KOVÁCS TIBOR – MILÁK ISTVÁN – OTTI CSABA

A BIZTONSÁGTUDOMÁNY BIOMETRIAI ASPEKTUSAI

A biztonságtechnika napjaink legrohamosabban fejlődő tudományága az egyén biometriai tulajdonságai alapján történő azonosítási eljárás. A biometrikus azonosítás nem a 21. század terméke, - hiszen arc-, hangfelismerésről az emberi civilizáció megjelenése óta beszélhetünk-, de az egyre kifinomultabb mikroelektronikai eszközök fejlődése lehetővé tette a biometrikus azonosítás elterjedését.

Mindennapi életünk részévé válhat a közeljövőben ezen eszközök rendszeres használata, mivel olyan azonosítási lehetőséget biztosít, amin igen nagy költség- és energia ráfordítással tudunk biztonsági rést találni a modern eszközök esetében. Legyen szó akár egy beléptető rendszerről, akár egy olyan ATM használatánál, - ahol nem egy kód, hanem a tulajdonos biometriai jellemzői alapján történik az azonosítás-, előnyt élvezünk a tulajdon, vagy a tudás alapú azonosítási módszerekkel szemben, hiszen biometria jellemzőink általában tulajdonunkat képezik, java részt felejthetetlenek, és rendelkezésünkre állnak. Ezek a jellemzők a modern technikai felhasználásával olyan azonosítási lehetőségeket biztosítanak, ami olyan nagyobb biztonsági kockázatú műveletek elvégzését, létesítményekbe való bejutást tesz lehetővé, amire már egy egyszerű kártyás, kód alapú rendszer elavult. A biometrikus azonosítás eszközei azonban nem szorítják ki a fent említett azonosítási eljárásokat, hiszen számos eszköznél ezek kombinálva jelentkeznek az azonosítási eljárás során.

1. A biztonságtudomány, biometria, és a biometrikus azonosítás

„*A biztonságtudomány célja a rendszerek biztonsági funkció központú elemzése, a rendszerbiztonság tervezése, részletes kidolgozása. Ezekből fakadóan a biztonságtudomány az egészségmegőrzés egyik eszköze és az objektív valóság létező állapotának egyik aspektusa is egyben. A biztonság iránti igény, akár a biztonsággal kapcsolatos problémák az emberi gondolkodással egyidős. A megismerés a kisebbtől a nagyobb felé, vagyis a kevésbé ismerttől a bonyolultabb megismerése felé halad, amelyben több kutató szakaszokat azonosít (ártatlanság, felfedezés, rendszer biztonság, biztonságtudomány). A biztonságtudomány rendszere horizontálisan a filozófia mellett a biztonság és biztonságtechnikai tudományra figyel, vertikális rendszerében a biztonsági filozófia és az egyes horizontális elemek helyezkednek el.*”[898]

A biometria, mint kifejezés a görög „bio” – élet és „metria” – mérés szavak összeillesztéséből ered. Általánosságban valamilyen élőlény valamilyen élettani jellemzőjét mérjük. A biometrikus azonosítás esetében az élőlény egy adott ember, és a biometrikus jellemzői saját személyi jellemzőinek tekinthető, amelyek alapját képezik a személyazonosságának és jogosultságainak meghatározásának. Definíciószerűen megfogalmazva a biometrikus azonosítás olyan automatikus technikát igénylő eljárás,

[898] Lasz György: A biztonságtechnika alapjainak megjelenése az objektumvédelem gyakorlatában. Hadmérnök 2011. 3. szám, 32. o.

amely „méri és rögzíti egy személy egyedi fizikai, testi jellemzőit, viselkedésbeli jellemvonásait, és ezeket azonosítás és hitelesítés céljára használja fel. A biometrikus felismerés alkalmazható személyazonosítás céljára, amikor a biometrikus rendszer azonosítja a személyt, az egész lajstromozott adatállományból kikeresve a megegyezőt, valamint használható ellenőrzés céljából, amikor a rendszer hitelesít egy személyt az előzőleg róla felvett és eltárolt minták alapján.”[899]

A biometrikus jellemzőknek két nagy csoportját különíthetjük el, a biológiai, valamint a viselkedési jellemzőket.[900]

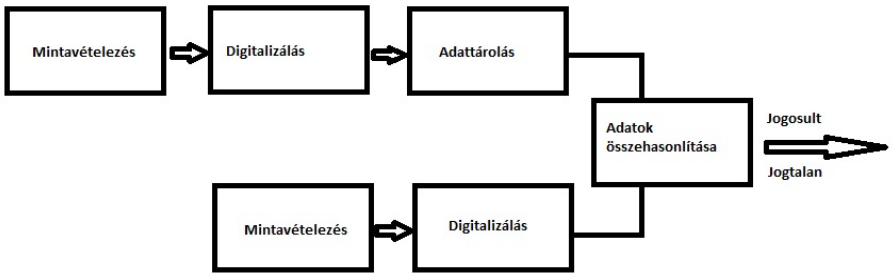
Biológiai jellemzők:
- bőrmintázat: ujjnyomat, ujjlenyomat, ujjnyom, tenyérnyomat, talplenyomat
- kézgeometria
- Érhálózat: tenyérerezet, ujjerezet
- arc: kép, termo gramm
- szem: írisz, retina
- illat
- DNS

Viselkedési jellemzők:
- kézírás (íráskép, dinamika)
- beszédhang
- gépelési ritmus
- járási mód

2. Az azonosítási eljárásról általában

Maga a folyamat két jól elhatárolható részből áll. Az első rész a regisztráció, amely a rendszer használatára jogosult személy valamilyen biometriai jellemzőjének mintavételezéséből (maszk), majd a kiolvasott adathalmaz digitalizálásából és az adatok tárolásából áll. A második rész az azonosítás, amely ugyancsak mintavételezésből, majd digitalizálásból, ezután az adatok összehasonlításából áll. Ezt követően, ha a minta megegyezik az adatbázisban tárolt mintával, akkor jogosultnak, ha nincs egyezés a tárolt és az éppen kiolvasott mintában, akkor jogosulatlannak nyilvánítja a rendszer az adott egyént a belépésre, vagy valamilyen cselekvés elkezdésére a védeni kívánt létesítményben, hálózatban, vagy valamilyen zártkörű rendszerben.

[899] Ketskeméty Gábor: Biometrián alapuló személyazonosító rendszerek, szakdolgozat. Budapesti Műszaki Főiskola Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar. Budapest, 2008. 4. o.
[900] Uo. 7. o.

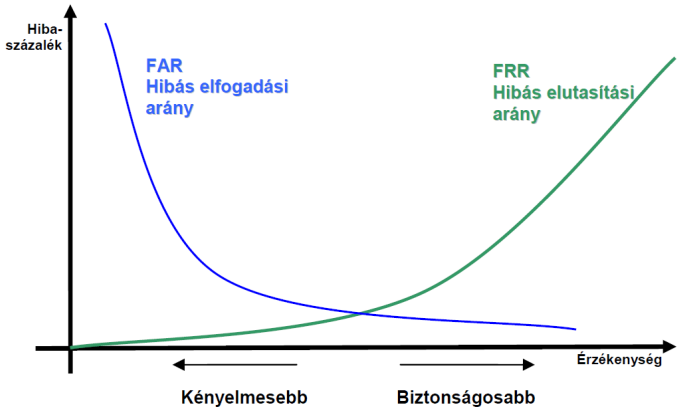


2. ábra: A biometrikus azonosítás folyamata

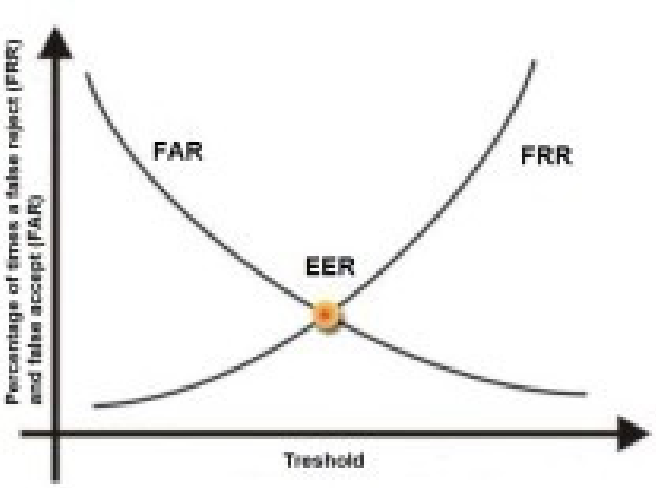
3. A biometrikus azonosítás mutatói, minősítő jellemzői

A folyamat egyfajta végeredményének tekinthetjük az eszköz rendeltetés szerinti működését, miszerint az adatbázisban szereplő mintát, és az aktuálisan beolvasott mintát egyezőnek, a mintát jelenleg birtokló egyént jogosultnak nyilvánítja a rendszer, vagy pedig az adatbázisban szereplő minták egyikével sem azonos az aktuálisan beolvasott minta, így a minta tulajdonosát jogtalannak ítéli az eszköz. Ezen eredményen belül azt az eshetőséget figyelembe véve, hogy maga az eszköz követ el valamilyen hibát az azonosítás során, két fő mutatót alkalmaznak az eszközök minősítésére. Megkülönböztetünk úgynevezett FAR (False Acceptance Rate) téves elfogadási arányt, valamint FRR (False Rejection Rate) téves elutasítási arányt. Abban az esetben, ha az alany valójában jogosult valamire, de a folyamat végeredménye nem támasztja ezt alá, FRR téves elutasítási arányról, ha valójában nem jogosult, de a folyamat hibásan jogosultnak nyilvánítja, téves elfogadási arányról, FAR-ról beszélünk.

A FAR-t és az FRR együttesen egy diagramon ábrázolva két görbét kapunk, amik egy ponton metszik egymást. Ezt a pontot nevezzük EER (Equal Error Rate) egyenlő hiba aránynak. Ebben a pontban a FAR és FRR ugyan azt az értéket veszi fel, tehát a hiba azonos.



3. ábra: FAR, FRR görbék



4. ábra: Az EER metszéspont

Említésre méltó néhány azonosítási eljárásra vonatkozó átlagolt FAR mutató:[901]

- hangazonosítás: 500:1
- ujjnyomat azonosítás: 1000000:1
- retina és íriszazonosítás: 10000000:1

Az eszközök minősítésére szolgáló mutatók még az úgynevezett ACOM (Anti-Cloning Operation Methods) és a MOA (Mission Oriented Application). Az ACOM megmutatja, hogy az eszköz működési elve milyen mértékben zárja ki a hamisított minta felhasználását. A MOA feladat orientált alkalmazás, mint mutató arra vonatkozik, hogy az adott eszközt milyen biztonsági igényű feladatokra lehet alkalmazni.

Ahogy azt már említettük az ACOM minősítő mutatóval kapcsolatban, kulcsfontosságú kérdés lehet, hogy az adott eszköz rendelkezik-e élőminta felismeréssel. Abban az esetben, ha egy eszköz rendelkezik élőminta felismerésére alkalmas technikai megoldással, az eszközt az azonosítási fajtájától függően jóval magasabb szintű biztonságot igénylő feladatok ellátására is alkalmazhatjuk. További minősítési szempont az automatizálhatóság, és a teljes azonosítási idő. A korszerű rendszerekben számítógép vezérelt olvasó terminálokról beszélünk. Az automatizálás együtt jár a teljes azonosítási idő csökkenésével. Képzeljünk el egy biometrián alapuló beléptető rendszert 500 jogosult felhasználóval. Reggel nyolc órakor, amikor mindenki egyszerre megérkezik, tegyük fel a munkahelyére, hatalmas káoszt, és az eszközök nem rendeltetésszerű használatát okozhatja a nagy értékű teljes azonosítási idő. Ügyelnünk kell arra a tényre, hogy az eszközök érzékenységének csökkentése, a gyorsabb áteresztést biztosíthatja ugyan, de a biztonságot csökkenti.

A biometrikus azonosítással szemben nyolc jellemzőt azonosítunk. Ez a nyolc jellemző a következő:

[901] Györgypál Csaba: Biometriai alapú azonosítás felhasználásának területei, jogi kérdései. Diplomamunka. Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar. Budapest, 2011. 9. o.
Kovács Tibor: Biometrikus azonosítás. Digitális jegyzet. Óbudai Egyetem, Budapest, 2010

- Általánosság, univerzalitás: az alkalmazni akaró társaság minden egyes tagja rendelkezik-e a mért jellemzővel.
- Egyediség: előfordul-e az az eset, hogy két vagy esetleg több személy pont ugyanazzal a jellemzővel rendelkezik.
- Maradandóság: az ember összes biometriai jellemzője közül változik-e az idő előre haladtával valamelyik.
- Megszerezhetőség: az egyes biometriai jellemzők mennyire másolhatók, eltulajdoníthatók.
- Teljesítmény: a jellemző azonosításánál mennyire járhatunk el pontosan, illetve gyorsan az adott módszer kapcsán.
- Elfogadottság: a társadalom részéről mennyire elfogadható ezen jellemzők felhasználása bizonyos esetekben.
- Megtéveszthetőség: mennyire megtéveszthető az a rendszer, aminél használnánk az adott jellemzőt.
- Mérhetőség: kapható-e a jellemzőkhöz olyan érzékelő vagy mérőeszköz, berendezés, amelynél használni tudom a jellemzőt.

4. Kockázatértékelés a biometrikus azonosító eszközök alkalmazása során

A fent említett mutatók alapján kiindulási pontot kapunk egy biometrikus azonosítást igénylő kivitelezés során, tehát hogy mit kell, és hova telepítenünk, hogy egy adott idő alatt a rendszert ért váratlan eseményekből keletkező kár várható értéke a lehető legkisebb legyen, a lehető legkisebb anyagi ráfordítással.

Természetesen az árak arányosan változnak a mutatók értékének változásával. Ha egy nagyobb biztonsági kockázatú folyamat zavartalan lefolyását kell biztosítanunk valamilyen biometrikus eszközzel, célszerű kockázatelemzést is készítenünk, hiszen ki kell választanunk azt az eszközt, ami a kockázatokat a lehető legnagyobb mértékben lecsökkentse költséghatékonyan.

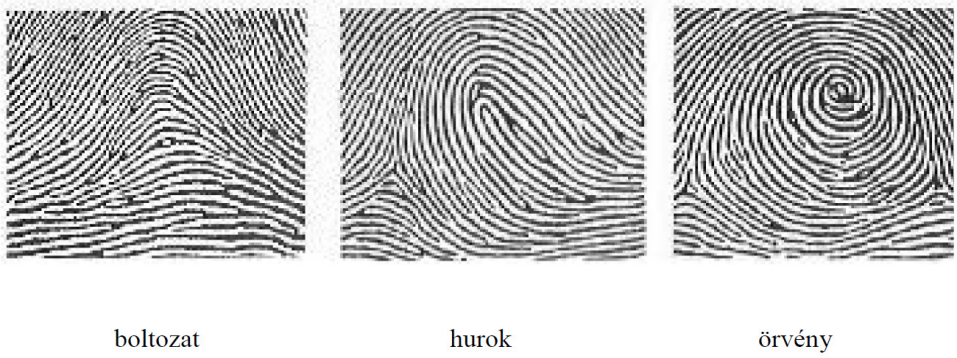
5. A gyakrabban használt azonosítási technológiák részletezése[902]

5.1. Ujjnyomat, tenyérnyomat azonosítás:

Néhol még a szakirodalomban is hibásan használják az ujjnyom, ujjnyomat, valamint az ujjlenyomat fogalmakat. Lényeges különbségek vannak ezen fogalmak között, mivel az azonosításhoz szükséges minta mindhárom esetben más és más. Az ujjnyom egy ember ujjának valamilyen felületen hagyott nyomata, ami általában hiányos, ezért azonosításra kevésbé alkalmas. Az ujjlenyomatot az ujjunk 360° körbeforgatásával készítünk, ezt általában a rendőrségi nyilvántartásokban használják. Az ujjnyomat, ami az

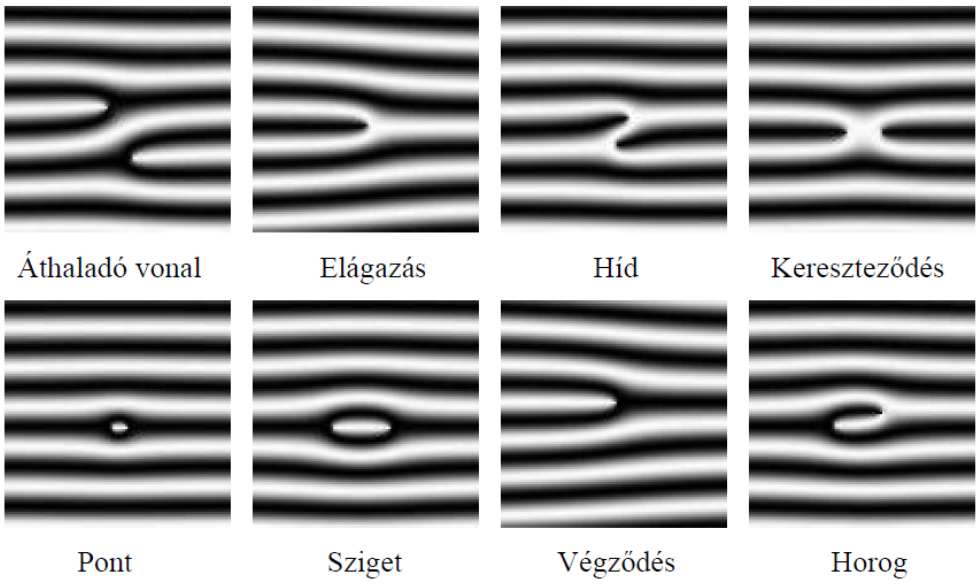
[902] A fejezethez kapcsolódó források:
Györgypál Csaba: Biometriai alapú azonosítás felhasználásának területei, jogi kérdései. Diplomamunka. Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar. Budapest, 2011. 9. o.
Kovács Tibor: Biometrikus azonosítás. Digitális jegyzet. Óbudai Egyetem. Budapest, 2010
Dőring András: Beléptető rendszerek. Digitális jegyzet. Óbudai Egyetem. Budapest, 2011
Bokor Attila: A biometrikus azonosítás jelene, múltja és jövője. Szakdolgozat. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar. Budapest, 2011. 15-38. o.
Kocsis Krisztián: Irodaház védelme biometrikus azonosítóval ellátott beléptető rendszerrel. Szakdolgozat. Budapesti Műszaki Főiskola Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar. Budapest, 2007. 42-46. o.

ujjbegy nyomata, a leginkább alkalmas a megfelelően részlet gazdag mintavételezésre. Az eljárás alapja a bőr maradandó gyűrődéseiből származó barázdák egyedi mintázata. Ezek a redők, az úgynevezett fodor szálak, különböző típusú nagyobb területű mintázatokat alkotnak egymással. Ilyen nagyobb egységek a boltozat, hurok, valamint az örvény mintázat.



5. ábra: Boltozat, hurok, és örvény mintázat

A fent említett nagyobb mintázatokon belül megkülönböztetünk kisebb, az adott ujjra jellemző, a fodor szálak végeiből, elágazásaiból, vagy összefutásaiból adódó jellegzetes pontokat. Ilyen jellegzetes pontok:



6. ábra: Fodorszálak alkotta alakzatok

Az egy ujjpercen fellelhető jellegzetes pontok száma meghaladhatja a százat is. A mintavétel történhet egyszerre az egész ujjról vagy vonalszkennerrel.

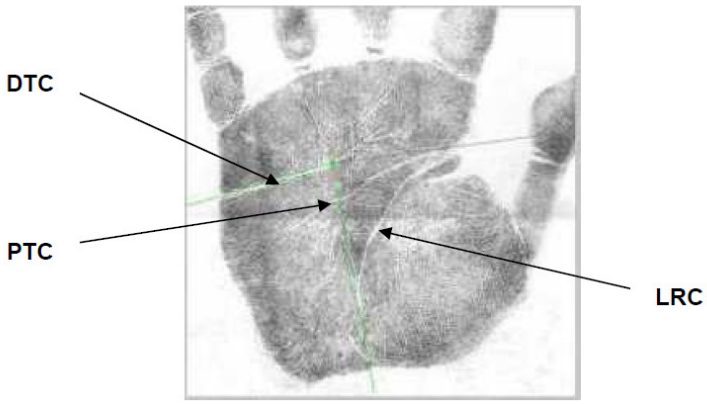
A kép rögzítési elvét tekintve az ujjnyomat azonosítók típusainak két fő csoportja van, az optikai, valamint a nem optikai elven működő azonosítók.

A nem optikai elven működő képrögzítés fajtái:

- Kapacitív elv – az ujj bőrfelületének kapacitása nem homogén. Ez az eltérő kapacitás mérhető. Kisméretű, olcsó, áramtakarékos, közepes minőségű eszköz.
- Rádiófrekvenciás elv – a szenzor rádiófrekvenciás jelet sugároz, amit az ujj visszasugároz. Nem csak az ujj felületéről készít képet, hanem a mélyebb rétegekről is, így sérült vagy szennyezett ujj esetén is sikeres lehet az azonosítás.
- Ultrahangos elv – a szenzor ultrahangot sugároz az ujjra és a visszaverődő hullámokból készíti a képet. Bőrfelszín alatti réteget szkenneli.
- Nyomásértékeléses elv – a szenzor egy piezo-elektromos nyomásérzékelő mátrix, ami értékeli az ujjfelület egyenetlenségeit.
- E- Mező szenzor – az ujj és a szenzor közötti elektromos mezőt hoz létre, ami felveszi az ujj mintázatát. Szennyezett ujj esetén is működik.
- Optikai elven működő képrögzítés fajtái:
- totálreflexiós – az ujj képe egy megvilágított prizma segítségével jut a képbontó eszközre. Jó a képminősége, de a szenzor mérete nagy.
- diffrakciós – hasonló a totálreflexióshoz, de prizma helyett Fresnel-lencsét használ, így jelentősen csökkenthető az eszköz mérete.
- közvetlen chip-szenzor – közvetlenül a szenzor felületére tesszük az ujjat, így jó minőségű, kisméretű eszköz készíthető.

A tenyérnyomat alapú azonosítási eljárás nagyon hasonló az ujjnyomat azonosításhoz. Az egész tenyér felületén megtalálhatóak az azonosítás alapjául szolgáló fodor szálak. A tenyér viszont tartalmaz olyan azonosításra alkalmas jellegzetességeket, mint a tenyéren keresztül futó ráncok, és az úgy nevezett fő vonalak. Egy emberi tenyér három fővonallal rendelkezik: szív vonal (Distal Transverse Crease – DTC), fejvonal (Proximal Transverse Crease – PTC) és az életvonal (Longitudinal Radial Crease – LRC).

További azonosításra alkalmas jellegzetesség a tenyér szövetmintázata, ami a tenyér egy kisebb részletén történik.



7. ábra: A tenyérnyomat és a tenyér fővonalai

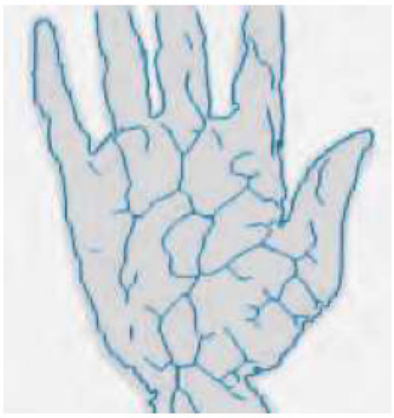
Az ujjnyomat és a tenyérnyomat azonosítás legfőbb előnyeként említhető hogy egyszerű használatú, valamint gyors. Hátrányként említhetjük, hogy az emberek bizonyos százalékának mintavételezésre alkalmatlan a bőr felülete, mivel munkakörükből adódóan olyan fizikai munkát végeznek, ami a bőr felületén maradandó sérüléseket hagynak, elkoptatva ezzel a fodor szálakat, így az azonosításhoz nincs megfelelő mennyiségű azonosítási pont.

5.2. Tenyérerezet azonosítás

A tenyér és ujj erezet azonosítás alapja a bőr alatt mélyen levő erezet kimutatása. A tenyeret a közeli infra (NIR) tartományú fénnyel kell megvilágítanunk. Ez a hullámhossz tartomány kb. 800-1000 nm között van, ami szemünkkel nem látható, mivel a látható elektromágneses sugárzás 350-750 nm tartományban van. A tenyérben lévő élő szövet kevésbé nyeli el, és másképpen veri vissza az infra sugárzást, mint az érhálózatban levő vér. A vér oxigén tartalma miatt jobban elnyeli az IR sugarakat, mint a környező szövet, így az erezetről megfelelő képalkotó eszközzel biometrikus azonosításra alkalmas képet kapunk.

Az erek metszéspontjainak egymáshoz viszonyított helyzetét, távolságát, az erek vastagságát, ami lényegében az azonosítás során kerül vissza olvasásra, egy algoritmus adathalmazként kinyeri a képből, és ezt tárolja a szoftver. A tenyér infra képe nem kerül letárolásra, aminek célja a kisebb méretű adat tárolás.

8. ábra: Az érhálózat képe



9. ábra: Az algoritmus által generált egyszerűsített kép

A tenyérerezet azonosítás legfőbb előnye az ujjnyomat, és tenyérnyomat azonosítással szemben, hogy az azonosításhoz szükséges jellegzetességek a külső hatásoktól védve vannak, hiszen az érhálózat mélyen a szövetek alatt van, így kevésbé sérülékenyebb, mint ujjpercünk fodor szálai.

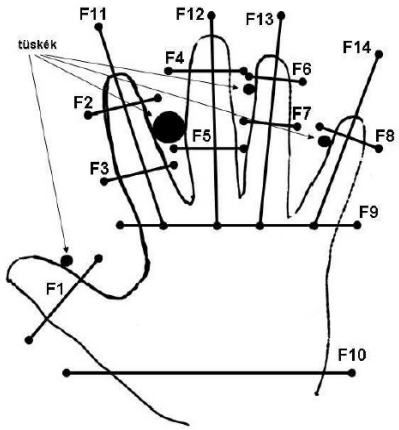
5.3. Kézgeometria azonosítás

A kézfej számítható, valamint mérhető geometriai tulajdonságai ugyancsak azonosításra alkalmasak.

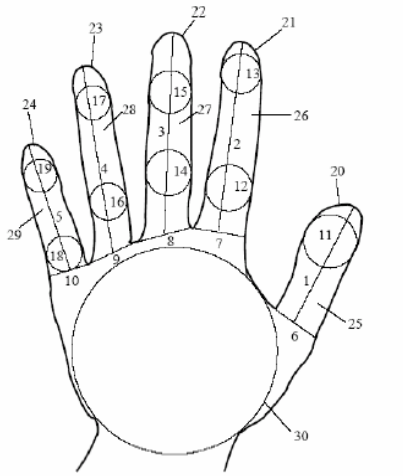
A mintavételezés, és az azonosítás során az ujjak hosszúsága, szélessége, a kézfej szélessége, valamint a tenyér és az ujjak méretarányai kerülnek mérésre, rögzítésre egy képalkotó eszköz segítségével.

Kétféle azonosító berendezést különböztetünk meg, a pozícionáló tüskés, valamint a pozícionáló tüske nélküli eszközöket. A pozícionáló tüske feladata a kéz megfelelő pozícionálása, tehát hogy a kézfej lehetőleg a regisztrálási elhelyezkedési állapothoz legyen hasonló a további mintavételezések során is. A pozícionáló tüskés azonosító eljárás során a rendelkezésre álló mintán összesen 14 tengely mentén mérik a kéz méreteit, az ujjak vastagságát ujjanként két tengelyen, kivéve a hüvelykujj és a kisujj vastagságát, mivel itt elegendő egy tengely felvétele a méréshez.

A pozícionáló tüske nélküli eszközök jóval több, mint egy 30 sajátossági értéket vesznek fel, az ujjak hosszát, az ujjak szélességét az ujjak tövénél, az ujjakba beírt körök sugarát, az ujjak kerületét, területét, valamint a tenyérbe írható kör sugarát.



10. ábra Mért paraméterek pozícionáló tüske esetén



11. ábra Mért paraméterek pozícionáló tüske nélkül

A kézgeometria azonosítás előnye hogy egyszerű, könnyen használható és nem érzékeny a kéz szennyeződéseire. Hátrány viszont hogy a kéz sérülései, deformálódása esetén az azonosítás sikertelen

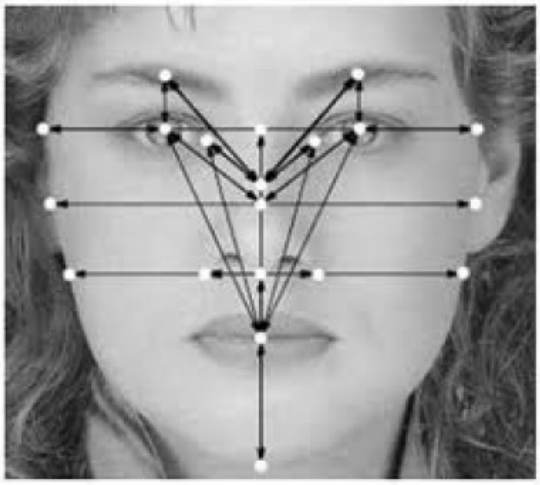
5.4. Arc alapú azonosítás

Az arc alapú azonosításnak két módszere van, a minta alapú, valamint a geometriai. A minta alapú azonosítás során egy már korábban letárolt mintával hasonlítják össze az arc globális tulajdonságait. Az összehasonlítás az arc részleteinek (szem, ajkak, orr) korrelációjával történik

A geometriai elvű arc azonosítás során az arc körvonalainak és különböző részleteinek egymáshoz viszonyított helyzetét méri és hasonlítja össze az adatbázisban tárolt adatokkal. Az azonosítás során mért paraméterek a következőek:

- a jobb és a bal szem két szélső pontja,

- a jobb és a bal orrcimpa két szélső pontja,
- a száj középpontja (stabilabb, mint a két szélső pont),
- az áll jobb és bal pozíciójának vízszintes pozíciója,
- az áll közepének függőleges pozíciója,
- a jobb (bal) szemöldök függőleges pozíciója,
- a jobb (bal) fülcimpa vízszintes pozíciója.



12. ábra Az arcfelismerő által mért paraméterek

Ha nem egy, hanem több képalkotó eszközt tartalmaz az azonosító, nem csak 2D, hanem 3D képet is képesek vagyunk készíteni, ami lehetővé teszi az eszköz magasabb szintű biztonsági feladatok ellátására való alkalmazását.

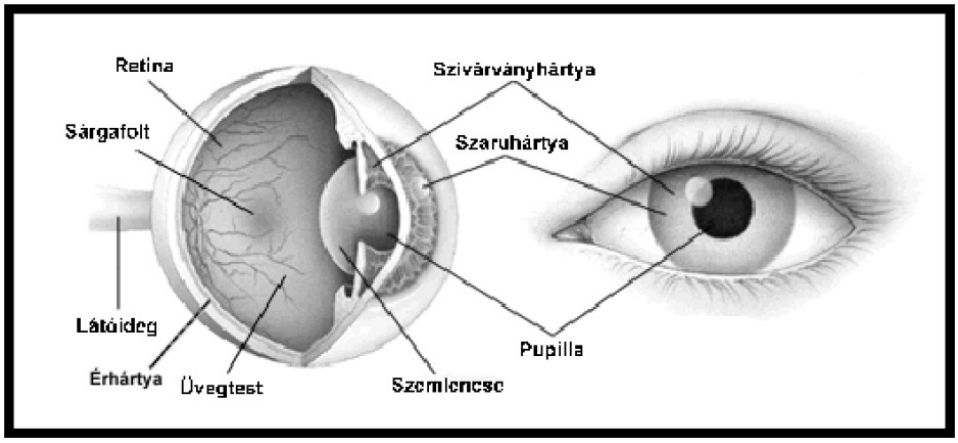
Az arcfelismerésben jelenleg nem igazán elterjedt eljárás az arc thermogramjával történő azonosítás. A thermogram az érhálózat egyedisége miatt ugyancsak alkalmas az azonosításra. Ez a szükséges képrögzítő eszköz, a hőkamera költségei miatt azonban nem terjedt el napjainkban. A digitalizált felvételen a mintát azonosító algoritmus ellenőrzi a relatív hőmérséklet különbségeket. Problémát jelent a korrelációban a háttér hősugárzásának kizárása. Előnye viszont hogy teljes sötétségben is alkalmazható, nincs szükség éjjellátó, infra képrögzítő eszközre.

5.5. Szem

A szem felépítése, mint ahogy a látás folyamata, nagyon összetett. Az alábbi főbb részekre oszthatjuk:

- szaruhártya – védi a szemet és megtöri a fényt,
- szivárványhártya (írisz) – a szembe jutó fény mennyiségét szabályozza,
- pupilla – szivárványhártyán lévő rés, ahol a fény be tud jutni,
- szemlencse – megtöri a fényt és a retinára irányítja,
- üvegtest – kitölti a szemgolyót,
- retina (ideghártya) – fényérzékelő sejtekkel borított hártya,

- sárgafolt – a retina egy kis területe, ami az éleslátásért felel,
- érhártya – sűrű érhálózattal ellátott hártya, ami az idegsejteket látja el,
- látóideg – ez gyűjti össze és vezeti el a fényérzékelő sejtektől a jeleket.



13. ábra: A szem felépítése

A szem mint testrész kétféle biometriai azonosítási lehetőséget biztosít, az írisz és retinaazonosítást.

Íriszazonosítás

Az írisz, más néven a szem szivárványhártyájának sajátosságai alapján történő biometrikus azonosítási eljárás az egyik legjobb gyakorlati jellemzőkkel bír. Annak az esélye, hogy két írisz megegyezzen 10^{70} nagyságrendű, míg a föld népessége csupán 10^{10} nagyságrendű. További előnyei hogy 400 azonosítási jellemző vizsgálatára képes (napjainkban hozzávetőleg csak 260-at használnak), valamint az élőminta vizsgálata könnyen megvalósítható a pupilla reflexek figyelésével. Az eljárás a szivárványhártya rajzolatának infravörös fénnyel történő elemzésén alapul. Az első azonosítási paraméter a trabekuláris hálózat, amelynek az írisz sugaras mintázatát adja. Az embrionális fejlődés nyolcadik hónapjában alakul ki, és az emberi élet során csak nagyon nagy fizikális behatás során változik, mivel betegségek során nem változik. Jellegzetességi pontok közé tartozik a körök, az árkok, és a korona rajzolata.

Infravörös letapogatás során a szivárványhártya láthatatlan erezetéről készül közeli kép, amelyet a részletgazdagság érdekében korrelálni kell a szempillák, és a szemhéjak zavaró hatásai miatt, mivel ezek takarhatják a kör alakot. A korreláció után már elkészíthető a fókuszált kép, amely tartalmazza az azonosításhoz szükséges egyedi paramétereket.

Az írisz azonosítás folyamata három fő lépésből áll:

- a video képkészítésből,
- a konvertálásból,
- és az azonosításból

A video képkészítés során rögzítésre kerülnek a szemhéj és a pupilla határvonalai, a pupilla tágulási mértéke és bemélyedései. A visszaverődő fény, és képen levő szempillák korrelációja után a képet dőlésszöghöz igazítja az algoritmus.

A felvett paramétereket 256 byte méretű kóddá, az ellenőrzés adatait ugyancsak 25a byte-os kóddá konvertálja az eszköz. Az azonosítás során az aktuális mintát összehasonlítja az adatbázisban levő mintákkal.

Retinaazonosítás

Az eljárás a fent említett tenyérerezet azonosítás elvéhez nagyban hasonlít. Alacsony intenzitású infravörös fénnyel világítják meg a szemfenéken található érhálózatot, a retinát. Az erekben levő vér az oxigéntartalmuktól függően jobban elnyelik a az infravörös fényt, mint a környező szövet. A mintázatot formázó fényt ezután visszatükrözik egy CCD szenzorra, ami a képrögzítést végzi.

Az írisz a retinaazonosítással szemben több szempontból is előnyt élvez. A retina változhat cukorbetegség, drogok, vagy nagyobb mennyiségű alkohol fogyasztása esetén, ami az azonosítás folyamán személyiségi jogi kérdéseket is felvet.

6. Összegzés

Cikkünkben definiáltuk a biztonságtudomány, a biometria, biometrikus azonosítás fogalmakat, valamint kitértünk az eszközökkel szemben támasztott követelményekre, és bemutattuk a szakmai gyakorlatban leginkább használt azonosítási eljárásokat.

Bár a biometrikus azonosítás mára már többet jelent a laikusok számára is, mint a science fiction filmekben látható eszközöket, azonban még közel sem elégíti ki a teljes felhasználási kört. Jövőbeni kilátások között lehet akár egy a bankkártyás fizetési rendszert ellátó biometrikus azonosítási folyamat, ez azonban további jogi kérdéseket is felvet. Az eljárásoktól függően, a kényelemhez és a megfelelő biztonsági szinthez mérten az élet minden területén alkalmazható a biometrikus azonosítás. Azt viszont a felhasználónak kell eldöntenie, hogy megbízik-e ezekben az eszközökben, és hajlandó-e a „jól bevált” kulcsait, kártyáit, igazolványait helyettesíteni valamilyen biometriai jellemzőjével.

A biztonságtudomány célkitűzésének lehet kijelölni a biometria előnyeinek köztudatba való integrálását, ezáltal megteremtve azt a fogyasztói kört, amely hajlandó olyan megtérülő biztonságtechnikai beruházást tenni, amely növeli biztonságát, csökkenti az adott folyamat során felmerülő kockázatokat.