HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Tajti Balázs
globee@freemail.hu

A BIOMETRIKUS UJJNYOMAT AZONOSÍTÁS ALKALMAZÁSÁNAK ÚJ LEHETŐSÉGEI

Absztrakt

Az emberiség létszámának gyarapodása megköveteli minden ember pontos azonosítását. Egyedül a biometrikus azonosítás alapul az emberek valódi, tőlük elválaszthatatlan azonosságán. A biometrikus azonosítás technológiája napjainkban egyre nagyobb teret hódít, és előre láthatólag ez a térhódítás csak gyarapodni fog. Rohamos elterjedése és széleskörű alkalmazhatósága miatt választottam kutatásom témájául ezt az azonosítási módszert. Kutatásom célja hogy bemutassam a személyazonosítás biometrikus lehetőségét és azok módszereit, részletesen ismertetve az ujjnyomat azonosítás technikáját. Kutatásom során elemeztem a biometriával foglalkozó cikkeket, tanulmányokat és internetes forrásokat, hogy az ujjnyomat azonosítás jövőbeli használhatóságáról és lehetőségeiről tájékozódjak, illetve hogy ezzel összefüggésben megismerjem az emberek véleményét a biometrikus formájú személyazonosítás módszerével kapcsolatban.

The growth of the population requires the accurate identification all of the people. Only biometric authentication based on people's real identity, which is inseparable from them. The biometric identification technology is becoming more and more popular, and this expansion will increase. Rapid spread and wide applicability is the reason, why I choose this identification method for my topic. My research aims, to demonstrate the possibility of biometric identification, its methods, and describe the fingerprint identification technique. During my research, I analyzed the use of biometrics from articles, studies, and internet resources, to get information about usability and possibilities about fingerprint identification, as well as get to know people's views of the form of the biometric identification method.

Kulcsszavak: *biometria, ujjnyomat, azonosítás ~ biometric, fingerprint, identification*

1. BEVEZETÉS

Az emberek pontos azonosításához évtizedek óta szerepelnek személyi igazolványunkon, gépjárművezetői engedélyünkön, útlevelünkön a legfontosabb azonosító tulajdonságaink, nevünk, címünk, születési dátumunk és helyünk. A számítógépes világban mindezen információk adatbázisokban szerepelnek, ahol mindannyian az igazolványainknak megfelelően egy-egy számsor szerint megtalálhatóak vagyunk. Bár ezen dokumentumaink rendelkeznek a pontos azonosításhoz szükséges arcképünkkel, az egyértelmű azonosításhoz mégis további egyedi azonosítókra van szükség. A biometrikus azonosítás nem más, mint bizonyos biológiai jellemzőink (ujjnyomat, kézgeometria, tenyérnyomat, írisz vagy retina vizsgálat, stb.) szerinti személyazonosítás. Ezeket a tulajdonságainkat speciális műszerekkel lemérik, majd digitális jelekké alakítva számítógépes adatbázisokban tárolják. Az azonosítás során ezen tulajdonságainkat vetik össze az adatbázisban szereplővel. A biometrikus azonosítás technológiája napjainkban egyre nagyobb teret hódít, és előre láthatólag ez a térhódítás csak gyarapodni fog.

2. BIOMETRIKUS AZONOSÍTÁS ÁLTALÁBAN

Mielőtt ismertetném a biometrikus azonosítás alkalmazását, fontosnak tartom, hogy információt adjak a szóban forgó azonosítási technikáról, ismertetve hol szerepel a személyazonosítás területén.

A személyazonosítás alapvetően az alábbi elveken alapul:

- Azonosító információ
- Azonosító tárgy
- Biometrikus azonosító

Azonosító információ: Valamilyen általunk ismert információ alapján. Általában numerikus kód vagy alfanumerikus jelsorozat (PIN, jelszó). Hátránya hogy az ember jelszavát elfelejtheti, ellophatják, vagy feltörhetik. Egyetlen előnye az egyszerűsége és olcsósága.

Azonosító tárgy: Valamilyen tárgy birtoklásán alapszik (belépőkártya, igazolvány, kulcs). Hátránya hogy könnyen elveszíthetjük, vagy ellophatják.

Biometrikus azonosítás: Ahogy bevezetőmben is említettem, a biometria nem más, mint a személyazonosítás egy olyan fajtája, ahol az ember egyedi biológiai jegyein, élettani vagy viselkedési jellemzőin alapul az azonosítási eljárás.

Az egyértelmű azonosításhoz az alábbi egyedi, személyenként eltérő jellemzőket használják:

Ujjnyomat-	Írás-
Tenyér és csuklónyomat-	Írisz-
Talplenyomat-	Retina-
Kézgeometria-	Hang-
Ujjerezet-	DNS-
Tenyérerezet-	Arc és alak-
Test hőkép-	Szag azonosítók, stb.

A biometrikus azonosítást már világszerte alkalmazzák, elsősorban beléptető rendszereknél, ahol a megbízhatóság alapját a nem átadható adat jelenti, így sem elveszíteni, sem ellopni nem lehet. Biometrikus azonosítónkat mindenhova magunkkal visszük, az olvasó szerkezetek kezelése pedig általában mindenki számára rendkívül egyszerű. Az azonosítás biometrikus formájának további alkalmazási lehetőségeiről a következő fejezetemben kívánok szót ejteni.

Fontos megemlíteni a biometrikus azonosítás biztonságának kérdését, amelyhez az FAR (False Accept Rate) illetve az FRR (False Reject Rate) mutatókat használjuk, magyarul Téves Elfogadás illetve Visszautasítás. [1]

FAR = Megmutatja, hogy az azonosítás milyen arányban ismert fel jogosulatlan felhasználót jogosultként.

FRR = Megmutatja, hogy az azonosítás milyen arányban utasít el jogosult felhasználót.

A pontosság az FAR és FRR értékgörbék metszéspontja, amely az EER (Equal Error Rate) érték. Néhány példa a rendszerek pontosságára (EER): [2]

- Hangazonosítás: 1 : 50
- Ujjnyomat azonosítás: 1 : 500
- Írisz azonosítás: 1 : 131.000
- Retinaazonosítás: 1 : 10.000.000+

A biometrikus azonosítás megfelelő formáját kiválasztva, ahogy a személyazonosítási eljárásokat elemeztük, láthatjuk, hogy egy rendkívül megbízható azonosítási módszerhez juthatunk, amely ténylegesen magát a személyt azonosítja. A biometria sok előnyén túl, hátrányokkal is számolnunk kell: [3]

- a módszerek legtöbbje rendkívül költséges, drága hardvert igényel,
- higiéniai szempontból a fizikai kontaktust igénylő megoldások problémásak,
- fogyatékkal élők számára egyes eljárások nem alkalmazhatóak,
- egyes fizikai jellemzők az idő múlásával vagy betegség következtében változhatnak, stb.

3. AZ AZONOSÍTÁS MÓDSZEREI

A korábbiakban csak felsorolás szintjén említett biometrikus azonosítási eljárásokból a fontosabbakat jelen fejezetben röviden kerül ismertetésre, külön részletesen kitérve az ujjnyomat azonosítás technikájára.

3.1. Biometrikus azonosítási módszerek

Tenyérnyomat azonosítás: A tenyérnyomat azonosítás nem egy általánosan használt biometrikus azonosítási forma, elsősorban bűntettek helyszínén lelhető fel. Azonosításukkor általában a tenyéren található fővonalak ráncolatát, a fodorszálakat illetve a szövetmintázatot elemzik, amelynek során gondos munkát követően az ujjnyomathoz hasonlóan jellegzetes információhordozót kaphatunk. (1. ábra) [4]

1. ábra. Tenyérnyomat azonosítás;
Forrás: http://www.chs81.com/sitebuildercontent/sitebuilderpictures/401pray/handprint.jpg;
http://stepintoyourlight.com/wordpress/wp-content/uploads/2009/11/Left-hand-print-244x300.jpg;
(2011. 09. 15.)

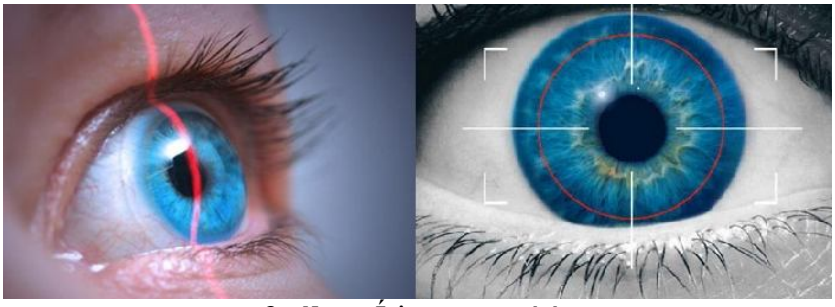
Kézgeometria azonosítás: A tenyérnyomatnál gyakrabban alkalmazott azonosítási eljárás, amelynek gyors leolvashatósága illetve pontossága adja előnyét. Működésének lényege, hogy a kéz felületéről és formájáról vesz mintát, és azt analizálja, így figyelembe veszi az ujjak hosszúságát és szélességét, a kézfej szélességét, illetve a tenyér és az ujjak méretarányát. A hatékony felismerést négy pozícionáló tüske segítségével érik el, amely azonos állásba helyezi a tenyeret a beolvasáshoz. Léteznek pozícionáló tüske nélküli felismerők is, ezek különböző sajátos értékeket elemeznek. Széles alkalmazási területtel rendelkezik, például munkaidő nyilvántartási rendszerek. Nagy előnye hogy más rendszerekkel is könnyen integrálható. [4] [5]

Ujj- és tenyérerezet azonosítás: Az ujj- és tenyérerezet azonosítás egy viszonylag új módszer a biometrikus azonosítás terén. A két módszer között lényegi különbség nincs, csak az eszköz más. A működés alapja, hogy az ujjat vagy tenyeret infravörös fénnyel megvilágítják, ami a különböző szövetekről a különböző szintű elnyelődés miatt, más intenzitással verődik vissza. Az érhálózatban lévő vér sokkal jobban elnyeli a fényt, így az szemmel látható módon kirajzolódik az eszköz számára. Az érhálózatokat más biometrikus azonosítási eljárásokhoz hasonlóan, jellegzetességeik alapján mérik. Előnyei közé tartozik, hogy nem befolyásolja felszíni sérülés, illetve szinte lehetetlen hamisítani. (2. ábra) [4] [6]

2. ábra. Tenyér érhálózat (bal) és ujj érhálózat olvasó (jobb)
Forrás: http://cache.gizmodo.com/assets/images/gizmodo/2008/07/palm-vein-scan.jpg; http://img.directindustry.com/images_di/photo-g/biometric-sensor-finger-vein-reader-396431.jpg

Írisz azonosítás: A szem szivárványhártyáján alapuló biometrikus azonosítás egyike a legjobb azonosítási módoknak, köszönhetően az akár 400 azonosítható jellemzőnek, amely segítségével a tévedés lehetősége minimálisra csökken. Az írisz életünk során nem változik, így az eljárás megbízhatósága nő. Annak az esélye, hogy két írisz megegyezzen, szinte kizártnak tekinthető, mivel az eljárás pontossága több mint 10^{70} nagyságrendbe esik.

A vizsgálat során a szivárványhártya látható és láthatatlan tulajdonságait elemzik. A látható közé tartozik az írisz sugaras mintázata, a körökkel, árkokkal és a koronával, a láthatatlan pedig az infravörös leolvasás során láthatóvá váló retinahártya erezet. Leolvasás során aktív illetve passzív felvételkészítésről beszélhetünk. Az aktív során a kamerához közel kell tartani a szempárját, míg passzív esetében a kamera az, ami bepozícionálja a szempárt. Az írisz azonosításon alapuló technika nagy hátránya, hogy a berendezések rendkívül bonyolultak, így áruk is magas. (3. ábra) [4] [7]



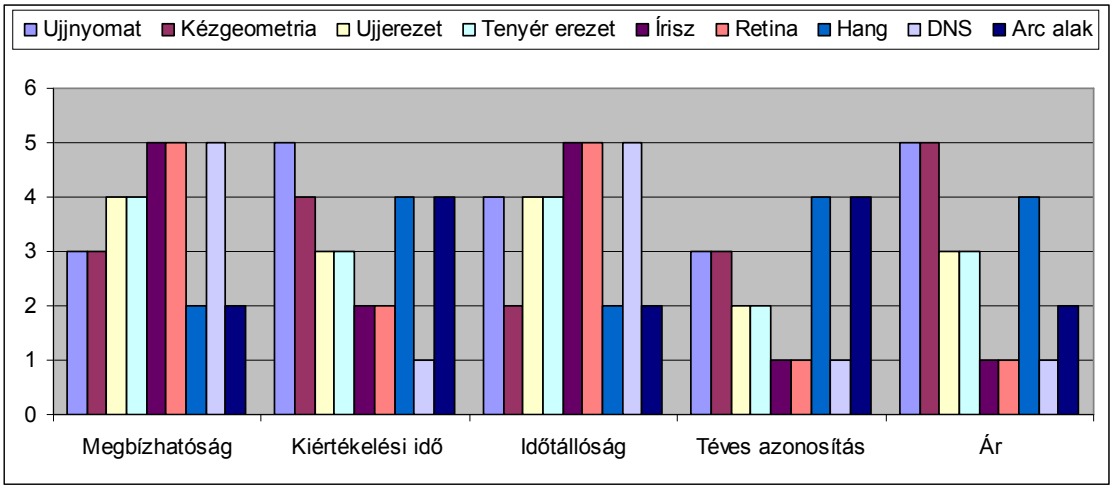
3. ábra. Írisz azonosítás

Forrás: http://www.airport-int.com/upload/image_files/articles/images/companies/1688/biometrics-sec01-l.jpg; http://fingerprint-security.net/wp-content/uploads/2011/05/Iris-Scan.jpg

Retina azonosítás: A retina alapú azonosítás során infravörös fénnyel világítják meg a szemfenéken található retinát, így az ujj- és tenyérerezet azonosítóhoz hasonlóan működve, az infrasugarak eltérő mértékben nyelődnek el, kirajzolva a szemfenék érhálózatát. A módszer egyik legnagyobb hátrányát jelenti, hogy a mintavételezési eljárás során az olvasóval közvetlen kapcsolatot kell kialakítania a szemnek, ami által nő a fertőzésveszély. Ilyen technológiát csak rendkívül ritkán alkalmaznak, általában nagy biztonságot igénylő helyszíneken. [8] [9]

DNS azonosítás: A DNS azonosítás eltér az eddig elhangzott azonosítási módszerektől, mivel a gyakorlati életben nem használható. Az eljárás egyrészről rendkívül időigényes, mivel nagyon bonyolult laborvizsgálatok szükséges elvégezni, másrészről egy emberi DNS bárhonnan beszerezhető, így akár egy hajszálból is másolható.

Az alábbi diagramom (1. Diagram) a különböző biometrikus azonosítási módszerek egyes tulajdonságainak értékelését kívánja bemutatni, 1-5-ig tartó skálarendszerben. Az 5-ös érték jelenti a legjobbat, az 1-es a legrosszabbat.



1. diagram. Biometrikus azonosítási módszerek tulajdonságainak értékelése

3.2. Az ujjnyomat azonosítás

Mielőtt ismertetném az ujjnyomat azonosítás technikáját, nézzük meg hogy pontosan mit is jelent az ujjnyomat. A daktiloszkópia három féle ujjról származó mintát különböztet meg:

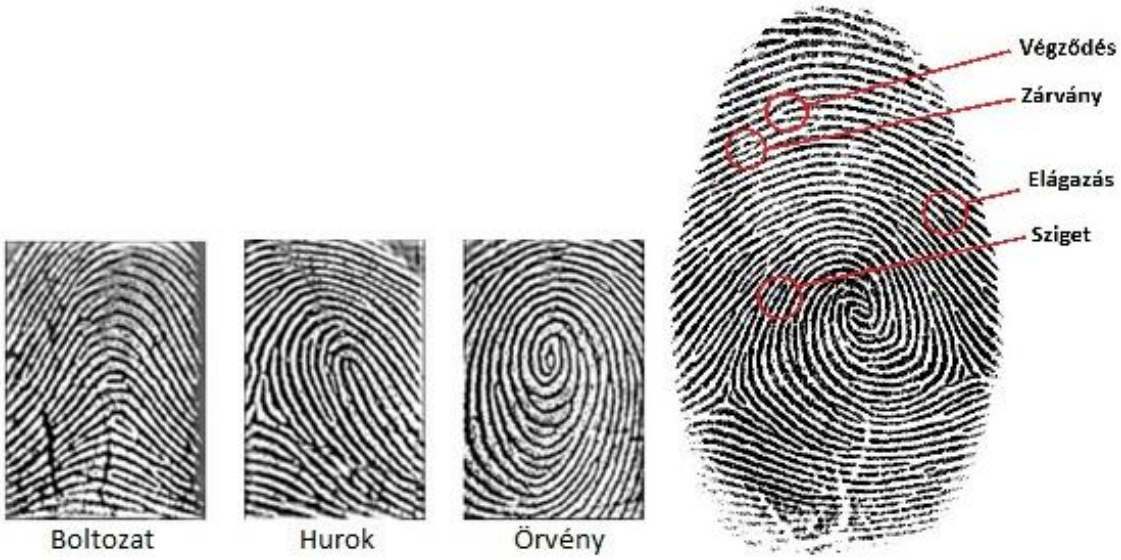
Ujjnyom: Azokon a tárgyakon lelhető fel, amiket az ember megérint. Általában rossz minőségű képet adnak.

Ujjlenyomat: Az ujjról készült jó minőségű képek, amelyek az ujjvégi ujjperc teljes, körömtől-körömig tartó lenyomatát képezi. Általában rendőrségi nyilvántartásokban használják.

Ujjnyomat: A síkfelületre helyezett ujj ott maradó, kétdimenziós lenyomata. Általában jó minőségű, a személyazonosításban használatos, a továbbiakban erről lesz szó. [16]

Az ujjnyomat azonosítási technika kulcsa, hogy az ujj barázdáltsága mindenkinek egyedi mintázatú. A mintázat 18 hetes korunkban alakul ki, és a későbbiekben sem változik, követi a kéz méretbeli változását. Az égés, vágás, kopás vagy marás során keletkező sebesülések 10-40 napon belül képesek regenerálódni. [17] Az ujjunkra tekintve láthatunk kis barázdákat, vonalakat, amelyeket fodor szálnak illetve fodor vonalnak nevezünk. A fodor szálak az ujjnyomat globális és lokális jellemzőit határozzák meg.

A *globális jellemzők* (4. ábra) a fodor vonal minták, amelyek három nagy csoportot alkotnak: [10] [12]



4. ábra. Globális és lokális ujjnyomat jellemzők

Boltozat: A barázdák az egyik oldalról a másik oldalra szinte egyenes vonalban, vagy boltozatot rajzolva haladnak át.

Örvény: A barázdák egy mag körül kör, spirális vagy ovális mintát követve rajzolódnak ki.

Hurok: A barázdák belépnek az ujjnyomat minta területére, majd a mag körül visszagörbülnek és a belépési vonalhoz közel hagyják el a minta területét.

A globális jellemzők relatív gyakorisága eltérő, a boltozaté 3%, az örvényé 25%, a huroké pedig 72%. [12]

A *lokális jellemzők* (4. ábra) a minuciákhoz kapcsolódnak. A minuciák nem mások, mint a barázdák jellegzetes mintái, ezek azok a tulajdonságok, amik nem egyeznek meg az embereknél. Ezeknek néhány jellemző típusai: Elágazás, híd, pont, sziget, kereszteződés, kettős híd, végződés, horog, oldalkontaktus, kettős elágazás, áthaladó vonal, stb. [13]

Az ujjról származó lenyomat azonosítás régóta ismert és használt módszer, már 1902-ben is alkalmazták a kriminalisztikában. A teljes ujjlenyomat kb. 100 jellegzetes minucia pontot tartalmaz, az ujjnyomat azonosítók pedig általában 60 minucia pontot hasonlítanak össze egy adott mintáról. A jelenleg használatos ujjnyomat olvasó rendszerek között jelentős különbségek lehetnek az olvasási technológia vagy a költségek szempontjából.

Nézzük át az ujjnyomat olvasási technikákat:

3.3. Ujjnyomat olvasó rendszerek

Az ujjnyomatok olvasására sokféle technikai megoldás létezik, a rendőrségi módszeren keresztül egészen az ultrahangos leolvasásig. Egyes ujjnyomat azonosítók képesek megvizsgálni, hogy az ujj élő-e, ezt pedig az ujj hőmérsékletének és\vagy nedvességtartalmának elemzésével végzik el. Az ujjnyomat azonosító eszközök közötti

hasonlóság, hogy mindegyik az ujjakon lévő fodor szálak egyediségét elemzi, tárolja le, és hasonlítja össze az azonosítandóval. (5. ábra)

5. ábra. Ujjnyomat olvasó rendszerek
Forrás: http://fingerprint-security.net/wp-content/uploads/2011/07/fingerprint-scan.jpg; http://www.procontrol.hu/GyartasFejlesztes/Termekeink/ProxerBio2/proxerbio_300.jpg

A különbség az olvasási technikákban van. Az olvasás alapvetően lehet optikai, illetve egyéb, nem optikai módszer.

Optikai elvű képfelvételek: [4] [14] A feldolgozandó ujjnyomatot egy képbontó eszköz felületére képezzük le egy optikai rendszer segítségével. A képbontó eszköz CMOS vagy CCD elem.

- Totálreflexiós: Az ujjunkat egy prizma felületére helyezzük, majd a megvilágítás során a kép egy képbontó eszköz felületére képződik le.
- Diffrakciós: A totálreflexióshoz hasonló működés, de prizma helyett fresnel lencsét alkalmazunk.
- Chip-szenzor: A szenzor felületére helyezzük az ujjunkat, a feldolgozandó információt pedig optoszálak vezetik a képbontó eszközre.
- Termikus elemzés: Az ujjnyomat olvasó érzékelőjéhez nem kell hozzáérni, csupán elhúzni az ujjat, amit szeletenként olvas le és alkotja meg a képet. A szenzor a bőr barázdáinak hőmérsékleti különbségét érzékeli.

Nem optikai elvű képfelvételek: [4] [14] Valamilyen egyéb, nem optikai elven működő eszközzel kerül az ujjnyomat beolvasásra.

- Rádiófrekvenciás elv: Rádiófrekvenciás jelet juttatunk az ujjra, amely azt visszasugározza a vevőantennaként szolgáló szenzor felületére. A rádiófrekvenciás jel, képes mélységi képet is alkotni az ujjunkról és barázdáiról.
- Kapacitív elv: Az apró kondenzátorokkal rendelkező szenzor felületére helyezzük az ujjunkat, amely eltérő kapacitást mutat a barázdák és a köztes völgyek függvényében. Az eltérő kapacitás kerül elektromos jellé alakítva kiértékelésre.
- Ultrahangos elv: A szenzor ultrahangot sugároz az ujjra, amelyről visszaverődő hullámokból mélységi képet alkot.
- Nyomásérzékelős elv: A szenzor felülete alatt piezo-elektromos nyomásérzékelő mátrix helyezkedik el, amely az ujjfelület egyenetlenségeit érzékelve alkot képet.

4. ALKALMAZÁSI LEHETŐSÉGEK

A biometrikus azonosítás már nem a jövő gondolata. Elegendő olyan mindennapi dolgokra gondolni, mint az új útlevelek, egyes laptopok és mobiltelefonok, és láthatjuk, hogy széles körben egyre gyarapszik a biometrián alapuló azonosító rendszerek felhasználási köre. A biometrikus azonosítási eljárásról már kijelenthetjük, hogy az a technológia, ami 15 évvel ezelőtt a távközlés, 10 évvel ezelőtt pedig az internet volt. A biometria egy olyan új technológia, amely rohamos ütemben fejlődik, és az élet egyre több területén fog aktívan jelentkezni.

A rohamos elterjedés mögött mind a kereslet, mind a kínálat szerepel. A keresleti oldalon megvan az igény a biztonságra. Az államok szeretnék tudni kik lépik át határaikat, a cégek pedig szeretnék tudni kik lépnek be épületeikbe. A kínálat oldalán pedig megjelennek a rendkívül kompakt és olcsó eszközök, amik könnyedén beépíthetőek bármilyen eszközbe.

Az emberek az új technológiát egyre elfogadottabbnak tartják, egyre gyakrabban alkalmazzák laptopjuk vagy telefonjuk védelmére, külföldön pedig már széles körben alkalmazzák jelenleg is, íme néhány példa:

- Chicago: A biometrikus fizetés lehetőségét tesztelik az autósok. Bizonyos benzinkutakon már ujjnyomattal is fizethetnek, az ujjnyomat érzékelős készülékek az autósok bankszámlájához kapcsolódnak, így a fizetés onnan történik. [15]
- Japán: Ujjnyomat érzékelős pénz automatákat alkalmaznak bizonyos bankok ATM rendszerei, pénzfelvétel céljára. (6. ábra) [16]
- Florida: Disney World-ben a beengedő kapuknál minden látogatótól ujjnyomatot vesznek és társítják a belépőkártyájukhoz. [15]
- Nagy-Britannia: Írisz felismerésen alapuló beléptető rendszer a nagyobb repülőtereken a gyakran visszatérő látogatók számára. [17]
- Egyesült Államok: 1996 óta alkalmaznak egyes büntetés végrehajtó intézményekben írisz felismerésen alapuló rendszert a rabok nyilvántartására. [18]

6. ábra. Ujjnyomat érzékelős ATM
Forrás: http://www.itcbd.com/wp-content/uploads/2010/09/Biometric-Solution.jpg;

Talán a legjobb példa a biometrián alapuló azonosítási rendszerek széles körű alkalmazására, az Egyesült Államok bevándorlási hivatalának rendszere. A rendszer a belépő személyek ujjnyomatát hasonlítja össze az adatbázisában szereplő több mint 2,5 millió azonosítójával. 2004-es bevezetése óta több mint 75 millió látogató ment keresztül a rendszeren, és körülbelül ezer alkalommal tagadták meg a belépést. [15]

A biometrikus azonosítás nem más, mint a jövő a jelenben. Lássunk néhány lehetséges felhasználási területét a biometrián, azon belül is az ujjnyomat azonosításon alapuló rendszereknek:

- Bank automaták szolgáltatásai: Ahogy más országokban már napjainkban is sikeresen működik, úgy hazánkban is várhatóan meg fog jelenni a bankkártya nélküli biometrikus azonosításon alapuló bank automata használat.
- Személyazonosítás: Mindenhol alkalmazhatóvá válik a biometrikus azonosítás módszere, ahol jelenleg is igazolnunk kell magunkat.
- Munkaidő nyilvántartás: Munkahelyünkön a munka megkezdése egy biometrikus azonosítással történik, ahogy a munkahelyünk elhagyása is, ezzel máris kiküszöbölhető a munkaidő eltitkolt rövidítése.
- Kasszánál történő fizetés: Bankkártyánk helyett elég ujjnyomatunkat használnunk, és a kasszánál történő fizetés gyorsabb és biztonságosabb is lesz.
- Belépés azonosítás: Munkahelyre történő belépés során biometrikus azonosítónkkal igazoljuk magunkat és jogosultságunkat a belépésre.
- Csekkbeváltás: Nem szükséges igazolvány hordása, elegendő az ujjnyomatunk használata.
- Otthoni biztonsági rendszer: Vagyonvédelmi rendszerünket, vagy intelligens otthonunkat nem kell kóddal aktiválni, biometrikus azonosítónk alapján felismer minket, a vagyonvédelmi rendszert iktatja, az intelligens épület automatika pedig előre meghatározott módon jár el.
- Bankkártya biztonság: A kód elleshető, kitalálható, ujjnyomatunk azonban csak kikényszeríthető, a kettő együttes alkalmazása viszont biztonságot adhat.
- Elektronikus fizetés: Elektronikus formában történő fizetés esetén elegendő egy géphez csatlakoztatható ujjnyomat azonosító, és a hitelesítés a jelszón túl már nagyobb biztonságot nyújt.
- Elektronikus hozzáférés: A fizetéshez hasonlóan hitelesít minket biometrikus azonosításunk alapján.
- Részvétel ellenőrzés: Kötelező részvétel esetén nem játszható ki az ujjnyomat olvasó rendszer, ott kell lennünk személyesen.
- Utazás szabályozás: Országok határait átlépve azonosíthatjuk magunkat, repülőgépes utazás során rendkívül hasznos.
- Távoli szavazás: Hazánkon kívül is leadhatjuk voksunkat egyszerűen azonosítva magunkat.
- Automata eszközműködtetés: Az intelligens otthont megteremtve, az automatizált gépeket, ujjnyomatunk alapján felprogramozhatjuk tevékenységekre.
- Jogosultság ellenőrzés: Például gépjárművek esetében központi ellenőrzés a jogosítvány meglétére.
- Szerver biztonság: Hitelesség ellenőrzése biometrikus azonosság alapján.
- Stb.

Az említett lehetőségek csupán néhányak a sok közül, hiszen az ujjnyomat azonosításon alapuló technikák mindenhol alkalmazhatóak ahol fokozott biztonságra van szükség, vagy ahol a mindennapi életben is szükséges személyazonosságunk igazolása, illetve kártyák és jelszavak, PIN kódok alkalmazása. [19]

4.1. Felmérések és vélemények

Kutatásom során sikerült a magyar lakosság véleményalkotásáról is képet kapnom. A felmérést a Polygon Informatikai Kft. készítette, kizárólag tájékoztató jelleggel kívánom bemutatni. A felmérésen 548 fő vett részt, akik 18 és 60 év közötti lakosok.

A felmérés négy kérdésből állt, amelynek során a biometrikus azonosítási eljárások ismertségét vizsgálták. A válaszadók 85%-a hallott már ilyen típusú azonosítási eljárásról, de mindössze 13%-uk találkozott már vele. A válaszadók jelentős része filmekből vagy híradásokból tájékozódott a technikáról. Bár a résztvevők nagy részének véleményalkotása

nem a személyes tapasztalaton alapszik, mégis csak a megkérdezettek 16%-a mondta, hogy soha nem vennék rá alkalmazására.

A lakosság jelentős része tehát kész befogadni és alkalmazni a biometrikus azonosítási technikákat, elsősorban olyan helyeken, mint a határforgalom, banki ügyintézés, vásárlás vagy hivatalos ügyek intézése, annak ellenére is, hogy többségük még nem használta soha, vagy nem rendelkezik róla mélyebb tudással. [20]

4.2. Biometriával kapcsolatos aggodalmak

Bár a biometrikus eljárások a szakértők véleménye alapján is biztonságosnak tekinthetők, nehezebb feltörni őket, de nem szabad megfeledkeznünk róla, hogy ezeknek a rendszereknek is vannak gyenge pontjai. Jelen dolgozatomban nem kívánok részletesen foglalkozni a biometrikus azonosítási technológiák veszélyforrásaival, azonban az alapvető aggodalmakat meg szeretném említeni.

Az általam feldolgozott források és tanulmányok alapján kijelenthetem, hogy az emberek aggodalma két fő csoportba osztható:

Az egyik a biztonság, amely a támadástól vagy feltöréstől való félelem. A biometrikus rendszerek feltörésének valós veszélyei vannak. A rendszerek legsebezhetőbb pontjai pedig a háttér adatbázisok, és a csatornák, amelyek a rendszer egyes elemeit összekötik. Biometrikus és kriptografikus módszerek okos kombinációival azonban megakadályozható, hogy ezeknek a rendszereknek az adatait a hackerek lehallgassák, továbbítsák vagy módosítsák.

A félelem másik forrása, a visszaélés, amelynek során az állam vagy a hatósági személyek visszaélnének adatainkkal és azt nyomon követésre használnák.

A fent említett két félelemforrás megfelelő törvényi szabályozással, odafigyeléssel és a kételyek eloszlatásával orvosolható, azonban figyelembe kell venni, hogy egyes emberek vallási alapon nem lennének hajlandóak használni az eszközöket.

Az aggodalmak ellenére a biometriai technológiák fejlődése megállíthatatlan, hisz egyrészről kényelmet, másrészről biztonságot nyújtanak az embereknek, és szinte biztosan állítható, hogy a jövőben egyre gyakrabban fogunk találkozni a személyazonosítás biometrikus lehetőségével.

5. ÖSSZEGZÉS

A biometrikus azonosításon alapuló technológiák az utóbbi éveket megfigyelve rendkívül gyors tempóban fejlődnek és terjednek el széles felhasználási körben. Ez a folyamat pedig megfelelő odafigyeléssel és adatvédelmi szabályozással egybekötve pozitív hatással, megkönnyítve hathat az emberek mindennapi életére. A biometrikus azonosítás a jövőben mind hétköznapibbá fog válni, és idővel nem lesz szükségünk semmilyen azonosító eszközre, csak személyes jelenlétünkre. Bár a hagyományos azonosító eszközök teljes felváltása a közeli jövőben még nem lehetséges, de valószínűsítem, hogy a bank automatától kezdve egészen a hivatali ügyek intézéséig minden biometrikus azonosítással fog történni. A világ a biometrikus azonosításnak köszönhetően meg volt változni, ez feltartóztathatatlan, a megfelelő használat azonban elsősorban tőlünk, emberektől függ.

Felhasznált irodalom

[1] [1] Bromba Biometrics: Biometrics FAQ, http://www.bromba.com/faq/biofaqe.htm; (2011. 09. 10.)

[2] Biometriai alapelvek, http://www.slideshare.net/szabojudo/biometriai-alapelvek; (2011. 09. 10.)

[3] Biometrián alapuló azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=143; (2011. 09. 13.)

[4] Dr. Kovács Tibor: Biometrikus azonosítás, Főiskolai digitális jegyzet, BMF, Budapest, 2009.

[5] Kézgeometria, http://handyman.hu/szakkifejezesek/kezgeometria/; (2011. 09. 15.)

[6] Vein Recognition Biometrics, http://www.findbiometrics.com/vein-recognition/; (2011. 09. 17.)

[7] Írisz azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=149; (2011. 09. 17.)

[8] Retina azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=148; (2011. 09. 20.)

[9] Retina azonosítás, http://www.recoware.hu/biometria/biometriai_azonositas/biometriai_azonositasi_modszerek_felsorolas_retina.html; (2011. 09. 21.)

[10] Ujjnyomat alapú azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=144; (2011. 09. 25.)

[11] Bunyitai Ákos: A ma és a holnap beléptetőrendszereinek automatikus személyazonosító eljárásai, Hadmérnök, VI. évfolyam, 1. szám, 2011

[12] Ujjnyomat azonosítás, http://sdt.sulinet.hu/Player/Default.aspx?g=9ef262fa-640b-4977-a546-43ef6613adaa&cid=d719a68c-3bea-46ce-9f54-dca11d4f8e9c; (2011. 10. 10.)

[13] Daktiloszkópia, http://www.biztostu.hu/mod/resource/view.php?id=145; (2011. 10. 13.)

[14] Ujjnyomat érzékelés technikák, http://oktel.hu/szolgaltatas/belepteto-rendszer/biometrikus-azonositas/; (2011. 10. 13.)

[15] Jövő már a jelenben, http://www.origo.hu/tudomany/20071105-biometrikus-azonositas-jovo-mar-a-jelenben.html?pIdx=1; (2011. 10. 15.)

[16] Ujjnyomat a kézpénzfelvételhez, http://www.digibiz.hu/elegendo-egy-ujjlenyomat-a-keszpenzfelvetelhez/20100604; (2011. 10. 17.)

[17] Írisz felismerés, http://www.nagyutazas.hu/magyar/utikalauz/article.php?id=557&no_results_total=80&lstresults=3; (2011. 10. 17.)

[18] Iris recognition, http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/now.html; (2011. 10. 17.)

[19] Future of biometrics, http://www.optel.com.pl/article/future%20of%20biometrics.pdf; (2011. 10. 20.)

[20] Felmérés, http://www.hwsw.hu/hirek/31920/biometrikus_azonositas_felmeres.html; (2011. 10. 20.)