

BIOMETRIJSKI SISTEMI – UPOTREBA I ZLOUPOTREBA

Brankica Popović¹, Miodrag Popović²

*¹Policijska akademija, Humska 22 Beograd
e-mail: cica@ptt.yu*

*²Elektrotehnički fakultet, Bulevar kralja Aleksandra 73 Beograd
e-mail: pop@el.etf.bg.ac.yu*

***Abstrakt:** Veliki je interes za korišćenje biometrike u aplikacijama za identifikaciju. Oni imaju niz prednosti u odnosu na sisteme zasnovane na znanju ili posedovanju. Sa aspekta sigurnosti neophodno je ukazati na ograničenja biometrijskih sistema, kao i odrediti stepen njihove ugroženosti od različitih napada. Posebno se ukazuje na problem ugrožavanja privatnosti prilikom neadekvatnog korišćenja ovakvih sistema.*

Ključne reči: biometrika, identifikacija, zloupotreba, sigurnost

1. UVOD

Prepoznavanje ličnosti izgleda jednostavno zbog toga što ga ljudi svakodnevno vrše na poslu, ulici, kući, na bilo kom drugom mestu gde dolaze u kontakt sa drugim ljudima. Međutim, u modernom svetu, ono nije tako lako kao što se čini. Tehnološki razvoj, postojanje globalne računarske mreže koja se svakim danom sve više širi, povećanje broja putnika na globalnom nivou, kao i automatizacija raznih poslova i usluga zahteva pouzdane metode za utvrđivanje i proveru identiteta. Naime prosečna osoba se dnevno identifikuje više od 10 puta prilikom korišćenja računara, telefona, kreditnih i platnih kartica, automatskih terminala za isplatu novca, primanja socijalne pomoći, korišćenja zdravstvenih usluga, ... [5]. Identifikacija ličnosti treba da bude brza, pouzdana, teška za prevaru, jeftina, i u velikom broju slučajeva društveno prihvatljiva za osobu koja treba da se identifikuje.

U oblasti sigurnosti poznata su 3 različita načina za proveru identiteta:

- Nešto što znaš (*knowledge*) – šifra, PIN (lični identifikacioni broj), neka lična informacija (npr. ime maminog psa i sl.);
- Nešto što imaš (*possession*) – karticu (npr. “pametne” ili slične);
- Nešto što jesi – *biometrika*

Biometrika koristi neke karakteristične podatke (poznate i pod nazivom biometrijski potpis ili ključ) o osobi, koji omogućavaju da se utvrdi identitet osobe. Primeri biometrijskih tehnika koje se danas ispituju ili koriste su: otisci prstiju, izged lica, geometrija šake, struktura oka, oblik uva, glas, potpis, ritam otkucaja dirki na tastaturi računara, DNK, [5,6,7,8]

Biometrika je oblast prepuna kontroverzi. Njeno korišćenje promovišu oni čiji je posao da spreče prevare, dok su oni koji se zalažu za očuvanje privatnosti prepuni sumnji. Biometrika može da pozitivno identifikuje osobu i time spreči čitav niz prevara vezanih za identitet, ali ona može i da, bez dozvole subjekta, prati njegove postupke i poveže lične

informacije iz različitih izvora, što je veliki napad na privatnost. Tu su još i nedovoljno ispitani izvori pretnji karakteristični samo za biometriku. Njeno korišćenje je moćno sredstvo u rukama jakih korporacija (zašto ne i vlada i njenih agencija), da vežbaju kontrolu nad pojedincem, ali i društvom u celini. Sve ovo baca novo svetlo na mogućnost korišćenja ali i zloupotrebe biometrike.

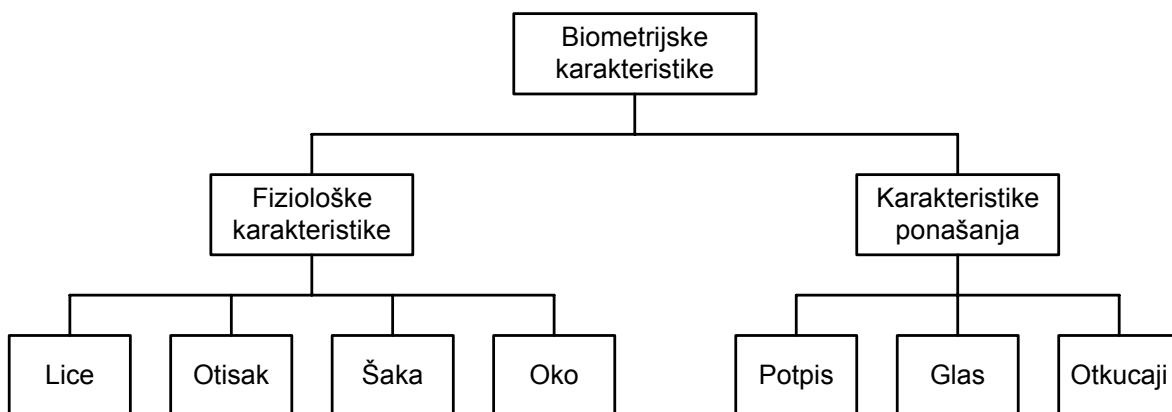
U radu ćemo se prvo upoznati sa osnovama biometrijskog sistema, njihovom tačnošću i uslovima njihovog korišćenja. Zatim ćemo prikazati moguće tačke napada na ove sisteme, kao i specifične pretnje koje su karakteristične samo za ove sisteme. Posebno je objašnjen i uticaj na privatnost kao jedan od bitnih faktora šire upotrebe ovih sistema.

2. BIOMETRIJSKI SISTEMI

Termin biometrika potiče od grčkih reči *bios* (život) i *metrikos* (merenje). Naime biometrika se oslanja na ono što jesi ili kako se ponašaš, umesto na ono što znaš (šifra) ili šta poseduješ (ID kartica). Biometrika meri jedinstvene biološke karakteristike (fiziološke i/ili karakteristike ponašanja) pojedinca koje se koriste za proveru autentičnosti i utvrđivanje identiteta [5].

Da bi se kvalifikovale da ih nazovemo biometrijskim, biološke mere moraju zadovoljiti sledeće uslove:

1. *Univerzalnost* - svaka osoba mora posedovati ovu karakteristiku;
2. *Jedinstvenost* – karakteristika mora biti različita za sve članove populacije;
3. *Nepromenljivost* – karakteristika ne sme da se menja pri različitim uslovima prikupljanja, i tokom vremena;
4. *Kolektibilnost* – karakteristika mora biti kvantitativno merljiva i prikupljiva [9].



Slika 1. Podela biometrijskih sistema po poreklu karakteristika.

Danas se koriste ili su u fazi istraživanja; lice, šaka, oko, otisak prsta, uvo, potpis, glas, obrazac kucanja, DNK (Slika 1).

Naravno pri odabiru biometrijskog sistema koji se koristi za utvrđivanje identiteta mora se voditi računa i o sledećim faktorima:

- *pouzdanost* – odnosi se na tačnost, brzinu, kao i na faktore koji mogu uticati na rad sistema;
- *prihvatljivost* – označava stepen spremnosti ljudi da prihvate korišćenje ovog sistema u svakodnevnom radu;
- *otpornost* – koliko je sistem otporan na potencijalno krivotvorenje i napade.

U Tabeli 1. dat je pregled različitih biometrijskih tehnologija kao i percepcija u kojoj meri one ispunjavaju gore navedene faktore.

	univerzalnost	jedinstvenost	nepromenljivost	kollektivnost	pozdanost	prihvatljivost	otpornost
biometrika							
Lice	V	N	S	V	N	V	N
Otisak prsta	S	V	V	S	V	S	S
Geometrija šake	S	S	S	V	S	S	S
Iris	V	V	V	S	V	N	V
Retina	V	V	S	N	V	N	V
Potpis	N	N	N	V	N	V	N
Glas	S	N	N	S	N	V	N

Tabela 1. Komparacija različitih biometrika. V, S i N označavaju Visoko, Srednje i Nisko respektivno

Biometrijski sistem generalno radi u dva moda:

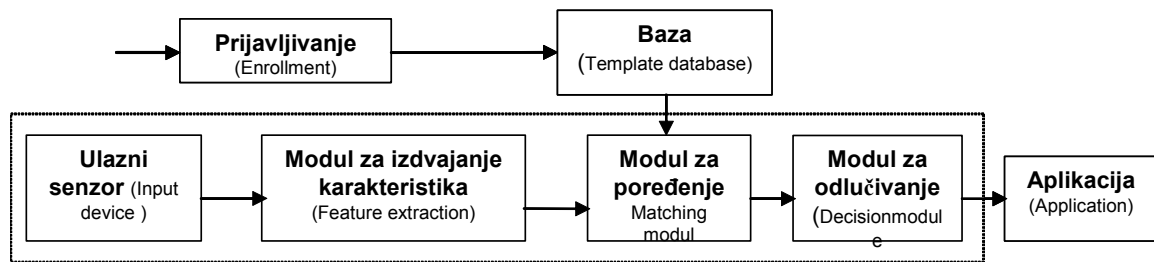
- A. **Verifikacija** – vrši se kada neka osoba tvrdi da ima neki identitet (u tradicionalnim sistemima to se radilo uz pomoć lozinke, ID kartice i sl.); sistem potvrđuje ili odbija identitet upoređivanjem biometrijskih karakteristika sa šablonom (*template*) prethodno sačuvanim u bazi i izvodi se poređenje jedan–prema–jedan (*one-to-one* comparasion). Ovo je takozvano ‘**pozitivno prepoznavanje**’ čiji je cilj da se spreči da više ljudi koristi isti identitet.
- B. **Identifikacija** – sistem mora da izvrši prepoznavanje osobe tako što će uporediti njene biometrijske karakteristike sa svim šablonima sačuvanim u bazi da bi našao najveće poklapanje. Tom prilikom se izvodi jedan–prema–mnogo (*one-to-many*) poređenja i ovo se naziva ‘**negativno prepoznavanje**’ gde sistem može utvrditi da li je osoba ono što implicitno tvrdi da nija. Cilj je da se spreči da jedna osoba koristi više identiteta.

Važno je naglasiti da se metode *possession&knowledge* mogu koristiti samo za verifikaciju, dok se za identifikaciju tj. negativno prepoznavanje jedino može koristiti biometrika.

Svaki biometrijski sistem ima četiri modula (Slika 2.) [11]:

1. *ulazni uređaj-senzor* (sensor module) – koji uzima i digitalizuje biometrijsku karakteristiku (npr. skener za otiske prstiju);

2. *modul za izdvajanje karakteristika* (feature extraction module) – koji obrađuje digitalizovan podatak radi izdvajanja karakteristika koje ga čine jedinstvenim i koje se mogu smestiti u šablon (template) (npr. izdvajanje minucija iz slike otiska);
3. *modul za poređenje* (matching module) – gde se porede izdvojene karakteristike sa podacima iz šablona sačuvanog u bazi;
4. *modul za donošenje odluke* (decision-making module) – gde se identitet prihvata ili odbija (verifikacija), ili utvrđuje na osnovu skora poređenja (identifikacija).



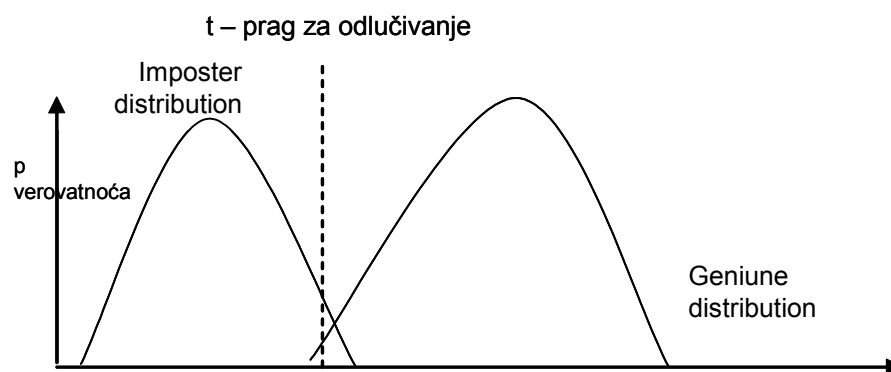
Slika 2. Blok dijagram biometrijskog sistema

Naravno ovome se mora dodati i peti modul tj. *baza* (template database) gde se čuvaju šabloni uzeti od osobe u postupku prijavljivanja (registracije-enrollment). Postupak prijavljivanja podrazumeva uzimanje biometrijske karakteristike od osobe, pravljenje šablona i njegovo dalje čuvanje. Baza može biti centralna; lokalna u odnosu na mesto gde se koristi (npr. zgrada gde se radi); ili može biti na uređaju koji korisnik nosi sa sobom (*smartcard* i sl.). Naravno može biti i kombinacija bilo koje dve ili čak sve tri. Takođe se ti podaci mogu čuvati tako da se mogu koristiti samo za tu aplikaciju i organizaciju, ili za više njih [2].

3. TAČNOST BIOMETRIJSKIH SISTEMA

Biometrijski sistemi kao izlazni rezultat daju stepen podudaranja (*matching score*) ulaznog podatka sa šablonom sačuvanim u bazi. Dva uzorka iste biometrike od iste osobe mogu da se razlikuju u zavisnosti od uslova i vremena njihovog uzimanja, pa se nemože očekivati njihovo apsolutno poklapanje. Što je stepen podudaranja veći to je sistem sigurniji da dva biometrijska uzorka dolaze od iste osobe. Ipak odluku sistema definiše neka granica (prag) koju korisnik postavlja u skladu sa aplikacijom za koju se biometrijski sistem koristi.

Rezultati dobijeni od poređenja parova uzoraka različitih osoba, kao i oni dobijeni od poređenja uzoraka iste osobe daju nam raspodele koje se zovu '*impostor distribution*' i '*genuine distribution*', i prikazane su na Slici 3. Vidimo da se u jednom delu preklapaju. Prilikom projektovanja biometrijskog sistema granica (prag) odlučivanja se projektuje u skladu sa specifičnim zahtevima aplikacije [1].



Slika 3. Uticaj praga na performanse (tačnost) biometrijskog sistema

Tačnost biometrijskih sistema može se odrediti preko dve specifične promenljive a to su:

- **FAR** (false accept rate) – lažno prihvatanje, gde se biometrijske karakteristike od dve različite osobe prihvataju kao da su iste
- **FRR** (false reject rate) - lažno odbijanje, gde se biometrijske karakteristike od iste osobe ne prihvataju tj. smatraju se uzorcima različitih osoba

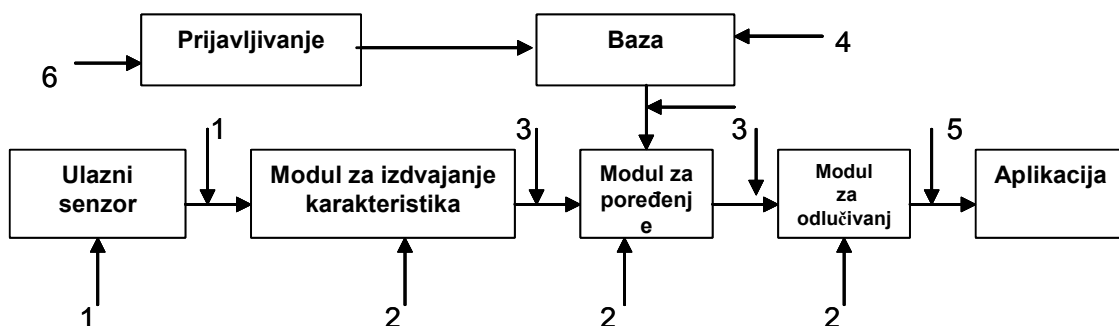
Smanjivanjem jednog faktora (greške) povećavamo drugi. Kako uspostaviti najbolji odnos zavisi od konkretne primene sistema i od toga gde ćemo postaviti prag za odlučivanje. Naime ako se želi maksimalna sigurnost da samo stvarno autorizovani korisnici prolaze kroz sistem, čak i po cenu da se ponekad i odbije autorizovani korisnik onda se smanjuje FAR po cenu povećanja FRR. Ovo je u slučajevima zaštite raznih sigurnosnih sistema. Sa druge strane za neke komercijalne aplikacije odbijanje autorizovanog korisnika može naneti velike štete, pa se tu smanjuje FRR na račun povećanja FAR.

4. BIOMETRIJSKI SISTEMI I MOGUĆE PRETNJE

Sigurnosne slabe tačke postoje u svakom sistemu, a na Slici 4. prikazane su slabe tačke biometrijskih sistema [10]:

- 1) Prva pretnja je prezentovanje lažne biometrike i to:
 - lažno predstavljanje tj. falsifikovanje podatka koji se stavlja pred senzor (*impersonation*);
 - predstavljanje prethodno ukradenog biometrijskog podatka čime se zaobilazi senzor (tzv. *replay* napad);
- 2) Druga pretnja je napad Trojanski konj:
 - modul za izdvajanje karakteristika može biti tako napadnut da proizvede unapred definisan set karakteristika (u nekom trenutku i pod određenim uslovima) i njima zameni karakteristike ulaznog signala;
 - napad na moduo za poređenje je takav da se lažno proizvede visok ili nizak skor poređenja što direktno utiče na modul za donošenje odluka, kao i na sam moduo za donošenje odluka gde se postiže generisanje željene odluke;
- 3) Napad na komunikacione kanale čiji je cilj da se presretnu karakteristike i to pre modula za poređenje, i odmah po izlasku iz tog modula radi promene istih;

- 4) Napad na bazu gde se čuvaju šabloni uzeti u postupku registracije; ovde je pretnja neautorizovana modifikacija jednog ili više šablona, čime se može postići lažno predstavljanje ili makar uskraćivanje određenih usluga korisniku koji na njih ima pravo
- 5) Vrlo važna pretnja gde se može promeniti odluka poslednjeg modula a u skladu sa kojom se definiše ponašanje aplikacije;
- 6) Često zanemarena pretnja sigurnosti, koja je i izuzetno važna, je prilikom postupka registracije. Svaki neautorizovani pristup ovom procesu može da prouzrokuje ozbiljne posledice po sigurnost. Naime može se registrovati lažni korisnik, ili pravom korisniku promeniti podaci, tako da je nadgledanje ovog procesa od kritičnog značaja za sigurnost celog sistema.



Slika 4. Vrste napada na određene tačke biometrijskog sistema

„Brute force“ napadi

Ukoliko napadač ima vremena i mogućnosti (što je slučaj u udaljenim nenadgledanim aplikacijama) da generiše i pruži sistemu veći broj šablona u pitanju je klasičan napad silom (*brute-force-attack*) koji je karakterističan za sisteme zaštićene šiframa. U slučaju biometrijskog sistema teže je izvršiti ovakav napad, zbog ne tako lakog generisanja biometrijskih šablona, ali je ipak moguće. Koliko je sistem zaštićen od ovakvih napada direktno zavisi od projektovanih grešaka FAR i FRR. Pokazano je da sistem projektovan sa FAR od 0,001% ima verovatnoću da bude prevaren u proseku 1 od 100000 pokušaja, što odgovara sigurnosti koja se ima sa šifrom od 5 znakova [9]. Pri tome treba voditi računa da je neuporedivo teže generisati 100000 biometrijskih šablona u odnosu na klasičnu šifru od 5 znakova (i u pogledu upotrebljenih resursa kao i vremena).

5. SPECIFIČNE PRETNJE U BIOMETRIJSKIM SISTEMIMA

Pretanja koja je karakteristična samo za biometrijske sisteme je napad tzv. lažnom biometrikom (*fake biometrics*).

Impersonation napadi: slučaj kada se senzoru predstavlja lažna biometrika. Npr. lažni prst, falsifikuje se potpis ili se na licu ima maska. Najnezaštićenije na ovu vrstu napada su lice i glas, ali su u praksi poznati slučajevi gde je sistem prevaren lažnim otiskom, pa čak i okom [4].

Replay napadi su u stvari lažno prijavljivanje prethodno dobijenih (ukradenih) biometrika ili njihovih karakteristika i dobijenih šablona, pri čemu se zaobilazi senzor.

Razvijaju se različiti metodi za sprečavanje ovakvih napada i to od kriptografije, zatim izazov-odgovor (*challenge/response*) sistem kojim se obezbeđuje prisustvo osobe u

trenutku davanja biometrijskih podataka, pa do istovremenog korišćenja više biometrijskih karakteristika u multimodalnim biometrijskim sistemima.

Razna istraživanja su sprovedena sa ciljem da se ustanovi koliko su postojeći biometrijski sistemi osetljivi na ovakav vid napada. Tako su prijavljeni u praksi provereni razni vidovi 'krađe identiteta' [3]:

- Llice – eksperimenti su pokazali da snimak lica (bez znanja subjekta koji je u pokretu) ako se stavi ispred kamere za prepoznavanje često ima za posledicu prihvatanje identiteta;
- Otisak – Matsumoto je sa grupom svojih saradnika dokazao da model otiska napravljen od silikona i želatina, a na osnovu pravog ili latentnog otiska skinutog recimo sa čaše, kod komercijalnih sistema za prepoznavanje preko otisaka u 80% slučajeva ima za posledicu prihvatanje identiteta. Takođe je pokazao da se relativno lako mogu prevariti i dodatni sistemi koji proveravaju 'živost' podatka [4];
- Iris – u Nemačkoj je takođe uspešno prevaren sistem za identifikaciju preko irisa tako što je korišćena odštampana slika ljudskog oka

U biometrijskim sistemima se javlja specifičan problem koji se ne pojavljuje u sistemima koji koriste *knowledge&possession* metode. To je zamena kompromitovane biometrike. Krađa identiteta u slučaju biometrijskih sistema ima nesagledive posledice. Naime ako se desi da vam neko ukrade karticu ili lozinku, jednostavno ćete poništiti istu i dobiti drugu koja je različita. Ali ukoliko je iz bilo kog razloga biometrika kompromitovana onda je to zauvek. Naime čovek poseduje ograničen broj biometrijskih podataka (jedno lice, 10 prstiju, 2 oka...). Još ako je biometrijski podatak korišćen u više različitih aplikacija, to znači da su svi ti podaci dostupni onome ko je došao u posed biometrijske karakteristike.

Mora se naglasiti da krađa identiteta (ili zloupotreba biometrijskih podataka) ne mora biti delo pojedinca. Naime korporacije mogu koristiti biometrijske podatke radi uskraćivanja određenih prava bivšim radnicima, ili onima koji su već registrovani u policijskim biometrijskim bazama i sl. Vladine agencije mogu koristiti ove podatke radi uskraćivanja prava i sloboda licima za koje to smatraju potrebnim npr. traženim teroristima (čak i mimo zakonskih propisa).

6. BIOMETRIKA I PRIVATNOST

Privatnost tumačimo mogućnošću da živimo slobodni bilo kog uticaja, da ostanemo autonomni i da sami kontrolišemo pristup ličnim podacima [9]. Danas se biometrijski sistemi koriste u svim oblastima života, od finansijskih, medicinskih, poslova komunikacija pa do različitih poslova osiguranja, zaštite, vladinih agencija, kriminalistike i forenzike.

Mnogi su razlozi otpora pojedinca upotrebi ovih sistema. Tako neke biometrike (otisak, lice, DNK) nose negativnu konotaciju upotrebe u kriminalistici. Druge se opet kulturološki doživljavaju nedostojnim čoveka. Religiozni aspekt se takođe ne sme zanemariti gde se spominje "znak zveri" i citira Otkrovenje 13:16-17 .

Kod problema privatnosti razmatramo 3 aspekata:

1. nenamerno proširivanje funkcionalnog delokruga biometrijskih sistema – pošto su biometrijske karakteristike u suštini biološke mogu se iz njih dobiti i dodatne

informacije (npr. medicinske) koje se mogu iskoristiti za diskriminaciju pojedinca ili grupa;

2. nenamerno proširivanje aplikativnog polja rada – dolazi do neželjene identifikacije u slučajevima kada osoba zakonski koristi drugi identitet (zbog bezbednosti i sl.); štaviše mogu se povezati informacije vezane za ponašanje, navike i sklonosti pojedinca dobijene iz više različitih aplikacija čime se postiže značajna moć nad njim;
3. skriveno prepoznavanje – biometrijske karakteristike nisu tajne, moguće ih je dobiti bez saglasnosti osobe. Ona je samim tim uskraćena za privatnost i anonimnost na koju imaju pravo

Ili ako ovo sistematizujemo dobićemo da biometrija ugrožava:

- *privatnost osobe* – u odnosu na način na koji se zahteva uzimanje biometrijskih podataka ;
- *privatnost ličnih podataka* – koji se takođe zahtevaju prilikom registracije; sakupljanjem i razmenim podataka daje se mogućnost potpune kontrole nad populacijom čiji se biometrijski podaci imaju;
- *privatnost slobodnog ponašanja* – pošto se uz pomoć biometrike mogu pratiti radnje i ponašanje osobe, organizacije mogu praćenjem ponašanja da pokušaju da spreče neželjene akcije. Međutim mogu i da dele ove informacije sa drugima npr. radi odgovarajućeg nastupa na tržištu, ili sa vladinim organizacijama i sl.
- *Nemogućnost anonimnosti i prijavljivanje pod pseudonimom*. Predstavlja jako oružje za razne agencije i vlade ali i neiscrpni izvor mogućih zloupotreba od istih;

Tu je i problem crnog tržišta baza biometrijskih podataka. Tako bi se slike irisa mogle koristiti za analizu u medicini (iridologija), pa se može zamisliti koliko bi ovakva baza mogla vredeti nekim kompanijama ili npr. osiguravajućim društvima.

Oni koji se zalažu za privatnost ističu potrebu da biometrijska baza bude decentralizovana, još bolje i da je nema tj. da svaki uzeti uzorak kao šablon bude sačuvan na kartici koja je u isključivom posedu pojedinca koji je biometrijski podatak i dao. Naravno tu se javlja problem zamene ukradene ili oštećene kartice, ali se određena razmišljanja u ovom pravcu moraju ozbiljno uzeti u obzir [12].

Možemo reći da su biometrijske tehnologije stvorile okruženje u kojem razne vladine agencije i korporacije mogu da steknu enormnu moć nad pojedincem. Prihvatanje “imperativa tehnologije“, dopušta mogućnosti velikih zloupotreba sa nesagledivim posledicama po privatnost. Mora se zato prvo urediti oblast korišćenja biometrike na sledeći način:

- tehnološka regulativa koje će se pridržavati svi proizvođači biometrijske opreme;
- zakonska regulativa koja će na novi način urediti ovu oblast;
- moratorijum na uvođenje biometrijske tehnologije dok se ne regulišu uslovi i zaštititi privatnost pojedinca

7. ZAKLJUČAK

Najslabije sigurnosne tačke svakog sistema su autentizacija korisnika. Biometrija koja je donela izuzetan napredak u ovoj oblasti. Međutim i ovi sistemi imaju svojih ograničenja sa određenim implikacijama po sigurnost. Postoje i velike sumnje u pogledu zloupotrebe biometrike, kao i njenog uticaja na privatnost. Donošenje zakonskih propisa u ovoj oblasti, definisanje standarda i pravila ponašanja mogu delimično razvejati ove sumnje. Međutim

činjenica da je biometrika jedinstveni i univerzalni identifikator koji i bez saglasnosti subjekta može povezati njegove različite lične podatke, kao i mogućnost namernog zaobilaženja zakonskih regulativa (delimično suspendovanje ljudskih prava i sloboda u SAD-u posle napada 11.09.2001 godine tzv. *Patriot Act*) nalažu detaljnu analizu i odeđivanje oblasti stvarne potrebe njenog korišćenja, kao i primene dodatnih tehnika radi sprečavanja zloupotreba i očuvanja privatnosti.

8. LITERATURA

- [1] Bolle R.M., Connell J.H., Ratha N.K., "Biometric perils and patches", *Pattern Recognition*, Vol. 35, pp. 2727-2738, 2002
- [2] Clarke R., "Biometrics and Privacy", available at <http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html>
- [3] Forte Dario, "Biometrics: Future Abuses", *Computer Fraud & Security*, Vol. 2003, Issue 10, pp. 12-14, 2003
- [4] Matsumoto T., Matsumoto H., Yamada K., Hoshino S, "Impact of Artificial Gummy Fingers on Fingerprint Systems", *Proceedings of SPIE* Vol. 4677, pp. 275-289, San Jose, USA, 2002
- [5] Miller, B., "Vital signs of identity", *IEEE Spectrum*, Vol. 31, No. 2, pp. 22-30, February 1994.
- [6] Phillips, P.J., R.M. McCabe, and R. Chellappa, "Biometric image processing and recognition", *Proc. 9th European Signal Proc. Conf. EUSIPCO-98*, Vol. I, pp. 1-8, Rhodes, Greece, 8-11 Sept. 1998.
- [7] Popović B., Popović M., "Policijska prevencija kriminala upotrebom AFIS-a Automatskih Sistema za Identifikaciju preko otisaka", *Zbornik radova sa savetovanja Mesto i Uloga Policije u Prevenciji Kriminaliteta*, pp. 518-532, Beograd 2002.
- [8] Popović M., "Biometrijski sistemi za identifikaciju ličnosti za upotrebu u policijskoj prevenciji kriminaliteta", *Zbornik radova sa savetovanja Mesto i Uloga Policije u Prevenciji Kriminaliteta*, pp. 533-547, Beograd 2002.
- [9] Prabhakar S., Pankanti S., Jain A.K., "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy Magazine*, Vol. 1, No.2, pp. 33-42, 2003.
- [10] Ratha N.K., Connell J.H., Bolle R.M., "Biometric break-ins and band-aids", *Pattern Recognition Letters*, Vol. 24, pp. 2105-2113, 2003.
- [11] Ross A., Jain A.K., "Information fusion in biometrics", *Pattern Recognition Letters*, Vol. 24, pp. 2115-2125, 2003.
- [12] Tomko G., "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?", *Privacy Laws & Business 9th Privacy Commissioners/Data Protection Authorities Workshop*, Spain, September 1998 available at www.dss.state.ct.us/digital/tomko.htm.

BIOMETRIC SYSTEMS – USE AND ABUSE

Brankica Popović¹, Miodrag Popović²

¹Police Academy, Humska 22 Belgrade
e-mail: cica@ptt.yu

²Faculty of Electrical Engineering, University of Belgrade
Bulevar kralja Aleksandra 73, 11120 Belgrade
e-mail: pop@el.etf.bg.ac.yu

***Abstract:** There is a great interest in use of biometric identification systems. They have some advantages over traditional knowledge&possession based systems. It is necessary to emphasis their limitations regarding security and different sources of attack. Privacy aspect is the issue in inadequate use of biometric systems.*

Key words: biometrics, identification, abuse, security