

CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Biometrija

CCERT-PUBDOC-2006-09-167

CARNet CERT u suradnji s **LS&S**

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža i sustava**.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

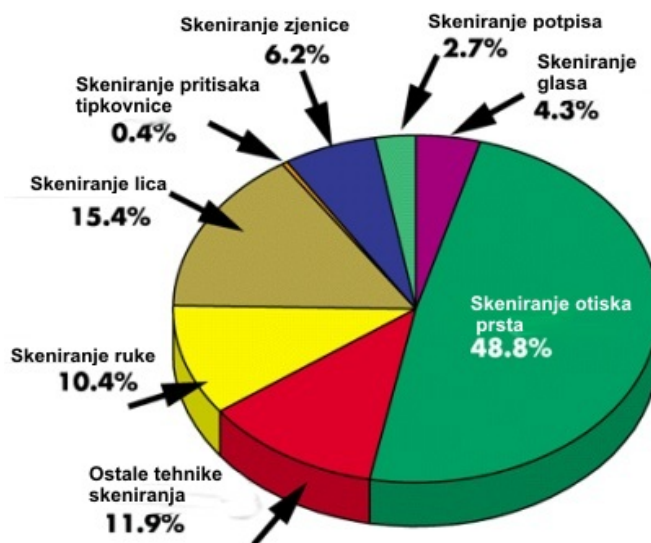
1. UVOD	4
2. OSNOVNI PRINCIPI RADA BIOMETRIJSKIH TEHNIKA	5
2.1. DIGITALIZACIJA KAO OSNOVA BIOMETRIJE	5
2.1.1. Fourierove transformacije	5
2.2. UMJETNA INTELIGENCIJA	5
3. VRSTE BIOMETRIJSKIH METODA	6
3.1. FIZIČKA BIOMETRIJA	6
3.1.1. Čitanje DNK zapisa	6
3.1.2. Skeniranje rožnice	7
3.1.3. Prepoznavanje lica	7
3.1.4. Geometrija šake	8
3.1.5. Provjera vena	8
3.1.6. Otisak prsta	9
3.2. BIOMETRIJA PONAŠANJA	9
3.2.1. Prepoznavanje glasa	9
3.2.2. Prepoznavanje rukopisa ili potpisa	10
3.2.3. Dinamika tipkanja	10
3.2.4. Dinamika hoda	11
3.2.5. Dinamika mirisa	11
3.3. MULTIMODALNA BIOMETRIJA	12
3.4. USPOREDBA BIOMETRIJSKIH TEHNIKA	12
4. ZAKLJUČAK	14
5. REFERENCE	14

1. Uvod

Biometrija (grč. *bios* – život, *metron* – mjera) predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi temeljeno na jednoj ili većem broju njihovih fizičkih i ponašajnih karakteristika. U informatičkoj tehnologiji se biometrijska autentikacija odnosi na tehnologije koje mjere i analiziraju fizičke (otisci prstiju, rožnica oka, prepoznavanje lica i sl.) i ponašajne karakteristike (rukopis, tipkanje, hod i sl.) čovjeka. Iako se biometrija prvenstveno koristi za potrebe autentikacije, ista se primjenjuje i u drugim područjima kao što je prepoznavanje korisnikovog govora u svrhu bržeg pisanja.

Biometrija objedinjuje korištenje specijalnih uređaja koji prate određene fizičke ili ponašajne karakteristike te programa koji analiziraju dobivene informacije. Pri tome su sastavni elementi biometrije uzorkovanje (pretvaranje analognog signala u digitalni) kao i umjetna inteligencija. Dobivene informacije se obrađuju u računalu, stvara se umjetna inteligencija, računalo prepoznaje uzorke i uspoređuje se sistem učenja računala s ljudskim mozgom. Cilj je korištenje računala kao posrednika u uzorkovanju, dok programski paket preuzima odluku što će poduzeti s digitaliziranim uzorcima. To obuhvaća sveukupan proces digitalizacije, prepoznavanja uzoraka, umjetne inteligencije, a sve sa ciljem kako bi se računalo unaprijedilo u procesu učenja i kako bi samostalno bilo u stanju upamtiti i koristiti uzorke.

U ovom dokumentu opisani su osnovni principi rada, klasifikacija te međusobna usporedba biometrijskih tehnika.



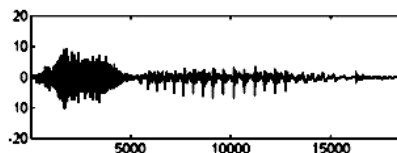
Slika 1: Učestalost korištenja biometrijske tehnologije

2. Osnovni principi rada biometrijskih tehnika

U ovom poglavlju opisani su neki osnovni elementi na kojima se temelje biometrijske tehnike. U prvom redu to je digitalizacija, tj. pretvaranje analognog u digitalne signale, a potom tu je i umjetna inteligencija na kojoj je potrebno temeljiti određene oblike biometrijskih tehnika.

2.1. Digitalizacija kao osnova biometrije

Najvažniji moment u procesu prepoznavanja uzoraka je digitalizacija. Naime za potrebe računalne obrade podatke dobivene skeniranjem i sl. potrebno je prevesti u digitalni format s kojim računalno može raditi. To je proces u kojem se analogni signal pretvara u digitalni te prepoznaje programskom opremom. Što je kvalitetnija oprema, to su veće šanse za prepoznavanje uzorka. Analogni signal se pretvara u digitalni korištenjem elektroničkog DAC (eng. *digital audio-video converter*) uređaja. Sam proces se u suštini sastoji od niza Fourierovih transformacija, kvantizacija i ostalih pojmova koji služe da matematički što vjernije opišu ulazni signal. Nisu svi DAC-ovi jednaki i kvalitetni. DAC se nalazi u sklopovskom senzoru za prepoznavanje uzoraka pa što je senzor kvalitetniji (a time i skuplji), dobiva se bolje uzorkovani uzorak.



Slika 2: Izgled digitaliziranog uzorka

2.1.1. Fourierove transformacije

Brza Fourierova transformacija ili kraće FFT (eng. *Fast Fourier Transformation*) je jedna od najlakših i najkorištenijih tehnika za opisivanje i obradu signala. Radi s relativno malom rezolucijom, a opisivanje i obradu signala se obavlja u digitalnom signalnom procesoru – DSP (eng. *Digital Signal Processor*) pomoću Fourierovih transformacija. Njima se opisuje krivulja uzorka i njegovih harmonika pri čemu se prevode u par sinusnih funkcija. Tehnika je nazvana po Josefu Fourieru.

2.2. Umjetna inteligencija

Umjetna inteligencija je dio računalne znanosti koja se bavi zahtjevima za obavljanje poslova iz domene percepcije, shvaćanja i učenja uzoraka. To je široko područje gdje istraživači nailaze na mnoštvo problema i koriste se raznim metodama kako bi zadovoljili svoje pretpostavke.

Jedan od glavnih zadataka umjetne inteligencije je odrediti kojim će se zadacima baviti i kako će se vrednovati napredak. Ispočetka su se znanstvenici trudili da postignu veću inteligenciju kod programa kao što je npr. kvalitetnije igranje šaha. Skeptici nisu tome vjerovali ali je umjetna inteligencija ostvarivala vidljiv napredak. Već su 60-ih godina postojali programi koji su mogli obavljati turnire u šahu, a 1997 godine je razvijen šahovski sistem „Deep Blue“ u kojem je sudjelovao Gari Kasparov, nepobijeđeni šahist unazad 20 godina.

Istovremeno umjetna inteligencija nastoji napraviti programe koji će razumjeti ljudski govor i koji će moći smisleno komunicirati s ljudima. Umjetna inteligencija je dosad objasnila prirodu problema shvaćanja, i postavila osnovne pretpostavke inteligentnih sustava, a trenutno se radi na razvoju kognitivnih modela koji bi trebali objasniti ljudsku kogniciju.

Umjetna inteligencija kao podloga za biometriju je potrebna zbog dijela zvanog „neuronske mreže“ koji se primjenjuje u analizi signala i slika. Teorijsko ishodište i inspiracija neuronskih mreža je u ljudskom mozgu. Cilj je spajanje sposobnosti ljudi da dobro prepoznaju oblike, lica i glasove i sposobnost računala da izvršava numeričke proračune i radi s velikom količinom podataka na osnovi istih.

3. Vrste biometrijskih tehnika

Biometriju se može definirati kao model identifikacije osobe, baziran na fizičkim karakteristikama ili karakteristikama ponašanja, a odnosi se na nešto što osoba posjeduje ili što osoba zna kako bi izvršila osobnu identifikaciju. Neki autori daju još općenitiju definiciju te definiraju kako se biometrija bavi identifikacijom pojedinaca, temeljenoj na njihovim biološkim karakteristikama ili karakteristikama ponašanja, odnosno da predstavlja svojevrsnu metodologiju za rješavanje identifikacije prema navedenim kriterijima.

U samim počecima izvedbe i upotrebe biometrijskih sustava, prednost je davana fizičkim karakteristikama u odnosu na ponašajne karakteristike. Prevladavalo je mišljenje da fizičke značajke, u odnosu na ponašajne, posjeduju „uočljivost“. Prema tome mišljenju, prevladavalo je i uvjerenje kako su fizičke karakteristike pouzdanije od ponašajnih, jer one imaju tendenciju manjih razlika unutar grupa, nego li to imaju ponašajne karakteristike. U nastavku su navedene glavne biometrijske metode temeljene na fizičkim i ponašajnim karakteristikama.

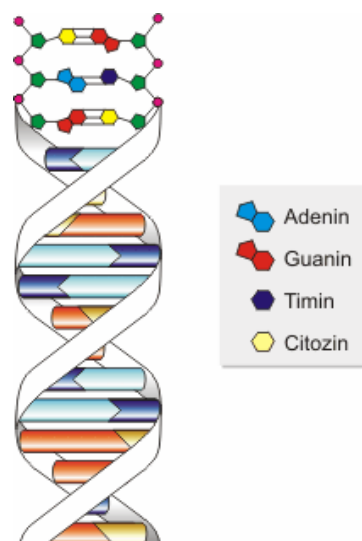
3.1. Fizička biometrija

Fizička biometrija je dio biometrije koja se bavi uzorkovanjem fizionomije ljudskoga tijela i njegovim jedinstvenim karakteristikama. Temelj fizičke biometrije je ljudska fizička jedinstvenost koja omogućuje raspoznavanje ljudi na osnovi iste i korištenje pripadajućih opisa uzoraka za njihovo prepoznavanje. Prepoznati uzorci mogu se koristiti u kombinaciji s ostalim klasičnim zapisima kojima se jedinstveno opisuju osobe.

3.1.1. Čitanje DNK zapisa

Čitanje jedinstvenog DNK - deoksiribonukleinske kiseline (eng. DNA - *Deoxyribonucleic acid*) je relativno nova grana biometrije koja se bavi prepoznavanjem DNK osobe. S pretpostavkom da svaka osoba sadrži sebi svojstveni DNK, pristupilo se mogućnosti izrade svojevrsnog čitača DNK zapisa. Pošto se očita DNK neke jedinke, isti se uspoređuje s pohranjenih zapisom u bazi podataka i na taj je način moguće provoditi autentikaciju korisnika prilikom pristupa nekom sustavu ili prostoru. U kombinaciji s drugim biometrijskih tehnikama može se osigurati vrlo visoki stupanj zaštite i prepoznavanje ukoliko se doista radi o osobi kojoj su pridodana izvjesna ovlaštenja. Ova tehnika se može upotrijebiti i u vojne i civilne svrhe, a postoji velika vjerojatnost da će se u budućnosti podaci o osobnoj DNK pohranjivati i u osobnoj iskaznici.

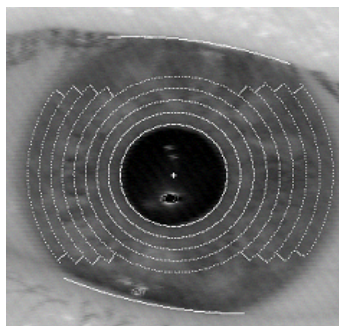
DNK analiza se danas koristi u brojnim sferama kao što su dokazivanje očinstva ili rodbinske povezanosti ili u pravosuđu u kojem su na taj način identificirani brojni kriminalci, ali su i brojni neopravdani osuđeni zatvorenici pušteni na slobodu.



Slika 3: Shematski izgled DNK molekule

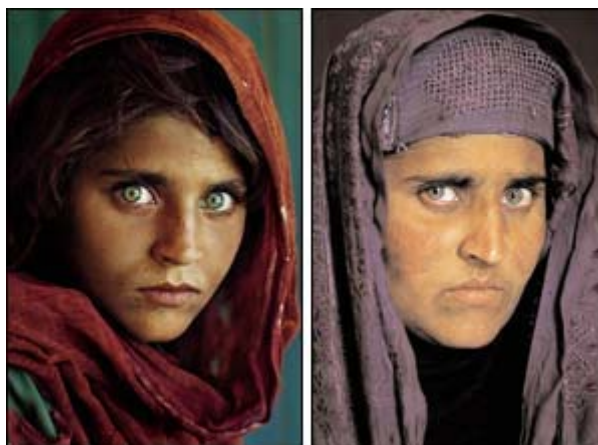
3.1.2. Skeniranje rožnice

Skeniranje rožnice je tehnologija koja se najviše koristi prilikom kontrole ulaska osoba u neki prostor, vođenju statistike posjetitelja, a slične varijante su i u upotrebi prilikom skeniranja korisničkih dokumenata. Prepoznavanje uzorka se odvija pomoću kamere koja snima zapis o korisničkoj rožnici, a pod pretpostavkom da je svaka jedinstvena, može se koristiti u smislu jednoznačnog označavanja. Dobivena slika rožnice se pomoću specijalnih programa opisuje pomoću točaka i daje veću mogućnost jednoznačnog opisivanja uzorka. Pomoću tehnologije opisivanja rožnice moguće ju je opisati s 242 jedinstvenih točaka, dok je npr. u tehnologiji prepoznavanja otiska prstiju predložak moguće opisati s 7 do 22 točaka.



Slika 4: Izgled predloška rožnice opisan točkama

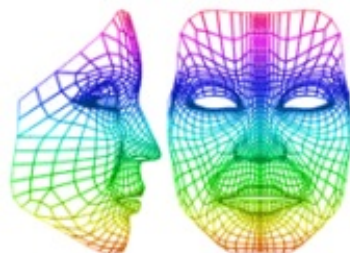
Na sljedećoj slici prikazan je primjer korištenja metode skeniranja rožnice za potrebe autentifikacije djevojke iz Afganistana koja je prvi put snimljena u svojoj mladosti 1984 godine. Svoju popularnost je stekla u svijetu zbog svojih zelenih očiju te ratne situacije u Afganistanu koju je djevojka ocrtavala svojim izrazom lica. Svi pokušaji da se ta osoba kasnije pronađe bili su neuspješni sve do 2001. godine kada je metodom skeniranja rožnice djevojka, tada već odrasla žena, uspješno prepoznata u svom rodnom selu.



Slika 5: Afganistanska djevojka – nekad i sad

3.1.3. Prepoznavanje lica

Ova biometrijska tehnologija je jedna od relativno jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu. Dovoljno je osobno računalo i video kamera. U praksi je dovoljno da osoba prođe pored kamere i da ju sustav zabilježi, dok se prepoznavanje osobe obavlja pomoću prepoznavanja oblika. Pri analizi uzorka zahtijeva se izdvajanje ključnih indikatora, karakterističnog odraza, određivanje relativne važnosti indikatora kroz izbor njegovih koeficijenata i njihovog međusobnog djelovanja. Početna faza prepoznavanja skenira odraz lica u različitim mjerilima i onda ocjenjuje po ključnim indikatorima segmente odraza i pod određenom vjerojatnošću određuje da li se radi o odrazu lica ili okoline. U drugoj fazi se određuje položaj glave što mora uzrokovati određene korekcije prilikom prepoznavanja i zahtijeva korekcije x, y i z osi. Kako bi se što bolje prepoznala osoba, poželjno je posjedovati njen snimljeni uzorak iz većeg broja kutova.

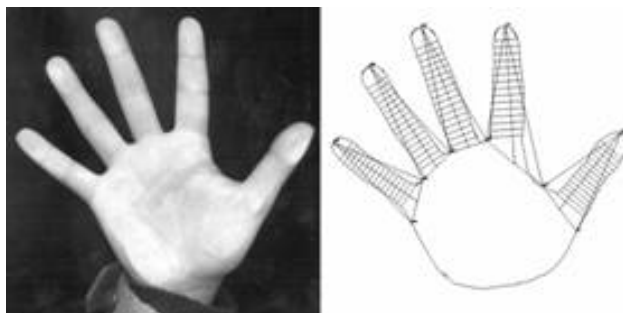


Slika 6: Biometrijski uzorak prepoznavanja lica

Jedna varijanta biometrijske metode koja je slična metodi prepoznavanja lica, je metoda prepoznavanja uha. Naime, oblik uha i struktura hrskavog tkiva na površini uha različiti su među osobama, ali to nije velika jedinstvenost pa ova metoda nije često korištena. Pristupi prepoznavanju uha temelje se na poklapanju vektora duljine izbočenih točaka na površini od lokacije graničnih znakova na uhu.

3.1.4. Geometrija šake

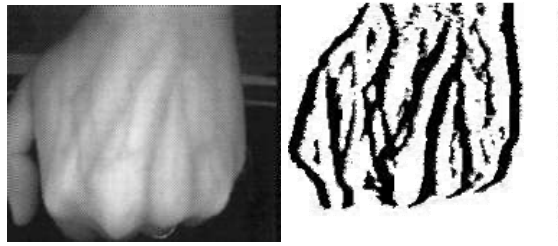
Autentikacija temeljena na raspoznavanju karakteristika šake dostupna je već više od dvadeset godina. Kako bi se postigla autentikacija, sustav može mjeriti fizičke karakteristike šake ili prstiju. To uključuje dužinu, širinu, debljinu i površinu područja šake. Jedna korisna karakteristika je to što neki sustavi zahtijevaju mali biometrijski uzorak (nekoliko okteta). Geometrija šake je postigla prihvatljivost u doseg aplikacija pa se često može uočiti u kontroli fizičkog pristupa u komercijalnim i rezidencijalnim aplikacijama, u vremenskim i poslužiteljskim sustavima te u generalnim aplikacijama za osobnu autentikaciju.



Slika 7: Uzorak šake opisan krivuljama

3.1.5. Provjera vena

Zapisi o biometrijskom opisu vena se koriste kao dodatni dio u jednoznačnom opisivanju osobe. Vene su veliki, nepromjenjivi i uglavnom skriveni predlošci. U kombinaciji s geometrijom ruke ili tehnologijom opisivanja otiska prstiju postiže se vrlo visok stupanj prepoznavanja osobe. Ova tehnologija se može koristiti i prilikom fizičke kontrole prolaska kao inteligentna vrata, brave i ostale fizičke barijere u koje korisnici dolaze u kontakt s rukama. Na primjer banke u Japanu koriste ovu tehnologiju, što je riješeno zakonom. Kamere za prepoznavanje uzorka vena se obično koriste i infracrvenim senzorom jer on raspoznaje one detalje koje ljudsko oko nije u mogućnosti registrirati.



Slika 8: Digitalizirani predložak vena dobivenih infracrvenim spektrom

3.1.6. Otisak prsta

Uzorci pora i brazdi od trenja individualnih otisaka prstiju su jedinstveni za tu osobu. Otisci prstiju su jedinstveni za svaki prst osobe, uključujući i jednojajčane blizance. Jedna od komercijalno najdostupnijih biometrijskih tehnologija, uređaji za raspoznavanje otisaka prstiju za stolna i prijenosna računala, su sada široko dostupni od mnogih proizvođača po niskim cijenama. S tim uređajima, korisnici više ne trebaju unositi zaporke - umjesto toga, samo dodir pruža trenutni pristup računalu.

Sustavi za otiske prstiju mogu se također koristiti u identifikacijskom modu. Nekoliko država u SAD provjerava otiske prstiju kod prijave ljudi za socijalne povlastice, kako bi osigurali da prijavljeni ne dobiju povlastice pod krivotvorenim imenima. Država New York ima preko 900 000 ljudi upisanih u takav sistem.



Slika 9: Digitalizirani predložak otiska prsta

3.2. Biometrija ponašanja

Biometrija ponašanja opisuje fizikalne karakteristike (kao kretanje u prostoru, glas, izgled...) čovječjeg tijela koje su dijelom jedinstvene za svaku osobu. Dobiveni uzorci se opisuju krivuljama koje se koriste za opis ponašanja pa je na osnovi istih moguće raspoznavati različite ljude. Navedene tehnike se koriste u kombinaciji s tradicionalnim načinima jednoznačnog opisivanja ljudi.

3.2.1. Prepoznavanje glasa

Prepoznavanje glasa koristi se u svrhu autentikacije različitih korisnika na temelju njihovih jedinstvenih glasovnih karakteristika. Naime, da bi se korisnik autenticirao, isti mora izgovoriti neki tekst koji je prethodno izgovorio i koji je spremljen u bazu podataka. Tu postoji visoka jedinstvenost pošto ljudi uglavnom različito izgovaraju iste rečenice (tonalitet, brzina, prekidi). Ipak, ukoliko bi netko snimio autentikaciju ovlaštene osobe, isti bi ju mogao ponoviti pa je stoga ovu metodu autentikacije potrebno koristiti u kombinaciji s drugim metodama. Danas se ova metoda zasnovana na prepoznavanju glasa nalazi na većini raspoloživih mobitela u svrhu bržeg uspostavljanja telefonskih poziva.

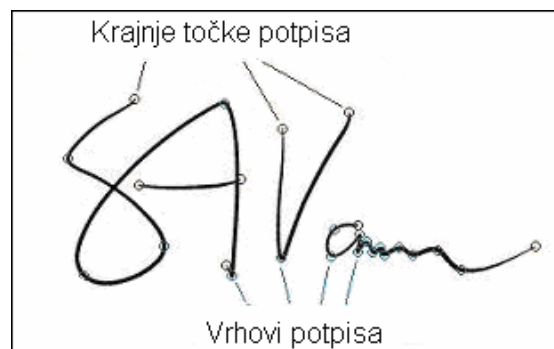
Prepoznavanje glasa ima i druge namjene kao što je preslikavanje glasa u tekstualne zapise. Postupak prepoznavanja govora se u tom slučaju sastoji od toga što se izgovorene riječi u kratkom vremenu unutar računala prepoznaju i prikazuju na zaslonu. Najnoviji programi za prepoznavanje govora omogućuju prepoznavanje tzv. prirodnog govora ili, kako ga neki nazivaju, kontinuiranog govora. To

znači da nema potrebe za korištenjem pauze između svake riječi. Samo treba govoriti i računalo će pokušati shvatiti značenje izgovorenih riječi. Riječi se trenutno prikazuju na zaslonu i unutar nekog tekstualnog dokumenta. Moguće je diktirati paragrafe, slati elektroničku poštu, stvarati izvještaje i pisma te sve to i obrađivati.

Svrha tehnologije prepoznavanja govora na prethodno navedeni način je veća produktivnost korisnika, što znači da je moguće obaviti više posla u istom intervalu vremena. Koristeći se tehnologijom prepoznavanja govora moguće je raditi brže i efikasnije nego što je to moguće klasičnim načinom utipkavanja teksta u računalo. Broj riječi se odnosi na prosječan broj riječi koje izgovori običan korisnik pod čime se podrazumijeva ispravljanje pogrešno interpretiranih riječi. Testiranjem je utvrđeno kako je za 900 ispisanih riječi potrebno 18 minuta klasičnom metodom tipkanja, a ukoliko se koristi programsko rješenje za prepoznavanje govora (Dragon Naturally Speaking), vrijeme unosa se smanjuje na 6.5 minuta [11].

3.2.2. Prepoznavanje rukopisa ili potpisa

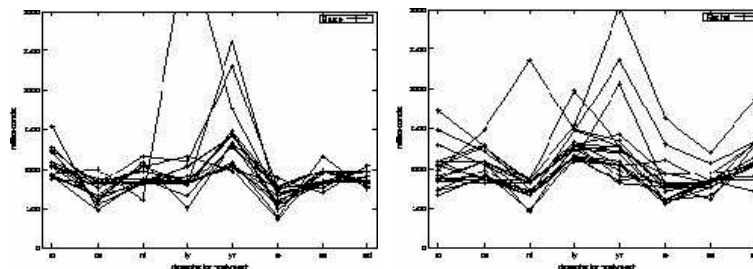
Ova tehnologija koristi dinamičku analizu potpisa kako bi autentificirala osobu. Tehnologija je bazirana na mjerenju brzine, pritiska i kuta koje koristi osoba kada se potpisuje ili kada piše nespecificirani tekst. Jedno od smjerova prema kojima se je usredotočila ova tehnologija su i *e-business* aplikacije, ali i druge aplikacije gdje je potpis prihvaćen kao metoda osobne autentifikacije.



Slika 10: Potpis opisan krivuljama i njihovim međusobnim odnosima

3.2.3. Dinamika tipkanja

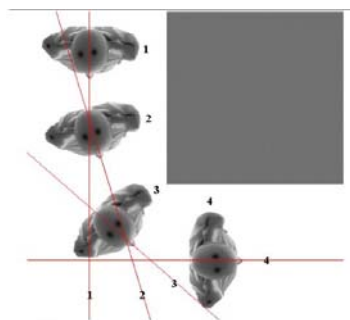
Ova tehnika se razvila tijekom drugog svjetskog rata u primjeni kod radiotelegrafista jer je uočeno da se po brzini tipkanja mogu razlikovati pošiljatelji poruka. Ako se danas govori o dinamici tipkanja onda se podrazumijeva dinamika tipkanja po tipkovnici. Kao tehnika je vrlo nenametljiva jer nije potrebno uvoditi nikakve dodatne uređaje za detektiranje, osim zvučne kartice. Eventualno je moguće posjedovati i specijalizirani program koji bi na razini operacijskog sustava pratio korisnikovo tipkanje. Glavna karakteristika na kojoj se ova tehnika bazira je vremenski razmak između korisnikovog pritiskanja na tipkovnicu.



Slika 11: Grafički prikaz brzine tipkanja iste riječi za dvije različite osobe

3.2.4. Dinamika hoda

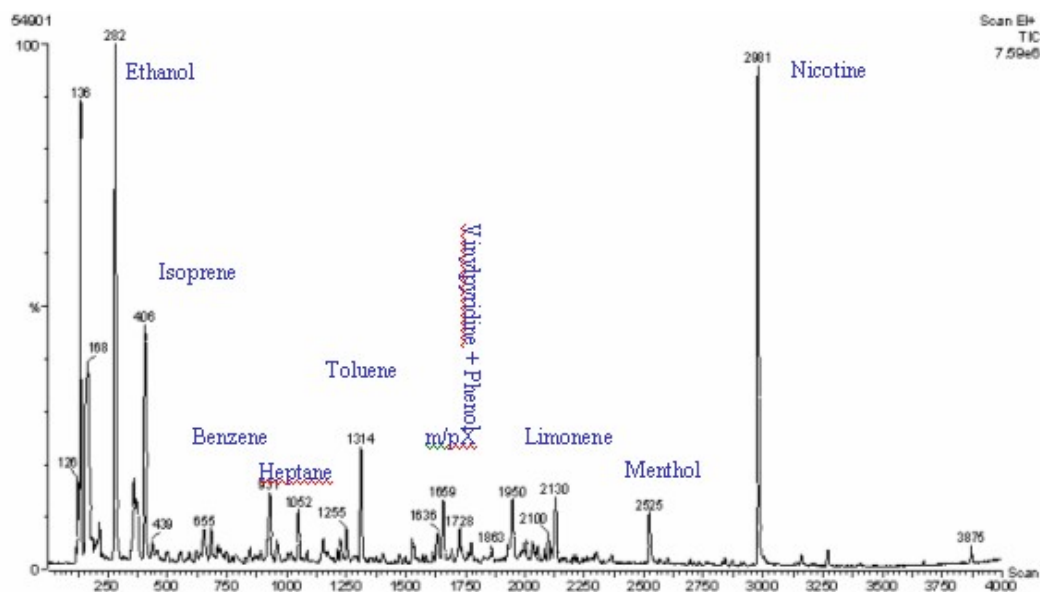
Ljudsko hodanje predstavlja kompleksnu prostorno-vremensku biometriju ponašanja. Njegova karakteristika je to što nije jedinstven za svakog od pojedinaca, ali je po svojim karakteristikama karakterističan u svrhu provjere identiteta s obzirom na karakter, situaciju u kojoj se nalazi osoba i na njeno zdravstveno stanje. Hod nije nepromjenjiv, pogotovo kod dužeg vremenskog perioda jer se osoba umara. Uzorak hoda se dobiva iz video zapisa učinjenog video kamerom. Sve provjere dinamike hoda se temelje na karakterizaciji nekoliko različitih pokreta svakog od zglobova prilikom izvođenja određene radnje.



Slika 12: Prikaz kuta pod kojim osoba zaobilazi prepreku

3.2.5. Dinamika mirisa

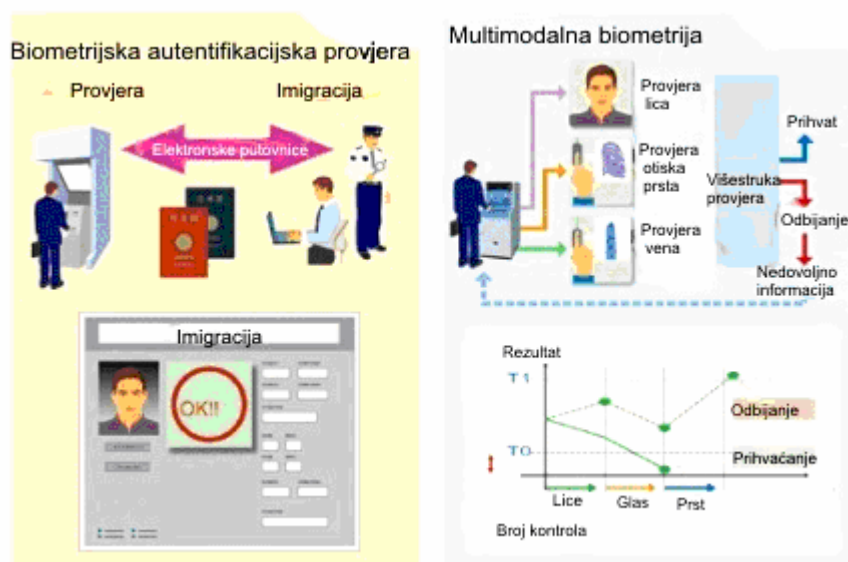
Svaki objekt u prirodi ima svoj miris koji je karakterističan za njegov kemijski sastav. Biometrijski sustavi koji detektiraju mirise rade na principu upuhivanja zraka preko kemijskih senzora od kojih je svaki osjetljiv na određenu grupu mirisa, tj. na njegova kemijska svojstva. Miris se opisuje mjerenjima obuhvaćenom od senzora i u njegovom intenzitetu na svakome od njih. Pošto miris ima više funkcija u prirodi kao što su komunikacija, privlačenje partnera, zaštita okoliša ili obrana, onda se može upotrijebiti i u civilne, ali i u vojne svrhe. Pretpostavljajući da svaka osoba sadrži karakterističan miris, moguće je po parametrima svakog od senzora odrediti o kojoj se osobi radi i odrediti glavnu notu mirisa od sporedne. Posebno je važno razlikovati miris osobe od parfema na njoj pa je u tom polju potrebno još istraživanja kako bi se odijelili mirisi.



Slika 13: Krivulje koje opisuju dinamiku mirisa za različite spojeve

3.3. Multimodalna biometrija

Multimodalna biometrija podrazumijeva kombiniranje svih prethodno navedenih biometrijskih tehnika. Ukoliko se u praksi koristi veći broj prethodno nabrojenih tehnika, može se izgraditi jedan sigurni informacijski sustav. U praksi je to kombinacija fizičkih i biometrija ponašanja koji podrazumijevaju provjeru i identifikaciju. U praksi se koriste u graničnim prijelazima za kontrolu ulaska ili izlaska, za kontrolu pristupa nekom prostoru, civilnoj identifikaciji, mrežnoj sigurnosti. Multimodalna biometrija se koristi i kao potpora standardnim postupcima za provjeru identiteta ili ukoliko iz izvornih dokumenata i zapisa nije moguće dobiti dovoljan broj podataka kojima bi se opisala neka osoba. Preporučljiva je kombinacija standardnih sigurnosnih mehanizama i biometrijskih jer uvijek postoji mogućnost zloupotrebe. Jedan od primjera je lažni predložak otiska prstiju. Ukoliko se koristi samo jedna tehnika kao što je prepoznavanje otiska prstiju, tada je moguća situacija u kojoj treća osoba posjeduje lažni otisak prstiju s kojim obavlja autentikaciju u ime neke osobe. No, ukoliko se koristi verifikacija lica, ili još bolje raspoznavanje rožnice i provjera vena, tada se s većom mogućnošću može utvrditi kako se doista radi o toj osobi ili se može detektirati slučaj pokušaja krađe identiteta.



Slika 14: Primjer multimodalne biometrije u carinskoj kontroli

3.4. Usporedba biometrijskih tehnika

U sljedećim tablicama prikazana je paralelna usporedba više biometrijskih tehnologija s obzirom na sljedeće karakteristike:

- univerzalnost - opisuje u kojoj mjeri se tehnika može primijeniti u svakodnevici,
- jedinstvenost - opisuje u kojem postotku je navedena kategorija jedinstvena s obzirom na pojedinca,
- trajnost - opisuje promjenjivost s obzirom na vrijeme tj. koliko pojedinac zadržava navedenu karakteristiku,
- prikupljivost - opisuje s kojom lakoćom se dobiva uzorak navedene kategorije,
- izvedivost - opisuje u kojoj mjeri je moguće u praksi implementirati navedene biometrijske metode i
- prihvatljivost - opisuje u kojoj mjeri je moguća implementacija, a da se ne naruše ljudska prava.

METODE BIOMETRIJE / KARAKTERISTIKE	Univerzalnost	Jedinstvenost	Trajnost
Lice	Visoka	Niska	Srednja
Otisak prsta	Srednja	Visoka	Visoka
Geometrija dlana	Visoka	Srednja	Srednja
Šarenica	Visoka	Visoka	Visoka
Mrežnica	Visoka	Visoka	Srednja
Termogram	Visoka	Visoka	Niska
Uho	Srednja	Srednja	Visoka
DNK	Visoka	Visoka	Visoka
Potpis	Niska	Niska	Niska
Glas	Srednja	Niska	Niska
Dinamika tipkanja	Niska	Niska	Niska
Miris	Visoka	Visoka	Visoka
Hod	Srednja	Niska	Niska

Tablica 1: Usporedba biometrijskih tehnika prema univerzalnosti, jedinstvenosti i trajnosti

METODE BIOMETRIJE / KARAKTERISTIKE	Prikupljivost	Izvedivost	Prihvatljivost
Lice	Visoka	Niska	Visoka
Otisak prsta	Srednja	Visoka	Srednja
Geometrija dlana	Visoka	Srednja	Srednja
Šarenica	Srednja	Visoka	Niska
Mrežnica	Niska	Visoka	Niska
Termogram	Visoka	Srednja	Visoka
Uho	Srednja	Srednja	Visoka
DNK	Niska	Visoka	Niska
Potpis	Visoka	Niska	Visoka
Glas	Srednja	Niska	Visoka
Dinamika tipkanja	Srednja	Niska	Srednja
Miris	Niska	Niska	Srednja
Hod	Visoka	Niska	Visoka

Tablica 2: Usporedba biometrijskih tehnika prema prikupljivosti, izvedivosti i prihvatljivosti

4. Zaključak

Biometrija svakodnevno postaje sve češćim oblikom autentikacije u različitim sferama života pa je tako korištenje automatiziranog sustava radi prepoznavanja nečijeg identiteta praćenjem njegovih fizičkih karakteristika ili ponašanja, već duže vrijeme dio stvarnosti. Velika prednost biometrije je u problemima povezanim s zaporkama. Zaporke se mogu izgubiti, zaboraviti ili razotkriti od strane zlonamjernih korisnika ili napadača. Tim problemima dodatno doprinose i potreba za što većim brojem korištenih zaporki uslijed čega korisnici zaboravljaju pojedine ili koriste iste na različitim mjestima. Stoga se, gdje je to fizički moguće, implementiraju biometrijske metode za pristup lokalnoj mreži.

Ipak, osnovna namjena biometrije je kontrola ulaska ili izlaska s određenih fizičkih lokacija. Kako bi se to ostvarilo, trenutno su u primjeni različiti oblici biometrijskih tehnika, ali najpotpunije rješenje može se postići kombiniranjem različitih metoda – multimodalnom biometrijom.

Biometrija svoju primjenu pronalazi i u kontroli radnog vremena zaposlenika. Naime korištenje kartica ili zaporki ostavlja mogućnost međusobne solidarnosti između zaposlenika gdje jedan zaposlenik lažira autentikaciju drugog zaposlenika. Također, očekuje se da će biometrija imati značajnu ulogu i u bankarskom sustavu.

Iako biometrija posjeduje značajne prednosti, prvenstveno povećavanje razine sigurnosti u smislu autentikacije korisnika, ista ipak ima i svoje nedostatke. Naime, za primjenu biometrije potrebno je posjedovati specijalizirane uređaje koji će na različite načine obavljati uzorkovanje i obrađivanje dobivenih podataka. Ti specijalizirani uređaji mogu biti skupi ili nepogodni zbog fizičke okoline i sl. Također, jedan od nedostataka određenih biometrijskih tehnika je i mogućnost lažnih autentikacija. Naime, korisnik može prilikom autentikacije podmetnuti snimku tuđeg glasa, otiska pa čak i potpisa. Stoga je nužno ne zasnivati proces autentikacije na samo jednoj metodi.

5. Reference

- [1] The hidden Markov model, http://www.cse.ucsc.edu/research/compbio/html_format_papers/hughkrogh96/node4.html, rujana 2006.
- [2] Home page for David B. Leake, CS Dept., Indiana U., <http://www.cs.indiana.edu/~leake>, rujana 2006.
- [3] Genetic Programming, <http://citeseer.nj.nec.com/correct/211802>, rujana 2006.
- [4] Iris scanning For New Jersey Grade School, <http://informationweek.com/hardware//177103027>, rujana 2006.
- [5] Tehnologija prepoznavanja lica, http://www.sistemvideo.hr/info_lice.shtml, rujana 2006.
- [6] Biometric Gold, <http://homepage.ntlworld.com/joseph.rice/>, rujana 2006.
- [7] Prepoznavanje govora računalom, <http://www.pefri.hr/~apetric>, rujana 2006.
- [8] Digital Ink Signatures – Concepts and Technologies, <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dntablet/html/tbconinksig.asp>, rujana 2006.
- [9] Odabrane teme iz biometrije, http://www.foi.hr/CMS_library/privatno/baca.miroslav/nastavni_sadrzaji/OTB1.ppt, rujana 2006.
- [10] Crowd Dynamics Ltd, <http://www.crowddynamics.com/Thesis/Images/>, rujana 2006.
- [11] Dragon Naturally Speaking, <http://www.nuance.com/naturallyspeaking/>, rujana 2006.