Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-610-615

JEDAN METOD FORMIRANJA XOR BIOMETRIJE OTISAKA PRSTIJU GABOROVOM FILTRACIJOM

Srđan Barzut[1], Milan Milosavljević[2]
[1]Tehnikum Taurunum – Visoka inženjerska škola stukovnih studija, Srbija
[2]Univerzitet Singidunum, Srbija

Abstract:
U cilju ostvarivanja visokog nivoa zaštite biometrijskih podataka otisaka prstiju u homomorfnim šifarskim sistemima, od presudne važnosti je transformacija obeležja otisaka prstiju u vektorski opis fiksne dužine. Osim toga, tako generisan metrički prostor mora biti snabdeven Hemingovom metrikom. Uobičajeno je da se ovakav opis biometrijskih karakteristika naziva XOR biometrija. Ovi zahtevi eleminišu sve do sada korišćene sisteme za prepoznavanje otisaka prstiju zasnovanih na minucijama. U ovom radu predložen je jedan sistem generisanja XOR biometrije otisaka prstiju, zasnovan na banci Gaborovih filtara različitih prostornih radijalnih uglova. Rezultujuća binarna reprezentacija fiksne dužine, testirana je u scenariju autentifikacije sa pridruženim mehanizmom izdavajanja asociranih kriptoloških ključeva, zasnovanim na principima kodova za ispravljanje grešaka. Početni eksperimentalni rezultati potvrđuju perspektivnost predloženog pristupa i otvaraju mogućnost daljeg unapređenja performansi.

Key words:
biometrija,
autentifikacija,
biometrijska diskretizacija,
zaštita biometrijskih šablona,
biometrijski kriptosistemi.

UVOD

Otisak prsta je jedinstven za svakog čoveka, zadržava svoje karakteristične detalje vremenom i već dugo ima primenu za autentifikaciju. Najpopularnije i najčešće korišćene tehnike kao osnovu za poređenje otisaka prstiju koriste minucije. Minucije se izdvajaju iz otiska i čuvaju kao skup tačaka u dvodimenzionalnoj ravni $m = \{x, y, \theta\}$ gde (x, y) ukazuju na koordinate tačke, a θ predstavlja ugao minucije. Pre poređenja radi se poravnavanje otisaka koristeći specifične singularne regione. Poređenjem skupa karakterističnih tačaka dva otiska, zapravo radimo poređenje dva otiska.

Globalne informacije o teksturi otiska se koriste prvenstveno za njihovu klasifikaciju. Međutim, tekstura prstiju poseduje informacije o različitim prostornim frekvencijama, različitoj orijentaciji ili fazi, a njenom dekompozicijom u više prostornih frekvencija i orijentacija, može se dobiti potrebna diskriminantnost i za njihovo poređenje. Svaka tačka iz jednog otiska prsta može se povezati sa dominantnom lokalnom orijentacijom i merom koherencije lokalnog toka šare. Ova kvantitativna merenja se posmatraju kao obeležja prilikom poređenja.

Biometrijski šabloni predstavljaju digitalnu reprezentaciju obeležja odgovarajuće biometrijske karakteristike. Da bi odgovorili na sigurnosne izazove, prilikom generisanja i upotrebe šablona, trebalo bi da se zadovolje sledeći uslovi: jednosmernost funkcije kojom se zaštićeni šabloni generišu, uticaj na performanse sistema, opozivost šablona i međusobna nepovezivost zaštićenih šablona generisanih na osnovu istih biometrijskih podataka. Generisanje zaštićenog biometrijskog šablona može se podeliti na osnovu pristupa načinu zaštite na: šifrovanje klasičnim algoritmima, transformisanje karakteristika i biometrijske kriptosisteme. Biometrijski kriptosistemi razvijeni su da zaštite neki kriptografski ključ primenom biometrije ili da na osnovu biometrijskih karakteristika generišu kriptografski ključ. Time istovremeno rešavaju probleme zaštite biometrijskih šablona i upravljanja kriptografskim ključevima. Postoje razvijeni efikasni biometrijski sistemi zasnovani na jednostavnim principima tehnika za korekciju grešaka i XOR logičkih operacija, ali oni zahtevaju binarnu reprezentaciju biometrijskih obeležja fiksne dužine, što predstavlja izazov za postojeće načine izdvajanja obeležja iz nekih biometrijskih karakteristika. U ovom radu predložen je jedan metod formiranja XOR biometrije otisaka prstiju Gaborovom filtracijom.

IZDVAJANJE OBELEŽJA IZ TEKSTURE OTISKA PRSTA

Određivanje referentne tačke

Kada se analizira, otisak prsta poseduje jedan ili više regiona gde papilarne linije formiraju karakteristične oblike. Ovi regioni se nazivaju singulariteti ili singularni regioni i mogu se svrstati u tri tipologije: petlja, delta i spirala. Najbolji izbor za referentnu tačku za predloženi metod je centralna tačka jezgra otiska. Međutim, precizno određivanje te tačke predstavlja veliki izazov i aktuelni je predmet interesovanja naučne javnosti. Zbog navedenih manjkavosti prilikom detekcije svih vrsta singulariteta na osnovu Poinker indeksa i sličnih metoda, u [1] je referentna tačka definisana kao tačka u kojoj papilarna linija ima maksimalnu konkavnu zakrivljenost na jednoj slici otiska prsta. Određivanje takve referentne tačke radi se pomoću definisanja polja orijentacije O za sliku otiska, gde O(i,j) reprezentuje lokalnu orijentaciju papilarne linije u pikselu (i,j) [2]. Zbog kompleksnosti, lokalna orijentacija se određuje na nivou bloka određene veličine, umesto na nivou svakog piksela, pa se ulazna slika I deli u nepreklapajuće blokove veličine w x w. Za svaki piksel se izračunavaju gradijenti ¶x(i,j) i ¶y(i,j), pomoću Sobelovog (engl. Sobel) ili Mar-Hildret (engl. Marr-Hildreth) operatora. Procena lokalne orijentacije O svakog bloka izračunava se u centralnom pikselu svakog bloka. Matematički posmatrano, O predstavlja ortogonalni pravac u odnosu na dominantni pravac Furijeovog spektra svakog prozora. Da bi se ujednačilo, procenjeno polje orijentacije se filtrira niskopropusnim filtrom, a prethodno se slika orijentacije konvertuje u kontinualni vektor polja Φx i Φy. Rezultujući vektor se zatim filtrira:

$$\Phi'_x(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\,\Phi_x(i-uw, j-vw) \quad (1)$$

$$\Phi'_y(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\,\Phi_y(i-uw, j-vw) \quad (2)$$

gde je W dvodimenzionalni niskopropusni filtar, a wΦ x wΦ predstavljaju dimenzije filtra. Na osnovu dobijenih vrednosti zatim se izračunava polje orijentacije O' , kao u

$$O'(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right). \quad (3)$$

Izdvajanjem samo sinusne komponente iz polja orijentacije O', određuje se referentna tačka, izdvajanjem piksela na osnovu intenziteta (maksimalna vrednost), kao u

$$\varepsilon(i,j) = \sin(O'(i,j)) . \quad (4)$$

Izdvajanje referentne tačke u zoni konkavnih papilarnih linija se postiže integraljenjem intenziteta piksela u prethodno empirijski određenim regionima RI i RII i određivanjem njihove međusobne razlike.

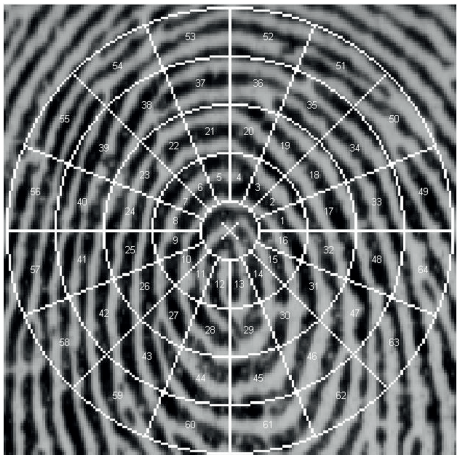
Određivanje regiona od interesa

Na osnovu referentne tačke izdvaja se region od interesa koji se deli na *i* sektora S_i na osnovu parametara: (x_c, y_c) su koordinate referentne tačke, *B* je broj koncentričnih staza oko referentne tačke, *b* je širina svake staze izražena brojem piksela, a *k* je broj sektora u jednoj stazi. Izbor navedenih parametara u određenom biometrijskom sistemu zavisi od rezolucije i veličine slika otisaka prstiju. Širina staze se bira da obuhvati u proseku jedan par ispupčenja i udubljenja u otisku, što za prosečnu sliku rezolucije 500 dpi odgovara širini od 20 piksela (*b=20*). Time se postiže da jedan sektor sadrži lokalne informacije koje obuhvataju npr. jednu minuciju. Izborom veće širine može se javiti suprotan efekat, da lokalne informacije budu modulisane sa globalnim informacijama o otisku prsta. Iz istih razloga, svaka staza se deli na 16 sektora (*k=16*). Unutrašnji krug oko centralne tačke se ne koristi zbog loše koherentnosti. Formiranjem 4 staze sa po 16 sektora u svakoj, dobijamo ukupno 64 sektora, koji se kvantitizuju u 256 različitih vrednosti. Izgled jednog otiska sa određenim ROI podeljenim na sektore, prikazan je na sl. 1.

NORMALIZACIJA I FORMIRANJE BANKE FILTARA

Normalizacija regiona od interesa radi se kako bi se eliminisao šum senzora i efekat deformacije nivoa sive usled različitog pritiska prsta na senzor. Zbog toga, normalizacija se radi na nivou piksela u svakom sektoru zasebno, na konstantnu srednju vrednost i varijansu. Ukoliko bi se normalizacija radila na osnovu srednje vrednosti i varijanse cele slike, ne bi bilo moguće kompenzovati promenljivost intenziteta u različitim regionima slike, nastalih usled elastične osobine prsta. $I(x,y)$ predstavlja nivo intenziteta u pikselu (x,y), M_i i V_i procenjena srednja vrednost i varijansa sektora S_i, M_0 i V_0 su željena srednja vrednost i varijansa respektivno, a $N_i(x,y)$ je nomalizovan nivo intenziteta u pikselu (x,y) na osnovu:

$$N_i(x,y) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 \times (I(x,y)-M_i)^2}{V_i}}, & I(x,y) > M_i \\ M_0 - \sqrt{\dfrac{V_0 \times (I(x,y)-M_i)^2}{V_i}}, & I(x,y) \le M_i \end{cases} \quad (5)$$



Sl. 1. Region od interesa podeljen na sektore

Gaborovi filtri mogu da eliminišu šum i izdvoje strukturu otiska prsta u određenoj orijentaciji unutar slike [3].

Time se postiže da se minucija ističe kao anomalija u lokalnim paralelnim ispupčenjima, a to su informacije koje želimo da izdvojimo pomoću Gabor filtra. U prostornom domenu, simetrični Gaborov filtar ima sledeći opšti oblik:

$$G(x,y;f,\theta)=e^{\left[-\frac{1}{2}\left(\frac{x'^2}{\delta_{x'}^2}+\frac{y'^2}{\delta_{y'}^2}\right)\right]}\cos(2\pi x'f), \quad (6)$$

$$x'=x\sin\theta+y\cos\theta, \quad (7)$$

$$y'=x\cos\theta-y\sin\theta, \quad (8)$$

gde je u našem slučaju f prosečna frekvencija papilarnih linija ($f=1/K$, gde je K prosečno rastojanje između dva ispupčenja), θ ugao u odnosu na x osu, a $\delta_{x'}$ i $\delta_{y'}$ su prostorne konstante Gausove anvelope duž x' i y' ose, respektivno, čije su vrednosti empirijski određene i odgovaraju $K/2$. Normalizovan region od interesa se kovoluira sa osam Gaborovih filtara sa različitim vrednostima ugla θ odnosu na x osu (0°, 22,5°, 45°, 67,5°, 90°, 112,5°, 135° i 157,5°), što je prikazano na sl. 2. Slika otiska kovoluirana filtrom sa uglom od 0°, izdvaja one papilarne linije koje su paralelne sa x osom, a ostali sa odgovarajućim radijalnim pomerajem za primenjeni ugao. Tako se u svakom od osam filtara izdvajaju lokalna obeležja iz slike otiska prsta, a svih osam zajedno sadrže većinu globalnih informacija. Od osam filtriranih slika, formira se vektor obeležja - *FingerCode*.

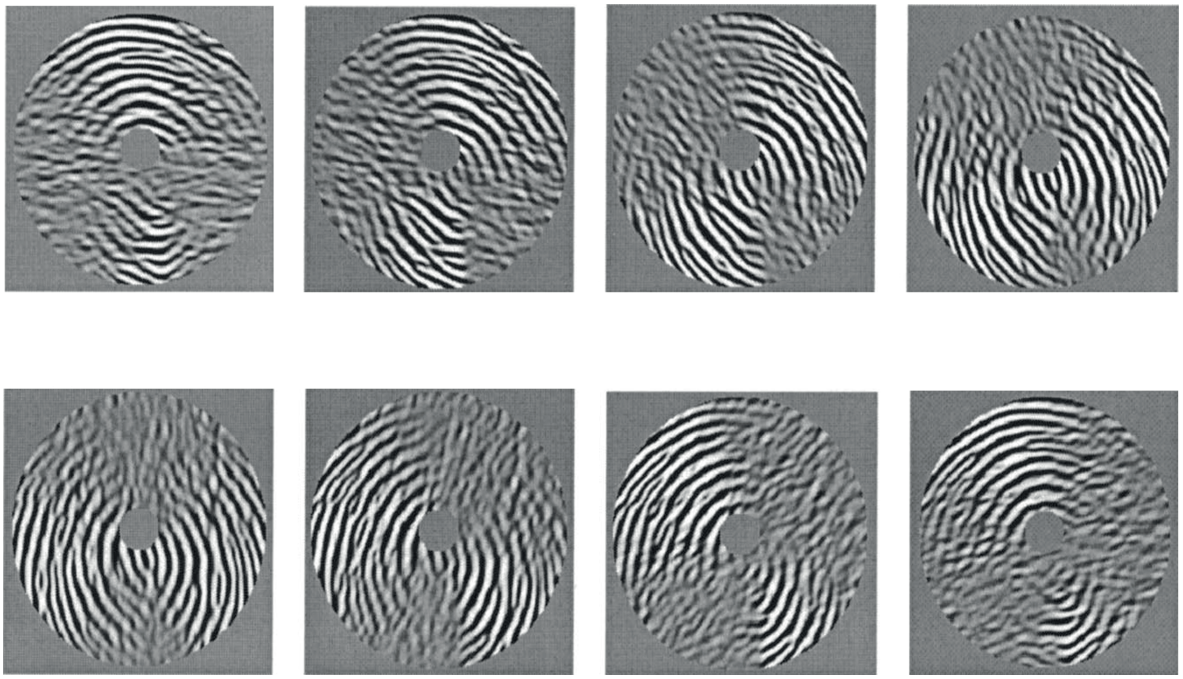
VEKTOR OBELEŽJA

Apsolutna prosečna devijacija (engl. *Avarege absolute deviation* - AAD) svakog sektora u svih osam filtriranih slika određuju komponente vektora obeležja. Intenzitet svakog sektora predstavlja karakterističnu vrednost - obeležje za taj sektor, a skup svih sektora u svih osam filtriranih slika čini vektor obeležja jednog otiska. Ako je $F_{i\theta}(x,y)$ filtrirana slika sa uglom θ za sektor S_i, za svako $i \in\{0,1,2,...,63\}$ i $\theta \in\{0°, 22,5°, 45°, 67,5°, 90°, 112,5°, 135° i 157,5°\}$, vektor obeležja $V_{i\theta}$ je apsolutna prosečna devijacija u odnosu na srednju vrednost, definisana sa:

$$V_{i\theta}=\frac{1}{n_i}\left(\sum_{n_i}\left|F_{i\theta}(x,y)-P_{i\theta}\right|\right), \quad (9)$$

gde je n_i broj piksela u sektoru S_i, a $P_{i\theta}$ je srednja vrednost piksela $F_{i\theta}(x,y)$ u sektoru S_i. Zbog načina izdvajanja regiona od interesa i njegove podele na sektore, zatim filtriranja pomoću osam Gaborovih filtara, vektor obeležja koji se formira ovom metodom ima uvek fiksnu dužinu, što je osobina koja omogućava da se on primeni u biometrijskim kriptosistemima koji rade u binarnom domenu.

Poređenje dva otiska u [1] bazirano je na pronalaženju Euklidovog rastojanja između njihovih odgovarajućih vektora obeležja. Neki od osnovnih problema prilikom poređenja dva otiska prsta su translacija i rotacija otisaka. Translacija otisaka je rešena pomoću referentne tačke koja služi kao centralni orijentir, a u odnosu na koju se ceo postupak generisanja vektora obeležja oslanja. Invarijantnost otisaka usled rotacije je postignuta cikličnim rotacijama obeležja u vektoru obeležja, čime se simulira rotacija otisaka sa korakom 22,5°, odnosno sa uglovima: 0°, 22,5°, 45°, 67,5°, 90°, 112,5°, 135° i 157,5°. Međutim, zbog prirode formiranja sektora, karakteristični detalji otiska prsta invarijantni su samo na male rotacije koje su u opsegu od ±11,25°. Zbog toga, prilikom registracije otiska formiramo još jedan vektor obeležja na osnovu slike otiska koja je rotirana za ugao 11,25° u odnosu na referentnu tačku. Prilikom poređenja registrovanih šablona i priloženog uzorka, poređenje se radi sa svim cikličnim permutacijama, oba vektora obeležja (početnog i rotiranog za ugao od 11,25°), čime je postignuta potpuna invarijantnost na rotaciju. Najmanje Euklidovo rastojanje, od svih permutacija oba vektora obeležja se uzima kao finalni rezultat poređenja.



Sl. 2. Region od interesa konvoluiran sa Gabor

FORMIRANJE XOR BIOMETRIJE OTISAKA PRSTIJU

Biometrijski kriptosistemi zasnovani na otiscima prstiju su u dosadašnjim implementacijama uglavnom bazirani na šemi fazi trezora (engl. *Fuzzy vault*) [6], koja je razvijena kako bi se minucije mogle primeniti u kriptosistemima. Međutim, oslanjanje samo na minucije isključuje ostala obeležja koja se nalaze u bogatoj teksturi otisaka prstiju. Primena teksture otisaka prstiju ima svojih prednosti u biometrijskim sistemima, moguće je izdvojiti više diskriminatornih informacija, nemaju zahtevnu obradu slike za izdvajanje i poređenje minucija, a šabloni koji se izdvajaju su vektori obeležja fiksne dužine. Biometrijski kriptosistemi bazirani na šemi fazi povezivanja (engl. *Fuzzy commitment scheme - FCS*) [5] [7], zasnovani su na jednostavnim principima tehnika za korekciju grešaka i XOR logičkih operacija, ali zahtevaju binarnu reprezentaciju biometrijskih obeležja fiksne dužine, što predstavlja izazov za postojeće načine izdvajanja obeležja iz nekih biometrijskih karakteristika, među kojima se nalaze i otisci prstiju. Uz odgovarajuće procese diskretizacije vektora obeležja, moguće je implementirati jednostavnu šemu fazi povezivanja i primeniti principe XOR biometrije.

Diskretizacija obeležja teksture otiska prsta

Za FCS potrebna je reprezentacija biometrijskih obeležja fiksne dužine i u binarnom obliku. Zbog toga potrebno je uraditi diskretizaciju vektora obeležja, koji se sastoji od realnih brojeva. Kao najjednostavnije rešenje primenjen je princip kvantizacije na osnovu izabrane granične vrednosti, gde se svaki element vektora obeležja koduje sa jednim bitom. S obzirom da je svaki element vektora obeležja V_i {0,1,2,...,255}, na osnovu izabrane granične vrednosti T važi:

$$B_i = \begin{cases} 1, & ako\ je\ V_i > T \\ 0, & ako\ je\ V_i \le T \end{cases}, \tag{10}$$

gde je B_i diskretizovan binarni šablon, a T je izabrana granična vrednost. Graničnu vrednost određujemo kao medijanu skupa elemenata vektora obeležja svakog biometrijskog uzorka i realizujemo je kao dinamičku vrednost koja se određuje prilikom svakog uzorkovanja. U literaturi se mogu pronaći slične realizacije ovog pristupa, gde se za graničnu vrednost koristi empirijski određena fiksna vrednost na osnovu skupa za obučavanje, koja je zajednička za sve otiske prstiju u sistemu ili se prilikom registracije šablona odredi granična vrednost koja je fiksna za taj identitet. Zajedničko za obe metode je da se granična vrednost čuva u bazi podataka kao vid pomoćnih podataka i ta vrednost se prilikom autentifikacije koristi za diskretizaciju uzorka. Eksperimentalno je utvrđeno da predložena dinamička vrednost daje bolje rezultate, s obzirom da se i pored normalizacije slike zadržavaju određene varijacije u otiscima prstiju prilikom uzorkovanja, kao posledica šuma senzora, jačine pritiska i sl. Takođe, eksperimentalno je utvrđeno da se isti rezultati mogu ostvariti računanjem srednje vrednosti elemenata u skupu umesto medijane.

Primenom tehnike za kvantizaciju sa jednim bitom, formiramo binarni šablon dužine koja odgovara broju elemenata vektora obeležja, ali se javljaju gubici na diskriminativnosti. Zbog toga primenili smo unapređenu tehniku za diskretizaciju sa dva bita po elementu vektora obeležja, koja formira četiri opsega za kvantizaciju na osnovu tri granične vrednosti. Prvo se određuje granična vrednost T_2 računanjem medijane kao u prethodnom slučaju. Tako dobijena medijana deli skup elemenata vektora obeležja na dva podskupa, nad kojima se ovaj postupak ponavlja kako bi odredili druge dve granične vrednosti T_1 i T_3, pa za šablon t imamo:

$$(B_i)_t = \begin{cases} 00, & ako\ je\ (V_i)_t \le (T_1)_t \\ 01, & ako\ je\ (T_1)_t < (V_i)_t \le (T_2)_t \\ 10, & ako\ je\ (T_2)_t < (V_i)_t \le (T_3)_t \\ 11, & ako\ je\ (V_i)_t > (T_3)_t \end{cases}. \tag{11}$$

Određivanje pouzdanosti bita

Kako bi poboljšali diskriminativnost binarnih biometrijskih šablona, statističkim tehnikama određujemo pouzdanost svakog bita pomoću obučavajućeg skupa. Obučavajući skup čine svi otisci prstiju koji se koriste prilikom registracije. Na osnovu njih određuje se pouzdanost svakog bita šablona jednog identiteta, a eksperimentalno su testirane različite vrednosti bita koji se odbacuju iz binarnog šablona. Pozicije odbačenih bita čuvaju se u bazi podataka kao pomoćni podaci i ne odaju informacije o samom šablonu. Tehnika za određivanje pouzdanosti bita zasnovana je na Bajesovoj teoremi određivanja aposteriornih verovatnoća i određivanja Bajesove greške sistema [4].

Izbor tehnike za korekciju grešaka

U cilju konstruisanja biometrijskog kriptosistema, potrebno je izabrati odgovrajuću tehniku za korekciju grešaka. Greške koje se javljaju u nekom komunikacionom kanalu, mogu se podeliti na: usnopljene (engl. *burst error*) i greške na nivou bita. U [7] formirana je dvoslojna metoda za korekciju grešaka u kojoj su implementirani Hadamard i Rid-Solomon kôdovi. Greške koje se javljaju na nivou bita ispravljaju se pomoću Hadamard kôdova, dok se za greške u nizu koriste Rid-Solomon kôdovi. Međutim, imajući u vidu argumente iznete u sigurnosnoj analizi ovih tehnika u [8], gde su prikazane ranjivosti ovih tehnika na napade zasnovane na statističkim podacima, u skladu sa preporukama autora izabrana je jedna od tehnika za korekciju grešaka koja radi na nivou celog bloka - BCH kôd.

Bose-Chaudhuri-Hocquenghem kôdovi su ciklične tehnike za korekciju grešaka. Binarni BCH kôd otkrio je 1959. godine *Hocquenghem*, kao i *Bose* i *Chaudhuri* u svom nezavisnom otkriću 1960. godine. Binarni BCH kôd se sastoji od tri parametra *(n,k,t)*, gde je *n* dužina bloka (dužina biometrijskog šablona) i može imati vrednosti definisane sa $n=2^m-1$, *k* je dužina poruke koja se kôduje (dužina tajnog ključa), a *t* je broj bita koji mogu biti ispravljeni.

Predlog biometrijskog kriptosistema

Predloženi biometrijski kriptosistem zasnovan na FCS i otiscima prstiju, inspirisan je istim takvim kriptosistemom predloženom u [7] koji koristi dužicu oka. Koncept predloženog pristupa je prikazan na sl. 3. Na kriptografski ključ *k* se primenjuju tehnike BCH kôda za korekciju grešaka, čime se dobija pseudo-kôd θ_{ps} dužine 511 ili 1023 bita, u zavisnosti od izabranog metoda za diskretizaciju otiska prsta i tehnike uklanjanja nepouzdanih bita. Dobijeni kôd se zatim XOR operacijom kombinuje sa binarnim kôdom otiska prsta iste dužine θ_{ic}, čime se dobija zaštićeni kôd θ_{lock},

$$\theta_{lock} = \theta_p \oplus \theta_c \,. \tag{12}$$

Zaštićeni kôd θ_{lock}, heš vrednost ključa $H(k)$ i pozicije uklonjenih bita iz izvornog šablona R ne otkrivaju informacije o samom ključu i čine pomoćne podatke. Pomoćni podaci su potrebni za ispravnu rekonstrukciju ključa i mogu se čuvati u bazi podataka biometrijskog sistema ili u pametnim karticama. Prilikom rekonstrukcije ključa, zaštićeni kôd se XOR operacijom kombinuje sa priloženim uzorkom kôda otiska prsta θ'_{ic}, čime se dobija pseudo-kôd θ'_{ps},

$$\theta'_p = \theta_{lock} \oplus \theta'_c = \theta_p \oplus \varepsilon \,. \tag{13}$$

Pomoću primenjenih tehnika za korekciju grešaka, dobija se rekonstruisani ključ *k'* čija se validnost proverava poređenjem njegove heš vrednosti sa onom koja se nalazi u pomoćnim podacima.

REZULTATI

U tabeli 1 dati su prijavljeni rezultati u [1] na osnovnom algoritmu koji koristi metriku Euklidovog rastojanja. Za eksperimentalno testiranje predloženog koncepta korišćena je javno dostupna baza otisaka prstiju „FVC2002 DB2B" sa takmičenja dobavljača opreme održanog 2002. godine (engl. *Fingerprint Vendor Competition*). Baza sadrži 800 otisaka prstiju, od čega je po 8 otisaka istog prsta. U tabeli 2 dati su ostvareni rezultati za predloženi XOR biometrijski autentifikacioni sistem sa diskretizacijom na 1 bit po elementu vektora obeležja i sa različitim vrednostima izuzetih nepouzdanih bita *r*, određenih pomoću obučavajućeg skupa od po dva uzorka svakog indentiteta. U tabeli 3 je primenjena diskretizacija sa 2 bita po elementu obeležja, a obučavajući skup čine 3 otiska svakog identiteta.

Tabela 1 - FAR i FRR vrednosti ostvarene u [1]

Granična vrednost	FAR [%]	FRR [%]
30	0,1	19,32
35	1,07	7,87
40	4,59	2,83

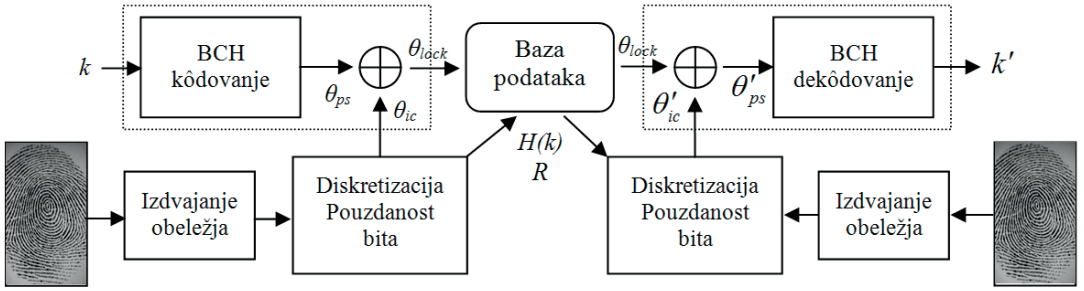
Tabela 2 - FAR i FRR vrednosti ostvarene za šablon dužine 512 bita

	r=0	r=64	r=96	r=128	r=160	r=192
FAR	12,78%	5,74%	3,7%	2,41%	2,78%	3,33%
FRR	5%	6,67%	6,67%	6,67%	5%	5%
FAR	0%					
FRR	25%	25%	21,67%	21,67%	21,67%	21,67%

Tabela 3 - FAR i FRR vrednosti ostvarene za šablon dužine 1024 bita

	r=0	r=64	r=128	r=192	r=256	r=320	r=386
FAR	0,89%	0,67%	0,67%	0,67%	0,67%	1,33%	1,33%
FRR	4%	4%	4%	4%	4%	4%	4%
FAR	0%						
FRR	22%	22%	20%	18%	20%	22%	22%

Prikazani rezultati su ostvareni na kompletoj bazi, odnosno iz nje nisu uklonjeni otisci prstiju koji ne zadovoljavaju osnovne kriterijume za poređenje na osnovu teksture otisaka prstiju (npr. referentna tačka nije na slici ili je blizu ivice slike). U literaturi se uglavnom objavljuju rezultati bez takvih otisaka i oni se ne uzimaju u obzir. U tabeli 4 su prikazani početni rezultati predloženog biometrijskog kriptosistema. Skup za obučavanje koristi se samo za formiranje što bolje reprezentacije u šablonu, primenom pravila većine bita (engl. *Majority vote*) i za sada nema primenu u odstranjivanju nepouzdanih bita, zbog limita koji postoje u ulaznim parametrima izabrane tehnike za ispravljanje grešaka. U BCH kôdu, vrednost *n* je dužina bloka (dužina biometrijskog šablona) i može imati vrednosti definisane sa $n=2^m-1$, pa je za eksperiment izabrana vrednost od 1023 bita. Ni u ovom eksperimentu iz baze otisaka nisu eliminisani otisci koji ne zadovoljavaju kriterijume kvaliteta uzorka.



Sl. 3. Koncept predloženog biometrijskog kriptosistema

Tabela 4 - FAR i FRR ostvarene vrednosti u predloženom biometrijskom kriptosistemu

(n,k,t)	(1023,133,127)	(1023,123,170)
FAR	0%	0%
FRR	20%	3,33%

ZAKLJUČAK

Binarni opis biometrijskih karakteristika i XOR biometrija predstavlja pravac u kojem treba fokusirati buduća istraživanja na ovu temu. Ovi zahtevi eleminišu sve do sada korišćene sisteme za prepoznavanje otisaka prstiju zasnovanih na minucijama, jer iako postoje pionirski predlozi za diskretizaciju minucija u binarni oblik, ta rešenja imaju još mnogo nedostataka i nisu primenljiva. U ovom radu predložen je jedan sistem generisanja XOR biometrije, zasnovan na banci Gaborovih filtara različitih prostornih radijalnih uglova primenjenih na teksturi otisaka prstiju.

Zaštita biometrijskih podataka se realizuje tako što se biometrijske karakteristike čuvaju i obrađuju u obliku digitalnih zaštićenih reprezentacija karakteristika – zaštićenim šablonima. Razvojem tehnika zaštite šablona došlo se do izvesnog sjedinjavanja biometrije i kriptografije u vidu biometrijskih kriptosistema, koji istovremeno rešavaju probleme upravljanja kriptološkim ključevima i zaštite biometrijskih šablona. Time je ostvaren značajan napredak, i u polju biometrije, i u kriptografiji.

Formiranje novog biometrijskog kriptosistema za otiske prstiju baziranog na jednostavnoj šemi fazi povezivanja, u početnoj je fazi istraživanja. Ostvareni rezultati su dobri, zahtevaju dodatnu analizu i unapređenja. Početni eksperimentalni rezultati potvrđuju perspektivnost predloženog pristupa i otvaraju mogućnost daljeg unapređenja performansi.

Multimodalni biometrijski kriptosistemi su izuzetno aktuelna tema istraživanja, što potvrđuje broj radova na tu temu u poslednjih nekoliko godina. S obzirom na značaj ove teme, budući rad će biti usmeren na dalje istraživanje zaštite multimodalnih biometrijskih šablona, kao i na generisanje i upravljanje ključevima u kriptografskim sistemima, na osnovu multimodalne XOR biometrije..

LITERATURA

[1] Jain A., Prabhakar S., Hong L., Pankati S., „Filterbank-Based Fingerprint Matching“, IEEE Transactions on Image Processing, Vol. 9, No. 5, 2000.

[2] Rao A.R., „A Taxonomy for Texture Description and Identification“, Njujork, Springer-Verlag, 1990.

[3] Daugman J.G., “High confidence recognition of persons by a test of statistical independence”, IEEE Trans. Pattern Anal. Machine Intell., vol.15, no. 11, pp. 1148–1161, 1993.

[4] Fukunaga K., Introduction to Statistical Pattern Recognition, 2nd Edition, Academic Press, Indijana, 1990.

[5] Juels A., Wattenberg M., „A fuzzy commitment scheme“, Proceedings of 6th ACM Conference on Computer and Communications Security, str. 28–36, Singapur, 1999.

[6] Juels A., Sudan M., „A fuzzy vault scheme“, Proc. of IEEE International Symp. on Information Theory, 2002.

[7] Hao F., Anderson R., Daugman J., „Combining cryptography with biometrics effectively“, Technical Report 640, University of Cambridge, 2005.

[8] Stoianov A., Kevenaar T.A.M., Van der Veen M., „Security issues of biometric encription“, IEEE International conf. science and technology for humanity, Toronto, 2009.

A METHOD OF FORMING AN XOR BIOMETRICS FROM FINGERPRINTS BY USING GABOR FILTRATION

Abstract:
In order to achieve a high level protection of biometrics data from fingerprints in homomorphic cryptosystems, crucial importance is fingerprint feature transformation in vectorial description of a fixed length. In addition, generated metric space must be provided with Hemmings metrics. It is common to name this description of biometric features XOR biometrics. These requirements eliminate all systems now used for fingerprint identification based on minutiae. In this paper, we propose a system to generate an XOR biometrics of fingerprints, based on filterbank of Gabor filters of different spatial radial angles. The resulting binary representation with fixed length was tested in a authentication scenario with associated mechanism for extraction of associated cryptology keys, based on the principles of error correcting codes. Initial experimental results confirm the perspective of the proposed approach, and open the possibility of further performance improvement.

Key words:
Biometrics,
Authentication,
Biometric discretization,
Biometric Template Security,
Biometric Cryptosystems.