



Doc dr Vojkan Vasković*

UDK 336.71:57.087

PRIMENA BIOMETRIJSKIH METODA IDENTIFIKACIJE U BANKAMA

Razvojem računarske tehnike krajem 20 i početkom 21 veka, mogućnosti biometrijske identifikacije dobijaju kako na kvalitetu i brzini tako i na raznovrsnosti primenjenih tehnologija.

Biometrijske metode prepoznavanja se ubrzano šire i uvode u sektor bankarstva i finansija. Primenjuju se u sistemima zaštite ali sve više i u sistemima plaćanja. Predviđanja su da će ove metode sve češće da se primenjuju i da će njihova upotreba biti sve univerzalnija.

* Beogradski univerzitet TF Bor

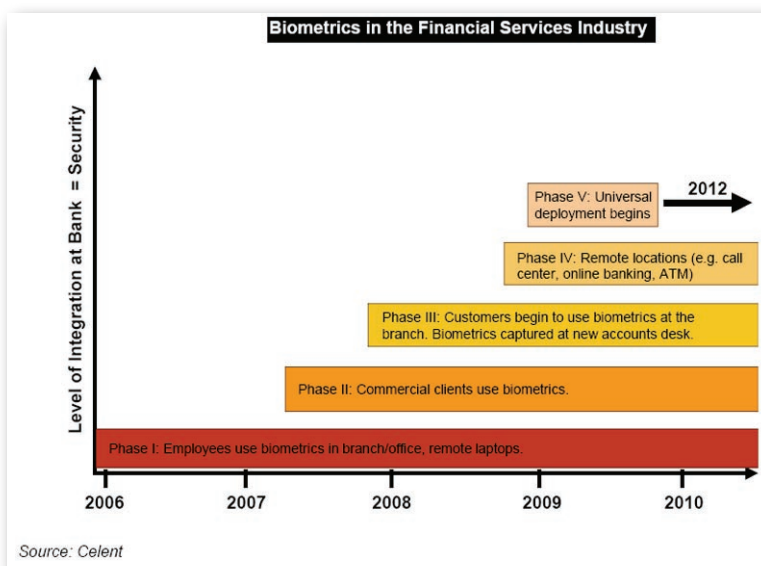
Biometrijski bazirana identifikacija (*Biometrics-based identification*): biometrijska identifikacija je bazirana na fizičkim karakteristikama osobe. Spada u najstarije metode identifikacije. Ove metode u rudimentarnim oblicima su primenjivali Sumeri i Egipćani a u doba Vavilona otisak prsta na glinenoj pločici je korišćen prilikom sklapanja ugovora. Kasnije tokom istorije kao biometrijska metoda identifikacija korišćena je tetovaža kod ljudi (označavanje kriminalaca u Francuskoj) ili žigosanje kod životinja kao dokaz vlasništva. U 19 veku započinje se sa korišćenjem otiska prsta kao metode za identifikaciju kriminalaca i ova metoda u 20 veku postaje opšte prihvaćena a policije svih zemalja prave baze podataka zasnovanih na ovoj metodi. Razvojem računarske tehnike krajem 20 i početkom 21 veka, mogućnosti biometrijske identifikacije dobijaju kako na kvalitetu i brzini tako i na raznovrsnosti primenjenih tehnologija. Proizvođači ovih uređaja su uložili značajna sredstva u istraživanje i razvoj metoda kao što su otisak prsta i ruke, skeniranje oka, prepoznavanje govora, prepoznavanje lica, ali se uvek postavljalo pitanje kako će korisnici ovih sistema da reaguju. Korisnici (građani koji daju svoje biometrijske podatke) uglavnom smatraju da su mnogi od ovih metoda neprijatni, nametljivi ili imaju kriminalnu konotaciju. Poseban problem kod ovih metoda je to, što kada je jednom biometrijski podatak ukraden, nije moguće da se zameni. Biometrijski zapis napravljen (dobijen) u digitalnom obliku može biti kopiran i korišćen za obmanu vrlo lako. Jednom kompromitovana biometrija ne može se izmeniti. Ovo je manji problem kod zatvorenih mreža ili pojedinačnih sistema, ali za udaljenu identifikaciju preko Interneta postaje ozbiljan problem. Industrija koja se bavi biometrijskim metodama preporučuje standardan set principa za očuvanje privatnosti. To je redovno kriptovanje biometrijskih podataka pre bilo kakvog slanja i stroga kontrola distribucije

podataka. Teško je predložiti kako će sigurno biti korišćeno rasprostranjena identifikacija identiteta preko Interneta.

Najčešće primene

Svedoci smo da se ove metode sve češće primenjuju u najrazličitijim poslovima. Neke od primena su sledeće:

- Kontrola dolaska zaposlenih na radno mesto
- Zaštita određenih prostora od ulaska neautorizovanih osoba
- Zaštita pristupa opremi (automobili, lap top računari, telefoni)
- Kontrola pristupa računarskim mrežama.
- Biometrijski potpis prilikom preuzimanja novca (plaćanje karticom na kasi sa biometrijskim potpisom).



Treba napomenuti da se biometrijske metode prepoznavanja ubrzano šire i uvode u sektor bankarstva i finansija. Primenjuju se u sistemima zaštite ali sve više i u sistemima plaćanja. Predviđanja su da će ove metode sve češće da se primenjuju i da će njihova upotreba biti sve univerzalnija.

Metode biometrijske identifikacije

Biometrijski sistemi identifikacije se oslanjaju na tehnike merenja i statističke analize ljudskih karakteristika. Metode biometrijske identifikacije mogu se podeliti u dve grupe:

- statička biometrijska identifikacija -

proverava fizičke karakteristike koje su jedinstvene za korisnika. Kod ovog tipa autentifikacije obično se proveravaju otisci prstiju, šake, oblik lica ili dužica oka.

- **d i n a m i č k a b i o m e t r i j s k a i d e n t i f i k a c i j a** - proverava različita ponašanja koja su karakteristična za korisnika. Kod ovog tipa autentifikacije najčešće se proveravaju glas ili rukopis korisnika.

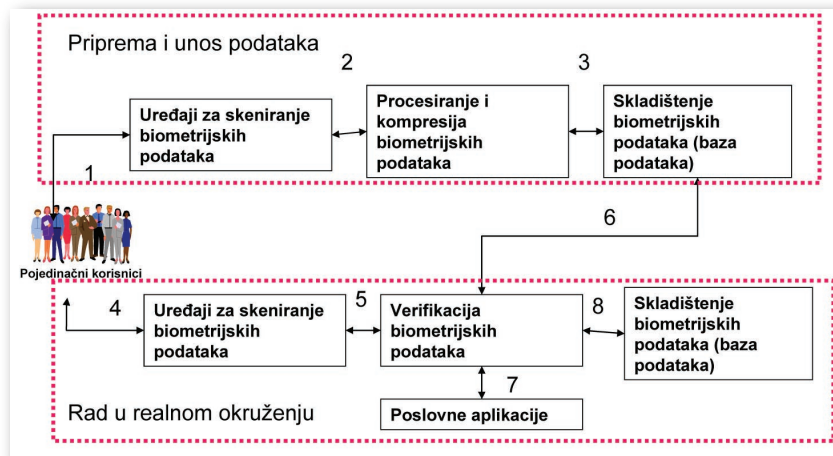
Kada se govori o

sistemima biometrijske identifikacije treba napomenuti da svi imaju određenih problema pri prepoznavanju skinutih (skeniranih) podataka. Za svaku metodu proizvođači daju procenat slučajeva pri kojima se javlja pogrešno očitavanje. U zavisnosti od primenjene biometrijske metode identifikacije proporcionalno se javlja i broj pogrešnih identifikacija.

Opšti model biometrijske identifikacije

Sve pobrojane tehnike biometrijske identifikacije sadrže u sebi osnovni model poslovanja. Model se sastoji od dva odvojena dela. U prvom delu je uzimanje biometrijskih podataka njihova kompresija i skladištenje u bazu podataka. Ovim se obezbeđuje da kada se korisnik pojavi i zatraži identifikaciju postoji podatak o njemu sa kojim će uporediti. Ovde su moguće dve varijante: Jedna varijanta je da prilikom uzimanja biometrijskog otiska, sistem pronalazi u bazi podataka odgovarajući zapis i upoređuje ga sa uzetim otiskom. Logika ovog sistema je pitanje "Da li sistem zna ko je vlasnik uzetog biometrijskog podatka", a to se postiže upoređivanjem skinutog podatka i podatka u bazi. Druga varijanta je da prilikom uzimanja biometrijskih podataka isti se upoređuju sa podacima koji se nalaze na smart kartici ili nekom drugom nosiocu podataka koji se lokalno ubacuje u čitač kako bi podaci bili upoređeni. Logika ove varijante je "Da li je

vlasnik biometrijskog otiska zaista onaj za koga se izdaje", to jest da li je identifikacija pozitivna i vlasnik prepoznat na osnovu dokumenta.



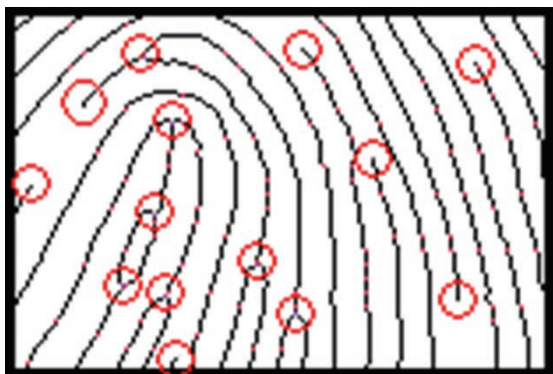
Proces uzimanja podataka (1-3) i proces prepoznavanja (4-8)

1. Uređaj za skeniranje biometrije prihvata biometrijske podatke.
2. Procesiranje prihvaćenih podataka, njihova kompresija i priprema za upis u bazu podataka.
3. Upis podataka u lokalnu bazu podataka, neku centralnu bazu ili upis na lokalni prenosni uređaj (smart kartica...)
4. Skeniranje biometrijskih podataka
5. Procesiranje biometrijskih podataka i priprema za upoređivanje sa ranije uzetim podacima.
6. Upoređivanje uzetih podataka i podataka koji su ranije upisani. Ovde postoje dva načina prepoznavanja i to:
 - a. "Da li ja znam ko si ti" uzeti biometrijski podaci se upoređuju sa podacima koji se nalaze u bazi podataka na računaru - (varijanta jedan)
 - b. "Da li si ti onaj za koga se izdaješ" podaci se upoređuju sa podacima koje je korisnik doneo (smart kartica) - (varijanta dva)
7. Rezultati upoređivanja se prosleđuju aplikaciji na dalje poslovno procesiranje
8. Konačni upis događaja sa svim pratećim podacima.

Identifikacija otiskom prsta

Identifikacija otiskom prsta je stara policijska metoda poznata od davnina. Verovatnoća da dva čoveka imaju isti otisak prsta je jedan

prema milijardu. Postoji više načina na koji se raspoznaju otisci prstiju. Identifikacija se zasniva na skeniranju i lociranju karakterističnih tačaka na prstu, a zatim se ti podaci upoređuju sa prethodno uzetim otiscima.



Oko 3% je onih koji su odbijeni (toliko je laganje sistema). Otisak prsta spada u najstarije poznate metode i najčešće korišćene metode. Najveće baze podataka i najbolji algoritmi za pretraživanje razvijeni su upravo za potrebe ove biometrijske metode. Lako je pogoditi da su to upravo policijske baze podataka i policijski algoritmi za pretraživanje tih baza podataka. Postoji veći broj tehnika za prepoznavanje i one se rangiraju prema nivou osetljivosti (broju skeniranih tačaka) a u zavisnosti od traženog nivoa zaštite. Osim za potrebe policije često se koristi u vojnim ustanovama, zaštićenim laboratorijama i bankama. Banke često koriste ovaj metod da bi osigurale računarske centre.

Ova metoda prepoznavanja sve češće se primenjuje na laptop računarima kao tehnika za sprečavanje neovlašćenog korišćenja ali

od nedavno su se pojavili i mobilni telefoni sa skenerom za prst. Nije daleko od ideje da kombinacija mobilnog telefona, skenera za prst i digitalnog sertifikata u telefonu daje potpunu identifikaciju dovoljnu za obavljanje bilo koje finansijske transakcije.

Skeniranje ruke je u suštini proširena i modifikovana verzija otiska prsta.



Case study sistem plaćanja zasnovan na otisku prsta

Sistem "Pay by Touch" omogućava biometrijsku autentifikaciju, šeme lojalnosti, ućlanjenje u sistem i mogućnost plaćanja. Sve to je omogućeno u realnom okruženju i "on line" preko Interneta.

Tehnologija rada može da se opiše sledećim koracima: Za početak obavezna je registracija korisnika. Registracija se može obaviti kod bilo kog trgovca koji je već ranije pristupio ovom sistemu. Znači ako korisnik želi da se koristi ovim sistemom prvo mora da pronađe listu prodavnica koje su registrovanje za ovaj način plaćanja. Prilikom registracije korisnik daje svoje podatke i obavezan je da stavi na uvid vozačku dozvolu (sistem za sada radi samo u SAD, a tamo je vozačka dozvola validan identifikacioni dokument) ili ID broj kako bi se ovi podaci povezali sa brojem računa u banci i sa mogućim lojaliti šemama Ovo identifikovanje je potrebno kao dokaz u slučaju

da korisnik kupuje alkoholna pića (mora da je punoletan). Korisnik daje svoj otisak prsta i prazan ček koji se takođe skenira. Skenirani ček više služi kao dokaz da korisnik zaista ima račun u banci i za automatizovano prikupljanje podataka. Korisnik treba da odabere i jedan broj (sedmocifreni - obično lični telefonski broj) koji je u ovom slučaju samo ključ za pretraživanje baze podataka. Razlika između "password-a ili PIN-a" i broja za pretraživanje je u tome što ovaj broj nije tajan. Preporučeno je da to bude telefonski broj korisnika jer ga je lako zapamtiti. Ovaj broj služi samo za brže pretraživanje baze podataka otisaka prsta. Password u ovom slučaju služi za logovanje na elektronski novčanik (wallet) u koliko se sistem koristi za plaćanja "on line". Korisnik koji je prijavljen na sistem dobija wallet kome pristupa preko Interneta i može ga ažurirati, brisati ili dodavati podatke iz kuće sa svog računara, iz prodavnice koja ima pristup Internetu ili sa infokioska koji je povezan na Internet. Treba napomenuti da korisnik nije u mogućnosti da ovlasti drugu osobu da se koristi ovim sistemom i jedino lično može da plaća.

Trgovac sa svoje strane je dužan da uz kasu priključi POS sa skenerom za prst, a ukoliko radi i uklanjanje novih korisnika mora da ima i skener za čekove.



Pay by Touch sistem plaćanja

Proces plaćanja u realnom okruženju (prodavnici) se odvija na sledeći način. Korisnik uzima robu i dolazi na kasu gde se pravi račun za plaćanje, unosi sedmocifreni broj i stavlja prst na skener koji mu uzima

otisak prsta a zatim se proverava u bazi podataka identitet korisnika upoređivanjem sa ranije datim otiskom (prilikom registracije). Ako se ustanovi poklapanje račun je namiren skidanjem sredstava sa računa u banci.

Na Internetu postupak rada je sledeći: Na sajtu trgovca korisnik pronalazi robu i kada treba da plati aktivira softverski novčanik na svom računaru. Unosi iznos za plaćanja, stavlja prst na skener i skida otisak prsta i unosi sedmocifreni broj a softverski novčanik završava proces kriptovanja i slanja podataka na server za proveru. Ako je sve korektno odrađeno transakcija se završava i korisnik dobija potvrdu (broj) pod kojim je transakcija zavedena.

Razlog za korišćenje ovog sistema plaćanja je čisto finansijske prirode. Kartični sistemi uzimaju proviziju od 2% pa naviše po svakoj transakciji a to znači da na 30 dolara prilikom plaćanja karticom trgovac gubi iznos oko jedan dolar. U koliko je plaćanje preko sistema "Pay by Touch" provizija po svakoj transakciji je 15 centi fiksno bez obzira koliki je iznos plaćen.

Dobra strana ovog sistema plaćanja je što korisnik ne mora tokom plaćanja da unosi osetljive podatke kao što su korisnički ID (PIN kartice), password ili osetljive finansijski podatke kao što su broj računa ili broj kartice.

Loša strana ovog sistema je što korisnik ne sme da se poseče, ogrebe prst ili na bilo koji drugi način ošteti površinu prsta jer u tom slučaju ostaje bez "novčanika", naime sistem neće prepoznati otisak.

Brzina rada sistema je zaista impresivna sudeći po podacima koji su stavljeni na uvid javnosti. Postupak plaćanja traje oko 14 sekundi i sastoji se od procedure unosa sedmocifrenog broja u numeričku tastaturu i stavljanja prsta u skener za prst. Ova dva podatka su dovoljna da se plaćanje direktno poveže sa korisnikovim bankarskim računom i da se uradi standardna debit transakcija.

Postupak plaćanja i-čekom

Čekovi predstavljaju najčešće korišćeni bezgotovinski sistem plaćanja kako u svetu tako i u našoj zemlji. U svetu se koriste za individualna plaćanja, plaćanja između firmi i za sva plaćanja među organizacijama. Kod nas

se koriste za individualna plaćanja sa našim specifičnim dodatkom, "čekom na poček". Jedan ovako važan instrument plaćanja nije mogao da ostane po strani, a da se ne razviju metode za njegovo korišćenje preko Interneta. Posebno kada se zna da je izdavanje čekova, njihovo korišćenje i završna obrada čekova veoma skupa. U praksi je prvo primenjen elektronski ili e-ček Elektronski ček se zasniva na ideji da elektronski dokument može da zameni papirni dokument i da kriptografski potpis može da zameni ručni potpis. Osim toga e-ček može da zameni papirni ček bez potrebe kreiranja novog instrumenta plaćanja bez promene regulative i ustaljenje komercijalne prakse. Ovako dizajniran sistem plaćanja podrazumevao je da korisnik ima instaliran softver na svom računaru a da se identifikacija obavlja preko PIN-a i smart kartice. Softver i kartica su predstavljali problem jer je svaka promena mesta sa koga će se odraditi transakcija zahtevao reinstalaciju. Da bi se taj problem prevazišao razvijen je sistem gde se sve odvija na Internetu i potrebno je samo logovati se na sistem.

Preduslov za korišćenje ovog sistema plaćanja je postojanje aktivnog čekovnog računa u nekoj od banaka, koja ima sklopljen ugovor sa provajderom i-čeka. Korisnik se loguje na sistem (na Internetu) i dobija sliku čeka koga treba da popuni, gde unosi sve podatke kao na standardnom papirnom čeku dok sistem automatski dodaje ostale potrebne podatke.

The screenshot shows a web form for filling out a check. The form is divided into several sections:

- Personal Information:** Fields for 'Your name as it appears on your check' (John Doe), 'Your phone number' ((253) 555-1212), and 'Check number' (1011).
- Address:** Fields for 'Your address as it appears on your check' (1234 Any Street), 'Your city, state & zip code' (Any Town, WA 98000), and a timestamp '08/21/2001 11:11:14 AM'.
- Payment Details:** A section for 'Pay To The Order Of' (Test Transactions Only) and the amount '\$195.99' (One Hundred Ninety-Five Dollars and 99 Cents).
- Banking Information:** Fields for 'Memo' (PayByCheck Demo), 'Signature' (John Doe), and 'Bank Routing Code and Bank Account Number' (123456789, 1234567891234).
- Buttons:** A 'Help' button is located at the bottom right.

Popunjavanje i-čeka

Kada je ček konačno popunjen, potrebno ga je potpisati a tu nastaje problem.

This account is secured with ICASI...

Please provide a finger-scan to use this account.



Your computer is identified as: 10.10.0.16

Zahtev za potpisivanje i-čeka



Potpisivanje i-čeka

Potpisivanje i-čeka je biometrijski skeniranjem prsta. Podaci o korisnicima se čuvaju na serveru provajdera. Osnovna karakteristika ovog sistema plaćanja je da ček u suštini predstavlja nalog banci po kome ona treba da postupi. Provajderi i-čeka ne primaju sredstva od kupaca, već samo formiraju dokumenta koja se mogu koristiti u procesu plaćanja i poravnjanja. Prilikom uzimanja otiska i slanja koristi se SSL (kriptografska zaštita) za zaštitu na komunikacionim kanalima.

Problemi plaćanja otiskom prsta

Treba napomenuti da otisak prsta nije teško falsifikovati a još ga je lakše nelegalno skinuti sa neke površine bez znanja njegovog vlasnika. Ovakvi sistemi mogu dobro funkcionisati za plaćanja u lokalnim samouslugama ili na Internetu za mikro plaćanja sve dotle dok motiv krađe nije naročito izražen (mali iznosi plaćanja, poznat kupac, poznat trgovac) ali šta će se desiti kada prometi narastu a sa njima i motivi za krađu.

Kada je u pitanju plaćanje čekovima treba napomenuti da je to samo nalog banci da postupi po uputstvima. Pre početka formiranja čeka korisnik mora da se uloguje i prođe proceduru

identifikacije tako da biometrijski potpis nije naročito bitan za sam proces plaćanja.

Problem sa korišćenjem biometrije prsta naročito može biti izražen kod teških krivičnih dela jer se već dogodilo da su kriminalci otkrili prst vlasnika automobila sa biometrijskom identifikacijom kako bi oteli automobil.

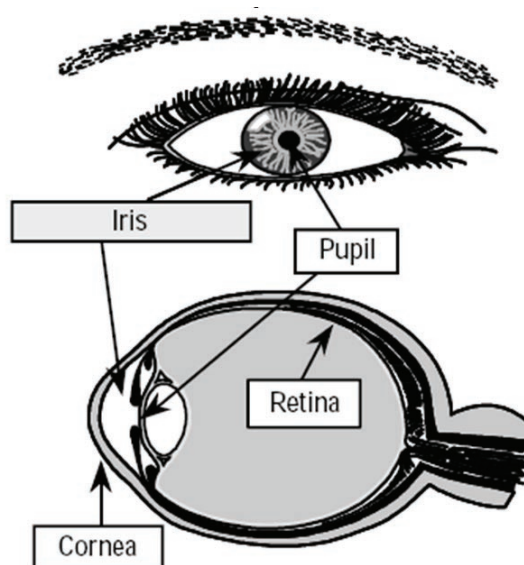
Biometrijski sistemi plaćanja koji koriste oko za identifikaciju

Prepoznavanje skeniranjem mrežnjače je tehnologija koja za prepoznavanje koristi karakteristike krvnih sudova na dnu oka. Ovo je najpouzdanija biometrijska metoda identifikacije. Do danas nije pronađen način da se mrežnjača falsifikuje. Osnovna karakteristika mrežnjače je da se ne menja tokom celog života osobe. Provera dali je osoba živa ili mrtva nije potrebna jer mrežnjača mrtve osobe brzo propada. Tehnologija skeniranja podrazumeva da je oko blizu skenera i potrebno je fokusirati se na određenu tačku. Ovde nije moguće skeniranje preko naočara. Skeniranja traje 10-15 sekundi i za to vreme je oko osvetljeno svetlošću slabog intenziteta.

Do danas su razvijene dve metode određivanja identiteta pomoću oka:

- Skeniranje i prepoznavanje dužice (irisa)
- Skeniranje i prepoznavanje mrežnjače (retine) oka.

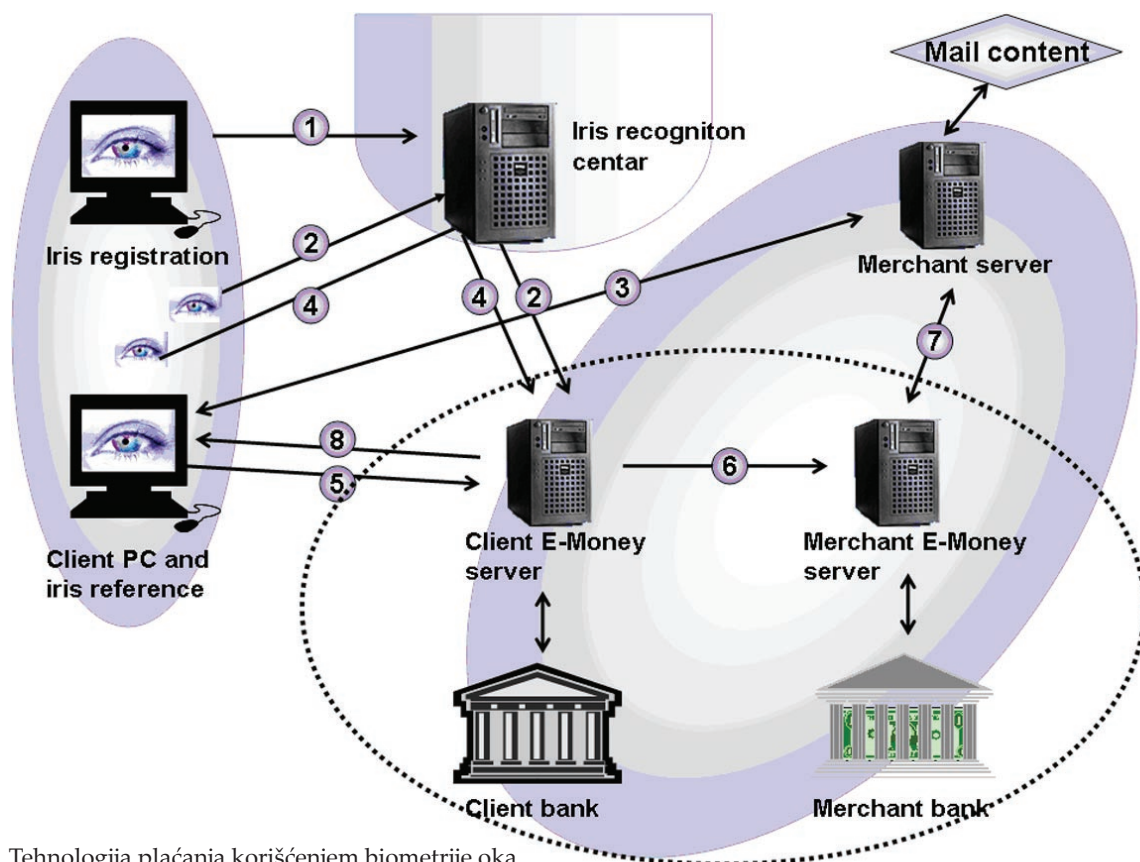
Prepoznavanje dužice se zasniva na analizi pojedinosti prstena u boji koji okružuje zenicu (irisa). Na dužici postoji više od 200 tačaka koje su karakteristične i mogu se iskoristiti za identifikaciju osobe. Karakteristike kao što su prsteni, brazde i pegice su jedinstvene za svakog pojedinca do te mere da se levo i desno oko iste osobe razlikuju. Ove karakteristike omogućavaju uspešnu identifikaciju i verifikaciju osoba. Snimanje dužice može se izvesti specijalizovanom ili običnom kamerom sa daljine (pola metra) čak se može obaviti skeniranje kroz naočare. Sistem može biti tako dizajniran da proveri da li je osoba živa ili je u pitanju veštačko oko. Provera se izvodi tako što se oko naglo osvetli, a zatim se analizira da li je došlo do skupljanja zenice.



Jedno od predloženih rešenja za sistem plaćanja preko Interneta zasniva se na tehnologiji rada tako što se zenica oka koristi samo za identifikaciju korisnika. Drugim rečima postoje dva servera: jedan gde se drži baza podataka snimljenih zenica oka korisnika, dok je drugi novčani server na kome se nalaze podaci o stanju novca na računu korisnika.

Tehnologija rada pri plaćanju:

1. Prvi korak u procesu plaćanja je da se korisnik registruje i da njegov snimak zenice bude memorisan u bazi podataka. Proces je tako dizajniran da pri registraciji obavezno se pored snimka oka uzimaju na uvid i papirni identifikacioni dokumenti kako bi se otvorio bankarski račun.
2. U drugom koraku je potrebno napuniti račun sa koga će biti izvršeno plaćanje. To podrazumeva da u trenutku pokretanja prve transakcije na "novčanom serveru" mora postojati slog sa upisanim sredstvima raspoloživim za trošenje.
3. U trenutku kada korisnik želi da nešto kupi na sajtu trgovca pokreće se standardna procedura pravljenja korpe i formira se porudžbina.
4. Procedura plaćanja podrazumeva da se prvo proverava identifikacija korisnika, to jest da on na svom računaru kao dodatni uređaj ima skener (kameru) koja je u mogućnosti da snimi zenicu oka i da taj snimak prosledi na server gde se nalaze podaci za proveru.
5. Korisnik daje instrukcije za plaćanja novčanom serveru.
6. Transakcija prebacivanja sredstava sa računa



Tehnologija plaćanja korišćenjem biometrije oka

korisnika na račun trgovca.

7. Povratna informacija da je procedura plaćanja izvršena.
8. Povratna informacija da je procedura plaćanja uspešno okončana.

Kao što se iz priloženog vidi tehnologija rada je prilično jednostavna i laka za upotrebu. Od dodatne opreme se zahteva samo kamera za snimanje zenice oka što danas nije veliki izdatak i malo softvera na računaru.

Dinamički potpis kao biometrijski metod je posebno interesantan sa stanovišta automatske verifikacije potpisa u komunikacijama finansijske prirode. Upošteno kod poslova finansijske prirode često imaju posla grafolozi koji dokazuju da li je neki potpis originalan ili je lažni. Ideja uzimanja dinamičkog potpisa je da se korisnik na tabletu (uređaj za pisanje po senzitivnoj ploči) potpiše a uređaj registruje karakteristike potpisa. Uređaj na kome se vrši provera beleži oblik slova način na koji se pero vodi različite pritiske na pojedinim mestima, tako da stvara jedinstvenu sliku potpisa. Upošteno uređaj na kome se vrši identifikacija na osnovu dinamičkog potpisa je specijalno

pero povezano sa računarnom, senzitivna tabla ili kombinacija jednog i drugog.



Ovakvi tableti su uobičajeni u prodavnicama širom Kanade i USA i koriste se za potpisivanje prilikom plaćanja karticama. Naime tamo se često ne štampaju slipovi sa POS terminala (ili kase) već se korisnik potpisuje na tabletu i njegov biometrijski potpis se dalje čuva.

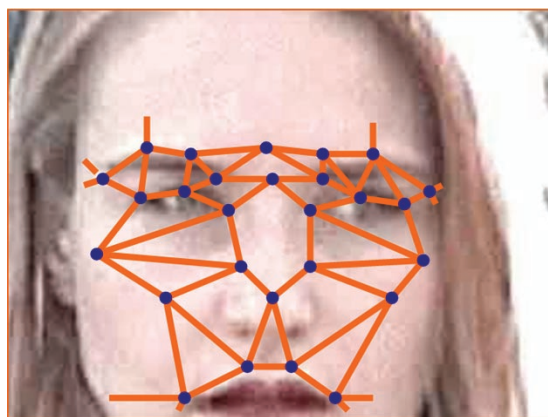
Identifikacija glasom je veoma atraktivan biometrijski metod zato što je prihvatljiv od strane korisnika. Zbog svojih dobrih osobina veći broj firmi je razvio metodu i algoritme

za prepoznavanje glasa. Matrica na osnovu koje se vrši prepoznavanje glasa formira se na osnovu kombinacije većeg broja faktora (više puta izgovorena rečenica). Ovakvo formiranje matrice je potrebno da bi se sprečilo oponašanje glasa neke osobe ili korišćenja snimljenog glasa. Ovaj vid identifikacije najčešće se koristi za srednje zaštićene sisteme na mestima gde je velika frekvenca prolazaka. Identifikacija glasom se često upotrebljava za zaštitu računara pri uspostavljanju "dial-up" računarskih veza. Interesantna primena ovog vida identifikacije je za praćenje uslovno puštenih zatvorenika koji su obavezni da se mašini jave do određenog vremena kako bi potvrdili svoje prisustvo na određenom mestu.

Ova tehnologija je počela da se primenjuje u školama u SAD od 2007. godine za potrebe distribucije obroka (užina). Daci jednostavno izgovore svoje ime i identifikacioni broj u automat koji im izdaje hranu. Dobra strana ove tehnologije je što značajno ubrzava identifikaciju i propusnost kanala distribucije. Problem se sastoji u tome što je glas promenljiv tokom vremena ili se menja prilikom bolesti tako da ova metoda teško da može ozbiljno da se prihvati za potrebe plaćanja. Ovaj pilot projekt pre treba shvatiti kao pokušaj da se u uslovima masovne primene testira tehnologija.

Prepoznavanje tehnike rada je metod koji je preuzet iz vremena telegrafije kada je jedan operator mogao da prepozna drugog operatora samo na osnovu "ruke koja šalje" Metod se sastoji u analiziranju načina kucanja operatora na terminalu. Moderni sistemi imaju mogućnost da prepoznaju osobu na osnovu načina kucanja bez potrebe da se ona predstavi. Što je brži način kucanja to je i prepoznavanje lakše i pouzdanije. Ovaj biometrijski metod bi imao dosta prednosti. Nema potrebe za bilo kakvom prijavom ili verifikacijom prisustva na sistemu. Mašina sama prepoznaje korisnika. Nema dodatnih ulaganja za opremu jer je dovoljna tastatura. Ovaj metod je još uvek u razvoju i potrebno je razrešiti mnoge probleme koji se javljaju. Banalna stvar je kada se na sistemu promeni tastatura operater mora da se prilagodi na novu da bi postigao brzinu. Postoje mnogi problemi koje treba rešiti da bi ovaj metod bio raspoloživ za komercijalnu upotrebu.

Identifikacija izgleda lica. Ovo je metod koji se najbrže razvija. Postoje nekoliko komercijalnih sistema. Privlačnost ovog načina prepoznavanja je očekivana jer se zasniva na sličnosti načina na koji ljudi prepoznaju druge osobe. Postoji veliko interesovanje na zapadu od strane vladinih agencija, kao i velikih bankarskih sistema za razvoj ovih metoda identifikacije. Tehnologija se zasniva na registrovanju karakterističnih tačaka na licu, i njihovom rasporedu koji se pamti u komprimovanom obliku.



Postoji potreba za nizom specifičnih upotreba ovog metoda kao što je zaštita aerodroma od terorista njihovo prepoznavanje ili možda mnogo neprijatnija metoda za kontrolu stanovništva.

Predviđanja su da će ova metoda u bankama da se koristi za potrebe personalizacije korisnika usluga banke. Ideja se zasniva na tome da prilikom ulaska korisnika u ekspozituru kamera snimi i izvrši prepoznavanje korisnika i dok on dođe do službenika na šalteru banke ovaj već ima sve njegove podatke tako da može da mu se obrati kao starom znancu.

Prepoznavanje rasporeda vena

Tehnika prepoznavanja vena je relativno nova metoda. Zasniva se na prepoznavanju rasporeda vena u šaci ali pošto meri i kretanje krvi u šaci jedna je od metoda koja automatski registruju da li je korisnik živ u trenutku kada se uzimaju biometrijski podaci.

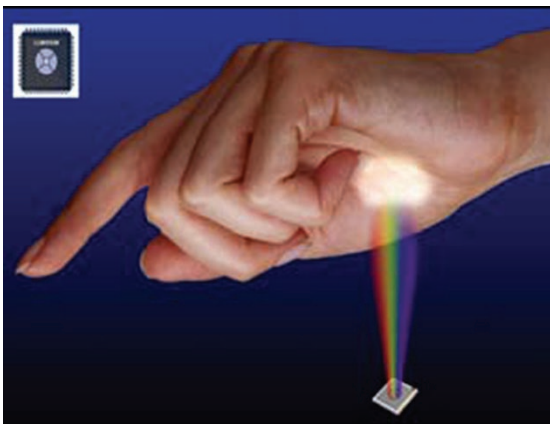


DNK analiza. U razvoju su ili postoje još neke biometrijske metode raspoznavanja kao što je metod na osnovu analize krvi ili na osnovu DNK. Ovi metodi su još u domenu poverljivih materijala tako da se o njima malo zna.

Lumiguard sistem

Ova tehnologija se zasniva na karakteristikama kože koje su specifična za neku osobu. Tehnologija je bazirana na spektroskopskoj analizi kože. Merenje se obavlja na prstu, šaci ili ručnom zglobov tako što se određeni deo kože osvetli zrakom specifičnih osobina i zatim se radi analiza reflektovanog zraka. Sama koža se sastoji od više slojeva i kada se osvetli izvorom svetlosti odbijena difuzna svetlost dozvoljava mogućnost da se analiziraju fizičke karakteristike osobe. Ovo su jednoznačne karakteristike osobe sa dodatnom mogućnošću ove tehnologije da odmah prepozna da li je ta osoba živa u trenutku kada se skida biometrijska karakteristika.

Sam senzor koji se koristi u ovom sistemu je veoma mali (veličine metalnog novčića) i lako ga je zapakovati u mobilni telefon ili privezak za ključeve.



Kombinacija ovog sistema identifikacije i mobilnih uređaja otvara mogućnosti za mobilna plaćanja, s tim da se ovim metodom obavlja samo identifikacija korisnika a da se ostatak transakcije plaćanja obavi standardnim postupkom. Tehnologija je u fazi ispitivanja i testiranja ali je najavljeno da će se koristiti za potrebe identifikacije i plaćanja u mobilnom okruženju

Zaključak

Biometrijska identifikacija je oblast koja se ubrzano razvija. Tehnologija koja prati ove metode je sve pouzdanija ali sa njihovim razvojem kod korisnika sve više izaziva strah od neovlašćene primene ili zloupotreba. Posebno se ovo odnosi na probleme privatnosti i više zemalja je zakonski regulisalo ovu oblast.

Sistemi plaćanja postaju sve kompleksniji i zahtevniji. Biometrijski sistemi plaćanja, bar za sada se čine kao jedno od mogućih rešenja, mada se već sada naziru veliki problemi u domenima privatnosti. Posebno veliki problem je što je biometrijske podatke teško sačuvati. Treba li nositi tamne naočare da bi se sprečilo neovlašćeno uzimanje biometrijskih podataka zenice oka ili nositi rukavice kako bi se sprečilo uzimanje otiska prsta.

Problemi koji prate sisteme za biometrijsku identifikaciju su:

- Uređaji koji se koriste za biometrijsku identifikaciju i softverska rešenja koja prate su još uvek skupi.
- Biometrijski sistemi identifikacije su nametljivi i dehumanizovani.
- Stvaraju nelagodnost pri korišćenju.
- Primena biometrije trajno isključuje osobe sa hendikepom (oštećeno oko, nedostatak prsta, koža koja nije čitljiva za skenere).
- Trajnost uređaja nije proverena u praksi jer je tehnologija još uvek relativno nova.
- Nepouzdanost pojedinih sistema (procenat laganja).
- Obuka korisnika za rad sa ovakvim sistemima.
- Problemi privatnosti. Svi pobrojani sistemi imaju veliki broj protivnika koji smatraju da je ovakvo prikupljanje podataka problematično jer zadire u privatnost korisnika. Formiranje podataka

za biometrijsku identifikaciju mora biti zakonski regulisano.

- Formiranje centralizovanih baza podataka. Ovo je takođe problem privatnosti.
- Baze biometrijskih podataka predstavljaju idealnu metu za "kradljivce identiteta". Jednom ukradena biometrija trajno isključuje korisnika iz poslovanja.
- Nedostatak standarda. Svaki proizvođač uređaja za biometrijsku identifikaciju razvija samostalno rešenje. Ovako samostalan razvoj bez međusobne komunikacije dovodi do toga da biometrijski otisak sa jednog uređaja neće dati iste rezultate na drugom što će značajno povećati broj odbijenih pokušaja plaćanja i izazvati nezadovoljstvo korisnika.

Najvažniji problem koji ovakvi sistemi nisu u stanju da reše je "što ne mogu biti opšti" i rešavati probleme po svim kanalima komunikacije. Veoma često se koriste uporedo sa nekom dugom metodom identifikacije tako da se postavlja pitanje "da li su uopšte nepohodni za identifikaciju" jer se ona lakše i brže obavlja na drugi način.

Činjenica je, da se ova tehnologija favorizuje u odnosu na sve ostale. Biometrijska identifikacija će preovladati ali se postavlja pitanje kakve posledice će imati društvo u

celini. Važno je napomenuti da postoji velika potreba za boljim sistemima autentifikacije jer postojeći ne obezbeđuju dovoljno visok nivo.

Sa druge strane postoje zahtevi za povećanjem zaštite i regulacijom u oblasti biometrijske identifikacije i zakonsku regulativu tek treba razvijati.

Najznačajniji detalj na koji treba obratiti pažnju je da ovu tehnologiju najviše forsiraju veliki proizvođači opreme. Ovo se može protumačiti da nedostatak posla i zasićenost tržišta inicira razvoj pratećih tehnologija.

Činjenica je da su ovakvi sistemi pogodni za korišćenje u sistemima plaćanja ali samo u realnom okruženju. Internet nije najpogodniji za rad ovakvih sistema. Slanje biometrijskih podataka preko Interneta generiše čitav niz rizika koji teško mogu da se kontrolišu bez obzira na mogućnosti kriptografske zaštite.

Svi sistemi za biometrijska plaćanja podrazumevaju da se biometrija koristi samo za identifikaciju korisnika. Veliki problem svih sistema je što je biometrija javni podatak i nije ga moguće sakriti. Prepoznavanje osobe na osnovu javnog podatka može se prihvatiti. Obavljati plaćanja koristeći javni podatak predstavlja veliki problem, posebno kada su u pitanju plaćanja preko Interneta.

Literatura

1. Sistemi plaćanja u elektronskom poslovanju, dr Vojkan Vasković, FON.
2. *Biometric Technologies: Are We There Yet?* www.celnet.com
3. IVRS Based Bill Payment System: Tele-Bhuktan Sanjay Dubey
4. An introduction to biometric, white paper.
5. www.lumiguard.com
6. www.oki.com

Abstrakt

Biometrijska identifikacija je kroz istoriju dobro poznata metoda i primenjivala se od najranijih vremena. Počev od toga da su se nekada robovi žigosali, zatim zatvorenici a kasnije (za vreme II svetskog rata) pripadnici pojedinih nacija. Ove metode izazivaju strah ili u najmanju ruku oprez pri samoj pomisli da će biti primenjene. Kako se tehnologija razvijala tako su se usavršavale biometrijske metode. Pronalaskom fotografije slika postaje osnova za identifikaciju. Slika predstavlja u suštini biometrijski otisak lica na fotografskom papiru. Svojeručni potpis korisnika na papiru nije ništa drugo do njegov biometrijski potpis, a to je metod potvrđivanja identiteta koji se primenjuje od pamtiveka. U svim vremenima uzimanje biometrijskih podataka predstavljalo je atak na privatnost ali tek sa uvođenjem računara i centralizovanih baza podataka, ovako prikupljanje podataka postaje problematično. Savremena tehnologija je donela nove metode a računari su učinili da se analize uzetih podataka mogu obraditi brzo i sa velikom tačnošću. Posebno opasno je što računari omogućavaju da se podaci iz različitih izvora (baza podataka) ukrste i pretražuju, što je u ranijim vremenima bilo teško ako ne i nemoguće. Primena biometrijskih metoda identifikacije u finansijskim institucijama primenjuje se od davnina (svojeručni potpis, otisak prsta) jer je u svim vremenima bilo potrebno da se korisnik identifikuje i autentifikuje pre nego što mu se novac stavi na raspolaganje. S obzirom na potrebe bankarskih organizacija za pouzdanim metodama identifikacije i autentifikacije svojih komitenata, normalno je, da je i primena novih tehnologija brzo prihvaćena i ubrzano se uvodi u procese rada.

Definicija

Biometrijski sistemi identifikacije se definišu kao: "automatizovani, uglavnom računarski bazirani sistemi, koji koriste različita fiziološka svojstva i/ili merenje ponašanja ljudskog tela koja se mogu koristiti za konkretnu identifikaciju određene osobe". "Oxford English Dictionary", kaže da je to "primena statističkih analiza nad biometrijskim podacima".

Abstract

Biometric identification is, historically, a well-known method which has been applied since the ancient times, starting with slaves, then prisoners, and later on (during the World War II) members of the certain nations being branded. Such methods raise fear or, to say the least, caution at the mere thought that they will be applied. With the technological development biometric identification methods also improved. The invention of photography made photos a basis for identification. Essentially, a photo is a biometric face print on the photographic paper. User's personal signature put on paper is nothing but his/her biometric signature, and this has been an identity authentication method for ages. Obtaining one's biometric data has always been seen as invasion of privacy, but it was not until computers and centralized databases were introduced that this kind of data collection became problematic. Modern technology has provided new methods, and the use of computers enabled the analyses of the collected data to be conducted quickly and accurately. What is especially dangerous, however, is that computers now make it possible to cross-search the data from different sources (databases), an operation which was difficult, if not impossible, in the past. Biometric identification method has been applied by financial institutions for a long time already (personal signature, finger print) since it has always been necessary to identify and authenticate the user before he/she is allowed to use the money. Given the needs of banking organizations concerning the reliable methods of identification and authentication of their clients, it is only natural that the application of these new technologies has been swiftly accepted and is being rapidly introduced into the operational processes.

Definition

Biometric identification systems are defined as the "automatized, mainly computer-based systems, using different physiological characteristics and/or body language monitoring in order to identify a specific person". Oxford English Dictionary defines the term as the "application of the statistical analyses on the biometric data".