DOI: 10.19279/TVZ.PD.2016-4-3-16

OTPORNOST AUTENTIFIKACIJE BIOMETRIJSKOM METODOM OTISKA PRSTA NA PROBIJANJE

SECURITY OF BIOMETRIC SECURITY SYSTEMS BASED ON FINGERPRINT AUTHENTICATION

Kristijan Pukšič[1], Marinko Žagar[2]

[1]Student TVZ-a
[2]Tehničko veleučilište u Zagrebu

Sažetak

Cilj ovoga rada je istraživanje otpornosti na prijevaru autentifikacije biometrijskom metodom otiskom prsta. U radu su opisane metode identifikacije otiskom prsta, uspoređivanja i klasifikacije otisaka prstiju do sigurnosti biometrijskih uređaja, posebna pažnja posvećena je testiranju otpornosti biometrijskog sustava za kontrolu pristupa na silikonske krivotvorene otiske prstiju. Prikazan je postupak stvaranja silikonskih otisaka prsta te je napravljeno testiranje otpornosti sustava pomoću istih.

Ovim radom dokazano je da svi biometrijski sustavi za kontrolu pristupa otiskom prsta ne pružaju potrebnu razinu zaštite.

Ključne riječi: *biometrija, otisak prsta, autentifikacija, silikonski otisak prsta*

Abstract

Main goal of this work is getting known with biometrics, with its methods that are used for authorization and authentication, and with its technologies. In this work we gave detailed descriptions of fingerprint identification methods, matching and classifying fingerprints and security of fingerprint devices. Special attention has been dedicated to the resistance of biometric system for access control to fake silicon fingerprints. Procedure of creating fake silicon fingers has been shown as well as testing of biometrics system resistance to it. With this work, it is proven that biometric systems for access control with fingerprint do not provide necessary protection.

Keywords: *biometrics, fingerprint, authetication, silicon fingerprint*

1. Uvod

1. *Introduction*

Tisućama godina, određene tjelesne karakteristike kao što su lice osobe, glas i način hoda, korištene su kako bi se ljudi mogli međusobno prepoznati. U sredini XIX. stoljeća, Alphonse Bertillon, šef odjela kriminalne identifikacije policijskog odsjeka u Parizu, razvio je i usavršio ideju korištenja različitih tjelesnih mjera (visina osobe, dužina stopala, boja kose) za identifikaciju kriminalaca.

U kasnom XIX. stoljeću, baš kada je njegova ideja stekla popularnost, zasjenjena je od daleko značajnijeg i praktičnijeg otkrića, različitosti ljudskih otisaka prstiju. Nedugo nakon ovog otkrića, mnogi važni policijski odjeli prihvatili su ideju "zapisivanja" otisaka prstiju kriminalaca i njihovo spremanje u bazama podataka (prvotno kartoteke). Kasnije je policija stekla sposobnost da "podigne" otisak, tipično fragmentiran, sa mjesta zločina i uspoređuje ga s otiscima iz baze podataka da bi odredila identitet kriminalca.

Biometrija je automatizirana metoda prepoznavanja osobe bazirana na fizičkim karakteristikama ili karakteristikama ponašanja.

Izraz "biometrija" dolazi od 2 grčke riječi, BIOS (grčki bios - život) i METRIKOS (grčki metrikos - mjeri), i znači "životna mjera". Počeo se koristiti početkom 20 stoljeća i odnosio se na područje statističkih i matematičkih metoda koje se primjenjuju na probleme analize podataka u biološkim znanostima.

Statističke metode koje su obuhvaćale poljoprivredna eksperimentiranja radi usporede polja sa različitim sortama pšenice, analizu podataka bolničkih nalaza za procjenu relativne učinkovitosti terapija na bolesti ili za analizu

podataka ekološkog istraživanja oko učinaka zračnih i vodenih onečišćenja na pojavljivanje ljudskih bolesti u regiji ili zemlji, primjeri su primjena koje spadaju pod naziv zvan "biometrija".

Izraz "biometrija" danas se koristi da bi se prikazala autentičnost osobe preko analize fizičkih karakteristika, kao što su otisci prsta ili karakteristika vezana uz ponašanje kao što je potpis [1].

Fizičke karakteristike koje se obično koriste u biometrijskoj ovjeri vjerodostojnosti uključuju lice, otiske prstiju, otisak ruke (dlana), oči i glas. Mnoge fizičke karakteristike pojedinaca jedinstvene su i stoga biometrija pruža pouzdaniji sustav ovjere vjerodostojnosti nego ID kartice (eng identity document), ključevi, lozinke ili drugi tradicionalni sustavi [1].

Osnovna fizička obilježja koja se koriste kao biometrijske karakteristike moraju zadovoljavati uvjete univerzalnost, raznolikost i trajnost .

Biometrijski sustavi su sustavi prepoznavanja po uzorku koji prepoznaju osobu temeljeno na vektorskim obilježjima koji se dobivaju od specifičnih fizičkih karakteristika ili karakteristika ponašanja koje neka osoba posjeduje.

Ovisno o primjeni, biometrijski sustav djeluje na način ovjere ili identifikacije.

U načinu ovjere, sustav potvrđuje identitet osobe uspoređivanjem biometrijskih karakteristika već snimljenih u bazu podataka. U takvom sustavu, pojedinac koji želi biti prepoznat potvrđuje identitet (obično putem osobnog identifikacijskog broja, korisničkog imena, pametne kartice ili slično), i sustav izvodi jednu usporedbu da odredi da li je prepoznavanje istinito.

Ovjera identiteta odgovara na pitanje "Da li sam ja taj koji tvrdim da jesam", identitet korisnika je poznat te se tipično upotrebljava za pozitivno prepoznavanje gdje je cilj spriječiti višestruko korištenje istog identiteta, 1:1.

U načinu identifikacije, pojedinac ne potvrđuje svoj identitet nekim brojem već sustav uspoređuje stečeni uzorak sa svim uzorcima snimljenima u bazi. Identifikacija odgovara na pitanje "Tko sam ja?", identitet korisnika nije poznat te se tipično upotrebljava za negativno prepoznavanje gdje je cilj spriječiti jednog korisnika da koristi više identiteta, 1:N.

Dok tradicionalne metode osobnog prepoznavanja kao na primjer lozinke, brojevi, ključevi i znakovi rade za pozitivno, jedino biometrija može biti korištena za negativno prepoznavanje [1].

Da bi se olakšalo uspoređivanje, element ekstraktora obrađuje ulazni otisak radi generiranja kompaktnog ali izraženog prikaza, zvanog predložak.

Ovisno o primjeni, biometrijski sustav mogao bi spremiti predložak u njegovoj središnjoj bazi podataka ili ga zabilježiti na pametnoj kartici koja je izdana pojedincu.

1.1 Biometrijske pogreške sustava

1.1 *Biometric systems errors*

Dva uzorka iste biometrijske karakteristike, na primjer dva otiska desnog kažiprsta, nisu potpuno isti zbog nesavršenog prikaza stanja (prljavi senzor, suhi prsti), promjene u korisničkim fiziološkim karakteristikama ili karakteristikama ponašanja (kao na primjer rezovi i ozljede na prstu), ambijentnih stanja (kao na primjer temperatura i vlažnost) te korisničke interakcije sa senzorom (kao na primjer mjesto stavljanja prsta).

Slika 1 *Usporedba starog i novog otiska*

Figure 1 *Comparison of old and new fingerprints*

Otisci prsta iste osobe prije i nakon 3 mjeseca. Posjekotine ili ožiljci na prstu mogu uzrokovati netočno prepoznavanje[1].

Odgovor biometrijskog sustava prepoznavanja tipičnog je rezultata "s" (obično jedan broj) da izmjeri sličnost između ulaznih podataka i prikazanih predložaka iz baze podataka. Radi jednostavnosti, pretpostavlja se da sustav zapravo prikazuje odgovarajući rezultat korisniku. Neki sustavi mogli bi

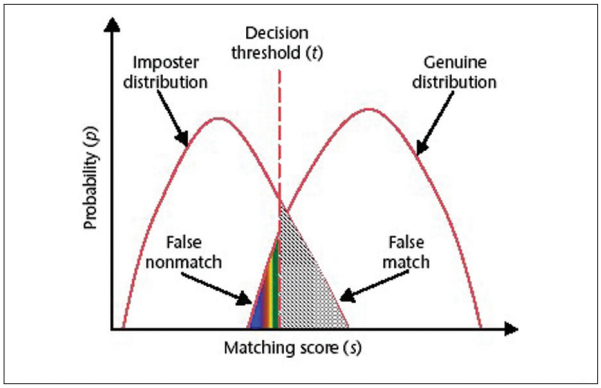
1 www.biometrics.cse.msu.ed

prikazati samo konačnu odluku temeljenu na predodređenim kriterijima ili pragu.

Što je viši rezultat to je sustav sigurniji da dvije biometrijske izmjere dolaze od iste osobe [1].

Prag "t" uređuje odluku sustava. Ako sustav zaključi da parovi biometrijskih uzoraka generiraju viši ili jednaki rezultat naspram "t" onda su to "mate pairs" (pripadaju istoj osobi). Dakle, ako par biometrijskih uzoraka generira niži rezultat nego "t" onda su to "nonmate pairs" (pripadaju različitim osobama).

Distribucija rezultata generiranih od parova uzoraka različitih osoba zove se "impostor distribution" (distribucija varalica) a rezultat distribucije generiran od parova uzoraka iste osobe naziva se "genuine distribution" (istinska distribucija), slika 2.



Slika 2 *Greške procjene biometrijskih sustava kod uspoređivanja više otisaka prsta* [2]

Figure 2 *Biometric systematic error of the estimate* [3]

Biometrijski potvrdni sustav može napraviti dva tipa pogrešaka:

- mjere od dvije različite osobe su u biti od iste osobe (netočna podudarnost ili lažno prihvaćanje, FMR (eng False Match Rate)
- dvije mjere od iste osobe su u biti od dvije različite osobe (netočna nepodudarnost ili lažno odbijanje, FNMR (eng False Non-Match Rate)

Operativni biometrijski sustav radi razmjenu između netočne podudarnosti procjene (FMR) i lažne non-match procijene (FNMR). Zapravo, oba FMR i FNMR su funkcije sustavnog praga "t". Ako dizajneri sustava smanje "t" da bi sustav bio više tolerantniji prema ulaznim varijacijama i smetnjama, FMR poraste. S druge strane, ako podignu vrijednost "t" da bi sustav više osigurali, FNMR poraste [1].

Osim ova dva priznanja stupnjeva pogreške, također se upotrebljavaju mjere neuspjeha prema hvatanju (FTC, eng Failure to capture rate) i neuspjeha upisa (FTE, eng Failure to enroll rate) da bi se sažela biometrijska točnost sustava. FTC procjena, koja se primjenjuje samo kada biometrijski uređaj izvrši "automatsko-hvatačku" funkciju, bilježi postotak neuspjelog automatskog hvatanja uzorka biometrijskog uređaja kada je prikazan biometrijskom karakteristikom. Ovaj tip pogreške tipično se događa kada uređaj ne može locirati biometrijski signal dovoljne kakvoće, na primjer, ako primi jako slab otisak prstiju ili zatvoreno lice.

FTE procjena, s druge strane, bilježi postotak neuspjelog upisivanja u sustav prepoznavanja. Postoji razmjena između FTE procjene i opažene točnosti sustava (FMR i FNMR). FTE greške događaju se kada sustav odbije predloške slabe kvalitete tijekom stavljanja na popis. Dakle, baza podataka sadržava jedino visoko-kvalitetne predloške, i time se točnost sustava poboljšava.

Zbog međuzavisnosti između otkaznih mjera i stupnjeva pogreške, sve ove pogreške (FTE, FTC, FNMR i FMR) čine važnu izvedbu biometrijskog sustava.

Dobivanjem biometrijske točnosti sustava u načinu ovjere, možemo približno zaključiti njegovu točnost u identifikacijskom načinu preko pojednostavljujućih pretpostavka. Obilježimo identifikacijski "lažni nonmatch" i "lažni match" s FNMRN i FMRN, gdje N predstavlja broj identiteta u bazi podataka sustava [1].

Zahtjevi biometrijske točnosti sustava ovise najviše o primjeni. Na primjer, u nekim forenzičkim primjenama, kao na primjer kriminalna identifikacija, FNMR procjena (kao i FMR) je kritičan nacrt objave. Naime, ne želi se promašiti kriminalac čak ni kod rizika od ručnog pregledavanja velikog broja potencijalno netočnih mjera koje biometrijski sustav identificira. No, FMR bi mogao biti jedno od najvažnijih faktora kod primjena s visokom razinom sigurnosti kontrole ulaza, gdje je glavni cilj odvratiti varalice.

Različite biometrijske primjene stvaraju različite razmjene između netočne podudarnosti i lažnih nonmatch procjena (FMR i FNMR). Neshvaćanje

2 www.biometrics.cse.msu.edu

3 www.biometrics.cse.msu.edu

stupnjeva pogrešaka glavni su izvor zbrke u točnosti sustava kod prodavača i zajednica korisnika[4].

U nekoliko civilnih primjena, zahtjevi za učinkovitošću leže između ove dvije krajnosti, i moramo uzeti u obzir vrijednosti FMR i FNMR-a. U primjenama kao, na primjer, ATM ovjera karticom, kriva mjera bi značila gubitak nekoliko stotina dolara, dok visok FNMR može dovesti do gubitaka cijenjenih mušterija. Slika 5 opisuje razmjene FMR i FNMR-a u drugačijem tipu biometrijske primjene [1].

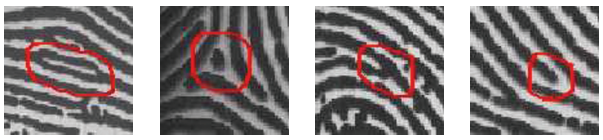
2. Metoda prepoznavanja putem otisaka prstiju

2. *Methods for identification through fingerprint*

Otisak prsta najstarija je metoda ovjere identiteta. U ranom 20-om stoljeću službeno je prihvaćena kao odobrena metoda ovjere identiteta na zakonodavnom sudu.

Jedinstveni otisak prsta kod čovjeka se formira 10 tjedana nakon začeća i više se neće mijenjati osim u slučaju ozljeda kao što su porezotine i opekline ili kemijska oštećenja. Ova svojstva otiska prsta čine ga poželjnim kandidatom za ovjeru identiteta [2].

Identifikacija putem otisaka prstiju oslanja se na uspoređivanju uzoraka zajedno sa otkrivanjem određenih karakteristika brazde, točke identiteta ili detaljne točke i usporedbu srodnih pozicija detaljnih točaka sa ispisom, uobičajeno tintna slika osumnjičenog ispisa.



Otok Točka Bifurkacija Kraj brazde

Slika 3 *Glavne karakteristike brazde*

Figure 3 *The main characteristics of the ridge*

Identifikacijske detaljne točke sastoje se od bifurkacija, krajeva brazdi, točaka, brazdi i otoka. Jedan otisak prsta može imati oko 100 ili više identifikacijskih točaka koje se mogu koristiti za identifikacijske svrhe. Nema određenih zahtjeva za veličinu otiska jer broj točaka nađenih na slici otiska prsta ovisi o lokaciji ispisa. Na primjer, područje koje okružuje ušće (delta) vjerojatno će sadržavati više točaka po četvornom milimetru nego područje bliže vrhu prsta koje nema toliko točaka.

Automatska identifikacija otiskom prsta prati slijedeća četiri postupka [3]:

- stjecanje uzorka otiska prsta
- obrada uzorka otiska prsta
- izdvajanje bitnih detalja uzorka otiska prsta
- usporedba uzorka otiska prsta

kraj brazde		most	
bifurkacija		dvostruka bifurkacija	
točka		trifurkacija	
otok (kratka brazda)		suprotstavljena bifurkacija	
jezero (ograda)		presjek brazdi	
udica (greben)		suprotstavljena bifurkacija /kraj brazde	

Slika 4 *Osnovne i pomiješane karakteristike brazde (detaljne točke)*

Figure 4 *Basic and mixed ridge characteristics*

2.1 Uspoređivanje uzorka otisaka prstiju

2.1 *Comparing the fingerprints sample*

Tehnike uspoređivanje otisaka prstiju mogu se podijeliti u 2 kategorije: tehnike bazirane na detaljnim točkama i tehnike bazirane na međusobnoj povezanosti.

Tehnike bazirane na detaljnim točkama prvo pronalaze detaljne točke i onda označavaju njihova mjesta na prstu. Iako, postoje određeni problemi kada se koristi ovaj pristup. Teško je precizno izvući detaljne točke kada imamo otisak prsta koji je loše kvalitete. Isto tako, ova metoda ne uzima u obzir cijeli uzorak brazdi i dolina.

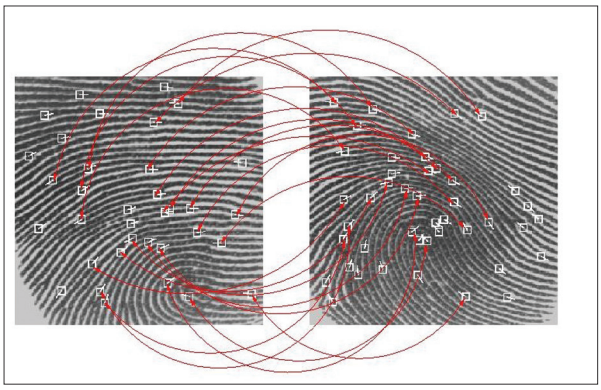
Tehnike bazirane na međusobnoj povezanosti sposobne su zaobići neke probleme pristupa s detaljnim točkama. Iako, i one imaju nekoliko mana. Tehnike bazirane na međusobnoj povezanosti

4 www.biometrics.cse.msu.edu

zahtijevaju preciznu lokaciju evidentirane točke i na njih utječe premještanje te rotacija slike.

Slika 5 *Tehnika uspoređivanja bazirana na detaljnim točkama*

Figure 5 *Detailed points comparisons technique*



Slika 6 *Tehnika uspoređivanja bazirana na međusobnoj povezanosti*

Figure 6 *The technique of comparing based on interconnectedness*

Razvijaju se algoritmi koji su još više otporniji na smetnje u uzorcima otisaka prstiju i donose povećanu preciznost u realnom vremenu. Komercijalni sustav ovjeravanja baziran na otiscima prstiju zahtijeva vrlo malu lažnu povratnu frekvenciju FRR (eng False Reject Rate) za danu lažnu prihvaćenu frekvenciju FAR (eng False Accept Rate) [4].

Ovo je vrlo teško za postići sa bilo kojoj tehnikom te se istražuju metode različitih tehnologija uspoređivanja da bi se povećala cjelokupna preciznost sustava.

3. Sigurnost biometrijskih sustava

3. *Biometric systems security*

Upotreba biometrije, u današnje vrijeme, znatno se povećala i smatra se izrazito sigurnom metodom za identifikaciju i autorizaciju pojedinaca. Neke druge tehnike kao što su lozinke, PIN-ovi i ID kartice jednako su rasprostranjene ali posjeduju nedostatke u obliku lakog zaboravljanja, mogu se izgubiti i ukrasti [6]. Nadalje, tradicionalne tehnike ne razlikuju lažno predstavljanje sa ukradenim identitetom od izvornog identiteta. Rješenje za povećanje sigurnosti ovih metoda nalazi se u korištenju biometrije koja ima velike prednosti naspram tradicionalnih metoda zbog nemogućnosti gubitka ili krađe identiteta [7]. Zbog tih se karakteristika upotreba biometrije znatno povećala i sada je vidljiva u skoro svakom segmentu potrošačke elektronike, od mobitela, automobila, računala, kontrole pristupa pa do elektronskog bankarstva.

Ipak, usprkos svim prednostima, biometrijski sustavi imaju svoje nedostatke u obliku:

- nedostatka tajnovitosti (svima je poznato lice pojedinca i svi mogu doći u posjed otiska prsta)
- činjenice da biometrijska karakteristika ne može biti zamijenjena (zaboravljena lozinka se lako može promijeniti ali se 'ukradeni' otisak prsta ne može zamijeniti)
- nedostataka biometrijskih senzora (vremenski uvjeti kao što su zima, kiša, sunce, vlažnost, dan/noć te fizičko oštećenje i direktan pristup znatno utječu na rad senzora)[5].

Upravo ovi nedostaci biometrijskih sustava omogućavaju potencijalnim napadačima pokušaj lažnog predstavljanja biometrijskim sustavima i pristup zaštićenim podacima/prostorijama te se mogu podijeliti na nekoliko razina napada:

- napad na razini obrade i prijenosa biometrijskog uzorka
- napad na razini stjecanja biometrijskih podataka
- napad na biometrijske podsustave
- napad prilikom pristupa biometrijskim sustavima

3.1 Umjetni krivotvoreni otisci prstiju

3.1 *Artificial falsified fingerprints*

Iako biometrijski uređaji na prvi pogled pružaju dojam izvrsne sigurnosti i nadasve praktičnosti, iz gore navedenog vidljivo je da to baš i nije tako. Razina sigurnosti biometrijskih uređaja direktno je povezana sa kvalitetom i razinom ugrađenih sigurnosnih mehanizama, odnosno arhitekturom sigurnosnih mehanizama

biometrijskih uređaja, te još više, sa kvalitetom i upornošću potencijalnog napadača.

Biometrijski uređaji bazirani na otiscima prstiju osjetljivi su na niz napada kao što su registrirani prst, neregistrirani prst, genetski klon registriranog prsta te možda i najčešće korišteni napad na biometrijske uređaje otiskom prsta, napad umjetnim otiskom prsta [8].

Registrirani prst

Krađa otiska prsta stavljanjem izvornog prsta u kalup, prisilom korisnika da stavi prst na senzor direktno ili pod prisilom opojnih sredstava.

Odvajanje prsta od tijela izvornog vlasnika.

Neregistrirani prst

Napadač koristi svoj vlastiti prst da bi se pokušao spojiti kao neki drugi korisnik. Uspješnost ovakvoga napada ovisi o FAR razini biometrijskog uređaja, ili u slučaju kategoriziranog sustava kao što je 'loops' ili 'arches', sa predstavljanjem sličnog neregistriranog uzorka kao kod registriranog prsta.

Genetski klon registriranog prsta

Napadač koristi genetski klon otiska prsta ili koristi sličnost otiska prsta blizanaca. Uspješnost ovakvoga napada ovisi o FAR razini biometrijskog uređaja jer otisci prstiju blizanaca nisu jednaki.

Umjetni otisak prsta

Napadač koristi umjetne otiske prstiju napravljene od lako dostupnih materijala kao što su žele, silikon, kopirni aparat, glina, vosak i slično. U ovom načinu, napadač treba imati pristup originalnom otisku prsta i izradom kalupa od izvornog prsta ili korištenjem latentnih otisaka napraviti umjetni otisak [8].

Za napad na biometrijske uređaje koji koriste tehniku otisaka prstiju, najčešća metoda napada je metoda korištenjem umjetnih otisaka prstiju. Takva metoda napada najprihvatljivija je napadačima jer ne zahtjeva direktan kontakt sa žrtvom (vlasnikom izvornog prsta), zbog lake dostupnosti materijala potrebnih za izradu lažnih otisaka prstiju te zbog lakog i brzog procesa izrade dovoljno kvalitetnog lažnog otiska prsta.

Uspješnost ovakvih napada vrlo je visoka kod biometrijskih uređaja u komercijalnog upotrebi, posebno kod privatnih korisnika, dok je dosta manja kod primjena u državnim institucijama, institucijama visoke sigurnosti i kod forenzike zbog korištenja multimodalnih metoda, odnosno zbog korištenja više biometrijskih karakteristika potrebnih za ovjeru.

FMR faktor, odnosno faktor lažnog prihvaćanja, glavni je uzrok visoke tolerancije biometrijskih uređaja tehnikom otiskom prsta na lažne otiske prstiju. Naime, zbog sve veće upotrebe biometrijskih uređaja u komercijalnim primjenama (osobna računala, mobiteli, automobili, pristup objektima) i zbog sve veće dostupnosti biometrijskih tehnologija privatnim korisnicima, FMR faktor je uobičajeno smanjen na dovoljno nisku razinu koja omogućuje korisnicima više uspješnih od neuspješnih ovjera. Tim se postupkom ide na ruku zadovoljstvu privatnih korisnika ali se isto tako narušava sigurnost biometrijskih sustava, odnosno smisao njihovog postojanja, a to je sigurna i jednostavna ovjera/identifikacija korisnika.

FMR faktor ujedno određuje i sami materijal te tehniku koja će se koristiti za izradu lažnog umjetnog otiska prsta. Što je manji FMR faktor, to je manja potreba za kvalitetnijim materijalima, složenijim tehnikama izrade lažnog otiska prsta te kvalitetnijem izvornom otisku prsta (oštećeni latentni otisak). Što je FMR faktor veći, samim time potrebno je imati pristup kvalitetnijem izvornom otisku prsta (pristup izvornom prstu ili latentni uzorak visoke kvalitete) te pristup kvalitetnijim i skupljim materijalima i uređajima.

4. Izrada umjetnog otiska prsta

4. *Creation of artifical fingerprint*

Za potrebe istraživanja otpornosti biometrijskih sustava koji koriste metodu identificiranja otiskom prsta, bilo je potrebno izraditi lažni silikonski otisak prstiju i pri tome su korišteni slijedeći materijali.

Za izradu kalupa lažnog silikonskog otiska prsta:

- vosak (rastopljena obična svijeća)
- glina (glina za modeliranje)
- silikon (Kremer Latex Milch)
- slikarski kist

Za izradu lažnog silikonskog otiska prsta:

- silikon (Kremer Latex Milch, Pattex sanitarni silikon)
- grafit (Kremer Graphit-Schwarzpuder)
- vazelin

Za potrebe istraživanja korišteni su slijedeći uređaji:

- Anviz VF30
- Crossmatch Verifier 320 LC

- LG G2 mobitel
- IPHONE 6S mobitel

Za potrebe uzimanja, obrade i uspoređivanja uzorka izvornih i lažnih otisaka prstiju korištene su slijedeće aplikacije:

- EFinger (obrada i usporedba otiska prsta)
- Crossmatch (stjecanje izvornog i lažnog otiska prsta)

Slika 7 *Kremex Latex Milch i Graphit*

Figure 7 *Kremex Latex Milch i Graphit*

4.1 Metode rada

4.1 *Working methods*

Za potrebe testiranja otpornosti biometrijske identifikacije otiskom prsta na lažne silikonske otiske prstiju korištena je metoda dobrovoljnog pristanka izvornog korisnika koji dopušta da se njegov prst koristi za potrebe ovoga testiranja te da se od njegovog prsta napravi kvalitetan kalup te lažni silikonski otisak prsta.

4.2 Izrada kalupa izvornog otiska prsta

4.2 *The original fingerprint matrix production*

Otisak prsta sastoji se od vrlo sitnih i detaljnih grebena i dolina koji tvore detaljne točke prijeko potrebne za uspješnu ovjeru ili identifikaciju. Da bi se napravio dovoljno kvalitetan lažni otisak prsta koji će omogućiti uspješnu ovjeru, napravljen je dovoljno kvalitetan kalup (negativ otiska prsta) od izvornog otiska prsta. Detaljne točke trebaju biti maksimalno očuvane prilikom postupka izrade lažnog otiska prsta.

Za izradu kalupa od izvornog otiska prsta korišteni su slijedeći materijali:

- vosak (rastopljena obična svijeća)
- glina (glina za modeliranje)
- silikon (Kremer Latex Milch)
- slikarski kist

4.2.1 Vosak

4.2.1 *Wax*

Kao jedan od najdostupnijih materijala za izradu kalupa izvornog otiska prsta koristi se vosak od svijeće.

Svijeća se stavi u posudu koja se grije te se zbog velike temperature vosak svijeće otopi i pretvori u tekućinu. Odabere se prikladno mjesto te se tekući vosak izlije u odgovarajućoj količini. Nakon što je tekući vosak pripremljen, izvorni prst stavlja se u njega te se čeka dok se vosak ponovo ne stvrdne. Nakon jedne minute, izvorni prst može se maknuti iz voska te je kalup izvornog otiska prsta spreman za daljnje korištenje.

Slika 8 *Kalup od voska svijeće*

Figure 8 *The wax candles matrix*

4.2.2 Glina

4.2.2 *Clay*

Glina za modeliranje je vrlo dostupan i jednostavan materijal za izradu kalupa.

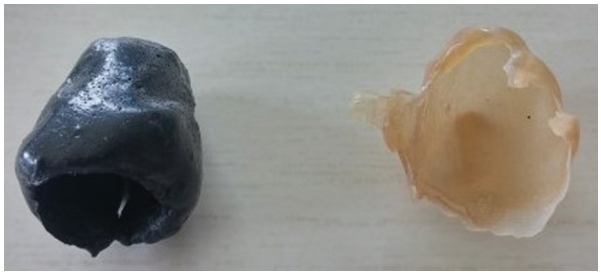
Odvoji se dovoljno gline za izradu kalupa te se pripremi na prikladnoj površini. Nakon što je glina pripremljena, u nju se pritisne izvorni prst te se pričeka jednu minutu. Nakon jedne minute glina je spremna za sušenje te je potrebno pričekati 24 sata nakon čega je kalup od gline spreman za daljnje korištenje.

Slika 9 *Kalup od gline*
Figure 9 *Clay matrix*

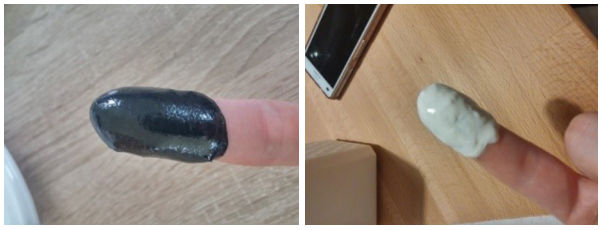
4.2.3 Silikon

4.2.3 *Silicone*

Za izradu kalupa od silikona korišteno je tekuće latex mlijeko, odnosno Kremer Latex Milch. Prednost ovoga silikona je to što je vrlo viskozno te ima sposobnost hvatanja najsitnijih detalja prsta. Samim time vrlo je poželjan materijal za izradu kalupa izvornog otiska prsta. Slikarskim kistom, silikon se nanosi na površinu prsta u nekoliko slojeva. Što je sloj tanji, silikon će se prije osušiti. Nakon nanosa nekoliko slojeva silikona na površinu prsta, te dovoljno dugog vremena sušenja, kalup se laganim pokretima odvoji od prsta te je spreman za daljnje korištenje.



Slika 10 *Silikonski kalupi (grafitni i obični)*
Figure 10 *Silicone matrix (graphite and ordinary)*



Slika 11 *Izrada silikonskih kalupa*
Figure 11 *Production of silicone mold*

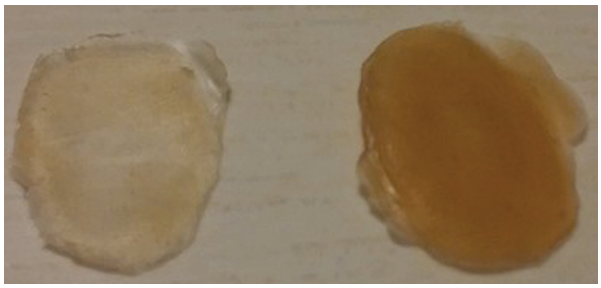
4.2.4 Izrada lažnog silikonskog otiska prsta

4.2.4 *Making of false silicon fingerprint*

Nakon što su pripremljeni kalupi izvornog otiska prsta (negativi), krenulo se sa izradom lažnog silikonskog otiska prsta.

Za izradu lažnog silikonskog otiska prsta korišteni su slijedeći materijali:

- silikon (Kremer Latex Milch, Pattex sanitarni silikon)
- grafit (Kremer Graphit-Schwarzpuder)
- vazelin



Slika 12 *Silikonski otisci prstiju*
Figure 12 *Silicone fingerprint*

Koristeći slikarski kist, kalupi od gline i voska, u tankim slojevima, premažu se sa latex mlijekom. Nakon što se tanki sloj silikona osuši,

nanosi se novi sloj sve do dobivanja dovoljno debelog sloja pogodnog za kvalitetan uzorak otiska prsta. Nakon nekog vremena sušenja, silikon je spreman za odvajanje te je silikonski uzorak prsta spreman za daljnje korištenje.

Slika 13 *Izrada silikonskog otiska prsta u kalupu od voska*

Figure 13 *Production of silicon fingerprint in a mold of wax*

Silikonski kalup, prije dodavanja silikona za izradu otiska prsta, premazuje se sa vazelinom koji služi kao odvajač silikona. Silikon se lijepi na silikon te ne bi bilo dobro da se nepovratno ošteti stečeni silikonski kalup. Nakon što se tanki sloj vazelina na površini silikonskog kalupa osuši, u tankim slojevima se sa slikarskim kistom nanosi latex mlijeko. Nakon što se tanki sloj silikona osuši, nanosi se novi sloj sve do dobivanja dovoljno debelog sloja pogodnog za kvalitetan uzorak otiska prsta. Nakon nekog vremena sušenja, silikon je spreman za odvajanje te je silikonski uzorak prsta spreman za daljnje korištenje.

Ukoliko se silikonski otisak prsta želi testirati na kapacitivnim senzorima, latex mlijeko se, prije premazivanja u kalup, miješa sa grafitom u prahu. Nakon dobrog miješanja, silikon se u tankim slojevima premazuje unutar kalupa te se nakon sušenja dobiva silikonski otisak prsta koji se može koristiti i na kapacitivnim senzorima (npr. mobiteli).

4.3 Stjecanje uzorka izvornog i lažnog otiska prsta

4.3 *Acquisition of the original sample and false fingerprint*

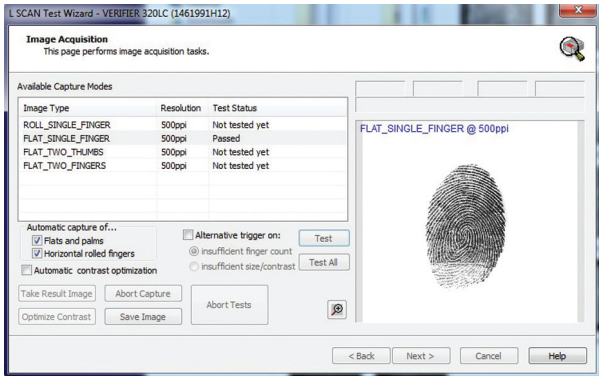
Za stjecanje uzorka izvornog i silikonskog otiska prsta korištena je aplikacija Crossmatch L SCAN koja dolazi sa biometrijskim uređajem Crossmatch Verifier 320 LC.

Otvaranjem aplikacije automatski se aktivira biometrijski uređaj te se prislanjanjem izvornog i silikonskog otiska prsta dobivaju željeni uzorci. Silikonski otisak prsta u pravilu daje nešto lošiji uzorak koji se može poboljšati nakon nekoliko pokušaja te različitih pritiskom silikonskog otiska na senzor.

Crossmatch L SCAN aplikacija stečene uzorke sprema u bmp formatu.

Slika 14 *Crossmatch Verifier 320 LC biometrijski uređaj*

Figure 14 *Crossmatch Verifier 320 LC biometric device*



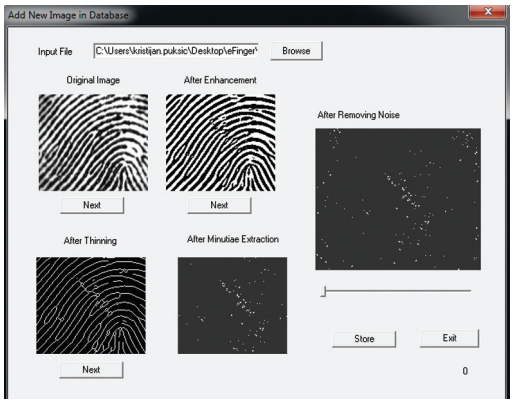
Slika 15 *Crossmatch L SCAN, stjecanje uzoraka otisaka prstiju*

Figure 15 *rossmatch L SCAN, sampling fingerprints*

4.4 Obrada stečenog otiska prsta

4.4 *Processing of the acquired fingerprint*

Nakon što je otisak izvornog i silikonskog prsta stečen, spreman je za daljnju obradu koja se, za prigodu ovog testiranja, vrši putem EFinger aplikacije.



Slika 16 *Obrada uzoraka prstiju, izdvajanje detaljnih točaka*

Figure 16 *Fingers sample processing, detailed points positioning*

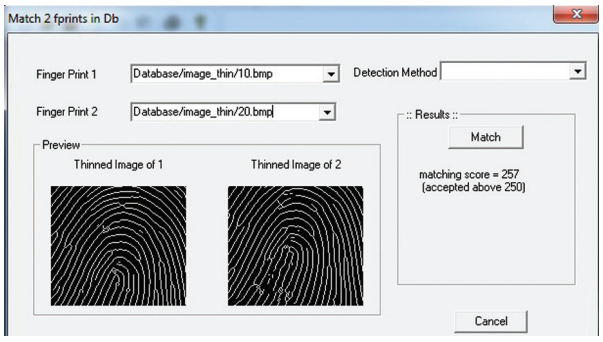
EFinger aplikacija nudi mogućnost unosa novostečenog uzorka otiska prsta u svoju bazu, te detaljnu obradu otiska prsta kao što je poboljšanje kvalitete (micanje šumova), stanjenje brazdi za što lakše izdvajanje detaljnih točaka, te na kraju izdvajanje detaljnih točaka.

4.5 Usporedba izvornog i lažnog otiska prsta

4.5 *A comparison of the original and fake fingerprint*

Usporedba izvornog i silikonskog otiska prsta vrši se preko EFinger aplikacije. Nakon unosa i obrade stečenog otiska prsta, aplikacija nudi mogućnost odabira dvaju uzoraka koja se prema određenoj metodi mogu usporediti.

Ukoliko dobiveni rezultat prelazi granicu od 250, aplikacija smatra da se radi o uzorku iste osobe.



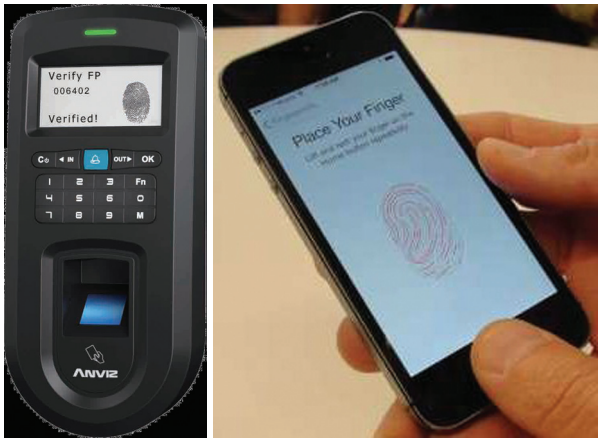
Slika 17 *Proces usporedbe izvornih i silikonskih otisaka prstiju*

Figure 17 *The process of comparing the original and silicone fingerprints*

4.6 Testiranje otpornosti biometrijskih uređaja na lažne silikonske otiske prstiju

4.6 *Stress testing biometric device to fake silicone fingerprints*

Nakon usporedbe izvornog i silikonskog otiska prsta putem EFinger aplikacije, te nakon uspješno dobivenog rezultata usporedbe, napravljeno je testiranje otpornosti biometrijskog sustava. Za testni biometrijski sustav uzet je Anviz VF30 uređaj.



Slika 18 *Anviz VF30 i IPhone 6S uređaj*

Figure 18 *Anviz VF30 and IPhone 6S device*

Na uređaju je prvo registriran izvorni otisak prsta te se nakon toga krenulo sa pokušajem spajanja koristeći silikonski otisak prsta.

Nakon trećega puta, sustav je uspješno prihvatio silikonski otisak prsta kao valjani.

Anviz VF30 uređaj ima osjetljivost FAR 0.00001% i FRR 0.001% što znači da je napravljen poprilično kvalitetan silikonski otisak prsta.

Napravljen je i test sa kapacitivnim senzorom na IPhone 6S mobitelu. Za testiranje je korišten silikonski otisak prsta sa primjesom grafita u prahu.

Prvo je testirana funkcionalnost silikonskog otiska na kapacitivnom ekranu. Test je uspješno prošao te se sa silikonskim grafitnim otiskom moglo upravljati mobitelom.

Nakon toga je napravljena registracija izvornog otiska prsta te pokušaj spajanja na mobitel putem silikonsko grafitnog otiska prsta. Nakon nekoliko pokušaja mobitel je silikonsko grafitni uzorak prepoznao kao valjani.

5. Zaključak

5. *Conclusion*

Glavno pitanje na koje odgovara ovaj rad je koliko su pouzdani biometrijski uređaji za kontrolu pristupa otiskom prsta i koju razinu sigurnosti pružaju krajnjim korisnicima. Rezultati koji su dobiveni kroz izradu silikonskih krivotvorenih otisaka prstiju i kroz njihovo korištenje na biometrijskim uređajima poprilično su razočaravajući. Naime, testiranje je pokazalo da su materijali potrebni za izradu silikonskih krivotvorenih otisaka prstiju dostupni svuda oko nas. Ne postoji nikakva zabrana kupovanja niti nadzor, radi se o materijalu koji se koristi za neograničen broj primjena kao npr. u školama, umjetnosti, kućanstvu. Upute za izradu silikonskih krivotvorenih otisaka također su širom dostupne, pogotovo putem interneta. Detaljno su objašnjeni koraci te razni materijali sa kojima se mogu napraviti isti.

Nakon iznenađujuće lake i brze izrade silikonskog krivotvorenog otiska prsta napravljeno je testiranje na optičkom biometrijskom uređaju za kontrolu pristupa. Biometrijski uređaj je, već nakon trećeg puta, bez ikakvog problema prihvatio krivotvoreni silikonski otisak kao valjani. Napravljeno je testiranje i sa otiscima napravljenima u različitim kalupima (glina, silikon, vosak) i rezultati su relativno isti.

Testiranja su napravljena i na senzorima mobitela najnovijih generacija, sa jednakim rezultatom. Iako senzori na mobitelima koriste drugačiju tehnologiju za prepoznavanje otiska prsta, ukoliko je napadač upoznat sa tehnologijom, dovoljno kvalitetan krivotvoreni otisak prsta može se napraviti bez velikog napora.

Vidljivo je da ovakva razina sigurnosti i tehnologije možda zadovoljava većinu potrošača koji koriste biometriju u potrošačkoj elektronici kao što su mobiteli, miševi, USB memorije i kojima je cilj pamtiti što manje lozinki i PIN-ova, ali za profesionalnu upotrebu, za sigurnost podataka visokog rizika i značaja, za državne i sigurnosne primjene, potrebno je nešto više (korištenje više biometrijskih karakteristika za ovjeru i identifikaciju, ili nasumično odabrani redoslijed prikaza biometrijske karakteristike).

6. Reference

6. References

[1] Anil K. Jain, Arun Ross and Salil Prabhakar; An Introduction to Biometric Recognition, Department of Computer Science and Engineering, Michigan State University

[2] The Biology of Prenatal Development, The Fetal Period, http://www.ehd.org/resources_bpd_illustrated.php?page=3&language=20

[3] Wei-Yun Yau, Zujun Hou, Vutipong Areekul, and Suksan Jirachawengd; Biometrics: From Fiction to Practice Chapter 2: Fingerprint Recognition, Institute for Infocomm Research, A*STAR, Singapore Kasetsart University, Bangkok, Thailand

[4] Anil K. Jain, Arun Ross and Salil Prabhakar; An Introduction to Biometric Recognition, Department of Computer Science and Engineering, Michigan State University, West Virginia University, Salil Prabhakar, Algorithms Research Group, DigitalPersona Inc.

[5] J. Galbally; J. Fierrez; F. Alonso-Fernandez; M. Martinez-Diaz: Evaluation of direct attacks to fingerprint verification systems, Universidad Autonoma de Madrid, EPS, C/Francisco, Tomas y Valiente 11, Madrid,

[6] Mojtaba Sepasian, Cristinel Mares, Wamadeva Balachandran; Liveness and Spoofing in Fingerprint Identification Issues and Challenges, School of Engineering & Design, Brunel University Uxbridge, Moddlesex,

[7] Abdulmonam Omar Alaswad; Ahlal H. Montaser; Fawzia Elhashmi Mohamad; Vulnerabilities of Biometric Authentication "Threats and Countermeasures", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958, © International Research Publications House

[8] Mojtaba Sepasian, Cristinel Mares, Wamadeva Balachandran; Vitality Detection in Fingerprint Identification, School of Engineering & Design, Brunel University Uxbridge, Moddlesex

AUTORI · *AUTHORS*

Marinko Žagar – nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 4, No. 1, 2016.

Korespodencija
marinko.zagar@tvz.hr