UPORABA SISTEMOV ZA PREPOZNAVO ČLOVEŠKIH OBRAZOV

Borut Batagelj, Franc Solina

Laboratorij za računalniški vid
Fakulteta za računalništvo in informatiko, Univerza v Ljubljani
E-pošta: {borut.batagelj, franc.solina}@fri.uni-lj.si

POVZETEK: *Najrazličnejše metode za prepoznavo človeških obrazov so postale dandanes tudi v komercialnih sistemih že zelo razširjene. V članku bomo predstavili pregled sistemov, ki se uporabljajo v realnem okolju na različnih področjih. Podrobneje bomo pogledali izdelke podjetij, ki so bili analizirani na zadnjem velikem preizkusu prepoznave obrazov (FRVT 2002). Na koncu bomo povzeli glavne rezultate preizkusov in predstavili omejitve, ki jih je za širšo in zanesljivejšo uporabo sistemov za prepoznavo obrazov potrebno še odpraviti.*

1. UVOD

Eden izmed razlogov zakaj se metode za prepoznavo obrazov v zadnjih letih tako hitro razvijajo, je tudi njihov velik potencial uporabe v vladne in komercialne namene. Že leta 1995 je Chellappa s sod. [2] predstavil nekaj sistemov, ki so uporabljali tehnologijo za prepoznavo obrazov ter naštel njihove slabe in dobre lastnosti. Sisteme je kasneje [3] razdelil v 5 glavnih kategorij uporabe. Že leta 1997 je bilo na voljo najmanj 25 sistemov za prepoznavo obrazov 13 različnih podjetji [4]. Od takrat se je zaradi vedno novih področjih uporabe ter izboljšav obstoječih metod za prepoznavo število komercialnih izdelkov samo še povečevalo. Najopaznejša podjetja in njihovi izdelki so gotovo tista, ki so se prijavila na zadnji preizkus uspešnosti FRVT (Face Recognition Vendor Test) 2002 [14]. Pri teh sistemih največkrat ni znano katere tehnologije se uporabljajo za detekcijo, prepoznavo in nazadnje za primerjavo, kar dodatno dokazuje, da so ti sistemi vključeni v komercialne izdelke in zaradi tega zaščiteni.

Med vsemi biometričnimi metodami velja prepoznava obraza za najmanj vsiljivo tehniko. To dokazuje tudi dejstvo, da je bila metoda za prepoznavo obrazov izbrana s strani mednarodne organizacije letalstva kot najbolj primerna metoda za kontrolo v letalskem prometu.

V 2. poglavju predstavimo obstoječe sisteme za prepoznavo obrazov po posameznih področjih uporabe. V 3. poglavju povzamemo njihove omejitve oziroma trenutne težave s katerimi se srečujejo. Članek zaključimo z ugotovitvami in primeri sistemov, ki se bodo pojavili v bližji prihodnosti.

2. PODROČJA UPORABE IN TIPIČNE APLIKACIJE

V poglavju bomo predstavili najbolj tipične aplikacije oziroma sisteme, ki uporabljajo tehnologijo prepoznave obrazov za najrazličnejše namene. Sisteme smo razdelil v 10 različnih kategorij uporabe. V vsaki kategoriji bomo predstavili nekaj najbolj tipičnih predstavnikov sistemov, ki delujejo v realnem okolju ter opisali njihove omejitve.

2.1 Identifikacija obraza

Osnova sistemov za identifikacijo ljudi na podlagi obraza je slika obraza. V nasprotju z ostalimi sistemi za identifikacijo je za te sisteme potrebna zgolj prisotnost osebe. Uporaba biometričnih podatkov za preverjanje identitete ima tudi določene prednosti glede varnosti. Tako lahko z zamenjavo numeričnih gesel z biometričnimi karakteristikami naredimo sisteme bolj prijazne in varne za uporabnika. Zmanjša se tveganje zlorab ukradenih gesel ali izgubljenih kartic. Dobrodošla izboljšava za operaterje je tudi sistem za avtomatsko kontrolo dostopa v varovana poslopja. Največ sistemov za identifikacijo obraza, ki skrbijo za kontrolo dostopa, je nameščenih v prilagojenih okoljih, kjer je število oseb, ki lahko vstopijo, omejeno. Takšne sisteme bomo podrobneje predstavili v naslednjem poglavju. Najprej pa predstavimo dva sistema, ki delujeta na drugih področjih.

Leta 2000 je bil za iskanje duplikatov v registru volivcev Združenih držav Amerike uporabljen program *FaceIt* podjetja *Identix* [20]. Obstajali so namreč primeri, ko je bila oseba registrirana več kot enkrat. Med primeri, ki jih je sistem našel, so nato ročno preverili ali sta osebi res enaki.

S sistemom *faceFinder* podjetja *Viisage* [22] so opremili številne uprave javnih zaporov in pisarne za izdajo vozniških dovoljenj. Ta program je bil uporabljen tudi za preverjanje naključno izbranih prosilcev za izdajo permanentne vize za vstop v Združene države Amerike. Tako zajete slike prosilcev nadalje uporabljajo pri preverjanju potencialnih oseb, ki bi lahko ogrozile varnost države.

2.2 Kontrola dostopa

Sistemi za kontrolo dostopa v prostore oziroma računalniške sisteme navadno uporabljajo zelo majhno podatkovno bazo ljudi, katerih identiteto je potrebno preveriti. Tudi slika obraza je v takšnih sistemih navadno zajeta pod prilagojenimi pogoji (frontalna slika, enakomerna osvetlitev). Zaradi tega so sistemi v takšnih okoljih zelo uspešni tudi brez sodelovanja uporabnika s sistemom. Uporabniku se na primer ni potrebno dotakniti sistema za potrditev prstnega odtisa ali približati očesa za preverjanje očesne šarenice. Še večjo zanesljivost dosežemo, če sistem za prepoznavo obrazov združimo z ostalimi sistemi za preverjanje pristnosti, kot so sistemi za preverjanje prstnih odtisov ali očesne šarenice. Raven zadovoljstva med uporabniki takšnih sistemov je zelo visoka. Na področju kontrole dostopa je bilo razvitih veliko komercialnih izdelkov. V nadaljevanju bomo nekatere od njih podrobneje predstavili.

Leta 2000 je podjetje IBM začelo prodajati prenosne računalnike Thinkpad serij A, T in X, z vgrajeno kamero in programom *FaceIt* za prepoznavo obrazov. Program je nenehno preverjal kdo je pred zaslonom računalnika. Ko je uporabnik zapustil računalniški sistem se je aktiviral ohranjevalnik zaslona in s tem se je dostop do sistema onesposobil. Pri prihodu uporabnika nazaj pred sistem je program preveril pristnost uporabnika in mu omogočil dostop. Če bi pred sistem pristopil drug uporabnik bi mu sistem na podlagi preverjanja dostop zavrnil.

Izdelek *FaceGate* [17] je primer še enega izdelka za kontrolo dostopa. Za kontrolo dostopa potrebuje sistem poleg vstopne kode ali kartice tudi sliko iz kamere. Sistem prilagodi matematični model obrazu na vhodni sliki in s tem ustvari identifikacijsko biometrično kodo posameznika. Ko želi oseba vstopiti v zgradbo, sistem preveri vstopno kodo in primerja sliko obraza s shranjeno biometrično kodo. Če se slika obraza ujema osebi vstop omogoči, v nasprotnem primeru pa zavrne.

Sistem *FaceKey* [18] kombinira za kontrolo dostopa sistem za prepoznavo obrazov in sistem za prepoznavo prstnih odtisov. S tem se še dodatno poveča zanesljivost sistema. Takšen sistem ne potrebuje vstopnih kod, gesel ali kartic. Prednost takšnih sistemov, ki kombinirajo dva biometrična podatka je tudi v tem, da se pri njih zelo zmanša verjetnost napake. Sistem lahko deluje kot samostojen sistem ali kot sistem, povezan v lokalno ali celo globalno mrežo.

Sistem *FaceVACS* [19] omogoča, da lahko običajne sisteme za kontrolo dostopa nadgradimo s sistemom za prepoznavo obraza. Pri vstopu se obraz obiskovalca zajame s pomočjo video kamere. Iz tako dobljene slike se izločijo obrazne značilke, ki se nato primerjajo s shranjenimi značilkami osebe. Dostop je omogočen le v primeru zadostnega ujemanja med značilkami. Za območja, kjer je potrebna večja varnost, se lahko sistem kombinira z vstopnimi karticami. Prilagodljiv komunikacijski vmesnik omogoča enostavno vgradnjo v obstoječe sisteme. Sistemi so med seboj povezljivi, slike vseh obrazov se shranjujejo in zgodovinski dnevnik omogoča časovni pregled vseh vstopov.

V Sloveniji je podjetje *Sistemi TAB* [25] razvilo integrirani multimedijski sistem za nadzor pristopa in evidenco prisotnosti *Smarti*. Sitem prepozna človeka po treh biometričnih parametrih, in sicer po obrazu, premikanju ustnic in po glasu. Kot druge podobne naprave omogoča tudi vrsto povezav z različnimi drugimi tehničnimi sistemi, kot so ključavnice, luči, alarmi, stroji in naprave, itd. Sestavni deli sistema so enota za prepoznavanje, podatkovni strežnik in odjemalski uporabniški program, ki je lahko nameščen kjer koli v računalniškem omrežju. Pošiljati je mogoče tudi video sporočila; v trenutku, ko sistem identificira osebo, ki ji je posneto sporočilo namenjeno, denimo ob prihodu v zgradbo, ga naslovniku tudi predvaja. Sistem poleg biometrične prepoznave omogoča še uporabo osebne identifikacijske številke (angl. Personal Identification Number, PIN), ki jo vtipkamo neposredno na zaslon. Sistem omogoča priklop katere koli dodatne opreme (čitalnik prstnih odtisov, magnetnih ali brezkontaktnih kartic, itd), tako da lahko stopnjo varnosti po potrebi še povečamo.

Poleg komercialnih izdelkov se v praksi uporablja kar nekaj sistemov, ki so bili razviti v okviru univerz. Omenimo sistem, ki združuje prepoznavo obraza in govora, ki so ga

razvili na univerzi Illinois [5]. Vsak uporabnik ima v podatkovni bazi shranjene slike obraza in zvočni zapis stavka, ki ga je v fazi učenja prebral. Za vstop v sistem se preveri vhodna slika iz kamere in ujemanje prebranega stavka s podatki shranjenimi v podatkovni bazi.

2.3 Varnost

Različni varnostni sistemi, ki uporabljajo tehnologijo prepoznave obrazov so bili nameščeni že na številna letališča po celem svetu. Čeprav lahko pri takšnih sistemih do določene meje kontroliramo pozicijo obraza ter pogoje osvetlitve, predstavlja največjo oviro še vedno preveliko število lažnih alarmov (napačno prepoznanih obrazov). Večina sistemov za prepoznavo obrazov namreč še vedno ne more zagotoviti majhnega števila napačno prepoznanih oseb pri še tako majhnem deležu lažnih alarmov. Zaradi tega je stopnja zaupanja v takšne sisteme pri ljudeh še vedno zelo nizka. V nadaljevanju bomo našteli nekaj primerov programov, ki skrbijo za varnost na letališčih in stadionih.

Oktobra 2001 so za namene varnosti na mednarodnem letališču FYI v Kaliforniji namestili sistem za prepoznavo obrazov podjetja *Viisage* [22]. Sistem deluje tako, da obvesti uslužbence varnostne službe letališča, če se slika osebe, ki vstopi na letališče, ujema s sliko katere od oseb na seznamu teroristov.

Na letališču v Sydneyu v Avstraliji skrbi za varnost sistem *SmartFace* podjetja *Visionics* [20]. Širokokotne kamere zajamejo vse prispele potnike in podatke pošljejo v računalnik, ki te slike obdela in obraze primerja z obrazi na listi nezaželenih, ki jih ima shranjene v podatkovni bazi. Če se kakšen obraz ujema z znanim obrazom se sproži tihi alarm osebju, ki skrbi za varnost.

Sistem podjetja *Imagis* [23] pa uporabljajo v sobi za zasliševanje na letališču Oakland v Kaliforniji. Sumljive osebe se primerja s slikami iskanih kriminalcev.

V Maleziji se na 16 letališčih uporablja sistem *FaceIt* [20], ki skrbi za večjo varnost potnikov in njihove prtljage. Pri kontroli prtljage se s pomočjo zelo majhne kamere zajame video posnetek potnika. Ta video posnetek se shrani na posebno pametno kartico, ki je del karte ter del prtljage. Sistem zagotovi, da lahko samo oseba, ki je predala prtljago vstopi v prostor za odhode in se kasneje tudi vkrca v letalo. Prav tako se kontrolira tudi prtljaga, če je naložena na pravo letalo. Med vkrcavanjem sistem v realnem času preveri sliko potnika s sliko shranjeno na karti. Dokler se sliki ne ujemata se tudi prtljaga ne naloži na letalo.

Sistem *faceFINDER* podjetja *Viisage* [22] so uporabljali tudi za preverjanje občinstva na stadionu. Na vhodu stadiona so bile nameščene kamere, ki so posnele vsakega obiskovalca, ki je vstopil. Kamere so bile povezane s posebnim kontrolnim centrom, kjer so se obrazi na slikah primerjali s slikami kriminalcev. Isti sistem je uporabila tudi policija v Avstraliji, ko je na nogometni tekmi preverjala obiskovalce z znanimi huligani, ki so imeli prepoved obiskovati tekme.

2.4 Nadzor

Podobno kot varnostni sistemi, dosegajo tudi nadzorni sistemi, ki uporabljajo tehnologijo prepoznave obrazov, nizko zadovoljstvo pri uporabnikih. Različni svetlobni pogoji, različno obrnjen obraz ter drugi spremenljivi faktorji vplivajo na to, da je prepoznava obraza v sistemih za nadzor velike množice ljudi še vedno težavna naloga.

Leta 1998 je podjetje *Visionics* [20] prvič predstavilo svoj sistem *FaceIt* za nadzor mestnega središča v Londonu. Na mestnem trgu so postavili 300 kamer, ki so bile v zaključenem krogu povezane s kontrolno sobo. Mestne oblasti so zatrdile, da je takšen sistem pripomogel k zmanjšanju kriminala za 34%. Podoben sistem so nato postavili še v Birminghamu. Program *FaceIt* uporabljajo tudi policisti na Floridi, da s pomočjo video kamer preiskujejo ulice in iščejo spolne iztirjence. V Virginiji so program namestili na javno ulico, da pregleduje obraze mimoidočih in jih primerja s 2500 slikami aktualnih kriminalcev, pogrešanih in pobeglih oseb. V New Yorku s pomočjo sistema za nadzor kontrolirajo obiskovalce kipa svobode. V pristanišču kjer obiskovalci zapustijo Manhattan jih posnamejo dve kameri in njihove slike primerjajo s slikami znanih teroristov. Kamere spremljajo turiste v vrsti, ki čakajo na ladjo.

2.5 Pametne kartice

Pametne kartice, ki vsebujejo spominske module in miniaturne procesorje, imajo že dovolj velike zmogljivosti, da jih lahko opremimo z biometričnimi podatki osebe. Večina kartic ima tudi že vgrajeno zaščito ter radiofrekvenčni vmesnik za oddaljeno komunikacijo s bralniki. Tako lahko pametne kartice s svojo zmožnostjo prenosljivosti in nadgradnje postanejo nekakšen vezni člen med virtualnim in fizičnim svetom. Sistem integriran na takšni kartici tako skrbi za preverjanje biometričnih podatkov kot tudi za nadgradnjo z novimi podatki v vsakem primeru ujemanja.

Podjetje *Maximus* [23] je na pametni kartici združilo biometrične podatke obraza ter podatke prstnega odtisa. S pomočjo takšne kartice lahko sistemi hitreje preverjajo identiteto potnikov, s čimer se skrajša čakanje. Bralniki kartic so namreč nameščeni v posebnih hitrih vrstah, kjer se preveri identiteta potnikov s primerjavo podatkov shranjenih na kartici s tistimi, ki jih naprava zajame med prehodom. Pred izdajo takšne kartice potnika preverijo in mu na podlagi slike obraza in njegovega prstnega odtisa izdelajo kartico.

Sistem *ZN-Face* [14], ki prav tako združuje biometrične podatke obraza in prstnega odtisa na pametni kartici, se uporablja na Berlinskem letališču za zaščito varovanih območji. Potencialne grožnje kriminalcev, ki so do sedaj uspešno vstopali v zavarovana območja s pomočjo ustreznih preoblek (pilotske uniforme) lahko takšni sistemi uspešno izključijo. Na vsakem vstopnem mestu se zajete značilnosti oseb preverijo s tistimi, ki so shranjene na pametni kartici in tako služijo kot verifikacija.

Tudi v Sloveniji se bo obrazna prepoznava uporabljala za namene izdelave biometričnih potnih listov. V začetku leta 2005 je namreč stopila v veljavo obvezujoča Uredba Sveta (ES) o standardih za varnostne značilnosti in biometrične podatke v potnih listih in

potovalnih dokumentih, ki jih izdajajo države članice. Uredba opredeljuje implementacijo dveh biometričnih elementov kot obveznih: obrazno prepoznavo in prepoznavo dveh prstnih odtisov. Biometrični podatki bodo zapisani na brezkontaktnem čipu, ki bo vgrajen v potni list.

Pametne kartice se večinoma uporabljajo za primere verifikacije. Natančnost ujemanja na kartici shranjene slike s tisto, ki jo zajamejo naprave, je odvisna predvsem od časa, ki je minil med zajetjema obeh slik. S tem, ko podatke na kartici posodobimo z novimi, lahko to časovno obdobje skrajšamo. V primeru podatkovnih baz z majhnim številom ljudi, je zanesljivost takšnih sistemov zadovoljiva.

2.6 Organi pregona

S pomočjo tehnologije prepoznavanja obrazov in informacij o kriminalcih lahko preiskovalci hitro najdejo in identificirajo osumljenca celo v primerih, ko nimajo popolnih podatkov. Včasih imajo o osumljencu znano samo skico očividca ali slab posnetek iz nadzorne video kamere. Prav zaradi tega je lahko uspešnost sistemov za prepoznavo obrazov v takšnih primerih zelo slaba. Vsekakor pa so sistemi za prepoznavo obrazov lahko zelo dober pripomoček za policijo.

Podjetje *Imagis* [23] je za varnostne organe pripravilo poseben program, ki omogoča kalifornijskim policistom in detektivom s pomočjo prenosnih naprav preko zaščitene internetne povezave ažuriran dostop do informacij o aretiranih osebah. Sistem, ki vključuje tudi prepoznavo obrazov, upravljanje s slikami in podatkovno bazo, predstavlja policijskim delavcem dodatno pomoč pri njihovem delu. S pomočjo sistema za prepoznavo obrazov in vedno ažurirane podatkovne baze obrazov policistom ni potrebno več izgubljati ure in ure, da bi identificirali sumljivo osebo. Policist enostavno zajame sliko osumljenca, ki jo lahko na terenu primerja z osebami v zbirki podatkov. Podobno poizvedbo lahko naredi za osebe, ki jih je zajela nadzorna kamera ali zmanjša množico možnih osumljencev na podlagi dodatnega opisa očividca.

Sistem podjetja *Imagis* so namestili tudi v igralnico za potrebe nadzora in kontrole obiskovalcev. V kombinaciji z globalno podatkovno bazo nezaželenih obiskovalcev in hazarderjev omogoča sistem igralnicam zelo učinkovito varnostno rešitev.

2.7 Zbirke digitalnih fotografij

Tehnologije za pridobivanje slik na osnovi opisnega besedila niso več kos vse večjim podatkovnim zbirkam digitalnih fotografij. To poskušajo rešiti nove tehnologije, ki slike kategorizirajo na podlagi njihove vsebine. Slik ne rabimo več opremljati z besedilom, ampak se le-te avtomatsko opremijo s ključnimi besedami glede na to, kaj prikazujejo. Najenostavnejše metode uporabljajo za ugotavljanje vsebine kar lastnosti slike kot so barva in tekstura. Takšne splošne značilke pa imajo svoje pomanjkljivosti, zato jih poskušajo raziskovalci uporabljati v kombinacijami z drugimi metodami za analizo slik in s tem povečati točnost označevanja slik. Med takšne metode spada tudi metoda odkrivanja in prepoznave obrazov na sliki. Čeprav se metoda prepoznave obrazov

večinoma uporablja za pridobivanje in indeksiranje obraznih slik (baza osumljencev), se jo uporablja tudi za preiskovanje podatkovnih zbirk, ki vsebujejo tako slike obrazov kot tudi slike neobrazov (družinski albumi).

Uspešnost takšnih sistemov je predvsem zaradi zelo velikega števila slik in s tem obrazov, ki jih moramo poiskati, še vedno relativno nizka. Uspešnost je zmanjšana tudi zaradi različnih pogojev, pod katerimi se obrazi na slikah pojavljajo.

Poznamo dva tipa sistemov, ki se uporabljata nad podatkovnimi zbirkami digitalnih fotografij. Prvi sistemi uporabljajo metode prepoznavanja obrazov za označevanje slik, drugi pa tehnike označevanja slik uporabljajo kot pomoč pri iskanju osebe.

Tako nam sistemi prvega tipa omogočajo avtomatsko organizacijo in s tem enostavnejše iskanje po veliki zbirki fotografij domačega albuma. Primer takšnega programa je *FotoFile* [6], ki s pomočjo prepoznave obraza avtomatsko izvede identifikacijo vseh oseb na fotografijah in na podlagi tega fotografije samodejno označi in združi v skupine. Uporabnik lahko takšno izbiro sistema potrdi ali ovrže in s tem sistem dodatno uči.

Sistemi drugega tipa pa nam omogočijo, da poiščemo v veliki zbirki obrazov osebo samo po spominu. Avtorja Navarrete in del Solar [7] sta uporabila metodo, ki temelji na odgovoru, ki ga vrne uporabnik glede na podobnost prikazanih slik s tisto ki jo ima v spominu. Idejo sta implementirala s pomočjo drevesne strukture samo-organizacijskih mrež (ang. tree-structured self-organizing map, TS-SOM), ki samodejno organizira slike obrazov v podatkovni bazi. Podobni obrazi se tako nahajajo na sosednjih pozicijah v drevesu mreže. Da pridemo do želene lokacije, kjer se nahaja obraz, ki ga iščemo nam sistem ponudi naključno izbrane slike med katerimi moramo izbrati tiste, ki so po našem mnenju najbolj podobne obrazu, ki ga imamo v mislih. Nato nam sistem ponudi naslednjo skupino slik, ki jo skrbno izbere glede na našo predhodno odločitev. Tako nam sistem ponuja nove in nove skupine slik dokler proces iskanja ne konvergira do želene slike. Drugi takšen sistem avtorjev Eickeler in Birlinghoven [8] temelji na skritem Markovem modelu. Raziskave, ki sta jih avtorja naredila, delujejo na podatkovni bazi s 250.000 slikami, kar dokazuje da je metoda primerna tudi za velike zbirke slik.

Veliko podatkovno bazo za namene preizkusa in nadaljnje uporabe smo izdelali s pomočjo instalacije 15 sekund slave [16]. Vsaka slika vsebuje najmanj en obraz, ki ga je program za iskanje našel. Tako najdene obraze naprej uporabimo za izgradnjo mozaika slavnih oseb ter shranimo v podatkovno bazo za kasnejše pošiljanje zahtevanega portreta uporabniku. Sistem za iskanje obraza lahko nadgradimo tudi s sistemom za prepoznavanje mimike in s tem vplivamo na umetniško transformacijo slike izbranega obraza. Nadalje pa lahko obraz obiskovalca tudi prepoznamo in s tem podatkovno bazo slik dodatno organiziramo in omogočimo da sistem v prihodnje obiskovalca prepozna in mu pri pošiljanju omogoči dostop do vseh njegovih portretov.

2.8 Upravljanje z večpredstavnostnimi vsebinami

Obrazi se pojavljajo povsod, pri napovedih novic, pri športu, v filmih ter v drugih večpredstavnih vsebinah. Če hočemo takšne večpredstavne vsebine razvrstiti glede na

to, kaj prikazujejo, moramo uporabiti metode kot so iskanje, sledenje obrazov in njihova prepoznava ter spremembe skozi čas. Na takšen način lahko video vsebine organiziramo v posamezne segmente in s tem omogočimo preiskovanje, hitro pregledovanje in izdelavo povzetkov. Metode za preiskovanje video vsebin na podlagi obraza so poleg metod kot so analiza govora, prepoznava govora in drugih tehnik analize slik zelo močno orodje pri avtomatskem indeksiranju in označevanju večpredstavnih vsebin.

Ena izmed težav pri uporabi metod za prepoznavo obrazov na video vsebinah je ta, da nimamo v naprej podane galerije slik in tako ne vemo kdo je najdena oseba na sliki. Metode morajo identiteto najdenih oseb poiskati iz same vsebine.

Haughton [9] je problem rešil tako, da imena nastopajočih poišče na internetnih straneh, ki opisujejo preiskovano video vsebino. Dodatno poišče imena v spremnem tekstu na samem posnetku s pomočjo tehnike OCR. Tako najdena imena potem poveže z osebami, ki nastopajo v videu in s tem zgradi galerijo. Za iskanje obrazov uporablja program *FaceIt*.

Avtorja Ma in Zhang [10] sta razvila interaktivni uporabniški vmesnik, ki omogoča uporabniku, da predhodno označi osebe na izbranih video segmentih, ki jih sistem izbere tako, da vsebujejo še neznane osebe. Za izbiro ključnih segmentov je uporabljen program za iskanje obrazov. Kasneje se za preiskovanje video vsebin pa uporablja metode prepoznave.

Integriran sistem za upravljanje z večpredstavnimi vsebinami je tako imenovan sistem *Infomedia*, ki je nastal v okviru projekta na univerzi Carnegi Mellon [12]. Cilj projekta je ustvariti informacijsko digitalno video knjižnico, ki bo pomagala pri učenju. Uporabniki lahko po indeksiranih in arhiviranih video vsebinah hitro iščejo in poizvedujejo z opisnimi poizvedbami kot so: “poišči izseke na katerih ljudje govorijo”, (metoda za iskanje obrazov) ali “poišči intervjuje z določeno osebo” (metoda za iskanje obrazov v kombinaciji s spremnim tekstom).

Sistem iVIEW je še en primer digitalne video knjižnice, ki podpira več jezikov in več načinov delovanja, izdelali pa so ga na Kitajski univerzi v Hong Kongu [11]. Shema prepoznavanja obrazov je zelo podobna tisti, ki jo je predstavil avtor Haughton. Zasnova sistema iVIEW temelji na internetnem uporabniškem vmesniku, ki je povezan s strežnikom.

Avtorja Wang in Chang [13] sta izdelala sistem, ki omogoča iskanje, sledenje in izgradnjo povzetkov iz stisnjenih video vsebin v realnem času. Za iskanje obrazov na video posnetku, avtorja izkoriščata informacije zapisane v MPEG stisnjenem videu, ki sta jih nadgradila s sledenjem. S sledenjem posameznim osebam skozi čas in prostor se lahko naučita tudi kako so te osebe med seboj povezane.

Orientacije obrazov in svetlobni pogoji so v večini večpredstavnih vsebin zelo različni, kar pripomore k temu da je uspešnost takšnih sistemov zelo nizka.

2.9 Interakcija med človekom in računalnikom

Za učinkovito in uporabniku prijazno interakcijo med človekom in računalnikom lahko običajne naprave kot so miška in tipkovnica zamenjajo bolj naravne vhodne "naprave" kot so človeški deli telesa (med njimi tudi glava). To dejstvo je motiviralo številne raziskovalce na področjih kot so sledenje, analiza mimike, sinteza in animacija človeškega obraza.

Čeprav je glavni cilj takšnih uporabniških vmesnikov, da prepoznajo in razumejo posamezne kretnje človeka, je prvi korak takšnih sistemov posamezne človeške dele poiskati in jim slediti. Kot najbolj razlikovalna značilka se tukaj ponuja barva kože, ki omogoča učinkovito lokalizacijo in slednje objektom kot so roke in obraz. Posamezne dele telesa najdemo s pomočjo segmentacije, tako da združimo posamezne barvne regije, ki vsebujejo kožno barvo. Kljub temu, da je bilo na področju prilagodljivih barvnih modelov že kar nekaj narejenega je to potrebno to področje še dodatno raziskati.

Od računalnika, ki bi imel sposobnost interakcije s človekom se pričakuje, da ima podobne komunikacijske sposobnosti kot jih ima človek. Ena takšnih sposobnosti je tudi prepoznava razpoloženja človeka. Človek namreč svojo razpoloženje najbolj izraža s pomočjo mimike svojega obraza.

Realistična slika 3D modela glave je eden ključnih faktorjev na poti k bolj naravni interakciji med človekom in računalnikom. Grafični model človeka je prava rešitev za vizualno predstavitev informacij. Primeri okolij kjer se takšen model uporablja, so kodiranje videa za prenos po ozki pasovni širini za namen vizualne telekomunikacije, prepoznava na podlagi avdio in vizualne informacije ter animacija govorečega modela glave pri računalniških agentih. V okoljih, kjer je veliko šuma, takšni modeli pripomorejo k boljšemu razumevanju govora in s tem k boljšemu odzivu uporabnika pri interakciji. Izkazalo se je, da virtualni agenti, ki skrbijo za prodajo, zbujajo pri kupcih zaupanje ter da govoreči modeli človeške glave pripomorejo k boljšemu učenju na računalniških sistemih.

2.10 Druga področja uporabe

Veliko sistemov za prepoznavo obrazov potrebuje za realizacijo sodelovanje s strokovnjaki na izbranem področju. Največkrat delujejo kot pomočniki ekspertom na tem področju.

Prvi primer takšnih sistemov je sistem za verifikacijo starinskih fotografij. Za zgodovinarje, življenjepisce in zbiratelje starin je izrednega pomena, da potrdimo identiteto osebi na starinski sliki. Zaradi velike časovne razlike med slikama, ki ju primerjamo ter zaradi večkrat zelo slabe kvalitete starinske slike predstavlja takšen sistem še vedno izziv.

Drugo področje uporabe so sistemi za prenos obrazne slike. Sliko lahko zakodiramo s pomočjo samo nekaj parametrov, kar je zelo uporabno za prenos slike obraza pri nizkih pasovnih širinah pri video telefoniji ter pri telekonferencah. Namesto, da bi se pošiljale

celotne slike ali video, se pošiljajo samo parametri, ki se nato na drugi strani prilagodijo modelu obraza in kar se da čimbolj rekonstruirajo pravo podobo originalnega obraza osebe. Sistem ima potencialno uporabo tudi v namene izobraževanja (v muzejih, v razredu) ter zabave (animirani junaki v računalniških igricah, interaktivni filmi, digitalni fotoaparati).

Sistemi za prepoznavo obraza se uporabljajo tudi kot pomoč ekspertom pri rekonstrukciji obraza iz znanih lastnosti ali ostankov, pri izdelavi fotorobotov ali kot pomoč pri simulaciji staranja skozi čas.

3. OMEJITVE TRENUTNIH SISTEMOV

Čeprav se tehnologija za prepoznavo obrazov že veliko uporablja, je to območje uporabe še vedno zelo omejeno. Da bi to spremenili je potrebno rešiti vsaj še dva problema. Prvi problem je robustnost sistemov v spremenljivih okoliščinah.

Uspešnost prepoznave je v primerih, ko imamo opraviti z veliko količino podatkov, še vedno premajhna. Spremembe osvetlitve, različni položaji obraza in časovna razlika med zajemom testne slike in slike iz galerije to še dodatno poslabšajo. Uspešnost prepoznave pri spremenljivih okoliščinah so preizkusili tudi na zadnjem velikem preizkusu FRVT leta 2002, kjer so preizkusili 10 najboljših komercialnih izdelkov [15]. Med najboljše tri so se uvrstila podjetja *Cognitec* [19], *Visionics (zdaj Identix)* [20], *Eyematic (zdaj Neven Vision)* [21].

Verifikacijo so preizkusili nad množico iz galerije, ki je vsebovala 37.437 oseb, testna množica pa je vsebovala 74.854 oseb, kjer je imela vsak oseba po dve sliki. Prvi trije najboljši sistemi so pri preizkusu, kjer so bili pogoji osvetlitve kontrolirani v zaprtem prostoru, dosegli uspešnost verifikacije 90% pri 1% napake, 80% pri napaki 0.1% in 70% pri napaki 0.01%. Vedeti moramo, da lahko samo v nekaterih sistemih zagotovimo kontrolirano okolje ter da je takšna uspešnost še vedno premajhna na letališčih, kjer imamo opraviti z velikim številom ljudi. Takšen sistem bi lahko uporabili na primer za kontrolo dostopa v situacijah, kjer imamo največ sto ljudi in lahko zagotovimo kontrolirano okolje. Pri preizkusu, kjer se je položaj obraza spreminjal je na podatkovni bazi s 87 osebami najboljši sistem dosegel identifikacijsko uspešnost 42%, ko se je položaj spreminjal za 45 stopinj levo in desno, ter 52% uspešnost pri spremembi 45 stopinj gor in dol. Pri preizkusu, kjer je bila časovna razlika med slikami eno leto, je uspešnost padla za 5%. Pri različnih osvetlitvah, kjer je bila slika iz galerije posneta v zaprtem prostoru, testna slika pa na prostem, je uspešnost padla pri napaki 1% iz 90% na 60%.

Sistemi za namene nadzora na javnih prostorih so vzbudili tudi skrb o poseganju v posameznikovo zasebnost. Ameriško združenje civilnih svoboščin (ACLU) namreč nasprotuje uporabi sistemov za prepoznavo obrazov na letališčih zaradi zelo majhne učinkovitosti in zaradi vmešavanja v zasebnost ljudi.

4. ZAKLJUČEK

V članku smo naredili pregled nad sistemi v različnih kategorijah uporabe. Za vsako kategorijo smo izpostavili omejitve trenutnih sistemov, ki se uporabljajo. Lahko vidimo, da so se metode za prepoznavo obrazov iz akademskih raziskovalnih laboratorijev že preselile v komercialne sisteme. Najuspešnejše aplikacije so še vedno tiste, ki uporabljajo majhno do srednje veliko podatkovno bazo oseb. Takšni sistemi se največkrat uporabljajo za kontrolo dostopa ali vstopa v računalniški sistem. Sistemi za kontrolo na letališčih ali za nadzor na javnih prostorih pa še vedno ostajajo izziv za raziskovalce. Takšni sistemi so pri velikem številu oseb, ki jih morajo pregledati ter zaradi zelo različnih pogojev zajemanja, še vedno nezanesljivi. S tesnejšim sodelovanjem med industrijskimi in univerzitetnimi raziskovalci lahko tudi takšni sistemi postanejo bolj zanesljivi in robustni.

Druga možnost izboljšave učinkovitosti prepoznave pa leži v kombinaciji različnih biometričnih in varnostnih metod. Tako lahko v kombinacijah s sistemi za prepoznavo obrazov uporabimo tudi prepoznavo zvoka, prstnih odtisov ali očesne šarenice. Kot varnostne metode pa lahko uporabimo rentgensko kontrolo, detektor kovin ali detektor kemičnih snovi.

V prihodnosti lahko pričakujemo da se bo področje uporabe sistemov za prepoznavo obrazov razširilo še na področja kot so avtomobilska industrija, industrija zabave, domači sistemi za zaščito računalniških sistemov, alarmnih sistemov, področja internetne zaščite, itd. Vsekakor pa bo vse več sistemov prisotnih za nadzor in kontrolo pri vstopih v zavarovana območja, za kontrolo vstopnic, za dodatno kontrolo na bankomatih in v potniškem prometu.

LITERATURA

1. T. Huang, Z. Xiong, Z. Zhang, University of Illinois (2005), Face Recognition Applications, *Handbook of Face Recognition*, Springer. New York., poglavje 16, str. 371-390.

2. R. Chellappa, C. Wilson, and S. Sirohey (1995), Human and machine recognition of faces: a survey. *Proceedings of the IEEE*, vol. 83-5, str. 704-740.

3. W. Zhao, R.Chellappa, A. Rosenfelda, J. Phillips (2000), Face recognition: a literature survey, *Technical Report, CS-TR4167R*, University of Maryland.

4. C. Bunney (1997), Survey: face recognition system, *Biometric Technology Today*, str. 8-12.

5. Z. Xiong, Y. Chen, R. Wang, T. Huang (2002), Improved information maximization based face and facial feature detection from real-time video and application in a

multi-modal person identification system, In *Proceedings of Fourth International Conference on Multimodal Interfaces (ICMI'2002)*, str. 511-516.

6. A. Kudhinsky, C. Pering, M.L. Creech, D. Freeze, B. Serra, J. Gvvizdka (1999), FotoFile: a consumer multimedia organization and retrieval system, In *Proceedings of CHI'99*, str. 496-503.

7. P. Navarrete, J. del Solar (2002), Interactive face retrieval using self-organizing maps, In *Proceedings, 2002 Int. Joint Conf. On Neural Networks: IJCNN2002*.

8. S. Eickeler, S. Birlinghoven (2002), Face database retrieval using pseudo 2D markov models, In *Proceeding of IEEE Int. Conf. On Face and Gestures (FG 2002)*.

9. R. Houghton (1999), Named faces: putting names to faces, *IEEE Intelligence Systems*, vol. 14-5, str. 45-50.

10. W.-Y. Ma, H. Zhang, An indexing and browsing system for home video (2000). In *Proc. Of 10th European Signal Processing Conference*.

11. M.R. Lyu, E. Yau, S. Sze (1998), A multilingual, multimodal digital video library system, In *ACM/IEEE Joint Conf. On Digital Libraries, JCDL 2002*, str. 145-153.

12. H. Wactlar, T.K.M. Smith, S. Stevens (1996), Intelligence access to digital video: informedia project, IEEE Computer, vol. 29-5, str. 46-52.

13. H. Wang, S.-F. Chang (1997), A highly efficient system for automatic face region detection in mpg video sequence, IEEE tras. On Circuits and Systems for Video Technology, Special Issue on Multimedia Systems and Technologies, vol. 7-4, str. 615-628.

14. W. Konen, E. Schulze-Kruger (1995), ZN-face: a system for access control using automated face recognition, In Poceedings of the International Workshop on Automatic Face and Gesture Recognition, str. 18-23.

15. P. Phillips, P. Grother, R. Michaels, D. Blackburn, E. Tabassi, M. Bone (2002). Face Recognition vendor test 2002: evaluation report. *http://www.frvt2002.org*.

16. F. Solina, P. Peer, B. Batagelj, S. Juvan, J. Kovač (2003), Color-based face detection in the "15 seconds of fame" art installation, *Conference on Computer Vision / Computer Graphics Collaboration for Model-based Imaging, Rendering, image Analysis and Graphical special Effects*, str. 38-47.

17. *http://www.premierelect.co.uk/faceaccess.html*
FaceGate.

18. *http://www.facekey.com*
FaceKey.

19. *http://www.cognitec-systems.de*
Cognitec Systems GmbH.

20. *http://www.identix.com*
Identix, Visionics.

21. *http://www.eyematic.com*
Eyematic Interfaces Inc.

22. *http://www.viisage.com*
Viisage Technology.

23. *http://www.imagistechnologies.com*
Imagis Technologies Inc.

24. *http://www.maximus.com/corporate/pages/*
Maximus.

25. *http://www.tab-systems.com*
Sistemi TAB