Suvremene tehnologije

Biometrijske metode u sigurnosnim sustavima

Autori: Krešimir Delač, dipl.ing., doc.dr.sc. Mislav Grgić, dipl.ing., prof.dr.sc. Sonja Grgić, dipl .ing.
kdelac@ieee.org

Provjera ili određivanje nečijeg identiteta do sada se temeljila na nečemu što osoba posjeduje (ključ, magnetska ili čip kartica) ili na nečemu što zna (zaporka). Ovaj se pristup pokazao nespretnim jer je ključ lako izgubiti, a zaporku zaboraviti. Kako bi se postiglo pouzdanije određivanje ili provjera nečijeg identiteta, u posljednje se vrijeme počela koristiti biometrija (biometrika). Riječ dolazi od dviju grčkih riječi: *bios* - život i *metron* - mjera. Biometrija je provjera ili određivanje identiteta na temelju nečega što osoba *jest*, a ne nečega što posjeduje ili zna. Detaljnija i točnija definicija bila bi: *automatsko određivanje ili provjera nečijeg identiteta putem mjerenja i uspoređivanja njegovih fizičkih osobina i/ili karakteristika ponašanja*. Da bi se neka karakteristika smatrala pogodnom za korištenje kao biometrijski identifikator, ona mora posjedovati sljedeće osobine:

1. *univerzalnost* - svi je moraju posjedovati
2. *jedinstvenost* - bilo koje dvije osobe moraju se moći dovoljno razlikovati pomoću te karakteristike
3. *trajnost* - karakteristika mora biti ista tijekom dugog razdoblja (ne smiju na nju utjecati bolesti ili starenje)
4. *mjerljivost* - mora se moći lako 'izmjeriti' (uzeti uzorak).

Sada možemo definirati i biometrijski sustav: *Biometrijski sustav je sustav za prepoznavanje uzoraka koji prepoznaje osobu na temelju vektora značajki dobivenog mjerenjem (uzorkovanjem) neke fizičke osobine i/ili karakteristike ponašanja te osobe.*

Režimi rada

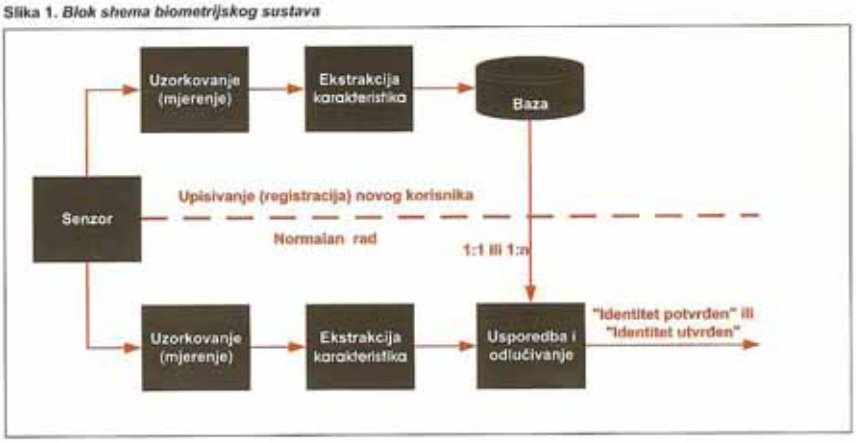
Ovisno o načinu primjene, biometrijski sustav može raditi u dva režima: 1) *provjera* (verifikacija, autentikacija) identiteta ili 2) *utvrđivanje* (identifikacija) identiteta. Režim provjere zahtijeva da osoba na neki način 'kaže' sustavu tko je, a sustav onda radi tzv. provjeru *jedan-na-jedan* i vraća rezultat koliko je neka karakteristika te osobe slična ranije pohranjenoj karakteristici pod tim imenom. Ustvari, sustav nam daje vjerojatnost da izmjerena i pohranjena karakteristika pripadaju istoj osobi, ili grublje, daje nam odgovor na pitanje: 'Jesam li ja onaj koji tvrdim da jesam?' Režim identifikacije je puno tehnički zahtjevniji proces i u njemu sustav radi tzv. *jedan-na-više* provjeru. Sustav sada vraća koliko je neka karakteristika slična svakoj pohranjenoj u bazi (radi tzv. *line-up*). Najviši rezultat imat će osoba čija je karakteristika pohranjena u bazi najsličnija nepoznatoj osobi, ili opet grublje, sustav daje odgovor na pitanje: 'Tko sam ja?'

Dijelovi biometrijskog sustava

Svaki biometrijski sustav u načelu se sastoji od četiri osnovna dijela: 1) senzor koji mjeri (uzorkuje) određenu biometrijsku karakteristiku, 2) modul za izvlačenje (ekstrakciju) karakteristika, 3) modul za usporedbu i odlučivanje (s ranije pohranjenim karakteristikama) i 4) baza podataka u koju se pohranjuju karakteristike. Kod upisivanja novog korisnika u sustav (engl. *enrollment*), sustav uzima izmjerenu karakteristiku, izvlači iz nje osobine i sprema ih u bazu (gornji dio slike 1.). Kod normalnog rada sustava, iz izmjerene se karakteristike izvlače osobine i uspoređuju se s prethodno pohranjenim vrijednostima (u modulu za usporedbu i odlučivanje).

Pitanje koje bi svakome tko malo razmisli o biometrijskim sustavima (npr. o sustavu temeljenom na raspoznavanju lica) moglo pasti na pamet je: 'A što ako ja njemu pokažem sliku nečijeg lica?' Jedna od glavnih prednosti biometrijskih sustava je upravo da mogu provjeriti je li korisnik uopće živ. Sustav temeljen na raspoznavanju lica može korisnika tražiti da se okrene npr. za 90°, pratiti taj pokret i tako eliminirati eventualni pokušaj varanja pomoću slike. Kod sustava temeljenih na šarenici oka, promjenom uvjeta osvjetljenja šarenica se steže i širi, čime sustav 'zna' da je 'oko živo'. Mnogi sustavi koji zahtijevaju kontakt nekog dijela tijela sa sustavom mogu mjeriti i temperaturu tog dijela tijela, otkucaje srce i sl.

Slika 1. ***Blok shema biometrijskog sustava***



Još jedna prednost biometrijskog sigurnosnog sustava je mogućnost tzv. negativnog raspoznavanja. Primjena je većinom u policijske ili forenzičke svrhe. U biti, sustav je u mogućnosti otkriti stvarni identitet osobe koja se pokušava lažno predstaviti i odgovoriti na pitanje: 'Jesam li ja onaj tko tvrdim da *nisam*?' (da ostanemo dosljedni terminologiji iz prethodnog poglavlja).

Pregled metoda - mjerenje fizioloških osobina

U ovom dijelu dajemo kratak pregled biometrijskih metoda. Napominjemo da su neke još u fazi znanstvenog istraživanja (recimo metode temeljene na mirisima ili hodu), dok se mnoge već i komercijalno koriste (što nipošto ne znači da je znanstveno istraživanje tih metoda završeno i da one rade sa stopostotnom učinkovitošću).

Otisak prsta (engl. *fingerprint*). Otisak prsta je uzorak izbočina i udubljenja koji se nalaze na površini jagodice prsta ruke. Taj se uzorak razvije tijekom prvih sedam mjeseci razvoja fetusa i ostaje nepromijenjen cijeli život (osim ako ga ne promijeni bolest ili ozljeda). Otisci prsta identičnih blizanaca su različiti kao i otisci svakog pojedinog prsta iste osobe. Kao sredstvo identifikacije koristili su ih još Kinezi, a njihova primjena u forenzičke svrhe automatizirana je 1960-ih godina. U početku se otisak prsta uzimao tako da se stvarala slika tintom, a prepoznavanje se radilo ručno – traženjem i uspoređivanjem karakterističnih dijelova svakog pojedinog otiska. Danas se koriste kompaktni optički senzori koji osim što daju digitaliziranu sliku uzoraka izbočina i udubljenja, također mogu mjeriti i temperaturu vrha prsta (koji dolazi u direktan kontakt sa senzorom) i puls, te na taj način provjeriti je li korisnik živ. Problemi kod uzimanja otiska prsta javljaju se ako je senzor prljav (prašina i sl.), ako je vrh prsta suh ili jako vlažan. Karakteristike koje se izdvajaju iz slike otiska sastoje se iz pozicija i orijentacije karakterističnih dijelova otiska (engl. *minutiae*). Prepoznavanje se obavlja uspoređivanjem takvih dvodimenzijskih uzoraka s pohranjenim predloškom.

Geometrija dlana (engl. *hand geometry*). Geometrija dlana je, pored otiska prsta, jedna od prvih biometrijskih metoda koja se koristila. Bit ove metode je mjerenje dimenzija prstiju, mjerenje oblika i veličine dlana, kao i utvrđivanje lokacije zglobova. Geometrija dlana je privlačna metoda zbog svoje relativne jednostavnosti implementacije i otpornosti na utjecaje vlage i sl. Međutim, nije pogodna za uporabu u sustavima visoke sigurnosti jer nije jako diskriminatorna i ne bi se trebala koristiti u sustavima s velikim brojem korisnika. Režim rada idealan za geometriju dlana kao biometriju jest verifikacija (dolazak radnika na posao, prijenosna računala), dok identifikacija kao režim rada ne dolazi u obzir. Limitirajući faktori su deformacije nastale uslijed artritisa ili nošenje nakita. Mogući problem je i činjenica da nekim ljudima smeta doticanje dlanom površina koje su i mnogi drugi ljudi doticali.

Otisak dlana (engl. *palmprint*). Kao i vršak prsta, ljudski dlan također ima jedinstven uzorak bregova i brazdi. Budući da je površina na kojoj su ti uzorci veća, smatra se da je ovaj uzorak čak bolji za prepoznavanje od otiska prsta.

Nedostatak je što je zbog veće površine koju je potrebno uzorkovati i senzor nužno veći, te samim time i skuplji. Kombiniranjem ove metode s geometrijom dlana dobiva se vrlo precizan i djelotvoran biometrijski sustav.

Lice (engl. *face recognition*). Raspoznavanje ljudi na temelju lica zadatak je koji svaki čovjek svakodnevno obavlja. Pokušati dati računalu tu mogućnost bilo je sasvim prirodno. Metoda je neinvazivna i naišla je na dobar prijem kod šire javnosti i zbog toga se upravo ova metoda odabrala za implementaciju na putne isprave (Europska unija bi ovo trebala implementirati do kraja 2008. godine). Lice je trodimenzijski objekt koji je prilikom mjerenja (uzorkovanja) izložen raznim uvjetima osvjetljenja, što otežava cijeli proces. Mijenjanje izraza lica i orijentacija u prostoru dodatno otežava raspoznavanje. Raspoznavanje se najčešće temelji na dvodimenzijskoj slici tog objekta iako je moguće i uzimanje trodimenzijskog uzorka pomoću laserske kamere. Prvi zadatak sustava za raspoznavanje lica je detektirati lice u snimljenoj slici. Ako se koristi videozapis, onda se lice (osim detektiranja) mora i moći pratiti kroz zapis. Nakon što je lice detektirano, obavlja se normizacija (izjednačavanje histograma, ispravljanja utjecaja rasvjete, razne geometrijske transformacije i sl.) kako bi se dobilo tzv. kanonsko lice iz kojeg se potom izvlače karakteristike na osnovi kojih će se obavljati raspoznavanje. Raspoznavanje lica pomoću slika uzetih u kontroliranim uvjetima (u nekoj prostoriji) prilično je dobro riješeno, a trenutačna tema znanstvenih istraživanja je raspoznavanje lica iz slika uzetih na otvorenom prostoru pod prirodnom rasvjetom običnom nadzornom kamerom relativno loše rezolucije (dakle, u nepovoljnim uvjetima).

Infracrveni termogram (engl. *infrared thermogram*) **lica, ruke ili uzorka vena na ruci**. Svako ljudsko tijelo zrači toplinu u točno određenom uzorku i taj je

uzorak moguće snimiti infracrvenom kamerom. Smatra se da je taj uzorak jedinstven za svaku osobu. Snimanje infracrvenom kamerom je neinvazivna metoda, ali problem se javlja ako osoba stoji kraj nekog drugog objekta koji zrači toplinu. Javlja se i problem privatnosti jer je ovo izuzetno pogodna metoda za tajno prepoznavanje. Slična tehnologija koja koristi skoro-infracrveno snimanje (engl. *near infrared imaging*) koristi se za prepoznavanje pomoću strukture vena na pozadini šake ili termograma lica. Problemi kod svih ovih metoda su orijentacija u 3D prostoru i cijena infracrvenih senzora.

Šarenica oka (engl. *iris*). Kompleksni uzorak šarenice oka idealan je za prepoznavanje i biometriju. Uzimanje uzorka je manje 'neugodno' od mrežnice jer je šarenica vidljiva i s udaljenosti od nekoliko metara. Širenje i stezanje šarenice koje se javlja kod promjena osvjetljenja idealno je za provjeru je li osoba koja se prepoznaje živa. Šarenice identičnih blizanaca su različite, izuzetno je teško kirurški promijeniti šarenicu, a umjetne šarenice se lako prepoznaju.

Mrežnica oka (engl. *retina*). Karakteristike se izvlače iz rasporeda žila u mrežnici oka. Taj se raspored razlikuje od osobe do osobe i za svako oko na istoj osobi. Budući da su žile zaštićene samim okom, teško je taj uzorak mijenjati ili replicirati, te ta osobina čini ovu metodu jednom od sigurnijih. Uzimanje uzorka zahtijeva suradnju osobe čiji se uzorak uzima jer on mora pogledati u jedan otvor (leću). Metoda je upitno prihvatljiva (što se tiče privatnosti) jer se može otkriti eventualna bolest oka. Mana je i to što se oko skenira laserskom zrakom, što mnogima izaziva nelagodu.

Uho (engl. *ear*). Pretpostavlja se da bi oblik uha i struktura hrskavičnog tkiva mogla biti dovoljno različita od osobe do osobe i pogodna za prepoznavanje. Metode statističkog prepoznavanja uzoraka dale su lošije rezultate nego kada su primijenjene na prepoznavanje lica. Preporučena metoda je mjerenje udaljenosti karakterističnih točaka na uhu do neke fiksne točke u sredini uha. Ova metoda je pogodna za primjene u sustavima gdje nije potrebna velika sigurnost.

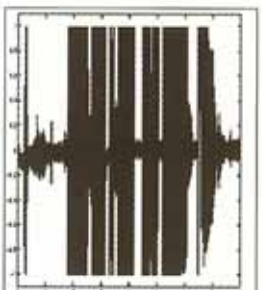
Tjelesni miris (engl. *odor*). Svako tijelo širi oko sebe miris (mogli ga mi osjetiti ili ne) koji je karakterističan za njegov kemijski sastav, i taj bi miris mogao služiti za prepoznavanje. Uređaj bi se trebao sastojati od niza senzora od kojih je svaki osjetljiv na neku komponentu. Metoda je prilično nesigurna jer bi intenzivan miris parfema mogao značajno utjecati na prepoznavanje.

DNK (DNA). Deoksiribonukleinska kiselina je vjerojatno najpouzdanija metoda. Ipak, primjena DNK za prepoznavanje ograničena je za forenzičke svrhe zbog barem dva razloga: 1) metoda je vrlo spora jer je potrebna složena kemijska analiza, 2) narušavanje privatnosti - lako je uzeti nečiju DNK iz koje bi se mogli vidjeti detalji o nečijem zdravstvenom stanju.

Pregled metoda - mjerenje karakteristika ponašanja

Potpis (engl. *signature*). Prepoznavanje osoba pomoću njihovog potpisa jedna je od najstarijih metoda uopće. Uzimanje uzorka za ovu metodu prepoznavanja podrazumijeva suradnju osobe koju se prepoznaje i uporabu instrumenta za pisanje i podloge u kojoj je senzor. Pisanje je karakteristika ponašanja i kao takva može se mijenjati kroz vrijeme i na nju mogu utjecati fizičke ili emocionalne promjene (npr. trešnja ruke pod velikim stresom ili sl.). Osim samog oblika potpisa, može se mjeriti i pritisak instrumenta za pisanje na podlogu i brzina (dinamika) pisanja. Ova metoda pogodna je samo za rad u režimu verifikacije.

Glas (engl. *voice*). Posebnosti glasa posljedica su fizičkih karakteristika kao što su oblik vokalnog trakta, usta, nosnih šupljina i usana te drugih dijelova koji sudjeluju u proizvodnji zvuka. Kao i kod većine biometrijskih metoda, osobine izvučene iz nečijeg glasa uspoređuju se s ranije pohranjenim osobinama. Osobine koje se koriste najčešće su mjerenje formanata ili karakteristika zvuka koje su jedinstvene za nečiji vokalni trakt. Algoritmi za uspoređivanje uzoraka (osobina) slični su kao i kod prepoznavanja lica. Metoda je jednostavna za implementaciju jer nije potrebna posebna oprema (običan mikrofon je dovoljan). Sustav traži od korisnika da izgovori neku frazu na osnovi koje se stvara tzv. *voice print* koji je pohranjuje u sustav. Istu frazu potrebno je ponoviti i prilikom prepoznavanja. Sustav je lako prevariti tako da se snimi nečiji glas kako izgovara zadanu frazu. Stoga sofisticiraniji sustavi traže određenu reakciju od korisnika (npr. da ponovi neki slučajan niz brojeva koje sustav sam izabere). Vrlo je malo sustava koji ne ovise o izgovorenom tekstu.



Hod (engl. *gait*). Analiza specifičnog načina hoda osobe jedna je od novijih biometrijskih metoda i potrebno je još mnogo istraživanja da bi se ova kompleksna prostorno-vremenska biometrijska metoda pustila u komercijalnu uporabu. Pogodna je samo za primjene u sustavima s nižim stupnjem sigurnosti. Način

hoda može se mijenjati tijekom vremena zbog promjene tjelesne težine ili bolesti (naročito zbog oštećenja mozga). Uzimanje uzorka je jednostavno (obično snimanje kamerom), što je razlog zbog kojeg je ova metoda prihvatljiva.

Dinamika tipkanja (engl. *keystroke dynamic*). Svaka osoba tipka po tipkovnici na karakterističan način. Teško je jako precizno ljude razlikovati na osnovi ove karakteristike, ali čini se da je ona dovoljna za rad u režimu verifikacije za sustave s niskim stupnjem sigurnosti.

Zaključak

Na kraju, svakako je važno naglasiti da svaki biometrijski sustav ima svojih prednosti i mana te da ne postoji jedan univerzalni sustav koji će dobro raditi u svakoj primjeni. Nijedan sustav nije 'optimalan' za sve primjene. Upravo zbog te činjenice u posljednje se vrijeme sve više istražuju različiti modeli integracije više biometrijskih metoda u jedan sustav. Pokazalo se da takvi sustavi mogu prevladati neka ograničenja sustava temeljenih na samo jednoj metodi.

Budućnost biometrijskih sustava kao osnovnog dijela sigurnosnih sustava zajamčena je. Osim što se smanjuje potreba za pamćenjem brojnih zaporki i PIN-ova, biometrijski sustavi daleko su manje podložni malicioznim napadima. Iako se na prvi pogled ne čini tako, biometrijske metode su i puno brže od tradicionalnih sigurnosnih metoda. Pomislite samo koliko vam treba da nađete, izvadite i uporabite ključ te otvorite vrata (istraživanja kažu, u prosjeku desetak sekundi). Dobar sustav temeljen na raspoznavanju šarenice oka prepoznat će vas i otvoriti ta ista vrata za manje od tri sekunde.

Problemi koje je još potrebno riješiti svakako su dodatna automatizacija i veća točnost raspoznavanja (npr. najtočniji sustavi za raspoznavanje lica rade s oko 90% točnosti i to u idealnim uvjetima – frontalna slika lica, uzeta u uvjetima idealne rasvjete). Sustavi za raspoznavanje otisaka prsta točniji su, ali imaju velikih problema s uzimanjem uzoraka, što čini i razvoj senzora temom koju je potrebno dodatno istražiti. Trenutačno je najveći problem standardizacija – dva sustava različitih proizvođača, temeljena na istoj metodi, za sada ne mogu međusobno komunicirati. Što se tiče prihvatljivosti pojedine metode u široj javnosti, svakako će se morati posebna pozornost posvetiti zaštiti privatnosti (naročito kod razvoja sustava) te je na razvojnim inženjerima najveća odgovornost. ■

Literatura

[1] Delac, K., Grgic, M., "A Survey of Biometric Recognition Methods", *Proceedings of the 46th International Symposium Electronics in Marine*, ELMAR-2004, Zadar, Croatia, 16-18 June 2004, pp. 184-193

[2] Jain A, Ross A., Prabhakar S., "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 4-19, January 2004

[3] Matyas V., Riha Z., "Toward Reliable User Authentication through Biometrics", *IEEE Security & Privacy*, Vol. 1, No. 3, May/June 2003, pp. 45-49