**Biometrikus azonosítás**

*A biometrikus azonosítás különböző fajtáinak működése egyaránt azon alapul, hogy a rendszer az emberi szervezet vagy viselkedés valamely egyedi sajátosságáról mintát vesz, azt digitális adattá konvertálja és adatbázisban tárolja, majd az aktuálisan levett mintát összeveti az ebben az adatbázisban tárolt mintákkal.*

A hivatalos definíció szerint **a biometria az alapján azonosít, ami az ember maga, nem pedig az alapján, amit** **tud** (kód, jelszó), **vagy amije van** (kártya, távirányító). Ez utóbbiak a megfejtésük vagy eltulajdonításuk esetén azok már valójában nem azt a személyt fogják azonosítani, akihez eredetileg hozzárendelték.

**A biometrikus azonosítás változatai**

A biometriai azonosítás során használnak **fizikai jellemzőket:** ujjlenyomat-, kéz- írisz-, arcazonosítást és DNS-elemzést, valamint azonosíthatnak **viselkedésbeli jellemzők** pl. gépelési stílus, aláírás vagy hang.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Mi szükséges ahhoz, hogy az emberi szervezet vagy viselkedés bizonyos tulajdonsága alkalmas legyen a biometrikus azonosításra?

* egyediség (mindenkinek van, de különbözik másokétól)
* permanencia (a korral, betegséggel járó változások során nem változik)
* mérhetőség (adattá konvertálható)
* gyors azonosíthatóság (elvárt teljesítmény)
* elfogadhatóság (a mintavételt ne utasítsák el pl. higiéniai okból)
* megbízhatóság (hamisítás, kikerülés elkerülésére)

**A biometrikus azonosítási metódus 4 lépése**

1. Mintavétel az adatbázishoz: ujjlenyomat, kéz, tenyér, hang stb. beolvasása mindenkiről, aki az azonosítási rendszerben érintett lesz.
2. Adatbázis létrehozása: a fiziológiás jellemzőkről beolvasott mintákat, illetve az azokból készült bináris kódot nevesítve, személyhez rögzítve eltárolja a rendszer.
3. Felhasználói mintavétel: a rendszer beolvassa az aktuális mintát az azonosítandó személyről, és ezt kódolja, ha szükséges.
4. Ellenőrzés vagy azonosítás: a beolvasott aktuális mintát a szoftver összeveti az adatbázisban rögzített adatokkal.

**A biometrikus beléptető rendszerek biztonsági mutatói**

Az alábbiakban összehasonlítjuk néhány biometrikus beléptető rendszer jellemzőit:

**Azonosítás FAR[[1]](#footnote-1)\* Idő (s) Megbízhatóság Állandóság Higiénia**

Arc 2000:1 1 alacsony nem megfelelő

DNS n.a. órák magas igen mintától függ

Érminta n.a. 0,4 közepes igen megfelelő

Hang 500:1 5 alacsony igen/nem kitűnő

Írisz 12 000 000:1 n.a. nagyon magas igen megfelelő

Kéz 700:1 <5 alacsony nem alacsony

Retina 10 000 000:1 10-15 nagyon magas igen megfelelő

Ujjlenyomat 1 000 000:1 0,2-0,4 közepes igen alacsony

**Adatvédelem és aggályok**

Az Európai Unió már 2004-ben úgy döntött, hogy az útleveleknek tartalmazniuk kell az ujjlenyomatot. (Magyarországon 2006-ban kezdték kibocsátani a biometrikus útleveleket.) Ezzel akkora nemzetközi adatbázis jött létre, amelynek a kezelése rendkívül komoly biztonsági követelményeket támaszt.

Szeptember 11. után a biztonságra való törekvés még jobban megerősödött, olyan méreteket öltve, amelyet előtte el sem tudtak képzelni. Például a rabosítás során levett ujjlenyomatok (vagy egyes országokban az írisz) adatai eredetileg csupán a büntetőeljárásban, illetve a bűnügyi nyilvántartóban voltak megtalálhatóak, de ma már a terrorizmus elleni harc intézkedéseinek következtében a mindennapok részévé váltak.

A modern kor azonosítási procedúrája automatizálódik, berendezések és szoftverek végzik a beérkezett és a tárolt információk összevetését, nem pedig a határőr vagy rendőr ellenőrzi a fotót és a személyt. Ezzel együtt 2012-re már több százezer hamis biometrikus útlevél került forgalomba az EU-ban, és több százezer olyan, amelynek az ujjlenyomat mintája értékelhetetlen. Főleg gyermekek és idősek ujjlenyomatai bizonyultak megbízhatatlannak, de az EP már végzi a biometrikus útlevelek felülvizsgálatát.



Magyar biometrikus útlevél

**Vigyázat, csalnak!**

A biometrikus beléptető rendszer biztonságosságát is a legsebezhetőbb pontja határozza meg. Ezért a műszaki fejlesztők és a csalók egyaránt a gyenge pontot keresik, nyilvánvalóan különböző okokból, de minden bizonnyal egymással versenyezve.

Már jó ideje nem számít komoly ujjlenyomat olvasó rendszernek a nemzetbiztonságban az, amelyet át lehet vágni egy levágott ujjal, de még a fejlettebbeket is becsaphatja ma még egy jól elkészített szilikon ujjlenyomat.

Kezdetben még egy nyomtatott fotó az íriszről vagy egy mesterséges szem elegendő volt a rendszerbe való illetéktelen bejutáshoz, majd javultak a leolvasók és jöttek a speciális kontaktlencsékkel való sikeres támadások. Ezek használata viszont ma már egyértelműen lebukáshoz vezet. A szemgolyó sejtjei olyan gyorsan halnak el, hogy értelmetlen próbálkozás lenne egy biometrikus azonosítás miatt eltávolítani azt a természetes helyéről.

Az arcfelismerő rendszereket ideiglenes álcákkal, sminkkel nem lehet befolyásolni, de maszkokkal (itt is a szilikon a nyerő) sikerülhet a csalás egyes esetekben. A legbiztosabb átvágás persze a plasztikai sebészet alkotta új arc, de orvosi okokból ez is korlátozott mértékben lehet hatásos. Esetleg meg kell kérni az egypetéjű ikertestvért, mert a tökéletesen egyforma ikerpárokat egyelőre még nem sikerült megkülönböztetni.

1. \* A FAR (False Accept Rate) mutató azt mondja meg, hány helyes azonosításra jut egy téves. [↑](#footnote-ref-1)