Veštačka Inteligencija

Tema:  
Biometrijski sistemi za kontrolu ulaska (Biometrics)

Profesor: Tim: Aleksandra Đokić 17080

Prof. Dr Leonid Stoimenov Radovanović Natalija Pavlović 17321

Mateja Pančić 17326

Sadržaj

[1. Uvod 3](#_Toc93763619)

[1. Istorija razvoja biometrije 5](#_Toc93763620)

[2. Autentifikacija 5](#_Toc93763621)

[3. Metodi autentifikacije 6](#_Toc93763622)

[4. Digitalizacija kao osnova biometrije 7](#_Toc93763623)

[5. Fourierove transformacije 8](#_Toc93763624)

[6. Vrste biometrijskih identifikacija 8](#_Toc93763625)

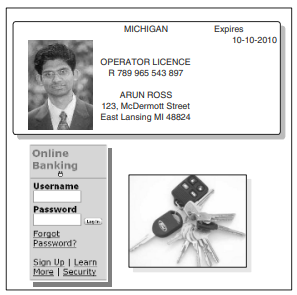
[7. Face Recognition (proces prepoznavanja lica) 9](#_Toc93763626)

[8. Literatura: 12](#_Toc93763627)

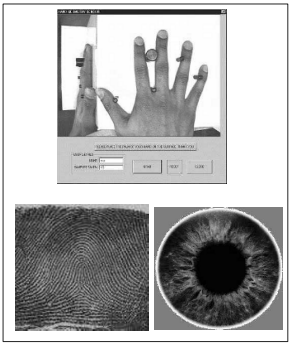
# Uvod

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.

Pomoću biometrike moguće je odrediti identitet na osnovu toga ko smo, a ne šta posedujemo, poput lične karte ili neke šifre koju pamtimo. Ovi tradicionalni sistemi ne mogu garantovati autentičnost korisnika jer može doći do krađe, kopiranja ili gubitka tih identifikatora, dok biometrijska identifikacija, sa druge strane, koristi jedinstvene identifikatore i samim tim je pouzadnija prilikom verifikacije autentičnosti korisnika.



*Tradicionalni način prepoznavanja*

****

*Biometrijsko prepoznavanje*

Drugim rečima, biometrijski sistem je obrazac sistema za prepoznavanje koji uzima biometrijske podatke pojedinačne osobe, upoređuje ih sa podacima sačuvanim u bazi podataka i izvršava radnju u odnosu na rezultate upoređivanja.

# 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 zebeleženi 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 vec 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.

# 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. Kada sistem ili osoba proverava identitet druge osobe ili sistema, vrši se autentifikacija što znači da svako ko je autentifikovan može da potvrdi da je ono što bi trebao biti. 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 [3]:

* 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 slučaj, 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“.

# Metodi autentifikacije

Danas postoje tri metoda autentifikovanja sebe drugoj osobi ili sistemu.(4)

* 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 kôd.  
Veliki sigurnosni problem je u tome što korisnici radi lakšeg pamćenja zadaju predvidljive  
lozinke retko menjaju i 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

# Digitalizacija kao osnova biometrije

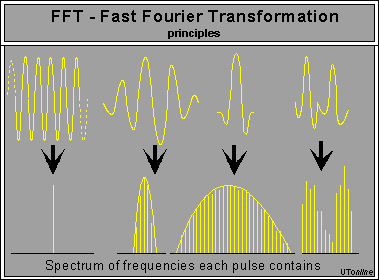
Najvažniji korak u procesu prepoznavanja uzoraka je digitalizacija. Naime, za potrebe računarske obrade podatke dobijee skeniranjem i sl. potrebno je prevesti u digitalni format s kojim računar može raditi. To je proces u kojem se analogni signal pretvara u digitalni te prepoznaje programskom opremom. 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 Fourierovih 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.



Slika: Izgled digitaliziranog uzorka

# Fourierove transformacije

Brza Fourierova transformacija ili kraće FFT (eng. Fast Fourier Transformation) je jedna od najlakših i najkorištenijih tehnika za opisivanje i obradu signala. Radi sa relativno malom rezolucijom, a opisivanje i obrade signala se obavlja u digitalnom signalnom procesoru – DSP (eng. Digital Signal Processor) pomoću Fourierovih transformacija. Njima se opisuje kriva uzorka i njegovih harmonika pri čemu se prevode u par sinusnih funkcija. Tehnika je nazvana po Josefu Fourieru.



Slika : Fourierove transformacije

# Vrste biometrijskih identifikacija

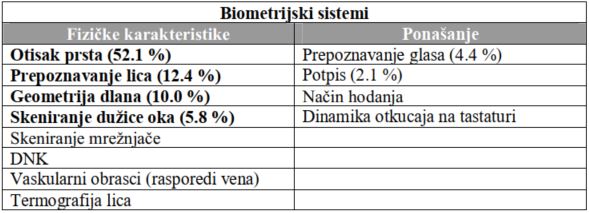
Biometrija se može definisati kao model identifikacije osobe, baziran na fizičkim karakteristikama ili karakteristikama ponašanja, a odnosi se na nešto što osoba poseduje ili ono što osoba zna kako bi izvršila identifikaciju, , pa se na osnovu toga i biometrijske identifikacije mogu, uslovno rečeno,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

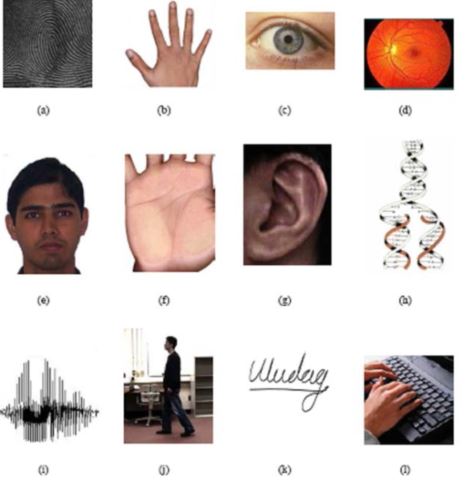
Na samom početku korišćenja biometrije, prednost je davana fizičkim karakteristikama u odnosu na ponašajne karakteristike. Prevladavalo je mišljenje da fizičke karakteristike, u odnosu na ponašajne, poseduju „uočljivost“. Prema tom mišljenju, prevladavalo je i uverenje kako su fizičke karakteristike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

# Fizička biometrija

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



Slika: Procentualna zastupljenost biometrijskih tehnika na tržištu



Slika : 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

# Čitanje DNK zapisa

Britanski znanstvenik sir Alec Jeffreys prvi je 1984. godine primijenio činjenicu o jedinstvenosti građe molekule DNK na identifikaciju nepoznatih počinitelja kaznenih djela, pa je metodu nazvao DNA-fingerprinting po uzoru na do tada neprikosnovenu daktiloskopsku metodu identifikacije. Analiza DNK je zasigurno jedna od najznačajnijih i najpouzdanijih biometrijskih metoda identifikacije. Koristi se u mnogim područjima istraživanja, a nama najzanimljivija primjena je u području kriminalistike i sudske medicine gdje se analiza DNK koristi za utvrđivanje identiteta nepoznate osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tijela, određivanje spola osoba, odnosno za traseološku identifikaciju, te kriminalistička istraživanja kaznenih djela. Kod analize DNK koriste se unaprijed određeni lokusi, za koje je poznato da sadrže određene parove baza koji se uzastopno ponavljaju, a istodobno pokrivaju veliku varijabilnost u ljudskoj populaciji, odnosno koji sadrže VNTR. VNTR ili varijabilni (polimorfni) ponavljajući sljedovi (engl. Variable number tandem repeats) su visoko polimorfni sljedovi i određeni su brojem ponavljajućih DNK sekvenci. Većina DNK sljedova odnosno sekvenci ne sadrži gene, već služi isključivo kao pomoćni genetički materijal. Kratke sekvence parova baza koji se učestalo ponavljaju, nazivaju se kratki ponavljajući sljedovi 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.

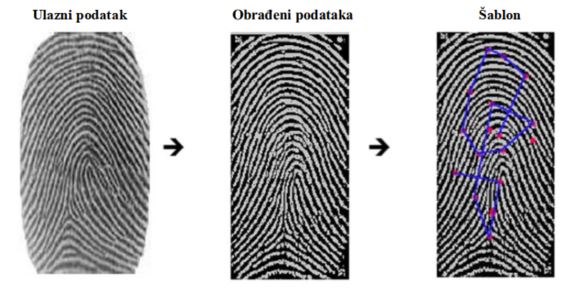
# Otisak prsta

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 računaru 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.

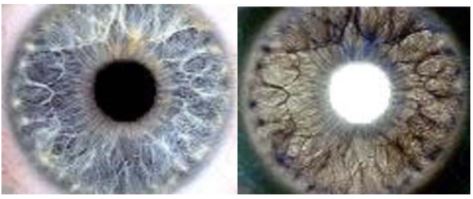
Različita je i tehnologija kojom se skenira otisak i ona se najčešće bazira na kapacitivnim, optičkim ili ultrazvučnim senzorima



Slika: Proces od originalne slike do šablona

# 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  
intezitet. To radi u cilju detekcije dilatacije zjenice. 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.



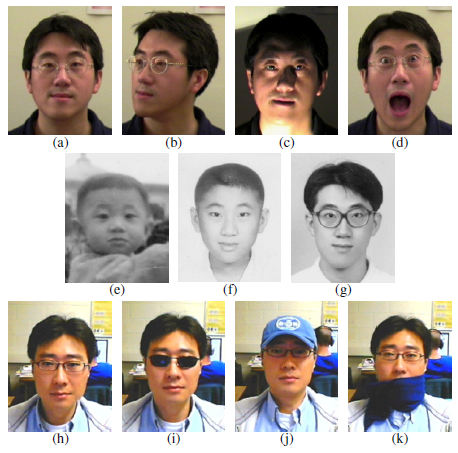
Slika:Rožnjača oka i njen negativ

# Face Recognition (proces prepoznavanja lica)

Lice je prednji deo čovekove glave krećući se od čela sve do brade uključujuči 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 prepozavanja lica ima i dobrih karakteristika kao što su mogućnost “hvatanja” lica sa velikih razdaljina sto omogućava korišćenje u vidu nadzornih kamera. Isto tako lice dosta govori o raspoloženje kao i biografskim informacijama osobe. U odnosu na druge vrste biometrike 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

## 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.

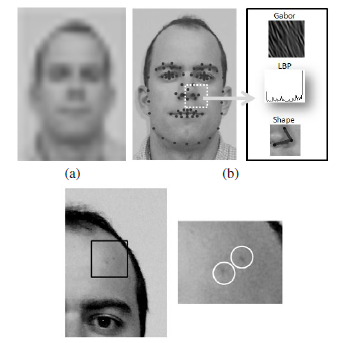
## Crte lica

Antropometrijske studije su pokušale da okarakterišu dimenzije lica na osnovu skupa anatomski 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

## 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 lice. 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. Sensing tehnologije se stalno poboljšavaju u cilju povećanja rezolucije slike, povećanjem broja detalja snimanjem lica koristeći više spektra (tj. vidljivi, infracrveni…) i olakšavaju rad 3D senzora u realnom vremenu.

## 2D Senzori

# 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.

# Prepoznavanje glasa

# Prepoznavanje rukopisa ili potpisa

# Prepoznavanje kucanja na tastaturi

# Prepoznavanje mirisa

# 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*](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