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-2014-984-989

KOMBINOVANJE BIOMETRIJE I LOZINKI U SAVREMENIM SERVISIMA AUTENTIFIKACIJE

Marko Marjanović

Abstract:
U radu se bavimo razvojem bezbednih sistema za autentifikaciju zbog velike potrebe koja postoji u aplikacijama savremenih poslovnih okruženja. Obzirom na razvoj i potencijal biometrijskih podataka, naša ideja u radu je da ostvarimo vezu između biometrije otiska prsta i tradicionalnih lozinki. Na ovaj način servis autentifikacije obezbeđuje dvo-faktorsku šemu koja je zasnovana na nečemu što jesmo i nečemu što znamo. Naša predložena šema sadržaće detaljno objašnjenje o načinu kombinovanja ova dva faktora preko kojih se obezbeđuje bezbedna autentifikacija. Zanemarujući osvedočene performanse biometrijskog sistema za prepoznavanje, uticaćemo na parametre transformacione funkcije za genrisanje biometrijskog obrasca koji će posedovati odgovarajuće informacione osobine za potrebe autentifikacije. Dobijanje dobre informacione vrednosti tako generisanog materijala nam omogućava generisanje kriptoloških ključeva visoke entropije. Evaluacija sistema biće izvršena na osnovu podignutog eksperimentalnog rešenja koje je zasnovano na Matlab programskom paketu i "CASIA" biometrijskoj bazi podataka.

Key words:
otisak prsta,
lozinka; autentifikacija,
kriptološki ključ.

UVOD

Dobro je poznato da su neke osobine ljudskog tela kao što su otisak prsta, DNK, iris, karakteristične za svaku osobu. Upravo nam te činjenice govore da je potrebno iskoristiti prednosti koje nam pruža biometrija. Kako je poznato da svaki sistem ima svoje mane tako je moguće poboljšanje sistema autentifikacije koji su zasnovani na biomterijskim uzorcima. U radu će biti objašnjeno na koji način je moguće ostvariti vezu između biometrije otiska prsta i tradicionalnih lozinki. Materijal koji je dobijen kombinacijom biometrije i lozinke će biti iskorišćen za generisanje kriptoloških ključeva koji mogu biti korišćenih u sistemima za bezbednost podataka. Evoluacija sistema biće izvršena na osnovu podignutog eksperimentalnog rešenja koje je zanovano na Matlab programskom kodu. Uticaćemo na parametre transformacione funkcije za generisanje biometrijskog obrasca koji će zadržati odgovarajuće informacione osobine za potrebe autentifikacije. Biometrijski uzorci otiska prsta koje ćemo koristiti su preuzeti sa CASIA baze biometrijskih uzoraka.

PREGLED U OBLASTI ISTRAŽIVANJA

Tokom istraživanja trenutnog stanja u oblasti generisanja ključa na osnovu biometrije kao i dvo-faktorske autentifikacije došli smo do nekoliko radova koji se bave pomenutim temama.

Bio-hešing: Dvo-faktorska autentifikacija spajanjem podataka otiska prsta i nasumičnog broja dobijenog iz tokena

U radu je opisan metod spajanja dva načina autentifikacije, otiska prsta i slučajnog broja dobijenog iz tokena. Uz pomoć novog pristupa dobija se jedinstven kompaktan kod za svaku osobu. Direktnim kombinovanjem odnosno množenjem pseudo-slučajnog broja i biometriskih podataka dobijenim uz pomoć Fourier-Melin transformacije (FMT) predstavlja veoma pouzdan mehanizam koji pruža visok nivo pouzdanosti. [1]

Predlog šifarskog sistema zasnovanog na biometrijskom ključu

U predloženom sistemu ulaz u biometrijsku fazu predstavlja slika otiska prsta koja se dobija uz pomoć skenera otisaka prstiju. Kroz ovu fazu neke jedinstvene karakteristike otiska prsta se izdvajaju da bi se formirala biometrisjka matrična funkcija. Tako formirana matrica se koristi kao ulaz za sledeću fazu u kojoj se generiše 128-bitni ključ koristeći jednu od šifarskih heš funkcija kao što je Secure Hash Algorithm (SHA-1) ili Message-Digest algorithm 5 (MD5). Otvoreni tekst se zatim šifruje generisanim ključem i jednim od algoritama za šifrovanje kao što je AES. [2]

Generisanje biometrijsog ključa za korišćenje u DES-u

Predloženi metod uzima ulaznu JPEG/JPG sliku a na izlazu daje 64-bitni ključ. Tako generisani ključ predstavlja ulaz u paritetnu drop tabelu DES generatora ključa. Ceo fokus rada je usmeren na drugi blok tj. generisanje 64-bitnog ključa od ulazne slike. Zatim se 64-bitni blok ključ generatora deli na podblokove predstavljajući u detalje način funkcionisanja blokova. Ulazna JPEG/JPG slika se prebacuje u binarnu sliku sa dva nivoa interesa. Crni pikseli predstavljaju grebene a beli predstavljaju doline i takva slika može da se koristi za dobijanje minucija putem algoritma. Siva slika se prebacuje u binarnu nakon čega se dobija poboljšani kontrast. U procesu istanjivanja smanjuje se debljina otiska grebena na jedan piksel. Zatim sledi faza obeležavanja minucija preko metoda 3x3 prozora. Nakon toga se odklanjaju lažne minucije. Kod završnog procesa set originalnih minucija se rekurzivno smanjuje dok se ne dobije 64-bitni ključ. [3]

TEORIJSKE OSNOVE ISTRAŽIVANJA

Biometrija (grč. bios-život, metron-mera) predstavlja skup automatizovanih metoda za jedinstveno prepoznavanje ljudi bazirano na jednoj ili većem broju njihovih fizičkih karakteristika.

Biološke mere moraju da zadovolje sledeće uslove da bi se kvalifikovale kao biometrijske a to su:

- Univerzalnost – svaka osoba mora posedovati ovu karakteristiku.
- Jedinstvenost – karakteristika se mora razlikovati od pojedinca do pojedinca.
- Nepromenljivost – karakteristika se ne sme menjati vremenom kao ni pri različitim uslovima prikupljanja.
- Kolektabilnost – karakteristika mora biti prikupljiva i kvantitativno merljiva. [4]

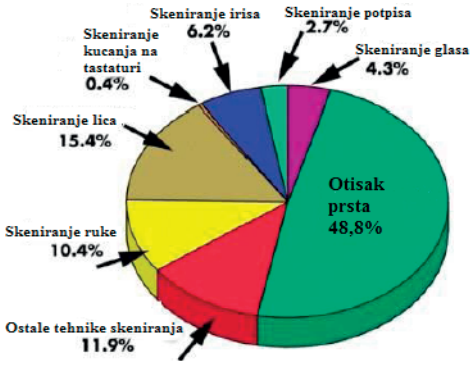
Najčešće korišćeni biometrijski sistemi

U biometrijskim identifikacionim sistemima prepoznavanje korisnika vrši se na osnovu njegovih fizičkih i/ili karakteristika ponašanja. Biometrijski sistemi se, shodno tome, mogu podeliti u dve osnovne kategorije i to:

- Sistemi zasnovani na prepoznavanju fizičkih karakteristika (otisak prsta, prepoznavanje lica, skeniranje irisa...).
- Sistemi zasnovani na prepoznavanju karakteristika ponašanja (prepoznavanje glasa, potpis, način hodanja...).

Na sledećem grafičkom prikazu možemo videti u kom procentualnom odnosu se koriste različite biometrijske tehnike.

Najčešće korišena biometrijska tehnika u sistemima autentifikacije je dakle otisak prsta. Ovaj podatak nam govori da već imamo razvijenu infrastrukturu (čitači otisaka prstiju) tako da početna pozicija ove biometrijske tehnike daleko ispred drugih. [5]



Sl.1. Odnos biometrijskih tehnika u praksi.

Otisak prsta

Grana biometrije koja se bavi proučavanjem otisaka prstiju se naziva daktiloskopija. Prema njoj otisak prsta predstavlja konfiguraciju ispupčenja i udubljenja. Ispupčenja se drugačije nazivaju i papilarne linije. Ove linije se pojavljuju još u vreme embrionog razvoja čoveka (6-7 nedelja) a u potpunosti se formiraju do 21. nedelje. Papilarne linije se razlikuju i kod jednojajčanih blizanaca.

Otiske prstiju možemo klasifikovati prema njihovim fizičkim karakteristikama odnosno prema obliku i pravcu kretanja papilarnih linija. Prema toj raspodeli postoji sedam osnovnih tipova otisaka prstiju: luk, jeloviti luk, petlja, dvostruka petlja, jamičasta petlja, spirala i mešoviti.

Sl.2. Tipovi otisaka prstiju.

Nisu svi tipovi otisaka prstiju podjednako zastupljeni. Petljasti tipovi čine najveći procenat od oko 60%, spiralni tip 30%, lučni tipovi i mešoviti tipovi po 5%. Pored ovih osnovnih karakteristika otisci prstiju poseduju i singularne tačke koje su veoma bitne za prepoznavanje i razlikovanje. Kod ovih tačaka dolazi do nagle promene usmerenosti papilarnih linija. Na slici ispod su prikazane singularne tačke.

SL. 3. Singularne tačke

Verifikacija otiska odnosno svrstavanje u određeni tip se vrši uz pomoć globalnih karakteristika dok se identifikacija vrši na osnovu lokalnih odnosno detaljnih karakteristika. Te detaljne karakteristike se naizivaju minucije. Iako iz otiska prsta možemo izvući skoro 100 minucija uglavnom je dovoljno ne manje od 10-12 minucija za pozitivnu identifikaciju. Imamo nekoliko osobina papilarnih linija koje ih čine pogodnim i sigurnim pri identifikaciji. Prva od tih osobina je nepromenljivost broja i rasporeda mincija. Ne može se svojevoljno izmeniti izgled papilrnih linija jedino se mogu trajno oštetiti. Druga bitna osobina je neponovljivost. Poznati francuski matematičar Baltasar je dokazao da je verovatnoća da se podudaraju dva otiska praktično jednaka 0. Poslednja od veoma bitnih osobina je grupisanje. Ova osobina omogućava klasifikaciju na osnovu opštih sličnosti što znatno smanjuje vreme potrebno za identifikaciju. [6]

Minucije predstavljaju karakteristične tačke na otisku prsta svakog pojedinca. Na osnovu tih tačaka se vrši prepoznavanje. Proces izdvajanja minucija iz slike otiska prsta možemo podeliti u tri faze: predobrada, izdvajanje minucija, završna obrada. Faza izdvajanja minucija ima dva procesa od kojih se prvo vrši stanjivanje otiska grebena na debljinu koja je pogodna za dalju obradu a nakon toga se obeležavaju minucije. Završna obrada slike otiska prsta predstavlja uklanjanje lažnih minucija da bi nakon te faze dobili prave karakteristične tačke nekog otiska prsta.

Kriptološko-teorijska osnova

Kriptologija je nauka o zaštiti podataka. Dugo je ova nauka bila primenljiva samo u profesionalnim sistemima koji su imali potrebu za ovakvim vidom zaštite (vojska, policija, bezbednosne agencije). Kako živimo u informacionom društvu gde svakodnevno nailazimo na veliku količinu informacija nameće se potreba da sačuvamo integritet tih podataka. Upravo ovakva situacija doprinosi ubrzanom razvoju kriptoloških mehanizama kao i razvoju načina izučavanja kriptologije.

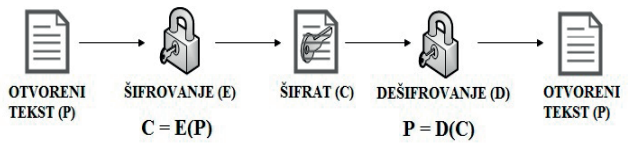
Lozinka je unapred dogovoreni tajni signal koji se koristi kao metod raspoznavanja. U prošlosti su lozinke uglavnom bile reči koje je potrebno izgovoriti da bi ste nekom dokazali da ste vi ona osoba koja se očekuje. U današnje vreme susrećemo se sa mnogim servisima koji zahtevaju da potvrdimo naš identitet nizom karaktera koji predstavlja lozinku. Idealna lozinka bi bila nešto što znamo, računar može to da potvrdi a niko drugi ne može da pogodi. U praksi ovakav scenario je skoro nemoguće postići. Da bi lozinka bila sigurna potrebno je zapamtiti a ne čuvati zapisanu. Međutim pamćenje kompleksnih lozinki nije ni malo lako tako da ljudi obično biraju manje kompleksne a samim tim i manje sigurne lozinke. Još jedan od problema predstavlja i potreba za korišćenjem više lozinki za raličite sisteme što nas ponovo usmerava na korišćenje i pamćenje slabijih lozinki. Sistemi koji su zaštićeni samo prostom lozinkom u današnje vreme su veoma ranjivi tako da se koriste viši nivoi zaštite tj. kriptološki ključevi.

Kriptološki kluč predstavlja informacioni parametar koji određuje izlaz kriptološkog algoritma odnosno na osnovu njega otvoreni tekst prelazi u šifrat. Način dobijanja ključa je veoma bitan zato što jačina ključa određuje sigurnost kompletnog šifarskog sistema. Da bi ključ bio siguran potrebno je da bude generisan iz slučajnog niza podataka. Apsolutnu slučajnost je teško postići i njena mera se predstavlja entropijom. Izvore slučajnosti moguće je postići softverski analizirajući slučajne događaje kao što su: kretanje miša, šum elektronskih komponenti, aktivnost procesora. Međutim, izvori ovakvih aktivnosti su ipak ograničeni. Generisanje ključeva iz prirode kao što je atmosferski šum, radioaktivni raspad daju mnogo bolje rezulate ali ih je teško meriti. Najpraktičnije rešenje za generisanje kritoloških ključeva nam daje sopstvena biometrija. Nikad nije moguće zabeležiti isti biometrijski otisak što nam daje mogućnost da na osnovu npr. jednog prsta generišemo veliki broj ključeva.

Šifarske sisteme možemo razlikovati po tome da li se isti ključ koristi za šifrovanje i dešifrovanje ili je u pitanju asimetrična kriptografija gde se koriste javni i tajni ključevi.

Simetrični šifarski sistemi predstavljaju sisteme šifrovanja tajnim ključem pri čemu je ključ za šifrovanje identičan ključu za dešifrovanje. Karakterišu se relativno velikom brzinom rada i jednostavnom implementacijom.

Kod šifrovanja poruke upotrebom simetričnih sistema, tajnost i autentičnost poruke zasnivaju se na autentičnosti ključa, a sistem je bezbedniji ukoliko se ključ generiše na što slučajniji način.



SL.4. Proces šifrovanja i dešifrovanja u simetričnim šifarskim sistemima

Advanced Encryption Standard (AES) je najrasprostranjenija simetrična šifra. Iako se izraz „Standard" odnosi samo na Vladu SAD-a, AES je obavezan za upotrebu i u raznim industrijskim standardima, a takođe se koristi i u komercijalne svrhe. U komercijalne standarde koji koriste AES spadaju standard za Internet sigurnost IPsec, TLC, standard za šifrovanje Wi-Fi komunikacije IEEE 802.11i, SSH (Secure Shell) mrežni protokol, Internet komunikacija preko Skype-a i razni drugi sigurnosni proizvodi. Razvijen krajem 1990-tih godina od strane NIST-a i zasnovan je na Rindael algoritmu.

AES je kao i DES, blokovska šifra sa simetričnim ključem standardizovana od strane NIST-a. Za razliku od DES-a, nije Fejstel šifra. Glavna posledica toga je da AES operacije moraju biti povratne da bi se nešto moglo dešifrovati. Takođe, za razliku od DES-a, AES algoritam ima komplikovanu matematičku strukturu.

Otporan na poznate napade, veoma je brz, moguć je paralelni dizajn, kao i implementacija na mnogim procesorima i pametnim karticama. Do danas nisu uočeni bolji napadi od brute-force napada na AES.

Funkcionalni parametrima AES-a su:

- Dužina bloka otvorenog teksta je 128, 192 i 256 bitova.
- Dužine ključa su 128, 192 i 256 bitova.
- Ima ukupno od 10 do 14 rundi, zavisno od dužine ključa.
- U svakoj rundi koriste se 4 funkcije:
  - Nelinearan sloj (ByteSub)
  - Sloj linearnog mešanja (ShiftRow)
  - Nelinearni sloj (MixColumns)
  - Dodatni sloj ključa (AddRoundKey).

Značajnu ulogu u svim kriptološkim sistemima imaju i heš funkcije. Heš funkcija predstavlja sumu poruke. Problem nastaje kada se iz različitih poruka dobija ista heš vrednost odnosno ista suma. Kriptografski cilj je da jedan heš odgovara samo jednoj poruci. Heš se koristi za proveru integriteta dobijene poruke. Izmena samo jednog znaka u poruci daje različitu heš vrednost. Dakle ako bi napadač promenio sadržaj presretnute poruke primalac bi mogao to da zna ako poznaje heš vrednost poruke pre slanja. Heš funkcije se ne koriste za šifrovanje. Njihova oblast primene se svodi na integritet prenesenih podataka, autentifikaciju učesnika u komunikaciji, neporecivost transakcija i sl. Suština heš funcija je u jednosmernosti koja predstavlja posledicu kompresije sa gubicima. Dužina heš vrednosti je kostantna za izbranu heš funkciju i ne zavisi od dužine otvorenog teksta dok je dužina šifrata uglavnom približna dužini otvorenog teksta. Takođe, ukoliko poznajemo ključ možemo izvršiti dešifrovanje dok iz heš vrednosti nije moguće dobiti poruku jer ne postoji inverzna funkcija. Najpoznatije heš funkcije su MD5, SHA i RIPEMD koje pripadaju MD4 grupi. [7]

Teorijsko-informaciona analiza

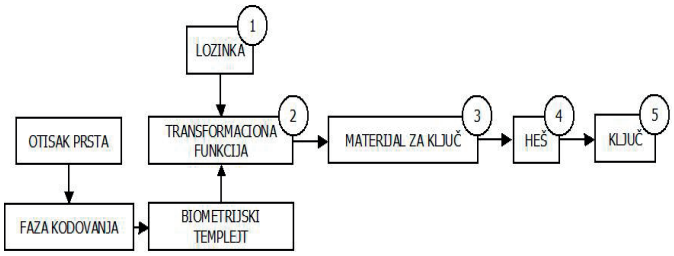
Entropija predstavlja meru neodređenosti pridruženu slučajnoj promenljivoj. Entropiju u teoriji informacija prvi je uveo Klod Šenon i ona predstavlja očekivanu vrednost informacije sadržane u poruci. Koncept je Klod Šenon prikazao u svom čuvenom radu iz 1948. godine „Matematička teorija komunikacija".

Šenonova entropija predstavlja apsolutnu granicu najbolje moguće kompresije bez gubitka bilo kakve komunikacije pod izvesnim ograničenjima: ako tretiramo poruke da su kodovane kao niz nezavisnih slučajnih promenljivih sa istom raspodelom, prva Šenonova teorema pokazuje da u graničnom slučaju, srednja dužina najkraće moguće reprezentacije za kodovanje poruka u datom alfabetu je njihova entropija podeljena sa logaritmom broja simbola u ciljanom alfabetu.

Koriteći entropiju možemo izvršti informacionu analizu dobijenih rezultata u radu. Uz pomoć NIST-ovog paketa testova koji su statistički paket koji se sastoji od 15 testova, možemo ispitati slučajnosti binarne sekvence koje proizvode hardver ili softver na bazi kriptografski slučajnih ili pseudoslučajnih brojeva. Ovi testovi se fokusiraju na različite vrste neslučajnosti koje bi mogle da postoje u nizu. [7]

PREGLED PREDLOŽENOG REŠENJA

Dvofaktorska autentifikacija kao metod poboljšanja klasične autentifikacije predstavlja predmet istraživanja ovog rada. Kombinovanjem biometrije otiska prsta i lozinke dolazimo do ključa koji se može koristiti u servisima autentifikacije. Na generičkoj šemi može se videti raspored procesa koje je potrebno sprovesti da bi smo došli do ključa.



Sl.5. Generička šema sistema.

Lozinka

Generisanje ključa iz biometrije unapređuje klasične sisteme autentifikacije iz razloga što uvodi neodređenost u fazi kreiranja ključa. Da bi smo uspeli da formiramo ključ koji ima dobra svojstva što se tiče neodređenosti odnosno entropije uvodimo lozinku kao dodatni parametar. Kod predloženog rešenja lozinka predstavlja jednu vrstu inicijalizacionog vektora. Dakle, sada imamo sistem koji se oslanja na dva faktora a to je biometrija i lozinka.

Transformaciona funkcija

Transformacija se postiže korišćenjem funkcije randintrlv u programoskom okruženju Matlab, kojom se elementi binarnog podatka dobijenog iz biometrije otiska prsta premeštaju nasumičnom permutacijom. Inicijalizacioni parametar za generator nasumičnih brojeva je u ovom slučaju naša lozinka koja određuje način permutacije elemenata. Funkcija je predvidiva i invertibilna za dato stanje iz razloga što se svaki put kada se pokreće Matlab eksperimentalno okruženje generator brojeva se takođe vraća na isto početno stanje ali svaka izmena inicijalizacionog parametra odnosno lozinke daje novu preraspodelu elemenata i uvodi neodređenost u načinu generisanja slučajnih brojeva odnosno u permutaciji elemenata biometrijskog templejta. Ovim smo postigli željeni efekat da i ako biometrija bude kompromitovana ne postoji način da se formira ključ bez poznavanja lozinke. Takođe, prilikom uzimanja otiska prsta nikada se ne može dobiti isti biometrijski templejt tako da je ulaz u transformacionu funkciju uvek drugačiji samim tim ključ je jako teško podvrgnuti uspešnoj kriptoanalizi.

Materijal za ključ

Nakon primene transformacione funkcije na biometrijski templejt dobijen iz slike otiska prsta dobijamo binarni niz koji predstavlja permutaciju elemenata binarnog niza biometrijskog templejta a to je predposlednji korak za dobijanje ključa.

Heš

Materijal za ključ koji smo dobili ne koristimo u otvorenoj formi već se koristi heš otisak.

PERFORMANSE PREDLOŽENOG REŠENJA

Jaka informaciona analiza dobijenog binarnog niza je od velike važnosti iz razloga što postavlja teorijske okvire za generisanje kvalitetnog kriptološkog ključa. Performanse predloženog rešenja ćemo iskazati korišćenjem aplikacije preko koje ćemo testirati dobijeni materijal. Korišćenjem Šenonove entropije dolazimo do prosečne količine informacija koje su sadržane u našem uzorku iz koga dobijamo ključ. Uzorak je potrebno analizirati i sa aspekta njegove uniformne distribucije.

Dobijeni uzorak ćemo podvrgnuti testovima za procenu informacionog sadržaja on kojih su za nas najvažniji :

- Frekvencijski test.
- Serijski test.
- Entopijski test.

Frekvecijski test predstavlja test učestalosti bitova u binarnom nizu. Dobar binarni niz ima približan broj nula i jedinica.

TABELA 1. FREKVENCIJSKI TEST

Frekvecijski test	Broj bitova
Vrednost bita (0)	3202
Vrednost bita (1)	4106

Serijskim testom ispitujemo koliki broj parova se nalazi u nizu. Približan broj sve četiri grupe parova u našem uzorku prikazuje da je dobijeni rezultat dobar.

TABELA 2. SERIJSKI TEST

Serijski test	Broj parova
Par (00)	1368
Par (01)	1833
Par (10)	1834
Par (11)	2272

Entropija predstavlja meru neodređenosti nekog niza odnosno prosečnu količinu informacije sadržane u nizu. Kako se ovde radi o binarnom nizu jedinica informacije je 1 bit. Dakle maksimalna entropija po jednom bitu bi iznosila 1 tako da reuzlat prikazan u tabeli nam prikazuje da je dobijena vrednost približna maksimalnoj entropiji- Dajte brojeve fusnotama odvojeno kao eksponente „superscripts“. Postavite konkretnu fusnotu na dno kolone u kojoj je citirana. Ne stavljajte fusnote u listu referenci. Koristite slova za fusnote u tabelama.

TABELA 3.ENTROPIJSKI TEST

Entrpopijski test	Vrednost
Monobit	0.9889
Bigram	0.9887
Trigram	0.9884
Matrice 4x4	0.9885

Uzorak koji smo testirali predstavlja binarni niz koji sadrži 7308 bita. Količina informacije koju smo dobili entropijskim testom po jednom bitu iznosi prosečno 0.988 tako da možemo dobiti količinu informacija koju sadrži niz ako pomnožimo broj bitova sa količinom informacije koju nose.

Količuna informacije niza = 7308 x 0.988 = 7220,3.

Testirali smo više dobijenih uzoraka i dobijeni rezultati entropiskog test su skoro identični prethodno navedenom (Entropija = 0.998). Dakle svi su približno maksimalnoj vrednosti entropije. Ukupna količina informacije koju je moguće iskoristiti za generisanje kriptološkog ključa je po jednom otisku u proseku 4335 bitova. Ovo je rezultat koji je dobijen nakon računanja zajedničke informacije. Tačnije, ovaj broj bitova predstavlja teorijski okvir.

Kako smo dobili teorijki okvir dužine dobijenog materijala veći od 1024 bita treba napomenuti da se nad ovim materijalom može dobiti heš vrednost velikih dužina što daje dodatnu vrednost predloženog sistema. Može se koristiti heš algoritam SHA-512 koji na izlazu daje heš vrednost dužine 512 bitova. Algoritam koristi 80 rundi za kompresovanje sa gubicima da bi došao do heš vrednosti. Za predloženi heš algoritam trenutno nije poznato da postoje kolizije.

ZAKLJUČAK

Razvoj servisa autentifikacije kao prevashodni cilj ovog rada je ostvaren na osnovu sistema koji nam omogućava generisanje kriptoloških ključeva korišćenjem dvo-faktorske šeme. Kombinacijom nečega što imamo (biometrija otiska prsta) i nečega što znamo (lozinka) poboljšavamo bezbednost autentifikacionih procesa koji su široko rasprostranjeni u komunikaciji na Internetu.

Prilagođena funkcija interliver koja ima široku primenu u komunikacijama nam je omogućila transformacionu funkciju koja koristi lozinku kao inicijalni parametar za permutaciju podataka dobijenih iz biometrije otiska prsta. Tako dobijeni materijal nam je omogućio generisanje ključeva velikih dužina, ali sa jasno postavljenim okvirima preko teorijsko informacione analize.

Razvijeni sistem nam omogućava generisanje više ključeva na osnovu originalnog biometrijskog templejta. Takođe, sistem ne čuva originalnu biometriju u bazi podataka već čuva heš vrednost tako da ne može doći do kompromitovanja biometrijskog uzorka. Dakle, ne postoji referentni podatak na osnovu koga napadač može da otkrije originalnu biometriju ili ključ.

Nad dobijenim ključevima je izvršena informaciona analiza koja nam je omogućila postavljanje teorijskih okvira.

Poboljšanje performansi predloženog rešenja je moguće postići upotrebom multimodalne biometrije. Spajanje više biometrijskih uzoraka u cilju razvijanja sistema autentifikacije predstavlja polaznu tačku za budući rad. Teorijsko-informaciona analiza biometrijskih uzoraka će nam omogućiti uvođenje novina u sisteme generisanja kripto-

loških ključeva korišćenjem multimodalne biometrije. Takvom analizom smo u mogućnosti da procenimo kolika je informaciona vrednost određenih delova biometrijskih uzoraka kao i procena njihove zajedničke informacije koja je idealna za generisanje ključeva.

LITERATURA

[1] Andrew Teoh Beng Jin, David Ngo Chek Ling and Alwyn Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition 37 2245-2255, 2004.

[2] K. Hassanain, M. Shaarawy, E. Hesham, "A proposal for a biometric key dependent cryptosystem", Vol 10, No 11, Global Jurnal of Computer Science, 2010.

[3] Rupam Kumar Sharma, Assam India, "Generation of biometric key for use in DES", International Jurnal of Computer Science Issues, Vol. 9, Issuse 6, No 1, ISSN(Online) : 1694-0814, 2012.

[4] Brankica Popović, Miodrag Popović, "Biometrijski sistemi – upotreba i zloupotreba, Singipedia Naučno-istraživački portal, 2010.

[5] Radovan Skendžić, "Savremeni trendovi u multimodalnoj biometriji", Singipedia Naučno-istraživački portal, 2011.

[6] Miloš Tripunović, "Otisak prsta – biometrijski sistemi", Infoteh-Jahorina Vol. 6, Ref. E-III-15, p 460-463, 2007.

[7] Mladen Veinović, Saša Adamović, "Kriptologija 1 – Osnove za analizu i sintezu šifarskih sistema", [Knjiga] – Beograd: Univerzitet Singidunum, 2013.

COMBINING BIOMETRICS AND PASSWORDS IN THE MODERN AUTHENTICATION SERVICE

Abstract:
This paper is the development of secure authentication systems due to the great need that exists in the application of modern business environment. Considering the development potential of the biometric data, our idea in this paper is to establish a link between fingerprint biometrics and traditional passwords. In this way the authentication service provides two-factor scheme that is based on something we are and something we know. Our proposed scheme will include a detailed explanation of how to combine these two factors over which provides secure authentication. Ignoring the demonstrated performance of biometric recognition system, we will impact parameter transformation functions for generating biometric pattern that will have the appropriate information for the authentication features. Getting appropriate informations from that kind of material we are able to generate crypto key with high entropy. Evaluation of the system will be made on the basis of experimental jacked solution is based on the Matlab software package and "CASIA" biometric database.

Key words:
fingerprint,
password,
autentification,
crypto key.