Identificare biometrica

Prof.dr. Maria BOLDEA, asist.dr. Costin Radu BOLDEA
Universitatea de Vest din Timisoara

The era of fast, accurate, cost-effective biometric identification systems has arrived. Societal activities increasingly threaten individual's and organization's assets, information, and, sometimes, even their existence. Instant, positive personal identification is a critically important step in controlling access to and protecting society's resources. Effective tools are now available.

***Keywords**: biometry, system, data security.*

1 Consideratii generale

Dezvoltarea si perfectionarea sistemelor de colectare si prelucrare a informatiei au dus la modernizarea sistemelor de acces. Astfel, în ultimul timp, sistemele de securitate bazate pe tehnologii biometrice se prezinta ca o alternativa viabila, cu un cost redus, la sistemele bazate pe cartele magnetice, coduri de bare sau parole. Se poate spune ca noile sisteme au dus la definirea unei alte clase de securitate, superioara fata de cea asigurata de sistemele traditionale.

Pentru a avea acces într-o incinta protejata la informatii sensibile, o persoana se poate identifica prin trei metode:

- printr-un obiect pe care-l detine (cheie, cartela);
- prin cunostinte secrete (parole, PIN-uri);
- prin trasaturi anatomice (ADN, amprente digitale, fata, iris, voce etc.).

*Tehnica de acces prin analiza trasaturilor anatomice se numeste **biometrie***. În momentul de fata, tehnologiile biometrice au la baza **identificatori fiziologici** (amprenta digitala, geometria palmelor, structura retinei, configuratia ADN) si **identificatori comportamentali** (timbrul vocal, dinamica scrisului, dinamica apasarii tastelor) ce permit recunoasterea absoluta a unei persoane.

Utilizarea biometriei pentru identificarea si autentificarea subiectilor umani a început sa ofere câteva avantaje unice fata de metodele traditionale. Numai autentificarea biometrica se bazeaza pe identificarea unei anumite parti intrinseci a fiintei umane. Sistemele bazate pe cartele magnetice, coduri de bare sau chei fizice pot fi pierdute, furate sau multiplicate. Parolele pot fi uitate, sparte sau observate intentionat sau neintentionat de o alta persoana. Uitarea parolelor sau pierderea „smart-cardurilor" înseamna o pierdere de timp pretios pentru administratorii de retea si utilizatori. *Trasaturile anatomice nu pot fi copiate usor si nici pierdute.* Biometria poate fi integrata în orice aplicatie care necesita securitate, accesul controlului, identificarea si verificarea utilizatorilor. Securitatea oferita de biometrie poate fi asistata de chei, parole, coduri PIN, astfel încât validarea accesului depinde de însasi persoana care o cere, nu de ceea ce stie, sau ceea ce are, ci de ceea ce este. De retinut ca resursele securitatii biometrice se bazeaza pe persoana care le utilizeaza, eliminând efectiv riscul care era asociat vechii tehnologii, în acelasi timp oferind un nivel mult mai înalt de securitate care convine atât utilizatorilor cât si administratorilor de sistem.

2. Tipuri de biometrie

Fingerprint/Finger length - amprenta digitala. Sistemul este bazat pe un senzor optic sau capacitiv, care transmite imaginea captata catre microcontroler sau catre PC în functie de sistemul în care este implementat.

Hand geometry/Hand&Finger - geometria mâinii. Un senzor optic scaneaza întreaga palma a utilizatorului. În acest scop mâna trebuie introdusa într-un dispozitiv mecanic dotat cu senzori de proximitate. **Iris/Retina Recognition - iris/retina.** Si aici un senzor optic scaneaza irisul sau retina înregistrând imaginea obtinuta într-o memorie dinamica sau statica.

Facial image Recognition/Facial thermo gram - maginea faciala. Scanarea se face cu senzori optici sau de temperatura. Imaginea captata este geometrizata 3D si retinuta.
Voice/Speaker - voce. Se face analiza spectrala a vocii utilizatorului, iar daca spectrul de frecventa este identic cu cel memorat, accesul este permis.
Signature - semnatura digitalizata. Aceasta poate fi memorata pe o cartela si comparata cu semnatura executata de utilizator înaintea accesului.
Keystroke - presiunea si ritmul apasarii tastelor.

3. Aplicarea metodelor biometrice pe ntru asigurarea securitatii datelor

Utilizarea metodelor biometrice de identificare în vederea asigurarii securitatii datelor se împarte în doua categorii:
- controlul accesului la documentele ce pot fi copiate de pe calculator si în încaperile unde se discuta informatii secrete;
- controlul utilizarii calculatorului si a accesului la informatiile pe care acesta le detine.

3.1. Controlul accesului

Controlul accesului la documentele ce pot fi copiate de pe calculator si în încaperile unde se discuta informatii secrete poate fi realizat utilizând metodele si sistemele prezentate anterior. Este valabil si pentru datele din calculator sau pentru locurile de depozitare a CD-urilor si dischetelor.

Metoda de identificare pe baza de amprente

Amprenta degetului este utilizata din secolul XIX la stabilirea identitatii. Odata cu dezvoltarea tehnologiei, oamenii de stiinta s-au orientat si catre acest domeniu. Tehnologia de recunoastere a amprentei se bazeaza pe analiza imaginii generata de un senzor, care contine puncte caracteristice alcatuite din terminatiile precum si din bifurcatiile de pe deget. Aceste puncte caracteristice, extrase din imaginea amprentei, sunt extrem de dese, ceea ce explica de ce amprenta este cel mai des utilizata în identificarea umana. Exista cam 70 de puncte masurabile, unice pentru fiecare amprenta, iar fiecare punct are 7 caracteristici unice. Daca se doreste o securitate maxima si se scaneaza cele 10 degete ale mâinilor se obtin 4900 de puncte independente pentru o singura persoana. Exista doua tehnologii importante utilizate pentru senzorii de amprenta digitala: optica si capacitiva.
Senzorii optici necesita o sursa de lumina care este refractata printr-o prisma. Degetul este plasat pe o placuta de sticla. Sursa lumineaza amprenta degetului, iar imaginea este capturata.
La **senzorii capacitivi** nu mai este necesar dispozitivul optic, imaginea amprentei se obtine masurând tensiunea creata între piele si placa din policarbonat a cititorului. Senzorii capacitivi trebuie sa aiba o suprafata similara cu cea a degetului. Ei sunt susceptibili la zgomot, inclusiv zgomotul de 50 Hz de la reteaua utilizatorului, precum si zgomotul intern al senzorului îi afecteaza. Descarcarea electrostatica, sarea de la transpiratie sau degetele uscate pot perturba captura imaginii de la senzor.
Datele cu privire la asezarea relativa a liniilor, crestaturilor, bifurcatiilor si intersectiilor sunt pastrate într-un fisier al bazei de date a utilizatorului si apoi comparate cu datele introduse în calculator de catre acest utilizator. Urmând instructiunile, subiectul introduce prin tastare un cod PIN format din 1-9 cifre. La semnal, degetul este pozitionat pe placa cititorului, iar apoi retras. Se creeaza un cod numeric. La semnal, se pozitioneaza din nou degetul, de mai multe ori, pentru comparare. Întreaga operatiune trebuie sa dureze mai putin de 2 minute. Dimensiunea fisierului este între 500 si 1500 biti. Majoritatea metodelor biometrice de identificare pe baza amprentelor sunt de fapt sisteme de verificare. Utilizatorul introduce datele de identificare prin tastarea unui PIN sau folosind un cititor de card-uri, iar apoi pozitioneaza un deget pe placa. Mesajul vizual si auditiv de confirmare sau infirmare se transmite în 5-7 secunde. Operatorii sistemelor curata deseori placile pentru a îndeparta murdaria ce ar putea afecta acuratetea în identificare. Pentru a evita problema legata de murdarirea placilor, a fost dezvoltat un sistem nou care obtine o imagi-

ne a amprentelor pe *baza de ultrasunete*. Unii sustin chiar ca acest sistem poate obtine amprentele unui chirurg care poarta manusi. Este posibil ca dispozitivele optice de recunoastere a amprentei sa fie pacalite de o amprenta latenta, reducând astfel siguranta întregului sistem. Pentru limitarea consecintelor acestui aspect au fost introduse *imaginile tridimensionale.* Amprentele latente pot fi furate, dar nu un model tridimensional al amprentei; pentru acest lucru ar trebui ca subiectul sa coopereze sau sa fie fortat sa coopereze. *Sistemele bazate pe acest fel de obtinere a amprentelor au un grad înalt de siguranta***.** Dar detectarea unui deget taiat? Folosirea unui *deget taiat* indica o infractiune grava, nu este acelasi lucru cu furtul unui cod PIN sau a unei parole. Un traductor care *detecteaza presiunea sângelui* poate indica daca degetul apartine unei persoane în viata. Poate fi de asemenea folosita si *detectarea conductivitatii electrice a pielii.* Poate fi folosita *tehnica de deplasare a degetului* pentru a detecta daca o persoana este fortata, deoarece miscarea degetului nu mai este aceeasi în conditii de stres.

Scanarea formei palmei

Datele privind *forma palmei si a degetelor (lungime, latime, înaltime)* se obtin prin intermediul unor imagini video, orizontale sau verticale. Subiectul este directionat sa pozitioneze palma pe placa, cu respectarea delimitarilor dintre degete. Beculetele aflate deasupra a 4 degete asigura pozitia corecta a palmei. O camera digitala înregistreaza o imagine de sus si din lateral, utilizând o oglinda la 45^0 pentru cea laterala. Subiectul este "invitat" sa-si retraga palma, iar apoi sa o repozitioneze înca de 2 ori. Citirile efectuate îmbraca forma unui cod. Timpul necesar este de sub 2 minute. Dimensiunea fisierului ce rezulta este de 9 biti. Scanarea formei palmei este o metoda care lucreaza numai ca un verificator al identitatii. Utilizatorul introduce PIN-ul prin tastare sau prin cititorul de carduri. Când apare pe ecran mesajul "pozitionati palma", utilizatorul trebuie sa duca la îndeplinire aceasta instructiune, respectând si delimitarile între degete. Când cele 4 beculete confirma pozitia corecta a palmei, iar datele necesare au fost culese, apare mesajul "retrageti palma". Mesajul vizual si auditiv de confirmare sau infirmare este trimis în 3-5 secunde. Se trimite urmatorul mesaj: "sistemul verifica daca palma utilizata este reala".

Fisierul de 9 biti este cel mai mic utilizat de vreo metoda biometrica. Sistemul de identificare prin scanarea formei palmei este fabricat de Recognition Systems Inc. O alta varianta, aceea a identificarii pe baza scanarii formei a numai 2 degete, este produsa de BioMet Partners.

Metoda de identificare pe baza vocii

Senzorii audio si de alta natura receptioneaza pâna la 7 nivele ale *tonurilor nazale, vibratiilor gâtului si laringelui, a presiunii exercitate asupra aerului de* catre *voce.* Majoritatea sistemelor utilizeaza un echipament similar cu cel al telefoanelor. Urmând indicatiile, subiectul ridica receptorul si introduce un cod PIN prin tastare de la butoanele telefonului. La semnalul auzit prin receptor, subiectul pronunta parola de acces, care poate fi PIN-ul + numele sau o propozitie formata din 4 pâna la 6 cuvinte. Se repeta pâna la de 4 ori. Timpul necesar este mai mic de doua minute. Dimensiunea fisierului rezultat variaza între 1000 si 10000 de biti, în functie de producator. În prezent, aceste sisteme opereaza doar ca verificatori ai identitatii. Raspunsul auditiv este primit prin receptor. Unele sisteme includ si un raspuns vizual. Operatiunea dureaza pâna la 10-14 secunde. Sunt utilizate diferite metode, inclusiv masurarea presiunii aerului, care este în crestere atunci când se pronunta consoanele “p” sau “t”. Unele sisteme mai sofisticate cer utilizatorului sa pronunte diverse cuvinte, în ordine arbitrara, dintr-o lista de 10 cuvinte înregistrate. Zgomotul din fundal poate afecta acuratetea sistemelor.

Scanarea retinei

Sistemul înregistreaza date cu privire la *tipul vaselor de sânge din portiunea aflata în spatele globului ocular,* utilizând o camera video pentru obtinerea imaginii. Subiectul este directionat sa îsi pozitioneze ochiul la o distanta de 1-2 inch fata de deschizatura aparatului si sa ramâna nemiscat. O lumina invizibila, de intensitate foarte scazuta, permite citirea

informatiilor de pe retina. Se tasteaza un cod PIN. Timpul necesar este de sub 2 minute. Imaginea scanata a retinei si informatiile culese sunt retinute într-un fisier de 96 de biti. La verificare, utilizatorul tasteaza PIN-ul. În mod automat, sistemul obtine date atunci când ochiul este pozitionat în fata deschizaturii aparatului si centrat pe punctul verde. Acceptarea sau neacceptarea este indicata pe ecranul LCD. Verificarea dureaza aproximativ 1,5 secunde. Recunoasterea necesita mai putin de 5 secunde. Sistemul are nevoie de "un ochi real si de o privire fixa" pentru a strânge informatiile oferite de scanare. Se înregistreaza variatii în functie de producator. Întrucât unele persoane transpira sau au ochi care lacrimeaza, umezind astfel dispozitivul, unii utilizatori sunt îngrijorati ca ar putea "capta" o boala (prin transfer). Deoarece sistemele anterioare foloseau o raza rosie pentru a culege informatiile, unii utilizatori au fost îngrijorati ca ar putea fi afectati de "laser". Nu s-au facut, însa, insinuari cum ca vreun utilizator ar fi avut de suferit de pe urma sistemului. Întrucât diabetul si infarctul pot cauza schimbari pe retina, ce pot fi depistate de sistem, unii utilizatori s-au îngrijorat la gândul ca managementul ar putea obtine, în mod neautorizat, informatii privind starea lor medicala, lucru care ar putea fi în detrimentul lor. Unii utilizatori potentiali ramân îngrijorati cu privire la posibilele efecte adverse asupra ochiului. Ei sustin ca sistemul proiecteaza o raza în interiorul ochiului pentru a scana retina. Drepturile de autor privind sistemele ce utilizeaza aceasta metoda sunt detinute de Eye Dentify Inc.

Scanarea irisului

Irisul (portiunea colorata care înconjoara pupila) are o structura bogata si unica prin *linii, puncte, fibre, filamente, cornee, cute si vase de sânge*. Imaginile sunt obtinute cu o camera video de 1/3 inch CCD, care poate realiza 30 imagini/secunda. Subiectul priveste o imagine a ochiului sau, furnizata de un LCD ce functioneaza ca o oglinda. Sistemul creeaza câteva zone de analiza pe imagine, stabileste caracteristicile fiecareia si realizeaza un cod al irisului. Apoi proceseaza 3 imagini, o alege pe cea mai buna si o salveaza, cu aprobarea operatorului. Fisierului, care contine date personale ale utilizatorului, i se adauga un cod PIN. Timpul necesar este de sub 2 minute. Codul stabilit pentru iris ocupa 256 biti. Sistemul poate opera ca un verificator, dar este folosit în principal pentru identificare, întrucât îndeplineste aceasta functie mult mai repede decât alte sisteme. Utilizatorul apasa pe butonul Start, înclina aparatul optic conform înaltimii sale si priveste imaginea ochiului sau. Daca sistemul e utilizat pentru verificare, atunci el este legat la un cititor de card-uri sau la o tastatura. Se transmite un mesaj, pe cale auditiva si vizuala, de identificare sau neidentificare, în aproximativ 2 secund. Timpul total pentru un utilizator cu experienta este de 2,5 pâna la 4 secunde. Irisul este un organ care ramâne, în principiu, neschimbat de la vârsta de 1 an pâna la moarte. Asadar, odata înregistrata, persoana va fi întotdeauna recunoscuta, exceptând situatiile în care sufera de anumite boli ale ochiului sau prezinta rani la nivelul acestuia. Drepturile de autor pentru realizarea sistemelor bazate pe scanarea irisului sunt detinute de IriScan Inc.

Metoda de recunoastere a semnaturii digitalizate

Viteza de scriere, directia si presiunea exercitata asupra instrumentelor de scris sunt înregistrate prin intermediul unor mici senzori ce se regasesc în interiorul instrumentului de scris sau pe placa de scris. Urmând indicatiile, subiectul semneaza, utilizând un instrument de scris sau o placa cu senzori. Sunt necesare 5 semnaturi. Unele sisteme înregistreaza doar 3. Pentru a preîntâmpina reproducerea semnaturii, se efectueaza o convertire în coduri, dupa care se adauga un PIN. Timpul necesar este de sub 2 minute. Dimensiunea fisierului ocupa aproximativ 1000-1500 biti. Utilizatorul se identifica prin tastarea unui PIN sau prin cititorul de card-uri. Apoi semneaza utilizând instrumentul de scris sau placa de senzori. Mesajul de confirmare sau infirmare se transmite pe cale auditiva si vizuala dupa aproximativ o secunda. Timpul total este de 5-10 secunde, în functie de timpul necesar pentru a semna.

3.2. Protejarea calculatorului si a datelor continute de acesta

Controlul accesului la calculator si la datele acestuia devine tot mai important. Datorita usurintei de accesare, pierderile înregistrate în acest domeniu le-au depasit pe cele rezultate din atacuri la persoana. Asadar, a devenit absolut necesara identificarea celor care acceseaza programe si informatii de maxima importanta. Utilizarea parolelor sau a PIN-urilor pentru a controla accesul la programele si fisierele calculatorului este o metoda destul de buna, dar care nu înlatura neajunsurile. Codurile stabilite sunt de obicei usor de identificat. Cele care sunt greu de retinut sunt scrise, de regula, pe o hârtie si pastrate într-un loc care poate fi descoperit. Mai mult, acest control opereaza doar la început, când se doreste a se intra într-un program sau fisier anume. ***Este nevoie, asadar, de o metoda biometrica capabila sa identifice în permanenta utilizatorul.*** Acest sistem nu trebuie sa permita accesul la date pâna în momentul în care operatorul este identificat ca fiind o persoana autorizata sa foloseasca si sa acceseze acele informatii. De asemenea, sistemul ar preveni accesul la programele sau fisierele protejate, pâna în momentul identificarii utilizatorului ca fiind o persoana autorizata. La fiecare 30 de secunde, sistemul ar trebui sa realizeze o identificare a utilizatorului, pe tot parcursul timpului în care acesta acceseaza date. Daca sistemul a identificat o persoana ca fiind neautorizata, programul accesat se va închide. Desigur, un astfel de sistem depinde de software-ul instalat, de masura în care acesta poate preveni violarea sau introducerea neautorizata a unor date. Disponibil în prezent este *Sistemul 'Identix TouchSafe*^{TM} care efectueaza o verificare a persoanelor ce acceseaza datele aflate în calculator. Se compune dintr-un *card electronic* si *o unitate de 5.4"´ 2.5"´ 3.6"* care realizeaza o *identificare dupa amprente* având în memorie o lista limitata de utilizatori. De fiecare data când trebuie facuta identificarea, utilizatorul trebuie sa-si înceteze activitatea si sa pozitioneze un deget pe cititor.

Identificarea în permanenta se poate realiza numai cu un sistem bazat pe o camera video. Daca este plasata într-un colt al monitorului, sistemul poate fi programat sa realizeze o identificare la fiecare 30 sau 60 de secunde. Întrucât utilizatorul priveste ecranul, în cea mai mare parte a timpului, s-ar putea folosi metoda de *identificare prin scanarea irisului* sau *a fetei*, fara a întrerupe activitatea acestuia. Daca utilizatorul nu a privit ecranul în cele 30 de secunde, apare screen saver-ul. Odata ce identificarea a fost facuta, sistemul se întoarce la programul sau. Daca persoana nu este identificata sau este neautorizata programele si fisierele sunt salvate si închise.

Primul sistem de aceasta natura este cel produs de *Miros Inc*, care lucreaza la o linie de produse numite *TrueFace*. Sistemul este bazat pe *identificarea fetei* si se afla în faza de testare pentru a se putea vedea nivelul de performanta atins. Un alt sistem bazat pe *scanarea irisului*, capabil sa asigure un control eficient privind accesul la informatiile din calculator si care se afla în fazele initiale de dezvoltare este *IriScan Inc*. Acuratetea sistemului a fost demonstrata, ceea ce face ca acest sistem sa fie un "candidat" ideal pentru a fi cel mai eficient în identificarea utilizatorilor. Cu certitudine, in viitor, sistemele biometrice vor deveni tot mai raspândite, probabil pâna la a ajunge ubicue, asa cum sunt astazi yalele .

Bibliografie

1. Hal Tipton and Micki Krause, *Handbook of Information Security Management*, Publisher: CRC Press LLC, 1998
2. Simon Liu and Mark Silverman, *A practical Guide to Biometric Security Tehnology*, electronic edition, http://www.findbiometrics.com, 2002
3. Yanping Ma, et al., *On the Use of Historical Control Information for Trend Test in Carcinogenesis*, Biometrics, Vol 58,No 4, pp 917-927
4. http://www.findbiometrics.com
5. http://www.biometricgroup.com
6. http://www.biometricaccess.com