

Biometrikus azonosító rendszerek

VARGA DOMONKOS, OLÁH ANDRÁS

Budapest Műszaki és Gazdaságtudományi Egyetem, Híradástechnika Tanszék
vargad@octopus.hit.bme.hu

Reviewed

Kulcsszavak: személyazonosítás, elektronikus letapogatás, biztonsági eljárások

Korunkban nagymértékben megnövekedtek a személyazonosító-rendszerekkel szemben támasztott követelmények. Ebben szerepet játszanak a világpolitikai események, amelyek veszélyeztetik az emberek személy- és vagyonbiztonságát. A hagyományos módszerek már alkalmatlanok ezen igények kielégítésére, ezért olyan új azonosító-rendszerek bevezetésére van szükség, mint amilyenek a biometrikus azonosítók.

Bevezetés

A biometria az emberek egyedi, változtathatatlan jellemzőinek számszerű leírásának tudománya. Jelen esetben a biometriát úgy lehet meghatározni, mint olyan mérhető testi, vagy viselkedésszerű jellemvonások összességét, amelyek mérése alkalmas arra, hogy egy adott személy azonosságát ellenőrizni lehessen (biometriák: ujjlenyomat, arc, kézgeometria, hang, aláírás, gépelési dinamika, DNS, írisz és retina). A biometrikus azonosítás célja olyan biztonsági rendszerek kialakítása, melyek az egyént nem egy kód és egy kártya segítségével azonosítják (ami bárkinek birtokába kerülhet), hanem saját személyi tulajdonságai alapján ismeri fel. Számos ilyen rendszer került kidolgozásra az elmúlt évtizedekben, és ezek a megoldások egyre sikeresebbek. A Biometrikus rendszerek elterjedését motiváló legfontosabb okok [1]:

- a jelszavak számának jelentős növekedése biztonsági kockázatot rejt;
- a jelszavak menedzselése jelentős költségkihatással jár;
- nő az egyre kényesebb információk eléréséhez szükséges jogosultságvizsgálat fontossága;
- nő az igény az eltérő biztonsági technológiák integrálására;
- nő az igény a legkorszerűbb hálózatos biztonsági technológia megvalósítására.

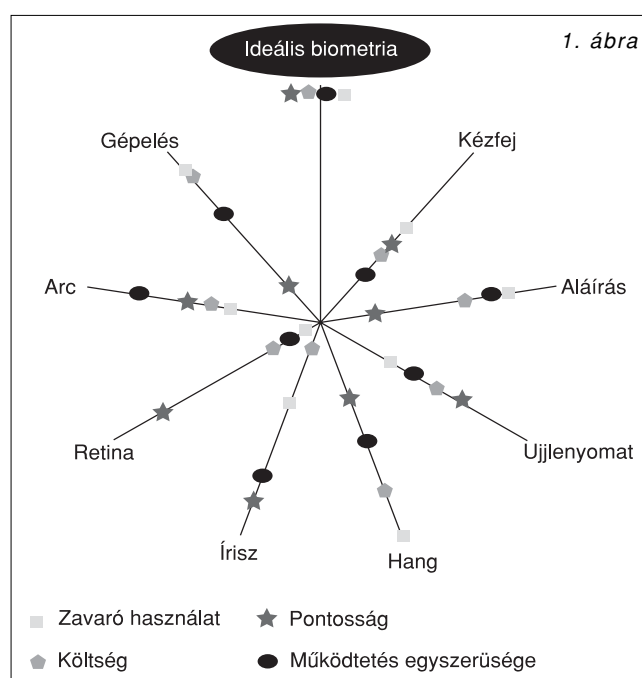
A biometrikus azonosítók két részre oszthatók. A **Személyigazoló (Szi)** rendszerek tipikusan „egy az egyhez”, vagy „egy a kevéshez” módon végzik a keresést. A biometrikus azonosításkor az azonosítandó személy tárolt adatai (pl. beléptető-kártyán és adatbázisban), mintái már ismertek, és ez kerül összehasonlításra az aktuális mintával.

Az úgynevezett **SzemélyAzonosítók (SZA)**, „egy a sokhoz” végzik a minták összehasonlítását, és nagy populációból választják ki a az azonosítandó személyt. Ezek a rendszerek általában lassúak, ugyanis az embert kizárólag biometrikus paraméterei alapján azonosítják, és a biometriájához keresnek az adatbázisból már azonosított személyt. Ez az eljárás a populáció növe-

kedésével egyre nagyobb bonyolultságú és ezzel együtt a megbízhatóság is csökken. Az SZA rendszerek használata kényelmes, mert nem kell bajlódni egyéb azonosító eszközökkel (pl. beléptető-kártya). Bizonyos algoritmusok és speciális adatbázis használatával az azonosítási idő csökkenthető. A megbízhatóság növelése azonban a téves visszautasítások számát növelheti, ami egy bizonyos fokon túl a felhasználót irritálhatja. Azonosítási idő megadásának ebben az esetben nincs értelme, hiszen az populációfüggő.

Az Szi előnye, hogy olcsóbb, gyorsabb, pontosabb, kevesebb a hibázási lehetőség és több felhasználót képes pontosan azonosítani, mint az SZA.

Napjainkban az azonosító rendszerek a kutatások fókuszában állnak, mert még számos megválaszolatlan problémára kell megoldást találnia a kutatóknak. Az egyik legfontosabb probléma, hogy miként lehet olyan személyazonosító rendszert létrehozni, mely egyszerre gyors, biztonságos és sok felhasználó azonosítására képes.



Általános célkitűzések

Az egyes biometrikus azonosítók teljesítőképességének analizálására a Zephyr-analízist használják, mely az azonosítókat négy főszempont szerint vizsgálja. Az origóhoz közeli pozíció a rossz (kedvezőtlen), a távoli pedig a jó (előnyös alkalmazás) minősítést jelenti (1. ábra).

1. Pontosság

Két főbb mérőszámot használnak az azonosítók megbízhatóságának mérésére:

- A *hibás elfogadás aránya* (FAR – False Acceptance Rates) annak a valószínűségét adja meg, hogy egy illetéktelen behatolót a rendszer tévesen elfogad.
- A *hibás visszautasítás aránya* (FRR – False Rejection Rates) annak a valószínűségét jelenti, hogy egy regisztrált felhasználót visszautasít a rendszer.

Biztonságtechnikailag természetesen az első szempont, az illetéktelen behatolás megakadályozása a lényegesebb, de felhasználói szempontból ugyancsak fontos, hogy gyors és pontos legyen az azonosítás (a rendszer ne csak minden tizedik próbálkozásra tudjon egy regisztrált felhasználót azonosítani). Az azonosítók hiba-aránya (FAR) 10^{-5} és 10^{-6} között van.

2. Költség

Kezdetben biometria alapon működő azonosítási technikákat elsődlegesen a különlegesen nagybiztonságú alkalmazásokban használták, de napjainkban már sokkal szélesebb körben lehet alkalmazásukkal találkozni (például számítógépes rendszerek felhasználói jogosultságának vizsgálata, épületben az ajtók nyitása-zárása, munkaidő nyilvántartás, riasztó rendszerek stb.). Az azonosító-rendszerekben elsősorban a szoftverek költsége a legszámottevőbb, a perifériák költsége nagyon változó lehet, a rendszerek ára azonban folyamatosan csökken.

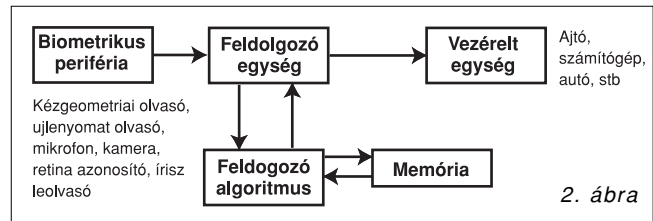
3. Működtetés egyszerűsége

Biometria azonosítók használata esetén fontos, hogy a felhasználó könnyen megtanulja az eszköz kezelését és mindennapi használata, se jelentsen nehézséget a felhasználó számára.

4. Zavaró használat

A biztonsági rendszerek tervezésekor nemcsak a technikai tényezőket kell figyelembe venni. Az egyik legfontosabb nem technikai jellemző a rendszer iránti bizalom (elhiszi-e a laikus felhasználó, hogy az azonosító-rendszer valóban csak őt képes felismerni, vagyis biztonságos). A másik ergonómikus jellegű: vajon mennyire kényelmes használni a rendszert, vagy hosszútávon is irritálja majd a műszer a felhasználóját.

Ahhoz, hogy a biometria azonosítók működését megértsük, elsősorban egy általános rendszer vizsgálatára van szükség (természetesen más rendszerfelépítések is elképzelhetők). A főbb funkciókat betöltő egységeket a 2. ábrán követhetjük nyomon.



2. ábra

- A biometrikus periféria feladata a biometria paraméterek beolvasása és ezen paraméterek átalakítása digitális jellé, melyet a feldolgozó egység már értelmezni tud. Ennek az egységnek az ára nagyon változó lehet a biometria paraméterektől függően. Nyilván egy mikrofon, vagy kamera ára tört része egy ujjlenyomat leolvasó árának.
- A feldolgozó egység végzi a rendszer irányítását: visszajelez a felhasználónak az azonosítás eredményéről és a vezérelt egységnek, engedélyezi/tiltja és végrehajtja a hozzáférést.
- A feldolgozó algoritmus végzi a felismerési feladatokat, amely általában egy összehasonlításból áll a tárolt és az aktuális minták között. A tárolt minták egy memóriában vannak elhelyezve, ezek a memóriák bővíthetők, de minden rendszer esetén van felső bővítési határ. Ennek többek között a biztonság is oka, hiszen minél több felhasználó van, annál nagyobb a valószínűsége, hogy a gép téved, vagy felismerő-rendszerek esetén az azonosításhoz szükséges számítási idő jelentősen nő. A tapasztalatok szerint, ha egy nagyon nagy populációjú rendszerre van szükség, akkor a tárolt mintákat, nem egy központi számítógép memóriájában tárolják el, hanem egy személyhez rendelt chip-kártyában. Így a rendszer megőrzi a gyorsaságát és a biztonságát. Nagy hátrány azonban az, hogy ebben az esetben szükséges a kártya használata, aminek elvesztése további kényelmetlenségeket okozhat.
- A vezérelt egység bármi lehet, amihez nagy biztonságra van szükség. A gyakorlatban legtöbbször számítógépes rendszerekben használják belépéshez, illetve épületekben ajtók jogosult használatát korlátozzák.

Jelenleg a következő biometriák használata a legelterjedtebb.

Azonosítás az arc alapján

Napjainkban az arcfelismerő rendszereknek korlátozott sikerük van a gyakorlati alkalmazásokban. Több paraméter vizsgálatára van lehetőség, a leggyakrabban az arc körvonala alapján történik a felismerés [1,2]. Ezen kívül használják az arc geometriai tulajdonságait (szemek távolsága az arc szélétől, két szem távolsága egymástól, orrhossz, szájszélesség, szemszélesség), profilját, illetve az arc thermogramját is azonosításra [1].

Léteznek kisebb, otthoni használatra tervezett rendszerek, amelyek kisebb, család méretű populációban képesek azonosításra. Ezen kívül vannak természete-

sen nagyobb populáción működő rendszerek is, (például kórházak betegfelvétele, számítástechnikai rendszerekhez történő beléptetés, bankok, kaszinók).

A létező megoldások általában kis populációs rendszereknél, vagy más biometria megoldásokkal ötvözve működnek sikeresen [1].

Azonosítás az írisz alapján

Az eljárás az emberi írisz egyénre jellemző részletgazdagságán alapul. A többszörös összehúzó redők, a kolangén szálak, az üregek, gyűrűk, barázdák, a kanyargó érhálózat, a foltok, hasítékok és lyukak olyan nem duplikálható szövet hoznak létre, melynek több, mint 400 mérhető változója van [3]. Még az egyetétű ikrek írisze sem egyezik meg. A biometriák közül ez a rendszer rendelkezik a legnagyobb biztonsággal. A rendszerek még az élő szemet is detektálni tudják. Az írisz felismerése videó alapú képkészítéssel kezdődik, melynek első lépése a szem és az írisz – a pupilla peremvonalát körülvevő színes terület – lokalizációja. Utána az eljárás rögzíti a pupilla képét, kiküszöböli a szemhéj takarásából és a csillogásból eredő visszaverődésből származó zavaró értékeket [3]. Az így kapott „előfeldolgozott” kép kerül feldolgozásra és felismerésre.



Az írisz mintájának feldolgozása egy úgynevezett IrisCode record-ot eredményez, amelyet tárolva a későbbi összehasonlítások referencia értékét kapjuk. A rendszer annyira megbízható, hogy akár több millió ember azonosítására is képes [1,3].

Azonosítás aláírás alapján

Az aláírás azonosító-rendszerek kidolgozása már régen elkezdődött. A cél azoknak a paramétereknek a megeléje volt, melyek alapján a felhasználót nagy biztonsággal lehetett azonosítani. Ezek az író egyénre jellemző paraméterek az író toll dőlésszögének változása, a toll sebességének a változása, és az írófelületre kifejtett nyomóerő és annak változása [4,5]. Ezen a paraméterek méréséhez két platformot dolgoztak ki, az egyik egy speciális toll használata [6], mely kábelén közvetíti az információt a feldolgozó egységnek, a másik egy speciális írófelület használata [7]. A két megoldást kombinálva is lehet alkalmazni.



Az aláírásellenőrző berendezések a gyakorlatban meglehetősen pontosnak bizonyulnak, és olyan alkalmazások esetén optimális a használatuk, ahol az aláírás már elfogadott azonosítási eljárás.

Fontos megjegyezni, hogy a megoldások adaptívítása ugyancsak kulcsfontosságú az aláírás azonosító rendszereknél, mert az egyén kézírása az idő múlásával, akár drasztikusan is megváltozhat [4].

Gépelési dinamika

A gépelési dinamika a felhasználónak folyamatos ellenőrzésével történik (amíg a felhasználó a gép előtt van a rendszer figyelme és ellenőrzi a személyazonosságát). Kizárólag számítógépes rendszereknél használatos biztonságtechnikai eljárás.

Analizálja a felhasználó gépelési dinamikáját ezerszer egy másodpercben. Bizonyított, hogy az emberre jellemző a gépelési technikája, vagyis biometrikus azonosítóként használható. Ezen rendszerek biztonsági foka ugyan nem éri el a többi biometrikus azonosító biztonsági fokát, de a folyamatos figyelés nagy előnyt jelent a többi rendszerhez képest [1].

Retina letapogatás

Az emberi retina, csak úgy mint az írisz, nem duplikálható szerv, minden egyén esetén különböző. Az infrával végzett letapogatás a szemhátal érhálózatának rajzolatát tapogatja le.

Bevezetett technológia, melyben a retina egyedi alakzatát egy kisintenzitású fényforrás optikai sokszorozó felhasználásával letapogatja. A szem hátsó falán futó érhálózat képe a halál beálltával megváltozik, és el nem távolítható a szervezetből [1], vagyis ellopása lehetetlen.



A retinaletapogatás meglehetősen pontos azonosító rendszer, nagy hátránya a kényelmetlen használat. A felhasználónak pár másodpercig egy érzékelőbe kell tekintenie, úgy hogy közben a feje mozdulatlan marad.

Azonosítás hang alapján

Az emberi hang spektrumát analizálják (hangfelismerésben leginkább kepsztrumot használnak) és ezt hasonlítják össze a tárolt mintával. Minden ember hangjának más a spektruma, így ez a technológia szintén alkalmas felismerésre.

A hang alapján történő felismerés az egyik legkézenfekvőbbnek tűnő módszer. Egyes alkalmazások falra szerelhető érzékelőket használnak, míg mások annak a lehetőségét dolgozták ki, hogy hogyan lehet beilleszteni a hangellenőrzést a konvencionális telefonkagylókba.

A hangfelismeréssel két főbb alkalmazási területen lehet napjainkban találkozni: az egyik, mint biztonsági rendszer funkcionál, a másik épületek ajtók nyitására záráására szolgál [1].

Azonosítás ujjlenyomat alapján

Az ujjlenyomat azonosítására két fő biometriát alkalmaznak:

- *Minutia*: ez az ujjlenyomatok rajzolatában a különböző elágazásokat, rajzolat megszakadásokat, hurokokat, kereszteződéseket és hidakat jelenti.
- *Mintázat*: az ujjlenyomatok tipikus mintázatait, az alábbi főbb típusokba tartoznak: sima ív, sima hurok, dupla hurok, véletlen szerű, éles ív, csigavonal.



E paraméterek vizsgálata lehetővé teszi, hogy az azonosítás gyakorlatilag teljesen megbízható lehessen, több mint 100 különböző paraméter vizsgálatára van lehetőség (még az egyetétű ikrek ujjlenyomata sem egyezik meg). A biometriai azonosítók nagy részét az AFIS (Automatic Fingerprint Identification System – Automatikus Ujjlenyomat Azonosító Rendszer) rendszerek adják. Az általi szervezeteknél (FBI, INTERPOL, Michigan State Police stb.) használják az azonosításnak ezt a módját. Ez az azonosítás típus külön rendszert képez a biometriai azonosítók körében. Az USA-n kívül több mint 30 országban alkalmaznak AFIS rendszereket.

A minutia-azonosítás hagyományos rendőri módszerének emulációját használják (optikai, vagy kapacitív érzékelőkkel), mások egyszerű alakzatazonosító eszközök, ismét mások sajátos, egyedi megközelítést alkalmaznak, határtartományokat és ultrahangos letapogatást foglalva magukba [1,8]. Egyesek ezek közül felismerik, amikor élő ujjat tesznek a szenzorra, mások nem. Jelenleg a biometrikus eszközök közül legnagyobb számban az ujjlenyomat-vizsgáló eszközöket használják.

Nem meglepő, hogy a számítógépes munkahelyek hozzáférését, csaknem kizárólag ujjlenyomat-azonosítókkal védik, a viszonylag alacsony költségek, kis méret és könnyű integrálhatóság miatt [1]. Ezeket az azonosítókat leggyakrabban a kis populációszám jellemzi. Az ujjlenyomat-azonosítók számítógépes biztonsági változata a hagyományos jelszavakat egy egyszerű érintéssel helyettesíti [8].

Kézgeometria

A kézgeometria a kéz alakjának geometriájának a vizsgálatát jelenti, az ujjformákat beleértve. Ezek a paraméterek ugyancsak személyre jellemzőek és azonosításra alkalmasak (több mint 90 paraméter analizálására van lehetőség). Nem részletes az analízis, hogy a mikrosérülések ne befolyásolják a vizsgálat eredményét [9].

Amint a név is sugallja, a kézgeometria a kéz és az ujjak fizikai karakterisztikáinak mérésével foglalkozik, ezt egy 3D-s szkennelést végrehajtó platform végzi. Ezekben a rendszerekben kéz, egy ujj, vagy két ujj azonosítását szokták megvizsgálni. A vizsgálat kiterjedhet a három verzió együttes használatára is.

Mint az egyik legjobban elterjedt módszer, a kézgeometria nem csak gyors és pontos, hanem könnyen is kezelhető. Ez a módszer nagy felhasználói bázis esetén is alkalmazható, vagy olyan felhasználóknál, akik a rendszert ritkán használják és ennél fogva kevésbé gyakorlottak a rendszer használatában [1]. A felismerés pontossága igen jó, eközben a rugalmas elfogadási szint, a szabályozás és konfigurálás a felhasználók igen tág körének igényeit elégíti ki.



A kézgeometria-olvasóknak széles alkalmazási területe van, beleértve munkaidő-nyilvántartást is, ahol nagyon népszerűnek bizonyultak [1,9]. Könnyen integrálható más rendszerekbe és folyamatokba, ezért megbízható azonosító rendszert tudnak létrehozni.

A kézgeometria-olvasóknak széles alkalmazási területe van, beleértve munkaidő-nyilvántartást is, ahol nagyon népszerűnek bizonyultak [1,9]. Könnyen integrálható más rendszerekbe és folyamatokba, ezért megbízható azonosító rendszert tudnak létrehozni.

Komplex Biometrikus Azonosító Rendszerek

Minden biometrikus azonosítónak megvan a maga előnye és hátránya a többi azonosítóhoz hasonlítva. A komplex biometrikus rendszerek az azonosítók jó tulajdonságait ötvözve igyekeznek a megbízhatóságot növelni és két-három biometria alapján azonosítják a felhasználót [10]. Napjainkban több ilyen rendszer is létezik.

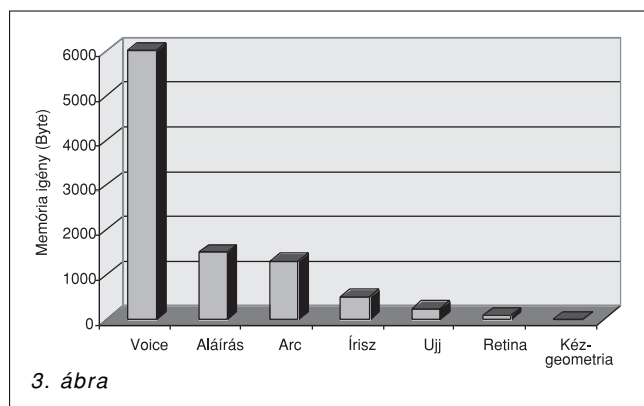
Olyan biometriákat választanak azonosításra, melyeket könnyű használni, és nem bonyolult a felhasználói interfész sem (hang, arc, szájmozgás stb.). Külön-külön azonban ezek az azonosítók nem lennének elég biztonságosak.

Az együttes alkalmazás során a bizonytalansági ráta nem összeadódik, hanem összeszorozódik. Ez azt jelenti, hogy három olyan biometria alkalmazásánál, ahol a téves belépési arány külön-külön 1:100-hoz, ezek kombinált használatával a téves belépés esélye sokszorosára, 1:1000000-ra változik [10]. Ez jelentős biztonsági javulást jelent.

Összefoglalás

A könnyű használatnak és a nagy megbízhatóságnak köszönhetően a biometrikus azonosítás lett a mérce a belépési jogosultságot ellenőrző alkalmazások terén. Az egyes azonosító rendszerekhez tartozó árak nagyon széles határok között mozognak. Egy biometriai azonosító-rendszernek az ára az alábbi fő részekeségekből tevődik össze: periféria, feldolgozó egység, memória, szoftver.

Az egyes azonosítókhoz tartozó biometriák memóriagénye is befolyásolhatja az egyes azonosítók elterjedését. A különböző biometriai rendszerek memóriagénye változó, amint azt a 3. ábra is mutatja [1].



A biometriai rendszerek használata a magánszférában egyre dinamikusabban nő. Mindezt a technológia rohamos fejlődése és az árak folyamatos csökkenése teszi lehetővé.

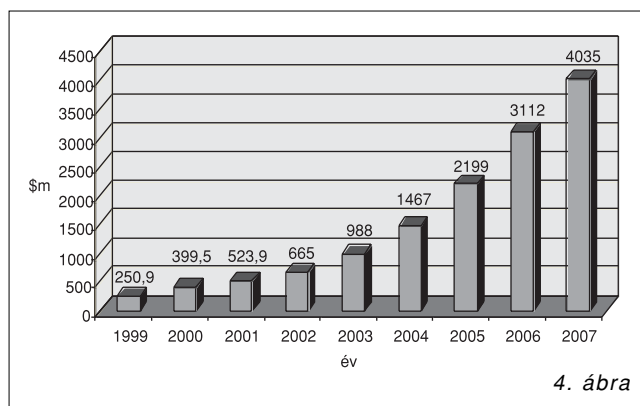
Azoknak a technológiáknak az elterjedése várható leginkább, melyekre a megoldások már kifinomultak (ujj, írisz, retina). Ezt követően azon azonosítók lesz a legnagyobb piaca, melyeknek használata nem okoz nehézséget, mert hozzátartoznak mindennapjainkhoz. Ide tartozik a hang és az aláírás alapú azonosítás. Az iparban egyre nagyobb számban lehet találkozni ezekkel a rendszerekkel, egyre inkább elfogadják a cégek, mint biztonsági technológiát.

Amint azt a 4. ábra is mutatja, a biometrikus azonosító-rendszerekből származó bevételek dinamikusan növekednek [1]. A növekedés dinamizmusát leginkább a PC/hálózati hozzáférés és az e-kereskedelem gerjeszti.

A biometrikus azonosító-rendszerek nagyon biztonságosnak tűntek az elmúlt évtizedekben, azonban ahogyan az elterjedtségük rohamosan nőtt, úgy kellett a kutató-fejlesztő cégeknek újabb nehézségekkel szembe nézniük. A biometrikus biztonsági rendszerek feltöréséhez új technikák alakulnak ki. Míg a hagyományos esetekben a biztonságot elsősorban jelszóval védték, addig itt olyan információról van szó, amit kitalálni, vagy ellopni lehetetlen.

Jelenleg a biometriai azonosítókat gyártó cégeknek a legnagyobb nehézsége az úgynevezett „azonosítók átverésének” a kivédése. A periféria becsapása, átverése teljesen más bonyolultságú feladat. Amíg valaki meg nem téveszti a perifériát, addig nem lehet tudni, hogy egyáltalán becsapható-e. Például az egyik biometriát gyártó cég a piacra hozott egy optikai biometriai azonosító-rendszert, amely csak élő ujjat fogadott el azonosításkor. A rendszer rendkívül biztonságosnak bizonyult, addig, amíg valaki rá nem lehelt a beolvasó szenzorra. A lehetetlent úgy érzékelt, mint ha élő ujjat tettek volna a perifériára, az optikán ott volt a nyoma az előző belépőnek, a rendszer beengedte a lehelőt. Egy más esetben az ujjlenyomat fénymásolatát sikerült használni sikeres belépéshez.

Ez azt jelenti, hogy eddig csak a biometriák sikeres és gyors azonosítása volt a kutatások fókuszában a biometrikus azonosítók elterjedését követően viszont teljesen új nehézségekkel kell szembenéznie a gyártó



cégeknek. Ez azt is jelenti, hogy amíg az összes technikai kérdés nem talál biztos választ, addig csak korlátozottan érdemes a biometrikus azonosítókat használni, vannak ugyanis olyan helyzetek, amikor a biometrikus azonosító rosszindulatú megtévesztésével nem kell számolni, ilyen helyzet lehet amikor az azonosítót használó ember közelben van (cégeknél biztonsági személyzet mellett van az ajtó, így ekkor jól látható, hogy mikor igyekeznek hamis módon befolyásolni az azonosítót).

Az elkövetkezendő néhány évben, a biometrikus azonosító-rendszerek elterjedésére lehet számítani, ugyanis egyre több helyen kell igazolnunk személyazonosságunkat és hozzáférési jogainkat. A biometrikus azonosítók mindezt nagy megbízhatósággal, kis költség- és kényelmesen képesek megvalósítani.

Irodalom

- [1] International Biometric Group, <http://www.biometricgroup.com>
- [2] Xiaguang J., „Extending the feature set for automatic face recognition”, thesis for the degree of doctor of philosophy, 1993.
- [3] Iridian Technologies, <http://www.sensar.com>
- [4] R. K. Abbas, „A prototype system for off-line signature verification using multilayered feedforward neural network”, thesis, 1994.
- [5] T. Wessels, C. W. Omlin, „Hybrid system for Signature Verification”, 1999.
- [6] H. S. M. Beigi, „An overview of handwriting recognition”, 1994.
- [7] CIC, <http://www.cic.com>
- [8] ActiveCard, <http://www.activcard.com/activ/products/other/biometrics/index.html>
- [9] A. Ross, „A prototype hand geometry-based verification system”, Biometrics Research, <http://biometrics.cse.msu.edu/>
- [10] BioID, <http://www.bioid.com>