Nadgradnja sistema za verifikacijo na podlagi prstnega odtisa

Matic Tovšak, Jernej Bule, Peter Peer

Fakulteta za računalništvo in informatiko, Laboratorij za računalniški vid, Univerza v Ljubljani,
Tržaška cesta 25, 1000 Ljubljana
E-pošta:{matic.tovsak, jernej.bule, peter.peer}@fri.uni-lj.si

Upgrade of a fingerprint verification system

The aim of this work is to present an upgrade of our existing fingerprint verification system [3]. In the first part we generally describe a functionality of a system and how it works. Later in the text, we focus on description of our system upgrade. It includes various system tests, including an analysis of results, integration of graphical user interface for end-user, and description of an algorithm for fingerprint verification. We made our analysis by performing tests on a set of fingerprints, obtained from eight persons, who will be the first users of our prototype system. The biggest problem in the system are badly captured fingerprints. Such low quality fingerprints result in poor performance of the system. Therefore, we also implemented algorithms for image quality assessment.

1 Uvod

Temeljni cilj razvoja vsakega biometričnega sistema, ki izrablja razpoznavnost prstnih odtisov, je učinkovita in zanesljiva možnost verifikacije ter indentifikacije oseb. Leta 2009 je bil razvit prototip sistema za verifikacijo oseb na podlagi prstnih odtisov [3]. Kot je razvidno iz članka [3], je bil primarni cilj projekta razviti sistem z dobro modularno zgradbo, ki bo omogočala enostavno nadgrajevanje in izboljševanje sistema. Zanesljivost sistema je bila v prvi fazi sekundarnega pomena, zato se je izkazalo, da je na tem področju še veliko prostora za izboljšave. Obstoječi sistem smo zato nadgradili ter mu dodali določene nove funkcionalnosti in izboljšave. Predenj se posvetimo slednjim, bomo najprej na kratko predstavili sistem ter splošno opisali njegovo delovanje.

2 Opis sistema

Delovanje sistema lahko opišemo v treh korakih: zajem prstnega odtisa, iskanje značilk ter odločanje. V nadaljevanju sledi kratek opis korakov algoritma za verifikacijo oseb na podlagi prstnega odtisa. Vsi koraki so predstavljeni splošno [3].

2.1 Zajem prstnega odtisa

Prstni odtis zajamemo s pomočjo optičnega čitalca prstnih odtisov. Čas pridobitve slike je zelo kratek, saj današnji čitalci zajemajo slike v časovnem intervalu ene sekunde. Zajem prstnega odtisa je zelo pomemben korak, saj so vsi nadaljni koraki obdelave odvisni od kvalitete zajetega odtisa.

2.2 Segmentacija

Pri segmentaciji poskušamo čim bolje ločiti prstni odtis od ozadja. S tem se izognemo procesiranju predelov slike, ki bodisi vsebujejo preveliko šuma, bodisi za nas niso zanimivi. Na ta način skrajšamo čas procesiranja in hkrati povečamo natančnost primerjanja odtisov. Natančna segmentacija je posebej pomembna za pravilno in zanesljivo iskanje značilk, singularnih točk.

2.3 Izboljšanje kvalitete slike prstnega odtisa

Včasih se zgodi, da pride pri zajemu prstnih odtisov do določenih nepravilnosti, kot so npr. prekinitve grebenov ali pa razne poškodbe (ureznine). Ker je učinkovitost algoritma za iskanje značilk zelo odvisna od kvalitete zajetih prstnih odtisov, lahko slabo zajet odtis močno zmanjša učinkovitost algoritma. Za takšne primere je nujno, da uporabimo algoritem za izboljšanje kvalitete slike prstnega odtisa. Takšni algoritmi popravijo strukturo obnovljivih regij in označijo neobnovljive regije kot nezmožne za nadaljno procesiranje.

2.4 Binarizacija

Namen binarizacije je doseči, da je vsak slikovni element predstavljen z 0 ali 1. Rezultat je slika, kjer so grebeni predstavljeni z bitom 1, ozadje pa z bitom 0.

2.5 Tanjšanje grebenov

Namen tega koraka je, da zmanjšamo debelino grebena na en slikovni element. Uporabljeni algoritem deluje tako, da začne odstranjevati slikovne elemente na zunanjih robovih grebenov, dokler niso debeli zgolj en slikovni element. Algoritem uporablja tudi štiri posebna pravila za tanjšanje diagonalnih črt.

2.6 Iskanje značilk

Osnovna tipa značilk sta razcep (angl. bifurcation) in zaključek (angl. ridge ending). Naloga algoritma za iskanje značilk je, da najde ta dva osnovna tipa. Ker pri

iskanju značilk večkrat pride do napak, je potrebno dobljene značilke dodatno obdelati.. Vse značilke zato preverimo še z algoritmom za verifikacijo značilk [4], odstranimo nepravilne značilke ter tako povečamo zanesljivost sistema.

2.7 Klasifikacija

S klasifikacijo želimo prstnemu odtisu določiti, v katerega od razredov spada. Galton–Henryev sistem določa pet razredov: lok, šotorast lok, leva in desna zanka ter spirala. Naša aplikacija prstnemu odtisu dodeli razred na podlagi singularnih točk (jedro, delta). Položaj singularnih točk izračunamo s poljem ukrivljenosti (angl. Curvature Map) [5], medtem ko tip singularne točke določimo z metodo Poincare Index [2].

2.8 Primerjanje

Primerjanje je zadnji korak sistemov za verifikacijo na podlagi prstnih odtisov. Obstaja več načinov primerjanja prstnih odtisov, pri čemer naš sistem uporablja primerjanje na podlagi značilk (sicer poznamo še korelacijsko metodo ter metodo primerjanja grebenov). Pri tem načinu primerjanja se prstni odtisi ujemajo takrat, ko obstaja potrebno število značilk, ki se ujemajo v tipu, lokaciji in usmerjenosti [1]. V koraku primerjanja torej dobimo odgovor na vprašanje, ali se vhodni prstni odtis ujema s katerim od odtisov, ki jih imamo registrirane v podatkovni bazi za neko osebo.

3 Nadgradnja sistema

Pred nadgradnjo smo najprej izvedli analizo učinkovitosti oziroma zanesljivosti sistema in sicer z dvema različnima optičnima čitalcema – DigitalPersona U.are.U4000B ter Secugen Hamster Plus.

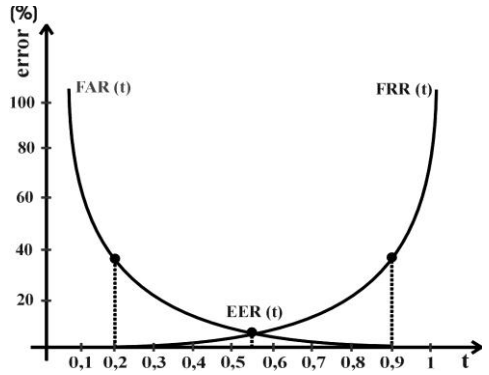
Ker bo sistem v prvi fazi nadzoroval vstop v laboratorij, smo teste izvedli na množici odtisov članov laboratorija. Test lahko opišemo v treh korakih: zajem in registracija prstnih odtisov, izvedba primerjanja ter analiza rezultatov. Sledil bo opis nadgradnje sistema.

3.1 Zajem in registracija

V prvem koraku smo zajeli odtise osmih članov laboratorija. Pri vsaki osebi smo s čitalcem zajeli deset odtisov desnega kazalca. Zajete prstne odtise smo nato registrirali in si na ta način ustvarili bazo, sestavljeno iz 80 prstnih odtisov.

3.2 Izvedba primerjanja

Za vsak čitalec smo opravili dva testa, ker smo za vsak test izračunali število nepravilno zavrnjenih FRR (angl. False Rejection Rate) ter število nepravilno sprejetih FAR (angl. False Acceptance Rate) prstnih odtisov. FRR pomeni, da gre za neujemanje dveh vzorcev iste osebe, medtem ko FAR pomeni, da se ujemata dva vzorca različnih oseb. Vse teste smo izvedli pri različnih odločitvenih pragih. Rezultate smo podali s krivuljo ROC (angl. Receiver Operating Characteristic), ki nam pokaže FRR ter FAR v odvisnosti od različnih vrednosti odločitvenega praga (slika 1). Sečišče krivulj FRR in FAR je točka, ki označuje ERR (angl. Equal Error Rate). Slednji nam pove, pri kateri vrednosti odločitvenega praga je verjetnost obeh napak izenačena.



Slika 1. ROC krivulja, ki prikazuje FRR in FAR v odvisnosti od različnih vrednosti odločitvenega praga t [3].

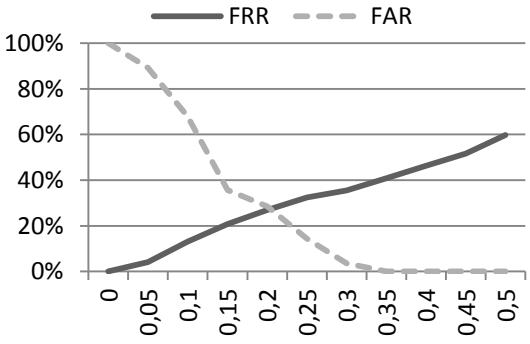
Pri prvem testu smo FRR izračunali tako, da smo vsak odtis neke osebe primerjali z ostalimi odtisi te iste osebe. Pri izračunu FAR smo prvi odtis neke osebe primerjali z ostalimi prvimi odtisi ostalih oseb.

Drugi test je bil drugačen. Tu smo FRR izračunali tako, da smo pri vsaki osebi registrirali tri prstne odtise, nato pa smo z njimi primerjali ostalih sedem odtisov. Pri izračunu FAR smo prve tri odtise neke osebe primerjali s prvimi tremi odtisi vseh ostalih oseb.

3.3 Rezultati

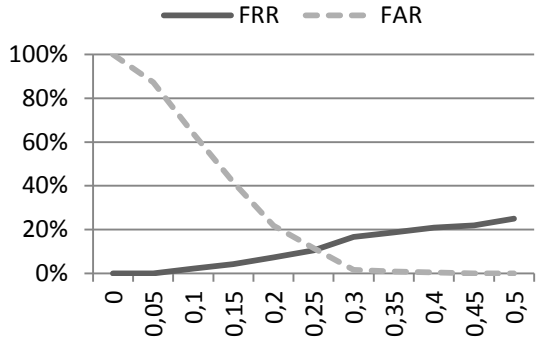
Z obema čitalcema smo izvedli omenjena testa tako, da smo najprej izvedli primerjanje z enim registriranim prstnim odtisom, nato pa še s tremi registriranimi odtisi. Vse teste smo izvedli pri različnih vrednostih odločitvenega praga. Slike 2-5 prikazujejo rezultate ROC, dobljene z obema čitalcema. Na abscisni osi prikazujemo vrednost odločitvenega praga, ordinatna os pa prikazuje odstotek FRR in FAR v odvisnosti od odločitvenega praga.

3.3.1 Secugen Hamster Plus



Slika 2. Secugen Hamster Plus – en registriran odtis.

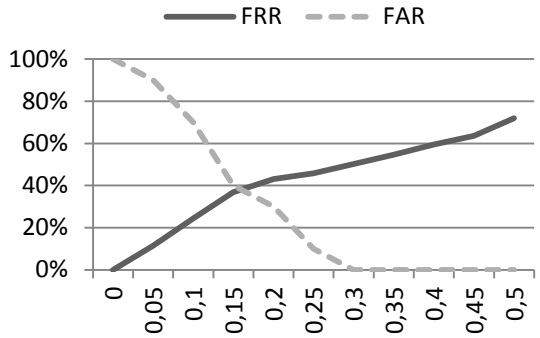
Pri enem registriranem odtisu dobimo slabe rezultate (slika 2). Če bi želeli imeti zanesljiv sistem, vidimo, da bi morali odločitveni prag postaviti na 0,35, vendar bi s tem sistem nepravilno zavrnil dobrih 40% odtisov, kar pa v realnem sistemu ni sprejemljivo.



Slika 3. Secugen Hamster Plus – trije registrirani odtisi.

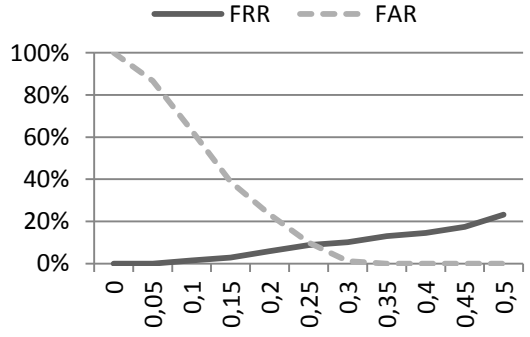
Pri treh registriranih prstnih odtisih se rezultati precej izboljšajo (slika 3). Pri odločitvenem 0,35 pragu znaša FRR slabih 19%, delež FAR pa pade pod 1%.

3.3.2 DigitalPersona U.are.U4000B



Slika 4. DigitalPersona U.are.U4000B – en registriran odtis.

V primerjavi s Secugen Hamster Plus imamo v tem primeru pri odločitvenem pragu 0,35 sicer enak odstotek FAR (0%), vendar opazimo, da znaša delež nepravilno zavrnjenih pri DigitalPersona U.are.U4000B okoli 55%, kar je 15% več kot pri Secugen Hamster Plus (slika 4).



Slika 5. DigitalPersona U.are.U4000B – trije registrirani odtisi.

Iz slike 5 je razvidno, da imamo pri odločitvenem pragu 0,30 že izredno majhen odstotek FAR (približno 1%), kar je malenkost manj kot pri Secugen Hamster Plus (približno 1,6%). Vidimo pa lahko opazno boljši rezultat FRR, ki pri DigitalPersona U.are.U4000B znaša približno 11%, pri Secugen Hamster Plus pa dobrih 16%. Vidimo lahko, da se razlike med čitalcema pri treh registriranih prstnih odtisih zmanjšajo.

Na podlagi dobljenih rezultatov smo ugotovili, da se pri enem registriranem prstnem odtisu v našem sistemu bolje obnese čitalec Secugen Hamster Plus. Pri treh registriranih prstnih odtisih se razlike med čitalcema zmanjšajo, tako da sta v tem primeru precej izenačena. Na testirani bazi odtisov je v skupnem seštevku Secugen Hamster Plus vseeno v manjši prednosti pred DigitalPersona U.are.U4000B.

3.4 Grafični vmesnik

Pred nadgradnjo je sistem vključeval grafični vmesnik, ki je omogočal ročni zajem prstnega odtisa, njegovo registracijo ter testiranje funkcionalnosti sistema. Te funkcionalnosti vključujejo ročno preverjanje korakov segmentacije, izboljšanja kvalitete slik odtisov, binarizacije, tanjšanja grebenov, iskanja značilk, klasifikacije in primerjanja. Ta vmesnik torej vsebuje funkcije za zajem odtisov, njihovo registracijo ter analiziranje rezultatov, zato je njegova primarna funkcija namenjena testiranju posameznih korakov sistema. Slednji je z nadgradnjo pridobil dodatne funkcije, še vedno pa se uporablja za testiranje sistema in je kot takšen v prvi vrsti namenjen razvijalcu.

Nadgradnja je sistemu prinesla tudi novo podobo v obliki novega grafičnega vmesnika, ki je namenjen končnemu uporabniku (slika 6), hkrati pa smo za potrebe razvoja, testiranja in nadaljnih izboljšav v ozadju obdržali star vmesnik.

Slika 6. Grafični vmesnik za končnega uporabnika, ki ga je sistem dobil z nadgradnjo. Vključuje nov grafični dizajn ter animacije in efekte, ki naredijo sistem za uporabnika bolj zanimiv, skrije pa detajle procesiranja.

Končnega uporabnika ne smejo skrbeti tehnične podrobnosti, zato je nova podoba vmesnika zasnovana na način, ki skuša biti uporabniku čimbolj prijazen. Za to poskrbita grafični dizajn ter dodane animacije, ki popestrijo uporabo takšnega sistema. Animacije vključujejo razne efekte, kot so animirana črta, ki preverja prstni odtis, animirano kroženje po odtisih iz baze ter animiran izris prstnega odtisa, ki mu sledi sporočilo o odobritvi oziroma zavrnitvi vstopa.

3.5 Verifikacija uporabnika

V sklopu novega grafičnega vmesnika smo implementirali tudi funkcijo, ki na podlagi vhodnega prstnega odtisa verificira (v trenutnem sistemu pravzaprav identificira) uporabnika in mu v primeru uspeha odobri vstop, sicer pa ga zavrne.

Algoritem najprej shrani imena vseh oseb, katerih odtisi se ujemajo z vhodnim odtisom. Poleg imen shrani tudi pripadajoče število ujemanj za posamezno osebo. Nato se na podlagi dobljenih številk izpiše ime osebe, ki vsebuje največje število ujemanj z vhodnim odtisom. Vkolikor se vhodni odtis ne ujema z nobenim odtisom v bazi ali pa dobi za neko osebo samo eno ujemanje, sistem uporabnika zavrne s sporočilom, da vstop ni dovoljen. Ujemanje vhodnega odtisa s samo enim od desetih registriranih odtisov je namreč premalo zanesljiv pokazatelj za pozitivno odločitev. Če sistem ugotovi, da se z vhodnim odtisom v enakem številu ujemata dve ali več oseb, sistem opozori uporabnika, da naj poskusi ponovno.

Poleg opisanega smo v sistem dodatno integrirali tudi metode za ocenjevanje kvalitete slik zajetih prstnih odtisov [6]. Rezultate razpoznave s slabim in dobrim odtisom prikazujeta tabeli 1 in 2. Izhodišče postopka razpoznave: vzame se registriran prstni odtis kot vhodni odtis in se ga primerja s preostalimi devetimi odtisi iste osebe ter vsemi odtisi ostalih registriranih oseb.

Tabela 1. Primer slabo zajetega prstnega odtisa – vhodni odtis je pravilno razpoznan v samo 50 odstotkih. Število ujemanj vhodnega odtisa z ostalimi je majhno (v povprečju 1,5, kar je premalo za zanesljiv sistem).

Oseba_A		
Prstni odtis (vseh 10 registriranih)	**Razpoznane osebe**	**Št. ujemanj z vhod. odtisom**
Oseba_A1	*Oseba_A*	*2*
Oseba_A2	/	*0*
Oseba_A3	*Oseba_A*	*2*
Oseba_A4	*Oseba_A*	*2*
Oseba_A5	/	*0*
Oseba_A6	*Oseba_B*,Oseba_A,Oseba_C	*3*, 2, 1
Oseba_A7	*Oseba_B,Oseba_A,Oseba_C*	*1, 1, 1*
Oseba_A8	*Oseba_A*	*3*
Oseba_A9	*Oseba_B,Oseba_D*	*1, 1*
Oseba_A10	*Oseba_A*	*3*
Skupaj (delež)	**5/10 (50%)**	

Tabela 2. Primer dobro zajetega prstnega odtisa – vhodni odtis je pravilno razpoznan v 90 odstotkih. Število ujemanj vhodnega odtisa z ostalimi je zadovoljivo (v povprečju 4,7).

Oseba_A		
Prstni odtis (vseh 10 registriranih)	**Razpoznane osebe**	**Št. ujemanj z vhodnim odtisom**
Oseba_A1	*Oseba_A*,Oseba_B	*5*, 1
Oseba_A2	*Oseba_A*,Oseba_B	*5*, 1
Oseba_A3	*Oseba_A*,Oseba_B	*6*, 1
Oseba_A4	*Oseba_A*	*2*
Oseba_A5	*Oseba_A*	*5*
Oseba_A6	*Oseba_A*	*6*
Oseba_A7	*Oseba_A*	*6*
Oseba_A8	*Oseba_A*	*6*
Oseba_A9	/	0
Oseba_A10	*Oseba_A*	*6*
Skupaj (delež)	**9/10 (90%)**	

4 Zaključek

Prototip sistema za verifikacijo oseb na podlagi prstnih odtisov se je s svojo modularno zgradbo izkazal kot dobra osnova za nadaljne raziskave in nadgradnje. Nov grafični vmesnik je v kombinaciji s funkcijo verifikacije uporabnika sistemu dodal praktično uporabno vrednost, tako da lahko sistem uporablja tudi končni uporabnik. Največ težav še vedno povzroča zanesljivost sistema, zato je na tem področju potrebno še marsikaj izboljšati. Sistem bomo v prvem planu izboljšali predvsem na področju določanja kvalitete slik zajetih odtisov ter iskanja singularnih točk.

Zahvala

Delo na projektu kompetenčnega centra je sofinancirano s strani MVZT in Evropskega sklada za regionalni razvoj ter podjetij Mega M d.o.o. in MIEL d.o.o.

Literatura

[1] M.U. Akram, A. Tariq, S.A. Khan, S. Nasir, »FingerPrint image: pre and post-processing«, *International Journal of Biometrics*, letnik 1(1), str. 63-80, 2008.

[2] J. Bo, T. H. Ping, X. M. Lan, »Fingerprint Singular Point Detection Algorithm by Poincare Index«, *The College of Electrical and Information Engineering, Zheijang Textile and Fashion College*, letnik 7(12), 2008.

[3] U. Klopčič, P. Peer, »Fingerprint-based verification system: a research prototype«, *Int. Conf. on Systems, Signals and Image Process.*, str. 150-153, 2010.

[4] P.M. Patil, S.R. Suralkar, F.B. Sheikh, »Rotation invariant thinning algorithm to detect ridge bifurcations for fingerprint identification«, *IEEE Int. Conf. on Tools with Artificial Intelligence*, str. 641 – 649, 2005.

[5] J. Qi, M. Xie, »A robust algorithm for fingerprint singular point detection and image reference direction determination based on the analysis of curvature map«, *IEEE Conf. on Cybernetics and Intelligent Systems*, str. 1051-1054, 2008.

[6] J. Bule, M. Tovšak, P. Peer, »Ocena kvalitete slike prstnega odtisa«, poslano v obravnavo, *ERK 2011*.