

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Matej Gorenšek

**Uporabe tehnologije za prepoznavanje obrazov za komercialne
namene**

Magistrsko delo

Ljubljana, 2017

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Matej Gorenšek

Mentor: izr. prof. dr. Damjan Škulj

**Uporabe tehnologije za prepoznavanje obrazov za komercialne
namene**

Magistrsko delo

Ljubljana, 2017

ZAHVALA

*Hvala mentorju doc. dr. Damjanu Škulju za vso strokovno pomoč
pri pisanju magistrske naloge.*

Hvala Damjanu Klemenčiču za vso pomoč pri izdelavi programa.

Hvala moji družini, ki mi je vedno stala ob strani in me podpirala.

Uporabe tehnologije za prepoznavanje obrazov za komercialne namene

Uporaba tehnologije za prepoznavanje obrazov za komercialne namene je v zadnjih letih doživela velik napredek. Glavni dejavnik, ki je vplival na to, je razvoj tehnologije. Danes je namreč mogoče slike zajemati že s skoraj vsemi napravami, ki nas obkrožajo. Prav tako so te naprave neprestano povezane s svetovnim spletom in nam omogočajo enostavno in hitro deljenje informacij z drugimi in njihovo hrambo na raznih spletnih mestih. Zaradi velike količine slik obrazov, ki so na voljo vsem, ki imajo dostop do spleta, so začela podjetja razvijati algoritme za prepoznavanje obrazov, da bi tako uporabnikom ponudila dodatne funkcionalnosti. Facebook je najbolj znan primer, ki je uporabnikom že leta 2010 ponudil možnost avtomatskega označevanja na slikah in jim tako omogočil hitrejše in enostavnejše deljenje informacij oz. slik. Ob tem so se pojavila pravna, etična in družbena vprašanja, saj so slike in biometrične lastnosti prepoznanih oseb postale del njihove baze, kjer obstaja možnost zlorabe in uporabe le-teh podatkov v druge namene. Facebook-ov algoritem in ostali algoritmi, ki se uporabljajo v komercialne namene, so z leti postali učinkovitejši in naprednejši, kar je mogoče zaznati z vedno večjim številom izvajalcev, ki danes te algoritme vgrajujejo v svoje programske ali strojne izdelke. Z magistrsko nalogo želim narediti primerjalno študijo učinkovitosti in uporabnosti algoritmov za prepoznavanje obrazov, ki se uporabljajo v komercialne namene. Študijo bom izvedel s programom, ki je dostopen na svetovnem spletu in ki ga bom prilagodil za uporabo v magistrski nalogi s tremi različnimi metodami prepoznavanja obrazov. Pridobljene rezultate bom nato primerjal z ostalimi raziskavami in podal ključne ugotovitve.

Ključne besede: prepoznavanje obrazov, metode, algoritmi, učinkovitost, omejitve, delovanje, ocenjevanje sistema

Commercial use of facial recognition technology

Commercial use of facial recognition technologies for commercial purposes has undergone a major development in recent years. The main reason for growing interest is the development of technology. Nowadays, it is possible to capture photographs with almost every device that surrounds us. Also, these devices are constantly connected to the internet and allow us sharing photographs with others and easily and quickly storing them on various web sites. Due to large amount of facial photographs that are generally accessible to everyone, companies began to develop facial recognition algorithms in order to provide them with additional functionality. Facebook is the best-known example, which in 2010 offered their users possibility to automatically tag photos, allowing to share them faster and easier. Legal, ethical and social issues arose, as the images and biometric features of the identified persons became part of their databases, and therefore possibly subject of abuse or use for non-intended purposes. Facebook's and other algorithms used in commercial purposes have become ever more efficient over the years, which can also be seen by an increasing number of providers that are now embedding them in their software or hardware products. Within my master's thesis, I make a comparative study of the efficiency and usability of facial recognition algorithms that are used for commercial purposes. I conduct a study with a web access program, which is adapted for the purposes of the thesis, with three different facial recognition methods. I then compare the obtained results with other researches and report on the key findings.

Key words: face recognition, methods, algorithms, performance, limitations, operation, system evaluation

KAZALO VSEBINE

1 UVOD	8
2 BIOMETRIJA IN BIOMETRIČNE METODE.....	13
2.1. Klasifikacija biometričnih metod.....	13
2.2. Biometrične značilnosti	13
2.2.1. Telesne značilnosti.....	14
2.2.1. Vedenjske značilnosti.....	19
3 ZGODOVINA BIOMETRIJE IN AVTOMATIČNEGA PREPOZNAVANJA OBRAZOV	21
4 DELOVANJE SISTEMOV ZA PREPOZNAVANJE OBRAZOV	23
5 PODROČJA UPORABE SISTEMOV ZA PREPOZNAVANJE OBRAZOV	26
6 OMEJITVE SISTEMOV ZA PREPOZNAVANJE OBRAZOV	31
7 ZAKONSKI IN ETIČNI VIDIKI UPORABE TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZOV	34
7.1 Varovanje osebnih podatkov.....	34
7.2 Zasebnost.....	36
8 DRUŽBENI VIDIK UPORABE TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZOV	39
9 UČINKOVITOSTI ALGORITMOV ZA PREPOZNAVANJE OBRAZOV	42
10 PROGRAM EMGU CV IMAGE PROCESSING WRAPPER.....	44
11 METODE PREPOZNAVANJA OBRAZOV	47
11.1 Metoda lastnih obrazov (analiza glavnih komponent)	47
11.2 Metoda Fisherjevih obrazov (linearna diskriminantna analiza)	53
11.3 Metoda lokalnih binarnih vzorcev (angl. <i>local binary pattern</i> - LBP)	56
12 ZBIRKA SLIK: MSRA-CFW	59
13 TEST PRIMERA PREPOZNAVANJ OSEB	62
13.1 Mere učinkovitosti.....	62
13.2 Opis postopka izvedbe	64
13.3 Izvedba prepoznavanja oseb.....	65
13.3.1 Metoda lastnih obrazov (analiza glavnih komponent)	66
13.3.2 Metoda Fisherjevih obrazov (linearna diskriminantna analiza).....	67
13.3.3 Metoda lokalnih binarnih vzorcev.....	69
13.3.4 Primerjava uspešnosti med metodami glede na število slik, vključenih v prepoznavo.....	71
14 SKLEP	73
15 LITERATURA	77
PRILOGA: SEZNAM OSEB, UPORABLJENIH PRI PREPOZNAVANJU	86

KAZALO SLIK

Slika 2.1: DNK vijačnica.....	14
Slika 2.2: Primer termografije obraza	15
Slika 2.3: Prstni odtis.....	16
Slika 2.4: Geometrija dlani.....	17
Slika 2.5: Odtis leve dlani	17
Slika 2.6: Šarenica oz. iris	18
Slika 2.7: Očesna mrežnica	18
Slika 4.1: Ključne obrazne točke	23
Slika 6.1: Primer različne osvetlitve obraza	31
Slika 6.2: Primer različne postavitve obraza	32
Slika 8.1: Zapuščeni zapor Panoptikon na Kubi	40
Slika 10.1: Originalni program EMGU CV image processing wrapper	45
Slika 10.2: Nov program EMGU CV image processing wrapper	45
Slika 12.1: Izbrisane slike iz mape osebe Chris Brown	60
Slika 13.1: Ureditve baze slike	65

KAZALO SHEM

Shema 4.1: Tokokrog sistemov za prepoznavanje obrazov	24
Shema 11.1: Primer matrike	49
Shema 11.2: Vektor matrike	49
Shema 11.3: Primer delovanja originalnega operatorja lokalnih binarnih vzorcev	56
Shema 11.4: Primeri različnih večnivojskih operatorjev: krožni (8, 1), (16, 2) in (8, 2)	57
Shema 13.1: ROC krivulja	64

KAZALO TABEL

Tabela 5.1: Področja uporabe tehnologije za prepoznavanje uporabe in primeri uporabe	29
Tabela 12.1: Struktura baze podatkov po spolu oseb	60
Tabela 12.2: Struktura baze podatkov glede na področje delovanja	61
Tabela 13.1: Rezultati prepoznavne metode lastnih obrazov (10 % slik v postopku učenja)	66
Tabela 13.2: Rezultati prepoznavne metode lastnih obrazov (20 % slik v postopku učenja)	67
Tabela 13.3: Rezultati prepoznavne po metodi Fisherjevih obrazov (10 % slik v postopku učenja)	68

Tabela 13.4: Rezultati prepoznavne po metodi Fisherjevih obrazov (20 % slik v postopku učenja)	68
Tabela 13.5: Rezultati prepoznavne metode lokalnih binarnih vzorcev (10 % slik v postopku učenja)	70
Tabela 13.6: Rezultati prepoznavne metode lokalnih binarnih vzorcev (20 % slik v postopku učenja)	70
Tabela 13.7: Rezultati prepoznavne uspešnosti med metodami (10 % slik v postopku učenja)	71
Tabela 13.8: Rezultati prepoznavne uspešnosti med metodami (20 % slik v postopku učenja)	72

1 UVOD

Ljudje imamo posebno prirojeno sposobnost, s katero rutinsko, na podlagi naših fizičnih lastnosti, kot so obraz, glas in hoja, vsakodnevno prepoznavamo druge, ne da bi se tega sploh zavedali (Li in Jain v Li in Jain 2011, 1). V znanosti temu pravimo biometrija (pogosto tudi biometrika). Beseda izhaja iz starogrške besede »bios« (življenje) in »metron« (meritev). Biometrija je veda, ki preučuje prepoznavanje ljudi na podlagi njihovih fizioloških in/ali vedenjskih značilnosti (Jain in drugi 2004, 1), ki so edinstvene in stalne za vsakega posameznika posebej. Jain in drugi (prav tako, 8–10), so definirali štirinajst najbolj razlikovalnih biometričnih značilnosti, ki se v znanosti najpogosteje uporabljajo za ugotavljanje identitete posameznika. Te značilnosti so: DNK, uho, podoba obraza, termografija obraza, roke in prepleta ven na roki, prstni odtis, gibanje (način hoje), geometrija dlani in prstov, šarenica oz. iris, tipkanje, vonj, odtis dlani, očesna mrežnica, podpis in glas (govor).

Uporaba različnih biometričnih značilnosti za preverjanje identitete nekoga ima v primerjavi z ostalimi načini, kot so gesla, PIN številke ipd., velike prednosti. Bančno kartico ali osebno kartico lahko izgubimo, osebno geslo ali PIN številko lahko pozabimo, biometričnih značilnosti pa ne moremo izgubiti ali jih pozabiti, navadno ostanejo večne, zahtevajo prisotnost posameznika v času identifikacije in jih je težko (vendar ne nemogoče) kopirati, ponarediti, deliti ali prenesti na drugo osebo (House of Commons, Science and Technology Committee 2015, 5).

Z razvojem cenovno ugodnih računalnikov in visoko tehnoloških mobilnih naprav se je predvsem ena biometrična značilnost začela vedno bolj uporabljati za prepoznavanje posameznikove identitete, to je podoba obraza (Li in Jain v Li in Jain 2011, 1). Prepoznavanje podobe obraza se je razširila na različna področja komercialne rabe in ne le za namene varnosti (Hossain in drugi 2015). S prepoznavanjem obrazov se dnevno srečujemo že pri interakciji človeka in računalnika, virtualni realnosti, pridobivanju podatkovnih baz, multimediji, računalniškem razvedrilu (angl. *computer entertainment*), informacijski varnosti, npr. za dostop do operacijskega sistema, medicinskih zapisih, spletnemu bančništvu, biometriji – npr. osebna identifikacija s potnim listom, vozniskim dovoljenjem, avtomatskih sistemih za prepoznavo – npr. pri sistemih za nadzor voznikov, domačih video nadzornih sistemih. (Suhas in drugi 2012, 15).

Z veliko količino slik in video posnetkov, ki so nam nenehno dostopni preko spleta in drugih podatkovnih baz, je prepoznavanje obrazov postalo pomemben del sistemov za poizvedovanje po slikah na podlagi vsebine ali krajše CBIR-sistemov (angl. *content based image retrieval system*) (Hjelmås in Low 2001, 263). Naše slike se že od nekdaj rutinsko zbirajo s strani raznih inštitucij, npr. ko zaprosim za voziško dovoljenje, potni list ali osebno izkaznico, kartico za dostop do knjižnice, avtobusno vozovnico (Introna in Wood v Norris in Wood 2004, 178). Prav tako sami slike sebe in drugih dnevno puščamo po raznih spletnih portalih kot je Facebook, Instagram, Snapchat ipd.

Prednost uporabe prepoznavanja obraza v primerjavi z drugimi biometričnimi značilnostmi, kot je npr. prstni odtis ali šarenica, je predvsem ta, da deluje povsem anonimno, saj lahko obraz zajamemo na daljino in na prikrit način – brez vednosti osebe, ki jo želimo identificirati (Li in Jain v Li in Jain 2011, 1). Zaradi tega je tudi njihova uporaba v varnostnih in nadzornih sistemih zelo razširjena.

Trenutno najbolj razširjena komercialna storitev, ki uporablja tehnologijo za prepoznavanje obrazov (angl. *facial recognition technology*), je Facebook, ki je uvedel storitev označevanja oseb na slikah (angl. *photo tag suggest*) za ameriške uporabnike konec leta 2010 ter za vse ostale uporabnike junija 2011 (Slotch 2011). Ta tehnologija omogoča uporabnikom pri deljenju slik z drugimi avtomatično zaznavo in prepoznavo oseb, ki so na njih prisotne. Uporabnik pa lahko osebe na sliki ročno označi tudi sam. Na takšen način se hitro, enostavno in večkrat tudi brez vednosti uporabnika poveže podoba obraza na sliki s podatki uporabnika na njegovem profilu. Kako popularen je Facebook za deljenje slik priča število naloženih slik, ki je oktobra 2012 znašalo 220 milijard in se je dnevno povečalo za 300 milijonov (Welinder v Li 2012, 173).

Algoritmi za prepoznavanje obrazov so prisotni tudi v vedno bolj priljubljeni aplikaciji za deljenje slik in videoposnetkov, Snapchat-u. Ta je septembra 2015 v svojo aplikacijo dodal funkcionalnost, ki uporabnikom omogoča uporabo posebnih animiranih učinkov na obrazih na slikah, ki so jo poimenovali Lenses (The Verge 2015).

Algoritmi za prepoznavanje obrazov so postali tudi del programov za urejanje slik. Google Picasa je omenjeno funkcionalnost dobila prvič leta 2009 z verzijo 3.5, prav tako Applov iPhoto verzija 9. Adobe je avtomatično zaznavo obrazov prvič predstavil s programom Photoshop CS6

leta 2012. Tudi v igričarski panogi ima zaznavanje obrazov velik pomen. Velik korak pri tem je naredil Microsoft s predstavitvijo dodatka Kinect za svojo igralno konzolo Xbox 360, ki s svojimi senzorji zaznava in prepozna vaše gibe in mimiko obraza. Isto tehnologijo uporablja tudi njihov operacijski sistem Windows 10, ki s funkcijo Windows Hello omogoča vpis uporabnika glede na prepoznavo njegovega obraza s kamero, nameščeno na napravi, preko katere želimo dostopati. Tudi pametni mobilni telefoni, spletne kamere in fotoaparati danes vsebujejo algoritme za prepoznavo obrazov, saj s tem omogočajo uporabnikom enostavnejše in hitrejše zajemanje slik z avtomatskim fokusiranjem in samodejno osvetlitvijo.

Poleg omenjenih komercialnih namenov uporabe pa je seveda najpomembnejši vidik uporabe na področju varnosti in nadzora, ki je najbolj zaslužen za razvoj in uporabo teh tehnologij tudi v komercialne namene. Predvsem se je zanimanje za uporabo sistemov za prepoznavanje obrazov povečalo 11. septembra 2011, po terorističnem napadu na Združene države Amerike (Bowyer 2004; Brey 2004; Introna in Wood v Norris in Wood 2004, 182). Tako je leta 2014 Ameriški zvezni preiskovalni biro (FBI) začel vzpostavljati sistem za prepoznavanje obrazov, s katerim ob pomoči vseh kamer, ki so pod nadzorom, zbirajo in arhivirajo podatke o ljudeh in njihovem gibanju znotraj ZDA (Mladina 2012). Leta 2014 je policija v Kanadskem mestu Calgary (kot prva policijska postaja) začela uporabljati program za prepoznavo obrazov, s katerim primerjajo slike obsojencev (angl. *mugshots*) s slikami in video posnetki s krajev zločinov (CBC News 2014). Prav tako je z uporabo podobne programske opreme začela južnoavstralska policija (ABC News 2016). Tudi na letališčih je uporaba algoritmov za prepoznavo obrazov vedno pogostejše v uporabi, saj se je s povečevanjem prometa na letališčih povečala tudi potreba po večjem varovanju potnikov kot tudi letaliških delavcev (Divyarajsinh in Brijesh 2013, 86).

Največja razlika med komercialnimi sistemi in sistemi na področju varnosti in nadzora je v posledicah, ki jih lahko prepoznana oseba čuti. Uporaba komercialnih storitev in izdelkov, ki uporabljajo tehnologije za prepoznavanje obrazov in jih uporabljamo zavestno, kot npr. Facebook, Snapchat, mobilni telefon itd., dopuščajo določene napake pri prepoznavanju, saj zaradi njih uporabniki ne čutijo nikakršnih družbenih ali pravnih posledic. Povsem drugače je pri uporabi teh tehnologij za namen varnosti s strani varnostnih agencij in organov pregona za namen varnosti in nadzora, saj lahko posledice, v primeru napake pri identifikaciji osebe, znatno vplivajo na napačno identificirano osebo.

V nadaljevanju magistrskega dela bom podrobneje raziskal delovanje in uporabo komercialnih tehnologij za prepoznavanje obrazov. V teoretičnem delu bom najprej podrobneje opisal biometrijo in biometrične metode. V tretjem poglavju bom na kratko predstavil zgodovino biometrije oz. podrobneje obrazne prepoznavne in ključne mejnike pri njenem razvoju. V četrtem poglavju se bom osredotočil na delovanje sistemov prepoznavanja obrazov, v petem na področja uporabe in v šestem njihove omejitve. Nato bom v sedmem poglavju opisal zakonske in etične vidike uporabe teh tehnologij in v osmem družbene vidike uporabe. S pregledom sekundarne literature bom v devetem poglavju preveril, kakšna je učinkovitost sistemov prepoznavanja obrazov, ki za prepoznavo uporabljajo različne algoritme. V desetem poglavju bom opisal program EMGU CV image processing wrapper, ki ga bom v praktičnem delu, spremenjenega za namen uporabe v svojem delu, uporabil za testiranje učinkovitosti prepoznavanja, in v enajstem opisal vse tri uporabljene metode, s katerimi bom izvedel prepoznavo. Teoretični del bom zaključil z dvanajstim poglavjem, v katerem je opisana podatkovna baza slik.

V praktičnem delu magistrske bom skušal prikazati, kako se z enostavnim programom za prepoznavanje obrazov, ki je prosto dostopen na spletu, in z nekaj programerskega znanja, lahko enostavno pridobi učinkovito orodje za identifikacijo oseb na slikah. S pomočjo testne baze slik slavnih ljudi, pridobljene na spletu, bom v trinajstem poglavju izvedel testiranje njegove uspešnosti in rezultate prepoznavne predstavil z ustreznimi kvantitativnimi statističnimi metodami – merami učinkovitosti. Postopek bom ponovil s tremi različnimi metodami prepoznavanj obrazov, ki jih program podpira. To so:

- metoda lastnih obrazov (angl. *eigenfaces*),
- metoda Fisherjevih obrazov (angl. *fisherfaces*) in
- metoda lokalnih binarnih vzorcev (angl. *local binary pattern - LBP*).

V zadnjem, štirinajstem poglavju, bom podal ugotovitve analize in primerjal učinkovitost prepoznavne med uporabljenimi metodami.

Cilj magistrske naloge je podati primerjalno študijo učinkovitosti in uporabnosti različnih metod za prepoznavanje obrazov na spletno dostopnem programu, pri enakih pogojih in isti podatkovni bazi. Raziskovalna vprašanja, na katera bom skušal odgovoriti, so:

1. ali so komercialni sistemi za prepoznavanje obrazov dovolj razviti, da lahko trdimo, da je njihova uporaba učinkovita in zanesljiva;

2. ali obstajajo razlike v učinkovitosti med različnimi algoritmi za prepoznavanje oseb;
3. ali obstajajo razlike med različnimi tehnikami prepoznavanja oseb, saj metoda lastnih obrazov in metoda Fisherjevih obrazov spadata med holistične oz. globalne tehnike prepoznavanja, metoda lokalnih binarnih vzorcev pa med lokalne oz. strukturne tehnike ter
4. ali različno število slik, uporabljenih v postopku učenja, vpliva na učinkovitost prepoznavne.

2 BIOMETRIJA IN BIOMETRIČNE METODE

Ljudje vsakodnevno uporabljamo različne človekove fizične karakteristike, kot so obraz, glas in hoja ter njihove kombinacije, za prepoznavanje drug drugega. Vedi, ki se ukvarja s tem, pravimo biometrija oz. biometrika (grško »bios« – življenje in »metrikos« – merjenje). Biometrične vede se tako ukvarjajo s prepoznavanjem unikatnih in značilnih človekovih karakteristik, ki so zbrana, zmerjena in shranjena z namenom avtomatične prepoznave.

2.1. Klasifikacija biometričnih metod

Glede na participacijo udeležencev lahko biometrične metode razdelimo v dve skupini: aktivne in pasivne (Bowyer 2004, 10). Prepoznavanje prstnih odtisov je primer aktivne participacije, saj je za identifikacijo določene osebe potrebna njena aktivna udeležba pri oddajanju prstnih odtisov. Medtem ko je metoda prepoznavanja na osnovi obrazov pasivna metoda, saj lahko v praksi osebo prepoznamo brez njenega zavedanja ali sodelovanja.

Sisteme za prepoznavanje obrazov lahko nadalje razdelimo v dve skupini glede na uporabnikovo sodelovanje (Li in Jain v Li in Jain 2011, 3):

1. postopek prepoznavne, kjer uporabnik sodeluje in
2. postopek prepoznavne, kjer uporabnik ne sodeluje.

Primer sodelovanja uporabnika je prijava osebe v računalnik, fizična kontrola dostopa, e-potni list, kjer je uporabnik prisoten v procesu prepoznavanja in je v njem tudi pripravljen sodelovati. V primeru nesodelovanja uporabnika, kar je pogosto pri sistemih nadzora, pa se oseba ne zaveda sodelovanja v postopku identifikacije.

2.2. Biometrične značilnosti

Prepoznavanje obrazov je ena izmed mnogih biometričnih značilnosti identifikacije oseb (Hjelmås in Low 2001, 263). Po Jain in drugi (2004, 8–10) obstaja štirinajst biometričnih značilnosti oseb, ki se v praksi najpogosteje uporabljajo za različne namene. Delimo jih v dve skupini (House of Commons, Science and Technology Committee 2015, 3): fizične (telesne) in vedenjske značilnosti. Te značilnosti se lahko pri prepoznavanju uporabljajo posamično ali v

kombinaciji, npr. prepoznavanje obrazov v kombinaciji z glasom in prstnim odtisom. Vsaka značilnost ima svoje prednosti in slabosti, na katerih temelji njihova uporaba.

2.2.1. Telesne značilnosti

1. DNK (Deoksiribonukleinska kislina): DNK je enodimenzionalna končna unikatna koda vsakega posameznika – z izjemo dejstva, da imata dvojčka identična DNK vzorca. Ta značilnost se najpogosteje uporablja v forenziki za prepoznavanje oseb. Slabost prepoznavanja na osnovi DNK so: (1) onesnaževanje in občutljivost, saj je mogoče enostavno ukrasti delček DNK neke osebe in ga uporabiti proti njej; (2) onemogočeno prepoznavanje v realnem času in na terenu, saj je za ugotavljanje ujemanja DNK potrebna zahtevna kemična metoda, ki jo je moč izpeljati le v laboratoriju; (3) iz DNK je mogoče pridobiti informacije o dovzetnosti osebe za določene bolezni, kar lahko privede do zlorabe podatkov o genetični kodi ter posledično do diskriminacije npr. pri zaposlovanju.

Slika 2.1: DNK vijačnica



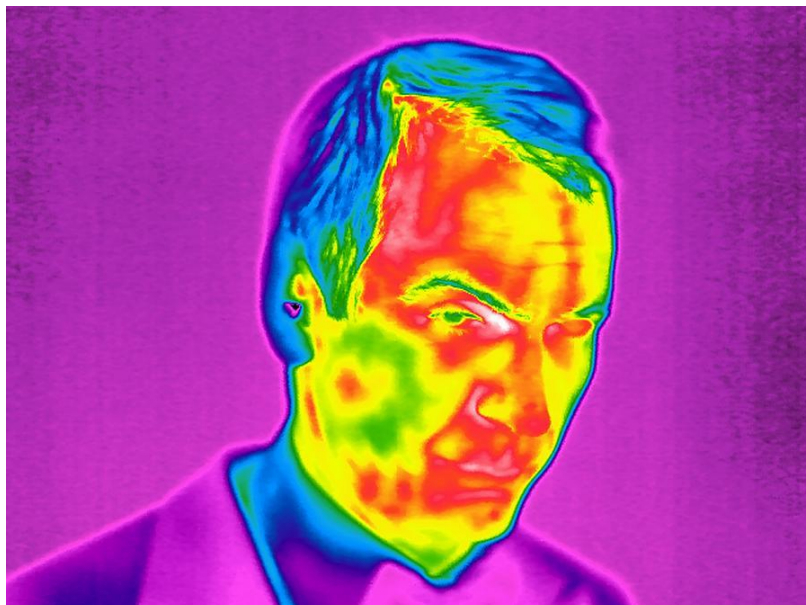
Vir: Wideshut (2017).

2. Uho: Oblika ušesa in tkivo zunanega ušesa (pinne) se razlikujeta med ljudmi. Metode, ki prepoznajo ušesa, delujejo na način, da primerjajo razdaljo med značilnimi točkami zunanega ušesa in lokacijo glavnih značilnosti njegove oblike.
3. Podoba obraza: Obrazna prepoznavanje je najmanj vsiljiva in najbolj uporabljena metoda prepoznavanja ljudi. Uporablja se za prepoznavanje zločincev, na letališčih itd. Najpogostejši postopek za prepoznavo temelji na: (1) lokaciji značilnih obraznih točk,

kot so oči, obrvi, nos, usta, brada in njihovo prostorsko razporeditvijo; (2) uporabi celotne obrazne slike. Sistemi, ki uporabljajo podobo obraza za prepoznavanje oseb, imajo določene pogoje, ki morajo biti upoštevani pri zajemu slike, kot sta npr. fiksno in enostavno ozadje ter osvetlitev. Takšni sistemi imajo lahko težavo pri prepoznavanju obraza iz slike, če je ta zajeta iz različnih kotov ali različno osvetlitvijo. Vprašanje, ki se pojavlja je, ali je slika obraza, brez kakršnih koli kontekstualnih informacij, dovolj za prepoznavo osebe iz množice identitet in z zadostno mero zaupanja.

4. Termografija obraza, roke in prepleta ven na roki: Toplotni vzorec, ki ga človek oddaja, je specifičen za vsakega posameznika in ga lahko zajamemo z infrardečo kamero. To omogoča prikrito prepoznavo, saj sistem prepoznavne na osnovi termografije ne potrebuje kontakta z osebo, ki jo želimo prepoznati, in je kot takšen nevsiljiv. Težava je lahko zajem termografske slike v nekontroliranem okolju, npr. v okolju, kjer nastaja toplota kot pri grelcih prostorov ali avtomobilskih izpustih, kjer je toplota v bližini človekovega telesa, ki ga želimo prepoznati. Podobna tehnologija se uporablja pri skeniranju zadnjega dela stisnjene pesti, na podlagi katere se ugotavlja razporeditev strukture ven na rokah. Ker so infrardeči senzorji dokaj dragi, to onemogoča širšo uporabo termografov za namen identifikacije oseb.

Slika 2.2: Primer termografije obraza



Vir: Fine Art America (2017).

5. Prstni odtis: Uporaba prstnega odtisa za identifikacijo je v uporabi že stoletja. Prstni odtis je vzorec izboklin in vdolbin na površini prsta, ki se formira v prvih sedmih mesecih razvoja zarodka. Prstni odtis je unikatna značilnost vsake osebe, saj so tudi prstni odtisi dvojčkov različni. Ker je cena čitalnikov prstnih odtisov z razvojem tehnologije postala vedno nižja, je to vplivalo tudi na to, da so čitalniki prisotni v vedno več modelih mobilnih telefonov, tablicah in prenosnih računalnikih. Natančnost trenutno prisotnih čitalnikov prstnih odtisov je primerna za uporabo v sistemih za preverjanje, ki vključujejo nekaj sto ljudi. Uporaba več prstnih odtisov ene osebe pa omogoča uporabo sistemov za prepoznavanje tudi v velikem obsegu, ki lahko vsebujejo bazo več kot milijon uporabnikov. Trenutno največja težava uporabe prstnih odtisov za prepoznavo v tako velikem obsegu je moč računalnika, saj je to izredno zahtevna računalniška operacija. Omejitve lahko predstavljajo tudi razni dejavniki, kot so določene genske bolezni, staranje, okolje in delo, ki v nekaterih primerih vplivajo na to, da je odvzem prstnega odtisa nemogoč.

Slika 2.3: Prstni odtis

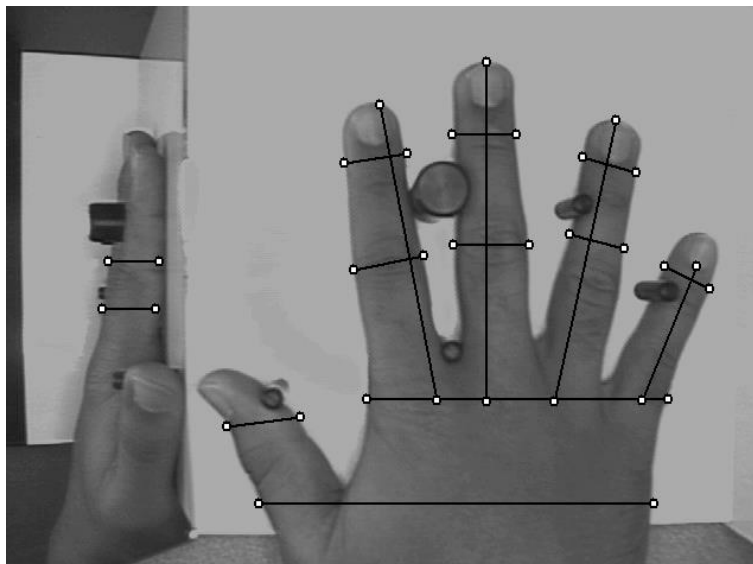


Vir: Winsupersite (2017).

6. Geometrija dlani in prstov: Sistemom, ki delujejo na podlagi prepoznave dlani, predstavljajo osnovo številne meritve človeške roke, kot so oblika ali velikost dlani ter dolžina in debelina prstov. Tehnika prepoznavanja na podlagi dlani je enostavna in relativno lahka za uporabo, zato so komercialni sistemi, ki temeljijo na prepoznavi geometrije dlani, nameščeni na številnih lokacijah po svetu. Ker geometrija dlani in prstov ni znana kot zelo razločevalna tehnika, njena uporaba ni primerna v sistemu, kjer želimo iz velike množice prepoznati posameznika. Prav tako se geometrija roke z rastjo spreminja. Tudi nakit in določene bolezni, kot je npr. rahitis, lahko predstavljajo izziv pri določanju točne geometrije dlani. Oviro predstavlja tudi fizična velikost teh

sistemov, saj zaradi velikosti niso uporabni za vgradnjo v manjše naprave, recimo prenosnike ali tablične računalnike.

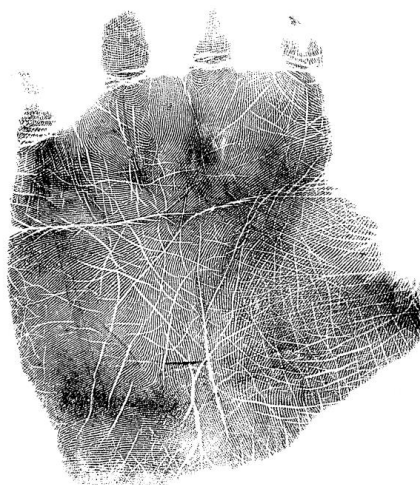
Slika 2.4: Geometrija dlani



Vir: 360biometrics (2017).

7. Odtis dlani: Kakor prstni odtis, tudi odtis dlani vsebuje določen vzorec izboklin in vdolbin, ki se pojavijo na njej. Ker je velikost dlani večja kot velikost prsta, je pričakovano, da bo odtis dlani bolj razločevalna lastnost od prstnega odtisa. Omejitev uporabe sistemov za skeniranje dlani je velikost skenerjev, saj so ti precej večji od čitalcev prstnih odtisov.

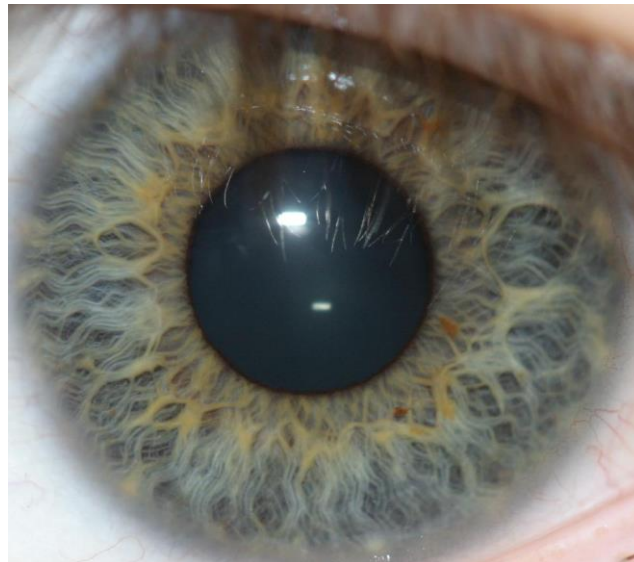
Slika 2.5: Odtis leve dlani



Vir: Wikimedia commons (2017).

8. Šarenica oz. iris: Šarenica oz. iris je po SSKJ sprednji, barvasti del žilnice za roženico. Njena tekstura vzorcev se začne razvijati že v obdobju razvoja fetusa in se stabilizira v prvih dveh letih življenja. Vzorec nato ostane vse življenje nespremenjen. Kompleksna tekstura šarenice nosi izredno značilno informacijo, ki je uporabna za prepoznavo. Natančnost in hitrost trenutno razvitih sistemov za prepoznavanje na podlagi šarenice je obetajoča in primerna za uporabo v sistemih za množični nadzor. Vse šarenice ljudi se med seboj razlikujejo, kot je to v primeru prstnega odtisa, in so različne tudi pri dvojčkih. Prav tako je izredno težko kirurško spremeniti strukturo šarenice in hkrati tudi izredno enostavno prepoznati umetno (npr. kontaktne leče). Tudi sistemi za skeniranje šarenice postajajo vedno bolj uporabniško prijazni in cenovno dostopni.

Slika 2.6: Šarenica oz. iris



Vir: Wikimedia commons (2017).

9. Očesna mrežnica: Ožilje očesne mrežnice ima bogato strukturo in naj bi bilo različno pri vsakem človeku. Očesna mrežnica trenutno velja za najbolj varno biometrično značilnost, saj je ni enostavno spremeniti ali replicirati. Postopke pridobitve slike očesne mrežnice poteka tako, da oseba pogleda v poseben okular in se osredotoči na specifično točko vidnega polja, kjer naredi vnaprej določen posnetek dela njenega ožilja. Ker postopek vključuje sodelovanje osebe, njen kontakt z okularjem in zavestno odločitev za sodelovanje v procesu skeniranja, to negativno vpliva na sprejemanje javnosti za njeno širšo uporabo.

Slika 2.7: Očesna mrežnica



Vir: Ocular Albinism (2017).

10. Vonj: Znano je, da ima vsaka oseba značilen vonj, ki je različen po kemijski sestavi in se ga lahko uporabi za prepoznavo. Prepoznavanje deluje na način, da je zrak z vonjem določene osebe vpihan v serijo različnih kemijskih senzorjev, ki določijo njegovo sestavo. Ni znano, če je možno zaznati spremembo vonja nekoga, ne glede na uporabo dezodoranta in prisotnosti različnih kemijskih sestav v okolici.

2.2.1. Vedenjske značilnosti

1. Gibanje (način hoje): Način hoje je kompleksna spatio-temporalna biometrična telesna značilnost. Je vedenjska značilnost, ki se lahko spreminja, še posebej skozi dolgo obdobje, zaradi spreminjanja teže, večjih poškodb sklepov ali možganov, vinjenosti. Način, na katerega hodimo, ni zelo značilna lastnost vsake osebe, ampak je dovolj nepristranska za uporabo pri prepoznavanju v nekaterih manj zaščitene primerih. Ker sistemi, ki delujejo na osnovi načina hoje, uporabljajo del hoje posameznika, posnete na video, ter beležijo več različnih gibov vsakega sklepa, je postopek obsežen in računsko zahteven.
2. Tipkanje: Način tipkanja je vedenjska biometrika, kjer lahko med posamezniki opazimo velike razlike v vzorcih tipkanja. Tipkanje sicer ne velja za unikatno biometrično značilnost vsakega posameznika, vendar nudi dovolj razločevalno informacijo, na podlagi katere lahko potrdimo identiteto nekoga.
3. Lastnoročni podpis: Tudi podpis je ena izmed biometričnih značilnosti vsakega posameznika. Čeprav je za preverjanje podpisa potrebna fizična prisotnost in privoljenje uporabnika za sodelovanje, je ta lastnost postala splošno sprejeta pri vladnih, pravnih in

poslovnih postopkih kot metoda verifikacije. Podpis je vedenjska značilnost, ki se spreminja skozi obdobje in nanjo vplivajo fizični in emocionalni dejavniki podpisnika. Prav tako je podpis mogoče ponarediti s strani profesionalnih ponarejevalcev.

4. Glas (govor): Govor je kombinacija fizioloških in vedenjskih biometrik. Posebnost posameznikovega glasu temelji glede na obliko in velikost organov, ki reproducirajo zvok (vokalnih poti (angl. *vocala tracts*), ust, nosne votline in ustnic). Te fiziološke karakteristike se pri posamezniku ne spreminjajo za razliko od vedenjskih karakteristik, ki se skozi čas spreminjajo zaradi staranja, zdravstvenih razlogov (npr. prehlada), čustvenega stanja itd.

3 ZGODOVINA BIOMETRIJE IN AVTOMATIČNEGA PREPOZNAVANJA OBRAZOV

Ideja o prepoznavi unikatnih človekovih karakteristik za namen prepoznavne ni nova, saj so se odtisi dlani, stopala in prstov že od nekdaj uporabljali zaradi svojih edinstvenih značilnosti. Prvi dokazi o uporabi biometrije segajo 32.000 let v preteklost, kjer so prazgodovinski ljudje uporabljali odtise dlani za podpisovanje na svojih slikah na stenah jam (Clottes 2002). Prav tako so Babilonci za podpisovanje sklenjenih kupčij uporabljali prstne odtise (Bucholtz in Davis 2015).

Pionir na področju uporabe biometrije je bil Alphonse Bertillon, biometrični raziskovalec in vodja oddelka za identifikacijo kriminalcev policije v Parizu. Leta 1882 je policijsko varnostni službi predstavil sistem merjenja številnih telesnih mer, ki je kmalu postal metoda za prepoznavanje storilcev kaznivih dejanj (Kindt 2013, 17). Čeprav je postajala njegova metoda vedno bolj popularna, jo je počasi začela nadomeščati bolj praktična in napredna metoda prepoznavanja prsnih odtisov – daktiloskopija.

Prvi primer njene uporabe je znan iz leta 1892, ko je Juan Vucetich, načelnik policijske postaje v La Plati, v Argentini, z njeno pomočjo rešil prvi zločin. Londonska policija Scotland Yard je kmalu prepoznala prednosti in uspehe uporabe daktiloskopije pri prepoznavi zločincev, ter jo začela uporabljati leta 1901, ko so vpeljali prvi sistem indeksacije prstnih odtisov. Uporaba prstnih odtisov se je tako začela hitro širiti in je bila do leta 1920 uporabljena po skoraj celem svetu.

Zaradi vedno večje popularnosti se je kmalu pojavila ideja po vpeljavi evidentiranja prstnih odtisov storilcev kaznivih dejanj, ki bi jih bilo možno primerjati s tistimi na mestu zločina. Veliko je pri tem pripomogel razvoj računalniške tehnologije. Tako je podjetje Printrak leta 1974 razvilo sistem za avtomatsko identifikacijo prstnih odtisov – AFIS (angl. *automated fingerprint identification system*). Prvi ga je aktivno začel uporabljati Zvezni preiskovalni urad Združenih držav Amerike (FBI).

Z razvojem računalniške tehnologije se je pojavilo tudi zanimanje za razvoj avtomatskega sistema prepoznavanja oseb na podlagi obraza. Obraz je namreč ena izmed najstarejših in najbolj osnovnih karakteristik, ki jo uporabljamo ljudje za prepoznavanje. Eden prvih

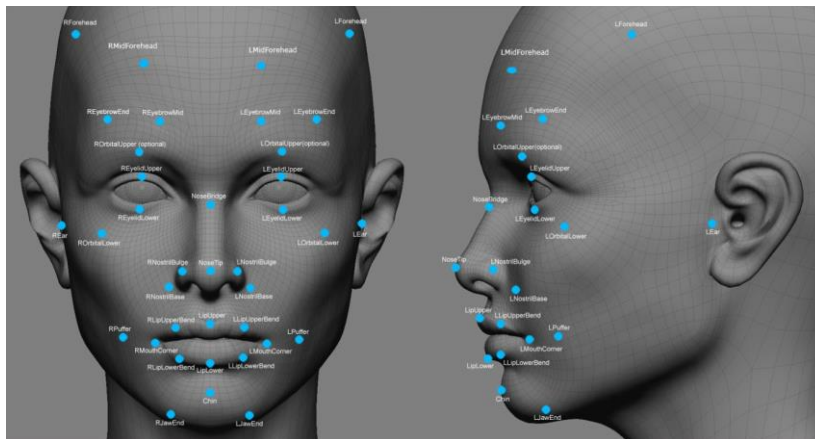
raziskovalcev na tem področju je bil Woodrow W. Bledsoe, ki je leta 1960 skupaj s Helen Chann in Charlesom Bissonom ustanovil podjetje Panoramic Research Inc. Podjetje je sodelovalo z ameriškim uradom za obrambo in več neimenovanimi obveščevalnimi službami. Rezultat sodelovanja je bil razvoj prvega pol-avtomatičnega sistema za prepoznavanje obrazov leta 1964, ki je iskal ujemanja glede na ročno označene obrazne značilnosti na slikah. Zanimivo je, da je že takrat Bledsoe prepoznal težave sistemov za prepoznavanje obrazov, s katerimi se še danes srečujejo – spremembe v osvetlitvi in postavitvi obraza, obrazne mimike ter staranje (Pabbaraju in Puchakayala 2010, 2).

Leta 1974 je Takedo Kanade razvil prvi sistem za avtomatsko prepoznavanje obrazov. Ta je temeljil predvsem na prepoznavanju obraza na osnovi geometričnih razmerij, kot sta dolžina in koti med glavnimi deli obraza (angl. *landmarks*). Razvoj avtomatičnih sistemov za prepoznavanje obrazov je do leta 1990 miroval, dokler nista Sirovich in Kirby v svojem delu za prepoznavanje uporabila metodo glavnih komponent (Li in Jain v Li in Jain 2011, 2), ki je obraz smatrala kot dvodimenzionalno (2D) razporeditev točk v prostoru.

Drugi pomembni mejniki prepoznavanja obrazov so: uporaba metode Fisherjevih obrazov, ki v prvem postopku prepoznavanja uporabi metodo glavnih komponent ter nato v drugem linearno diskriminantno analizo, s čimer se doseže večja učinkovitost; uporaba lokalnih filtrov, kot so Gaborjevi filtri, s katerimi se doseže bolj učinkovito prepoznavanje obraznih posebnosti; in uporaba AdaBoost metode strojnega učenja za prepoznavanje obrazov v realnem času (Li in Jain v Li in Jain 2011, 2).

4 DELOVANJE SISTEMOV ZA PREPOZNAVANJE OBRAZOV

Slika 4.1: Ključne obrazne točke



Vir: Techclinch (2017).

Sistemi za prepoznavanje obrazov delujejo v enem ali obeh načinih (Li in Jain v Li in Jain 2011, 2): (1) preverjanje obraza (ali avtentifikacija) in (2) identifikacija obraza (ali prepoznavanje). Preverjanje obraza pomeni primerjavo obraza ena na ena, kar pomeni, da sistem primerja poizvedovalni obraz (angl. *query face*) z vpisnim obrazom (angl. *enrollment face*). Identifikacija obrazov pa vključuje ujemanje ena proti mnogo, ki primerja poizvedovalni obraz z več obrazi v vpisni bazi.

Osnovo vsem sistemom prepoznavanja obrazov predstavlja zaznavanje obrazov (angl. *face detection*). Hjelmås in Low (2001, 236) pravita, da je zaznavanje obrazov nujen prvi korak vseh sistemov za prepoznavanje obrazov, katerega namen je lokalizacija in izločanje obraza iz ozadja. Od njegove zanesljivosti je odvisna učinkovitost in uporabnost celotnega sistema za prepoznavanje obrazov (Li in Wu v Li in Jain 2011, 277).

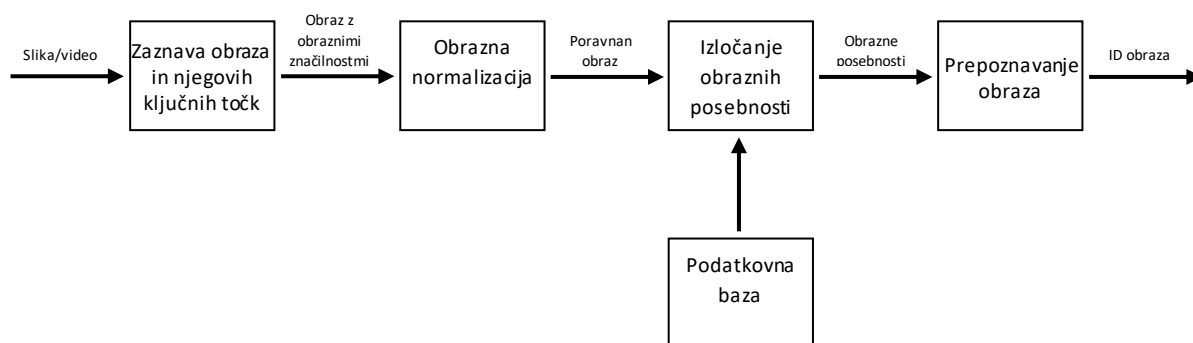
Ideja delovanja sistemov za prepoznavanje obrazov je izredno preprosta. Na določenem območju, ki ga želimo nadzirati, postavimo video kamere, preko katerih nadziramo mimoidoče ljudi, npr. v prostoru za vkrcanje na letališču, centru mesta, podzemni/železniški postaji. Namesto da je v nadzorni sobi neprestano prisotnih več ljudi, ki nadzirajo množico, lahko za te namene uporabimo računalnik, ki to počne samodejno namesto nadzornikov in v primeru pozitivne identifikacije osebe to sporoči z alarmom ali opozorilom. Pri tem je potrebno predpostaviti, da za prepoznavo uporabljamo bazo oseb, ki jih želimo prepoznati z njihovimi metapodatki. Nadzornik nato ob alarmu dodatno preveri sliko prepoznane osebe s sliko osebe

s seznama in na njeni podlagi ter podlagi priloženih metapodatkov o tej osebi ustrezno ukrepa (Bowyer 2004, 10).

Sistemi za prepoznavanje obrazov gredo, tako kot ostale biometrične metode, pri identifikaciji skozi štiri stopnje delovanja: 1. vključitev, 2. hramba, 3. prevzem (angl. *aquisition*) in 4. ujemanje (Nlets – the International Justice and Public Safety Network 2011, 11–12). V tem delu so avtorji raziskovali uporabo sistemov za prepoznavanje obrazov na terenu, in sicer pri organih pregona:

1. Vključitev: V prvi fazi sistem za prepoznavanje obrazov pridobi sliko obraza in izmeri njegove značilne karakteristike, kot so razlika med očmi, širina nosu, globina očesnih zrkel itd. Te točke so znane kot stičiščne točke (angl. *nodal points*), ki jih ima vsak človeški obraz in predstavljajo osnovo programom za prepoznavanje obrazov. Različni programi lahko uporabljajo različne stičiščne točke za prepoznavo obraza. Stičiščne točke se nato izvečejo iz slike obraza in na osnovi algoritma transformirajo v unikatno datoteko, imenovano vzorec (angl. *template*). Ta predstavlja sklop podatkov o unikatnih značilnostih osebe, ki jo želimo prepoznati.
2. Hramba: Vzorci se nato shranijo v bazo podatkov za potrebo ponovne prepoznave v prihodnosti.
3. Prevzem: Za namen identifikacije osebe sistem nato primerja pridobljeni vhodni biometrični vzorec osebe, ki jo želimo prepoznati, z biometričnim vzorcem oseb, shranjenih v bazi.
4. Ujemanje: V zaključni fazi se nato uporabniku sistema za prepoznavanje obrazov prikažejo slike potencialnih kandidatov iz baze, ki odgovarjajo osebi, ki jo želimo identificirati.

Shema 4.1: Tokokrog sistemov za prepoznavanje obrazov



Vir: Li in Jain v Li in Jain (2011, 4).

Tokokrog prepoznavne sistemov za prepoznavanje obrazov je sestavljen iz štirih stopenj (Li in Jain v Li in Jain 2011, 3–4):

1. Zaznava obraza: V tej stopnji program prepozna obraz in ga izloči iz slike. V primeru videa mora biti obraz prepoznan skozi več slikovnih okvirjev (angl. *frames*), z uporabo tehnologije za sledenje obrazom. Tako se določi groba ocena lokacije in velikosti obraza, medtem ko se s prepoznavanjem značilnih obraznih oznak (angl. *face landmarking*) določijo oči, nos, usta in ostali značilni obrazni orisi.
2. Normalizacija obraza (angl. *face normalization*): V naslednji stopnji se izvaja geometrijska in fotometrična normalizacija obraza. To je izredno pomemben korak, saj se od najsodobnejših metod za prepoznavanje obrazov pričakuje, da bodo prepoznale obraz ne glede na njegovo postavitev ali osvetlitev. Postopek geometrijske normalizacije preoblikuje obraz v standardni okvir z rezanjem njegovih delov, pri čemer se uporablja metoda zvijanja kot tudi preobrazbe za bolj izdelano geometrijsko normalizacijo. Fotometrična normalizacija pa je metoda normaliziranja obraza na osnovi osvetlitve in sivine (angl. *gray scale*).
3. Izločanje obraznih značilnosti: Je izvedeno na normaliziranem obrazu z namenom izločitve pomembnih podatkov, ki so uporabni pri razlikovanju obrazov različnih ljudi. Izločene obrazne značilnosti se uporabijo v naslednjem koraku prepoznavne obrazov. Natančnost sistema za prepoznavanje obrazov je močno odvisna od obraznih posebnosti, ki se izluščijo iz obraza in s katerimi nato obraz tudi predstavimo.
4. Prepoznavanje obraza: Cilj te stopnje je priti do informacije, kateri osebi v podatkovni bazi vhodni obraz pripada. Izločene obrazne posebnosti se primerjajo z enim ali več obrazov, prisotnih v dani bazi. Če je rezultat ujemanja nad postavljeno mejo ujemanja, lahko z določeno gotovostjo potrdimo njegovo identiteto oz. jo v nasprotnem primeru zavržemo.

5 PODROČJA UPORABE SISTEMOV ZA PREPOZNAVANJE OBRAZOV

Sistemi za prepoznavanje obrazov so v zadnjih letih doživeli velik raziskovalni preporod in razvoj, saj so v njih prepoznale potencial številne vlade kot tudi komercialne aplikacije. Trije glavni dejavniki, ki so vplivali na to, da je prepoznavanje obrazov postala pomembnejša biometrična metoda, so (Li in Jain v Li in Jain 2011, 1):

1. razvoj tehnologije, ki je pripeljal do te mere, da smo dnevno povezani v svetovni splet z napravami, ki omogočajo zajemanje slik, kot so npr. nadzorne kamere, fotoaparati in mobilni telefoni;
2. dostopnosti velike količine slik obrazov na spletu in
3. rastoče potrebe po večji varnosti.

Glede na Wagner in drugi (2012, 272) se sistemi za prepoznavanje v grobem delijo na uporabo v dveh kategorijah:

- v manj zahtevnih aplikacijah, kot so spletni iskalniki slik in programi za družinsko razvrščanje slik (npr. Google Picasa, Microsoft photo galery, Apple iPhoto) in
- v sistemih za prepoznavanje teroristov in nadzoru množic.

Predvsem na področju prepoznavanj teroristov in nadzora množic je v zadnjem času prevladovalo raziskovanje prepoznavanja obrazov. Kljub temu pa obstaja še vedno precej aplikacij za prepoznavanje obrazov, kjer uporabniki želijo visoko stopnjo učinkovitosti prepoznavanja, vendar so njihovi uporabniki zavezniki sistema in ne njegovi nasprotniki. Primeri takšnih aplikacij so npr. kontrola dostopa v zaščitnih ustanovah, računalniški sistemi, avtomobili, bankomati itd.

Jain in drugi (2004, 10–11) delijo uporabo biometričnih metod in posredno obrazno prepoznavo v tri večje skupine:

- komercialna uporaba: prijava v računalnik, zaščita elektronskih dokumentov, e-poslovanje, dostop do interneta, bankomati, kreditne kartice, fizična kontrola dostopa, mobilni telefoni, tablice, medicinski kartoni in učenje na daljavo;
- vladna uporaba: osebne izkaznice, prevzgojni objekti, voziške izkaznice, socialno varstvo, plačevanje izdatkov (angl. *welfaredisbursement*), mejna kontrola, kontrola potnih listov;
- forenzična uporaba: identifikacija trupel, kazenske preiskave, identifikacija teroristov, določanje starševstva, iskanje pogrešanih otrok.

10 različnih področij uporabe sistemov za prepoznavanje obrazov so v svojem delu podrobno predstavili tudi Huang in drugi (v Li in Jain 2011, 613):

1. Identifikacija obraza: Tem sistemom predstavlja osnovo za identifikacijo oseb slika obraza, za kar je potrebna prisotnost osebe, ki jo želimo identificirati.
2. Kontrola dostopa: Pri tem gre za uporabo sistemov za namen kontrole dostopa v prostore oz. v računalniške sisteme. Takšni sistemi so zaradi večinoma manjše podatkovne baze ljudi in uporabe slik, ki so navadno zajete pod prilagojenimi in istimi pogoji, zelo učinkoviti in uspešni ter lahko nadomestijo trenutno najbolj razširjeno in uporabljeno metodo za kontrolo dostopa – uporabo uporabniškega imena in gesla oz. samo gesla.
3. Varnost: Uporaba sistema za prepoznavanje obrazov na letališčih. Prednost uporabe na letališčih je ta, da je mogoče v veliki meri kontrolirati postavitev in osvetlitev obraza, vendar kljub temu še vedno ni mogoče zagotoviti majhnega števila napačno prepoznanih oseb. Podobni sistemi se uporabljajo tudi na stadionih za preverjanje obiskovalcev.
4. Nadzor: Nadzorne sisteme prav tako pesti ista težava kot varnostne sisteme, saj na prepoznavo oseb prav tako vplivajo različni dejavniki, zaradi katerih je njihova uporaba otežena. Te težave so vezane predvsem na različne svetlobne pogoje, postavitve obrazov itd. Njihov namen je predvsem nadzor množice ljudi z namenom zmanjšanja kriminala, saj lahko s takšnimi sistemi v množici ljudi iščejo znane in aktualne kriminalce, spolne iztirjence, pobegle in pogrešane osebe, teroriste ...
5. Pametne kartice: Razvoj pametnih kartic je prišel tako daleč, da jih lahko opremimo tudi z biometričnimi podatki osebe. Tako lahko postanejo vezni člen med virtualnim in fizičnim svetom. S tem, ko je na pametni kartici možno imeti biometrične podatke in podatke o prstem odtisu, lahko sistemi hitreje in učinkoviteje preverjajo identiteto uporabnikov.
6. Organi pregona: S pomočjo sistema, ki vsebuje tehnologijo prepoznavanja obrazov in informacije o kriminalcih, lahko preiskovalci hitro najdejo in identificirajo osumljene osebe. Tako policistom več ni potrebno zapravljati časa za identifikacijo osebe, saj lahko to storijo na mestu. To lahko poteka tako, da policist zajame sliko osumljenca in jo primerja s tistimi v bazi podatkov.
7. Zbirke digitalnih fotografij: Metoda prepoznavanja obrazov se lahko uporablja tudi za namene preiskovanja podatkovnih zbirk, ki vsebujejo tako slike obrazov kot ostale

elemente na slikah. Zaradi velikega števila slik je navadno uspešnost teh sistemov relativno nizka, predvsem zaradi različnih pogojev zajema slik.

8. Upravljanje z večpredstavnostnimi vsebinami: Gre za iskanje, sledenje in prepoznavanje obrazov pri večpredstavnostnih vsebinah, kot so npr. videi. Tako lahko video vsebine razvrščamo in omogočimo njihovo pregledovanje. Poglavitna težava tega je, da navadno nimamo vnaprej podane galerije slik in tako ne vemo, kdo je oseba na videu, zaradi česar morajo metode najdeno osebo poiskati iz same vsebine.
9. Interakcija med človekom in računalnikom: Ideja je, da bi običajno interakcijo ljudi z računalnikom, ki poteka preko miške in tipkovnice ali dotika, zamenjali različni človeški deli telesa (npr. glava). Torej bi interakcija lahko potekala s sledenjem, analizo mimike obraza, sintezo in animacijo glave. Glavni cilj takšne interakcije z računalnikom je prepoznavanje in razumevanje kretenj človeka.
10. Druga področja uporabe: Sistemi za prepoznavanje obrazov se uporabljajo tudi pri verifikaciji oseb na starinskih slikah ali za namene prenosa obrazne slike, kjer lahko s pomočjo določenih parametrov zakodiramo in jo pošljemo drugi osebi, zaradi česar nam ni potrebno pošiljati celotne slike. To je predvsem uporabno za prenose slik pri nizkih pasovnih širinah (npr. prenosi podatkov preko brezžičnih mobilnih omrežij).

Divyarajsinh in Brijesh (2013, 84–86) sta v članku *Face Recognition Methods & Applications* opisala 6 področij uporabe:

1. Prepoznavanje obraza: Sistemi za prepoznavanje obrazov prepoznajo ljudi po slikah njihovih obrazov. Z njimi se potrjuje navzočnost določene osebe, namesto da se to počne npr. s preverjanjem veljavnih osebnih izkaznic, ključev ali preverjanjem osebne identifikacijske kode oz. gesla. Primer takšne uporabe je mednarodni volilni registracijski sistem, ki se uporablja za namen odprave dvojnikov v primerih, kjer je bilo istim osebam dodeljenih več identifikacijskih števil. Sistem za prepoznavanje obrazov je neposredno primerjal obraze volivcev, namesto da bi za primerjavo uporabljal ID številke za razlikovanje med njimi. V primeru, ko sta si bila dva obraza zelo podobna, je bilo potrebno osebno preveriti, ali sta osebi bili resnično različni ali ne.
2. Kontrola dostopa: Pri večini primerov je skupina ljudi, kjer uporabljamo sisteme za prepoznavanje obrazov, majhna. Takšni primeri so kontrola dostopa v pisarnah ali za prijavo v računalnik. Slike, s katerimi primerjamo osebe, so navadno posnete pri naravnih razmerah, torej recimo frontalno in pri notranji osvetlitvi. Posledično je zato tudi natančnost takšnih sistemov zelo velika. Primer takšne uporabe je npr. uporaba

tehnologij za prepoznavanje obrazov pri računalniških monitorjih, ki neprestano preverjajo, kdo je pred računalnikom. To omogoča uporabniku, da lahko zapusti delovno mesto, ne da bi mu pri tem bilo potrebno zapreti datoteke in ga zakleniti, saj se računalnik po prednastavljenem času sam zaklene in tako zakrije mogoče občutljive podatke.

3. Varnost: Na letališčih je danes bolj kot kadarkoli pomembna varnost. To velja tako za uslužbence letališča kot potnike. Zato so sistemi za prepoznavanje obrazov prisotni v vedno več letališčih po svetu. Oktobra 2001 je bila na letališču Fresno Yosemite international uvedena Viisage-ova tehnologija prepoznavanja obrazov. Sistem je narejen tako, da opozori letališke varnostne delavce, ko prepozna znane teroristične osumljence na kontrolnih točkah letališča.
4. Iskanje po slikovnih bazah: Npr. po bazi voznških dovoljenj, prejemnikov prejemkov, pogrešanih oseb in otrok, migrantov, policijskih prekrškarjev (angl. *police bookings*).
5. Splošna prepoznavna identitete: Registracija volivcev, bančno poslovanje, elektronske reklame, identifikacija novorojenih, osebnih izkaznic, potnih listov, identifikacija zaposlenih.
6. Nadzor: Tako kot imajo varnostni sistemi na javnih mestih nizko stopnjo identifikacije, jih imajo tudi sistemi za nadzor. Slaba osvetlitev, lega obraza in ostali prisotni dejavniki zavirajo razmah sistemov prepoznavanja obrazov za nadzor množice. Vseeno je takšen sistem prisoten v centru Londona na območju Newham Borough, kjer je prisotnih 300 nadzornih kamer. Mestne oblasti trdijo, da je v tem predelu stopnja kriminala padla za 34 %. Podoben sistem je prisoten tudi v Birminghamu v Angliji.

Zhao in drugi (2003, 400) so v svojem delu predstavili štiri področja uporabe tehnologij za prepoznavanje obrazov in najbolj pogoste primere uporabe (glej tabelo 5.1).

Tabela 5.1: Področja uporabe tehnologije za prepoznavanje uporabe in primeri uporabe

Področje	Primer uporabe
Zabava	video igre, virtualna resničnost, programi usposabljanja
	interakcija med človekom in robotom, interakcija med človekom in računalnikom
Pametne kartice	voznške izkaznice, članstvo v programih
	priseljavanje, osebne izkaznice, potni listi, registracija volivcev

Informacijska varnost	starševski nadzor televizije, prijava v osebne naprave, prijava na namizje
	zaščita aplikacij, podatkovnih baz, kriptiranje datotek
	intranet zaščita, dostop do interneta, medicinski zapisi, varovanje terminalov za trgovanje
Organi pregona in nadzor	napredni video nadzor, nadzor nad televizijo zaprtega kroga (angl. <i>CCTV control</i>)
	nadzor portalov, analize po dogodkih
	kraje, sledenje in preiskovanje osumljencev

Vir: Zhao in drugi (2003, 400).

Čeprav je v teoriji mogoče zaznati več različnih namenov uporabe, je fokus mojega magistrskega dela na uporabi sistemov za prepoznavanje obrazov za komercialno uporabo, ki so vključeni v programe in aplikacije, ki jih ljudje vsakodnevno zavestno uporabljajo, kot so recimo Facebook, Snapchat itd.

6 OMEJITVE SISTEMOV ZA PREPOZNAVANJE OBRAZOV

Čeprav imajo tehnologije za prepoznavanje obrazov velik potencial, je obseg njihove uporabe še vedno precej omejen, še posebej če so slike zajete v nenaravnih pogojih (Li in Jain v Li in Jain 2011, 2). Po Huang in drugi (v Li in Jain 2011, 635) obstajata predvsem dve veliki omejitvi, ki vplivata na učinkovitost prepoznavanja in jih je potrebno odpraviti, da se bo lahko njihova uporaba razširila:

1. Tehnologije za prepoznavanje obrazov še vedno niso dovolj robustne za uporabo v nenaravnih okoljih, saj stopnja natančnosti v nenadzorovanih okoljih ni dovolj sprejemljiva, da bi jih lahko uporabljali v večjem obsegu (za npr. varnostne namene). Razlike v spremembi osvetlitve, različne postavitve obraza in čas, ki je potreben za primerjavo preučevane slike s slikami v galeriji, še dodatno zmanjšujejo učinkovitost sistemov za prepoznavanje obrazov. Te dejavnike so ocenili v raziskavi FRVT leta 2002 in leta 2006, kjer so testirali ene izmed takrat najbolj razvitih sistemov za prepoznavanje obrazov. Ugotovitve so pokazale, da je bil v letih med raziskavama narejen izjemen preskok pri prepoznavanju obrazov, saj se je odstotek prepoznavne dvignil iz 80 % na 99 % uspešnost, ob 0,1 % deležu napačno prepoznanih oseb (angl. *false alarm rate*). Zaključili so, da je takšen sistem morda bolj primeren za uporabo v okolju, kjer je baza uporabnikov velika le nekaj sto ljudi, gotovo pa sistema s takšnim deležem napačno prepoznanih oseb ni možno uporabiti na letališčih, kjer je število oseb, ki jih je potrebno prepoznati, precej večje.

Slika 6.1: Primer različne osvetlitve obraza



Vir: Illinois Image Formation and Processing (2017).

Slika 6.2: Primer različne postavitve obraza



Vir: Universitat Politècnica de Catalunya (2017).

2. Postavitve sistemov za nadzor, ki temeljijo na prepoznavanju obrazov, prav tako vzbuja skrb o mogoči zlorabi zasebnosti. Tako npr. Ameriška zveza za državljanske svoboščine (angl. *American Civil Liberties Union*) nasprotuje uporabi sistemov za prepoznavanje obrazov na letališčih zaradi neučinkovitosti in varstva zasebnosti. Po njihovem mnenju omenjene tehnologije prinašajo nevarnost, da se bo njihova uporaba razširila v orodje za vohunjenje nad državljani na javnih prostorih.

Zhao in drugi (2003, 440) prav tako vidijo osvetlitev in postavitev obraza kot dva pomembna dejavnika, ki vplivata na njihovo zanesljivost. Raziskava, ki so jo izvedli v delu *Face Recognition: A Literature Survey*, je pokazala, da v obvladovanih okoljih omenjena dejavnika nimata vpliva na delovanje, medtem ko je prepoznavanje obrazov v nekontroliranih okoljih še vedno velik izziv. Te težave so neizogibne, ko govorimo o prepoznavi obrazov iz slik, pridobljenih iz posnetkov nadzornih kamer v nenadzorovanih okoljih.

Po Iwai (v Horiuchi in Hada 2013, 2) obstaja sedem tehničnih izzivov, ki jih je potrebno pri prepoznavanju obrazov odpraviti, preden bo mogoče to orodje učinkovito uporabljati:

1. spremembe obrazne postavitve, velikost in različni koti slikanja,
2. spreminjanje izrazov na obrazu,
3. slabo okolje, kot je npr. slaba osvetlitev,

4. prepoznavanje v realnem času,
5. staranje,
6. modni dodatki, kot so očala,
7. prikrite slike (angl. *disguised photo*).

7 ZAKONSKI IN ETIČNI VIDIKI UPORABE TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZOV

Pravna vprašanja, ki se pojavljajo ob uporabi biometrije, se nanašajo na zasebnost, samostojnost, privolitev (angl. *informed consent*), zaupnost in svobodo. Hkrati se ob njihovi uporabi poraja tudi vprašanje etičnosti (House of Commons, Science and Technology Committee 2015).

Dejstvo je, da je preverjanje identitete sestavni del vsakega v sodobnem življenju. Naj bo to vstop v službo, prijava v internet ali polog gotovine. Neprestano se soočamo z zahtevo po preverjanju kdo smo. V večini primerov je namen preverjanja naše identitete ta, da z njim preprečimo nezakonite dejavnosti ali preprečimo dostop do nečesa zaščenega. V današnjem globaliziranem svetu, kjer smo z drugimi v interakciji tako v digitalnem kot fizičnem svetu, lahko naši osebni podatki enostavno potujejo skozi geografske meje, ne da bi pri tem vedeli kje so shranjeni in kdo jih hrani (House of Commons, Science and Technology Committee 2015, 5). Z vedno bolj razširjeno uporabo sistemov za prepoznavanje obrazov se namreč pojavlja vprašanje varnosti. Zato je izredno pomembno področje varovanja osebnih biometričnih podatkov njihova hramba in zaščita, saj se lahko podatki zlorabijo in uporabijo za sledenje posameznikom proti njihovi volji (Sadeghi in drugi 2009, 230).

7.1 Varovanje osebnih podatkov

V Sloveniji je varovanje osebnih podatkov definirano z Zakonom o varstvu osebnih podatkov (ZVOP-1), ki je v veljavi od 1. 1. 2005, kjer so v 3. poglavju od 78. do 81. člena definirani biometrični ukrepi. Biometrični ukrepi glede na Zakon zajemajo dva različna načina (postopka) prepoznavanja posameznika (ZVOP-1, 78. člen):

1. identifikacija oz. prepoznavanje (Kdo sem?): v tem postopku se ugotavljajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija;
2. istovetnost oz. avtentikacija (Ali sem tisti, za katerega se predstavljam?): postopek, s katerim se primerjajo lastnosti posameznika, tako da se lahko preveri njegova identiteta oziroma istovetnost.

Po Zakonu je uporaba biometrije dovoljena le v naslednjih primerih:

- Javni sektor (ZVOP-1, 79. člen):

(1) Biometrijske ukrepe v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

(2) Ne glede na prejšnji odstavek se biometrijske ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja.

- Zasebni sektor (ZVOP-1, 80. člen):

(1) Zasebni sektor lahko izvaja biometrijske ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Biometrijske ukrepe lahko izvaja le nad svojimi zaposlenimi, če so bili predhodno o tem pisno obveščeni.

(2) Če izvajanje določenih biometrijskih ukrepov v zasebnem sektorju ni urejeno z zakonom, je upravljavec osebnih podatkov, ki namerava izvajati biometrijske ukrepe, dolžan pred uvedbo ukrepov posredovati državnemu nadzornemu organu opis nameravanih ukrepov in razloge za njihovo uvedbo.

(3) Državni nadzorni organ je po prejemu posredovanih informacij iz prejšnjega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometrijskih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se lahko podaljša za največ en mesec, če bi uvajanje teh ukrepov prizadelo več kot 20 zaposlenih v osebi zasebnega sektorja, ali če reprezentativni sindikat pri delodajalcu zahteva sodelovanje v upravnem postopku.

(4) Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe po prejemu odločbe iz prejšnjega odstavka, s katero je izvajanje biometrijskih ukrepov dovoljeno.

Glavni nadzornik na področju varovanja osebnih podatkov v Sloveniji je z novim zakonom postal Informacijski pooblaščenec, ki je med drugim zadolžen za:

- izvrševanje inšpekcijskega nadzora nad izvajanjem določb tega zakona in druge naloge po tem zakonu in drugih predpisih, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije (ZVOP-1, 37. člen); sodelovanje z državnimi organi, pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov, mednarodnimi organizacijami, tujimi

nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji ter drugimi organi in organizacijami glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov;

- opravljanje preventivnih inšpekcijskih nadzorov pri upravljalcih osebnih podatkov s področja javnega in zasebnega sektorja (ZVOP-1, 47. člen);
- vodenje in vzdrževanje registra zbirk osebnih podatkov in skrbi, da je register ažuren ter javno dostopen prek svetovnega spleta (ZVOP-1, 28. člen);
- vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (ZVOP-1, 64. člen).

Varovanje osebnih podatkov je opredeljeno tudi z najvišjim splošnim aktom, Ustavo, v 38. členu. V njej je zagotovljeno varstvo osebnih podatkov in prepoved njihove uporabe v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.

Na področju varovanja osebnih podatkov je pomemben tudi Zakon o elektronskih komunikacijah (ZEKOM-1), ki je stopil v veljavo 15. 1. 2013. Ta v svojem 145. členu definira splošne določbe o varnosti obdelave, po katerih morajo izvajalci javnih komunikacijskih storitev (operaterji) sprejeti ustrezne tehnične in organizacijske ukrepe za zagotovitev zavarovanja svojih storitev. Zagotoviti morajo, da ima dostop do osebnih podatkov njihovih strank le pooblaščen osebje za z zakonom dovoljene namene, varovati shranjene ali poslane osebne podatke pred nenamernim ali nezakonitim uničenjem, nenamerno izgubo ali spremembo ter nepooblaščenim ali nezakonitim shranjevanjem, obdelavo, dostopom ali razkritjem in zagotavljati izvajanje varnostne politike pri obdelavi osebnih podatkov. Na takšen način se omejijo tveganja, povezana z dejanji, storitvami ali izdelki, ki posegajo v tajnost, zaupnost in varnost elektronskega komunikacijskega omrežja ali elektronske komunikacijske storitve.

7.2 Zasebnost

Drugo pomembno področje uporabe biometričnih metod je vidik zasebnosti, saj je urbano okolje, tako privatno kot javno, vedno bolj prežeto z nadzornimi kamerami (Gray v Norris in Wood 2003, 314). Ločimo več vrst zasebnosti (Belsey 1992, 83):

1. Fizična oz. telesna zasebnost: Predstavlja prostor, v katerem lahko živimo, delujemo in se gibljemo, ne da bi nas pri tem drugi fizično omejevali.
2. Mentalna ali komunikacijska zasebnost: Je prostor, ki omogoča osebi, da je sama s svojimi mislimi in občutki, ki jih lahko poljubno zapisuje in posreduje želenim osebam, brez strahu po prisluškovanju ali drugim možnim oblikam vdora.
3. Informacijska zasebnost: Predstavlja zaščito osebnih podatkov, kot npr. podatkov o našem zdravju, zaposlitvi, finančnih podatkih ipd.

Z razvojem informacijske tehnologije in njeno sposobnostjo zbiranja, analiziranja in širjenja podatkov o posameznikih se je pojavila potreba po učinkoviti zakonodaji za zaščito zasebnosti (Banisar in Davies 1999, 4). Pomembni trendi, ki ogrožajo zasebnost, so po mnenju avtorja (prav tako, 5):

1. Globalizacija: Odstranjuje geografske meje pri pretoku podatkov.
2. Konvergenca tehnologij: Odstranjevanje tehničnih mej med različnimi tehnologijami, ki so vedno bolj interoperabilne in lahko medsebojno izmenjujejo in obdelujejo različne tipe podatkov.
3. Multimedialnost: Možnost združevanja podatkov in pretvarjanja v druge oblike.

V Sloveniji je področje zasebnosti opredeljeno z Ustavo, v II. poglavju Človekove pravice in temeljne svoboščine, v 35. in 37. členu:

- 35. Člen (varstvo pravic zasebnosti in osebnostnih pravic): zagotavljanje nedotakljivosti človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic.
- 37. Člen (varstvo tajnosti pisem in drugih občil): Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Področje zasebnosti je glede na Splošno deklaracijo človekovih pravic (angl. *Universal Declaration of Human Rights*), ki jo je sprejela in razglasila Generalna skupščina Združenih narodov 10. decembra 1948 z resolucijo št. 217 A (III), prav tako ena izmed temeljnih človekovih pravic. V 12. Členu Deklaracije namreč piše: Nikogar se ne sme nadlegovati s

samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju: EKČP), ki je bila sprejeta leta 1950 in temelji na Splošni deklaraciji človekovih pravic, v svojem 8. členu priznava pravico do spoštovanja zasebnega in družinskega življenja. V tem členu je zapisano, da ima vsakdo: »... pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi (EKČP 1950).« Podpis Konvencije in njena ratifikacija je ključna obveznost držav, ki si prizadevajo za članstvo v Svetu Evrope.

Področje zasebnosti je prav tako do nedavnega urejala Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Ta je bila razveljavljena 4. 5. 2016, ko je bila v Uradnem listu Evropske unije objavljena nova Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. 4. 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov). Uredba je začela veljati 25. 5. 2016, njene določbe pa se bodo morale neposredno uporabljati v vseh državah članicah v dveh letih.

8 DRUŽBENI VIDIK UPORABE TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZOV

Sistemi za obrazno prepoznavo so orodje za prepoznavanje in razvrščanje potencialno nevarnih ljudi v urbanem okolju. S svojo navzočnostjo povečajo in izostrijo naš pogled ter zavedanje v upanju, da bodo nadzorniki prepoznali grožnjo, preden bo ta postala realnost. Toda želja po zaščiti družbe pred nevarnostjo z uporabo tehnologij za prepoznavanje obrazov lahko povzroči do sedaj naslutene nevarnosti. Tehnologija za prepoznavanje obrazov je tako postala še dodatna dimenzija vladnega in policijskega nadzora.

Nadzor je močno orodje, s katerim lahko skrbimo za družbeno kontrolo, ki je z digitalizacijo bistveno pridobilo na moči, intenzivnosti in obsegu (Graham in Wood, 2003, 228). Ross pravi (Ross v Kovačič 2003, 19), da je družbeni nadzor pozitiven, saj lahko visoko stopnjo družbene organizacije dosežemo le z določeno stopnjo reda oz. nadzora. Prav tako življenje v skupnosti ni mogoče, če njeni posamezniki niso podvrženi organizaciji in samonadzoru (Cooley v Kovačič 2003, 19).

Drugačen pogled na nadzor imata Marx in Weber, ki v njem vidita sredstvo kontrole ljudi. Marx (1986) na družbeni nadzor gleda skozi ekonomske odnose med tistimi, ki imajo nadzor nad ekonomskimi viri (kapitalisti) in delavci. Kapitalisti želijo z nadzorom svojih delavcev doseči njihovo poslušnost in disciplino ter tako povečati proizvodnjo in zmanjšati stroške. Weberu pa je orodje nadzora predstavljala birokracija, ki s točno določenimi vlogami glede na hierarhijo, pravili delovanja, redno plačo, delitvijo nalog in neobremenjenosti z lastništvom sredstev (uradniki niso lastniki sredstev) povečuje učinkovitost organizacij pri doseganju njihovih ciljev (Weber 1981).

Na področju razumevanja nadzora je bil pomemben tudi filozof Michel Foucault (1984), ki pravi, da je v modernih družbah pogoj za nadzor disciplina, zato jih je poimenoval tudi "disciplinske družbe". Z disciplino se po njegovem mnenju izdelujejo "krotka telesa". Z disciplinskimi mehanizmi sodobne družbe se: »subtilno in posredno vsiljujejo normativno delovanje posameznikov in ker se za discipliniranje posameznikov uporablja nadzor, je po Foucaultu le-ta sredstvo podrejanja« (Kovačič 2003, 20).

Foucaultova študija discipline v moderni družbi je temeljila na načrtu zapor Panoptikon, ki ga je razvil Jeremy Bentham. Ta je britanski vladi leta 1791 predstavil arhitekturni osnutek popolnega zapor, ki paznikom omogoča asimetrični nadzor nad zaporniki. Temelji na nezaupanju, saj zaradi krožne oblike zgradbe in postavitve celic, zaporniki vidijo in posredno lahko nadzorujejo druge zapornike, a ne vidijo paznikov, ki se nahajajo v sredinskem nadzornem stolpu, v zatemnjenem delu. Tako zapornik igra hkrati obe vlogi; nadzirano (oblikuje mehanizem samonadzora) in nadzorno (ima pogled na druge zapornike, a paznika ne more videti).

Slika 8.1: Zapuščeni zapor Panoptikon na Kubi



Vir: Viral Forest (2017).

Za razumevanje sodobnega nadzorovanja pa je pomemben tudi Gilles Deleuze. Po njegovem so zahodne družbe po drugi svetovni vojni postale disciplinarne družbe, ki so izpodrinile družbe nadzora. Disciplinarne družbe nadzor izvajajo tako, da posameznika uvrščajo v zaprta okolja, kot so družina, šola, tovarna, bolnišnica, zapor (Deleuze in Negri 2002, 173).

Lyonova študija nadzora (1994) pa temelji na namenu po vzpostavitvi usmerjenega in stalnega spremljanja, varovanja in nadzorovanja človeškega vedenja. Po njegovem (Lyon 2001) smo zahodne družbe postale družbe nadzora (angl. *surveillance society*). To je družba, ki je organizirana in strukturirana za uporabo tehnologij nadzora. Biti pod nadzorom pomeni imeti shranjene informacije o gibanju in aktivnostih določene osebe, v imenu organizacij in vlad, ki tvorijo našo družbo. Pridobljene informacije se nato razvrščajo, pregledujejo in kategorizirajo

ter uporabijo kot osnova odločitvam, ki vplivajo na naše življenje. Te odločitve se nanašajo na naše pravice, dostop do ugodnosti, delo, proizvode, storitve in pravosodje, kot tudi na zdravje, počutje in gibanje skozi javne in zasebne prostore (Murakami Wood 2006).

Nadzor je v moderni družbi tesno povezan z računalnikom in drugo informacijsko tehnologijo, ki nas obkroža, in tako vedno bolj koordinira naše dejavnosti v prostoru in času (Kovačič 2003, 22). Kovačič meni, da bi nadzor obstajal tudi brez informacijske tehnologije, vendar ga je ta poglobila in okrepila (prav tako, 26). Glavne značilnosti tehnologij nadzora po Marxu so (Lyon 1994, 68): nevidnost (oz. zelo majhna vidnost), neprostovoljnost, kapitalska in ne delovna intenzivnost, decentraliziranost, uvajajo obravnavanje posameznikov po skupinah in ne po specifičnih posameznikih in so bolj intenzivne ter razširjene.

Ker informacijsko tehnologijo dnevno uporabljamo in je prisotna vsepovsod, za sabo puščamo svojo elektronsko sled. S tem pojmom označujemo informacijo: »... ki se shranjuje rutinsko in kaže dejavnost nekega posameznika« (Kovačič 2003, 27). Prava moč tehnologij nadzor pa je v tem, da je zbrane podatke možno povezati, saj telekomunikacijski sistemi omogočajo povezovanje fizično ločenih - decentraliziranih sistemov nadzora. Na takšen način lahko enostavno pridobimo zaupne podatke o opazovancih in posledično posežemo v njihove pravice.

9 UČINKOVITOSTI ALGORITMOV ZA PREPOZNAVANJE OBRAZOV

Čeprav tehnologije, ki uporabljajo algoritme za prepoznavanje obrazov, izredno napredujejo, težko rečemo, da je učinkovitost računalnikov pri prepoznavanju boljša od človeške, saj imamo ljudje splošno bolj razvito zmožnost prepoznave v težavnih pogojih (Cho in drugi 2014, 1). Naša prednost je predvsem ta, da za prepoznavo uporabljamo tako holistične, kot lokalne tehnike prepoznavanja.

V študiji *Comparitive Study on Face Recognition Using HGPP, PCA, LDA, ICA and SVM* (Kadiya, 2012), je avtor raziskoval pet različnih algoritmov za prepoznavanje obrazov na dveh različnih podatkovnih bazah. Prva baza podatkov (ATT) je vsebovala slike oseb, ki so imele izredno majhne razlike v postavitvi obraza, medtem ko je druga baza (IDF) vsebovala slike oseb iz različnih zornih kotov. Stopnja prepoznave (angl. *recognition rate*) na ATT bazi je bila višja kot pri IDF bazi. Pri ATT bazi je bila točnost algoritmov med 91,3 % in 98,9 %, medtem ko je bila pri IDF bazi med 46,25 % in 86,3 %.

Na treh različnih vzročnih videoposnetkih sta učinkovitost algoritmov raziskovala tudi avtorja Jang in Lee (2016, 204). Prvi vzorec je vseboval posnetke obraza iz različnih zornih kotov, tretji vzorec posnetke obraza pri frontalni postavitvi, medtem ko je drugi vzorec vseboval vmesno postavitev obraza. Učinkovitost prepoznavanja je bila največja pri prvem vzorcu in najmanjša pri tretjem. Vsi trije algoritmi so bili pri prvem vzorcu med 83,18 % in 93,53 %, pri tretjem pa med 66,06 % in 63,99 %. Raziskava je tako med drugim potrdila, da je učinkovitost prepoznavanj v veliki meri odvisna od postavitve obraza na slikah.

Primerjavo algoritmov pri različnih postavitvah obraza so v članku raziskovali tudi Liu in drugi (2009). Test je bil narejen na štirih vzorcih, ki so se razlikovali glede na nevtralnost, osvetlitev, izraz (angl. *expression*) in položaj obraza. Najučinkovitejši algoritem pri vseh vrstah slik je bila metoda lokalnih binarnih vzorcev. Najslabše se je odrezala pri Expression slikah, kjer je dosegla 91,06 % učinkovitost, najbolje pa pri osvetljenem vzorcu, kjer je bila metoda 97,30 % uspešna.

Raziskava (Zuhaer in Al-Dabagh, 2014, 180) je v primerjavi s prejšnjimi skušala pojasniti, kako algoritmi prepoznavanja delujejo v primeru uporabe ene vzorčne slike v postopku učenja. Rezultati so pokazali, da ima večina algoritmov težave pri prepoznavanju v primeru, ko za

vzorec uporabimo le eno sliko. Učinkovitost prepoznavanja je bila v omenjenem primeru še vedno zelo velika in je znašala 92,6667 %.

Učinkovitost prepoznavanja obrazov v resničnem svetu sta skušala prikazati avtorja članka Unconstrained Facial Images: Database for Face Recognition under Real-world Conditions (Lenc in Kral v Pichardo Lagunas in drugi, 2015). V ta namen sta ustvarila bazo obrazov, ki so bili zajeti v realnih pogojih – s slabo osvetlitvijo in nizko kakovostjo slike. Test so izvedli v dveh delih. Prvi del so predstavljale slike, ki so vsebovale avtomatsko zaznane obraze iz slik, izrezane iz celotne slike, tako da so bili vsi obrazi enako veliki in ločeni od ozadja. Drugi del pa so sestavljale slike, na katerih je bilo poleg obraza tudi preostalo ozadje. Učinkovitost prepoznavanja najboljšega algoritma pri bazi slik z izrezanimi obrazi je bila 67,1 %, pri celotni sliki pa 43,2 %.

Vpliv velikosti oz. resolucije slik na učinkovitost prepoznavanja obrazov so raziskovali Peng in drugi (2012). Teste so izvedli na metodi glavnih komponent, linearni diskriminantni analizi in metodi lokalnih binarnih vzorcev. Ugotovitve so pokazale, da je najučinkovitejša metoda pri slikah z manjšo ločljivostjo linearna diskriminantna analiza, medtem ko metoda lokalnih binarnih vzorcev ni primerna za uporabo pri manjših slikah. Učinkovitost prepoznavanja je bila sorazmerno večja z večanjem velikosti slik.

Tudi Becker in Ortiz (2008) sta v svoji raziskavi skušala ugotoviti, kakšna bi bila učinkovitost sistemov za prepoznavanje obrazov v realnem svetu. Za bazo podatkov sta izbrala Facebook, kjer jima je uspelo s sedmimi uporabniškimi računi pridobiti preko 60.000 slik od več kot 500 uporabnikov. Ugotovitev raziskave je, da nobena izmed uporabljenih metod ni primerna za širšo uporabo na tako veliki podatkovni bazi slik, kot je Facebook. Najvišjo učinkovitost sta dosegli metodi podpornih vektorjev in linearne diskriminantne analize, ki je znašala 65 %, vendar na račun visokih računskih in spominskih zahtev.

Raziskava od Phillips in drugi (2003), v kateri so naredili evalvacijo komercialnih sistemov za prepoznavanje obrazov, je pokazala, da je stopnja učinkovitosti najboljših sistemov za prepoznavanje na ravni prepoznavne na osnovi prstnih odtisov, če so obrazi zajeti frontalno in ob enakomerni osvetlitvi. Prepoznavna v nenaravnih okoljih in ob različni postavitvi obraza ter osvetlitvi se je pokazala za bolj zahtevno težavo.

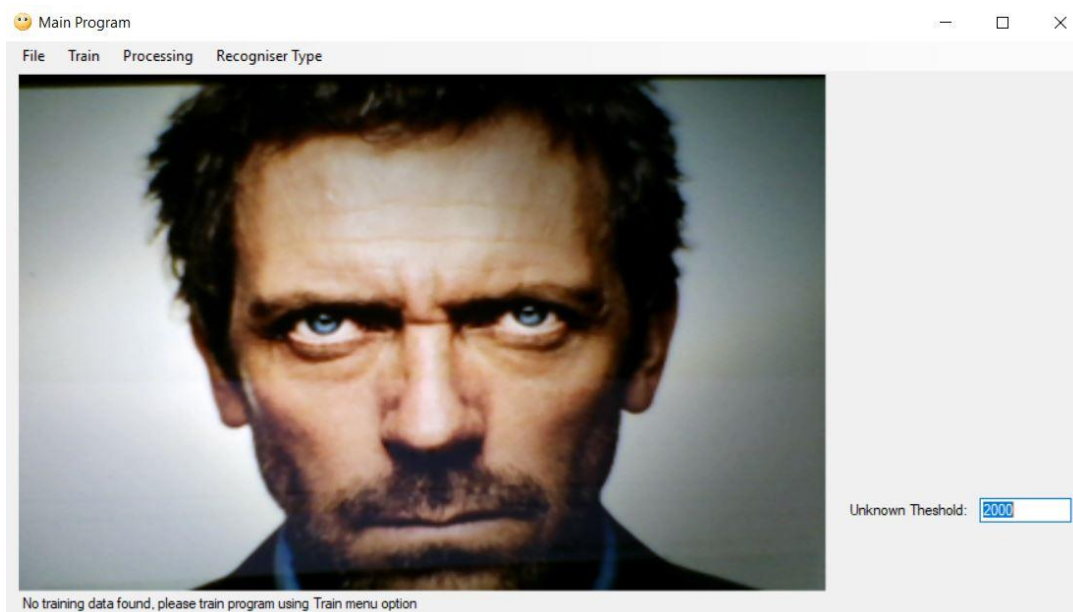
10 PROGRAM EMGU CV IMAGE PROCESSING WRAPPER

V praktičnem delu magistrske naloge bom s pomočjo prostokodnega programa za prepoznavanje obrazov EMGU CV image processing wrapper (Code Project 2014) izvedel prepoznavanje oseb na tesni bazi slik in ocenil njegovo uspešnost. Program uporablja odprtokodno knjižnico OpenCV (angl. *open source computer vision*), ki ponuja zbirko več kot 2500 algoritmov s področja računalniškega vida in strojnega učenja. Ti so lahko uporabni za detekcijo in prepoznavo obrazov, prepoznavanje predmetov, razvrščanje človeških dejanj iz videoposnetkov, spremljanje premikanja kamere, sledenje premikajočim se objektom, ekstrakcijo 3D modelov iz predmetov, izdelavo 3D-točkovnih oblakov iz stereo kamer, združevanje slik za izdelavo slike visoke ločljivosti celotnega področja, iskanje podobnih slik iz baze slik, odstranjevanje rdečih oči iz slik, spremljanje gibov oči, prepoznavanje pokrajine in določitev točk za preplastitev z nadgrajeno resničnostjo (angl. *augmented reality*) in podobno (OpenCV 2017). Razvoj knjižnice je leta 1999 začela družba Intel Research, ki je želela na ta način pohitriti in optimizirati delovanje aplikacij, ki so porabile veliko procesorske moči. Leta 2012 je podpora nad knjižnico prevzela neprofitna organizacija OpenCV.org. Knjižnica ima vmesnike za programske jezike C++, C, Python, Java in MATLAB ter vsebuje podporo za Windows, Linux, Android in Mac OS platforme.

Čeprav je knjižnica napisana v programskem jeziku C in C++, se lahko uporablja tudi v drugih programskih jezikih, za kar skrbijo mnogi vmesniki in ovoji (angl. *wrappers*). Eden izmed najbolj razširjenih ovojev je EMGU CV, ki omogoča uporabo vseh funkcionalnosti knjižnice iz .NET programskega okolja, v katerem so podprti programski jeziki C#, VB, IronPython ter VC++ (Shi 2013). Uporabljen program je v celoti napisan v programskem jeziku C# in vsebuje tri različne metode prepoznavanja obrazov, ki so podrobneje razložene v poglavju 11:

- metoda lastnih obrazov (temelji na analizi glavnih komponent),
- metoda Fisherjevih obrazov (temelji na linearni diskriminantni analizi) in
- metoda lokalnih binarnih vzorcev (angl. *local binary pattern - LBP*).

Slika 10.1: Originalni program EMGU CV image processing wrapper

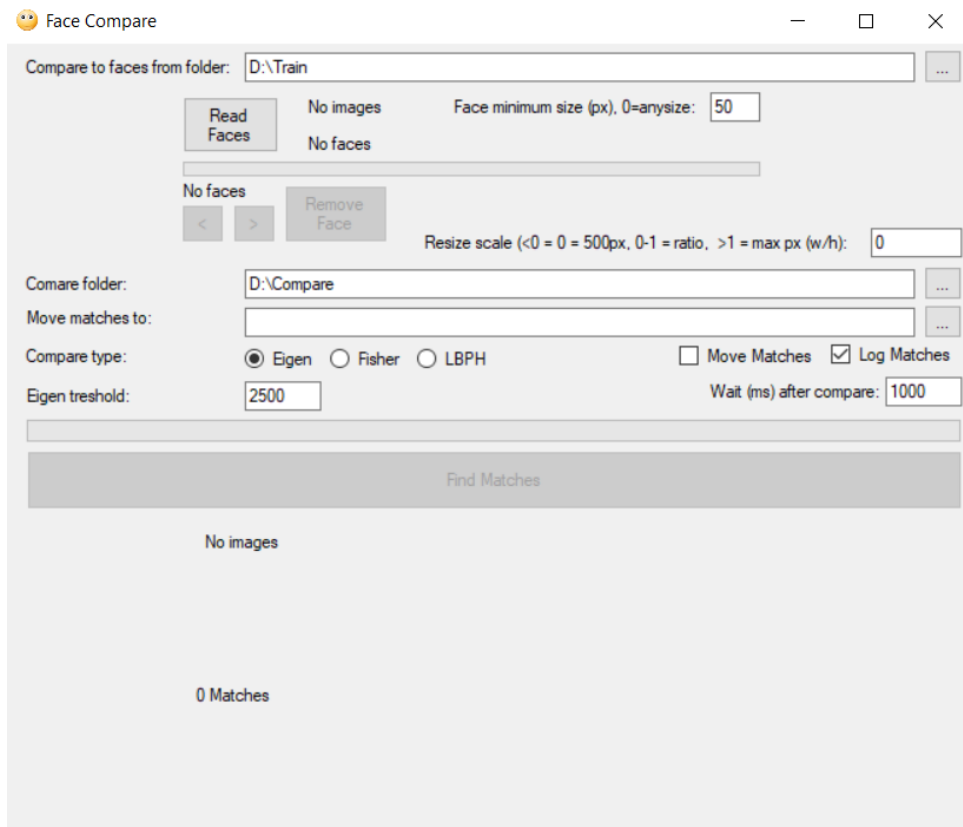


Vir: lasten.

Eigenfaces in Fischerfaces sta metodi, ki jih Zhao in drugi (2003, 409-410) razvrščajo v kategorijo **holističnih oz. globalnih tehnik** za prepoznavanje obrazov. Za njih je značilno, da za prepoznavanje uporabljajo lastnosti celotnega obraza. Medtem ko je metoda lokalnih binarnih vzorcev **lokalna oz. strukturna tehnika**, ki se osredotoča na lokalne značilnosti obraza, kot so nos, oči, usta itd. Glede na Kämäräinen in drugi (v Li in Jain 2011, 103), so lokalne tehnike bolj robustne in posledično bolj odporne proti različnim osvetlitvam in položaju obraza kot holistične, zato bom v teoretičnem delu skušal podano ugotovitev potrditi.

Program EMGU CV image processing wrapper mi je predstavljal osnovo za uporabo v magistrskem delu, saj je bil napisan za namen prepoznavanja oseb iz spletne kamere računalnika. Program sem s pomočjo programerja prilagodil tako, da ga je možno uporabiti na zbirki slik. Nov program deluje na način, da na osnovi učnih slik obrazov (vzorec za trening), ki se nahajajo v mapi Train, izvede prepoznavo na slikah, ki se nahajajo v mapi Compare. Rezultate prepoznavanja nato zapiše v tekstovno datoteko na način, da sliki pripiše ime osebe, s katero jo je prepoznal. Slikam, pri katerih ni našel ujemanja, pa pripiše "unknown".

Slika 10.2: Nov program EMGU CV image processing wrapper



Vir: lasten.

Tako prilagojen program nam je lahko vsakodnevno v pomoč pri iskanju določene osebe na osebnih ali spletnih bazah slik, razvrščanju slik v mape, identifikaciji osebe na podlagi ene slike v povezavi s podatki iz različnih družbenih spletnih strani, preko katerih je mogoče povezati sliko z imenom osebe (npr. Facebook, Instagram, LinkedIn ipd.), brskanju po raznih spletnih bazah slik itd.

11 METODE PREPOZNAVANJA OBRAZOV

V nadaljevanju so opisane tri metode prepoznavanja obrazov, s katerimi bom preveril uspešnost prepoznavanja na testni bazi slik.

11.1 Metoda lastnih obrazov (analiza glavnih komponent)

Metoda lastnih obrazov je najbolj znana in razširjena holistična metoda prepoznavanja obrazov, ki temelji na analizi glavnih komponent (Suhas in drugi 2012, 15).

Analiza glavnih komponent je metoda v faktorski analizi in hkrati ena izmed najbolj uporabljenih multivariatnih metod. Leta 1901 jo je osnoval Karl Pearson. Njena osnovna zamisel je opisati razpršenost n enot v m razsežnem prostoru (določen z m merjenimi spremenljivkami) z množico nekoreliranih spremenljivk, ki so linearne kombinacije originalnih merjenih spremenljivk. Tem linearnim kombinacijam pravimo komponente in zanje velja, da so med seboj neodvisne in urejene po pomembnosti, s tem da prva glavna komponenta pojasni največji del vsote varianc opazovanih spremenljivk, vsaka nadaljnja pa kvečjemu manjši del.

Z analizo glavnih komponent dosežemo, da nam za prikaz celotnega sistema variabilnosti, ni potrebno vzeti vseh m komponent, ampak le nekaj glavnih komponent, ki pogosto razložijo večji del variabilnosti. Cilj analize je torej poiskati nekaj prvih (glavnih) komponent, ki pojasnijo kar se da veliko razpršenosti opazovanih spremenljivk; torej, da kar se da močno korelirajo z njimi. To nam omogoča povzemanje podatkov s čim manjšo izgubo informacij, tako da se zmanjša razsežnost podatkov (pri tem pa ne predpostavlja specifičnega prostora).

Pri metodi glavnih komponent določimo uteži pri linearni kombinaciji spremenljivk, tako da je varianca te linearne kombinacije največja. Torej želimo poiskati take uteži a_1 , za katere bo varianca Y_1 največja:

$$a_1 = \operatorname{argmax}_a \operatorname{var}(X_a)$$

$$Y_1 = X_{a_1}$$

Ob pogoju:

$$a_1^T a_1 = 1$$

s katerim določimo, da je problem enolično rešljiv, saj je linearna kombinacija Y_1 prva komponenta.

Ko izračunamo prvo komponento (y_1) z največjo varianco, poiščemo drugo komponento tako, da je nekorelirana s prvo in ima zopet največjo varianco. Postopek ponavljamo vse do zadnje komponente. Število komponent določimo sami, glede na odstotek variance, ki ga želimo z njimi pojasniti. Rezultati so smiselni, če so variance glavnih komponent pozitivna števila.

Če analizo glavnih komponent impliciramo na uporabo pri prepoznavanju obrazov, lahko to storimo po naslednjem matematičnem postopku:

A. Transformacija slike

Sliko, predstavljeno v dvodimenzionalnem (2D) prostoru, moramo najprej transformirati v enodimenzionalni vektor (1D). Predpostavimo, da nam osnovo za to predstavlja X vhodnih normaliziranih sivinskih učnih slik obrazov $S_1, S_2, S_3, \dots, S_x$ določene dimenzije. Prednost uporabe sivinskih slik je, da na takšen način za tretjino zmanjšamo njihovo velikost, saj uporabimo le 8 bitov za predstavitev posamezne slikovne točke (angl. *pixel*). Vsaka slikovna točka lahko v primeru 8 bitne slike zavzame vrednost od 0 (črna) do 255 (bela).

Vsako sliko lahko predstavimo z matriko $m \times n$, kjer m označuje višino slike in n širino slike, merjeno v slikovnih točkah, $m, n \in \mathbb{N}$.

Shema 11.1: Primer matrike

$$S_x = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline S_{11} & S_{12} & & & & & & & & S_{1m} \\ \hline S_{21} & S_{22} & & & & & & & & S_{2m} \\ \hline & & & & & & & & & \\ \hline & & & & & & & & & \\ \hline & & & & & & & & & \\ \hline & & & & & & & & & \\ \hline & & & & & & & & & \\ \hline & & & & & & & & & \\ \hline S_{n1} & S_{n2} & & & & & & & & S_{nm} \\ \hline \end{array}$$

Vsak element slike vsebuje zapis o vrednost njegove intenzitete ($0 \leq X_{m,n} \leq 255$). Matriko slike nato predstavimo kot enodimenzionalni vektor dolžine $V = m \times n$, ki predstavlja linearno kombinacijo originalne slike obrazov (shema 11.2.). V primeru slike, velikosti 128 x 128 slikovnih točk, dobimo vektor s 16.284 vrednostmi.

Shema 11.2: Vektor matrike

[illegible]

B. Izdelava matrike slik

Nato sestavimo matriko vseh S_X vhodnih učnih slik obrazov določene dimenzije, kjer vsak V predstavlja vektor vhodne slike (3.):

$$\text{Matrika slik} = \begin{pmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ \vdots \\ V_r \end{pmatrix}$$

C. Izračunamo povprečni vektor/obraz

Nato izračunamo povprečni vektor/obraz Ψ iz celotne množice učnih slik obrazov, tako da vzamemo povprečno vrednost vsake slikovne točke. S tem dosežemo, da se iz vektorjev odstranijo informacije, ki so skupne vsem slikam in nam ne bodo v pomoč pri prepoznavanju obrazov. Prav tako na ta način zmanjšamo korelacijo med vhodnimi slikami.

$$\Psi = \frac{1}{M} \sum_{x=1}^M V_x$$

Od vsake učne slike obraza V_x odštejemo povprečni obraz Ψ in dobimo vektor ϕ_x , ki predstavlja povprečno centrirano sliko vsakega učnega obraza (angl. *mean centered image*).

$$\phi_x = V_x - \Psi$$

D. Izdelamo kovariančno matriko

Dimenzija vsakega povprečnega vektorja in učnega vektorja je $1 \times V$, pri čemer je $V = m \times n$. Ti podatki nam nato predstavljajo osnovo za analizo glavnih komponent, s katero sestavimo kovariančno matriko C od A :

$$C = \frac{1}{M} \sum_{i=1}^M \phi_i \phi_i^T = AA^T \quad (V \times V \text{ matrika})$$

kjer je $A = [\phi_1, \phi_2, \phi_3, \dots, \phi_M]$ velikosti $V^2 \times X^2$ in

Dimenzija $A = V^2 \times X^2$ in dimenzija $A^T = X^2 \times V^2$, torej je dimenzija kovariančne matrike C enaka $V \times V$ ($V = m \times n$).

E. Izračunamo lastne vektorje in lastne vrednosti

Iz kovariančne matrike nato izračunamo lastne vrednosti in lastne vektorje (lastne obraze). Dimenzija kovariančne matrike C je $V \times V$ in v primeru slike, velikosti 128×128 , znaša 16.384

x 16.384. Računsko je to torej že pri razmeroma majhni velikosti slik zahtevna operacija, saj vsi lastni obrazi niso uporabni, ker z njimi pojasnimo neznaten del variabilnosti. Posledično analize glavnih komponent, zaradi velike kovariančne matrike C , neposredno ne izvajamo in za to raje uporabimo manjšo matriko $L = A^T A$, ki je bolj ustrezna za nadaljnjo obdelavo in je dimenzije $X \times X$.

$$L = A^T A \quad (X \times X \text{ matrika})$$

Iz nove zmanjšane matrike $A^T A$ lahko izračunamo lastni vektor Av_i in lastno vrednost λ_i :

$$A^T Av_i = \lambda_i v_i$$

Če pomnožimo obe strani zgornje enačbe z A , dobimo:

$$AA^T Av_i = A\lambda_i v_i$$

$$AA^T (Av_i) = \lambda_i (Av_i)$$

$$C(Av_i) = \lambda_i (Av_i) \text{ ker je } C = AA^T$$

Lastni vektorji matrike C se nato enostavno izračunajo z zmanjšanjem dimenzij, kjer Av_i predstavlja lastni vektor in λ_i lastno vrednost.

Slabost metode glavnih komponent pri prepoznavanju obrazov je to, da ta pri zmanjšanju dimenzij obdrži nezaželene odlike, do katerih lahko pride zaradi različne osvetlitve ali obrazne mimike (Zuhaer in Al-Dabagh, 2014, 180). Zato je lahko njena učinkovitost pri razvrščanju slik, ki so zajete v slabih svetlobnih pogojih, nezadovoljiva.

F. Izbira K glavnih komponent (lastnih vektorjev)

V tem koraku izvedemo stiskanje podatkov in zmanjšanje dimenzij. Ko dobimo vse lastne vektorje matrike C , jih najprej razvrstimo po velikosti padajoče glede na njihove lastne vrednosti. Tako jih razvrstimo po njihovi pomembnosti (značilnosti). Lastnemu vektorju z največjo lastno vrednostjo pravimo glavna komponenta. Večja lastna vrednost pomeni večji

delež variance, ki ga določen lastni vektor pojasni oz. več karakterističnih značilnosti obraza, ki jih opiše. V tem koraku se nato odločimo, koliko glavnih komponent želimo obdržati. Lastne vektorje z majhnimi lastnimi vrednostmi lahko namreč odstranimo, saj pojasnijo le majhen del karakterističnih značilnosti obraza in na ta način zmanjšamo število dimenzij (Liton in Abdulla 2012, 136). V praksi je navadno število glavnih komponent, ki se uporabijo pri vhodnih slikah, 40 ali manj (Li in Jain v Li in Jain 2011, 5).

Pri tem sicer izgubimo nekaj podatkov, vendar če so lastne vrednosti majhne, je ta delež zanemarljiv. Če smo imeli v osnovi n dimenzij in izračunamo n lastnih vektorjev in lastnih vrednosti ter se nato odločimo obdržati prvih d lastnih vektorjev, bo imel končni set podatkov d dimenzij (Smith 2002, 16).

G. Sestava vektorja značilk (angl. *feature vector*)

Iz glavnih komponent, za katere smo se odločili, da jih bomo obdržali izmed vseh komponent, sestavimo vektor značilk:

$$\Omega = (\omega_1, \omega_2, \omega_3, \dots, \omega_n)$$

H. Izračun povprečne razdalje (Evklidove razdalje)

Ko izberemo glavne komponente in sestavimo vektor značilk, moramo izračunati še povprečno razdaljo (Evklidovo razdaljo) med testnim vektorjem značilk in vsemi trening vektorji značilk. Matematično je prepoznavna obrazov iskanje najmanjše Evklidove razdalje ε_k med testno točko in trening točko:

$$\varepsilon_k = \sqrt{\|\Omega_{test} - \Omega_i\|^2}$$

Evklidova razdalja med dvema vektorjema pri prepoznavanju obrazov torej predstavlja mero podobnosti med dvema ustreznima slikama/obrazoma.

11.2 Metoda Fisherjevih obrazov (linearna diskriminantna analiza)

Ko so na sliki obraza prisotne velike razlike zaradi osvetlitve ali postavitve, je velika razlika v podatkih lahko posledica prav teh sprememb. Metoda glavnih komponent zazna in obdrži večino teh razlik, kar lahko privede do manjše učinkovitosti sistema za prepoznavanje obrazov. Belhumeur in drugi (Shakhnarovich in Moghaddam v Li in Jain 2011, 26) so za rešitev te težave predlagali uporabo metode Fisherjevih obrazov, ki temelji na linearni diskriminantni analizi.

Ta je primernejša od metode glavnih komponent, saj je njena osnovna ideja poiskati takšno linearno transformacijo, da so razlike med skupinami po transformaciji kar se da velike, tj. najbolj razločevalne. To počne na način, da v obzir vzame razpršenost znotraj skupine, kot tudi med samimi skupinami. V praksi se ta metoda lahko uporablja za pojasnjevanje razlik med skupinami ali za napovedovanje, v katero skupino najverjetneje sodi določena enota. Metoda temelji na dveh predpostavkah. Predpostavlja, da je podprostor obraza linearen in da obstaja linearna razlika med skupinami. Linearna diskriminantna analiza je v teoriji večkrat navedena tudi kot Fisherjeva diskriminantna analiza.

Pri prepoznavanju obrazov se največkrat uporabi kombinacija metode glavnih komponent in linearne diskriminantne analize. Pri tem se metoda glavnih komponent uporabi za transformacijo slik v manj dimenzijski prostor in tako naredi matriko razpršenosti med razredi nesingularno (Suhas in drugi 2012, 17). V nadaljevanju je metoda opisana matematično.

A. Izračunamo povprečni vektor/obraz

Predpostavimo, da imamo normaliziran vzorec N vseh učnih slik, N_k število slik določenega razreda oz. oseb in x_{k_m} slik z indeksom m in razredom k . Pri metodi Fischerjevih obrazov (enako kot pri metodi glavnih komponent) najprej izračunamo povprečni vektor/obraz μ celotne množice učnih slik obrazov.

$$\mu = \frac{1}{N} \sum_{k=1}^N x_k$$

B. Izračunamo povprečni vektor/obraz vsake skupine

V naslednjem koraku izračunamo povprečni vektor/obraz μ_k še za vsako skupino.

$$\mu_k = \frac{1}{N_k} \sum_{m=1}^{N_k} x_{km}$$

Ti podatki nam predstavljajo osnovo, na podlagi katere izračunamo dve matriki razpršenosti.

C. Izračunamo matriko razpršenosti znotraj razreda S_W (angl. *within-class scatter matrix*)

$$S_W = \sum_{k=1}^C \sum_{x \in X_k} (x_k - \mu_k)(x_k - \mu_k)^T \quad \text{kjer je } C \text{ število razredov}$$

D. Izračunamo matriko razpršenosti med razredi S_B (angl. *between-class scatter matrix*)

$$S_B = \sum_{k=1}^C N_k (\mu_k - \mu)(\mu_k - \mu)^T \quad \text{kjer je } C \text{ število razredov}$$

E. Izračunamo optimalno transformacijsko matriko W

Naš cilj je najti takšno transformacijsko matriko W , s katero bomo zmanjšali razdalje med projekcijami vzorcev istih oseb (obdržali slike posameznikov čim manj razpršene) in maksimalno povečali razdalje med projekcijami vzorcev različnih oseb. Če je S_W nesingularna, je optimalna transformacijska matrika:

$$W_{opt} = \arg \max_W \frac{|W^T S_B W|}{|W^T S_W W|}$$

F. Izračunamo splošno lastno vrednost

W predstavlja lastne vektorje (Fisherjeve oblike) in λ_i pripadajoče lastne vrednosti matrike razpršenosti med in znotraj razredov.

$$S_B W = \lambda_i (S_W W)$$

Nastane težava, če je matrika razpršenosti znotraj razreda S_W singularna. Takšna težava je v praksi pogosta, saj večkrat pride do situacije, ko je število učnih slik v vzorcu precej manjše od njihove dimenzije. Da bi rešili težavo majhnega števila slik v vzorcu pri linearni diskriminantni analizi, so Belhumeur in drugi (714, 1997) predlagali rešitev s transformacijo slik v manjdimenzijski prostor z uporabo metode glavnih komponent. S kombinacijo metode glavnih komponent in linearne diskriminantne analize postane matrika S_W nesingularna. Optimalno transformacijsko matriko $W_{PCA+LDA}$ v tem primeru formuliramo z rešitvijo naslednjih optimizacijskih težav:

$$W_{PCA+LDA}^T = W_{PCA}^T W_{LDA}^T$$

$$W_{PCA} = \arg \max_W |W^T S_T W|$$

$$W_{LDA} = \arg \max_W \frac{|W^T W_{PCA}^T S_B W_{PCA} W|}{|W^T W_{LDA}^T S_W W_{PCA} W|},$$

kjer S_T predstavlja skupno matriko razpršenosti, definirano kot:

$$S_B = \sum_{k=1}^C (\mu_k - \mu)(\mu_k - \mu)^T$$

G. Izračunamo vektorje značilk

Iz vektorja $W_{PCA+LDA}^T$ izračunamo vektor značilk c vhodnega vzorca slik x_k .

$$c = W_{PCA+LDA}^T x_k$$

11.3 Metoda lokalnih binarnih vzorcev (angl. *local binary pattern - LBP*)

Metoda lokalnih binarnih vzorcev je dokaj nov pristop, ki se uporablja za prepoznavanje obrazov. Prvič so jo leta 2004 za namen prepoznavanja obrazov predlagali Ahonen in drugi (v Pajdla in Matas 2004). Omogoča nam opisovanje lokalnih prostorskih značilnosti slike, na način, da sliko razdeli v manjše dele. Te značilnosti so predstavljene z binarnimi vzorci, ki opišejo območje slikovnih pik v posameznih delih slike. Pridobljene značilnosti so nato predstavljene s histogramom, ki tvori predstavitev slike. Primerjava slik poteka tako, da se merijo podobnosti (razdalje) med njihovimi histogrami. Metoda lokalnih binarnih vzorcev se vedno bolj uporablja v aplikacijah za prepoznavanje obrazov, zaradi njene visoke razlikovalne moči in odpornosti na spremembe osvetlitve (Zuhaer in Al-Dabagh, 2014, 181).

Originalni operator lokalnih binarnih vzorcev:

Shema 11.3: Primer delovanja originalnega operatorja lokalnih binarnih vzorcev

g_0	g_1	g_2	114	255	55	1	1	0	$1x2^0$	$1x2^1$	$0x2^2$
$\rightarrow g$	g_p	g_3	255	114	198	$\rightarrow$		1	$1x2^7$		$1x2^3$
g_6	g_5	g_4	198	19	55	1	0	0	$1x2^6$	$0x2^5$	$0x2^4$

LPB vrednost centralne slikovne točke 114:

Binarna: 11010011

Decimalna: $1x2^0 + 1x2^1 + 0x2^2 + 1x2^3 + 0x2^4 + 0x2^5 + 1x2^6 + 1x2^7 = 211$

Originalni operator lokalnih binarnih vzorcev so leta 1996 razvili Ojala in drugi (v Kämäräinen in drugi v Li in Jain 2011, 84). Deluje tako, da primerja centralno slikovno točko z osmimi sosednjimi slikovnimi točkami, ki jo obdajajo (3 x 3 kvadrat). Vrednost vsake slikovne točke lahko v primeru sivinske slike, kjer uporabimo le 8 bitov za predstavitev slikovne točke, zavzame vrednost med 0 (črna) in 255 (bela). Če ima sosednja slikovna točka večjo ali enako sivinsko vrednost od centralne slikovne točke, potem ta zavzame vrednost 1, drugače dobi vrednost 0. Vrednost ene LPB centralne slikovne točke s koordinato (x,y) lahko izračunamo s formulo:

$$LBP(x, y) = \sum_{p=0}^7 s(g_p - g_c) 2^p$$

g_c predstavlja sivinsko vrednost centralne slikovne točke in g_p vrednost njegovih sosednjih slikovnih točk. Funkcija $s(z)$ je definirana kot:

$$s(z) = \begin{cases} 1, & z \geq 0 \\ 0, & z < 0 \end{cases}$$

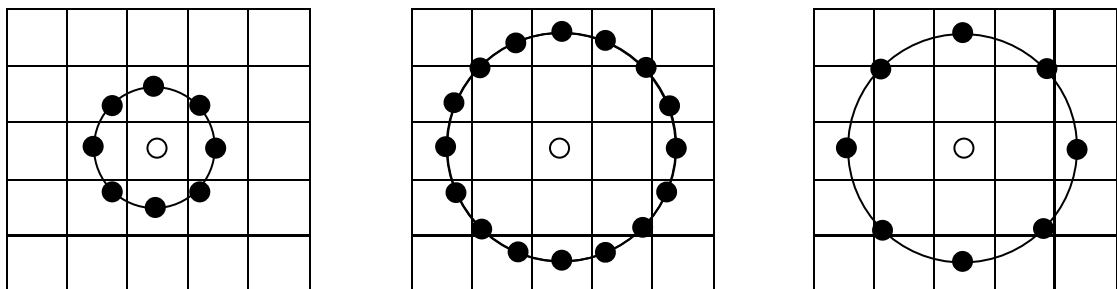
Vse LPB vrednosti slikovnih točk slike oz. celotno sliko nato statistično predstavimo v histogramu LPB ($LBPH$), ki vsebuje podatke o porazdelitvi lokalnih značilnosti slike, kot so robovi, točke, ravne površine (Ahonen in drugi v Pajdla in Matas 2004, 471).

$$LBPH(i) = \sum_{x,y} \delta\{i, LBP(x, y)\}, \quad i = 0, \dots, 2^7$$

Da bi bila metoda lokalnih binarnih vzorcev uporabna tudi pri različno velikih prostorskih strukturah slike, so Ojala in drugi (2002) originalni operator lokalnih binarnih vzorcev kasneje razširili na uporabo različno veliko sosednjih slikovnih točk – večnivojski operator lokalnih binarnih vzorcev. To lahko dosežemo z dvema dodatnima parametroma, in sicer s poljubnim polmerom (R) in številom sosednjih slikovnih točk (P).

$$LBP_{P,R}(x, y) = \sum_{p=0}^{P-1} s(g_p - g_c) 2^p$$

Shema 11.4: Primeri različnih večnivojskih operatorjev: krožni (8, 1), (16, 2) in (8, 2)



Vir: Ojala in drugi (2002).

Še ena razširitev originalnega operatorja so enakomerni vzorci (angl. *uniform patterns*), saj se je pokazalo, da se nekateri vzorci na slikah pogosteje pojavljajo kot drugi (prav tam). To pomeni, da se pri njih pojavita največ dva prehoda med ničlami in enicami. Tako so recimo vzorec 00000000 (nič prehodov), 01111110 ali 11100111 (dva prehoda) enakomerni, medtem ko 11001001 (štirje prehodi) ali 01010011 (šest prehodov) nista. V raziskavi so prišli do ugotovitve, da je delež enakomernih vzorcev pri operatorju (8, 1) znašal malo manj kot 90 % vseh vzorcev in koli 70 % pri operatorju (16, 2). Enakomerne lokalne binarne vzorce zapišemo kot $LBP_{P,R}^{u2}$.

12 ZBIRKA SLIK: MSRA-CFW

Za testiranje učinkovitosti različnih metod prepoznavanja obrazov je pomembno, da uporabimo takšno zbirko slik, ki se najbolj približa slikam, ki se uporabljajo za prepoznavanje v realni situaciji. Le program, ki bo zmožen prepoznati osebe na osnovi realne zbirke slik, bo zanesljiv in učinkovit. Zato sem v ta namen uporabil spletno dostopno zbirko slik slavnih oseb MSRA-CFW (Microsoft Research Asia - Celebrities on the Web), ki je bila zbrana za uporabo v raziskavi Finding Celebrities in Billions of Webpages (Zhang in drugi v Zhu, 2012).

Zbirka je sestavljena iz 202.792 slik obrazov 1.580 slavnih oseb. Prednost uporabe omenjene zbirke v primerjavi z drugimi spletno dostopnimi zbirkami je v velikemu številu slik, saj jih podobne zbirke vsebujejo le nekaj tisoč. Hkrati so bile slike zbrane preko spleta s spletnim brskalnikom Bing, zaradi česar vsebujejo velike razlike v postavitvi obraza, obrazni mimiki, osvetlitvi itd. Slike vsake osebe so razvrščene v mapi, poimenovani z njenim imenom in priimkom ter označene z zaporednimi številkami. Format slik je .jpg, njihova velikost pa je bila zaradi praktičnih razlogov omejena na 160 slikovnih točk glede na višino ali širino slike ($160 \times x$ ali $x \times 160$).

Zaradi velikega števila slik in posledično nepreglednosti nad dobljenimi rezultati, sem za namen učenja in prepoznavanja zbirko zmanjšal na vsega 250 naključno izbranih slavnih oseb. Slike vseh izbranih slavnih oseb sem nato preveril, iz njih odstranil podvojene slike ter tiste slike, ki osebi niso pripadale (za primer glej sliko 12.1).

Slika 12.1: Izbrisane slike iz mape osebe Chris Brown



Vir: lasten.

V drugem koraku sem omejil število vseh slik vsake slavne osebe na 40, tako da sem jih naključno izbral med vsemi slikami, ki so ji pripadale. Zaradi lažje analize sem pri postopku izbire fotografij uporabil le tiste fotografije posamezne slavne osebe, na katerih se pojavi ona sama. Skupaj je zbirka slik, ki sem jo uporabil za testiranje programa za prepoznavanje obrazov znašala 10.000 slik. Delež moških v uporabljeni bazi je znašal 58,8 % in delež žensk 41,2 % (glej tabelo 12.1).

Tabela 12.1: Struktura baze podatkov po spolu oseb

	Število	Odstotek
Moški	147	58,8 %
Ženski	103	41,2 %
Skupaj	250	100 %

Vir: lasten.

Uporabljene slavne osebe izhajajo iz sedmih različnih področij delovanja (glej tabelo 12.2). Največji delež se jih ukvarja z igrilstvom (62,4 %), sledi glasba s 17,6 % in šport z 8,4 %. Najmanj slavnih oseb izhaja iz IT področja (0,8 %) in režije (1,6 %). Celoten seznam slavnih oseb, uporabljenih pri prepoznavanju in njihova razvrstitev glede na spol ter področja delovanja, je priložen v prilogi.

Tabela 12.2: Struktura baze podatkov glede na področje delovanja

	Število	Odstotek
Igralstvo	156	62,4 %
Glasba	44	17,6 %
Šport	21	8,4 %
Politika	17	6,8 %
Moda	6	2,4 %
Režija	4	1,6 %
IT	2	0,8 %
Skupaj	250	100 %

Vir: lasten.

13 TEST PRIMERA PREPOZNAVANJ OSEB

13.1 Mere učinkovitosti

Pri prepoznavanju obrazov je učinkovitost lahko merjena na treh standardnih nalogah sistemov za prepoznavanje obrazov: preverjanje istovetnosti ali verifikacija (angl. *verification*), odprta identifikacija (angl. *open-set identification*) in zaprta identifikacija (angl. *closed-set identification*). Vse tri naloge so med seboj podobne, pri čemer odprto prepoznavanje predstavlja najbolj splošno uporabo (Phillips in drugi v Li in Jain 2011, 552).

Zaprta identifikacija je osnovno merilo učinkovitosti avtomatičnih sistemov prepoznavanja obrazov, katerega namen je identifikacija oseb. Njegovo glavno vprašanje je: kdo je ta oseba? Pri zaprtem prepoznavanju je raziskovana oseba vedno del podatkovne baze sistema (prav tako, 552).

Pri odprti identifikaciji raziskovana oseba ni nujno del podatkovne baze sistema. Njeno glavno vprašanje je: ali poznamo to osebo? V tem primeru se mora sistem odločiti, ali je raziskovana oseba v njegovi podatkovni bazi. Če je temu tako, potem mora sistem vrniti njeno identiteto. Odprta in zaprta identifikacija izvajata primerjavo ena proti mnogo (1:N).

Pri preverjanju istovetnosti pa oseba poda svoj biometrični vzorec (npr. svojo sliko) sistemu, s katerim želi potrditi svojo identiteto. Sistem se mora nato odločiti, ali predložena slika pripada tej osebi. Glavna naloga sistema je ugotoviti, ali je oseba res to, za kar se izdaja? Preverjanje istovetnosti je primerjava ena na ena (1:1).

Ker biometrične metode niso nikoli popolnoma zanesljive, bo prva mera, ki jo bom izračunal, klasifikacijska točnost (angl. *classification accuracy*), ki predstavlja razmerje med pravilno razvrščenimi primeri in vsemi primeri.

$$T = \frac{N_P}{N} \times 100$$

Klasifikacijski točnosti lahko drugače rečemo tudi povprečna stopnja prepoznavne (angl. *average recognition rate*).

Zanimalo me bo tudi, kako so bili razvrščeni napačno prepoznani primeri, saj lahko pri prepoznavanju obrazov pride do različnih napak razvrščanja zaradi: neenakih pogojev zajema slik (npr. parametrov sistema), sprememb biometričnih lastnosti oseb (npr. staranje), sprememb okolja (npr. osvetlitev) ali sprememb postavitve/položaja obraza. Poznamo dve vrsti napak, do katerih lahko pride pri razvrščanju: napačne potrditve (angl. *false acceptance* - *FA*) ali napačne zavrnitve (angl. *false rejection* - *FR*). Če pride do napačne potrditve, to pomeni, da je sistem osebo napačno prepoznal kot drugo osebo v njegovi podatkovni bazi (npr. sistem je Mateja identificiral kot Matica), kar lahko empirično ocenimo s stopnjo napačne potrditve (angl. *false acceptance rate* - *FAR*) (Poh in drugi 2012, 8).

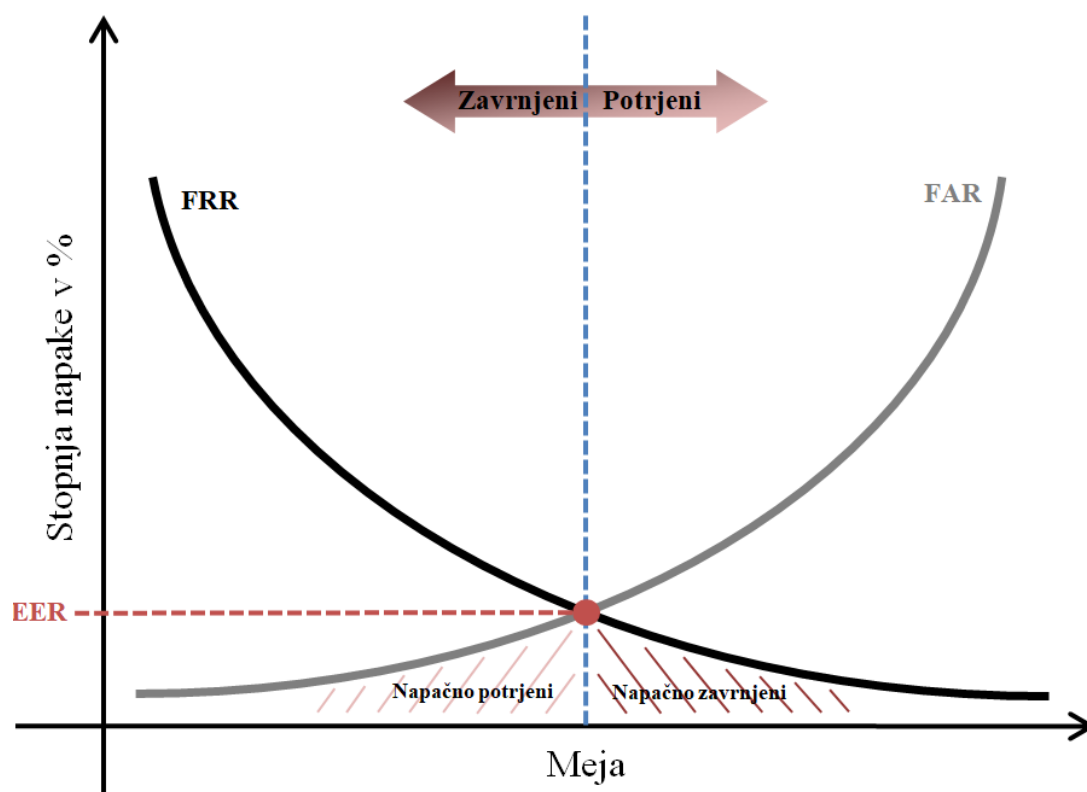
$$FAR = \frac{\text{Število napačno potrjenih primerov}}{\text{Število vseh uspešno potrjenih primerov}} \times 100$$

V primeru, ko sistem ni zmožen najti ujemanja, čeprav je slika osebe v njegovi podatkovni bazi, to napako lahko ocenimo s stopnjo napačne zavrnitve (angl. *false rejection rate* - *FRR*) (prav tam).

$$FRR = \frac{\text{Število napačno zavrnjenih primerov}}{\text{Število vseh uspešno zavrnjenih primerov}} \times 100$$

Če je sistem izredno občutljiv, ima nizko stopnjo napačne potrditve (FAR) in visoko stopnjo napačne zavrnitve (FRR). Pri manj občutljivem sistemu je situacija obratna. Manj občutljivi sistem prepozna skoraj vsakogar ($FAR > FRR$), zato je pri občutljivosti potrebno sprejeti kompromis, da sta stopnji napačne prepoznave in napačne zavrnitve kar se da enaki. Razmerje med obema napakama lahko prikažemo s pomočjo ROC krivulje (angl. *receiver operator characteristic*).

Shema 13.5: ROC krivulja



Točka na krivulji, ker sta stopnja napačne potrditve in stopnja napačne zavrnitve enaki, nam pove stopnjo enake napake (angl. *equal error rate* - *EER*). Nižja *EER* vrednost pomeni bolj natančen sistem in obratno (Brumnik in Balantič 2008, 785).

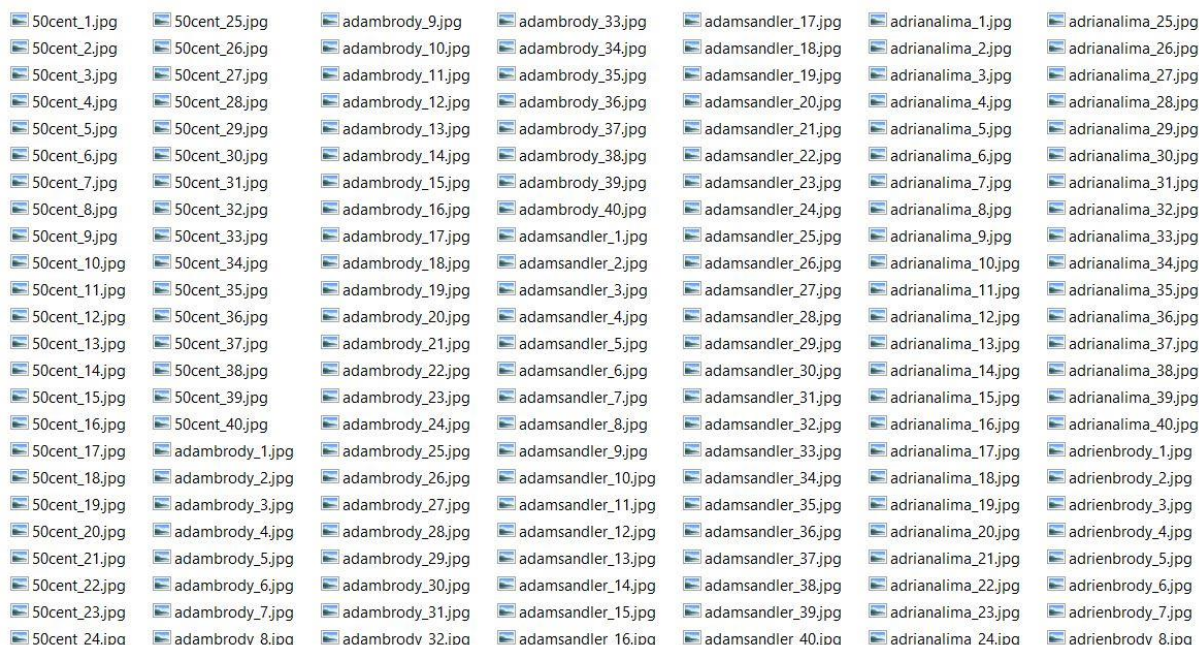
$$EER = \frac{FAR + FRR}{2}$$

13.2 Opis postopka izvedbe

Da sem prišel do kar se da primerljivih rezultatov testiranja, sem testiranje metod izvedel pri različno postavljenih mejah sprejetja in z različnim številom uporabljenih slik v fazi učenja. Najprej sem v postopku učenja uporabil štiri slike vsake slavne osebe, kar predstavlja 10 % vseh slik. V drugi fazi pa sem v postopku prepoznavanja uporabil osem slik (20 % vseh slik). Ostale slike sem uporabil v postopku prepoznavanja. S tem sem želel preveriti, ali različno število slik vpliva na rezultate prepoznavanja. Za lažjo analizo sem uporabljene slike preimenoval po imenih in priimkih oseb, ter jim dodal zaporedno številko od ena do štirideset

(glej sliko 13.1). To mi je omogočilo, da sem lahko enostavno prišel do napačno razvrščenih slik in skušal analizirati, kaj je bil vzrok, da so bile posamezne slike napačno identificirane.

Slika 13.2: Ureditve baze slike



Slike sem nato razdelil na tiste, ki bodo uporabljene za učenje, in tiste, na katerih bo potekalo prepoznavanje. V mapo Train sem prestavil slike posamezne osebe, ki bodo uporabljene v postopku učenja. Ostale slike, na katerih bo izvedena prepoznavna, pa sem prestavil v mapo Compare.

13.3 Izvedba prepoznavanja oseb

Izvedba prepoznavanja oseb je bila narejena v dveh fazah z različnim številom oseb, vključenih v prepoznavanje, ter s tremi različnimi metodami, ki jih program podpira. Uspešnost metod sem preveril z različnimi parametri, ki jih je mogoče pri vsaki metodi ročno nastaviti, tako da sem poskušal najti najbolj optimalno razmerje med številom napačno prepoznanih in neprepoznanih oseb. Pridobljeni rezultati so predstavljeni z merami učinkovitosti, predstavljenimi v poglavju 13.1. Pri primerjavi uspešnosti prepoznavanja med metodami sem upošteval najboljši rezultat posameznega algoritma.

13.3.1 Metoda lastnih obrazov (analiza glavnih komponent)

Metoda lastnih obrazov v postopku prepoznavne uporablja dva parametra, ki ju je mogoče ročno prilagajati za nastavitve učinkovitosti prepoznavne. Prvi parameter je število glavnih komponent, ki jih program obdrži pri rekonstrukciji obraza. Drugi parameter pa je prag sprejetja (angl. *prediction threshold*), ki predstavlja povprečno razdaljo med vsemi trening slikami in vsako sliko v postopku prepoznavne. Višja kot je vrednost pragu, večja je verjetnost ujemanja s sliko v postopku učenja. Če je rezultat prepoznavne za posamezno sliko nad določenim pragom sprejetja, program osebo prepozna in ji pripiše ime osebe, s katero jo je prepoznal. Vsi rezultati prepoznavne se zapišejo v .txt datoteko. Prednastavljen prag sprejetja je v programu nastavljen na vrednost 2000, zato sem prvo prepoznavo začel s to vrednostjo in jo prilagajal glede na rezultate prepoznavne. Pri vsaki metodi sem prepoznavanje izvedel s petimi različnimi pragovi sprejetja. Parametra, ki se nanaša na število glavnih komponent pri analizi, nisem spreminjal in sem obdržal njegovo prednastavljeno vrednost 80 skozi vseh pet poskusov, saj v literaturi nisem nikjer zasledil vpliva števila glavnih komponent na rezultate prepoznavne. V dokumentaciji algoritma metode je zapisano, da ni pravila, koliko glavnih komponent je priporočljivo obdržati pri rekonstrukciji obraza, saj so rezultati odvisni predvsem od vhodnih podatkov. Zato naj bi bilo 80 komponent v večini primerov zadostno število (OpenCV 2017). V spodnji tabeli so prikazani rezultati pri različnih pragovih sprejetja za metodo glavnih komponent in izračunane mere učinkovitosti prepoznavne.

Tabela 13.3: Rezultati prepoznavne metode lastnih obrazov (10 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
1700	5616	2596	788	0,624	0,462	0,140	0,301
2000	5737	2457	806	0,637	0,428	0,140	0,284
2300	5805	2388	807	0,645	0,411	0,139	0,275
2500	5823	2345	832	0,647	0,403	0,143	0,273
2700	5737	2404	859	0,637	0,419	0,150	0,284

Vir: lasten.

Iz rezultatov tabele (glej tabelo 13.1) je razvidno, da je bilo pri 10 % slik vsake osebe, ki so bile vključene v stopnji učenja z metodo lastnih obrazov, prepoznavanje najbolj učinkovito pri pragu sprejetja 2500. Pri tem pragu je bilo uspešno prepoznanih 5823 oseb od skupaj 9000 vključenih v prepoznavanje, kar predstavlja 64,7 % natančnost prepoznavne. Vrednost stopnje

enake napake (EER) znaša 0,273. Med neuspešno razvrščenimi slikami je bilo 2345 napačno prepoznanih in 832 neprepoznanih, kar skupaj znaša 3177 napačno prepoznanih oseb. Metoda je bila najmanj uspešna pri vrednosti pragu 1700, in sicer z 62,4 % natančnostjo prepoznavne in 0,301 EER.

Tabela 13.4: Rezultati prepoznavne metode lastnih obrazov (20 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
1700	5367	1972	661	0,671	0,367	0,123	0,245
2000	5397	1929	674	0,675	0,357	0,125	0,241
2300	5438	1881	681	0,680	0,346	0,125	0,236
2500	5460	1812	728	0,683	0,332	0,133	0,233
2700	5428	1795	777	0,679	0,331	0,143	0,237

Vir: lasten.

Pri 20 % slik vsake osebe, ki so bile vključene v stopnji prepoznavanja (glej tabelo 13.2), je bila metoda prav tako najuspešnejša pri pragu sprejetja 2500. Uspešnost prepoznavanja je v tem primeru znašala 68,3 % ob vrednosti EER 0,233. Skupaj neuspešno prepoznanih oseb od 8000 je bilo 2540. Najmanj uspešna je bila metoda pri pragu sprejetja 1700. Ko je bilo v postopku učenja vključenih 20 % slik, je bila metoda lastnih obrazov v primerjavi z rezultati, kjer je bilo v učenje vključenih zgolj 10 % slik, uspešnejša za 3,6 %.

13.3.2 Metoda Fisherjevih obrazov (linearna diskriminantna analiza)

Pri metodi Fisherjevih obrazov sta prav tako na voljo dva parametra, ki ju lahko poljubno nastavimo za boljšo učinkovitost razvrščanja. Prvi parameter predstavlja število komponent oz. skupin (oseb, ki jih želimo prepoznati) pri linearni diskriminantni analizi. Drugi parameter pa predstavlja prag sprejetja za neznane obraze. Če je vrednost pri prepoznavanju nad postavljenim pragom, metoda vrne vrednost -1, kar predstavlja neznano osebo. Pri razvrščanju parametra števila komponent ne bom spreminjal in bom v postopku prepoznavne obdržal vse komponente, bom pa prilagajal vrednost pragu sprejetja, kot sem to spreminjal pri metodi lastnih obrazov. Prednastavljen prag sprejetja je znašal 3500, zato sem prvo prepoznavanje izvedel s predlagano vrednostjo in nato glede na rezultate izvedel prepoznavanje še na štirih različnih pragovih sprejetja, da sem dobil kar se da najvišjo učinkovitost prepoznavanja. Rezultati prepoznavne z

metodo Fisherjevih obrazov pri različnih vrednostih pragu in 10 % slik vključenih v postopku učenja so prikazani v tabeli 13.3.

Tabela 13.5: Rezultati prepoznavne po metodi Fisherjevih obrazov (10 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
3000	5727	2492	781	0,636	0,435	0,136	0,286
3300	5825	2383	792	0,647	0,409	0,136	0,273
3500	5820	2353	827	0,647	0,404	0,142	0,273
3700	5833	2309	858	0,648	0,396	0,147	0,271
4000	5817	2292	891	0,646	0,394	0,153	0,274

Vir: lasten.

Metoda Fisherjevih obrazov je bila pri 10 % slik vsake osebe, ki so bile vključene v prepoznavo, najbolj uspešna pri pragu sprejetja 3700. Tu je metoda uspešno prepoznala 5833 slik, kar predstavlja 64,8 %. Število napačno prepoznanih oseb je bilo 2309, medtem ko je bilo neprepoznanih 858. Vrednost EER je znašala 0,271. Najslabšo učinkovitost prepoznavne je metoda dosegla pri pragu 3000, kjer je bila uspešnost 63,6 %.

Tabela 13.6: Rezultati prepoznavne po metodi Fisherjevih obrazov (20 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
3300	5405	1948	647	0,676	0,360	0,120	0,240
3500	5457	1902	641	0,682	0,349	0,117	0,233
3700	5476	1885	639	0,685	0,344	0,117	0,230
4000	5488	1842	670	0,686	0,336	0,122	0,229
4200	5396	1893	711	0,675	0,351	0,132	0,241

Vir: lasten.

Ko je bilo v postopek učenja vključenih 20 % slik vsake osebe, je bila metoda najbolj uspešna pri pragu 4000 (tabela 13.4). Njena učinkovitost je bila 68,6 %, kar je za 3,8 % več kot v primeru, ko je bilo v postopek učenja vključenih 10 % vseh slik. Vrednost EER je pri pragu 4000 znašala 0,229. Najslabšo učinkovitost je metoda dosegla pri pragu 4200, kjer je bila uspešnost 67,5 %.

13.3.3 Metoda lokalnih binarnih vzorcev

Za razliko od metode lastnih obrazov in metode Fisherjevih obrazov, je mogoče pri metodi lokalnih binarnih vzorcev spremeniti pet različnih parametrov za povečanje učinkovitosti prepoznavanja (OpenCV 2017):

- Radij: Velikost radija, uporabljenega za gradnjo krožnega lokalnega binarnega vzorca. Privzeta vrednost v dokumentaciji je ena in je pri prepoznavi ostala nespremenjena.
- Število vzorčnih točk: Število vzorčnih slikovnih točk, uporabljenih za gradnjo krožnega lokalnega binarnega vzorca. Predlagana vrednost iz dokumentacije je osem vzorčnih točk, ki je prav tako ostala nespremenjena. V dokumentaciji je dodana opomba, da je potrebno v primeru vključitve večjega števila vzorčnih točk v prepoznavo upoštevati, da je to računsko zahtevnejša operacija, za katero je potrebne več računalniške moči in več časa za prepoznavo.
- Število horizontalnih celic: Število slikovnih točk na horizontalni osi. Predlagana vrednost je osem in je ostala nespremenjena. Večje kot je število vključenih celic, gostejša je mreža in večja je dimenzija dobljenega vektorja.
- Število vertikalnih celic: Število slikovnih točk na vertikalni osi. Predlagana vrednost je osem in je ostala nespremenjena. Večje kot je število vključenih celic, gostejša je mreža in večja je dimenzija dobljenega vektorja.
- Prag sprejetja: Če je vrednost pri prepoznavanju nad postavljenim pragom, potem metoda vrne vrednost -1, kar predstavlja neznano osebo. Vrednost pragu sprejetja je edini parameter, ki ga bom pri metodi lokalnih binarnih vzorcev prilagajal. Prvotno je bila vrednost nastavljena na 100, kar mi je tudi predstavljalo referenčni prag za začetek prepoznave, ki sem ga nato spremenil še štirikrat glede na dobljene rezultate prepoznave.

Tabela 13.7: Rezultati prepoznavne metode lokalnih binarnih vzorcev (10 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
80	5799	2378	823	0,644	0,410	0,142	0,276
100	5844	2357	799	0,649	0,403	0,137	0,270
120	5845	2348	807	0,649	0,402	0,138	0,270
150	5863	2274	863	0,651	0,388	0,147	0,268
170	5833	2280	887	0,648	0,391	0,152	0,271

Vir: lasten.

Za najučinkovitejšo vrednost pragu prepoznavanja se je pri metodi lokalnih binarnih vzorcev ob 10 % slik, vključenih v postopku učenja, pokazala vrednost 150 (glej tabelo 13.5). Metoda je imela uspešnost pri tem pragu 65,1 %. Vseh uspešno prepoznanih oseb je bilo 5863. Vrednost EER znaša 0,268. Najmanj učinkovita je bila metoda pri pragu sprejetja 80, z 64,4 % uspešnostjo.

Tabela 13.8: Rezultati prepoznavne metode lokalnih binarnih vzorcev (20 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
70	5494	1832	674	0,687	0,333	0,123	0,228
80	5530	1758	712	0,691	0,318	0,129	0,223
100	5523	1747	730	0,690	0,316	0,132	0,224
120	5615	1641	744	0,702	0,292	0,133	0,212
150	5556	1621	823	0,695	0,292	0,148	0,220

Vir: lasten.

Ko je bilo v postopku učenja vključenih 20 % slik, je bila metoda lokalnih binarnih vzorcev najuspešnejša pri pragu sprejetja 120, kjer je dosegla 70,2 % uspešnost prepoznave (tabela 13.6). To je v primerjavi s prepoznavo, ko je bilo v učenje vključenih 10 % slik, 5,1 % izboljšanje. Stopnja enake napake znaša v tem primeru 0,212. Najslabšo uspešnost prepoznave je metoda dosegla pri pragu sprejetja 70, kjer je imela zgolj 68,7 % uspešnost ob vrednosti EER 0,288.

13.3.4 Primerjava uspešnosti med metodami glede na število slik, vključenih v prepoznavo

V zaključku analize bom primerjal še uspešnost med metodami, in sicer ločeno glede na število slik, vključenih v postopku učenja.

Tabela 13.9: Rezultati prepoznavne uspešnosti med metodami (10 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
Metoda lastnih obrazov	5823	2345	832	0,647	0,403	0,143	0,273
Metoda Fisherjevih obrazov	5833	2309	858	0,648	0,396	0,147	0,271
Metoda lokalnih binarnih vzorcev	5863	2274	863	0,651	0,388	0,147	0,268

Vir: lasten.

Iz tabele 13.7 je razvidno, da je bila pri prepoznavi, kjer je bilo pri učenju vključenih 10 % slik vsake osebe, najuspešnejša metoda lokalnih binarnih vzorcev, katere vrednost EER je znašala 0,267. Druga najuspešnejša metoda je bila metoda Fisherjevih obrazov z vrednostjo EER 0,271 in nato metoda lastnih obrazov z vrednostjo EER 0,273. Razlike v uspešnosti prepoznavanja med metodami so majhne, kar je razvidno iz deleža uspešno prepoznanih oseb, saj je razlika med najbolj in najmanj uspešno metodo zgolj 0,4 %.

Tabela 13.10: Rezultati prepoznavne uspešnosti med metodami (20 % slik v postopku učenja)

Meja	Število prepoznanih	Število napačno prepoznanih	Število neprepoznanih	T	FAR	FRR	EER
Metoda lastnih obrazov	5460	1812	728	0,683	0,332	0,133	0,233
Metoda Fisherjevih obrazov	5488	1842	670	0,686	0,336	0,122	0,229
Metoda lokalnih binarnih vzorcev	5615	1641	744	0,702	0,292	0,133	0,212

Vir: lasten.

Ko je bilo v postopek učenja vključenih 20 % slik vsake osebe, je bila prav tako najuspešnejša metoda lokalnih binarnih vzorcev. Njena stopnja enake napake je znašala 0,212. Na drugem mestu je metoda Fisherjevih obrazov (EER 0,229), za tem pa sledi metoda lastnih obrazov (0,233). Iz vrednosti EER je razvidno, da večjih razlik pri prepoznavanju med metodo lastnih obrazov in metodo Fisherjevih obrazov ni, saj je bila razlika med deležema uspešno prepoznanih oseb le 0,3 %. Večja razlika pri uspešnosti prepoznavanja je opazna pri metodi lokalnih binarnih vzorcev, saj je bila metoda pri 20 % slik, vključenih v učenje, uspešnejša od metode Fisherjevih obrazov za 1,6 %.

14 SKLEP

Z magistrskim delom sem želel podrobneje analizirati delovanje različnih metod prepoznavanja obrazov, ki se lahko uporabljajo za uporabo v komercialne namene. V raziskovanje me je pritegnila vedno večja razširjenost programov in aplikacij, ki jih vsakodnevno uporabljamo in vsebujejo algoritme za prepoznavo obrazov. Predvsem me je zanimal način delovanja, njihova učinkovitost in uporabnost. V ta namen sem podrobneje raziskal delovanje treh metod, in sicer metodo glavnih komponent, metodo Fisherjevih obrazov in metodo lokalnih binarnih vzorcev ter med njimi primerjal dobljene rezultate prepoznave.

Rezultati izvedbe prepoznavanja oseb na prosto dostopnem programu in zbirki slik slavnih oseb so pokazali, da so komercialni algoritmi prepoznavanja učinkoviti, saj je bila povprečna uspešnost vseh treh uporabljenih algoritmov pri 10 % vseh slik, vključenih v prepoznavanje, 64,9 %, medtem ko je bila pri 20 % slik uspešnost 69 %. Čeprav rezultati niso na ravni najboljših komercialnih programov, ki se uporabljajo za prepoznavanje oseb, lahko potrdim svojo tezo, da je uporaba komercialno dostopnih programov za prepoznavanje obrazov dovolj razvita za praktično uporabo, saj je njihova zanesljivost primerljiva z rezultati učinkovitosti algoritmov, uporabljenih pri drugih raziskavah (glej poglavje 9).

Iz analize je razvidno tudi, da ima število slik oseb, vključenih v postopku učenja, vpliv na rezultate prepoznavanja, saj so bili rezultati prepoznave v primeru, ko je bilo v postopku učenja vključenih 20 % slik, v povprečju za 5 % boljši kot v primeru, ko je bilo v postopku učenja vključenih 10 % slik. Pokazal se je tudi vpliv števila slik, uporabljenih v postopku učenja, na učinkovitost prepoznave uporabljenih algoritmov. Razlike med algoritmi so bile namreč večje, ko je bilo v postopku učenja vključenih več slik.

Prav tako so se pokazale razlike med holističnimi oz. globalnimi tehnikami, ki za prepoznavanje uporabljajo lastnosti celotnega obraza, ter med lokalnimi oz. strukturnimi tehnikami, ki se osredotočajo na lokalne značilnosti obraza. Rezultati so pokazali, da so lokalne tehnike, kamor spada metoda lokalnih binarnih vzorcev, uspešnejše pri prepoznavanju od holističnih tehnik, med katere spadata metoda lastnih obrazov in metoda Fisherjevih obrazov. Metoda lokalnih binarnih vzorcev je bila uspešnejša pri prepoznavanju pri 10 % in 20 % slik, vključenih v postopku učenja, od metode lastnih obrazov in metode Fisherjevih obrazov. Razlike med tehnikami so bile izrazitejše, ko je bilo v postopek učenja vključenih več oseb, saj je znašala

razlika med metodo lokalnih binarnih vzorcev, ko je bilo v postopku učenja uporabljenih 20 % slik, in ostalima dvema metodama 1,6 %. Ko je bilo v postopek učenja vključenih 10 % slik, je ta razlika znašala zgolj 0,3 %.

Tekom izvedbe raziskave sem opazil nekaj pomanjkljivosti izdelanega programa, uporabljene baze podatkov in postopka prepoznavanja, ki imajo vpliv na učinkovitost prepoznav. Glavne težave komercialnih sistemov za prepoznavanje obrazov, ki sem jih identificiral v magistrski nalogi, se nanašajo na detekcijo obrazov, uporabo ob nenaravnih pogojih (osvetlitev, postavitev obraza), velikost in kvaliteto slik ter velikost baze. Te pomanjkljivosti so predstavljene v nadaljevanju in so zajete v pripombah in navodilih za nadaljnje raziskovanje.

Analiza dobljenih rezultatov je pokazala, da je bilo prepoznavanje veliko bolj učinkovito pri slikah, na katerih je bila postavitev obraza osebe frontalna in ki so bile zajete v boljših svetlobnih pogojih. Pojavlja se vprašanje učinkovitosti programa ob nenaravnih pogojih, čeprav to pri komercialnih sistemih ni tako pomembno kot pri varnostnih, saj so slike večinoma zajete v dobrih svetlobnih pogojih in s frontalno postavitvijo obraza. Hkrati so bile za prepoznavo izbrane le slike, na katerih se pojavi ena oseba (zaradi lažje analize dobljenih rezultatov), kar bi prav tako lahko imelo vpliv na rezultate prepoznav, če bi slike vsebovale več oseb, ki bi jih bilo potrebno prepoznati.

Pregled rezultatov prepoznav je pokazal tudi težave pri zaznavanju obrazov. Program je v določenih primerih v ozadju zaznal drug obraz, ki ga je uporabil pri prepoznavanju, in ne želenega, ki je bil postavljen v ospredje. Pojavilo se je tudi nekaj primerov, kjer na sliki ni bilo zaznanega obraza (slika 14.1) ali pa je program namesto obraza zaznal nekaj drugega (slika 14.2). Zato je potrebno pri izdelavi programa za prepoznavanje nameniti dovolj pozornosti uporabljenemu algoritmu za detekcijo obraza. Brez učinkovitega algoritma za zaznavanje obrazov namreč ni mogoče narediti učinkovitega programa za prepoznavanje obrazov, saj obrazi ne bodo zaznani ali pa bodo napačno zaznani. Ker težav z detekcijo obrazov nisem predvidel pri izdelavi programa, slik, pri katerih ni bilo zaznanih obrazov ali pa so bili ti napačno zaznani, nisem mogel izločiti od napačno prepoznanih ali neprepoznanih. Pri nadaljnjem raziskovanju bi se bilo potrebno posvetiti tudi napakam, do katerih pride v postopku zaznavanja obrazov, in jih razvrstiti v posebno kategorijo.

Slika 14.1.: Primeri slik, kjer niso bili zaznani obrazi



Vir: lasten.

Slika 14.2.: Primer slike z napačno detekcijo obraza



Vir: lasten.

Pri nadaljnjem raziskovanju metod prepoznavanja obrazov bi bilo potrebno primerjati učinkovitost metod ob izdatnejšemu prilagajanju njihovih parametrov. Na primer povečanju ali zmanjšanju števila glavnih komponent pri metodi glavnih komponent ali različno velikega radija pri metodi lokalnih binarnih vzorcev. Že samo s prilagajanjem pragu sprejetja sem uspel doseči višjo učinkovitost prepoznavanja, zato predvidevam, da bi s podrobnim prilagajanjem vseh parametrov lahko dosegel še večjo učinkovitost prepoznavanja. Ob tem je potrebno upoštevati dejstvo, da lahko spreminjanje določenih parametrov znatno vpliva na čas, ki je potreben za prepoznavo. Določene računske operacije, ki potekajo med prepoznavo, so izredno zahtevne in zahtevajo veliko računalniške moči. Nastavitve parametrov so zato v veliki meri odvisne od samega namena uporabe programa za prepoznavanje in strojne opreme, ki nam je na voljo. Pretehtati je potrebno, ali nam je pri prepoznavanju pomembnejši čas, ki je potreben

za prepoznavo določene osebe, ali njegova učinkovitost. Že pri sedanjih parametrih in količini slike, je prepoznavanje na 9000 in 8000 slikah potekalo od 13 do 21 minut.

Na učinkovitost prepoznavanja vpliva tudi velikost in kakovost uporabljenih slik. Analiza je bila v mojem primeru narejena na manjših slikah, katerih velikost je znašala 160 slikovnih točk glede na višino ali širino slike ($160 \times x$ ali $x \times 160$). Uporaba manjših slik pri prepoznavanju ni vedno slabost in je tako kot pri parametrih prepoznavne, odvisna od namena programa. Velikost vhodnih slik namreč vpliva na hitrost in učinkovitost prepoznavne. Zato je potrebno slike, v primeru, da nam je pomembnejša hitrost programa od učinkovitosti, pred postopkom detekcije ustrezno pomanjšati.

Zadnji dejavnik, ki vpliva na hitrost prepoznavanja, pa je število oseb, ki jih želimo prepoznati. Če naša baza šteje nekaj 100 oseb, potem bo prepoznavanje počasnejše, kot če jih šteje nekaj deset, saj mora program preveriti tolikokrat večjo podatkovno bazo. Vse omenjene dejavnike, ki vplivajo na učinkovitost in hitrost prepoznavne, je potrebno pri izdelavi programa upoštevati in med njimi najti pravi kompromis, ki nam bo najbolj ustrezal glede na namen uporabe programa.

Ker imajo vse metode prepoznavanja obrazov svoje prednosti in pomanjkljivosti, je v prihodnosti mogoče pričakovati pojav programov, ki bodo uporabljali kombinacije več različnih metod, s čimer se bodo odpravile njihove pomanjkljivosti. Prav tako so študije pokazale, da so sistemi za prepoznavanje obrazov manj učinkoviti pri slikah ljudi v nenaravnih pogojih, kot je na primer slaba resolucija in slaba osvetlitev obraza, saj je te pogoje težko matematično opisati in jih implicirati v algoritmu. Odprava teh težav je zagotovo eden izmed večjih izzivov, s katerimi se bodo morali razvijalci sistemov prepoznavanja obrazov soočiti, da bodo le-ti bolj uporabni in učinkoviti.

Razvoj avtomatskega prepoznavanja obrazov je od leta 1964 izredno napredoval in se še naprej hitro razvija. Tehnologije, ki so nam na voljo danes, omogočajo širitev uporabe tehnologij za prepoznavanje obrazov na vsa področja našega življenja, saj senzor kamere predstavlja majhen strošek izdelave in ga je enostavno vgraditi v vsako napravo. Zato se moramo začeti zavedati, da bo avtomatsko prepoznavanje kmalu prisotno vsepovsod in bo znatno oblikovalo potek našega življenja.

15 LITERATURA

1. 360biometrics. 2017. Hand features. Dostopno prek: http://www.360biometrics.com/img/hand_features.gif (1. avgust 2017).
2. ABC News. 2016. *Facial recognition technology to become part of SA Police toolkit*. Dostopno prek: <http://www.abc.net.au/news/2016-08-01/sa-police-to-start-using-facial-recognition-technology/7677382> (1. avgust 2017).
3. Ahonen, Timo, Abdenour Hadid in Matti Pietikäinen. 2004. Face Recognition with Local Binary Patterns. V *Computer Vision - ECCV 2004*, ur. Pajdla, Tomás in Jiří Matas, 469–481. Springer: Berlin, Heidelberg. Dostopno prek: https://link.springer.com/chapter/10.1007/978-3-540-24670-1_36 (1. avgust 2017).
4. Banisar, David in Simon Davies. 1999. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *Journal of Computer & Information Law* 18 (1): 3–113. Dostopno prek: <http://repository.jmls.edu/cgi/viewcontent.cgi?article=1174&context=jitpl> (1. avgust 2017).
5. Becker, Brian C. in Enrique Ortiz. 2008. Evaluation of face recognition techniques for application to facebook. *8th IEEE International Conference on Automatic Face & Gesture Recognition, 2008*: 1–6. Dostopno prek: <http://ieeexplore.ieee.org/document/4813471/> (1. avgust 2017).
6. Belhumeur, Peter N., João P. Hespanha in David J. Kriegman. 1997. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. V *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19 (7): 711–720. Dostopno prek: <https://cseweb.ucsd.edu/classes/wi14/cse152-a/fisherface-pami97.pdf> (1. avgust 2017).
7. Belsey, Andrew. 1992. Privacy, publicity and politics. V *Ethical Issues in Journalism*, ur. Belsey, Andrew in Ruth Chadwick, 77–92. London in New York: Routledge. Dostopno prek: <https://books.google.si/books?id=qhW2UJLQLFMC&hl=sl> (1. avgust 2017).
8. Bowyer, Kevin W. 2004. Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine* 23 (1): 9–20. Dostopno prek: <http://ieeexplore.ieee.org/document/1273467/> (1. avgust 2017).
9. Brey, Philip. 2004. Ethical Aspects of Face Recognition Systems in Public Places. *Journal of Information, Communication & Ethics in Society* 2 (2): 97–109. Dostopno

- prek: <http://www.emeraldinsight.com/doi/abs/10.1108/14779960480000246> (1. avgust 2017).
10. Brumnik, Robert in Zvone Balantič. 2008. Reliability and Efficacy of Identification Systems and Supply Chain Management. V *Strojniški vestnik - Journal of Mechanical Engineering* 54 (11): 783–795. Dostopno prek: <https://www.dlib.si/details/URN:NBN:SI:DOC-8LWUO0AB/> (1. avgust 2017).
 11. Bucholtz, Ann in Amy Davis. 2015. *Forensic Studies: CSI for the Nonscientist: From Crime Scene to Crime Lab*. LawTech Publishing Group. Dostopno prek: https://books.google.si/books/about/Forensic_Studies_CSI_for_the_Nonscientist.html?id=2nKfCgAAQBAJ&redir_esc=y (1. avgust 2017).
 12. CBC News. 2014. *Facial recognition software to aid Calgary police in future investigations*. Dostopno prek: <http://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1.2822592> (1. avgust 2017).
 13. Cho, Hyunjong, Rodney Roberts, Bowon Jung, Okkyung Choi in Seungbin Moon. 2014. An Efficient Hybrid FaceRecognition Algorithm Using PCA and GABOR Wavelets. *International Journal of Advanced Robotic Systems* 11 (4): 1–8. Dostopno prek: <http://journals.sagepub.com/doi/full/10.5772/58473> (1. avgust 2017).
 14. Clottes, Jean. 2002. Chauvet Cave (ca. 30,000 B.C.). *The Metropolitan Museum of Art*. Dostopno prek: http://www.metmuseum.org/toah/hd/chav/hd_chav.htm (1. avgust 2017).
 15. Code Project. 2014. *EMGU Multiple Face Recognition using PCA and Parallel Optimisation*. Dostopno prek: <https://www.codeproject.com/articles/261550/emgu-multiple-face-recognition-using-pca-and-paral> (1. avgust 2017).
 16. Deleuze, Gilles in Antonio Negri. 2002. Družba nadzora: Gilles Deleuze: intervju s Tonijem Negrijem. *Filozofski vestnik* 23 (3): 167–177. Dostopno prek: <https://ojs.zrc-sazu.si/filozofski-vestnik/article/download/3575/3270> (1. avgust 2017).
 17. *Zakon o varstvu osebnih podatkov (ZVOP-1)*. Uradni list RS, št. 94/2007. Dostopno prek: <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906#> (1. avgust 2017).
 18. *Ustava Republike Slovenije*. Uradni list RS, št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 in 47/13. Dostopno prek: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=199133&stevilka=1409> (1. avgust 2017).

19. *Zakon o elektronskih komunikacijah (ZEKOM-1)*. Uradni list RS, št. 13/07, 102/07, 110/09, 33/11 in 109/12. Dostopno prek: <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3781> (1. avgust 2017).
20. *Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov*. 1995. Dostopno prek: <http://eur-lex.europa.eu/legalcontent/SL/TXT/PDF/?uri=CELEX:31995L0046&from=SL> (1. avgust 2017).
21. *Uredba (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)*. 2006. Dostopno prek: <http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679&from=SL> (1. avgust 2017).
22. Fine Art America. 2017. *Man's Face Thermogram Photograph by Tony Mcconnell*. Dostopno prek: <https://render.fineartamerica.com/images/rendered/search/poster/images-medium-5/3-mans-face-thermogram-tony-mcconnell.jpg> (1. avgust 2017).
23. Foucault, Michel. 1984. *Nadzorovanje in kaznovanje*. Ljubljana: Delavska enotnost.
24. *Splošna deklaracija človekovih pravic*. 1948. Dostopno prek: <http://www.varuh-rs.si/pravni-okvir-in-pristojnosti/mednarodni-pravni-akti-s-podrocja-clovekovih-pravic/organizacija-zdruzenih-narodov/splosna-deklaracija-clovekovih-pravic/> (1. avgust 2017).
25. Graham, Stephen in David Wood. 2003. Digitizing surveillance: categorization, space, inequality. *Critical Social Policy* 23 (2): 227–248. Dostopno prek: <http://journals.sagepub.com/doi/abs/10.1177/0261018303023002006?journalCode=cs pa> (1. avgust 2017).
26. Gray, Mitchell. 2003. Urban Surveillance and Panopticism: will we recognize the facial recognition society? V *Surveillance and Society* 1 (3), ur. Norris, McCahill in David Wood, 314–330. Dostopno prek: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3343> (1. avgust 2017).
27. Horiuchi, Takedo in Takuro Hada. 2013. A Complementary Study for the Evaluation of Face Recognition Technology. *Proceedings of the 47th international Carnahan Conference on Security Technologies (ICCST)*: 1–5. Dostopno prek: <http://ieeexplore.ieee.org/document/6922048/> (1. avgust 2017).
28. Hossain, Sarker Mohammad Sabbir, Abu Yousuf in Muhammad Sheikh Sadi. 2015. Towards an efficient face recognition approach. *International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*: 1–5. Dostopno prek: <http://ieeexplore.ieee.org/document/7307375/> (1. avgust 2017).

29. House of Commons Science and Technology Committee. 2015. *Current and Future Uses of Biometric Data and Technologies: Sixth Report of Session 2014-15, Report, Together with Formal Minutes Relating to the Report*. Dostopno prek: <https://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf> (1. avgust 2017).
30. Hjelmås, Erik in Boon Kee Low. 2001. Face Detection: A Survey. V *Computer Vision and Image Understanding* 83 (3), ur. Paragios Nikos, 236–274. Dostopno prek: <http://www.sciencedirect.com/science/article/pii/S107731420190921X> (1. avgust 2017).
31. Huang, Thomas, Ziyong Xiong, in Zhenqiu Zhang. 2011. Face Recognition Applications. V *Handbook of Face Recognition*, ur. Li, Stan Z in Anil K. Jain, 617–638. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).
32. Illinois Image Formation and Processing. 2017. *Face Recognition under varying illumination*. Dostopno prek: <http://www.ifp.illinois.edu/~tchen5/respic/wei.jpg> (1. avgust 2017).
33. Introna, Lucas D. in David Wood. 2004. Picturing algorithmic surveillance: the politics of facial recognition systems. V *Surveillance and Society* 2 (2/3), ur. Norris, McCahill in David Wood, 177–198. Dostopno prek: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3373> (1. avgust 2017).
34. Jain, Anil K., Arun Ross in Salil Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14 (1): 4–20. Dostopno prek: <http://ieeexplore.ieee.org/document/1262027/> (1. avgust 2017).
35. Jang, Unsoo in Eui Chul Lee. 2016. Performance Analysis of Pixel based Face Recognition Methods. *International Journal of Bio-Science and Bio-Technology* 8 (2): 97–206. Dostopno prek: http://www.sersc.org/journals/IJBSBT/vol8_no2/18.pdf (1. avgust 2017).
36. Kadiya, Hardik. 2012. Comparative Study on Face Recognition Using HGPP, PCA, LDA, ICA and SVM. *Global Journal of Computer Science and Technology Graphics & Vision* 12 (15): 55–58. Dostopno prek: [https://globaljournals.org/GJCST_Volume12/E-Journal_GJCST_\(F\)_Vol_12_Issue_15.pdf](https://globaljournals.org/GJCST_Volume12/E-Journal_GJCST_(F)_Vol_12_Issue_15.pdf) (1. avgust 2017).
37. Kämäräinen, Joni-Kristian, Abdenour Hadid in Matti Pietikäinen. 2011. Local Representation of Facial Features. V *Handbook of Face Recognition*, ur. Li, Stan Z in

- Anil K. Jain, 79–108. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).
38. Kindt, Els J. 2013. An Introduction into the Use of Biometric Technology. V *Privacy and Data Protection Issues of Biometric Applications 12*: 15–85. Dostopno prek: http://link.springer.com/chapter/10.1007/978-94-007-7522-0_2 (1. avgust 2017).
39. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije. Dostopno prek: http://www2.mirovni-institut.si/slo_html/publikacije/pdf/MI_politike_zasebnost_na_internetu.pdf (1. avgust 2017).
40. Lenc, Ladislav in Pavel Král. 2015. Unconstrained Facial Images: Database for Face Recognition under Real-world Conditions. V *Mexican International Conference on Artificial Intelligence (MICAI 2015)*, ur. Pichardo Lagunas, Obdulia, Oscar Herrera Alcántara in Gustavo Arroyo Figueroa. Dostopno prek: https://link.springer.com/chapter/10.1007/978-3-319-27101-9_26 (1. avgust 2017).
41. Lyon, David. 1994. *The Electronic Eye*. Cambridge: Polity Press/Blackwell.
42. --- 2001. *Surveillance Society*. Buckingham: Open University Press.
43. Li, Stan Z in Anil K. Jain. 2011. Introduction. V *Handbook of Face Recognition*, ur. Li, Stan Z in Anil K. Jain, 1–15. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).
44. --- in Jianxin Wu. 2011. Face Detection. V *Handbook of Face Recognition*, ur. Li, Stan Z in Anil K. Jain, 277–303. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).
45. Liu, Yi-Shin, Wai-Seng Ng in Chun-Wei Liu. 2009. *A Comparison of Different Face Recognition Algorithms*. Dostopno prek: https://www.researchgate.net/publication/239585582_A_Comparison_of_Different_Face_Recognition_Algorithms (1. avgust 2017).
46. Liton, Chandra Paul in Al Sumam Abdulla. 2012. Face Recognition Using Principal Component Analysis Method. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1 (9)*: 135–139. Dostopno prek: <http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-9-135-139.pdf> (1. avgust 2017).
47. Marx, Karl. 1986. *Kapital: Kritika politične ekonomije*. Ljubljana: Cankarjeva založba.

48. Mladina. 2012. *FBI vzpostavlja sistem prepoznavanja obrazov*. Dostopno prek: <http://www.mladina.si/115710/fbi-vzpostavlja-sistem-prepoznavanja-obrazov/> (1. avgust 2017).
49. Nlets – the International Justice and Public Safety Network. 2011. *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*. Dostopno prek: https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (1. avgust 2017).
50. Ocular Albinism. 2017. *Retina Scans*. Dostopno prek: <https://ocularalbinism.files.wordpress.com/2010/05/biggington-joan-le2.jpg> (1. avgust 2017).
51. Ojala, Timo, Matti Pietikäinen in Topi Mäenpää. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24 (7): 971–987. Dostopno prek: <http://dl.acm.org/citation.cfm?id=628808> (1. avgust 2017).
52. OpenCV. 2017. Dostopno prek: <http://opencv.org/> (1. avgust 2017).
53. Pabbaraju, Aditya in Srujan Kumar Puchakayala. 2010. *Face Recognition in Mobile Devices*. Dostopno prek: http://web.eecs.umich.edu/~silvio/teaching/EECS598_2010/final_report/Aditya_Srujan.pdf (1. avgust 2017).
54. Parmar, Divyarajsinh N. in Brijesh B. Mehta. 2013. Face Recognition Methods & Applications. V *International Journal of Computer Technology & Applications* 4 (1): 84–86. Dostopno prek: <https://arxiv.org/abs/1403.0485> (1. avgust 2017).
55. Peng, Yuxi, Berk Gökberk. Luuk Spreeuwers in Raymond Veldhuis. 2012. An Evaluation of Super-Resolution for Face Recognition. *33rd WIC Symposium on Information Theory in the Benelux*: 36–43. Dostopno prek: <http://doc.utwente.nl/80869/> (1. avgust 2017).
56. Phillips, P. Jonathon, Patrick Grother, Ross Micheals, Duane M. Blackburn, Elham Tabassi in Mike Bone. 2003. Face recognition vendor test 2002: evaluation report. *IEEE International Workshop on Analysis and Modeling of Faces and Gestures, AMFG 2003*. Dostopno prek: <http://ieeexplore.ieee.org/document/1240822/> (1. avgust 2017).
57. Phillips, P. Jonathon, Patrick Grother in Ross Micheals. 2011. Evaluation Methods in Face Recognition. V *Handbook of Face Recognition*, ur. Li, Stan Z in Anil K. Jain, 551–603. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).

58. Poh, N, C-H. Chan, J. Kittler, Julian Fierrez in Javier Galbally. 2012. *Description of Metrics For the Evaluation of Biometric Performance*. Dostopno prek: <https://www.beat-eu.org/project/deliverables-public/d3.3-description-of-metrics-for-the-evaluation-of-biometric-performance> (1. avgust 2017).
59. Sadeghi, Ahmad-Reza, Thomas Schneider in Immo Wehrenberg. 2009. *Efficient Privacy-Preserving Face Recognition*. Dostopno prek: http://link.springer.com/chapter/10.1007/978-3-642-14423-3_16 (1. avgust 2017).
60. Shakhnarovich, Gregory in Baback Moghaddam. 2011. V *Handbook of Face Recognition*, ur. Li, Stan Z in Anil K. Jain, 19–49. London: Springer London. Dostopno prek: <http://www.springer.com/us/book/9780857299314> (1. avgust 2017).
61. Shi, Shin. 2013. *Emgu CV Essentials*. Birmingham: Packt Publishing Dostopno prek: <https://www.packtpub.com/application-development/emgu-cv-essentials> (1. avgust 2017).
62. Slotech. 2011. *Facebook uvaja prepoznavanje obrazov*. Dostopno prek: <https://slo-tech.com/novice/t470909> (1. avgust 2017).
63. Smith, Lindsay I. 2002. A tutorial on principal components analysis. Dostopno prek: http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf (1. avgust 2017).
64. Suhas, Satonkar, Kurhe Ajay B. in Prakash Khanale B. 2012. Face Recognition Using Principal Component Analysis and Linear Discriminant Analysis on Holistic Approach in Facial Images Database. V *IOSR Journal of Engineering* 2 (12): 15–23. Dostopno prek: <https://pdfs.semanticscholar.org/222a/53efab0013a2385c3d0a8eb814cc0c9f0387.pdf> (1. avgust 2017).
65. Techclinch. 2017. *Facial recognition data points*. Dostopno prek: <http://www.techclinch.com/wp-content/uploads/2015/04/facial-recognition-data-points-820x437.jpg> (1. avgust 2017).
66. The Verge. 2015. *Snapchat introduces a 'lens store' to adorn your selfies with 99-cent filters*. Dostopno prek: <http://www.theverge.com/2015/11/13/9700312/snapchat-lens-store> (1. avgust 2017).
67. Universitat Politècnica de Catalunya. 2017. *Example of a person ID on the database (different pose views)*. Dostopno prek: <https://gtav.upc.edu/en/research-areas/faceposeid1> (1. avgust 2017).
68. *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin*. 1994. Dostopno prek: <http://www.varuh-rs.si/index.php?id=108> (1. avgust 2017).

69. Viral Forest. 2017. *Abandoned Presidio Modelo prison in Cuba*. Dostopno prek: <http://vrf.wpengine.netdna-cdn.com/wp-content/uploads/2014/12/abandoned-prison-in-cuba-031.jpg> (1. avgust 2017).
70. Wagner, Andrew, John Wright, Arvind Ganesh, Zihan Zhou, Hossein Mobahi in Yi Ma. 2012. Toward a Practical Face Recognition System: Robust Alignment and Illumination by Sparse Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 34 (2): 372–386. Dostopno prek: <http://ieeexplore.ieee.org/document/5871642/> (1. avgust 2017).
71. Weber, Max. 1981. *The Theory of Social and Economic Organization*. Oxford: Oxford University Press.
72. Welinder, Yana. 2012. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. V *Harvard Journal of Law and Technology* 26(1), ur. Li, Xiang, 166–240. Dostopno prek: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108 (1. avgust 2017).
73. Wideshut. 2017. *DNA*. Dostopno prek: <http://wideshut.co.uk/wp-content/uploads/2013/07/DNA1.jpg> (1. avgust 2017).
74. Wikimedia commons. 2017. *Left palm print*. Dostopno prek: https://upload.wikimedia.org/wikipedia/commons/thumb/8/89/Left_palm_print_-_1.gif/785px-Left_palm_print_-_1.gif (1. avgust 2017).
75. Wikimedia commons. 2017. *Colour Iris*. Dostopno prek: <https://upload.wikimedia.org/wikipedia/commons/d/d7/ColourIris.png> (1. avgust 2017).
76. Winsupersite. 2017. *Fingerprint*. Dostopno prek: <http://winsupersite.com/site-files/winsupersite.com/files/uploads/2015/05/fingerprint.png> (1. avgust 2017).
77. Microsoft Research. 2012. *MSRA-CFW: Data Set of Celebrity Faces on the Web*. Dostopno prek: <http://research.microsoft.com/en-us/projects/msra-cfw/> (1. avgust 2017).
78. Murakami Wood, David, Kristie Ball, David Lyon, Clive Norris in Charles Raab. 2006. *A Report on the Surveillance Society*. Dostopno prek: <https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf> (1. avgust 2017).
79. Zhao, Wenyi, Rama Chellappa, P. Jonathon Phillips in Azriel Rosenfeld. 2003. Face recognition: a literature survey. *ACM Computing Surveys* 35 (4): 399–458. Dostopno prek: <http://dl.acm.org/citation.cfm?id=954342> (1. avgust 2017).

80. Zuhaer, Mustafa and Nayef Al-Dabagh. 2014. Face Recognition Using LBP, FLD and SVM with Single Training Sample Per Person. *International Journal of Scientific & Engineering Research* 5 (5): 180–183. Dostopno prek: <https://www.semanticscholar.org/paper/Face-Recognition-Using-LBP-FLD-and-SVM-with-Single-Zuhaer-Al-Dabagh/437b6c2e703e3b4c391b05ef9ad4517e58f4650a> (1. avgust 2017).
81. Zhang, Xiao, Lei Zhang, Xin-Jing Wang in Heung-Yeung Shum. 2012. Finding Celebrities in Billions of Web Images. V *IEEE Transactions on Multimedia*, 14 (4), ur. Zhu, Wenwu, 995–1007. Dostopno prek: <http://ieeexplore.ieee.org/document/6140979/> (1. avgust 2017).

PRILOGA: SEZNAM OSEB, UPORABLJENIH PRI PREPOZNAVANJU

Št.	Ime in priimek	Spol	Področje
1.	50 Cent	moški	glasba
2.	Adam Brody	moški	igralstvo
3.	Adam Sandler	moški	igralstvo
4.	Adriana Lima	ženski	igralstvo
5.	Adrien Brody	moški	igralstvo
6.	Al Pacino	moški	igralstvo
7.	Alanis Morissette	ženski	glasba
8.	Alex Ferguson	moški	šport
9.	Alexis Bledel	ženski	igralstvo
10.	Alicia Keys	ženski	glasba
11.	Alyssa Milano	ženski	igralstvo
12.	Amy Winehouse	ženski	glasba
13.	Andy Garcia	moški	igralstvo
14.	Angela Merkel	ženski	politika
15.	Angelina Jolie	ženski	igralstvo
16.	Anne Hathaway	ženski	igralstvo
17.	Anthony Hopkins	moški	igralstvo
18.	Antonio Banderas	moški	igralstvo
19.	Arnold Schwarzenegger	moški	igralstvo
20.	Ashley Olsen	ženski	igralstvo
21.	Avril Lavigne	ženski	glasba
22.	Barack Obama	moški	politika
23.	Ben Affleck	moški	igralstvo
24.	Beyonce Knowles	moški	glasba
25.	Bill Gates	moški	IT
26.	Billie Piper	ženski	glasba
27.	Blake Lively	ženski	igralstvo
28.	Brad Pitt	moški	igralstvo
29.	Brittany Murphy	ženski	igralstvo
30.	Bruce Springsteen	moški	glasba
31.	Bruce Willis	moški	igralstvo
32.	Carrie Underwood	ženski	glasba
33.	Cate Blanchett	ženski	igralstvo
34.	Catherine Bell	ženski	igralstvo
35.	Channing Tatum	moški	igralstvo
36.	Charlize Theron	ženski	igralstvo
37.	Cheryl Cole	ženski	glasba
38.	Chris Brown	moški	glasba
39.	Christian Bale	moški	igralstvo

40.	Christian Slater	moški	igralstvo
41.	Christina Aguilera	ženski	glasba
42.	Clint Eastwood	moški	igralstvo
43.	Clive Owen	moški	igralstvo
44.	Colin Farrell	moški	igralstvo
45.	Colin Firth	moški	igralstvo
46.	Condoleezza Rice	ženski	politika
47.	Cristiano Ronaldo	moški	šport
48.	Dakota Fanning	ženski	igralstvo
49.	Daniel Craig	moški	igralstvo
50.	Daniel Day	moški	igralstvo
51.	David Beckham	moški	šport
52.	David Bowie	moški	glasba
53.	David Cameron	moški	politika
54.	David Hasselhoff	moški	igralstvo
55.	Dennis Quaid	moški	igralstvo
56.	Denzel Washington	moški	igralstvo
57.	Diane Kruger	ženski	igralstvo
58.	Diego Maradona	moški	šport
59.	Dmitry Medvedev	moški	politika
60.	Drew Barrymore	ženski	igralstvo
61.	Edward Norton	moški	igralstvo
62.	Elijah Wood	moški	igralstvo
63.	Elizabeth Banks	ženski	igralstvo
64.	Elle Macpherson	ženski	moda
65.	Ellen Degeneres	ženski	igralstvo
66.	Ellen Page	ženski	igralstvo
67.	Elton John	moški	glasba
68.	Emily Blunt	ženski	igralstvo
69.	Emma Watson	ženski	igralstvo
70.	Enrique Iglesias	moški	glasba
71.	Eric Bana	moški	igralstvo
72.	Eric Clapton	moški	glasba
73.	Ethan Hawke	moški	igralstvo
74.	Eva Green	ženski	igralstvo
75.	Eva Mendes	ženski	igralstvo
76.	Ewan McGregor	moški	igralstvo
77.	Faith Hill	ženski	glasba
78.	Fidel Castro	moški	politika
79.	Freddie Mercury	moški	glasba
80.	Gary Oldman	moški	igralstvo
81.	George Bush	moški	politika
82.	George Clooney	moški	igralstvo

83.	Gerard Butler	moški	igralstvo
84.	Geri Halliwell	ženski	glasba
85.	Gisele Bundchen	ženski	moda
86.	Gordon Ramsay	moški	igralstvo
87.	Gwen Stefani	ženski	glasba
88.	Gwyneth Paltrow	ženski	igralstvo
89.	Halle Berry	ženski	igralstvo
90.	Harrison Ford	moški	igralstvo
91.	Heath Ledger	moški	igralstvo
92.	Heidi Klum	ženski	moda
93.	Hilary Duff	ženski	igralstvo
94.	Hilary Swank	ženski	igralstvo
95.	Hillary Clinton	ženski	politika
96.	Hugh Jackman	moški	igralstvo
97.	Hugh Laurie	moški	igralstvo
98.	Hugo Chavez	moški	politika
99.	Ian Mckellen	moški	igralstvo
100.	Isla Fisher	ženski	igralstvo
101.	Jack Black	moški	igralstvo
102.	Jackie Chan	moški	igralstvo
103.	Jacques Chirac	moški	politika
104.	Jake Gyllenhaal	moški	igralstvo
105.	James Franco	moški	igralstvo
106.	James Mcavoy	moški	igralstvo
107.	Jamie Foxx	moški	igralstvo
108.	Jared Leto	moški	igralstvo
109.	Jason Statham	moški	igralstvo
110.	Javier Bardem	moški	igralstvo
111.	Jay Z	moški	glasba
112.	Jennifer Aniston	ženski	igralstvo
113.	Jennifer Garner	ženski	igralstvo
114.	Jennifer Lopez	ženski	igralstvo
115.	Jennifer Morrison	ženski	igralstvo
116.	Jessica Alba	ženski	igralstvo
117.	Jessica Simpson	ženski	glasba
118.	Jet Li	moški	igralstvo
119.	Jim Carrey	moški	igralstvo
120.	Joaquin Phoenix	moški	igralstvo
121.	John Cusack	moški	igralstvo
122.	John Legend	moški	glasba
123.	John Travolta	moški	igralstvo
124.	Johnny Depp	moški	igralstvo
125.	Jose Mourinho	moški	šport

126.	Josh Duhamel	moški	igralstvo
127.	Josh Hartnett	moški	igralstvo
128.	Joss Stone	ženski	glasba
129.	Jude Law	moški	igralstvo
130.	Julianne Moore	ženski	igralstvo
131.	Justin Timberlake	moški	glasba
132.	Kanye West	moški	glasba
133.	Kate Beckinsale	ženski	igralstvo
134.	Kate Hudson	ženski	igralstvo
135.	Kate Moss	ženski	moda
136.	Kate Winslet	ženski	igralstvo
137.	Katie Holmes	ženski	igralstvo
138.	Katy Perry	ženski	glasba
139.	Keanu Reeves	moški	igralstvo
140.	Keira Knightley	ženski	igralstvo
141.	Kelly Clarkson	ženski	glasba
142.	Kelly Rowland	ženski	glasba
143.	Kevin Bacon	moški	igralstvo
144.	Kevin Costner	moški	igralstvo
145.	Kevin Spacey	moški	igralstvo
146.	Kim Basinger	ženski	igralstvo
147.	Kim Kardashian	ženski	igralstvo
148.	Kimi Raikkonen	moški	šport
149.	Kirsten Dunst	ženski	igralstvo
150.	Kobe Bryant	moški	šport
151.	Kofi Annan	moški	politika
152.	Kristen Bell	ženski	igralstvo
153.	Kristen Stewart	ženski	igralstvo
154.	Kylie Minogue	ženski	glasba
155.	Lance Armstrong	moški	šport
156.	Lebron James	moški	šport
157.	Lenny Kravitz	moški	glasba
158.	Leonard Cohen	moški	glasba
159.	Leonardo Dicaprio	moški	igralstvo
160.	Lewis Hamilton	moški	šport
161.	Liam Neeson	moški	igralstvo
162.	Lil Wayne	moški	glasba
163.	Lindsay Lohan	ženski	igralstvo
164.	Lionel Messi	moški	šport
165.	Lisa Kudrow	ženski	igralstvo
166.	Liv Tyler	ženski	igralstvo
167.	Lucy Liu	ženski	igralstvo
168.	Margaret Thatcher	ženski	politika

169.	Maria Sharapova	ženski	šport
170.	Mariah Carey	ženski	glasba
171.	Marilyn Monroe	ženski	igralstvo
172.	Mark Wahlberg	moški	igralstvo
173.	Matt Damon	moški	igralstvo
174.	Matthew Mcconaughey	moški	igralstvo
175.	Matthew Perry	moški	igralstvo
176.	Meg Ryan	ženski	igralstvo
177.	Megan Fox	ženski	igralstvo
178.	Mel Gibson	moški	igralstvo
179.	Meryl Streep	ženski	igralstvo
180.	Michael Phelps	moški	šport
181.	Michael Schumacher	moški	šport
182.	Michelle Pfeiffer	ženski	igralstvo
183.	Michelle Rodriguez	ženski	igralstvo
184.	Mickey Rourke	moški	igralstvo
185.	Mike Tyson	moški	šport
186.	Mila Kunis	ženski	igralstvo
187.	Miley Cyrus	ženski	glasba
188.	Milla Jovovich	ženski	igralstvo
189.	Mitt Romney	moški	politika
190.	Naomi Campbell	ženski	moda
191.	Naomi Watts	ženski	igralstvo
192.	Natalie Imbruglia	ženski	glasba
193.	Natalie Portman	ženski	igralstvo
194.	Nelly Furtado	ženski	glasba
195.	Nicolas Cage	moški	igralstvo
196.	Nicole Scherzinger	ženski	glasba
197.	Nikki Cox	ženski	igralstvo
198.	Olivia Wilde	ženski	igralstvo
199.	Oprah Winfrey	ženski	igralstvo
200.	Orlando Bloom	moški	igralstvo
201.	Patrick Dempsey	moški	igralstvo
202.	Paul Mccartney	moški	glasba
203.	Paul Newman	moški	igralstvo
204.	Paul Rudd	moški	igralstvo
205.	Paul Walker	moški	igralstvo
206.	Prince Harry	moški	politika
207.	Prince William	moški	politika
208.	Quentin Tarantino	moški	režija
209.	Rafael Nadal	moški	šport
210.	Ralph Fiennes	moški	igralstvo
211.	Reese Witherspoon	ženski	igralstvo

212.	Richard Gere	moški	igralstvo
213.	Robbie Williams	moški	glasba
214.	Robert Downey	moški	igralstvo
215.	Robin Williams	moški	igralstvo
216.	Roger Federer	moški	šport
217.	Roman Polanski	moški	režija
218.	Russell Crowe	moški	igralstvo
219.	Ryan Gosling	moški	igralstvo
220.	Ryan Reynolds	moški	igralstvo
221.	Salma Hayek	ženski	igralstvo
222.	Scarlett Johansson	ženski	igralstvo
223.	Sean Connery	moški	igralstvo
224.	Serena Williams	ženski	šport
225.	Seth Rogen	moški	igralstvo
226.	Sharon Stone	ženski	igralstvo
227.	Shia Labeouf	moški	igralstvo
228.	Sigourney Weaver	ženski	igralstvo
229.	Snoop Dogg	moški	glasba
230.	Steve Jobs	moški	IT
231.	Steven Spielberg	moški	režija
232.	Sylvester Stallone	moški	igralstvo
233.	Taylor Swift	ženski	glasba
234.	Tom Cruise	moški	igralstvo
235.	Tom Hanks	moški	igralstvo
236.	Tony Blair	moški	politika
237.	Tyra Banks	ženski	moda
238.	Uma Thurman	ženski	igralstvo
239.	Val Kilmer	moški	igralstvo
240.	Valentino Rossi	moški	šport
241.	Vanessa Paradis	ženski	glasba
242.	Vin Diesel	moški	igralstvo
243.	Vladimir Putin	moški	politika
244.	Wayne Rooney	moški	šport
245.	Whitney Houston	ženski	glasba
246.	Will Smith	moški	igralstvo
247.	Winona Ryder	ženski	igralstvo
248.	Woody Allen	moški	režija
249.	Zac Efron	moški	igralstvo
250.	Zinedine Zidane	moški	šport