



# Veštačka Inteligencija

## Biometrijski sistemi za kontrolu ulaska (Biometrics)

Profesor:

Prof. Dr Leonid Stoimenov

Studenti:

Aleksandra Đokić 17080

Natalija Pavlović 17321

Mateja Pančić 17326

# Sadržaj

1. Uvod.....	4
2. Istorija razvoja biometrije .....	6
3. Autentifikacija.....	6
4. Metodi autentifikacije .....	7
5. Digitalizacija kao osnova biometrije.....	8
6. Vrste biometrijskih identifikacija.....	9
7. Fizička biometrija .....	9
7.1. Čitanje DNK zapisa .....	10
7.2. Otisak prsta .....	11
7.3. Skeniranje oka.....	12
7.4. Face Recognition (proces prepoznavanja lica) .....	13
7.4.1. Psihologija prepoznavanja lica.....	14
7.4.2. Crte lica.....	14
7.4.3. Dizajn sistema za prepoznavanje lica .....	15
7.4.3.1. 2D Senzori .....	16
7.4.3.2. 3D Senzori .....	17
7.4.3.3. Ekstrakcija i usklađivanje karakteristika.....	18
7.4.4. Prepoznavanje lica na osnovu izgleda .....	18
7.4.4.1. Analiza glavnih komponenti .....	19
7.4.4.2. Linearna diskriminativna analiza .....	19
7.4.5. Prepoznavanje lica na osnovu modela .....	20
7.4.5.1. Podudaranje grafika elastične grupe .....	21
7.4.6. Prepoznavanje lica zasnovano na teksturi.....	22
7.4.6.1. Skalarna invarijantna transformacija obeležja .....	22
7.4.6.2. Lokalni binarni obrazac .....	23
8. Biometrija ponašanja.....	24
8.1. Prepoznavanje glasa.....	25
8.2. Prepoznavanje rukopisa ili potpisa.....	25
8.3. Prepoznavanje kucanja na tastaturi .....	26
8.4. Prepoznavanje mirisa .....	27

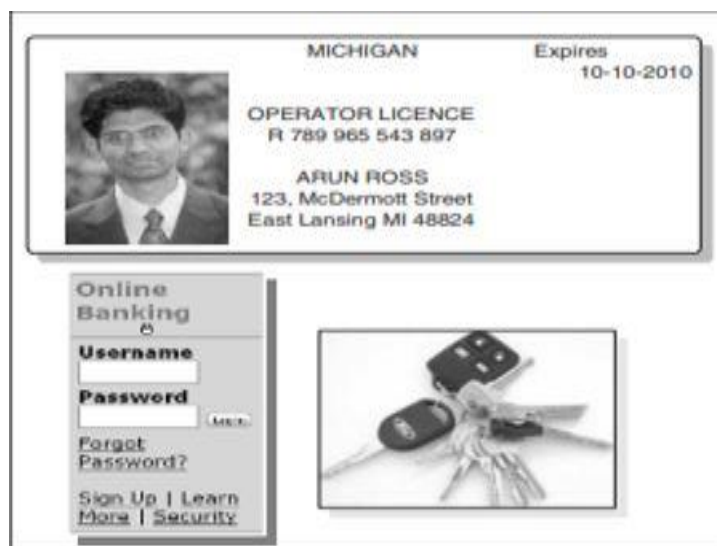
9. Poređenje biometrijskih tehnika.....	27
10. Zaključak.....	29
11. Literatura.....	30

# 1. Uvod

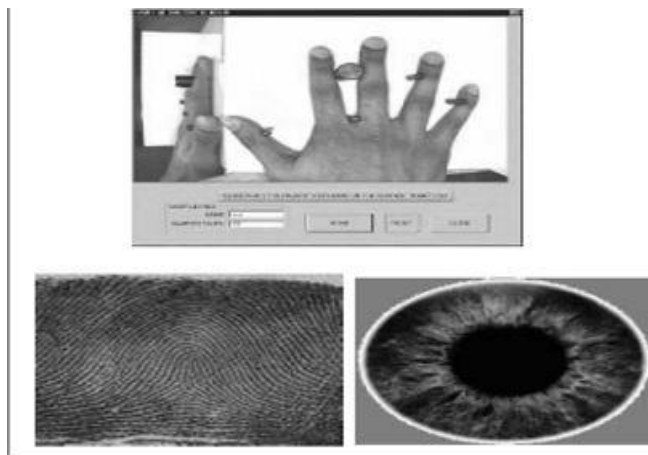
Biometrija je nauka koja se bavi prepoznavanjem identiteta osobe. Bazira se na fizičkim (otisak prsta, otisak dlana, DNK, prepoznavanje lica...), hemijskim ili oponašajućim (glas, pokret, stav...) karakteristikama osobe. Nudi pouzdano rešenje za mnoge aspekte prepoznavanja (pristup poverljivim informacijama, finansijski sistemi, mobilni telefoni...) koristeći automatske ili polu-automatske šeme za prepoznavanje osoba na osnovu njihovih bioloških karakteristika.

Pojam biometrija može imati različito značenje, zavisno od konteksta u kom se koristi. Sama reč potiče od grčkih reči **bios-** život i **metron-** meriti i označava granu biologije kojoj je cilj da matematički izračuna i odredi razne životne pojave, naročito pojave nasleđa.

Pojam identifikacija potiče od latinske reči **identificare-** ustanovljenje identičnosti, istovetnosti, a u savremenom društvu označava povezanost određenog podatka po ličnosti sa njom samom. Biometrijska identifikacija se temelji na uvažavanju čovekovih individualnih fizičkih osobina ili elemenata ponašanja, njihovom evidentiranju i arhiviranju, kao i njihovim poređenjem u procesu identifikacije sa osobinama osobe čiji se identitet utvrđuje ili potvrđuje.



Tradicionalni način prepoznavanja

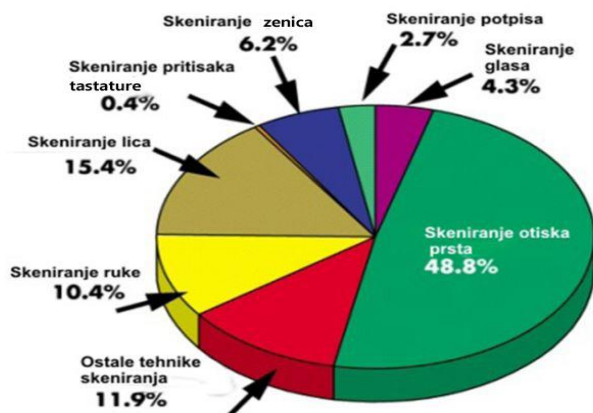


### Biometrijsko prepoznavanje

Imajući u vidu da su pojedine čovekove karakteristike ne menjaju u toku čitavog njegovog života, a isto tako da su njihove vrednosti karakteristične za tačno određenog čoveka (verovatnoća da se pronađu dve osobe sa istim otiskom prsta je gotovo isključena), biometrijske metode se uspešno mogu primenjivati pri identifikaciji osoba sa vrlo niskim nivoom greške. Suština biometrije se temelji na činjenici da ona proučava karakteristike koje su trajne, individualne i merljive, odnosno uporedive.

Biometrijski uređaji se sastoje iz:

- skenera, senzora ili kamere za usnimavanje individualnih karakteristika
- softversko-hardverskog dela koji učitane informacije pretvara u digitalnu, matematičkom jeziku razumljivu formu
- baze podataka individualnih karakteristika
- softverskog dela za komparaciju učitanih karakteristika sa bazom podataka



Učestalost korišćenja biometrijske tehnologije

## 2. Istorija razvoja biometrije

Jedan od najstarijih i najosnovnijih primera karakteristika, koje se koriste za prepoznavanje od strane drugih ljudi, je lice. Od samih početaka civilizacije, ljudi koriste lice za prepoznavanje osoba. Koncept prepoznavanja ljudi od strane ljudi vidljiv je i u npr. prepoznavanju govora (govornika, onoga koji govori), kao i u ostalim primerima prepoznavanja karakteristika svakodnevnog ponašanja. Ostale karakteristike, korišćene za prepoznavanje tokom istorije civilizacije su mnogo formalnije. Neki od primera su: otisci šake na slikama u pećinama, za koje se smatra da ih je ostavio praistorijski čovek pre 31000 godina, otisci prstiju kojima su rani kineski trgovci potvrđivali poslovne transakcije, na isti način kao i trgovci u Vavilonu oko 500 godine pre nove ere itd. Najstariji slučajevi korišćenja biometrije zabeleženi su još u starom Egiptu gde su trgovci evidentirali karakteristike drugih trgovaca sa kojima su sarađivali.

Nakon terorističkih napada na SAD 11.septembra 2001.godine, biometrijske tehnologije doživljavaju pravu ekspanziju. Proučavanje otisaka prstiju (što se dešavalo širom sveta), antropometrija je gubila na značaju, pa je francuska policija već 1890.godine uvela sistem otisaka prstiju radi identifikacije osoba.

Nakon terorističkih napada na SAD 11.septembra 2001.godine, biometrijske tehnologije doživljavaju pravu ekspanziju i postaje jedna od najznačajnijih tehnika borbe protiv terorizma.

## 3. Autentifikacija

Situacija u svetu danas čini bezbednost sve važnijom stavkom u našim životima pa samim tim i svakodnevna autentifikacija ima daleko veći značaj danas nego u ranijem periodu. Važno je pomenuti da autentifikacija samo potvrđuje identitet i ništa dalje ne čini sa njime niti definiše njegova prava pristupa.

Postoje dva osnovna tipa autentifikacije:

- Verifikacija,
- Identifikacija;

## **Verifikacija**

Kod verifikacije vrši se potvrđivanje identiteta neke osobe u smislu poređenja dobijenog podatka sa tačno određenim uzorkom u bazi podataka. Ovaj oblik autentifikacije predstavlja 1:1 sistem.

## **Identifikacija**

U slučaju identifikacije, vrši se provera podudaranja dobijenog uzorka sa svim sačuvanim uzorcima u bazi podataka s ciljem dobijanja podatka o identitetu neke osobe. Ovaj sistem predstavlja 1:N (1:više) sistem autentifikacije.

Oba tipa autentifikacije se koriste kod biometrijskih autentifikacionih sistema, a koji će biti upotrebljen zavisi konkretno od aplikacije. Pored ova dva osnovna tipa, postoji još i tzv. negativna identifikacija gde korisnik treba da potvrdi da njegov identitet ne odgovara traženom identitetu. U ovom slučaju, gde se takođe vrši 1:N pretraga, pozitivan odgovor o podudaranju se dobija samo u slučaju da se uneti podatak u najvećoj mogućoj meri poklapa sa sačuvanim šablonom, u suprotnom se prihvata tvrdnja korisnika da nije ta osoba koja se traži. Sistem se često koristi na aerodromima gde se putnici proveravaju da li su eventualno na „crnim listama“.

# **4. Metodi autentifikacije**

Danas postoje tri metoda autentifikovanja sebe drugoj osobi ili sistemu.

- Bazirana na znanju („šta znaš“)
- Bazirana na objektu („šta imaš“)
- Bazirana na biometriji („šta si“)

## **Bazirana na znanju**

Metoda se zasniva na tome da korisnik pamti neki podatak. Najčešće je to lozinka ili PIN kod. Veliki sigurnosni problem je u tome što korisnici radi lakšeg pamćenja zadaju predvidljive lozinke i one koje je lako pogoditi ili ih zapisuju na papir.

## **Bazirana na objektu**

Metoda se zasniva na posedovanju nečega što će potvrditi identitet osobe. To su najčešće ID kartice, pasoši, platne kartice...Dobra osobina je ta što korisnik nema potrebe da pamti bilo kakve informacije ali isto tako identifikacioni objekat se može izgubiti ili ukrasti, a samim tim

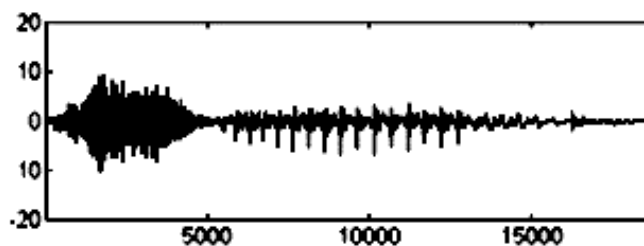
i falsifikovati. Jedina prednost u ovome je što korisnik odmah vidi da više ne poseduje objekat pa može brzo reagovati kako bi sprečio eventualne posledice.

### **Bazirana na biometriji**

Metoda se zasniva na tome da korisnik poseduje određeni biometrijski identifikator (otisak prsta, crte lica...) koji toj osobi pripada samim rođenjem i koji se tokom života ne menja ili se menja veoma malo. Ovde ne postoji mogućnost gubljenja ili zaboravljanja identifikatora, a i mogućnost falsifikovanja je neuporedivo manja nego kod prethodno pomenute dve metode autentifikacije

## **5. Digitalizacija kao osnova biometrije**

Najvažniji korak u procesu prepoznavanja uzoraka je digitalizacija. Naime, za potrebe računarske obrade podatke dobijene skeniranjem i sl. potrebno je prevesti u digitalni format s kojim računar može raditi. To je proces u kojem se analogni signal pretvara u digitalni te prepoznaje programskom opremom. Što je kvalitetnija oprema, to su veće šanse za prepoznavanje uzorka. Analogni signal se pretvara u digitalni korištenjem elektroničkog DAC (eng. digital audio-video converter) uređaja. Sam proces se u suštini sastoji od niza Furijeovih transformacija, kvantizacija i ostalih pojmova koji služe da matematički što približnije opišu ulazni signal. Nisu svi DAC-ovi jednaki i kvalitetni. DAC se nalazi u sklopovskom senzoru za prepoznavanje uzoraka pa što je senzor kvalitetniji (a time i skuplji), dobija se bolje prevedeni uzorak.



Izgled digitaliziranog uzorka



## 6. Vrste biometrijskih identifikacija

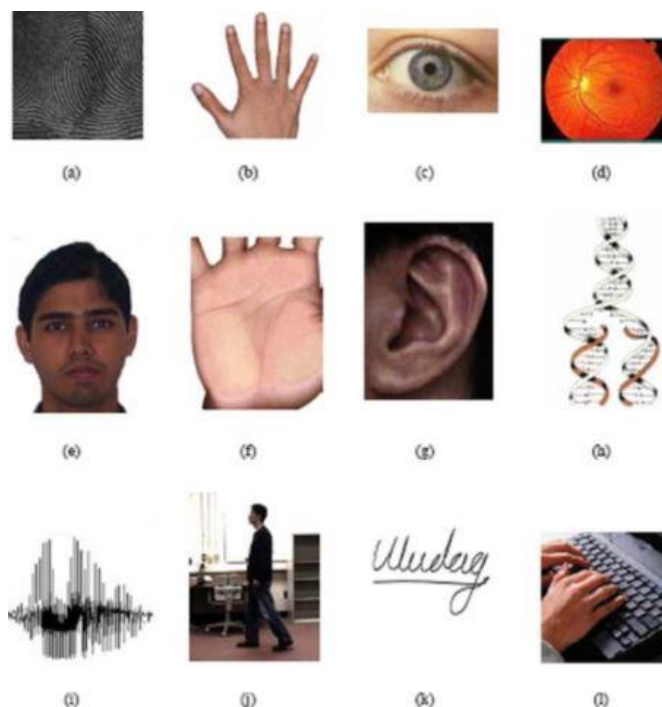
Biometrija se može definisati kao model identifikacije osobe, baziran na fizičkim karakteristikama ili karakteristikama ponašanja, a odnosi se na nešto što osoba poseduje ili ono što osoba zna kako bi izvršila identifikaciju, pa se na osnovu toga i biometrijske identifikacije mogu, uslovno rečeno, podeliti na dve osnovne grupe:

- Identifikacija na osnovu fizičkih karakteristika subjekta koje se mogu realizovati posmatranjem otisaka prstiju, fizionomije lica, geometrije dlana, irisa (dužice) oka, fundusa (retine) oka.
- Identifikacije na osnovu karakteristika ponašanja subjekta koje se mogu realizovati posmatranjem karakteristika glasa, potpisa, dinamike kucanja na tastaturi.

Na samom početku korišćenja biometrije, prednost je davana fizičkim karakteristikama u odnosu na ponašajne karakteristike. Prevladavalo je mišljenje da fizičke karakteristike, u odnosu na ponašajne, poseduju „uočljivost“. Prema tom mišljenju, prevladavalo je i uverenje kako su fizičke karakteristike pouzdanije od ponašajnih, jer one imaju tendenciju manjih razlika unutar grupa, nego li to imaju ponašajne karakteristike.

## 7. Fizička biometrija

Fizička biometrija je deo biometrije koji se bavi uzorkovanjem fizionomije ljudskog tela i njegovim jedinstvenim karakteristikama. Temelj fizičke biometrije je ljudska fizička jedinstvenost koja omogućuje raspoznavanje ljudi na osnovi iste i korišćenje pripadajućih opisa uzoraka za njihovo prepoznavanje. Prepoznati uzorci mogu se koristiti u kombinaciji sa ostalim klasičnim zapisima kojima se jedinstveno opisuju osobe.



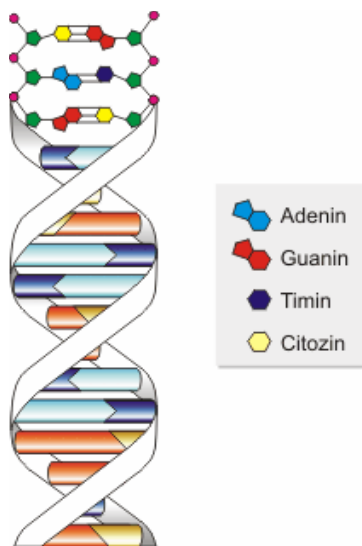
Najčešće korišćene biometrijske karakteristike. a) otisak prsta, b) geometrija dlana, c) dužica oka, d) rožnjača oka, e) crte lica, f) otisak šake, g) oblik uha, h) DNK, i) glas, j) hod, k) potpis, l) dinamika kucanja

## 7.1. Čitanje DNK zapisa

Britanski naučnik sir Alec Jeffreys prvi je 1984. godine primenio činjenicu o jedinstvenosti građe molekula DNK na identifikaciju nepoznatih počinitelja krivičnih dela, pa je metodu nazvao DNA-fingerprinting po uzoru na do tada neprikosnovenu metodu identifikacije. Analiza DNK je zasigurno jedna od najznačajnijih i najpouzdanijih biometrijskih metoda identifikacije. Koristi se u mnogim područjima istraživanja, a nama najzanimljivija primena je u području kriminalistike i sudske medicine gde se analiza DNK koristi za utvrđivanje identiteta nepoznate osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tela, određivanje pola osoba... Kod analize DNK koriste se unapred određeni lokusi, za koje je poznato da sadrže određene parove baza koji se uzastopno ponavljaju, a u isto vreme pokrivaju veliku varijabilnost u ljudskoj populaciji, odnosno koji sadrže VNTR.

VNTR ili varijabilni (polimorfni) ponavljajući nizovi (engl. Variable number tandem repeats) su visoko polimorfni nizovi i određeni su brojem ponavljajućih DNK sekvenci. Većina DNK nizova odnosno sekvenci ne sadrži gene, već služi isključivo kao pomoćni genetički materijal. Kratke

sekvence parova baza koji se učestalo ponavljaju, nazivaju se kratki ponavljajući nizovi ili STR (short tandem repeats). Iako se ove sekvence pojavljuju u DNK svake osobe, broj ponavljanja sekvenci jako se razlikuje od osobe do osobe. Upravo se na utvrđivanju broja i dužine ponavljanja tih sekvenci temelji identifikacija osoba metodama analize DNK.



Šematski izgled dnk molekula

## 7.2. Otisak prsta

Otisak prsta je najkorišćenija metoda identifikacije kod biometrijskih pametnih kartica. Svaka osoba ima jedinstven otisak prsta koji se sastoji od dolina i brazdi (udubljenja i ispupčenja) koji definišu različite šablone. Brazde mogu biti različitih oblika.

Autentifikacija putem otisaka prsta je veoma jednostavna. Prvo, korisnik se prijavi na sistem dajući svoj uzorak otiska. Senzor skenira prst. Dobijena slika se određenim algoritmima obradi i postavi u fajl na glavnom računar u ili lokalnom procesoru kod mobilnih uređaja. Sačuvani podatak predstavlja tzv. šablon korisnikovog otiska prsta. Pri verifikaciji otiska, podaci o otisku se upotrebom algoritma porede sa prethodno sačuvanim podatkom iz čega se kao odgovor dobija podudaranje ili ne podudaranje otisaka. Cela procedura se odvija brzinom od 1-2s.

Postoje dva osnovna pristupa prilikom analize otiska prsta. Prvi analizira samo ukrštanja i završetke zavijutaka otiska, dok drugi prati celokupan pravac svake linije. Otisak skeniran

prvom metodom zauzima oko 250 B, dok drugom metodom otisak zauzima oko 100 KB. Naravno, postoji i razlika u brzini prepoznavanja otiska jer se u prvoj metodi upoređuje nekoliko karakterističnih tačaka, dok se u drugoj metodi upoređivanje vrši u kompletnoj bazi podataka, što može da traje satima ili danima.

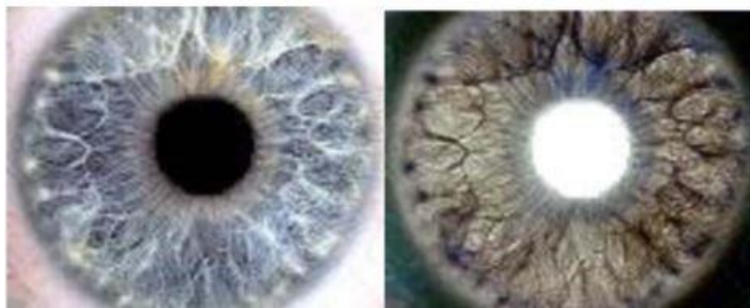
Različita je i tehnologija kojom se skenira otisak i ona se najčešće bazira na kapacitivnim, optičkim ili ultrazvučnim senzorima



Proces od originalne slike do šablona

### 7.3. Skeniranje oka

Skeniranje rožnjače je tehnologija koja se najviše koristi prilikom kontrole ulaska osoba u neki prostor, vođenju statistike posetioca, a slične varijante su i u upotrebi prilikom skeniranja korisničkih dokumenata. Rožnjača poseduje preko 200 detalja koji se mogu upotrebiti za poređenje i identifikaciju, kao što su prsteni, brazde i pegice. Te šare su jedinstvene za svakog pojedinca, čak se levo i desno oko iste osobe razlikuju. Zbog toga se ova metoda uspešno može koristiti i za identifikaciju, a ne samo za verifikaciju. Za snimanje dužice dovoljna je obična kamera. Vreme verifikacije je obično manje od 5 sekundi. Da bi se izbeglo korišćenje veštačkog oka, sistem može da osvetli oko i da vidi da li dolazi do skupljanja zenice odnosno, nakon izvršenog skeniranja, čitač uključuje vidljivu svetlost i varira njen intenzitet. To radi u cilju detekcije dilatacije zenice. Dilatacija zenice je prirodna osobina oka koja se ne može preneti na falsifikat. Ukoliko dilatacija postoji, čitač sa sigurnošću konstatuje da je reč o prirodnom oku.



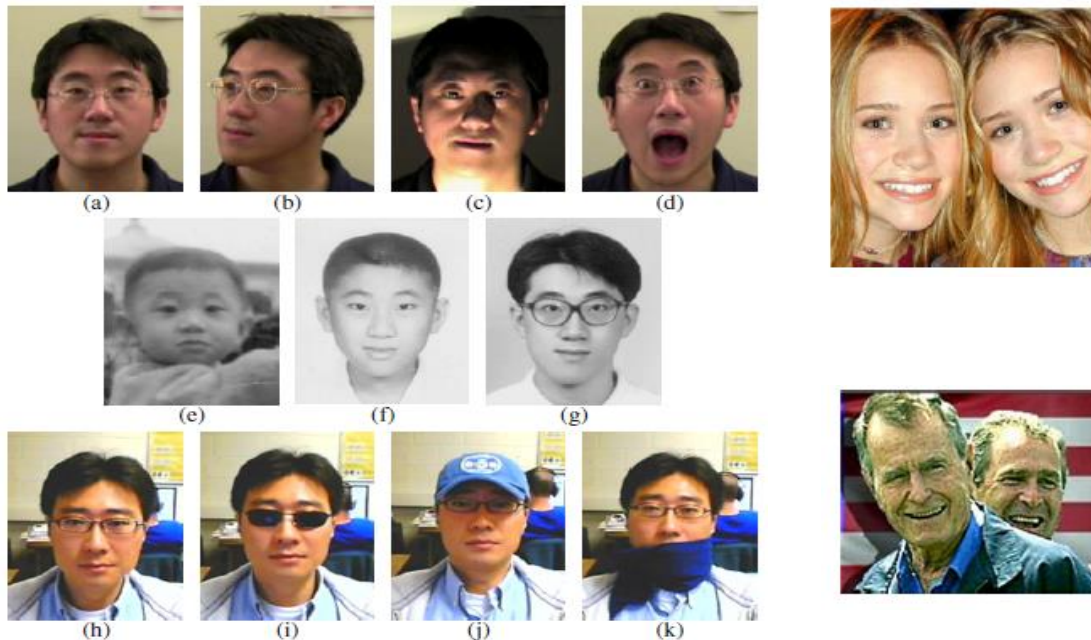
Rožnjača oka i njen negativ

## 7.4. Face Recognition (proces prepoznavanja lica)

Lice je prednji deo čovekove glave krećući se od čela sve do brade uključujući oči, usta, obraze, nos kao i ostale delove. Ono predstavlja deo koji najviše interaguje sa ostatkom sveta kao i deo čoveka koji se najviše koristi za sagledavanje i doživljavanje sveta oko sebe. Smatra se da je lice najviše korišćena biometrijska osobina koja se koristi od strane ljudi za prepoznavanje drugih, kao i autentifikaciju identiteta među ljudima. Samim tim praksa je da se slike ljudskih lica ugrađuju u različita dokumenta u cilju lakše i tačnije identifikacije ljudi.

Proces prepoznavanja lica može da se definiše kao proces uspostavljanja identiteta neke osobe na osnovu njegovih/njenih karakteristika lica. Najprostije rečeno predstavlja upoređivanje dve slike i određivanje da li obe slike pripadaju istoj osobi. Kod procesa javljaju se neki problemi kao što su moguća razlika u godinama, pozi, osvetljenju, izrazu lica kao i promene u izgledu u vidu promene kose, šminke, modnih dodataka, operacija itd. Iako se jave određene sličnosti u procesu prepoznavanja lica one mogu biti posledica rodbinskih veza što dodatno otežava posao. Obučavanje mašina da prepozna ista lica uzimajući u obzir sve navedene moguće promene kao i sličnosti u odnosu na druge ljude je veoma težak posao pogotovo zato što tačna kognitivni i neuronski procesi uključeni kod ljudi za prepoznavanje lica jos uvek nisu do kraja poznati.

Uprkos ovim nedostacima proces prepoznavanja lica ima i dobrih karakteristika kao što su mogućnost "hvatanja" lica sa velikih razdaljina što omogućava korišćenje u vidu nadzornih kamera. Isto tako lice dosta govori o raspoloženju kao i biografskim informacijama osobe. U odnosu na druge vrste biometrije ljudi su više voljni da podele svoje podatke u vidu slike što i pokazuje povećanje popularnosti društvenih mreža sa takvom funkcijom.



Promene u izgledu koje mogu uticati na proces prepoznavanja. Sličnosti u izgledu ljudi.

#### 7.4.1. Psihologija prepoznavanja lica

Osnovni mehanizam percepcije lica kod ljudi proučava se u cilju dizajniranja sistema za prepoznavanje, mašina koje mogu da oponašaju čoveka i njegovu sposobnost prepoznavanja i razumevanja lica. Veoma je teško direktno posmatrati funkcije mozga, zato se indirektna zapažanja obično koriste da bi razumeli mehanizam koji podržava prepoznavanje ljudskog lica. Na primer, na osnovu zapažanja da ljudi mogu da prepoznaju karikature i crte lica, zaključuje se da ljudi percipiraju lice na osnovu određenih karakteristike višeg nivoa. Studije koje koriste napredne tehnike snimanja mozga kao što su funkcionalna magnetna rezonanca (fMRI) očekuju da otkriju precizne mehanizme obrade lica u ljudskom mozgu.

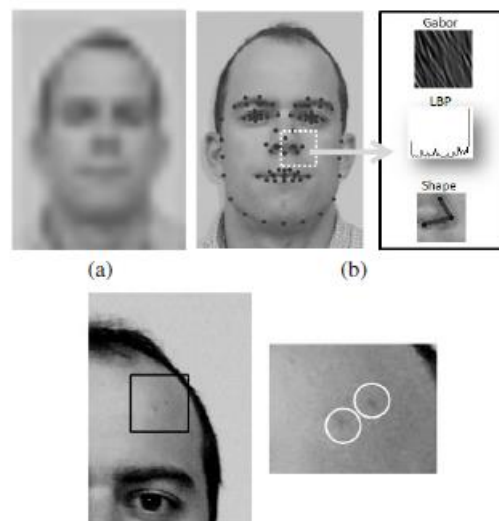
#### 7.4.2. Crte lica

Antropometrijske studije su pokušale da okarakterišu dimenzije lica na osnovu skupa anatomske značajnih obeležja ili pomoćnih tačaka. Antropometrijska merenja su korišćena za proučavanje

obrasca rasta kod ljudi kao i razumevanja karakteristika u odnosu na pol i etničku pripadnost. Međutim, ova merenja se ne koriste u velikoj meri u automatizovanim sistemima za prepoznavanje lica zbog njihovog uočenog nedostatka prepoznatljivosti.

Karakteristike lica se mogu organizovati u sledeća tri nivoa:

1. Detalji nivoa 1 sastoje se od grubih karakteristika lica koje je lako uočiti. Primeri uključuju opštu geometriju lica i globalnu boju kože. Takve karakteristike se mogu koristiti za brzo razlikovanje između kratkog okruglog lica i izduženog tankog lica, lica koja pokazuje pretežno muške ili ženske karakteristike ili lica različitih rasa.
2. Detalji nivoa 2 sastoje se od lokalizovanih informacija o licu kao što je struktura komponenta lica (npr. oči), odnos između komponenti lica, i precizan oblik lica. Karakteristike lokalnih regiona lica mogu se predstaviti pomoću geometrijskih ili teksturnih deskriptora.
3. Detalji nivoa 3 sastoje se od nestrukturiranih, mikro nivoa na licu, što uključuje ožiljke, pege, promene boje kože i mladeže.



Detalji nivoa 3

#### 7.4.3. Dizajn sistema za prepoznavanje lica

Tipičan sistem za prepoznavanje lica sastoji se od tri modula: akvizicija slike, detekciju lica i podudaranje lica. Slika lica dobijena od senzora može se kategorisati na osnovu spektralnog



opsega (npr. vidljivi, infracrveni i termalni) koji se koriste za snimanje slike i prirode tehnika sinteze slike (npr. 2D, 3D i video). Detekcija lica (poznat i kao lokalizacija lica ili segmentacija) se odnosi na proces kojim se određuje pozicija lica na slici i određuje se njegov prostorni obim. Ovaj zadatak može biti značajno izazovan kada se lice objekta nalazi u pretrpanoj pozadini ili kada je više slika lica u različitim razmerama dostupno u okviru iste slike. Zbog karakterističnih šara očiju, kod većine komercijalnih prepoznavanja lica sistemi prvo detektuju dva oka pre lokalizacije prostornog opsega lica. Smatra se da je detekcija lica u 3D slikama lakši problem u poređenju na 2D slike zbog dostupnosti informacija o dubini. U video strimovima detekcija lica se vrši detekcijom lica na svakoj slici u sekvenci slika videa. Automatsko prepoznavanje lica zahteva da podaci o licu budu u mašinski čitljivom formatu. Konvencionalne 2D fotografije, 3D slike i video snimci su to tri glavna tipa formata slika koji se koriste u sistemima za prepoznavanje lica.

#### 7.4.3.1. 2D Senzori

Obzirom da je lice trodimenzionalni objekat, 2D slike ne mogu lepo prikazati sve crte lica. Prednji deo lica sadrži više detalja u odnosu na lice koje se gleda s profila i prema tome očekuje se da da preciznije podudaranje prilikom prepoznavanja osobe. Konfiguracije sa više kamera koje hvataju slike lica iz više različitih uglova korišćene su za rešavanje problema sa varijacijama poza. Varijacije u osvetljenju i prostorna rezolucija u velikoj meri utiču na 2D sisteme za prepoznavanje lica. Da bi se to izbeglo, koriste se novi senzori visoke rezolucije, aktivne “pan-tilt-zoom” (PTZ) kamere, i infracrvene kamere.



Slike lica uslikane u vidljivom bliskom infracrvenom spektru na različitim talasnim dužinama.



Sistemi za prepoznavanje lica funkcionišu na kratkoj udaljenosti koja je ograničena na 1 do 2 metara. Kada se posmatra sa veće udaljenosti, lice je uslikano niskom rezolucijom što može da dovede do neprepoznavanja lica.



Slike uslikane 2D kamerom 640x480 rezolucije kada je korisnik na 3 različite udaljenosti

Jedan od načina za rešavanje ovog problema niske rezolucije jeste generisanje slike lica veće rezolucije od date slike niske rezolucije kroz proces super-rezolucije. Drugi način da se poboljša rezolucija jeste korišćenje visoko rezolucionih kamera ili PTZ.

#### 7.4.3.2. 3D Senzori

Postoje 2 vrste 3D sistema za snimanje lica: jedna se zasniva na laserskom skeniranju, a druga na stereografskoj rekonstrukciji. Smatra se da laserski skeneri pružaju preciznije 3D modele lica, dok stereografske kamere pružaju mogućnost snimanja u skoro realnom vremenu sa malim gubitkom u preciznosti.



Primeri 3D kamera.

Postoji značajna zainteresovanost za razvijanje sistema za prepoznavanje lica koji prihvataju video snimak kao ulaz. Prepoznavanje lica u video snimku zainteresovalo je zbog široke rasprostranjenosti postavljanja nadzornih kamera. Mogućnost automatskog prepoznavanja lica u realnom vremenu sa video snimka je velika olakšica i između ostalog, za identifikaciju ljudi koristeći postojeću mrežu nadzornih kamera. Video snimkom dobijaju se dve karakteristične informacije: više kadrova iste osobe i privremene informacije te osobe čije je lice usnimljeno. Višestruki kadrovi prikazuju različite poze, što omogućuje dobar izbor kvalitetnog kadra (kvalitetnu sliku lica s predaj) za dobro prepoznavanje. Privremene informacije na video snimku odgovaraju dinamičkom pokretu lica u videu. Međutim, teško je utvrditi da li postoje detalji vezani za identitet lica u pokretu (istraživanja u psihologiji su pokazala da pokreti lica imaju neku diskriminatornu karakteristiku koja može biti korisna za utvrđivanje identiteta).

#### 7.4.3.3. Ekstrakcija i usklađivanje karakteristika

Postoje 3 glavna pristupa za usklađivanje usnimljenih lica: na osnovu izgleda, na osnovu modela i metode zasnovane na teksturi.

- Metode na osnovu izgleda stvaraju prikaz celog regiona lica mapiranjem visokodimenzionalne slike lica u manji dimenzionalni podprostor.
- Metode na osnovu modela pokušavaju da naprave 2D ili 3D modele lica koji olakšavaju podudaranje slika lica u prisustvu varijacije poza.
- Metode zasnovane na teksturi pokušavaju da pronađu karakteristike koje su nepromenljive.

#### 7.4.4. Prepoznavanje lica na osnovu izgleda

Šeme na osnovu izgleda zasnivaju se na predstavljanju date slike lica kao funkcije dostupnih različitih slika lica ili kao funkcija nekoliko osnovnih lica. Na primer, vrednost piksela na lokaciji  $(x,y)$  na slici lica može biti predstavljena kao ponderisani zbir vrednosti piksela u svim slikama u  $(x,y)$ .

#### 7.4.4.1. Analiza glavnih komponenti

Analiza glavnih komponenti (PCA) je jedna od najstarijih automatizovanih metoda za prepoznavanje lica. Ova analiza se postiže izvođenjem dekompozicije sopstvenih vrednosti matrice kovarijanse podataka. PCA uključuje sledećih pet koraka:

1. Neka je  $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N$  skup, gde svaki  $\mathbf{x}_i$  predstavlja  $d$ -dimenzionalni vektor kolone. Izračunati prosek skupa kao

$$\boldsymbol{\mu} = \frac{1}{N} \sum_{i=1}^N \mathbf{x}_i.$$

2. Definirati matricu podataka  $\mathbf{X}$  na sledeći način:  $\mathbf{X} = [(\mathbf{x}_1 - \boldsymbol{\mu}) (\mathbf{x}_2 - \boldsymbol{\mu}) \cdots (\mathbf{x}_N - \boldsymbol{\mu})]$ .
3. Izračunati matricu kovarijanse podataka kao

$$\mathbf{C} = \mathbf{X}\mathbf{X}^T$$

gde je  $\mathbf{X}^T$  transponovanje matrice  $\mathbf{X}$ . Pošto je  $\mathbf{X}$   $d \times N$  dimenzionalna matrica, veličina kovarijanse matrice  $\mathbf{C}$  je  $d \times d$ .

4. Izračunati sopstvene vektore matrice kovarijanse  $\mathbf{C}$  rešavanjem sopstvenog sistema

$$\mathbf{C}\mathbf{E} = \lambda\mathbf{E}$$

Ovde,  $\mathbf{E} = [\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_d]$  gde su  $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_d$   $d$  sopstveni vektori matrice  $\mathbf{C}$ .

5. Bilo koji vektor podataka  $\mathbf{x}$  može biti predstavljen kao ponderisani zbir sopstvenih vektora i mogu se izračunati kao  $\boldsymbol{\omega} = \mathbf{E}^T \mathbf{x}$ , gde je  $\mathbf{E}^T$  transponovanje matrice  $\mathbf{E}$ . Imajući u vidu da je  $\boldsymbol{\omega} = [\omega_1, \omega_2, \dots, \omega_d]^T$   $d$ -dimenzionalni vektor kolone, gde je  $\omega_j$  težina povezana sa sopstvenim vektorom  $\mathbf{e}_j$ , za  $j = 1, 2, \dots, d$ . Ove težine su takođe poznate kao sopstveni koeficijenti.

#### 7.4.4.2. Linearna diskriminativna analiza

PCA se može nazvati metodom učenja bez nadzora, jer se oznaka klase (informacije o identitetu korisnika) nikada ne koristi tokom učenja o osnovama lica. Zbog toga se ne može očekivati velika tačnost prepoznavanja lica zasnovana na PCA. Linearna diskriminativna analiza (LDA) eksplicitno koristi oznaku klase podataka o obuci i sprovodi analizu podprostora sa ciljem

minimiziranja unutar klase varijacije i maksimiziranje međuklasnih varijacija. Prema tome, očekuje se da LDA pruža veću tačnost prilikom prepoznavanja lica. LDA koeficijenti se mogu odrediti na sledeći način:

1. Neka je  $(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)$  gde svako  $x_i$  predstavlja  $d$ -dimenzionalni vektor kolone,  $y_i \in \{1, 2, \dots, c\}$  je odgovarajuća oznaka klase i  $c$  broj klasa. Izračunati srednju vrednost svake klase kao

$$\mu_j = \frac{1}{N_j} \sum_{y_i=j} x_i,$$

gde je  $N_j$  broj uzoraka iz klase  $j$  i  $j = 1, 2, \dots, c$ .

2. Definirati matrice rasipanja unutar i između klasa ( $S_w$  i  $S_b$ , respektivno) za date podatke kao

$$S_w = \sum_{j=1}^c \sum_{y_i=j} (x_i - \mu_j)(x_i - \mu_j)^T,$$

$$S_b = \sum_{j=1}^c N_j (\mu_j - \mu)(\mu_j - \mu)^T,$$

gde je  $\mu = (1/N) \sum_{i=1}^N x_i$ .

3. LDA podprostor je napravljen tako da minimizira  $S_w$  i maksimizuje  $S_b$ , što se istovremeno postiže maksimiziranjem  $S_w^{-1} S_b$ . Sopstveni vektori koji maksimiziraju  $S_w^{-1} S_b$  mogu se odrediti na sličan način kao kod PCA, tj. rešavanjem sledećeg sopstvenog sistema

$$S_w^{-1} S_b \mathbf{E} = \lambda \mathbf{E}.$$

4. Bilo koji vektor podataka  $\mathbf{x}$  može se predstaviti kao ponderisani zbir sopstvenih vektora i ove težine mogu se odrediti kao  $\omega = \mathbf{E}^T \mathbf{x}$  gde je  $\mathbf{E}^T$  transponovanje matrice  $\mathbf{E}$ .

#### 7.4.5. Prepoznavanje lica na osnovu modela

Metode zasnovane na modelu pokušavaju da izvuku reprezentaciju nezavisnu od poze slike lica. Mogu omogućiti podudaranje u različitim pozama. Ove šeme uglavnom zahtevaju

otkrivanje nekoliko fundicionalnih ili orijentirnih tačaka na licu (npr. uglovi očiju, vrh nosa, uglovi usta, brada), što dovodi do povećane složenosti u odnosu na metode zasnovane na izgledu.

#### 7.4.5.1. Podudaranje grafika elastične grupe

Šeme Podudaranja Grafika Elastične Grupe (EBGM) predstavljaju lice kao označen graf sa svakim čvorom koji je orijentirna tačka na licu.

Grafikon grupe lica (FBG) može se konstruisati u dve faze. U prvoj fazi dizajner mora ručno označiti željene fundicionalne tačke i da definiše geometrijsku strukturu grafa slike za jednu (ili više) početnih slika. Tokom ovog procesa, ručna intervencija je potrebna samo ukoliko su fundicionalne tačke pogrešno identifikovane. U drugoj fazi, FBG se dobija iz pojedinačnih grafova slika kombinovanjem reprezentativnog skupa pojedinačnih grafova u strukturu.



Određivanje grafova slika za slike lica sa različitim pozama.

Uz FBG, referentne tačke za novu sliku lica se pronalaze maksimizovanjem sličnosti između grafika prilagođenog datoj slici i FBG-a identične poze. Ovaj process je poznat kao Podudaranja Grafika Elastične Grupe (EBGM) i sastoji se od tri sledeća koraka:

- Pronaći približnu poziciju lica grubim skeniranjem ulazne slike pomoću kondenzovanog FGB-a (prosečan graf dobijen uzimanjem srednje Gaborove mlaznice na svakoj gomili). Ovo se postiže diskretnim izdvajanjem Gaborovih mlaznica na izolovanim lokacijama date slike i poređenjem sa mlaznicama u kondenzovanom FBG-u, uzimajući u obzir geometrijsku strukturu FBG-a.

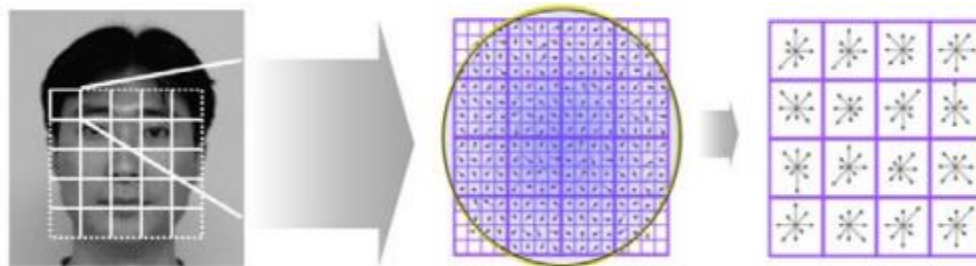
- Precizirati položaj i veličinu lica tako što će se ponovo pretražiti slika potpunim FBG-om, čija veličina i odnos stranica sistematski variraju. Prilikom određivanja sličnosti između Gaborovih mlaznica na datoj slici i gomile mlaznica u FBG-u, uzima se u obzir samo FBG mlaz koji najbolje odgovara datoj slici.
- Precizno locirati fundicionalne tačke pomeranjem svih čvorova lokalno i relativno jedni prema drugima radi dalje optimizacije sličnosti grafa.

#### 7.4.6. Prepoznavanje lica zasnovano na teksturi

Šeme zasnovane na izgledu obično koriste sirove vrednosti intenziteta piksela, koji su prilično osetljivi na promene ambijentnog osvetljenja i izraze lica. Alternativa je da se koriste šeme za predstavljanje karakteristika koje karakterišu teksturu slike koristeći distribuciju lokalnih vrednosti piksela.

##### 7.4.6.1. Skalarna invarijantna transformacija obeležja

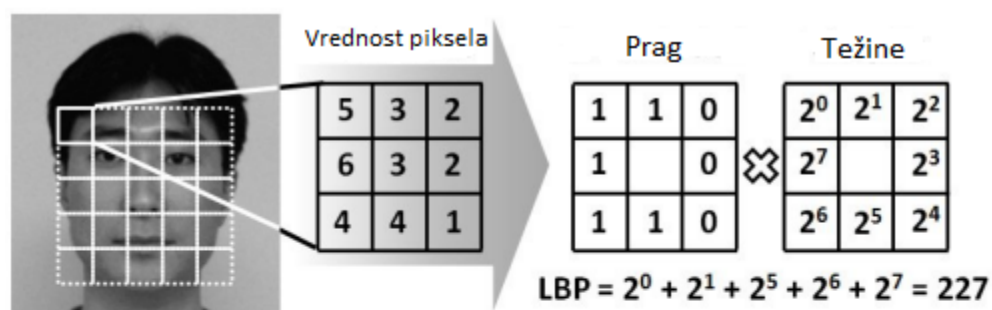
Skalarna invarijantna transformacija obeležja (SIFT) je jedna od najpopularnijih šema lokalnog predstavljanja koja se koristi za prepoznavanje objekata. Proračun SIFT karakteristika sastoji se iz dve faze: (a) izdvajanje ključne tačke i (b) izračunavanje deskriptora u lokalnom okruženju na svakoj ključnoj tački. Baš kao referentne tačke u metodi zasnovanoj na modelu, ključne tačke mogu se koristiti za postizanje tolerancije na varijacije poza. Međutim, broj ključnih tačaka u SIFT-u može biti prilično veliki (reda stotine) i pronalaženje korespondencije između ključnih tačaka sa dve različite slike je izazovan zadatak. Ako pretpostavimo da su slike lica prethodno grubo poravnate (npr. lokacije oka), može se zaobići process prepoznavanja ključnih tačaka i deskriptor se može konstruisati direktno iz cele slike lica. Slika lica je obično predstavljena sa više parčeta i SIFT deskriptor je konstruisan od svakog parčeta. Konačni deskriptor se dobija spajanjem svih deskriptora iz svih parčeta.



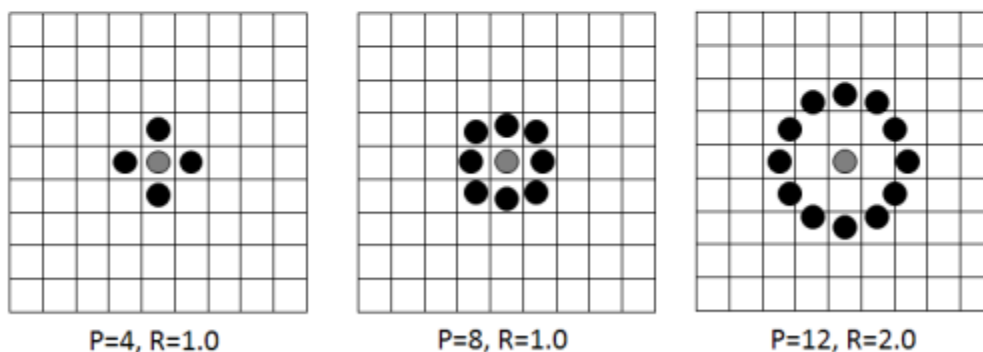
Šematski dijagram konstrukcije SIFT deksriptora. Proces otkrivanja ključne tačke može se zaobići ako su slike lica prethodno poravnate.

#### 7.4.6.2. Lokalni binarni obrazac

Lokalni binarni obrazac (LBP) se uspešno koristi kao lokalni deskriptor teksture u opštem prepoznavanju objekata kao i u prepoznavanju lica. Osnovni LBP operator upoređuje vrednosti intenziteta 8 susednih piksela sa vrednost intenziteta centralnog piksela u regionu i predstavlja rezultat kao 8-bitni binarni string.



(a) Lokalni binarni obrazac (LBP)



(b) Višeskalarni binarni obrazac (MLBP)

Šematski dijagram (a) Lokalno binarnog obrasca (LBP) i (b) Višeskalarnog LBP-a.

Višeskalarni LBP (MLBP) je proširenje osnovnog LBP-a. MLPB uvodi parametar  $R$  kao poluprečnik, što znači da upoređeni susedi su  $R$  piksela udaljeni od centralnog piksela. Postoji i drugi parametar  $P$ , koji predstavlja broj tačaka uzorkovanja duž kruga poluprečnika. Uglavnom, MLBP sa većom vrednošću za  $P$  obezbeđuje detaljnije informacije o lokalnom region. Međutim, kada  $P$  postane veće, povećava se i dimenzija deskriptora. Manje vrednosti  $R$  dovode do otkrivanja mikro detalja, dok veće vrednosti ističu karakteristike makroa. Nakon LBP kodiranja svakog piksela, slika lica se deli na nekoliko manjih prozora i izračunava se histogram lokalnih binarnih obrazaca u svakom prozoru. Broj bitova u histogramu je 8 i  $2^P$  za osnovni LBP i MLBP, respektivno. Globalni vektor obeležja se zatim generiše spajanjem histograma od svakog pojedinačnog prozora i normalizacijom konačnog vektora. Konačno, dve slike lica mogu se upariti izračunavanjem sličnosti (ili udaljenosti) između njihovih vektora karakteristika.



Slike Lokalnog binarnog obrasca (LBP) kodirane različitim razmerama.

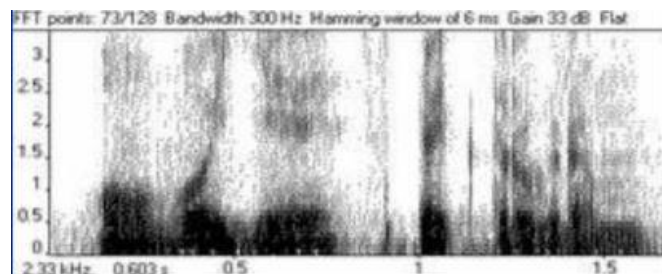
## 8. Biometrija ponašanja

Biometrija ponašanja opisuje fizikalne karakteristike (kao kretanje u prostoru, glas, izgled...) čovečjeg tela koje su delom jedinstvene za svaku osobu. Dobijeni uzorci se opisuju krivama koje se koriste za opis ponašanja pa je na osnovu istih moguće raspoznati različite ljude. Navedene tehnike se koriste u kombinaciji s tradicionalnim načinima jednoznačnog opisivanja ljudi.



## 8.1. Prepoznavanje glasa

Prepoznavanje glasa koristi se u svrhu autentifikacije različitih korisnika na temelju njihovih jedinstvenih glasovnih karakteristika. Verifikacija glasa zasniva se na poređenju korisnikovog zvučnog zapisa sa prethodno snimljenim zapisom i ima za cilj da odredi o kojoj se osobi radi. Verifikacija i prepoznavanje glasa beleži ritam, frekvenciju, visinu, tonalitet glasa i sl. Za snimanje glasa moguće je koristiti i običan ili telefonski mikrofona, mada se pouzdanost skeniranja povećava upotrebom kvalitetnijih mikrofona. Ovo nije naročito pouzdana metoda, pa se tako koristi u verifikacione, a ne identifikacione svrhe i često se koristi u kombinaciji sa drugim metodama. Vreme verifikacije je oko pet sekundi. Veličina dobijenog zvučnog zapisa je reda veličine 2-10Kb. Kako bi se izbegao falsifikat korišćenjem snimka, sistem traži istovremeno i visoke i niske frekvencije zvuka jer je to u većini snimaka nemoguće reprodukovati, tačnije, one se mogu naći samo u pravom glasu. Takođe, neki sistemi generišu nasumičan niz brojeva koji osoba treba da izgovori. Prednost ove metode je što je potrebna oprema izuzetno jeftina i svaki današnji kompjuter, uz odgovarajući softver, može da se iskoristi kao platforma za prepoznavanje glasa. Danas je ova metoda zasnovana na prepoznavanju glasa nalazi na većini raspoloživih mobilnih telefona u svrhu bržeg uspostavljanja telefonskih poziva. Prepoznavanje glasa ima i druge namene kao što je preslikavanje glasa u tekstualne zapise.



Slika: Otisak glasa

## 8.2. Prepoznavanje rukopisa ili potpisa

Ova tehnologija koristi dinamičku analizu potpisa kako bi autentificirala osobu. Tehnologija je bazirana na merenju brzine, pritiska i ugla koji koristi osoba kada se potpisuje ili kada piše

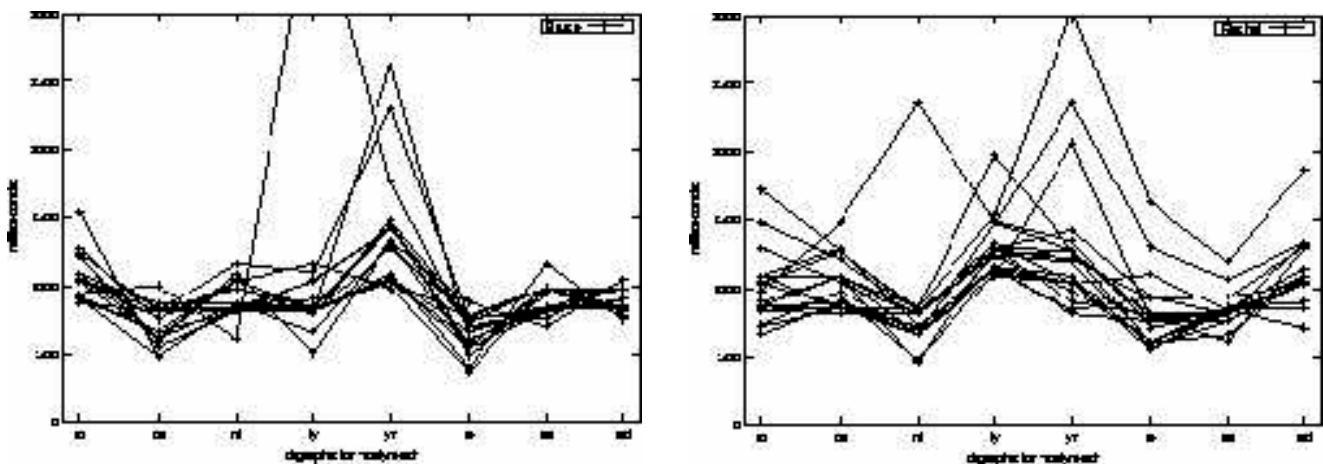
nespecificirani tekst. Jedno od smerova prema kojima se fokusirala ova tehnologija su i ebusiness aplikacije, ali i druge aplikacije gdje je potpis prihvaćen kao metoda autentifikacije.



Slika: Potpis opisan krivama i njihovim međusobnim odnosima

### 8.3. Prepoznavanje kucanja na tastaturi

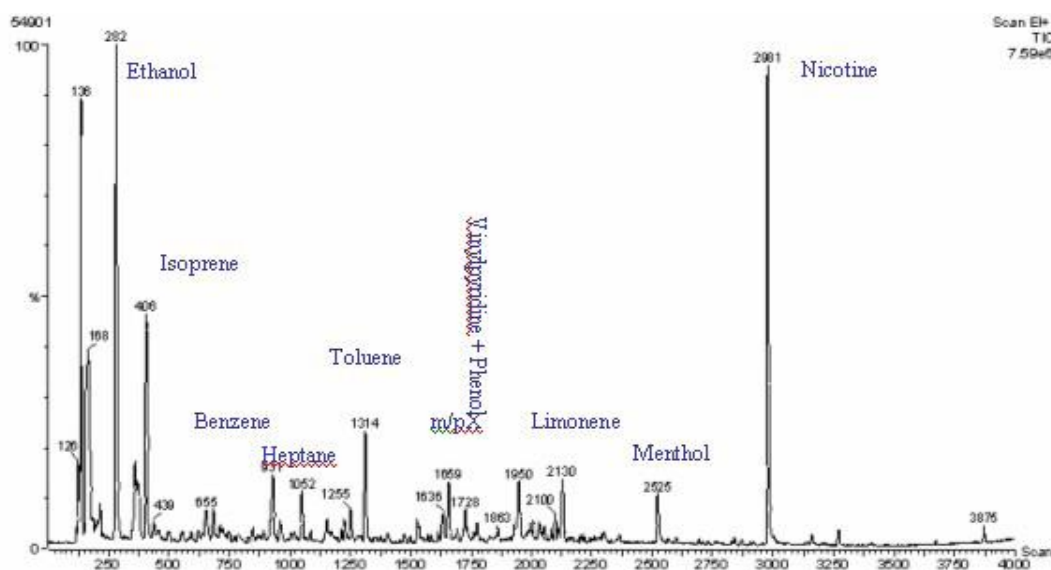
Biometrija ponašanja dinamike kucanja na tastaturi koristi način i brzinu kucanja pojedinca po tastaturi kako bi ustanovila jedinstveni patern kojim korisnik kuca radi buduće autentifikacije. Pritisci tastature su podeljeni na statičko i dinamičko kucanje, koji se koriste u razlikovanju autorizovanih i neautorizovanih korisnika. Informacije o vibracijama se mogu koristiti prilikom kreiranja šablona koji se koriste prilikom identifikacije i verifikacije. Glavna karakteristika na kojoj se ova tehnika bazira je vremenski razmak između korisnikovog pritiskanja na dugme tastature.



Grafički prikaz brzine kucanja iste reči dve različite osobe

## 8.4. Prepoznavanje mirisa

Svaki objekat u prirodi ima svoj miris koji je karakterističan za njegov hemijski sastav. Biometrijski sastavi koji detektuju mirise rade na principu duvanja vazduha preko hemijskih senzora od kojih je svaki osjetljiv na određenu grupu mirisa, tj. na njegova hemijska svojstva. Miris se opisuje merenjima intenziteta na svakom od senzora. Pošto miris ima više funkcija u prirodi kao što su komunikacija, privlačenje partnera, zaštita okoline ili odbrana, onda se može upotrebiti i u vojne svrhe. Pretpostavljajući da svaka osoba sadrži karakterističan miris, moguće je po parametrima svakog od senzora odrediti o kojoj se osobi radi i odrediti glavnu notu mirisa. Posebno je važno razlikovati miris osobe od parfema na njoj pa je u tom polju potrebno još istraživanja kako bi se odvojili mirisi.



Slika: Krive koje opisuju dinamiku različitih supstanci

## 9. Poređenje biometrijskih tehnika

U sledećim tablicama prikazana je paralelno poređenje više biometrijskih tehnologija prema sljedećim karakteristikama:

- univerzalnost - opisuje u kojoj meri se tehnika može primeniti u svakodnevici,

- jedinstvenost - opisuje u kojem postotku je navedena kategorija jedinstvena s obzirom na pojedinca,
- trajnost - opisuje promjenjivost s obzirom na vreme
- prikupljivost - opisuje s kojom lakoćom se dobija uzorak navedene kategorije,
- izvedivost - opisuje u kojoj meri ju je moguće u praksi implementirati
- prihvatljivost - opisuje u kojoj meri je moguća implementacija da se ne naruše ljudska prava.

METODE BIOMETRIJE	UNIVERZALNOST	JEDINSTVENOST	TRAJNOST
LICE	VISOKA	NISKA	SREDNJA
OTISAK PRSTA	SREDNJA	VISOKA	VISOKA
GEOMETRIJA DLANA	VISOKA	SREDNJA	SREDNJA
ROŽNJACA	VISOKA	VISOKA	VISOKA
DNK	VISOKA	VISOKA	VISOKA
POTPIS	NISKA	NISKA	NISKA
GLAS	SREDNJA	NISKA	NISKA
DINAMIKA KUCANJA	NISKA	NISKA	NISKA
MIRIS	VISOKA	VISOKA	VISOKA

Tabela: Poređenje biometrijskih tehnika prema univerzalnosti, jedinstvenosti i trajnosti

METODE BIOMETRIJE	PRIKUPLJIVOST	IZVODLJIVOST	PRIHVATLJIVOST
LICE	VISOKA	NISKA	VISOKA
OTISAK PRSTA	SREDNJA	VISOKA	SREDNJA
GEOMETRIJA DLANA	VISOKA	SREDNJA	SREDNJA
ROŽNJACA	SREDNJA	VISOKA	NISKA
DNK	NISKA	VISOKA	NISKA
POTPIS	VISOKA	NISKA	VISOKA

GLAS	SREDNJA	NISKA	VISOKA
DINAMIKA KUCANJA	SREDNJA	NISKA	SREDNJA
MIRIS	NISKA	NISKA	SREDNJA

Tabela: Poređenje biometrijskih tehnika prema prikupljivosti, izvodljivosti i prihvatljivosti

## 10. Zaključak

Biometrija svakodnevno postaje sve češći oblik autentifikacije u različitim sferama života pa je tako korišćenje biometrije radi prepoznavanja nečijeg identiteta praćenjem njegovih fizičkih karakteristika ili ponašanja, već duže vreme deo stvarnosti. Osnovna namena biometrije je kontrola ulaska ili izlaska sa određenih fizičkih lokacija. Kako bi se to ostvarilo, trenutno su u primeni različiti oblici biometrijskih tehnika, ali najpotpunije rešenje može se postići kombinovanjem različitih metoda – multimodnom biometrijom. Biometrija svoju primenu pronalazi i u kontroli radnog vremena zaposlenika korišćenjem kartica sa čipovima. Takođe, očekuje se da će biometrija imati značajnu ulogu i u bankarstvu.

Iako biometrija poseduje značajne prednosti, prvenstveno povećavanje sigurnosti u smislu autentifikacije korisnika, ista ipak ima i svoje nedostatke. Iako biometrija postaje sastavni deo sistema za upravljanje identitetima, za sada, ipak ne obezbeđuje 100% tačnosti. Faktori koji utiču na to su spoljni uticaji, neuniverzalnost, nesvojstvenost i nedostatak dovoljno nepromenljivih informacija. Još jedna mana biometrije je to što ova tehnologija može biti zloupotrebljena. U društvu je vođena velika polemika i zabrinutost, da bi biometrijski podaci mogli da se shvate kao povreda lične privatnosti, međutim bilo koja baza ličnih podataka ako se nepropisno koristi i zloupotrebljava može biti pretnja po privatnost određene osobe.

Ove dileme bile su tema mnogih konferencija na mnogim evropskim forumima, ali u ovoj oblasti u zemljama Zapadnog Balkana, pa samim tim i u Srbiji malo ko se ozbiljnije bavio ovom tematikom.

Kroz razvoj novih tehnologija verujemo da će i ova oblast napredovati i sve više se usavršavati, te samim tim neće dolaziti do zloupotrebe i da ćemo jednog dana reći da se osećamo relativno sigurno u društvu u kojem živimo uprkos raznim terorističkim i kriminalnim pretnjama, što je svrha i cilj sigurne i odgovorne upotrebe biometrije i biometrijskih podataka.

## 11. Literatura

1. Introduction to biometrics- Anil K. Jain, Arun A. Ross, Karthik Nandakumar
2. <https://en.wikipedia.org/wiki/Biometrics>
3. <https://www.jumio.com/identification-authentication-verification-compared/>
4. M.Pettersson, M.Obrink. How secure is your biometric solution ? Precise Biometrics White Paper, Lund, Sweden, February 2002.
5. Genetic Programming, <http://citeseer.nj.nec.com/correct/211802>
6. R.Volner, P.Boreš. Multi-Biometrics Techniques, Standards Activities and Experimenting, Electronics and Electrical Engineering No 8., Czech Technical University in Prague, 2006
7. <https://hrcak.srce.hr/file/117825>
8. <https://link.springer.com/article/10.1007/s12559-020-09755-z>
9. [https://en.wikipedia.org/wiki/Keystroke\\_dynamics](https://en.wikipedia.org/wiki/Keystroke_dynamics)
10. <https://sr.wikipedia.org/sr/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%98%D0%B0>
11. Handbook of Biometrics edited by Anil K. Jain Michigan State University, USA Patrick Flynn University of Notre Dame, USA Arun A. Ross West Virginia University, USA