

Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Gépszerkezettani és Biztonságtechnikai Intézet



TUDOMÁNYOS DIÁKKÖRI DOLGOZAT

Ellenszenv a biometriával szemben

Szerző: Bartus Attila

had-és biztonságtechnikai mérnök szak,
BSc szak, III. évf.

Konzulens: Őszi Arnold

PhD aspiráns, Alkalmazott Biometria Intézet

Lezárás dátuma: 2014. Április. 13.

Tartalomjegyzék

Tartalomjegyzék	1
1 Hipotézis.....	3
2 Biometrikus azonosításról.....	3
2.1 Biometrikus azonosítási formák.....	5
2.1.1 Ujjnyomat.....	5
2.1.2 Arcdetektálás.....	6
2.1.3 Tenyérerezet.....	7
2.1.4 Kézgeometria.....	8
2.1.5 Írisz	8
2.1.6 Retina	9
2.2 Tévhitek a biometriával szemben.....	10
2.3 Félelmek a biometriával szemben	10
3 Eredmények.....	14
3.1 Kontaktusosság értelmezése.....	14
3.2 Vizsgált eszközök	15
3.2.1 Suprema BioEntry Plus	15
3.2.2 FingerKey DX-2000.....	16
3.2.3 iLock Iris Access 2020	17
3.2.4 HandKey II	17
3.2.5 Retina azonosítók	18
3.2.6 L-1 Identity Solutions.....	19
3.2.7 Face ID F810	19
3.3 Vizsgált szempontok.....	20
4 Összefoglalás.....	23
5 Irodalomjegyzék.....	25
6 Ábrajegyzék.....	26

1 Hipotézis

Napjainkban egyre szélesebb körben használjuk a biometriát. Ahogy az emberek kezdik megismerni ezeket a technológiákat, kialakul bennük egy érzés, miszerint nem szívesen használják. Számos esetben találkoztunk már az úgynevezett “kontaktusosság” problémájával, ami a felhasználó és az eszköz között létrejött kapcsolatot jelenti. Ezeknek az eszközöknek az elhelyezése előtt nem csak a technikai szempontokat kell figyelembe venni, hanem az ezeket használók belevetett bizalmiszintjét is. Értem ez alatt, hogy a felhasználó aki egy kéz-geometria azonosítóval lép be a munkahelyére, elhiszi-e, hogy az csak őt fogja beengedni a saját biometrikus adataival. A másik tényező a technológia kényelmi szintje. Dolgozatomban azt vizsgálom, hogy a ma használt biometrikus megoldásokat hogyan kell használniuk az embereknek, ami kiválthatja az ellenszenvet. Bemutatom, hogy mik azok a fő szempontok amik zavaró tényezők a használat során és ezek segítségével sorrendet állítok fel a biometrikus technológiák között. A biometrikus eszközök fő problémája, hogy kellemetlenséget okoznak. Ujjunkat a szenzorra kell helyezni, más formáknál fejünket fixen kell tartani vagy éppen olyan felületekre kell tenni kezünket, amikhez többen hozzáérnek nap mint nap. Ezek nem jelentenek gondot az olyan helyeken ahol kiemelt biztonságra van szükség, mint például a bankokban, de a magánszférában való elterjedését ez nagyban gátolja.

2 Biometrikus azonosításról

A biometrikus azonosítások az ember szervezetének vagy más, viselkedési tulajdonságainak, egyedi jellemzőinek felismerésén alapulnak. Jelenleg az ujjnyomat a legelterjedtebb, de egyre inkább kezdenek teret nyerni az arc-, hang-, írisz- retina-, kéz- és DNS azonosítási formák is.

A biometrikus azonosítási módszerek mind egy úgynevezett mintaillesztő algoritmuson alapulnak. Az azonosítási eljárás két fő részből áll. Az első, amikor regisztráljuk az egyén valamely biometriai jellemzőjét, majd eltároljuk azt. Ezt nevezzük mintavételezés folyamatának. A másik, amikor a mintavételezéssel kezdve, a digitalizálás után az eszköz megkeresi és összehasonlítja az adatbázisban tárolt mintákkal, majd

jogosult vagy jogosulatlanként kezeli a felhasználót. Az adatbázisban eltárolt adatok adatvédelem alatt állnak.

Az azonosítási sebesség az eszközök fejlődésével folyamatosan csökkent. A ma használt eszközök már képesek elvégezni az egész azonosítási folyamatot akár egy másodperc alatt. Azonban a valóságban a beléptetés nem csak az azonosítás folyamatáról szól, hanem a teljes áthaladásról az adott ellenőrző ponton.

Gyakorlati szempontból vizsgálva a biometrikus eszközöket nyolc szempontnak kell megfelelnie:

- gyorsaság,
- együtt kell működnie a biztonsági rendszerrel,
- robusztus kivitel,
- sok személyt kell kezelnie,
- pontosság,
- biztonsági szintje megfelelő legyen,
- gazdaságosság,
- megbízhatóság.

Ezeket a jellemzőket jelenleg egyik ma használatos eszköz sem elégíti ki. Erre a problémára a megoldás a több azonosító fajta egyidejű használata jelenti. Ezek ötvözése akár 100% közeli biztonságot is nyújthat.

A biometriában használt két legfontosabb mutató a téves elfogadási arány (False Acceptance Rate, a továbbiakban: FAR) és a téves elutasítási arány (False Rejection Rate, a továbbiakban: FRR). Amennyiben a felhasználó jogosulatlanul próbál belépni, de az eszköz mégis jogosultként kezeli FAR téves elfogadási arányról beszélünk, ha pedig a jogosult alanyt jogosulatlannak nyilvánítja, abban az esetben FRR téves elutasítási arányt kapunk.

A biometrikus azonosítás során nyolc jellemzőt vizsgálhatunk. Általánosság univerzitás, egyediség, maradandóság, megtéveszthetőség, teljesítmény, megszerezhetőség, mérhetőség és elfogadottság. Dolgozatom témája az elfogadottság

méréséről szól. Jelentése, hogy “a társadalom részéről mennyire elfogadható ezen jellemzők felhasználása bizonyos esetekben”

Jelen dolgozatomban csak azokkal az azonosítási technológiákkal foglalkozom, amelyeknél kontaktusosság alakul ki a felhasználó és a készülékek között. [1] [2] [3] [4]

2.1 Biometrikus azonosítási formák

2.1.1 Ujjnyomat

Az ujjnyomat azonosítás során a ujjunkon lévő barázdák egyediségét elemzi a készülék. Ez a mintázat 18 hetes korunkban alakul ki, ezt követően már nem fog megváltozni, ráadásul ha sérülés éri ujjunkat csak idő kérdése és regenerálódni fog. Ezt használják ki a leolvasó berendezések. Az ujjnyomatok olvasására többféle technikai megoldás létezik. Elsőként a daktiloszkópiai értelmezését ismertetném az ujjról származó mintáknak.

Ujjnyom: amikor megérintünk egy bögrét, akkor az ujjnyomunkat hagyjuk rajta. Jellemzően rossz minőségű és azonosításra nem alkalmas.

Ujjlenyomat: Az ujjról készült teljes kép, ami az ujjvégi ujjperc, körömtől-körömig tartó lenyomatát jelenti. A rendőrségi nyilvántartásba vételkor ezt a módszert alkalmazzák.

Ujjnyomat: Egy sík felületen hagyott kétdimenziós lenyomata az ujjunknak. A legtöbb azonosító eszköz ezt használja.

A fejlettebb ujjnyomat azonosítók képesek megvizsgálni, hogy az ujj élő-e, amit a hőmérsékletének és/vagy nedvességtartalmának elemzésével állapít meg. Elmondható, hogy az összes ilyen eszköz az ujjunkon található fodorszálok egyediségét elemzi és tárolja el. Ezeket a mintákat később az azonosítás során összehasonlítja a letárolt összes mintával, ami időbe telik. Az azonosítás szempontjából a pontoság a legfontosabb szempont, ezt az érzékelők fejlesztésével tudják elérni. Ezek a képfelvételi elv szerint

optikai, kapacitív, rádiófrekvenciás, ultrahangos és nyomásérzékelés elvén alapulóak lehetnek. A gyakorlatban jellemzően két féle érzékelő típust használnak:

Kapacitív érzékelők: a szenzoron elhelyezett ujj felületén lévő völgyek és fodorszálok miatt eltérő kapacitást mutat, ami elektromos jelként jelenik meg.

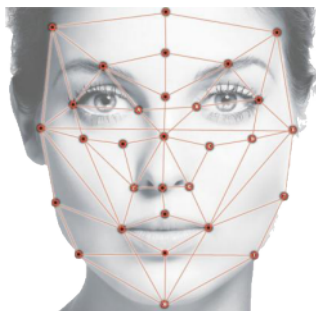
Optikai érzékelők: ez a legelterjedtebb. Az olvasó egy CCD scanner, amely az üveglapra helyezett ujjról készít egy képet és azt digitalizálja. LED diódákat használnak barázdák megvilágítására. [3] [5]



1.ábra: Ujjnyomat

2.1.2 Arcdetektálás

Az arcfelismerő az azonosítandó személy arcvonásait vizsgálja, ezt hasonlítja az előzőleg letárolt, időnként karbantartott mintával. Annak érdekében, hogy a haj és a háttér változásait kiküszöböljék, csak az arc középső részét szokták használni a felismeréshez. Amennyiben van szerencsénk egy felismerő szoftvert megfigyelni működés közben, láthatjuk, hogy az algoritmus először megkeresi az arcunk körvonalát, ezt egy négyzetbe helyezi. Ezt követően a négyzeten belül vizsgálja, a felismeréshez szükséges pontok elhelyezkedését. Általában az arcfelismerő programok egyszínű, nem változatos háttér előtt működnek. A gyártók más és más algoritmusokat használnak. Ettől függ az eszközök megbízhatósága. [1] [10]



2.ábra: Arcazonosítás

2.1.3 Tenyérerezet

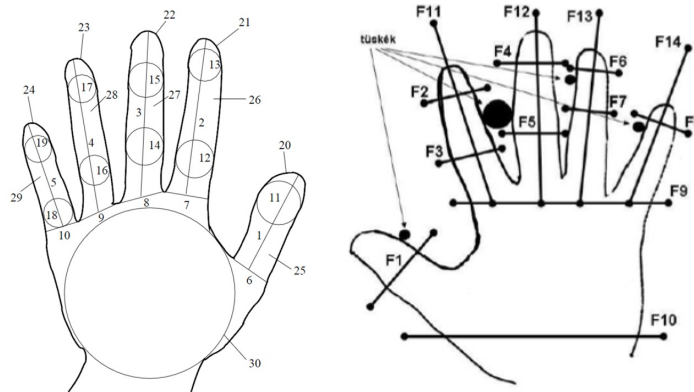
A mintát, amely jelen esetben a tenyerünk, infravörös (NIR) fénnel világítják meg. Ez a tartomány a 800-1000 nm között helyezkedik el, amit szemünkkel már nem láthatunk. A különböző szövetek miatt más az elnyelődés és a visszaverődő fény intenzitása. Az ereinkben folyó vér sokkal jobban elnyeli a fényt, mint a körülötte lévő szövet. Az így készített kép alapján egy érhálózati térképet készíthetünk, ami egyedi és állandó. Az érhálózat jellegzetességei az elágazások szögei, vastagságuk és az erek elágazásai. Két nagy előnye, hogy nem befolyásolja a szennyeződés és szinte lehetetlen hamisítani, mert csak élő szervezet képes a vér áramoltatására. Ugyan ezt az elvet használják az ujj erezet azonosítók is. [4]



3.ábra: Tenyérerezet

2.1.4 Kézgeometria

A kézfej mérhető geometriai tulajdonságait vizsgálja. A mintavételezés során egy képalkotó eszköz az ujjak hosszúsága, szélessége, a kézfej szélessége valamint a tenyér szélessége és az ujjak méretarányait elemzi. Két fajta berendezést különböztethetünk meg, a pozícionáló tűskés és a tűske nélküli azonosítókat. A tűskék feladata, hogy a regisztrálás után az azonosítás folyamán is ugyan úgy helyezhessük el kézfejünket a sikeres olvasás érdekében. A pozícionáló tűskés változatnál a kézfejet 14 tengely mentén mérik. A tűske nélküli eszközök az ujjak hosszát, szélességét a tövüknél, az ujjakba beírt körök sugarát, kerületét, területét, valamint a tenyérbe írható kör sugarát elemzi. [8]



4.ábra: tűske nélküli kézgeometria azonosító

5.ábra: tűskés kézgeometria azonosító

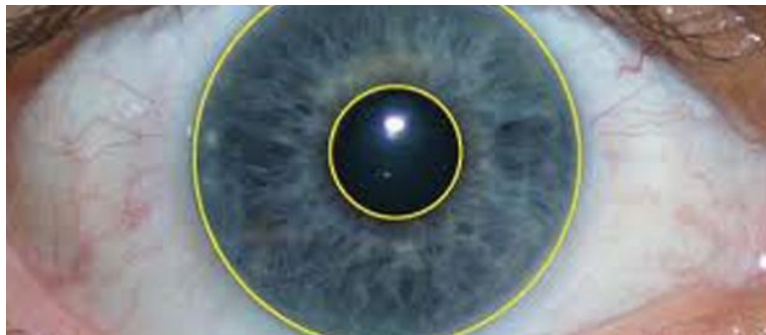
2.1.5 Írisz

Infravörös megvilágítás mellett készíti el a szivárványhártya részletes képét egy hétköznapi mondható CCD kamerával. Matematikai mintafelismerési technikával dolgozik ami a képet feldolgozva az egyedi jellemzők alapján állítja össze az azonosításra szolgáló adatsort. Ezt követően összeveti az adatbázisban tárolt adatokkal. Legnagyobb előnyei a gyorsaság és pontosság. Az írisz egy belső látható szerv és emiatt ez a legkevésbé sérülékeny. Több ország alkalmazza útleveleikben azonosításra kényelmi okokból. Az infravörös fény több szempontból is fontos a használat során. Az emberek

többségének sötét barna a szeme és csak ebben a tartományban (750-1050nm) mutatja meg a szerkezetét. Fontos szempont az is, hogy mivel az emberi szem által láthatatlan fényről beszélünk, ezért ez kevésbé tolaakodó, valamint a visszaverődő fény nem befolyásolja a szivárványhártya mintáját. Jellegzetességei: gödröcskék, körök, árkok, korona, szövetszálak. [6] Működése során az azonosító először megkeresi az írisz határait, majd a fókuszálás után elkészíti a képet. Két féle módon teheti ezt meg:

Aktív mód: a felhasználó az azonosításhoz a készülékhez 15-30 cm közelségbe hajol amíg az vissza nem jelez.

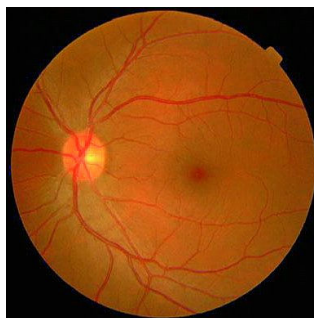
Passzív mód: 30-100 cm távolságban magától megkeresi az íriszt és automatikusan ráfókuszál.



6.ábra: írisz minta

2.1.6 Retina

Az ujj és tenyérerezet olvasókhoz hasonlóan itt is a megvilágított érhálózat eltérő infra fény elnyelődését használják ki. A szem hátsó falán lévő erek mintázatát térképezi fel. A mintavételezési eljáráshoz pár centiméter közelségbe kell hajolni, közben egy alacsony intenzitású infravörös sugárral átvilágítva szemünket megállapítja a szemfenék érhálózatát. Hátránya, hogy túlságosan közel kell hozzá hajolni és emiatt fertőzésveszély is kialakulhat. Ezeket a technológiákat csak kiemelt biztonságot igénylő helyeken használják. [2] [7]



7.ábra: retina minta

2.2 Tévhitek a biometriával szemben

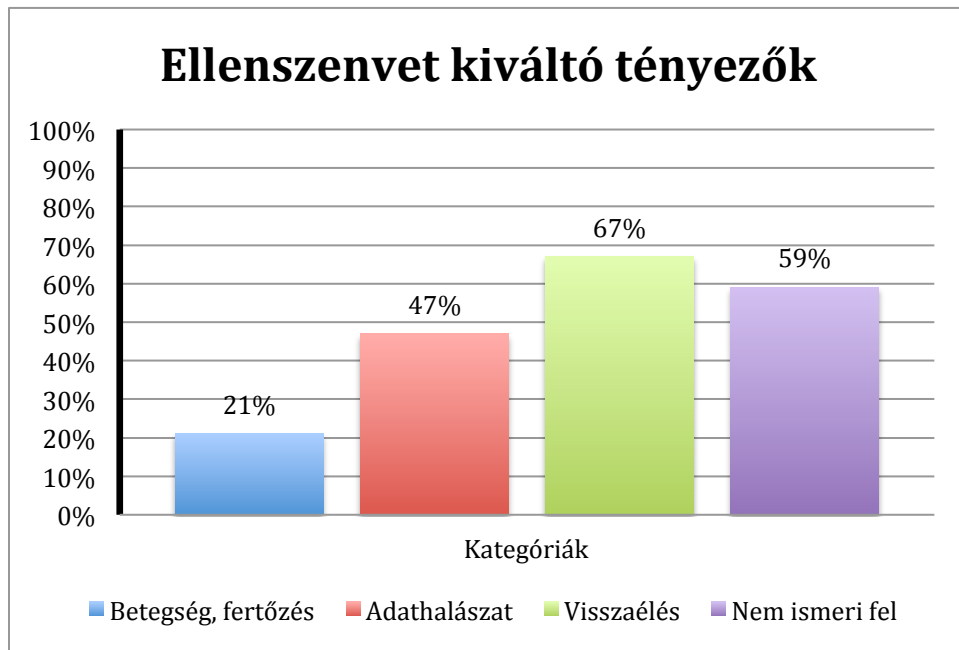
A félretájékozottság valószínűleg a filmek félrevezető, olykor fantasztikus jeleneteinek köszönhetőek. Bár komoly tudás és technikai háttér áll a fejlesztések mögött, a biometrikus azonosítás egyáltalán nem megfizethetetlen a közhiedelemmel ellentétben. Egy általam végzett felmérésen kiderült, hogy a legismertebb azonosítási forma az ujjnyomat. Az ujjnyomat azonosítás nem nyújt 100% biztonságot, mert hamis mintákkal is elérhető a sikeres azonosítás. A leolvasása nem minden egyes embernél működőképes egy adott időpillanatban. Bizonyos embereknél genetikai okokból használhatatlan az azonosításhoz. Egyes anyagok és tevékenységek használhatatlanná teszik az ujjnyomatát. Ilyen lehet például a téglák pakolása, kézkrém használata és ha megvágjuk az ujjunkat. Egy másik szembetűnő és sokat hallott félelem, hogy a retina és írisz azonosító készülékek lézert használnak és ez árt a szemnek. Természetesen szó sincs arról, hogy károsítaná a szemünket. Valójában az az infra fény nem a látható tartományban van. Egyik eszköz sem használ lézer fényt!

2.3 Félelmek a biometriával szemben

Kutatásom során találtam egy 2006-ban készült felmérést a biometrikus eszközök ismertségéről. Ezt alapul véve készítettem egy ehhez hasonlót, melyben képet kaptam a 2014-es helyzetről. Ezt kizárólag tájékoztató jelleggel kívánom bemutatni ugyanis az online kérdőív nem szolgálhat tudományos kutatás alapjául. Arra voltam kíváncsi, hogy napjainkban milyen véleménnyel vannak az emberek ezekről a technológiákról és

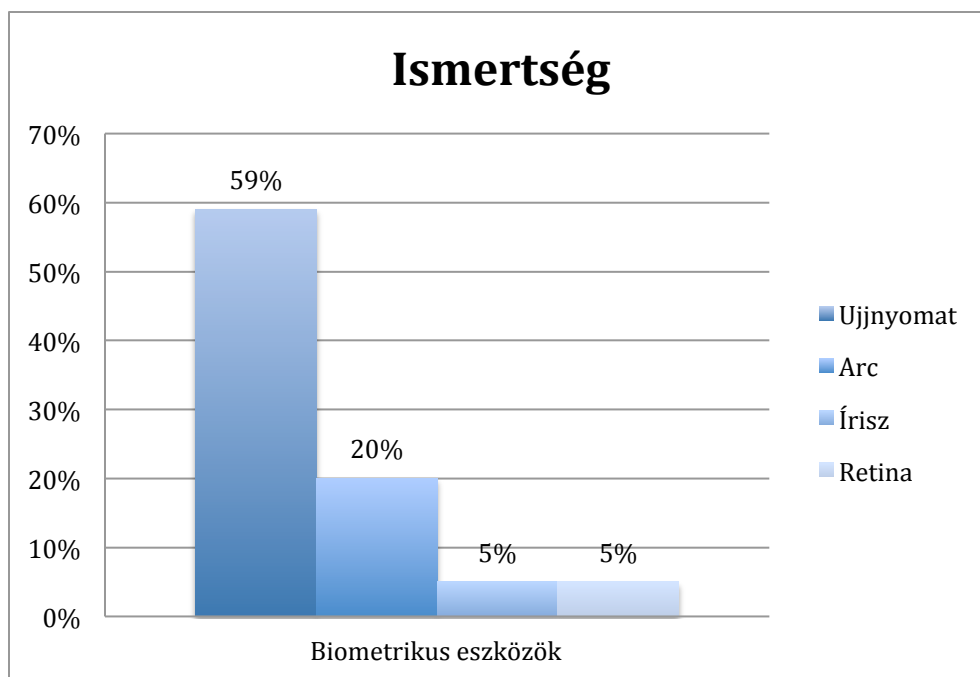
szerintük ezek mekkora biztonságot nyújtanak. A kérdések között szerepeltek az ellenszenvet kiváltó főbb tényezők, melyeket saját tapasztalataim alapján állította össze.

A kérdőívet háromszáztíz alany töltötte ki.



8.ábra: Ellenszenvet kiváltó tényezők

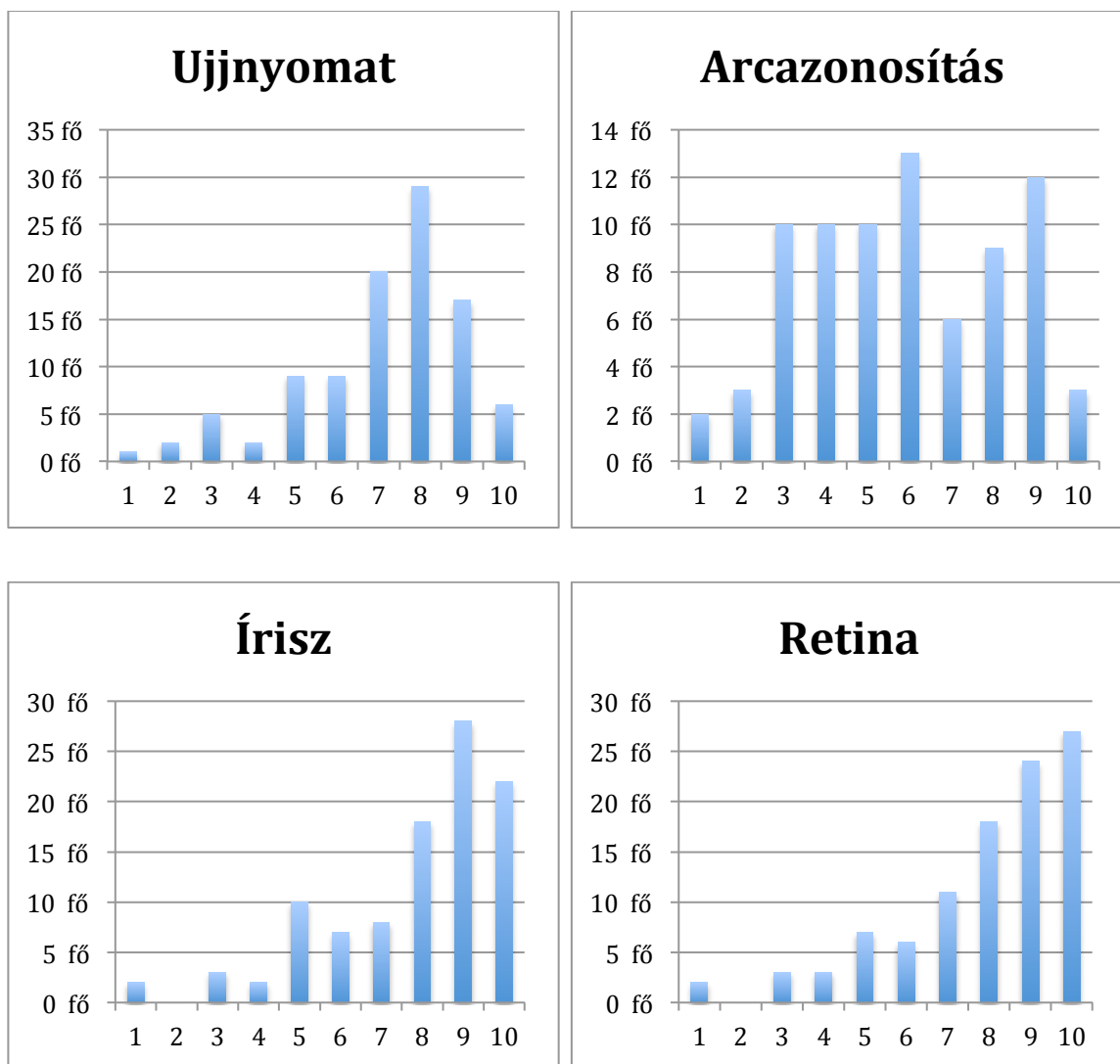
A grafikonon jól látható, hogy a visszaélés az, amitől a legtöbb félnek. Ez a válaszolók 67%-át jelenti. A második legtöbbet elért szavazatot a „biometrikus eszköz nem ismeri fel” kapta. Mivel a kérdőívet az Óbudai Egyetem hallgatói töltötték a legnagyobb számban ezért ez az ott is ismert problémák miatt várható eredmény volt. Az érdekesség, hogy a betegségtől félnek a legkevesebben. Irodalomkutatásom során kijelenthetem, hogy a legtöbb esetben ezzel a tényezővel találkoztam, amire azt hittem, hogy toronymagasan a legnagyobb félelmet kiváltó ok lesz. Saját meglátásom szerint ez az itthoni tájékozatlanságnak köszönhető. Az összes irodalom amiben találkoztam ezekkel a problémákkal külföldi, általában az Egyesült Államokból származtak. A következő grafikon a biometrikus azonosító technológiák ismertségét mutatja be.



9.ábra: Ismertség

A meglévő adatok alapján jól látható, hogy a legismertebb az ujjnyomat volt. Ez a legrégebbi módszer a felsoroltak közül. Sokat fejlődhetett az évek során és ennek köszönhetően jobban elterjedt.

A biztonságra vonatkozó kérdésekre, hogy melyik technológiát gondolják a legmegbízhatóbban a következő lett az eredmény:



10.ábra: biometria biiztonság

A 10. ábrán látható, hogy a pontozás alapján a retina és az írisz kapták a legtöbb adható azaz „10” pontot. Érdekesség továbbá, hogy a válaszolók nagy része saját bevallása szerint még nem használta ezeket, mégis ezt tartották a legmegbízhatóbbnak.

3 Eredmények

3.1 Kontaktusosság értelmezése

Az eszközhöz többször is fizikailag hozzá kell érni, amikor rendeltetésszerűen használják. Ez a minta, a szenzor és a nyomógombok kapcsolatát jelenti. A kontaktus kialakulása miatt a minta szennyezi az eszközt és ez fordítva is igaz. A megközelítés és kapcsolatfelvétel szerint négy állapotot figyelhetünk meg:

1. állapot: Nincs kontaktus az azonosítandó minta és az eszköz között illetve nincs megközelítési kényszer (arcfelismerés alapján történő azonosítás ideális esetben az átlépni kívánt beléptető pont felé való közeledési hajlandóságot használja ki).
2. állapot: Továbbra sincs kontaktus az azonosítandó minta és az eszköz között, de megközelítési kényszer van esetlegesen apróbb pozicionálási szabályok (íriszazonosító).
3. állapot: Kontaktus áll fenn az azonosítandó minta és az eszköz között. (Általánosságban amúgy is használt biometrikus jellemző alapján történő azonosítás, nem áll fenn a eszköz az idegenkedés az eszköz felé mivel az azonosítandó terület sérülésérzékenysége nem magas (ujjnyomat azonosítás, tenyérgeometria vagy érhálózat alapú azonosítás).
4. állapot: Kontaktus továbbra is fenn áll az azonosítandó minta és az eszköz között továbbá olyan biometrikus jellemző alapján történő azonosítást végzünk ami kiválthat idegenkedést a felhasználó irányában ennek következtében valószínűsíthető az óvatosabb megközelítés ez szintén lassabb áteresztőképességhez vezet (Retina azonosítás = sérülékeny terület a szem kontaktus az eszközzel esetleges fertőzés veszéllyel is kell kalkulálni ez az egyik fő kiváltója a felhasználói idegenkedésnek).

3.2 Vizsgált eszközök

Az Óbudai Egyetem, Alkalmazott Biometria Intézetében (ABI) szakmai gyakorlat során volt lehetőségem tesztelni az 11. ábrán található azonosító eszközöket.

Ujjnyomat azonosító	BioEntry Plus, FingerKey DX-2000
Arcazonosító	Face ID F810
Írisz azonosító	iLock Iris Access 2020
Retina azonosító	Nem volt
Ujj erezet azonosító	L-1 Identity Solutions
Kéz geometria azonosító	HandKey II

11.ábra: Biometrikus azonosító eszközök

3.2.1 Suprema BioEntry Plus

A Suprema számos olyan készüléket gyártott már amit manapság is előszeretettel használnak a gyakorlatban. Többek között az Óbudai Egyetemen Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán is egy ilyen eszköz van felszerelve. Pontosabban egy Suprema BioEntry Plus. Témám választása főként ennek köszönhető, ugyanis a problémákat először ezen az eszközön tapasztaltam. Több karnak a hallgatója használja nap mint nap és egy jó alapnak tartom a bemutatás elkezdéséhez.

A BioEntry Plus egy IP alapú ujjnyomat beléptető berendezés mely optikai szenzorral van felszerelve és RF kártya olvasására is alkalmas. Használata során meg kell érintenünk a szenzort, majd amíg vissza nem jelez a LED ott kell tartanunk rajta ujjunkat. Számos esetben elutasítja a felhasználókat, tehát az FRR érték sokkal magasabb a gyártó által megadott technikai adatoknál. A legnagyobb ellenszenvet kiváltó tényezők a túlzottan sok téves elutasítás és a kontaktus „érintés” a szenzorral.



12.ábra: Suprema BioEntry Plus

3.2.2 FingerKey DX-2000

Ez egy elavultnak mondható készülék, de számomra azért fontos, mert használatához nem elég az ujjunk szenzorra való helyezése, hanem egy a felhasználót azonosító kódot is be kell ütnünk a sikeres azonosításhoz. Ugyan biztonság szempontjából jobbnak mondható, de használója több időt fog eltölteni a belépéssel és ez nagyobb ellenszenvet válthat ki, mint például a fentebb említett Suprema BioEntry Plus esetében, ahol csak ujjunk megfelelő pozicionálásra volt szükség.



13.ábra: FingerKey DX-2000

3.2.3 iLock Iris Access 2020

Az írisz azonosítása talán az egyik legkevesebb kellemetlenséggel járó azonosítási forma. A legtöbb esetben nem kell mást tennünk, mint megmutatni a szemünket. Igaz ujjunkkal nem kell megérintetnünk semmit, mégis ellenszenvet kiváltó technológia, ugyanis a hitelesítés elvégzéséhez 15-30 cm-re oda kell hajolnunk. A legtöbb esetben nagyon érzékenyek a megvilágításra és szemünknek tökéletesen látszódnia kell. Gondolok itt arra, hogy szemhéjunkt olykor megerőltetve kell kinyitnunk és emiatt tovább tarthat az azonosítás. Sok esetben már az is elég, ha megtanuljuk használni. Rövid idő alatt elsajátítható az a mozdulatsor ami rögtön sikeres belépéshez vezet, de ennek megtanulása türelmet igényel. Emiatt ilyen készülékeket tömeges beléptetésre nem is használnak. Jellemzően nagyobb biztonsági igényű helyeken használják.



14.ábra: iLock Iris Access 2020

3.2.4 HandKey II

Negyedik generációs kézgeometria azonosító, ami az emberi kéz háromdimenziós alakját tárolja el. Egy alacsony energiájú infravörös fényt használva világítja meg a kezét, amit egy CMOS kamera rögzít. A hitelesítés elvégzéséhez egy egyéni kódra is szükség van. Mivel egyik legnagyobb előnye, hogy könnyen összeköthető a munkaidő nyilvántartó rendszerekkel ezért általában nagyobb cégek alkalmazzák. Ennél a készüléknél többször is kapcsolatnak kell kialakulni a használójával. Először is a kód beütése, ami igaz nem biometrikus adatnak számít, de mégis kapcsolat alakul ki. A másik problémás tényező, hogy nagy felületen ér hozzá a kezünk ami sokkal több szennyeződés

átadását tesz lehetővé. Helyes használat esetén ez a készülék is gyorsan működik, ezért sokan haladhatnak át rajta rövid idő alatt. Minél több ember használja annál nagyobb az esélye, hogy valamilyen betegség vagy fertőzés is lerakódik rajta. Gondolják ezt az emberek. Dolgozatomban ilyen vizsgálatokra nincs módomban kitérni, de számolnunk kell az ilyen eshetőségekkel is. Ez a fajta kapcsolat viszont nem minden kézgeometria olvasónál áll fent. Vannak olyan eszközök is amelyeknél elég csak oda tartani kézfejünket minden féle fizikai kapcsolat nélkül.



15.ábra: HandKey II

3.2.5 Retina azonosítók

Bár ilyen eszközt nem tudtam tesztelni, működése szempontjából a legnagyobb ellenszenvet kiváltó tényező az infravörös fény ami megvilágítja a retinát. Ez egy kellemetlen érzést okoz és annak tudata, hogy “infravörös” fényt használ a legtöbb emberben rossz előérzetet kelt, ugyanis attól félnek, hogy sérülhet a szemük. Természetesen erre nem kerülhet sor. Másik negatív tényező, ami az előzőt is érinti egyben, hogy fejünket mozdulatlanul kell tartani és adott helyre fókuszálni az azonosítás idejére. Ez kényelmetlenné teszi használatát. Valójában a legnagyobb veszélyt az okozza, hogy különösen közel kell hajolni emiatt egészségügyi kockázatai is lehetnek.

3.2.6 L-1 Identity Solutions

Működését tekintve megegyezik a kézerezet azonosítókkal, de ez a készülék ujjunk erezetét vizsgálja. Infravörös fénnel világítja meg ujjunkat amiben a fény visszaverődésének intenzitása adja meg az egyediséget. Ez az eszköz az ujjnyomat olvasókhoz hasonlóan pontos elhelyezését igényli. Itt nem egy szenzorra kell helyezni ujjunk, de két ponton is érintkezik vele bőrünk. Ezt követően egy egyedi azonosító kód beírására is szükség van.



16.ábra: L-1 Identity Solutions

3.2.7 Face ID F810

Arcfelismerő. Jelen pillanatban ezek a készülékek számítanak a biometria terén a legelfogadottabbnak, amennyiben azt nézzük, hogy mit kell tennünk hogy felismerjenek. Az egyik leggyorsabban fejlődő technológia ami annak köszönhető, hogy sokkal szélesebb körben használható mint mondjuk az ujjnyomat. Akár egy számítógép beépített webkamerája is el tudja végezni ezt a feladatot, ha a megfelelő szoftvert használjuk. Természetesen ezek nem nyújtanak akkora biztonságot, mint az erre a célra kifejlesztett Face ID. Az egyik legnagyobb előnye a többi biometrikus azonosítási formával szemben, hogy használata természetes, könnyű és nem akadályozza az embereket mozgásukban.

Gondolok itt arra, hogy nem kell tennünk semmit a felismerés érdekében, hiszen magától elvégzi a feladatát.



17.ábra: Face ID F810

3.3 Vizsgált szempontok

Szakmai szemmel vizsgálva a mérő személyek szubjektív véleménye alapján állítottam össze az alábbi szempontrendszert. Két konkrét tényező az azonosítási idő és a felhasználó és biometrikus eszköz közötti távolság.

A távolság minden azonosítási formánál más és más. Az ujjal történő belépés esetén hozzá kell érnünk a szenzorhoz, míg az arc azonosításánál elég csak a kamera által vizsgált területen lenni. Mondhatni ez a két véglet, ami jól mutatja, hogy mekkora a kényelmi különbség a kettő között.

Rohanó világunkban az idő az egyik legfontosabb érték. Az egyetemen számos sikeres és sikertelen belépést figyeltem meg az elmúlt évek során. Egy Suprema BioEntry Plus ujjnyomat azonosítón kell azonosíttatniuk magukat a hallgatóknak, ami sokszor megmagyarázhatatlan okok miatt vagy nem ismeri fel vagy elutasítja a mintát. Természetesen tisztában vagyok azzal, hogy az esetek 50-60%-ban a minta helytelen pozicionálása a hiba oka, de mivel ez idővesztéssel jár a használója számára kiemelt szempontként kell kezelni a negatív hatást keltő tényezők között.

Az azonosítási formák a technológiából adódóan máshogy működnek. Van ahol elég csak a szenzorhoz érni esetleg gombokat kell nyomni és olyan is akad ahol szemünket átvilágítva tud csak azonosítani. Az egyéb szempontoknál ezeket próbáltam összegyűjteni.

A táblázatba foglalt adatok azt mutatják meg, hogy az adott technológiára mi jellemző. A végleges eredmény azoknak a pontoknak az összessége amik igazak voltak az általam vizsgált készülékeknél, melyek megegyeznek a fentebb bemutatottakkal. A pontok nagyságának a mértéke egyenesen arányos a felhasználókban kiváltott ellenszenvvel. Ez alapján állítottam fel azt a sorrendet amit az összesített táblázat (19. ábra) tartalmaz.

Technológiák	Kategóriák									Eredmény (pont)
	Távolság			Idő (azonosítás)			Egyéb szempontok			
	>10 cm	kb. 10 cm	érintéssel	<2 s	<3 s	<4 s	gombot kell nyomni?	Meg kell állni?	Világít a szembe?	
Arc azonosítás	x			x						2
Kézerezet azonosítás	x	x	x	x	x			x		6
Kéz geometria azonosítás	x	x	x	x	x			x		6
Ujjnyomat azonosítás	x	x	x	x	x		x	x		7
Írisz azonosítás	x	x		x	x	x	x	x		7
Retina azonosítás	x	x		x	x	x	x	x	x	8

18.ábra: Eredmények

A 19. ábrán látható, hogy a pontozás alapján, az arcazonosítás váltja ki a legkevesebb ellenszenvet a használóikból. Bárhol alkalmazható és szinte csak a minimális kapcsolatot kell létrehozni használata során. A legnagyobb ellenszenvet a retina azonosítás kapcsán érzékelnek a felhasználók. Az is elmondható, hogy talán ez az azonosítási forma van a legkevésbé elterjedve.

1	Arc
2	Kéz
3	Tenyér
4	Ujjnyomat
5	Írisz
6	Retina

19. ábra: biometrikus sorrend

4 Összefoglalás

Kutatásom során azonosítottam azokat a tényezőket, amik az emberek és az azonosító eszközök között létrejöhetnek, majd ellenszenvet válthatnak ki. Ezek a tényezők vagy másként nevezve szempont rendszerek még közel sem tökéletesek. A legtöbb ember az azonosító technológiákat sem ismeri és ezért nem is tudják pontosan meghatározni azok hibáit.

Készítettem egy közvélemény kutatást, melyet több, mint háromszázan töltöttek ki. Választ kaptam arra a kérdésemre, hogy az emberek mit tartanak veszélyesnek egy biometria eszköz használata során és miként vélekednek a felsorolt technológiák biztonságosságáról.

Külön-külön minden technológiánál ismerttettem azt, hogy ezek a tényezők hogyan jelennek meg és miként hatnak az emberekre. Eredményeim azt mutatják, hogy a legkisebb ellenszenvet az arcazonosítás váltja ki, míg a legnagyobbat a retina alapú technológiák.

Fontos figyelembe venni, hogy ezek a technológiák azért lettek kifejlesztve, hogy nagyobb biztonságot nyújtsanak. Alkalmazásuknak, tehát az „ellenszenv” nem szabhat határokat. Belátható, hogy a biometrikus azonosító rendszereket úgy kell megtervezni, hogy minimális ellenszenvet váltsanak ki az azt használó emberekből. Például a tömegközlekedési rendszer esetén a lehető legkisebb ellenszenvet kell kiváltania az utasokból.

Úgy gondolom, hogy időre lesz szükség ahhoz, hogy elfogadottá váljon a biometria alkalmazása a hétköznapijainkban is. Bár ezek külön használata nem nyújt megfelelő védelmet. Valószínűsítem, hogy a megoldás a komplex rendszerek kiépítésében rejlik.

Fontosnak tartom azt, hogy az emberek megismerjék ezeket és valós képet kapjanak működésükről. Biztosra veszem, hogy a közeljövőben az elmúlt évekhez hasonlóan egyre szélesebb körben használjuk majd ezeket az eszközöket és beépülnek mindennapjainkba. Misem mutatja ezt jobban, mint hogy 2013 utolsó negyedében

piacra dobott mobil készülékek, már képesek az ujjnyomat azonosításra. Több éve alkalmazzák az arcazonosítás szoftveres módszereit és ez azt jelenti, hogy már elkezdődött az a folyamat, ami mindannyiunk életét megkönnyítheti.

Jövőbeli célom, hogy jobban megismerhessem ezeket a technológiákat és ennek köszönhetően finomíthassam azt a szempontrendszert ami alapján a gyártó, cégek ajánlhatják a telepítés megkezdése előtt az eszközöket.

5 Irodalomjegyzék

[1] <http://www2.mit.bme.hu/services/vimm3241/tanul/beadott/regi/SzigetvariMadai/main.htm>

[2] <http://oktel.hu/szolgalatas/belepteto-rendszer/biometrikus-azonositas/>

[3] Tajti Balázs, A biometrikus ujjnyomat azonosítás alkalmazásának új lehetőségei, Hadmérnök, VII. Évf 1. Szám – 2012 március

[4] Kovács Tibor, Milák István, Otti Csaba, A biztonságtudomány biometriai aspektusai

[5] <http://www.securinfo.hu/termek/biometria/1144-a-biometrikus-azonositas-modszerei-ujjnyomat-azonositas.html>

[6] <http://www.securinfo.hu/termek/biometria/738-iriszazonositas.html>

[7] <http://oktel.hu/szolgalatas/belepteto-rendszer/biometrikus-azonositas/>

[8] Őszi Arnold, A biometria alapú munkaidő-nyilvántartás elmélete és gyakorlata, Hadmérnök, VI. Évf. 1. szám – 2011. március

[9] http://www.hwsz.hu/hirek/31920/biometrikus_azonositas_felmeres.html

[10] Stan Z. Li Anil K. Jain, “Handbook of Face Recognition”

6 Ábrajegyzék

1. ábra ujjnyomat

[Forrás:

http://news.bbcimg.co.uk/media/images/63146000/jpg/_63146121_fingerprint_types.jpg
letöltve: 2014.03.28.

2. ábra arcaazonosítás [Forrás: <http://heyce.com/images/facerec.png>] letöltve: 2014.04.01.

3. ábra tenyérerezet [Forrás:<http://handyman.hu/wp-content/themes/handyman/images/biometria/kezerezet-azonositas.png>]

letöltve: 2014.03.28.

4. ábra tüske nélküli kézgeometria azonosító

[Forrás:<http://www.intechopen.com/source/html/40073/media/image2.jpeg>] letöltve: 2014.04.01.

5. ábra tüskés kézgeometria azonosító

[Forrás:<http://www.intechopen.com/source/html/40073/media/image6.jpeg>] 2014.04.01.

6. ábra írisz minta [Forrás: http://syntecoptics.com/wp-content/themes/theme1456/timthumb.php?src=http://syntecoptics.com/wp-content/uploads/2013/06/eye_min.jpg&w=630&h=270&zc=1] letöltve: 2014.04.03.

7. ábra retina minta [Forrás: <http://blog.m2sys.com/wp-content/uploads/2012/06/retina.jpg>] letöltve: 2014.04.01.

8. ábra Ellenszenvet kiváltó tényezők [Forrás: Szerző által készítve]

9. ábra Ismertség [Forrás: Szerző által készítve]

10. ábra Biometriai biztonság [Forrás Szerző által készítve]

11. ábra Biometrikus azonosító eszközök [Forrás: Szerző által készítve]

12. ábra Spurema BioEntry Plus [Forrás: Szerző által készítve]

13. ábra FingerKey DX-2000 [Forrás: Szerző által készítve]

14. ábra iLock Iris Access 2020 [Forrás: Szerző által készítve]

15. ábra HandKey II [Forrás: Szerző által készítve]

16. ábra L-1 Identity Solutions [Forrás: Szerző által készítve]

17. ábra Face ID F810 [Forrás: Szerző által készítve]

18. ábra Eredmények [Forrás: Szerző által készítve]

19. ábra Biometrikus sorrend [Forrás: Szerző által készítve]