokola.

## Literatura

- [1] Introduction to biometrics Anil K. Jain, Arun A. Ross, Karthik Nandakumar
- [2] Face Recognition by means of advanced contributions in machine learning, Ph.D. thesis, Virginia Espinosa Duro
- [3] Center For Strategic & International Studies: How Accurate are Facial Recognition Systems – and Why Does It Matter?
- [4] 9TO5Mac - In-screen Touch ID potentially signals a backward step ahead
- [5] Forbes - Improving User Experiences In The Hospitality Industry
- [6] Comparitech - Facial recognition report highlights growing, variable global market
- [7] TechCrunch - Šmile to pay”
- [8] NetChoice - Americans Want Facial Recognition Use By Law Enforcement Improved, But Not Banned
- [9] The Brussels Times