Óbudai Egyetem

Doktori (PhD) értekezés

A biometrikus azonosítás helye és szerepe az e-kereskedelemben

Őszi Arnold

Témavezető: Prof. Dr. Kovács Tibor CSc / PhD

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos

Tagok:

Dr. Kiss Sándor

Dr. Simon Ákos

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár, ÓE

Titkár:

Dr. Szűcs Endre adjunktus, ÓE

Tagok:

Dr. Simon Ákos egyetemi docens, külső

Dr. Palik Mátyás egyetemi docens, külső, NKE

Dr. habil. Szunyogh Gábor egyetemi docens, ÓE

Bírálók:

Dr. Balla József r. ezredes, külső, NKE

Dr. Kiss Sándor egyetemi docens, külső, NKE

Nyilvános védés időpontja

2019.……..

TARTALOMJEGYZÉK

BEVEZETÉS

A profitot termelő, sikeres e-kereskedelmi rendszerek már működnek. Célom egy olyan környezet létrehozása, amely a vásárlói oldalon ezeket a rendszereket biztonságosabbá teszi egy biometrikus azonosító eszköz bevezetésével. 1 Az eszközök és eljárások összessége, amelyek a személyek mérhető testi, fizikai tulajdonságait használják fel valamilyen mintavételezési technika segítségével azonosításra vagy a személyazonosság megállapítására. [1] A biometria szóösszetétel a görög bios (élet) és a metricos (mérni) szavak összetételéből keletkezett. A fogalom az ember biológiai, anatómiai és viselkedési eltéréseinek számítógép általi felismerése. [2]

Az e-kereskedelem és a bankkártyák számának gyors növekedésével emelkedett az ezekkel történő visszaélések száma is [3]. Ezeket általában eltulajdonított, talált kártyákkal vagy felhasználói adatokkal követik el. Ezért is vált szükségessé az azonosítás hatékonyságának növelése.

Jelenleg az e-kereskedelmi rendszerek biztonsági szintje fejlesztésre szorul: a miden kétséget kizáróan beazonosítható partnerek üzletbiztonsága alapvető követelmény kell, hogy legyen. Erre nyújthat megoldást a biometrikus azonosítás. A biometrikus adatot nem lehet elfelejteni, mint például egy jelszót vagy egy kódot, nem lehet „kölcsönadni", vagy eltulajdonítani – mint ahogy ez megeshet egy tudás-, vagy egy birtoklás alapú rendszerrel (PIN-kód, különböző típusú kártyák). Sajnálatos módon a biometrikus azonosítás bevezetése rendkívül összetett feladat, megtervezésekor, létrehozásakor számos körülményt szükséges figyelembe venni (felhasználói környezet, alkalmazott technika, elfogadottság, bevezethetőség, stb.).

A biometrikus azonosítás folyamatosan, egyre több helyen kerül bevezetésre a mindennapi életben – elegendő csak a számítástechnikai és kommunikációs rendszereinkre gondolni. Szükség van rá, hogy a technológiát folyamatosan javítsuk, hiszen az számos potenciális sérülékenységgel rendelkezik. Ez természetesen rávetül az e-kereskedelemre is. A jelenleg működő rendszereken folyamatosan találnak biztonsági hiányosságokat, réseket, amelyeket – elvileg – azonnal szükséges (lenne) kijavítani.

Valós gyakorlati tapasztalataink alapján elmondható, hogy a biometrikus eszközök gyakran instabilan működnek. Ennek oka, hogy változik a használati környezet és/vagy az alkalmazó fizikai állapota (például ujjnyomat-azonosítás esetén az ujj nedvességtartalma, arc-felismerésnél a smink, az arckifejezés, vagy a megvilágítás is képes meghiúsítani az azonosítást).

Az e-kereskedelemben minimális követelményként jelentkezik a rendszerrel szemben, hogy az legyen képes a fizető személyét egyértelműen és megbízhatóan beazonosítani. A felismerő detektáló egységet ne zavarják meg egyéb környezeti eszközök, az azonosított mindenképpen valós személy legyen. Nem fordulhat elő téves azonosítás sem.

Az alkalmazott technikáról, eszközről a kiválasztási döntés többnyire nem minden kétséget kizáróan objektív (azaz például szempontrendszer alapján történő). Ár alapján, tetszetősség, vagy egyéb kényelmi szempontok szerint (például adott helyre befoglaló méret alapján elhelyezhető-e?) történik a kiválasztás. Szükség van tehát egy olyan megközelítésre, amely teljesen objektív paraméterrendszer alapján adja meg a legmegfelelőbb technológiát. Értekezésem témáját tekintve: a szóba jöhető biometrikus technológiák közül melyek és milyen mértékben felelnek meg leginkább az e-kereskedelem feltételeinek.

Disszertációm ismerteti és elemzi az e-kereskedelem jelenlegi helyzetét, a lehetséges biometrikus azonosítási lehetőségeket, majd kitér azokra a szempontokra, amelyek szerint vizsgálni szükséges az egyes technológiákat. Végül fontosság és súlyozás figyelembevételével meghatározásra kerül, hogy mely technológia és milyen mértékben alkalmas az e-kereskedelem által elvárt követelmények teljesítésére. A hivatkozással nem rendelkező ábrákat a szerző készítette.

A tudományos probléma megfogalmazása

Az elektronikus pénz biztonsága – akárcsak a készpénzé - kiemelten fontos. Annak problémamentes transzferálása nélkül az e-kereskedelem nem is létezik. Lényeges, hogy a pénz csak akkor cseréljen gazdát, amikor a tulajdonosa ezt kifejezetten jóváhagyta. Több ilyen módszer is jelen van már: közös jellemzőjük azonban az, hogy egyik sem magát a tulajdonost azonosítja, hanem egy kód ismeretét, egy kártya meglétét, stb., tehát tudás vagy birtoklás alapú.

A biometrikus azonosítás az egyetlen, amely valóban a személyt azonosítja, így ez a legbiztonságosabb ilyen eljárás. Az e-kereskedelemben alkalmazott megbízható biometrikus ügyfél-beazonosítás (vagy a tranzakcióban résztvevőké: eladó és vevő) kulcsfontosságú és megoldásra váró probléma.

Célkitűzéseim

Az értekezés elkészítésekor a következő célokat tűztem ki:

1. Elemezni az e-kereskedelem jelenlegi helyzetét, megállapítani annak gyenge pontjait.
2. Kimutatni, miként lehet hatékonyan növelni az elektronikus kereskedelem biztonságát a biometrikus azonosítás integrálásával.
3. Elemezni és értékelni az egyes biometrikus technikákat, technológiákat, hogy eldönthető legyen, melyik alkalmas a biztonságos e-kereskedelmi tranzakciók lebonyolításának feladatára.
4. Elkészíteni az eszköz azonosítási folyamatba illesztési protokollját.
5. Végső soron: egy olyan alkalmazás megalkotása, amely a jövőben a jelenlegi azonosítási módszereket kiváltja.

A téma kutatásának hipotézisei

A téma kutatásának első fázisában a következő hipotéziseket állítottam fel:

1. **Megadható biometrikus eszközökre a feladatorientált biztonsági küszöb (MOST – Mission Oriented Security Threshold) fogalma.** Lényeges, hogy megállapítható legyen, hogy az egyes (biometrikus) módszerek, eszközök egy konkrét feladat végrehajtására alkalmasak-e vagy sem.
2. **A MOST megadására felállítható egy teljes szempontrendszer.** A biztonsági küszöb megadásához reprodukálható, leellenőrizhető módon megalkotható egy teljes szempontrendszer. Ennek alávetve az adott módszert, vagy eszközt eldönthető, hogy az a követelményeket teljesíti-e vagy sem.
3. **Az e-kereskedelem biztonsági hatékonysága biometrikus azonosítás alkalmazásával növelhető.** Az elektronikus pénzmozgások között nagy számmal található olyan, amelyet nem a pénz tulajdonosa indított. Ezeket az eseményeket fontos kiszűrni, hogy javuljon a rendszer megbízhatósága. A feladatra a biometrikus azonosítás alkalmas.

Kutatási módszerek

A téma több ismeret-területet is érint, így például a biológiai és az informatikai tudományokat is. Az értekezés elkészítése során alkalmazott kutatási módszereket úgy kellett megválasztani, hogy azok kielégítsék a holisztikus, teljességre törekvő látásmód követelményeit.

Kutatómunkám során célként tűztem ki, hogy a témának ne csak az elméleti összefüggéseit dolgozzam fel, hanem annak gyakorlati megvalósítását is vizsgáljam. Így a disszertáció amellett, hogy leírja és elemzi az elméleti aspektusokat, jelentős mértékben épít saját gyakorlati méréseimre és tapasztalataimra.

Az elméleti módszerekről és összefüggésekről számos magyar és külföldi szakirodalmat dolgoztam fel. Ennek során alkalmaztam az analízis és szintézis módszereit. Kiemelt figyelmet kapott a gyakorlati megvalósítással kapcsolatos tapasztalataim teljeskörű összefoglalása.

A végrehajtott feladatokhoz kapcsolódó következtetések levonásához az indukció és dedukció módszereit alkalmaztam, végezetül pedig javaslatokat fogalmaztam meg.

Kísérleteimet összehasonlító, tapasztalati (empirikus) vázra építettem.

1 AZ E-KERESKEDELEM ÉS ANNAK BIZTONSÁGA

Az e-gazdaság minden olyan gazdasági tranzakciót magába foglal, amelyet az Internet vagy más hálózat segítségével bonyolítanak a termeléstől, az irányításon keresztül az eladásig. [4, p. 3.]

Az e-gazdaság egy része az e-kereskedelem. E-kereskedelemnek nevezhető bármilyen olyan tevékenység, ahol az adás-vétel lebonyolítására elektronikus csatornát alkalmazunk - fizikai csekkek, bankjegyek, érmék vagy egyéb elfogadott fizető eszköz valós mozgatása nélkül.

1.1 Az e-kereskedelem fejlődése

Az e-kereskedelem megállíthatatlan fejlődését mutatja be a fejezet, a számítástechnika megjelenésétől napjainkig.

1.1.1 Megjelenése

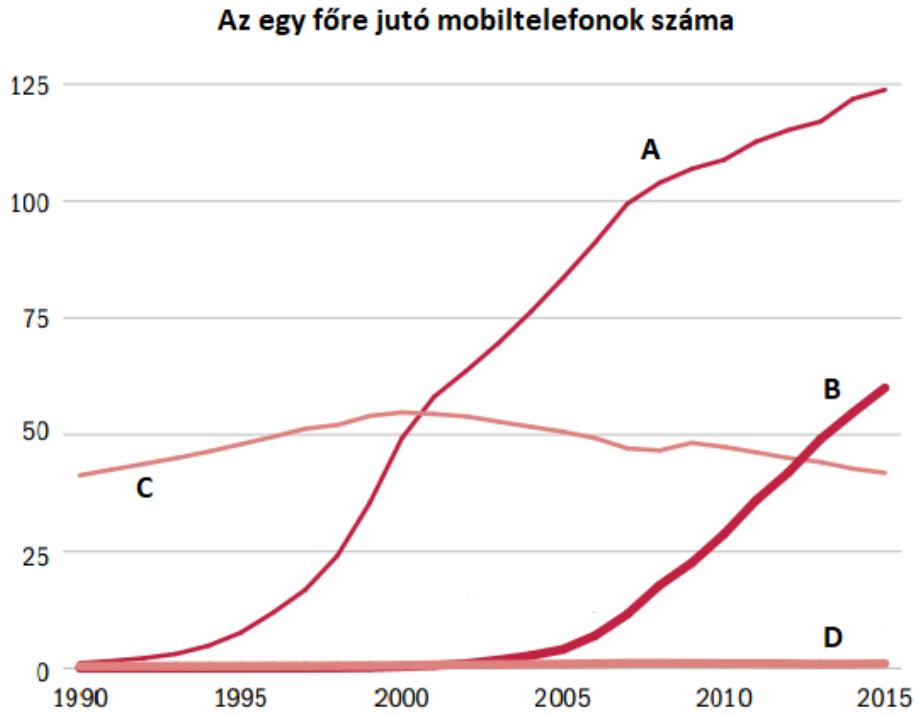
A XX. század közepén jelentek meg a számítógépek, amelyek azonnal fejlődési pályára állnak. A számítástechnika hajnalán csak önmagukban működő berendezéseről beszélhetünk. Nem sokkal később ezeket a különálló elemeket összekapcsolták, így létrejöttek a ma már jól ismert hálózatok. Ezek hamarosan az egész világra kiterjedtek, lehetővé téve a gyors információáramlást egymástól távoli pontok között.

Az 1990-es években jelentek meg a „dotcom” vállalatok, akik az elektronikus kereskedelemben lévő lehetőségeket először próbálták kiaknázni. 2000-ben az ilyen cégek forgalma visszaesett, sokan közülük megszüntették szolgáltatásaikat. 2004-2005-től lendült fel igazán az e-kereskedelem, amely fejlődése azóta is töretlen. [5]

1.1.2 Felfutási időszak

Az 1. ábra jól mutatja az e-kereskedelem méreteit és annak szigorúan monoton növekedő jellegét. 2016-ban Kínában az eladott áruk 19%-a elektronikus úton cserélt gazdát. Ez az arány világviszonylatban jelenleg 10% és várhatóan 2020-ra 15%-ra emelkedik majd.

Ezen vásárlások nagy része még mindig asztali számítógépen vagy laptopon zajlik, azonban egyre növekszik az okostelefonokon történő üzletkötések mértéke. Az online kereskedelem rohamosan növekvő mértékét mutatja be a 2. ábra. [6]

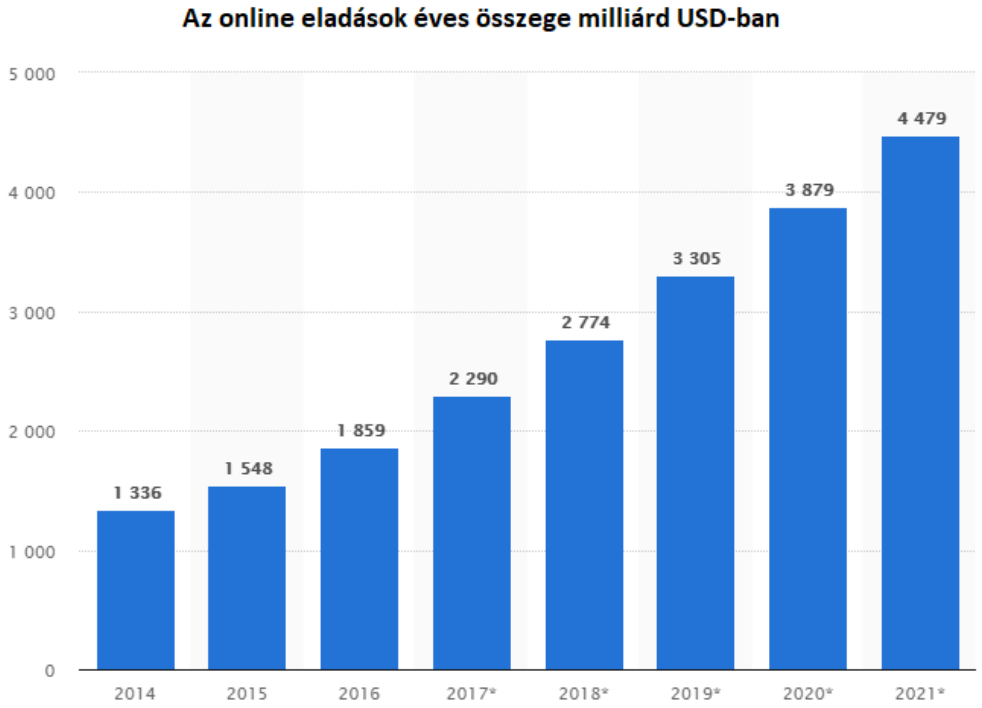


1. ábra: Az egy főre jutó vezetékes valamint mobiltelefonok száma százalékosan [7] (A: mobiltelefonok a fejlett országokban; B: mobiltelefonok a fejlődő országokban; C: a vezetékes telefonok a fejlett országokban; D: a vezetékes telefonok a fejlődő országokban).

Európában a kiskereskedelmi forgalom 3,4%-a bonyolódik valamely internetes felületen. Ennek 8,8 %-a különböző országok között zajlik. Az e-kereskedelemben a legtöbb esetben nem találkozik személyesen az eladó és a vevő egymással, éppen ezért az e-kereskedelem – többnyire megelőlegezett - bizalomra épül. [8]

Sajnálatos módon a web-áruházak 70%-a jogilag nem megfelelő módon működik. Ez a magas érték ugyanakkor nem jelenti azt, hogy minden esetben csalásról van szó. A

hiányosságok a törvényben előírtak be nem tartását jelentik, amely előírások hozzájárulnak ahhoz, hogy a vevő az őt megillető teljes körű információt megkapja és élhessen jogaival. [9]



2. ábra: Az online eladások éves összege milliárd USD-ban [6] (*-gal jelölve a becsült értékek)

Az e-kereskedelem jelentős mértékben van jelen Magyarországon is. A klasszikus web-üzletek 2010-es forgalma a GKIeNET felmérése szerint 130 milliárd forint, az aukciós piacé körülbelül 30 milliárd forint míg, a szolgáltatási ágazaté körülbelül 250 milliárd. [9]

Az online bankkártyás fizetések száma is jelentős mértékű, 2012-ben 3 millió felett volt, a bankkártyás fizetések összértéke 30 milliárd Ft, az egyes online fizetések átlagos összege 10.000 Ft-ra tehető.

1.1.3 Jelenlegi helyzet, várakozások

Ma Magyarországot tekintve a lakosság 73%-a használ internetet. A 100 főre jutó használatban lévő mobiltelefonok száma átlagosan 119. Világviszonylatban ezek az értékek 44% illetve 98, tehát hazánk a világátlag felett helyezkedik el.

2019 januárjában a következő adatok mutatják, hogy milyen nagy méreteket öltött a digitális térhódítás:

- 7.676 millió a Föld populációja,
- 5.112 millió a mobiltelefont használó személyek száma,
- 4.388 millió az internet használók száma,
- 3.484 millió a közösségi médiát aktívan használók száma,
- 3.256 millió azok száma, akik a mobil eszközön használják a közösségi médiát. [10]

Világviszonylatban, azok az emberek, akiknek mobiltelefonuk van, átlagosan 1,73 készülékkel rendelkeznek. A működő mobiltelefonok száma 8.842 millió db. [10]

A világban 2018. januártól 2019. januárig 2.818 millióan használták az e-kereskedelmet, az a teljes lakosság 37%-a. Minden felhasználó évente átlagosan 634 USD értékben vásárol. Az e-kereskedelem forgalmát kategóriákra lebontva az 1. táblázat mutatja be.

e-kereskedelem területe	**Összeg (milliárd USD)**
utazás	750
öltözködés és divat	524
elektronikai eszközök	392
játékok és hobbi	386
bútorok	272
élelmiszer és higiénia	209
videójátékok	70
digitális zene	12

[10]

1. táblázat: Az e-kereskedelem kategorizált forgalma

Ezen kívül megfigyelhető, hogy az emberek egyre nagyobb számban költöznek városokba, 1960-ban a Föld lakosságának 33,6%-a volt városlakó, 2019-re ez az érték 55,3%-ra emelkedett. [11]

Jelenleg a pénzmozgás nagyobbrészt online történik. Napjainkban a médiában szinte folyamatosan arról tájékoztatnak minket, hogy újra és újra több millió bankkártya adatot lopnak el az interneten a bűnözők. Az ilyen típusú bűnözést nem lehet földrajzilag egzaktul behatárolni, hiszen ilyen támadásokat eddig 82 országból jelentettek. [12]

A kiber-bűnözést tekintve világviszonylatban 1.000 milliárd USD esik áldozatul évente a nem jogos bankszámlaadatokkal történő visszaélés következtében. [13]

Lényeges tehát, hogy a vásárlói (a fizető) jogosultságot minden kétséget kizáróan lehessen megállapítani – például a biometrikus azonosítás révén.

1.2 Az e-kereskedelem technikai felépítése

A megoldást úgy kell megtervezni, hogy az karbantartható legyen. Legyen lehetőség arra is, hogy az egyes modulokat a majdani használat során egyszerűen cserélhessük le korszerűekre (például egy biometrikus eszköz elavulása után a rendszer legyen képes jelentős strukturális átalakítás nélkül az új biometrikus eszköz fogadására).

1.2.1 A rendszer technikai felépítése

Egy e-kereskedelmi rendszer 4 alapvető összetevője:

1. A bank(ok).
2. Az e-kereskedelmi rendszer tulajdonosa, üzemeltetője.
3. A felhasználó személyi számítógépe.
4. A biometrikus azonosító eszköz.

A rendszer négy elemének a feladata a következő:

A bank(ok) a vásárlótól az eladóig eljuttatják a pénzt. Általában számláról számlára mozog a pénz átutalással, de lehetséges virtuális bankszámlák használata és bankon kívüli lehetőség alkalmazása (pl. PayPal) is.

Az e-kereskedelmi rendszer tulajdonosa (üzemeltetője) egy honlapot tart fenn, amelyen keresztül bejelentkezhetnek a felhasználók, megérkezhetnek a rendelések, létrejöhet a fizetés és esetenként a kiszállítás állapota is nyomon követhető.

A felhasználó személyi számítógépe megjeleníti az előzőekben említett tartalmakat. A tervezésnél figyelembe kell venni, hogy a megoldás a lehető legtöbb hardver alkalmazásával is működőképes legyen ugyanakkor nem csak asztali PC-vel és laptopokkal, de tabletekkel és okostelefonokkal is kompatibilisnek kell lennie.

A biometrikus azonosító eszköz a rendszer kritikus, és talán a legfontosabb eleme. Feladata, hogy pontosan azonosítsa a megrendelőt, vagyis a személyt, aki a megvásárolt termékért fizet. Az eszköz gyakorlatilag nem tévedhet. A rendszer a bank adatbázisában tárolt mintát hasonlítja össze a biometrikus azonosító eszköz által felvettel. Sikeres azonosítás esetén az alkalmazás engedélyezi az e-kereskedelmet bonyolító szervernek a vásárlást és a vásárló számlájáról az eladó számlájára utalja a virtuális pénzt.

1.2.2 A rendszer megtervezésének lépései

Egy biometriát alkalmazó e-kereskedelmi rendszer igen összetett. A megoldás komplexitása gyakorlott rendszertervező szakembert igényel.

A bonyolult rendszereket nem lehet jól átlátni, viszont alaposan megkönnyíthetjük a helyzetünket, ha azt kisebb egységekre bontjuk. Az így létrehozott (kisebb) egységek már gond nélkül „megfoghatók” és jól értelmezhetők. A komplex egység tervezése folyamán az egyes kisebb részegységeket külön-külön célszerű vizsgálni.

A rendszerek halmaza a következő hierarchia szerint épül fel:

- Egy-egy rendszer (ilyen lehet például a kommunikációs vagy az információs rendszer);
- Alrendszer: önálló egységek, de nem érik a teljes rendszer struktúráját (például: jelhálózatok, adatbázisok);
- Komponens: a rendszer szintű tervezés középső szintje (jelvevők, adat-megjelenítők, adatbázis programok, energiaellátás);
- Alkomponens: elemi részegységek (jelerősítők);
- Részek: önállóan működésképtelenek, ezért részekkel kombinálandók (transzformátor, LED, algoritmus, burkolat). [14]

A tervezés fázisai a következők:

1. A koncepció kidolgozása, a rendszer céljának pontos meghatározása.
2. A minimális követelmények megadása. Ezek lehetnek funkcionálisak, minőségre, dizájnra vonatkozók, vagy a vevő által meghatározottak.
3. A pontos konfiguráció kidolgozása.
4. Megvalósíthatósági elemzés készítése.
5. Határidők és mérföldkövek kitűzése.
6. A költségkeret és a költségek eloszlásának megtervezése.
7. Mérnöki tervezés.
8. A rendszer fizikai megalkotása, próbaüzeme, üzemeltetése.
9. A működés folyamán karbantartás, felújítás, az esetleges hibák szervízelése.
10. Az élettartam végén és/vagy új koncepció kidolgozásakor: a rendszer lebontása, a hulladék újrahasznosítása

A koncepció kidolgozásához tudnunk kell, hol alkalmazzák majd a megoldást. Ezért az egyes esetekben nem lehet sablonszerűen ugyanúgy eljárni. Hogy mennyire eltérő lehet a környezet elég arra gondolni, hogy ugyanannak a megoldásnak működnie kell:

- kormányzati,
- cégek közötti,
- cég-magánszemély,
- magánszemély-magánszemély,
- cég-alkalmazott relációban is.

Komoly kérdésként merül fel az is, hogy egy-egy rendszert mennyi ideig kívánjuk (célszerű) üzemeltetni? Meghatározható-e az elavulás időpontja? A helyes válasz az, hogy természetesen igen. Ez abban a pillanatban következik be, amikor az adott feladatot a rendszer már nem képes hiba nélkül megoldani.

A megvalósíthatósági elemzésnek számos területre kell kiterjednie, nevezetesen:

- technikai megvalósíthatóság, kockázatelemzés,
- gazdasági megvalósíthatóság (költség-haszon): mennyibe kerül a megoldás, milyen előnyökkel jár, Return on Investment (ROI),
- működési / szervezeti megvalósíthatóság,

- célszemélyek elemzése, várható felhasználási igény meghatározása,
- időterv megvalósíthatóság, tarthatók-e a határidők?
- jogi megvalósíthatóság: megfelel-e az alkalmazási területen lévő jogi előírásoknak a rendszer?

1.2.3 A kiválasztás szempontjai

A jó megoldást akkor tudjuk megtalálni, ha pontosan megértettük a problémát. A probléma jelen esetben az, hogy a felhasználók azonosítása nem minden körülmények között hibamentes - másképpen fogalmazva: a csalások lehetőségét a lehető legkisebbre, kvázi nullára kell szorítani. Ilyen rendszert kell tehát alkotni.

Lényeges, hogy a rendszer mind az ergonómiai szempontoknak, mind az egyszerű kezelhetőségnek feleljen meg. A szoftver működtetéséhez ne legyen szükség speciális ismeretekre, az új hardver elemek kezelése legyen egyértelmű. Gyakorlati példa, hogy a biometrikus azonosító eszközt nem helyesen alkalmazza a felhasználó, a rendszer pedig mindezt nem ismeri fel (például nem figyelmeztet a helyes pozícionálásra – hanem minden ilyen jellegű vizsgálat nélkül elutasít).

Vizsgálandó kérdés a rendszer üzemeltetési környezete. Olyan megoldást kell tervezni, amely megállja a helyét ipari, irodai és otthoni környezetben is. Lehet elvárás, hogy a megoldás alkalmazható legyen mobil eszközökön.

Minden egyes esetben kockázatelemzést kell készíteni a rendszer alkalmazásához. Ennek tartalmaznia kell a lehetséges kockázatokat, azok bekövetkezési valószínűségét és a bekövetkezés esetén a kár mértékének a leírását.

1.2.4 A kiválasztott biometrikus azonosítási módszer fontossága

Az e-kereskedelem céljaira kiválasztott biometrikus azonosítási módszernek olyannak kell lennie, hogy az hosszú távon, legalább (10-15 év) alkalmazható legyen.

Például a hangfelismerés könnyen reprodukálható, amennyiben a hangot rögzítjük, majd visszajátsszuk. Ezen kívül a betegségek jelentős része jár a hang megváltozásával, amely a beszélő felismerését az esetek döntő többségében megzavarja.

Az ujjnyomat-azonosítás az emberek 3%-ánál nem alkalmazható. Ezt okozhatja ideiglenes sérülés, vagy gyakrabban valamilyen észrevétlen szennyeződés az ujjon. Az ujjnyomat esetén az élőminta felismerés költséghatékonyan még nem megoldott.

Az ujjerezet nem tartalmaz elegendő egyedi pontot egyes emberek esetén, így az azonosítás nem jár minden esetben sikerrel, illetve a felhasználói bázis ennek következtében kicsi.

A kézgeometria alapú azonosítás szintén lehetne jó megoldás, azonban az azonosítást végző eszköz túl nagy, mobil eszközökben nem használható.

1.3 Sérülékenységi pontok az e-kereskedelem területén

A sérülékenységi vizsgálatok célja, hogy a talált hiányosságok javításra kerüljenek még az előtt, mielőtt valaki kihasználná a rendszer ezen gyengeségeit. Ezeket a vizsgálatokat általában hivatalosan, szerződéses megrendelésre készítik, de akadnak szép számban felkérés nélkül ilyen jellegű tevékenységet folytatók (például etikus hekkerek).

Az informatikai világ bűnözői előszeretettel élnek vissza bankkártya adatokkal. A pénzügyi részlegek támadása 95%-ot tesz ki és a kereskedelmet irányító informatikai rendszerekkel szemben hajtják végre a legtöbb sikeres ilyen akciót (21,7%). [15, p. 19]

A e-kereskedelem biztonsági szintjének megállapítása érdekében szükséges az összes biztonsági megoldás vizsgálata a tűzfalaktól kezdve az adatbázisok biztonságán keresztül egészen a social engineering elleni védelemig. [16] A biztonság szerencsére számos megoldással növelhető: ilyen például a PKI (Public Key Infrastructure), a proxy szerverek, titkosító programok, digitális certificate-ek, digitális aláírások, tűzfalak. [17] [18]

1.3.1 Egy lehetséges sérülékenységi vizsgálati módszer

Közhelyes, de ettől még igaz, hogy tökéletes eszköz és tökéletes program sem létezik, illetve, hogy a támadók mindig egy lépéssel a védekezők előtt járnak. A sérülékenységi vizsgálatok célja, hogy kiderüljön, mennyire nehéz egy támadónak bejutnia a védett rendszerbe és ott számára nem engedélyezett információszerzést vagy változásokat létrehozni, sikeres műveleteket végrehajtani.

A következőkben egy általam megalkotott vizsgálati módszer kerül ismertetésre, amely specifikus a biometrikus vásárló-azonosítással kapcsolt e-kereskedelmi rendszerre.

A metódus a következő területeket érinti:

- felderíthetőség,
- titkosítás,
- lehallgathatóság,
- tranzakciók másolhatósága.

A legtöbb rendszer számos sebezhetőséggel rendelkezik informatikai oldalról. Ezeket folyamatosan találják meg a szakemberek és különböző fórumokon osztják meg egymással. A közismertebbek közül néhány: *securiteam, securityfocus* vagy *wikileaks*.

A „White hat hacker” gyűjtőnév azokat az informatikában elmélyült szakértőket foglalja magába, akik a rendszerek sérülékenységeit megtalálva nem élnek vissza a megszerzett adatokkal, hanem a programok tökéletesítését segítik. Ők többnyire szerződéssel dolgoznak hivatalos megrendelésre. A titoktartási résszel készült megállapodás pontosan leírja, hogy a rendszer mely elemeit vizsgálhatják és milyen módon, hiszen a beavatkozások a működő informatikai környezet részleges vagy teljes leállását is okozhatják.

A feladat elvégzése után a vizsgáló egy rövid, valamint egy részletes dokumentációt ad át a megrendelőnek és többnyire egy prezentációban mutatja be a talált biztonsági réseket. A végeredmény egy javaslattétel, ami konkretizálva lehet tréning a felhasználóknak, szoftverbeállítás, de akár a hardver és szoftverelemek cseréje is.

A hálózat gyenge elemei lehetnek aktív és passzív eszközök, desktopok, szerverek, hálózati eszközök, switchek, rooterek, tűzfalak.

Minden esetben információgyűjtéssel kezdik a támadók a munkájukat. Nevezetesen:

- A cég vagy szervezet és a vele összefüggő honlapok áttekintése (lehet, hogy a honlapnak egy tágabb IP-tartományt tartanak fent, ekkor az egész tartományban kereshetőek a szolgáltatások például a portok feltérképezésével).
- Milyen webszervert használnak, annak milyenek a beállításai, vannak-e hibái, hiányosságai?
- Milyen mailszervert használnak, annak milyenek a beállításai?

- Milyen az alkalmazott wifi, annak milyenek a beállításai, vannak-e hibái, hiányosságai?
- Melyek a fontosabb jelszavak?
- A fontosabb személyek elérhetőségei.
- A cég vagy szervezet felépítése.
- Kulcsszavak gyűjtése, amelyeket jelszónak használhatnak az adott helyen.
- Esetleges hibák a forráskódban.

A cég vagy szervezet honlapjait az esetek döntő többségében úgynevezett „googlehack" eljárással szokták felderíteni, ami azt jelenti, hogy irányított, „paraméterezett" google kereséssel jutnak el az adott információhoz.

Ezután megpróbálják támadni a feltárt egységeket. Amennyiben tudják, hogy mivel állnak szemben, akkor pontosan tudják azt is, hogy milyen sérülékenységeket kell keresni.

Jellemzően először egy saját gépparkon gyakorolják be a támadók a támadásokat, mielőtt az éles akciót végrehajtanák. Ekkor lemásolják a hardver elemek hierarchikus felépítését és a szoftveres környezetet, de arra is figyelnek, hogy a tesztkörnyezetükben az egyes szoftverek verziója egyezzen meg a valós rendszerével. Utánajárnak, hogy az adott programoknak hol vannak sérülékenységi pontjai, részei. Ezeket akár internetes fórumokon is megismerhetik. Majd gyakorlatot szereznek a saját rendszeren, a valódi cél támadása előtt - az egyszerűbb megoldásoktól a bonyolultabbak felé haladva.

A jelszavakkal kapcsolatban tény, hogy sokan ugyanazt a jelszót használják több helyen. Így, amennyiben sikerül megszerezni egy személy jelszavát egy gyengén védett környezetből, akkor ugyanezzel esetleg lehetséges az erősen védett helyre való bejutás is. Másik lényeges informatív elem, hogy az emberek általában a személyesen rájuk jellemző számokat, szavakat, jelsorozatokat használják jelszóként.

Cég vagy intézet esetén például a honlap minden egyes szava lehet valahol egy jelszó. A támadók ezt kihasználva a honlap tartalmának letöltésével jutnak lehetséges jelszavakhoz. Ezt legtöbbször a *httrack* alkalmazással teszik meg. Például a *webextractor*-t használva adott típusú adatokat tudnak letölteni (például telefonszámokat vagy email-címeket).

A 2014-es statisztikák szerint a vírusfertőzések 80%-a trójai program. [19, pp. 165-166.] A zero-day sérülékenység például egy olyan hiba a rendszerben, amelyet korábban nem ismertek, és most frissen fedezték fel. Ezek a legveszélyesebbek a támadók kezében, hiszen nincs kidolgozva a védekezés ellenük.

A támadó megtalálása sokszor nehéz, mert általában zombi-gépeket használ. A zombi-gépek ártatlan személyek számítógépei, azonban a támadó utasítja ezeket, hogy ezek hajtsák végre a támadást a cél ellen. A megtámadott egység naplófájljaiban olyan bejegyzéseket fog majd találni a helyi rendszergazda, hogy a védett gépeket az a vétlen személy támadta meg, akinek a gépét „zombi géppé" alakították, így a valós támadó kilétére soha nem derül fény.

A sebezhetőségek felderítésére két módszer létezik: a kézi és a gépi. A kézi esetében a támadó, aki jól ismeri a támadott környezet elemeit, megpróbál bejutni a rendszerbe az általa ismert módszerekkel. A gépi módszer ugyanezt teszi automatikusan, azonban vannak különbségek a két lehetőség között. A kézi csak azt keresi, ami nagy valószínűséggel ott van a rendszerben. Például, ha a célpont nem használ adatbázist, akkor nem kezdi el futtatni az adatbázis-sérülékenységekre vonatkozó teszteket, így sokkal kevesebb bejegyzést hagy a logokban, tehát kevésbé észrevehető és nehezebb visszakövetni is. A gépi (pl. Nessus) sokkal gyorsabban dolgozik, alkalmazása kevesebb szakértelmet igényel, ezen kívül sokkal több lehetőséget próbál ki - a frissen felfedezett sérülékenységeket is beszámítva. Ebből következik a hátránya is, hiszen a naplókban rengeteg bejegyzést hagy. A modern eszközök felismerik a tevékenységet és kizárják a támadót, mielőtt az megtalálná a támadott rendszer gyenge pontját. Másik hátránya a gépi módszernek, hogy az általa talált sérülékenységek - tapasztalataim szerint - 80%-ban hamis vagy téves riasztás.

A kommunikáció a legtöbb esetben TCP/IP protokollon keresztül történik. Az adatok áramlása adott állomások adott portjai között megy végbe, így, amikor megfigyeljük, hogy mely portok között halad az adatcsomag, nem csak a küldő és a fogadó állomásról deríthetünk ki információkat, de lehallgathatjuk, vagy megmásíthatjuk az egységek közötti kommunikációt is.

A következőket kell mindenképpen vizsgálni:

- Mit lehet letölteni (az menyire fontos, kihasználható-e)?

- Milyen hibákat tartalmaz a rendszer és létezik-e hozzá olyan eljárás, amelylyel ez kihasználható?
- A jelszavak megszerezhetőek-e?
- Lehet-e illetéktelenül törölni fontos adatokat?

1.3.2 Az informatikai rendszer jellemzőinek vizsgálata

A következőkben megadom a feltétlenül vizsgálni szükséges részleteket. Ezek részleteiben:

Felderíthetőség

Kérdés, hogy a jelenleg elterjedt felderítő alkalmazásokkal milyen mértékben lehet detektálni a hálózat elemeit. Fontos tudni, hogy a felderítés folyamán milyen mértékben lehet megállapítani, hogy a rendszer mely elemekből áll, illetve az összetevők tulajdonságai elérhetőek-e (például a gyártó, a típus, vagy a verziószám). A felderítést a legtöbb esetben a portok feltérképezésével végzik.

Amennyiben nyitott portok vannak egy rendszeren, akkor azok potenciális támadási lehetőségekként működnek. Csak a feltétlenül szükséges portokat szabad nyitva hagyni és csak azon egységek számára, amelyeknek ez szükséges. Így elkerülhető, hogy egy nyitott portot kihasználva támadást hajtsanak végre a rendszerben. A portokat a gyakrabban az nNap alkalmazással derítik fel. Ez igen jól konfigurálható, számos scan módszert ismer.

Az ilyen vizsgálatokat két nagy csoportba oszthatjuk. Az egyik a *portscan*, amely esetén egy host-ot vizsgálunk annak felderítése érdekében, hogy mely portok nyitottak rajta. A másik nagy csoport a *portsweep*, amely esetén több host-ot vizsgálunk annak felderítésére, hogy a keresett port melyik host-on van nyitva.

A keresés eredményei a következők lehetnek:

- Nyitott port: a host válaszol, tehát a portot hallgatja egy szolgáltatás.
- Zárt: a host azt a választ adja, hogy a port zárva.
- Blokkolt: a host nem válaszol.

Több port scan megoldás létezik. A TCP connect() egyszerűbben programozható, de a kísérletek láthatóak a célhost-on. Ezen kívül létezik számos módszer, amellyel nem

készül log a célhost-on, ilyen például a TCP SYN. Mások a régi rendszerek hiányosságait használják ki. Jellemzően elmondható, hogy amennyiben ismert a host típusa, akkor ki lehet választani az adott host-ot legjobban felderítő módszert. [16]

Titkosítások

A titkosítások alapvetően lehetnek szimmetrikusak vagy aszimmetrikusak.

- szimmetrikusak: a kódoláshoz és a dekódoláshoz ugyanazt a kulcsot használják,
- aszimmetrikusak: a kódoláshoz és a dekódoláshoz eltérő kulcsot alkalmaznak.

A szimmetrikus titkosítás előnye, hogy jóval gyorsabb, mint az aszimmetrikus. Hátránya, hogy a feladónak és a címzettnek is ismernie kell a kulcsot, amit csak biztonságos csatornán javasolt elküldeni a feladótól a címzettnek, hiszen a kulcs megszerzésével bárki olvashatja az üzenetet.

A szimmetrikus kulcs alkalmazása esetén a kódolás és a dekódolás ugyanazzal a kulccsal történik. A kulcs lehet jelszó vagy kulcsfájl, esetleg ezek kombinációja.

Az algoritmusok kombinálhatók is, így például, ha AES-el titkosított egy adat, azt még titkosítható Serpent algoritmussal is és a végeredményt tovább titkosítható Twofish-el. A biztonság akkor a legmagasabb szintű, ha ezeknél egymástól teljesen különböző kulcsot választanak.

Szimmetrikus titkosítás legtöbbször a tárolt adatok titkosítására szogál.

Az aszimmetrikus titkosítás alkalmazása esetén a kódolási és dekódolási folyamat lassabb, mint a szimmetrikus módszereknél, emiatt ezt az eljárást nem szívesen használt nagyméretű adatok esetében.

Az aszimmetrikus titkosítás esetén a kódolás egy nyilvános kulcs segítségével, míg a dekódolás egy másik, úgynevezett titkos kulcs segítségével történik. A gyakorlatban a működés lényege az, hogy a kommunikáció résztvevői rendelkeznek saját nyilvános és titkos kulccsal.

A nyilvános kulcs segítségével titkosítható az adat, amely ezután már csak a hozzá tartozó – kizárólag a címzett birtokában lévő – titkos kulcs segítségével fejthető vissza. A nyilvános kulcsról tudni kell, hogy nem állítható elő belőle a titkos kulcs, és a nyilvános kulcs segítségével nem dekódolható az üzenet. [20]

Jelenleg a jelszavak törésének számos módja terjedt el. Ezek ellen megfelelő védelmet a megfelelően választott jelszó adhat, amely például tartalmaz kis-, nagybetűt, számot és írásjelet, hossza minimum 10 karakter hosszúságú. [21]

Lehallgatás (sniffing) és annak megakadályozása

A bankkártya adatokat ismerve ATM-ből lehet pénzt felvenni és az interneten vásárolni akár a számla tulajdonosának beleegyezése nélkül is. Hozzávetőlegesen 10 millió dollárt tulajdonítanak el minden 24 órában ezzel a módszerrel.

A sniffing lehet aktív és passzív. Passzív sniffing esetén nem állapítható meg, hogy a kommunikációt elfogták, mert a támadó csak lehallgat. Általában nem titkosítják az adatot a következők: HTTP, ftp, pop3, telnet, Simple Network Management Protocol (SNMP).

Néhány gyakran alkalmazott célprogram, amellyel a rendszer biztonsága tesztelhető:

- A driftnet-v, amely megjeleníti a célszámítógép interneten lehívott képeit.
- Az ettercap-g és a dnsniff listázza a számítógépbe bevitt felhasználóneveket és a mellé beírt jelszavakat.
- A WinSniffer egy sniffer alkalmazás. Figyeli a bejövő és kimenő adatokat és dekódolja a következő protokollokon áthaladó felhasználóneveket és jelszavakat: FTP, POP3, HTTP, ICQ, Simple Mail Transfer Protocol (SMTP), telnet, Internet Message Access Protocol (IMAP), Network News Transfer Protocol (NNTP). Amennyiben a felhasználónév és a jelszó titkosítva kerül átküldésre, úgy a winsniffer nem nem képes megfejteni azokat.

Lehetőség van rá, hogy lehallgassanak egy tetszőleges hálózatot. Ez lehet vezetékes vagy vezeték nélküli hálózat. Ezen célra legmegfelelőbb a *Wireshark*. A program egy egyszerűen elérhető, ingyenes csomaggyűjtő és csomagmegjelenítő alkalmazás. A programmal ellenőrizni kell, hogy azon adatokat, amelyeket a hálózaton keresztül küld a rendszer valóban a megfelelő titkosítással látták-e el. Mivel a program minden forgalmat megjelenít, ezért a gyakorlatban egy átláthatatlan információhalmazhoz lehet jutni. Ezt a halmazt szűrni kell, hogy megtalálható legyen a keresett üzenet.

Néhány szűrő példaként, amivel a *Wireshark* által listázott adatok szűkíthetőek:

- ip.dsteq www.uni-obuda.hu (csak a www.uni-obuda.hu–val folytatott kommunikációt listázza).
- ip.src == 192.168.1.1 (csak a 192.168.1.1. host–al folytatott kommunikációt listázza).
- eth.dsteq ff:ff:ff:ff:ff:ff (csak a Layer 2 broadcastpacket-eket listázza).
- host 172.18.5.4 (csak a 172.18.5.4. IP címre küldött és az onnan érkező kommunikációt listázza).
- net 192.168.0.0/24 (adott IP cím tartományon lévő hálózati forgalmat listázza).
- port 80 (csak a 80-as port (HTTP) forgalmát listázza).

Egy ajánlott megoldás lehet a lehallgatás problémájára az *ssltuneling*. Ez biztonságossá teszi a kommunikációt a gép és a szerver között azáltal, hogy az adatot a nyílt csatornán titkosítva továbbítja. [16]

Naplók

Fel kell deríteni, hogy a rendszer naplózza-e az eseményeket, és ha igen, akkor milyen szinten. Egy esetleges támadás esetén például a naplóból kiolvasható, hogy mikor és honnan érkezett a támadás. Amennyiben a támadó nem fordított kellő figyelmet saját maga elrejtésére, akkor az is kiderülhet, hogy pontosan ki volt az elkövető. Érdemes tehát naplózni azt, hogy ki mikor hová lépett be és pontosan milyen műveleteket végzett.

A naplók használatával ugyan nem előzhetőek meg a támadások, de a segítségükkel azok visszanyomozhatók: így generális prevencióként is működnek, hiszen amennyiben a támadó tudja, hogy az általa megtett lépéseknek nyoma marad egy log-fájlban, akkor inkább el sem kezdi a tevékenységét. [16]

Tűzfalak és DMZ

A tűzfal szoftver és hardverkomponensekből felépülő egység. Hardver szempontjából legtöbbször egy router vagy egy proxy tölti be ezt a szerepet. A jó tűzfal megakadályozza a külső támadások döntő többségét.

A DMZ a demilitarizált zóna rövidítéséből kapta a nevét. Ez egy alhálózat, amely egy helyi hálózat részeit tárja fel egy nagyobb hálózat, jellemzően az internet felé. Az

internet felől csak a hálózat azon eszközei látszódnak, amelyek a DMZ részét képezik, így a helyi hálózat biztonságát növeli a megléte. [16]

A vezeték nélküli rendszerek

A legelterjedtebb vezeték nélküli kommunikációs csatorna a wifi. Nyílt wifi esetén bárki láthatja a küldött és fogadott adatokat, míg titkosított wifi esetén a jelszó megszerzése után válnak a küldött adatok megjeleníthetővé a támadó számára.

A social engineering

A social engineering ugyan nem kapcsolódik közvetlenül a számítástechnika területéhez, azonban a biztonság szempontjából kritikus, ezért ezen területet is vizsgálni szükséges.

A kérdés úgy hangzik, hogy mit lehet meg tudni a célpontról, valamint hogyan lehet felhasználni a gyűjtött információt.

Maga a fogalom egyidős az informatikával. A módszer az emberek túlzott segítőkészségét használja ki, így felderíthetők telefonszámok, adatok sőt még jelszavak is. Az emberek jóhiszeműen rávehetőek arra, amit önmaguktól talán soha nem tennének meg, például telepítenek szoftvereket idegenek utasítására, biztonsági beállításokat módosítanak, vagy a támadónak belépést engedélyeznek a védett rendszerbe.

Minden esetben szükséges ellene védekezni. A legjobb módszer az, amikor például egy oktatás alkalmával felhívják a dolgozók figyelmét ezekre a veszélyekre és tudatosítják náluk, hogy csakis és kizárólag akkor adjanak ki információt és módosítsanak bármit a rendszeren, ha meggyőződtek róla, hogy a kérést kiadó személy valóban az, akinek mondja magát.

A social engineering ellen véd az is, hogy a szoftvereket használó személyeknek nincs teljes hozzáférése, csak azon részeket látják, amellyel valóban feladatuk is van.

CVSS (Common Vulnerability Scoring System)

A CVSS feladata, hogy a feltárt sérülékenységeket veszélyességük szerint rangsorolja. Ezzel az egyes sérülékenységek veszélyességének mértéke skálázható, egymással összehasonlítható. Alkalmas rá, hogy az újonnan megjelenő sérülékenységek pontszámát

meg lehessen állapítani, ha publikált sérülékenységek döntő többsége már listázásra került a központi CVSS adatbázisban.

PayPass rendszerek

A PayPass is rendelkezik sérülékenységgel. Amerikában 2003-tól, Magyarországon 2009 óta használják. A PayPass egy érintés nélküli azonosítással ellátott bankkártya. Magyarországon PIN-kódos megerősítés nélkül 5.000Ft alatt használható. A kártya tulajdonosa csak a vásárlásokat követő nap kap értesítést a telefonjára a napi forgalmáról.

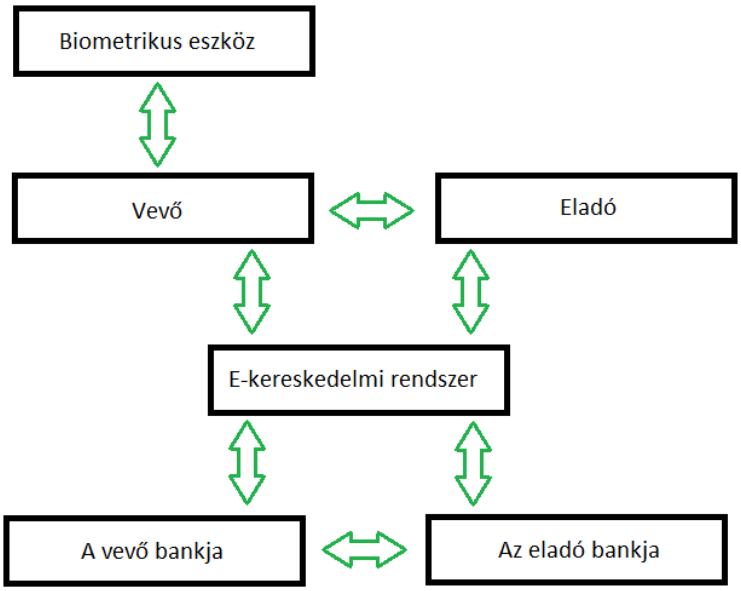
A PayPass kártyákból bárki számára érintés nélkül kiolvashatók a tulajdonos számlaadatai, lehetséges egy ilyen kártyát lemásolni és azzal egy másik országban illetéktelen sikeres vásárlást végrehajtani. [22, pp. 153-162.]

Megoldás a felmerült sérülékenységekre

Az előbbiekben feltárt problémákra a biometriával kiegészített e-kereskedelem esetében a következő - általam kidolgozott – folyamat jelenthet megoldást (3. ábra):

1. Egy nyilvános template előállító algoritmust ad ki a bank. Ez az algoritmus a vásárló gépén fut le.
2. A biometrikus eszköztől a vásárló gépéig az adat titkosítás nélkül halad (amennyiben nincs egybeépítve).
3. A vásárló gépe elvégzi a template előállítását és elküldi a banknak. Ezt a banktól kapott algoritmussal generálja.
4. A bank hajtja végre az összehasonlítást a kapott és a tárolt template között.

Azért, hogy ne lehessen egy template-et újra felhasználni, időbélyeggel kell ellátni azt és PGP módszerrel titkosítani a csomagot. Így a csomagot csak a bank fejtheti meg, hiszen nála van a titkosított csomag felbontására alkalmas egyetlen titkos kulcs.



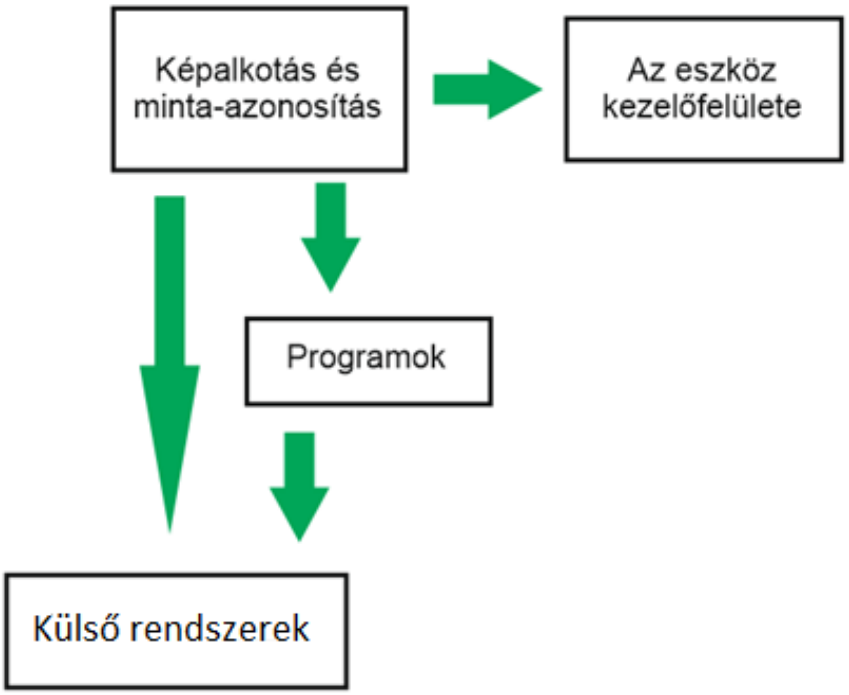
3. ábra: A megvalósítás egyszerűsített elvi vázlata

A fejezetben összefoglaltam, hogy az e-kereskedelemben alkalmazott informatikai megoldások milyen gyakori hiányosságokkal rendelkeznek. A biztonság növeléséhez fel kell deríteni a sérülékenységeket és meg kell szüntetni őket. Ez összetett feladat, a fejezetben kitértem azon fontos elemekre, amelyek vizsgálata feltétlenül szükséges.

2 A BIOMETRIKUS AZONOSÍTÁS MÓDSZEREI, AZ EGYES MÓDSZEREK ERŐS ÉS GYENGE PONTJAI

A vizsgálatokat 3 szintre bontottam annak megfelelően, hogy hol jelentkeznek a sérülékenységek, nevezetesen (4. ábra):

1. Képalkotás és minta-azonosítás.
2. Kommunikáció a programokkal.
3. Kommunikáció a külső rendszerekkel.

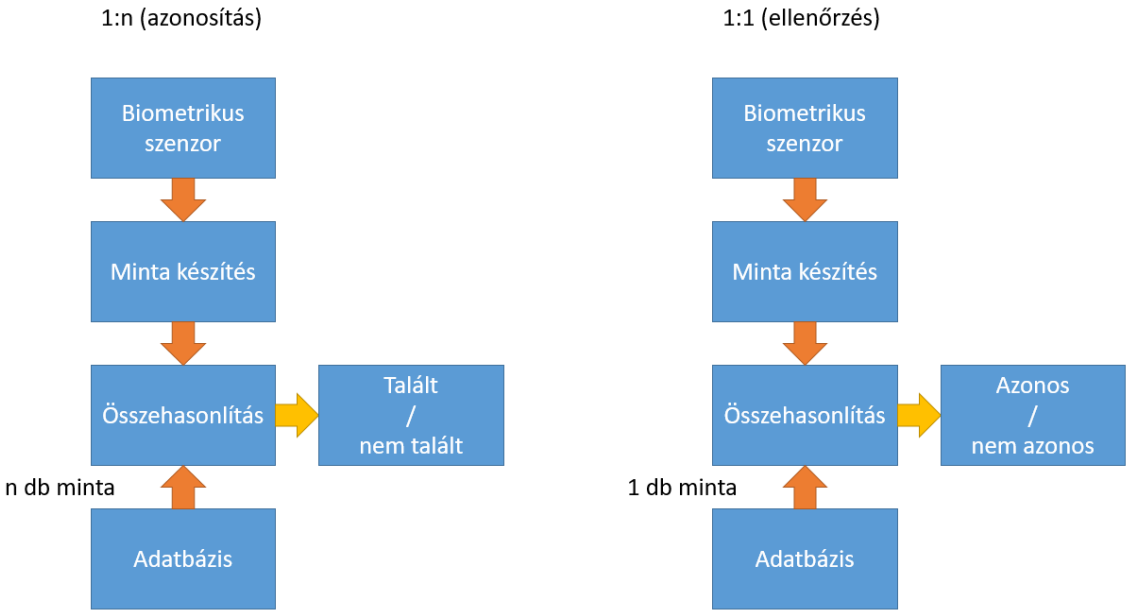


4. ábra: A sérülékenységi vizsgálatok három szintje

A fejezet arra fókuszál, hogy kimutassa: az egyes technológiák miként felelnek meg az e-kereskedelemben történő alkalmazás feltételeinek.

Biometrikus azonosítás esetén a felhasználók először regisztrálják magukat, pontosabban a biometrikus mintájukat egy adatbázisban. Az azonosítás során azt vizsgálják, hogy az aktuálisan mintát adó személy biometrikus mintája szerepel-e az adatbázisban, és ha igen, akkor melyik az. Ezt nevezzük 1:n-hez típusú azonosításnak. A másik lehetőség, amikor az azonosítást végző személy biometrikus mintája nem a teljes adatbázissal,

hanem csak egyetlen mintával kerül összehasonlításra. Ez utóbbi az 1:1-hez típusú összevetés, vagyis ellenőrzés. Mindezeket az 5. ábra szemlélteti. [23, pp. 15-20.] [24, pp. 172-190.]



5. ábra: 1:n (azonosítás) és 1:1 (ellenőrzés) típusú minta-összehasonlítások

A biometrikus azonosítás az emberi test és viselkedés egyedi jellemzőinek felismerésén alapul. Ennek megfelelően a következő, leggyakrabban használatos módszerekről beszélhetünk: arc, DNS, ujjnyomat, írisz, retina, kéz, ujjak, fül alakja, az arc valamint a kéz hőképe, a kéz erezete, a járás, az aláírás, egy gomb megnyomásának a módja, a hang, szag, stb. Ezek kombinációját is alkalmazzák. Hátránya, hogy az egyszerűbb megoldások könnyen megtéveszthetők, a magas igényeket kielégítő hardver-szoftver termékek nagyon drágák, felléphetnek higiéniai, illetve adatvédelmi problémák is.

Minden biometrikus azonosító rendszer lényegében egy mintaillesztő algoritmuson alapszik, amely a választott biometrikus jegyről készített korábbi felvételek (sablon), illetve az azonosítási eljárás során vett minta egyezősége alapján engedélyezi a hozzáférést vagy tagadja meg azt. A biometrikus jegyekről készített felvételek (sablonok és minták) a jogi szabályozás szerint személyes szenzitív adatoknak tekintendők. Ezek a jegyek

magát a felhasználó személyét azonosítják, így megfelelnek az Adatvédelmi Törvényben rögzített személyes adat definíciójának, tehát a biometrián alapuló azonosító rendszer esetén szükséges a tárolt sablonok és az azonosítási folyamat során a felhasználótól vett minták megfelelően biztonságos kezelése. [24, pp. 172-190.]

Biometrikus minta (template) elektronikusan tárolt változata jellemzően valamilyen vektormező, amely egy adott személyre jellemző biometrikus minta digitálisan leképzett képe. Lehet titkosított, vagy titkosítás nélküli. Általában nem állítható vissza belőle az eredeti minta. 1:1 típusú ellenőrzéshez a korábban létrejött TEM fájlkiterjesztést alkalmazzák gyakrabban, míg az 1:n-típusú azonosításhoz a később megjelent BUR-t.

A biometrikus azonosítási folyamatnak egy, az alapműködésbe automatikusan kódolt, szigorúan maximált hibahatár tűrést szükséges tartalmaznia. Tehát minden biometrikus azonosítás egy előre megadott hibaszintet tolerál. Ennek alapvető oka, hogy a szenzor szinte sohasem pontosan ugyanazt a mintát generálja.

A biometrikus rendszereket jellemzően három fő területen alkalmazzák, ezek a következők:

1. Kormányzati célokra, mint személyazonosító igazolványok, útlevelek, stb.
2. Kriminalisztikai felhasználás, elkövetők azonosítása, bűnügyek felderítése, eltűnt személyek felkutatása, stb. [25]
3. Egyéb felhasználás banki szolgáltatásoknál, okostelefonok, távoktatás, kórházi ellátás, stb.

A biometrikus technológiákat a következőképpen lehet csoportosítani: [26, pp. 73-77]

- Fizikai
    - Aktív (akaratlagos felhasználási együttműködést igényel)
        - DNS
        - Retina
        - Írisz
        - Érhálózat
    - Passzív (nem igényel együttműködést a felhasználótól)
        - Arckép
        - Arc geometria

        - Fül geometria
- Viselkedési
    - Aktív
        - Hang
        - Gépelés dinamika
        - Aláírás
    - Passzív
        - Járás

A fenti felsorolásban a passzív módszerek tehát nem feltétlenül igénylik a felhasználó együttműködését, ezért például a személy tudta nélkül is azonosíthatóak az egyének. Az aktív esetekben a felhasználó erős együttműködésére van szükség, tehát a felhasználó viselkedhet akár úgy is, hogy sikertelen legyen az azonosítás. [26, pp. 73-77]

A következő biometrikus technológiák azonnal kizárhatók az e-kereskedelemben történő alkalmazásból: [26, pp. 73-77]

- A járás felismerés, mert nagy teret igényel és a megbízhatósága is vitatott.
- A fülgeometria, fülhőtérkép, archőtérkép, mert kevésbé tesztelt, nem kiforrott technológia, jelenleg nem képes stabilan megbízható eredményt produkálni.
- Az aláírás felismerést jelenleg nem használják azonosításra, csak hitelesítésre, ezért nem szükséges részletesebben vizsgálni a technológiát.

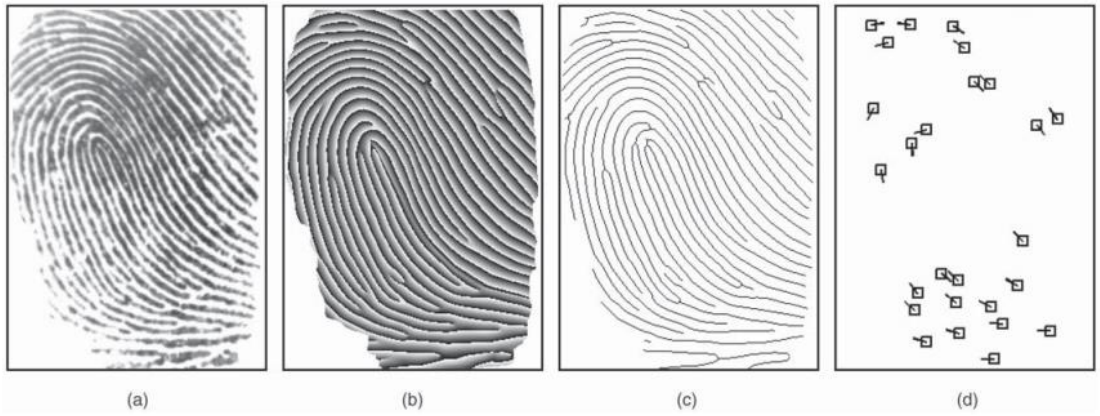
A továbbiakban a feladatra alkalmas azonosítási módszerek jellemzőit vizsgálja az értekezés.

2.1.1 Ujjnyomat

Definíció szerint megkülönböztetünk ujjnyomatot, amely egy sík felületre természetes módon helyezett ujj ott maradó mintázata, valamint ujjlenyomatot, amely az ujj körbe forgatásával létrehozott mintázat. Az elektronikus azonosításhoz jellemzően az ujjnyomatot alkalmazzuk. [27]

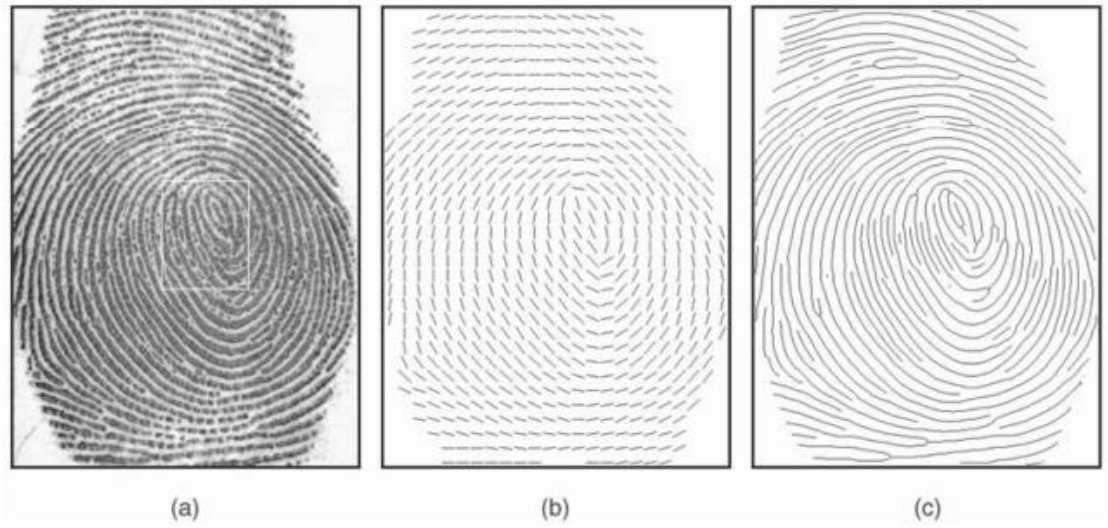
Jelenleg a legelterjedtebb azonosítási forma és egyben a legrégebbi is, hiszen számítógép segítségével több, mint 25 éve hasonlítanak össze ujjnyomatokat. Az ujjnyomat az ujj felületén található völgyek és fodorszálak mintázata. Ezek azonosításhoz használt

pontjai a minutiák, amelyek generálását a 6. ábra mutat be. Az ábra (a) képe az eredeti, szenzoron képződő képét mutatja be, a (b) ábra az előző szoftveresen javított változata, a (c) a fodorszálak elhelyezkedése és a (d) jelű a hozzá tartozó minutiákat mutatja.



6. ábra: Minutiák generálása az ujjnyomat esetében a (d) jelű képen [28, pp. 209-223.]

Az ujjnyomat azonosításhoz használnak még irányvektor mátrixot is, ez a 7. ábra (b) képénél látható, az (a) kép az eredeti kép, még a (c) képen a fodorszálak elhelyezkedését láthatjuk.



7. ábra: Iránymátrix az ujjnyomat esetében a (b) jelű képen [28, pp. 209-223.]

Az azonosítás a legtöbb esetben a minutiák egymáshoz viszonyított helyzete alapján történik. Az emberi kéz ujjnyomatai általában már a magzat hét hónapos korában kialakulnak és nem változnak az élet folyamán (természetesen leszámítva az ujjat érintő baleseteket). [29] [30]

Az ujjnyomat olvasási technikákat a következő módon csoportosíthatjuk, létezik: optikai, kapacitív, rádiófrekvenciás, ultrahangos és nyomásérzékelés elvén alapuló.

Az optikai elven működő ujjnyomat olvasók a feldolgozandó képet egy optikai rendszerrel egy képbontó eszköz felületére képezik le, amely elektromos jellé alakítja azt. A felhasznált optikai megoldás alapján további csoportosítás adható meg: totálreflexiós elvű, holografikus, diffrakciós és direkt chip-szenzor. Részleteiben:

- A totálreflexiós elvű ujjnyomat olvasók esetében a leképezendő minta egy prizma felületén helyezkedik el, amit annak másik oldalán világítanak meg. Az ellentétes oldalon helyezkedik el a képbontó eszköz, aminek a felszínére képződik le az ujjnyomatról a prizma által visszavert kép.
- A holografikus elvű ujjnyomat olvasók esetében - a totálreflexiós elvhez hasonlóan - is alkalmaznak prizmát, azonban itt az ujjat nem a prizma felszínén, hanem egyik oldalára helyezik. A módszer előnye a jó képminőség, torzításmentesség és a kitűnő kontraszt, hátránya az optikai úthosszak miatti nagyobb méretű olvasó.
- A diffrakciós elvű eszköz működése a totálreflexiós elvű olvasókéhoz hasonló, azonban a diffrakciós eszközökben az olvasó méretének csökkentése érdekében nem prizmát használnak, hanem speciális felületű üveglemezt. A lencse felületi kialakítása elemi prizmák sokaságával egyenértékű optikai hatást nyújt.
- Direkt chip-szenzor esetén a szenzor felületére helyezett mintát közvetlenül képezi le a képbontó eszköz felületére. Nem alkalmaz összetett optikai rendszert, hanem az ujjbegy képe elemi üvegszálakon keresztül közvetlenül jut a szenzorhoz. A kép torzításmentes.

Kapacitív elvű ujjnyomat olvasók működése arra épül, hogy a szenzor felületére helyezett ujj eltérő kapacitásképet mutat az ujj felületén lévő völgyek és fodorszálak függvényében. Ezt detektálják és elektromos jellé alakítva továbbítják. Ezzel a technológiával kisméretű és közepes minőségű szenzorok készíthetők. A kapacitív jellegből adódóan módszer érzékeny az elektrosztatikus kisülésekre.

A rádiófrekvenciás elven alapuló ujjnyomat olvasók esetében a szenzor keretén keresztül rádiófrekvenciás jelet juttatnak az ujjra, amely adóantennaként visszasugározza azt a vevőantennaként szolgáló szenzor-felületre. A szenzor által alkotott kép nemcsak az ujj felületét képezi le, hanem mélységi képalkotást is szolgáltat. Ennek köszönhetően a képalkotás sérült, nagyon száraz vagy szennyezett ujjak esetén is sikeres lehet.

Ultrahangos elven alapuló ujjnyomat olvasók esetén a szenzor ultrahangot (frekvenciája 20 kHz körüli) bocsát a ráhelyezett ujjra és a visszaverődő hullámokból képet alkot. A leképezés mélységi, tehát a technológia jól alkalmazható szennyezett ujjak esetén is. Jó minőségű képalkotást tesz lehetővé.

A nyomásérzékelés elvén alapuló ujjnyomat olvasók esetén a szenzor felülete alatt érzékeny piezo-elektromos nyomásérzékelő mátrix található, amely detektálja az ujjfelület egyenetlenségeit és ezekből képet alkot. Az így készült kép közepes minőségű, viszont a felületi szennyeződések nem zavarják a képalkotást. [29] [24, pp. 172-190.] [31, p. 80] [32, pp. 23-28]

Az ujjnyomat olvasási technikákat csoportosíthatjuk az alkalmazott képvétel (leképezés) módja szerint is. Ezen szempont szerint megkülönböztethetők teljes ujjnyomat képet készítő-, vonal-, és rolled szkenner típusok.

- A teljes képet készítő szkenner egy időben mindig az ujj teljes sík felületéről (vagy annak nagyobb részéről) készít képet.
- A vonal szkenner egy időben mindig az ujj kis részéről (vonalnyi „felületről") alkot képet, amelyet a teljes ujj lehúzása után a képalkotó szoftver szerekszt össze teljes képpé.
- A rolled szkenner teljes (körbe forgatott) képet készít (ujjlenyomat), amelyeket elsősorban bűnügyi, idegenrendészeti nyilvántartási célokra használnak fel. [33, pp. 44-51.] [31]

Jelenleg az optikai, azon belül a prizmás technológia a legelterjedtebb.

A legkorszerűbbnek a multispektrális képalkotó technológia mondható, amely a korábbi technológiák hiányosságait jó hatásfokkal küszöböli ki. Ezek a hiányosságok például a száraz vagy nedves ujj, az ujj erős nyomása miatt bekövetkező torzítás és az élőminta felismerése.

A multispektrális optikával rendelkező szenzort alkalmazó ujjnyomat azonosító eszköz akkor is képes használható képet készíteni, amikor más ujjnyomat azonosítók erre alkalmatlanok. Ezt úgy éri el, hogy multispektrális megvilágítást alkalmaz, amely különböző hullámhosszúságú fotonokból áll. Ezáltal a szenzor „látja" a bőr felületét és az alatta lévő réteget is. Ennek a megnövelt adatmennyiségnek köszönhető az, hogy azonosítás szempontjából sikeresebb tud lenni más ujjnyomat olvasó szenzorokhoz képest. Az ujj bőrfelszín alatti rétegét látva lehetséges az, hogy egy „szennyezett" ujj esetén is értékelhető képet kapjon az olvasó. Az élőminta felismerés szoftveresen állítható. Viszont amikor ezt a funkciót bekapcsoljuk, akkor az eszköz a túl nedves vagy túl száraz ujjat már nem képes a megfelelő minőségben beolvasni.

A szenzor valóban képes arra, hogy igen szélsőséges környezetben is működjön: az ujjnyomatot akkor is sikeresen azonosítja, ha a szenzor párás, poros feltételek között működik, vagy éppen vékony gumikesztyűt visel a felhasználó. A két szolgáltatás közül (extrém környezet és élőminta felismerés) azonban mindig csak egy érhető el a rendszer adminisztrátora számára. [34]

Az előzőekben leírtak leglényegesebb elemeit fogalja össze röviden a 2. táblázat.

Módszer	**Jellegzetesség**	**Megjegyzés**
Optikai totálreflexiós	prizma	általánosan elterjedt
Optikai holografikus	prizma	jó képminőség
Optikai diffrakciós	üveglemez	a totálreflexiósnál kisebb méret
Optikai Direkt chip-szenzor	üvegszálak	torzításmentes
Kapacitív	kis méret	okostelefonokban alkalmazott
Rádió frekvenciás	mélységi képalkotás	száraz és szennyezett ujj esetén is alkalmazható
Ultrahangos	mélységi képalkotás	jó képminőség
Nyomásérzékelés	piezo-elektromos érzékelők	független az ujj szennyeződésétől

2. táblázat: az ujjnyomatot azonosító technikák összehasonlítása

2.1.2 Írisz alapú azonosítás

Az írisz alapú azonosítás során a szem szivárványhártya-mintázata alapján történik az azonosítás. A felvételt egy infratartományban működő CCD kamera készíti el. A rendszer egyik nagy előnye, hogy az azonosítási folyamat során nem kell fizikai kontaktusba kerülnie az azonosító eszköznek és a személynek.

Az írisz azonosítás történetiségét tekintve azt a 19. századra vezetjük vissza, amikor Alphonse Bertillon a test mérésével foglalkozott annak érdekében, hogy segítse a rendőrség munkáját a személyek azonosításában.

Az automatizált írisz azonosító elmélete 1936-tól létezik és a szemész Frank Burch nevéhez köthető. Aran Safir és Leonard Flom szabadalmaztatták Bruch elméletét és felkérték a Harvard matematikusát, John Daugman-t, hogy dolgozzon ki egy algoritmust írisz azonosításra. Az algoritmus 1994-ben került szabadalmaztatásra. Dr. John Daugman 1998-ban 400 különböző tulajdonságot talált a szem szivárvány-hártyáján, amelyek mindegyike alkalmas azonosításra. Ezekből háromdimenziós kontúr-térkép készül. Ezt digitalizálva 2048 számjegyű kódot kapunk. Ezt hasonlítják össze az adatbázisban tároltakkal (75%-os egyezésnél $1:10^{12}$ a hiba lehetősége, a módszer tehát nagy megbízhatóságú). A Daugman módszerrel tárolt minta kis tárigényű (akár 256 Byte is elég). A passzív leolvasó drága, az aktív viszont a felhasználók között nem népszerű (a „gép” utasításokat ad). [24, pp. 172-190.] [35]

Az írisz átlagos átmérője 12 mm, míg a pupilla mérete az írisz átmérőjének 10%-tól annak a 80%-áig változhat. Színét elsősorban az írisz számos rétege közül a stromal rétegben található pigment sejtek sűrűsége határozza meg. Az írisz kialakulása az embrionális élet harmadik hónapjában kezdődik meg. A felszínén található egyedi mintázat az első évben alakul ki, míg a stroma pigmentációja az első néhány évre tehető. A mintázatok kialakulása véletlenszerű és nem köthető semmilyen genetikus faktorhoz. Az egyetlen gének által meghatározott jellemzője a pigmentáció, ami a színt határozza meg. Így még egyazon személy két írisze is teljesen különböző mintázatú lehet, viszont kialakulása után változatlan marad az egész életen át. Egyedisége és stabilitása folytán a mintázat ideális biometrikus jellemző. [36]

A felvételt az íriszről az esetek döntő többségében infratartományban készítik, mivel a hagyományos fénnyel megvilágított sötét színezetű szem képe nem mutatja az azonosításhoz szükséges részletességet. Az infrafény alkalmazása még a sötét és fekete színű írisz esetén is felfedi az írisz mintázatát. Az élőminta felismerése a pupillareflexek detektálásával történik.

Az azonosítás folyamata 4 fő lépésből áll:

1. Felvételkészítés (Acquisition)
2. Szegmentáció (Image pre-processing)
3. Normalizáció (Feature extraction)
4. Kódolás-összehasonlítás (Encoding/matching modules)

Részleteiben:

A *felvétel készítése* általában infra tartományban történik, ezért a képet monokróm szürkeárnyalatos képként kezeljük. Akkor a leghatékonyabb az azonosítás, ha a felvétel készítésekor az íriszből a legtöbb felület látható (tehát legyen a szem nagyra nyitva, a szemhéj lehetőleg ne takarjon le belőle részeket).

Ezt követi a *szegmentáció*. Ez tulajdonképpen az írisz elkülönítése digitális képen. Az írisz területét két kvázi koncentrikus kör közötti körgyűrű írja le, melyeket az írisz és a szemfehérje, valamit az írisz és a pupilla határai definiálnak. Színes kép alkalmazása esetén a sötét szemű egyéneknél az írisz és a pupilla közötti kontraszt túl kicsi lesz, ami sikertelenné teheti a szegmentációt. Az azonosítási eljárást nagyban befolyásolja a szegmentáció pontossága, mivel téves adatok alapján generált kód biztosan rossz azonosítási eredményhez vezet.

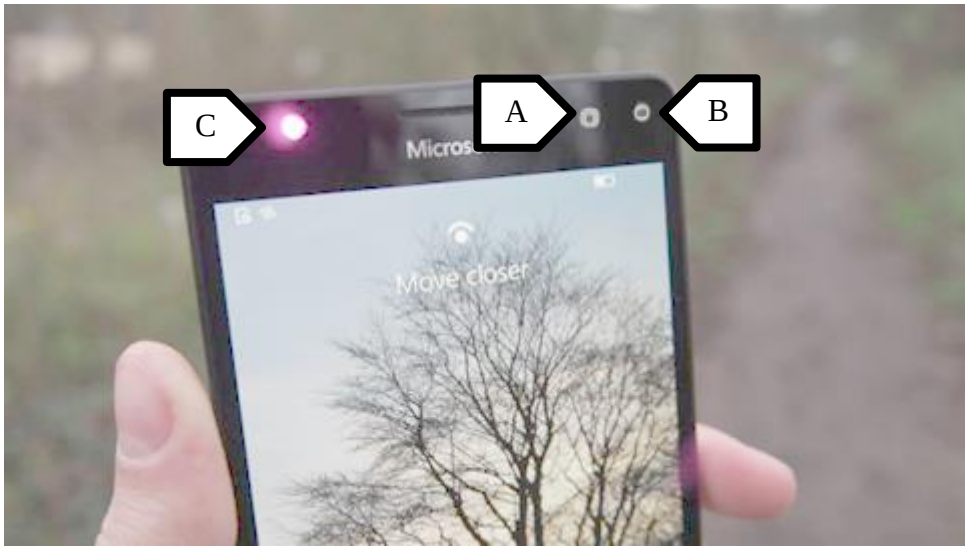
A sorban a harmadik a *normalizáció,* amikor is a szegmentáció eredményei alapján polárkoordinátás alakra (téglalap) transzformálja az írisz eredeti mintázatát. Ezzel az eljárással kiküszöbölhető a pupilla megvilágítás-függő összehúzódásából adódó különbség. A vízszintes irányú elfordulás kompenzálására a kódok összehasonlítása során kerül sor.

Végül a *kódolás* következik. A pontos személyazonosítás érdekében az íriszmintázatban tárolt legjellemzőbb információt kell felhasználni. Ennek a metrikának két jól

elkülöníthető értéket kell adnia két azonos íriszből nyert kód (intra-class) és két különböző íriszből nyert kód (inter-class) összehasonlítása esetén. A Gabor filter optimális közös lokalizációt ad mind térben, mind frekvencia-spektrumban. Ez annak köszönhető, hogy a Gabor filter nem más, mint egy sinus/cosinus görbe és egy Gauss-görbe kompozíciója. A sinus tökéletesen lokalizált a frekvenciaspektrumban, viszont egyáltalán nem lokalizált térben. Térbeli lokalizációt nyerhetünk viszont, ha moduláljuk egy Gauss-görbével, ellenben ez a spektrumbeli lokalizáció kárára válik. Egy jel dekompozícióját Gauss-modulált cosinus (valós rész), valamint Gauss-modulált sinus (képzetes rész) segítségével végezhetjük el. [36]

Az azonosítás hibáinak leggyakoribb okait jómagam is többször vizsgáltam. A főbb problémák, hogy az írisz mintázatát takarja a szemhéj, valamint az írisz megvilágítását biztosító fényforrás tükröződést okoz azon. Szemüveg viselése esetén a lencsén megjelenő reflexiók nehezítik meg a felismerést. [29] [32, pp. 71-90]

Már léteznek kísérleti összeállítások arra vonatkozóan, hogy az írisz azonosítás okostelefonokon is elérhető legyen. Ezek jelen vannak már a kereskedelmi forgalomban, de működésük még nem megbízható.



8. ábra: Mobil telefonba épített írisz azonosító [37]

A 8-as ábrán látható Microsoft Lumia 950 XL. Az előlapi kamera (A) mellett helyezkedik el a kisebb látószögű beépített írisz azonosító kamera (B). A felvétel készítését infra tartományú LED megvilágítás (C) segíti. Az eszköz képes az íriszt használni a lezárt képernyő feloldására, bár a gyártó megjegyezte, hogy még béta verzióban működik a funkció, és nem teljesen tökéletes, fejlesztése jelenleg is folyamatban van. [38]

9. ábra: Laptophoz csatlakoztatható írisz azonosító eszköz

A 9. ábrán az IrisKey látható, amely laptophoz vagy asztali számítógéphez csatlakoztatható. Egy tükör segít a szemre irányítani a kis látószögű kamerát (az ábrán nyíllal megjelölve). Az ehhez hasonló azonosítók nem rendelkeznek olyan szoftverrel, amely közvetlenül alkalmassá tenné azokat az e-kereskedelemben történő alkalmazásra, azonban általában olyan a fejlesztői környezet, hogy ahhoz célprogram írható.

2.1.3 Arc-felismerés

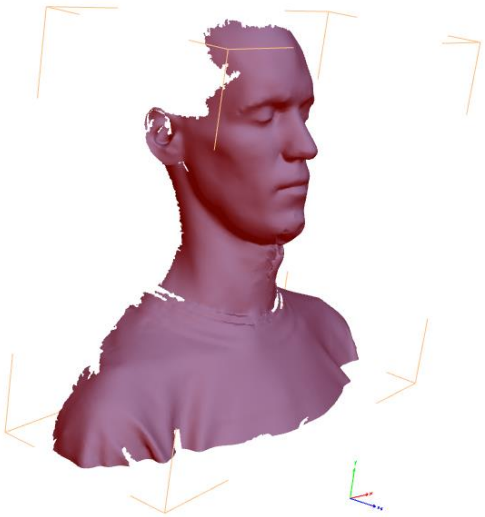
A biometrikus eszközök fejlesztői az arcfelismerés hatékonyságának javítására szintén jelentős energiákat mozgósítanak. A tapasztalataim azt mutatják, hogy még mindig kihívás az aktuálisan felvett arcképet összehasonlítani az adatbázisban szereplővel. Amennyiben a rendszer nagy felhasználószámmal dolgozik, akkor ezek a zavaró hatások még erősebben rontják az azonosítás sikerességét.

A leggyakoribb zavaró hatások a 2D arcazonosításkor:

- a megvilágítás,
- a kamera nézőpontja,

- az arc elfordulása,
- az arckifejezés,
- az öregedés,
- a smink,
- a szemüveg.

A felsoroltak következménye, hogy az arcról készült képek összehasonlításával kevésbé megbízható, mint például az írisz azonosítás.

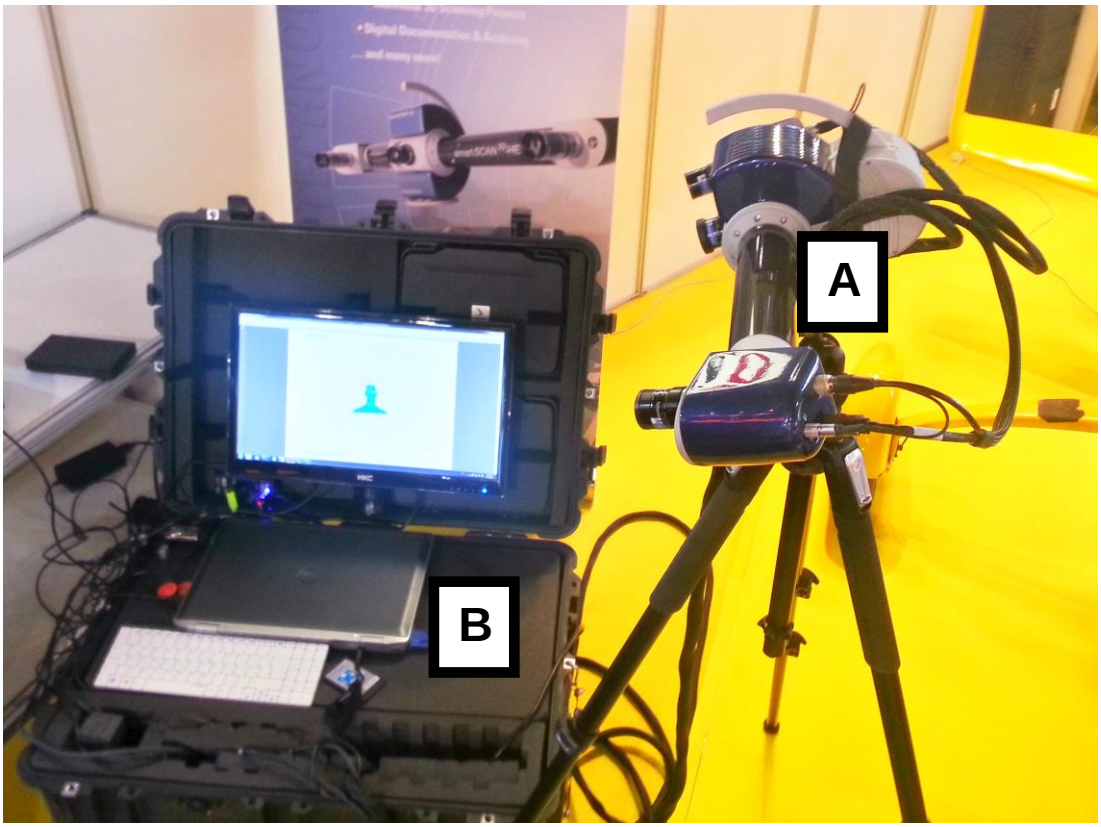


10. ábra: A 3D arcazonosítás gyakorlati megvalósulása

A 3D arcfelismerés a 2D zavaró hatásait jó hatásfokkal zárja ki, azonban a 3D csak közelről alkalmazható és általában a felhasználó jóval nagyobb fokú együttműködését igényli. Ez azt jelent, hogy az azonosított személynek fél, egy méterre kell a kamerától állnia. Ennél nagyobb távolság esetén már kérdőjeles a 3D arcazonosítás sikerességére. [29] [32, pp. 43-70]

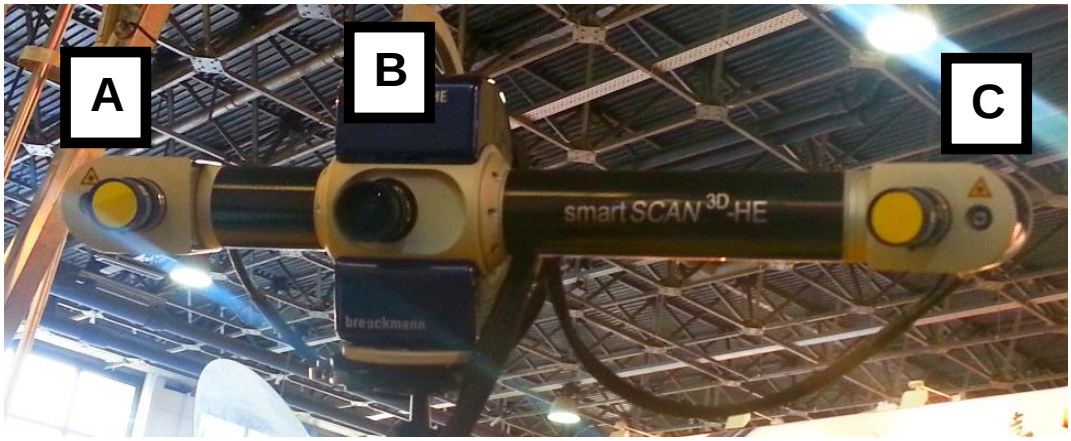
A 10. ábrán jól látható egy kép arról a 3D adathalmazról, amellyel az ilyen azonosítók dolgoznak. Megfigyelhető, hogy ebben az esetben az egyes pontok szín információi nincsenek eltárolva. Ezért tehát a 3D arcazonosítás nem veszi figyelembe a bőrön lévő foltokat, kisebb sérüléseket vagy a sminket. Ez a technika hatékonyságát nagyban javítja.

A módszert többen különbözőképpen valósították meg. A smartSCAN 3D HE típusú eszköz (11. ábra) technológiája azt is lehetővé teszi, hogy akár mikrométeres nagyságrendű felbontással készítsen képet az arcról. Lényeges viszont, hogy ez az azonosításhoz szükségtelelen felbontású, az így előállított nagyszámú térbeli pont több órára növelni meg az azonosítási időt.

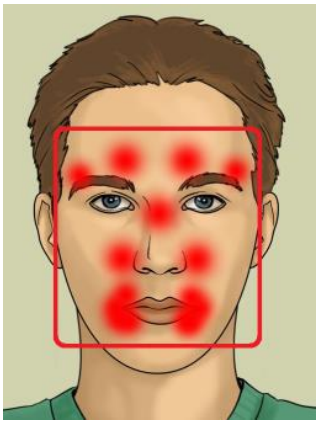


11. ábra: A-val jelölve: 3D képalkotó készülék, mellyel a korábban bemutatott 3D arcfelvétel készült, B-vel jelölve: a feldolgozást végző mobil számítógép

A lézerfényt alkalmazó eszköz szemből készített képe a 12. ábrán látható. Jól megfigyelhető, hogy a lézeres kivetítő egységek (A-val és B-vel jelölve) egymástól távol helyezkednek el. A kamera képén az arcon megjelenő lézer helyzetéből meghatározható az adott pont távolsága, így a rendszer képes összeállítani az egyes képpontok pontos helyzetét a térben.



12. ábra: A smartSCAN 3D HE szemből, A-val és C-vel jelölve a lézeres kivetítő egységek, B-vel a központi kamera



13. ábra: Az arcfelismerő rendszerek által vizsgált jellegzetes területek

A 13. ábrán látható piros keret jelöli azt a területet, amelyen belül az arcazonosító rendszerek dolgoznak. Az ábrán a piros területek jelzik azokat a jellegzetes területeket, amelyeket az arcazonosítók figyelembe vesznek.

A legtöbb beléptető rendszerben alkalmazott arcazonosító eszköz az infra tartományban működik. A háttér feketének látszik, ami megkönnyíti az arc detektálását. A megvilágítás mindig konstans, hiszen ugyanonnan, vagyis szemből érkezik. Ez javítja a felismerést.

Az algoritmust tekintve létezik geometriai alapú, sablonillesztő, eigenface-módszerrel dolgozó és neurális hálós modell is.

Az arc-thermogram infrakamerával készül, az arc hőtérképét mutatja. A kép mintaazonosító algoritmust használva ellenőrzi a relatív hőmérsékletkülönbségeket az arcon, amelyek függetlenek a kortól, egészségi állapottól és a test hőmérsékletétől is. 19.000 adatpont felvételével képes megkülönböztetni akár egypetéjű ikreket - mindezt, akár sötétben is. Az azonosítás még az arc eltakarása esetén is elvégezhető. Egy ilyen képet mutat a 14.ábra, amelyen megfigyelhetjük a melegebb arcbőrt (B) és a hidegebb hajat (A), ruházatot (C) és hátteret (D). [24, pp. 172-190.]

14. ábra: Hordozható hőkamerával készült arc-thermogram

2.1.4 Tenyérerezet alapú azonosítás

Az egyik legújabban elterjedt biometrikus technológia. A korábbi megoldások a kézháton elhelyezkedő erek mintázatát azonosították. A jelenlegi eszközök a tenyér (ujj) érhálózatának mintázatát használják.

Az erezetről a felvétel általában az emberi szem számára nem látható 740 és 1000 nm hullámhossz közötti infravörös tartományban készül, mivel a deoxidált hemoglobin elnyeli ezt az infravörös sugárzást, így az erek sötétebbnek „látszanak”. Ezen vonalak alapján történik meg az azonosítás.

15. ábra: Kézerezet azonosítóval ellátott számítógép egér

Az érhálózat mintázata egyedi minden embernél, még az egypetéjű ikrek esetében is. További előnye, hogy a módszer belső biológiai jellemzőt használ azonosításra (az ereket), amelyek kevésbé sérülékenyek mint más biometrikus jellemzők (például ujjnyomat, hang). A hamis minta előállítása is jóval összetettebb feladat, ugyanis az erek teljes mintázata az ember szem számára nem látható. Tapasztalataim

szerint nagy hatásfokkal zárja ki a megvilágítottság, hőmérséklet és a napfény zavaró jeleit is. [29] [32, pp. 253-270]

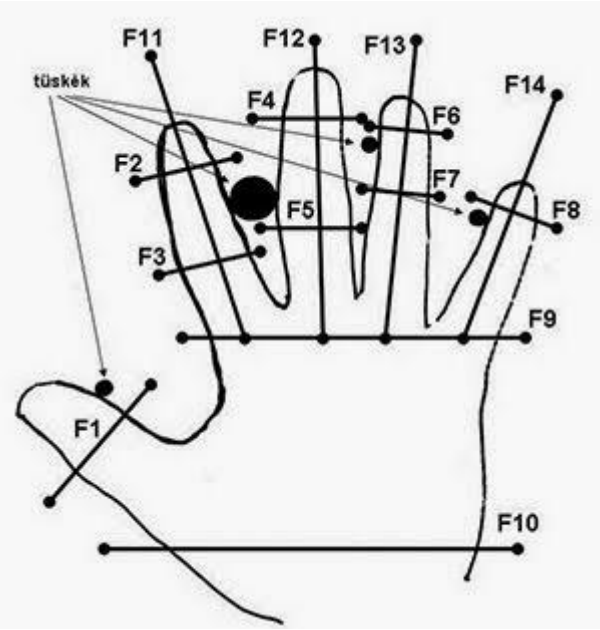
A 15. ábra egy kézerezet azonosítóval ellátott számítógép-egeret ábrázol, amely a jövőben alkalmas lehet arra, hogy személyi számítógépekkel összekapcsolva akár az e-kereskedelem biztonságát növelje. Az azonosító felület az ábrán A-val jelölve.

2.1.5 Kézgeometria

Gyors, pontos, könnyen kezelhető módszer. Nagy felhasználói bázis esetén is alkalmazható, vagy olyan felhasználóknál, akik a rendszert ritkán használják és ennél fogva kevésbé gyakorlottak. A felismerés pontossága igen magas, a megbízhatóság még tovább is növelhető más biometrikus jegyekkel (pl. ujjnyomat) való kombinálással. [24, pp. 172-190.]

A módszer jellemzője, hogy a kézről infra tartományban felvételt készítenek. Az így kapott képről megállapítható a kéz elemeinek geometriája. Egyes eszközök esetén különböző szögből is készítenek képeket, így a kézről kvázi 3D képet lehet kapni, amely növeli az azonosítás hatékonyságát. A torzítás minimalizálása érdekében a kamerát minimum fél méterre érdemes elhelyezni a kéztől. Ezt úgy érhető el, hogy tükrös rendszert építenek a készülékbe – sajnálatos módon még így is relatív nagyméretű marad az olvasó.

Éppen a méretei miatt kevésbé elterjedt technológia. Előnye, hogy a kéz tisztaságának mértéke nincs hatással az azonosításra. A módszer az ujjak hosszát, szélességét, a területet, az ízületeknél lévő szögeket, valamint ezek arányait vizsgálja. Ennek következtében az azonosítást megnehezíti, vagy akár lehetetlenné is teszik a kéz deformációs megbetegedései, elváltozásai, a bandázs, a kesztyű vagy nagyobb gyűrű viselése. [29] [32, pp. 91-107.]



16. ábra: A kéz geometriai jellemzői [37]

A kézgeometria azonosító eszköz általában 30 körüli mérési pontot rögzít. Ez tartalmazza a kézfej hosszát, szélességét és felületét, az ujjpercek hosszúságát, alakját. Erre mutat példát a 16. ábra. Az olvasási és kiértékelési folyamat összesen kevesebb, mint egy másodpercet vesz igénybe. A nagyszámú felhasználóra tekintettel a kézgeometria olvasók antibakteriális réteggel kerültek kialakításra, mely kellően higiénikus felületet és könnyű, hatékony tisztíthatóságot biztosít. [39, pp. 90-95.]

2.1.6 Retina

A retina anatómiailag a szemfenék fényérzékeny felülete. A szem optikai rendszere a retinára vetíti a tárgyakat, amelyek a retinán alkotnak éles képet. A retina gyakorlatilag tehát a szemfenéken elhelyezkedő ideghártya. A retinát vizsgálva, azon jól megfigyelhető a szemfenék érhálózata, amely egyedenként eltérő mintázatot mutat. Egyedisége az ujjnyomatnál nagyságrendekkel nagyobb, ezért biometrikus azonosításra kiválóan alkalmazható.

A szem sajátosságai alapján történő azonosítás területén 1935 óta folynak intenzív kutatások. Ebben az évben jelent meg egy cikk a New York State Journal of Medicine folyóiratban [40, pp. 901-906], amely először vetette fel, hogy a vérerek mintázata a retinahártyán felhasználható lenne egyének azonosítására. Kezdetét vette az a jelentős kutatási és fejlesztési munka, amelynek célja mind az írisz, mind pedig a retina mintázatok feltérképezése, illetve ezek egyediségének vizsgálata.

Az azonosítás során általában infravörös spektrumú fénnyel világítják meg a retinát, amelyről egy, közvetlenül a szemlencse előtt elhelyezkedő kamera készít felvételt. Az így készített képen jól kirajzolódik a szemfenék érhálózata (a retinán található vérerek

intenzívebben nyelik el az infravörös fényt, mint a környező szövetek). A retina-erezetet formázó fényt ezután visszatükrözik egy videokamerára, amely rögzíti a mintát.

Biometrikus azonosítók esetén ritkán használt technológia, mert túl nagyméretű az eszköz és használata kényelmetlen. Ezen technológiával nagy pontossággal meghatározható az egyén személyazonossága. Felléphetnek bizonyos fertőzés-veszélyek, továbbá egyes betegségek, pl. cukorbetegség esetén az érhálózat sérülhet. Tehát maga a biometrikus jellemző nem tökéletesen stabil. [29] [24, pp. 172-190.]

2.1.7 Hang

A hang az egyik legkönnyebben elérhető és a legolcsóbban vizsgálható biometrikus jellemző. Egyre kevésbé használt technológia, szerepét más biometrikus módszerek veszik át. Létezik szövegfüggő és szövegfüggetlen beszéd-felismerés. Az ember hangja gyakran több okból kifolyólag megváltozhat - ez okozza a technológia pontatlanságát.

A módszer hiányossága abból adódik, hogy képtelen kezelni azt, hogy a hangképzés igen komplex folyamat, a hangszínt nem csak az anatómiai adottságok, de az érzelmi állapot, a beszélt nyelv sajátosságai, az aktuális hangulat, valamint a betegségek is befolyásolják. Ezért még ma is kihívás egy stabilan, nagy hatásfokkal működő beszéd-felismerő rendszert létrehozni. [29] [32, pp. 151-170.]

A hagyományos technikai megoldást tekintve az azonosítandó személyek egy-egy rövid tárolt hangmintáját (pl. jelszó vagy egy rövidebb mondat) hasonlítják össze az éppen elmondott szöveggel. Ha szabad beszéd alapján történik az azonosítás, akkor az adott személy beszédstílusát jellemző paraméterek alapján végezhető az el. E paraméterek értékeit több különböző hangminta alapján lehet meghatározni. A hangminták összehasonlítására célelektronikák léteznek az időtartományból frekvenciatartományba történő konvertálásra. A hangminták spektruma mellett az egyes rendszerek vizsgálhatják a hangminta egyéb dinamikai jellemzőit, a beszéd sebességét, illetve a hangsúly változását is. Hátránya, hogy légúti betegség esetén nem használható, valamint könnyen hamisítható. [24, pp. 172-190.]

2.1.8 DNS

A DNS a dezoxiribonukleinsav szóból alkotott mozaikszó. Az angol nyelvű szakirodalomban rövidítése DNA vagy teljes nevén deoxyribonucleic acid. Ez az összetett molekula a genetikai információt tárolja magában.

Valójában nem a „DNS”-t, hanem a „DNS mintázatát” azonosítjuk, azonban a Biztonságtudomány tématerületén ez a három betűs elnevezés terjedt el, így a továbbiakban én is így fogom használni. Igaz, hogy az egymással rokoni viszonyban állók DNS-e hasonlóságot mutat, azonban kijelenthető, hogy minden ember DNS-e egyedi.

Az emberi DNS 3 milliárd bázispárjának elrendezése egyedi, a sorrend megállapítása azonosítaná az adott személyt. Az eljárás azonban rendkívül hosszadalmas lenne, s a "nukleotid-térkép" 99 százaléka mindenkinél egyforma. A személyek azonosításához tehát az árulkodó egy százalékot kell megkeresni. [41]

Nagy azonosítási pontosságot tesz lehetővé, azonban lassú és drága technológia. A berendezés mérete is igen nagy, befoglaló mérete nagyságrendileg 500 x 500 x 1000 mm. Ehhez csatlakozik még a nagy számítási kapacitással rendelkező szerver számítógép.

A DNS-minta szinte bárhonnan elérhető, ebben rejlik a hátránya is, hiszen egy nem jelenlévő személy DNS mintáját is lehetséges azonosítani. Ezért fontos kérdés, hogy az azonosítás felügyelt, vagy felügyelet nélküli térben történik-e.

A kezdetekhez képest ma jelentősen csökkent az azonosítási idő és az azonosítás ára is, de ez még mindig nem teszi versenyképessé a módszert a többivel szemben. [29]

2.1.9 Nem biometrikus azonosítási technikák

Alapvetően két azonosítási lehetőség létezik a biometrikus módszeren kívül, az egyik a tudás, a másik pedig a birtok alapú.

Tudás alapú például a PIN-kód vagy a jelszó. Előnye, hogy nem kell fizikailag egy tárgyat a felhasználónak magánál tartania, így nem fordul elő, hogy ellopják tőle vagy elhagyja azt. Hátránya, hogy elfelejthető, így a jogosult személy nem tudja érvényesíteni

jogosultságát. Másnak elmondható a jelszó, így nem jogosult személyek képesek azonosítani magukat jogosultként. A kód el is tulajdonítható, ha például leolvassák mások a tulajdonos figyelmetlenségéből.

A birtok alapú azonosítási módszerek egy fizikai tárgyat azonosítanak, jellemzően RFID tag-et, vonalkódot, mágneskártyát vagy lyukkártyát. Előnye az azonosításhoz az azonosító eszköznek mindenképpen jelen kell lennie. Hátránya, hogy kölcsönadható és eltulajdonítható, a legtöbb esetben másolható is. Jelenleg az RFID a legjobban elterjedt megoldás. A *tag* (RFID transzponder, egy microchip-ből és egy kis antennából áll) rádióhullámok segítségével kommunikál a leolvasást végző egységgel. A kommunikáció a legtöbb RFID tag esetében azt jelenti, hogy a tag információkat képes fogadni, tárolni, feldolgozni, titkosítani és a benne tárolt egyedi azonosítóval együtt továbbítani a vevőnek. [42, pp. 17-25.]

Lehetőség van arra is, hogy a fenti megoldásokat kombináljuk, akár biometrikus azonosítási eljárással, így nagyobb biztonság érhető el gyakran a kényelem és gyorsaság rovására. Az említett azonosító eljárásokat kombinálhatjuk biometrikus azonosítással is, így az azonosítás biztonsága növekszik.

2.1.10 Egyéb technológiák, összefoglalás

A biometrikus azonosító eljárások közül szinte minden egyéb technológiát kizárhatunk, ha figyelembe vesszük az elvárt szempontokat.

Fülgeometria azonosítás esetén kamerával kell felvételt készíteni, a technológia olcsó. Az összehasonlítás alapja a fül strukturális analízise által nyert információk halmaza. A fül „középpontját” kell meghatározni, ami a hallójárat peremének egy pontja, majd adott irányok mentén vizsgálják a fülcimpa jellemző vonalainak és ennek a pontnak a távolságát. Előnye, hogy nagyobb távolságból is elvégezhető az azonosítás. Megbízhatósága nem bizonyított, ezért egyelőre a fül alakját, mint biometrikus azonosító jegyet, folyamatos vizsgálatoknak vetik alá. [24, pp. 172-190.]

A kézírás nem tisztán biometriai alkalmazás (mivel nem testi jellemzők alapján végezzük el az azonosítást). Nem igényel komoly olvasó-berendezést, egy egyszerű digitalizáló táblával a mintafelvétel megoldható. Nem csak a szöveg statikus tulajdonságait, azaz az írásképet, hanem a vonalvezetés dinamizmusát is ellenőrizhetjük és ellenőrizni is

kell (a dinamikát nem lehet másolni). A hatékony azonosításhoz a következőket kell figyelembe venni:

- a betűk alakja, mérete, dőlése, kötése,
- az ékezetek formája, dőlése, a betűhöz viszonyított helyzete, kettős ékezetek írása,
- a tollkezelés (a személy hol emeli fel, és hol nem a tollat),
- az írás lendülete, dinamikája. [24, pp. 172-190.]

A lényeges azonosítási technológiákat összefoglalja a 3. táblázat.

Módszer	**Működési elv**	**Előny**	**Hátrány**	**Megjegyzés**
Ujjnyomat	optikai/egyéb	Egyszerűen használható	Nem mindig alkalmazható	Másolható a minta
Írisz	optikai	Nagy pontosság	Magas ár	A használatot be kell gyakorolni
Arc	optikai	Egyszerűen használható	Nem mindig alkalmazható	Fényviszonyokra érzékeny
Tenyér-erezet	optikai	Nagy pontosság	Magas ár	Nagy eszközméret
Kézgeometria	optikai	Stabil működés	Nagy méret	A kéz szennyeződésire érzéketlen
Retina	optikai	Nagy pontosság	Nagy méret	Lassú, kellemetlen használat
Hang	hang	Alacsony ár	Nem megbízható	Könnyen megtéveszthető
DNS	mérés	Nagy pontosság	Magas ár, lassú sebesség, nagy méret	A legpontosabb technológia

3. táblázat: A biomtrikus azonosítási módszerek összehasonlítása

Minden biometrikus azonosító módszer egy mintázat-összehasonlító algoritmusra épül. A biometrikus mintán (arc, ujjnyomat, írisz stb.) jellegzetes pontokat keres a szoftver, majd ezek egymáshoz viszonyított helyzete alapján végzi az összevetést. Nagyfokú azonosság esetén - amelynek szintjét általában a felhasználó is megszabhatja - a mintákról kijelenthető, hogy ugyanattól a személytől származnak.

A fejezetben feldolgoztam a lényegesebb, elterjedtebb biometrikus azonosítási technológiákat. Egymással összehasonlítva ezek jelentős különbségeket mutatnak.

Fontos, hogy adott feladatra vonatkozóan minden számba jöhető technológiának ismerjük az előnyös, valamint a hátrányos tulajdonságait. Általánosságban kijelenthető tehát, hogy nincs jó és rossz technológia, mert mindig a megoldandó probléma határozza meg, hogy melyik az adott célra a leginkább megfelelő módszer.

2.2 A biometrikus azonosítás informatikai környezete

A következőkben az eszköz és a hozzá kapcsolódó egységek közötti kapcsolatot és annak biztonságának meghatározását mutatom be.

Jogosultságkezelés. Van-e az „admin” és a „user” között különbség? Hány jogosultsági szint állítható be?

Az eszköz menürendszerének jogosultságkezelése:

1. billentyűzeten felhasználó hozzáadása, törlése vagy módosítása lehetséges,
2. a billentyűzeten az eszközbeállítások módosíthatók vagy sem,
3. nincs billentyűzet.

Jelszóelvárás. A jelszó komplexitása szerint:

1. a belépéshez nem szükséges jelszó,
2. a jelszó nem módosítható,
3. elfogad egykarakteres jelszót,
4. elfogad négykarakteres jelszót,
5. jelszó komplexitása elvárt (pl. számot, nagybetűt tartalmaznia kell a jelszónak).

Jelszócsere.

1. a belépéshez nem szükséges jelszó,
2. a jelszó nem módosítható,
3. a jelszó módosítható,
4. időnként kéri a jelszó lecserélését, de nem kötelező megváltoztatni,
5. időnként kéri a jelszó lecserélését és kötelező megváltoztatni (a korábbi jelszavak sem használhatók újra).

Vizsgálandó az egyes egységek közötti a kommunikáció, így a biometrikus eszköz és a program, illetve a biometrikus eszköz és a beléptető rendszer vonatkozásában.

Csatlakozófelületek:

1. USB
2. RS-232
3. RS-422
4. RS-485
5. TCP/IP[1]
6. CAN BUS (beléptető rendszer is használja)

Kommunikációs csatornák letiltása. Letilthatók-e az egyes kommunikációs csatornák (a nem használt, de aktív kommunikációs csatornák támadási felületet jelentenek a rendszeren):

1. nem
2. igen

Képesség a Kliens-szerver üzemmódra (Architektúra). Meg kell vizsgálni, hogy el lehet-e választani a szervert a klienstől. Ez azt jelenti, hogy a kliens program és az adatbázis nem ugyanazon a számítógépen fut. Amennyiben nem oldható ez meg, akkor előfordulhat, hogy nem felel meg az esetleges helyi rendszerbiztonsági előírásoknak.

[1] Az internet protokoll, a TCP/IP betűszó angol rövidítésből keletkezett: Transmission Control Protocol / Internet Protocol (átviteli vezérlő protokoll/internet protokoll). A TCP/IP egy olyan protokollkészlet, amelyet arra dolgoztak ki, hogy hálózatba kapcsolt számítógépek egymás között megoszthassák erőforrásaikat.

A szervert szerverteremben ajánlott tartani, de mindenképpen egy védett helyen. Így sokszor nem elfogadható, hogy például a portán lévő gépen fut az adatbázis. Ezért szükség van rá, hogy a szerver és a kliens legyenek külön gépre telepíthetők.

Besorolás:

1. nem
2. igen

Nyílt protokoll. Nyílt protokoll esetén a kommunikáció során elküldött adatok felépítése mindenki számára nyíltan elérhető. A nyílt protokollok gyakran biztonságosabbak, üzembiztosabbak, azonban lehallgatásuk is könnyebb lehet, hiszen ismert a kommunikáció felépítése. Például Wiegand kommunikáció esetén a kommunikáció a szabályok ismeretében könnyen lehallgatható és visszajátszató egy egyszerű modul segítségével.

1. igen
2. nem

Kommunikációs jelszó. Szükséges-e jelszó a csatlakozáshoz?

1. nem
2. igen

Hitelesítés. Azonosítja-e a terminál és a szerver egymást? Amennyiben igen, mi alapján? Milyen mértékű a titkosítás:

1. nem titkosított az adat
2. titkosított az adat
3. titkosított az adat és hitelesítést is használ
4. titkosított az adat és időbélyeget is használ

Elvárás, hogy a fogadó egység győződjön meg róla, hogy az adatot az küldte, akitől azt várja (lásd: MSZ ISO IEC 27001 A12.2.3 szabvány!).

Rádiós csatorna. Hátrány, ha a támadónak fizikailag nem kell ott lennie, elegendő, ha a hatótávolságon belül van (ezt a támadó tudja növelni például nagyobb nyereségű antennák alkalmazásával, vagy az adóteljesítményének növelésével). Lényeges tehát, hogy mennyire biztonságos a választott csatorna.

Rádiós biztonságtechnikai rendszerek kommunikációját a 433-as protokoll írja le, míg az újabbak a 866-as protokoll szerint működnek.

Wifi: fel kell sorolni, hogy milyen titkosításokat tud kezelni. Sajnos jelenleg mindegyik feltörhető, de ennek ellenére jobb egy magasabb biztonsági szintet képviselő megoldást alkalmazni.

1. igen
2. nem

Adatbázis. Az adatbázis helye szerint:

1. a szerveren nem, csak az eszközön
2. szerveren és eszközön
3. az eszközön nincs adatbázis, minden belépésnél a szerverről kérdezi le

Az adatbázis formátuma.

1. textállomány
2. saját nem titkosított
3. valamilyen ismert adatbázis titkosítás nélkül
4. saját titkosított
5. valamilyen ismert adatbázis titkosítással (pl. MySQL, MSSQL, firebird)

A titkosítás hatásköre.

1. semmit nem titkosít
2. a kártyaszámot és a biometrikus mintát titkosítja
3. minden adatot titkosít

Titkosítás. Titkosított-e a protokoll:

1. nem: (pl. FTP, telnet)
2. igen: (pl. HTTPS, SSH, IMAPS, VPN, SFTP)

Az alkalmazott titkosítás típusa.

1. saját
2. DES
3. AES

Kulcsméret.

1. 16 bit vagy kevesebb
2. 32 bit
3. 64 bit

4. 128 bit
5. 192 bit
6. 256 bit vagy több

Naplózás. Van-e naplózás az eseményekről? Hol tárolt a napló?

1. nincs
2. csak az eszközön tárolódik a napló
3. a szerveren is tárolódik a napló
4. a napló hitelesítéssel és időbélyeggel ellátott, tehát a benne lévő események utólagos rögzítése nem lehetséges

A napló eseményei: események/riasztások:

1. belépések a kártyával/biometrikus adattal
2. hibaesemények
3. bejelentkezés/kijelentkezés a szoftverbe/szoftverből
4. áramellátás megszakadása
5. beállítások módosítása
6. a kommunikáció megszakadt
7. hibák helyreállása
8. figyelmeztetések, veszélyhelyzetek, katasztrófa

Az egyes események részletessége:

1. időpont
2. esemény megnevezése
3. felhasználó neve/ID száma
4. az esemény helye
5. az esemény körülményei (pl. karbantartás közben, munkaidő alatt, a vezérlő panel meghibásodásakor)

Webszerverek. Futtat-e webszervert az eszköz?

1. nem
2. ki-be kapcsolható
3. igen, saját fejlesztés (milyen sérülékenységei vannak?)
4. igen, nem saját fejlesztés (pl. apache, jboss, IIS)

Nyitott portok és szolgáltatások. Ezeket kell ellenőrizni és felsorolni, hogy mely portokon válaszol (lehetőleg csak az a port legyen nyitva, amit használ is az eszköz, ugyanis más portok nyitva hagyása biztonsági rést képezhet).

A nyitott portokat „ping” paranccsal tesztelhetjük manuálisan, amely egy ICMP csomag.

Portok engedélyezése. Milyen jogosultsággal lehet engedélyezni a portokat és honnan:

1. A kommunikációs portok nem tilthatók le.
2. A kommunikációs portok letilthatók, de az eszközről újra engedélyezhető.
3. A kommunikációs portok letilthatók és csak kliensről vagy szerverről engedélyezhető újra.

2.2.1 Az ideálisan felépített informatikai rendszer jellemzői

Az előzőekben leírtak alapján összeállítható az ideális informatikai rendszer jellemzői (4. táblázat).

Vizsgált elem	Lehetséges válaszok száma	Megjegyzés
Eszköz menürendszere	3	billentyűzet megléte, jogosultságok
Jelszóelvárás	**5**	**a jelszó minimális komplexitása**
Jelszócsere	5	lehetőségei és kötelező idő-intervalluma
Csatlakozófelületek	6	Az eszköz más eszközzel való kommunikációjára
Kommunikáció letiltható-sága	2	A nem használt csatornák deaktiválhatósága
Kliens-szerver lehetőség	2	A kliens és szerver fizikai elválasztása
Nyílt protokoll	2	A kommunikáció bizalmassága
Kommunikációs jelszó	2	Szükséges-e?
Hitelesítés	**4**	**A terminál és a szerver azonosítja egymást**
Titkosítás	**4**	**A terminál és a szerver közötti kommunikációban**
Wifi	2	Alkalmaz-e?
Adatbázis helye	3	szerveren / eszközön
Adatbázis formátuma	**5**	**a titkosítás megléte**
A titkosítás hatásköre	3	mindent titkosít-e?
Kommunikáció titkosítása	2	az eszközök között
Titkosítás típusa	3	Saját vagy ismert
Kulcsméret	**6**	**bit-ben megadott méret**
Naplózás	4	a napló megléte és helye
Napló események fajtái	8	8 különböző fontos esemény
Napló események részle-tessége	5	5 különböző részlet
Webszerverek	4	milyen fejlesztés?
Nyitott portok	3	letiltás lehetősége

4. táblázat: az ideális informatikai rendszer jellemzői (összefoglaló táblázat, a lényeges elemek félkövér betűtípussal kiemelve)

3 SZEMPONTRENDSZER MEGHATÁROZÁSA AZ E-KERESKEDELEM VÁSÁRLÓI OLDALÁN ALKALMAZHATÓ BIOMETRIKUS AZONOSÍTÓKHOZ – A BIOMETRIKUS MINTÁK SÉRÜLÉKENYSÉGE

Saját, több mint tíz éves szakmai tapasztalataimra alapozva elmondhatom, hogy egy adott feladatra alkalmazott biometrikus eszköz nem minden esetben teljesíti optimálisan az elvárt követelményeket (azonosítási sebesség, pontosság, stb.). Komoly etikai problémákat vet fel, amikor a gyártó adatlapjai (data sheet) – remélhetőleg nem szándékosan, hanem oda nem figyelésből – a valóságtól eltérő értékeket, adatokat tartalmaznak.

A gyártó természetesen végez laboratóriumi teszteket, azonban általában nem valós felhasználókkal tesztel (ez nem is várható el mondjuk egy tízezres alkalmazói kört megcélozva), hanem egy előre kiadott és optimalizált template[2] adatbázison futtatja a teszteket. A gyakorlatban viszont a biometrikus adat rögzítése és eredménye az említett folyamattól jelentősen eltér.

Nem ritkán előfordul, hogy a felhasználási helyen a regisztráció hibásan történik, amelyre a legtöbb eszköz nem figyelmeztet. Az azonosítás során a rendszer a regisztráció alatt rögzített képpel hasonlítja össze az aktuális mintát. Amennyiben a regisztrációs minta gyenge minőségű, akkor a későbbiekben az összehasonlítási folyamat sikeressége is természetszerűleg alacsonyabb lesz.

A gyártók által kiadott műszaki adatlapokon feltüntetettektől – az üzemeltetési környezettől függően - eltérhet a gyakorlat. A leglényegesebb üzemeltetési paraméterek, mint a hőmérséklet, a levegő-páratartalom és ezek stabilitása - ott, ahol az eszköz telepítésre került -, a leglényegesebbek a működtetés szempontjából.

[2] Jellemzően valamilyen ez vektormező, amely egy adott személyre jellemző biometrikus minta digitálisan leképzett képe. Lehet titkosított, vagy titkosítás nélküli. Általában nem állítható vissza belőle az eredeti biometrikus minta.

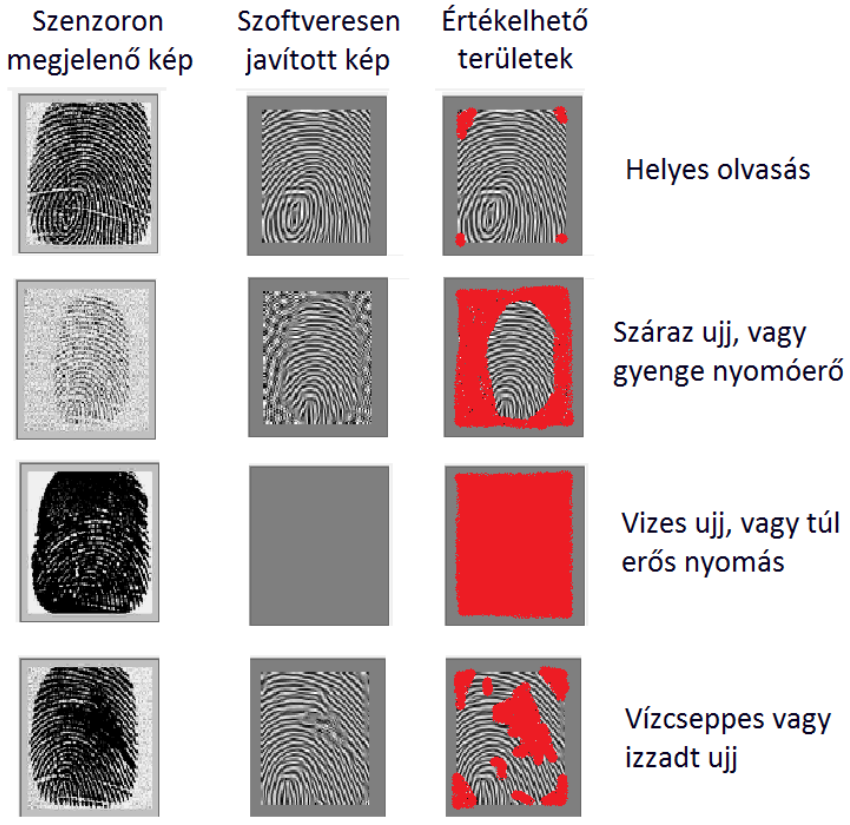
Sok esetben maguknak a felhasználóknak fizikai, biológiai, antropológiai paraméterei (sérülések, idegen anyagok vagy testi deformációk) nem alkalmasak a sikeres biometrikus azonosításhoz. [43, pp. 1-10.]

3.1 A minta megfelelősége az azonosítás végrehajtásához

A fejezet elsősorban saját tapasztalataimat rendszerezi. A lehetséges mintaforrásokat számba véve feltárja azokat a sérülékenységi elemeket, amelyek a biometrikus azonosítás sikerességét veszélyeztethetik.

3.1.1 Ujjnyomat

Ujjnyomat-azonosítás esetén az ujjbegy hámrétegének azonosításra alkalmas (egészséges) állapotban kell lennie: amennyiben a bőr hidratáltsága alacsony, akkor a fodorszálak túl halványan, vagy egyáltalán nem látszódnak a szenzor számára. Ekkor a fodorszálakkal együtt a minutia pontok is „láthatatlanok” maradnak.

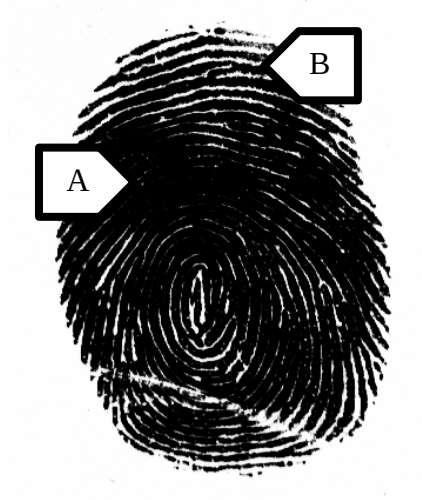


17. ábra: Az ujjnyomat-azonosítás hiányosságai, piros színnel az értékelhetetlen területek

A 17. ábrán látható néhány jellemző, gyakori hiba, amelyek esetén előfordulhat, hogy nem értékelhető nyomatot ad az ujj. Például vizes, nedves ujj esetén a barázdák egybeolvadását figyelhetjük meg. Gyakran nem csak két szomszédos fodorszállal történik ez, hanem az ujjbegy jelentős részén megfigyelhető a jelenség.

18. ábra: Az ujjnyomat képe kiszáradt (dehidratált) ujjbegy esetén

A 18. ábrán az látható, hogy száraz, kiszáradt hám esetén az ujjnyomat képe azért nem lesz értékelhető, mert a fodorszálak rajzolata nem „látszódik” a szenzor számára. Ez az eset következik be például a hagyományos „táblás” oktatásban az egésznapos krétahasználat után. Olyan területek figyelhetők meg a mintán, amelyekről lehetetlen megállapítani a mintázatot (az ábrán A-val jelölve). A jelenség hasonló ahhoz, mint amikor egy ujjnyomat-olvasóra az ujjat nagyon gyenge erővel nyomja rá a felhasználó. Ugyanakkor az ujj egyes rész-területei értékelhetők maradnak (az ábrán B-vel jelölve).



19. ábra: Az ujjnyomat rajzolata erősen nedves ujjbegy esetén

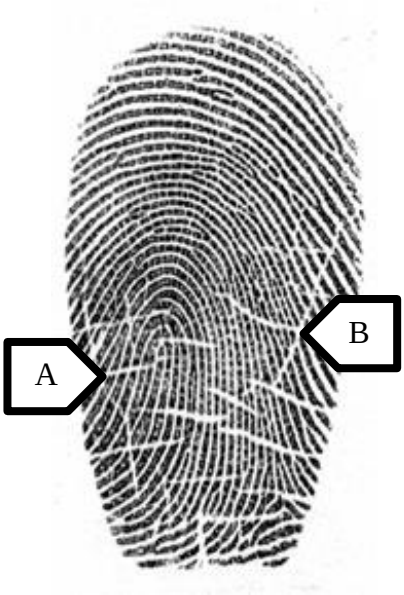
Amennyiben erősen nedves az ujjbegy, akkor a fodorszálak rajzolata összemosódik a képen, a minutiapontok felismerhetetlenné válnak az érintett területen. Ez történik például kézmosás után, ha a szárítás elmarad. Erre mutat példát a 19. ábrán az A terület, míg a B-vel jelölt (nem érintett) rész értékelhető marad.

20. ábra: Az ujjnyomat sérülése

A 20. ábra az ujjsérüléseket mutat be az A-val illetve B-vel megjelölt területen. Egy ilyen esemény maradandóan megváltoztatja az ujjnyomat képét, abban új minutiapontok jönnek létre. Ez egyrészről előnyös, hiszen így több pont áll rendelkezésre az azonosításhoz, másrészről viszont hátrány lehet, hiszen az eredeti (ős) ujjnyomat képe megváltozott.

21. ábra: Az ujjnyomat képe kémiailag maradandóan sérült ujj esetén

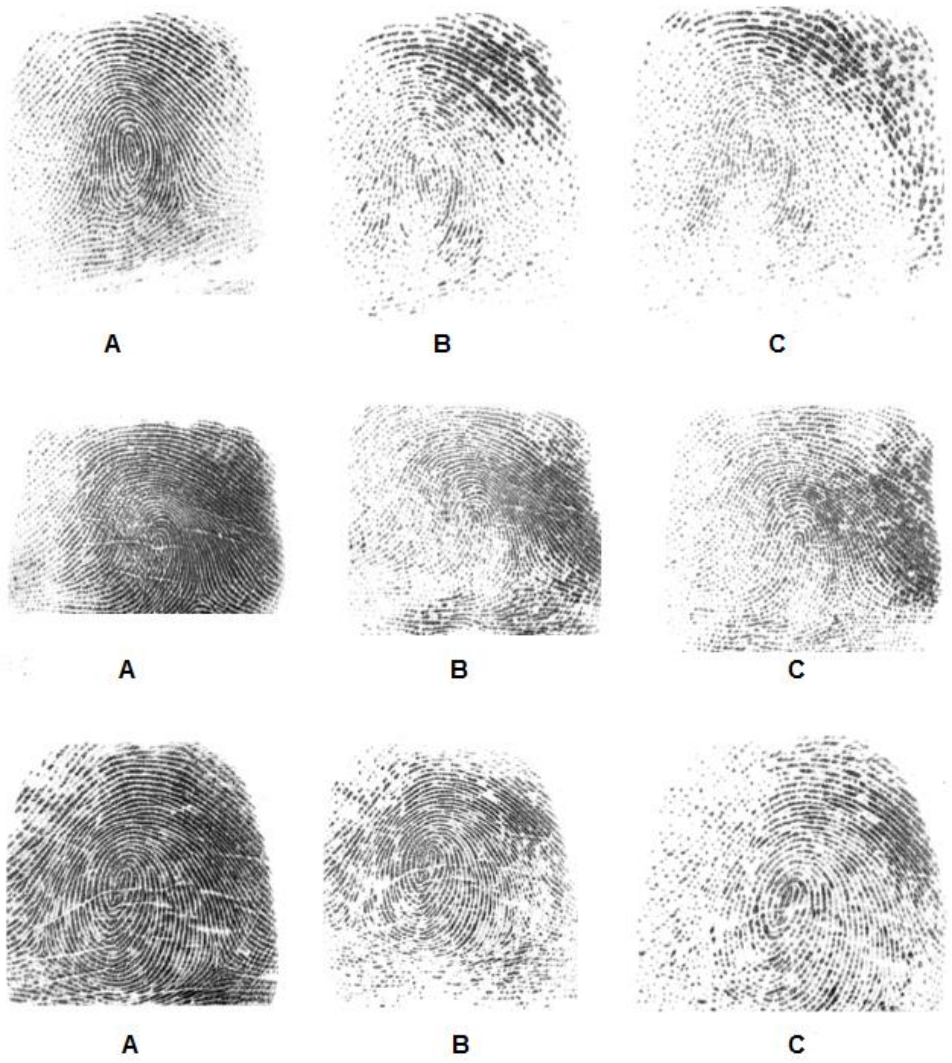
Vegyi anyagtól maradandóan sérült ujjbegy esetén a szenzor a 21. ábrán látható képet generálja. A kép A-val jelölt részén HNO_3 (salétromsav) okozott maradandó elváltozást a bőr felszínén. A képen megfigyelhető, hogy az ujjnyomat képe az eredetihez képeset jelentősen változott: az ujjnyomat mintázata az A területen nem értékelhető, a B helyen az ősmintázattól eltérő, míg a C részen változatlan maradt.



22. ábra: A bőr öregedésének természetes jelei az ujjnyomaton

A 22. ábrán A-val és B-vel megjelölt területen egy másik jelenség látható, ezek az egyenes fehér vonalak a bőr természetes öregedése miatt alakulnak ki.

A kézmosás is hatással lehet az ujjnyomat mintázatára: érdekesség, hogy a legtöbb esetben gyengíti az azonosíthatóságot. A Biometrikus Laboratóriumban több mint 200 mérést végeztem, ezzel kapcsolatban az eredményeket szemlélteti a következő, 23. ábra.



23. ábra: A kézmosás hatása az ujjnyomat mintázatára

A 23. ábrán az A-val jelölt ujjnyomat kézmosás nélkül készült, a B-vel jelölt esetben csak folyóvízzel, a C-vel jelölt ujjnyomat képének elkészítése előtt pedig szappannal és vízzel is sor került a kézmosásra. A 30 s-os kézmosások után azonnal, törölközővel szárazra töröltem a kezet (ujjakat), majd további 30 s levegőn történő szárítás után Suprema Realscan-10 eszközzel készültek a felvételek. Az ábra C oszlopa jól szemlélteti,

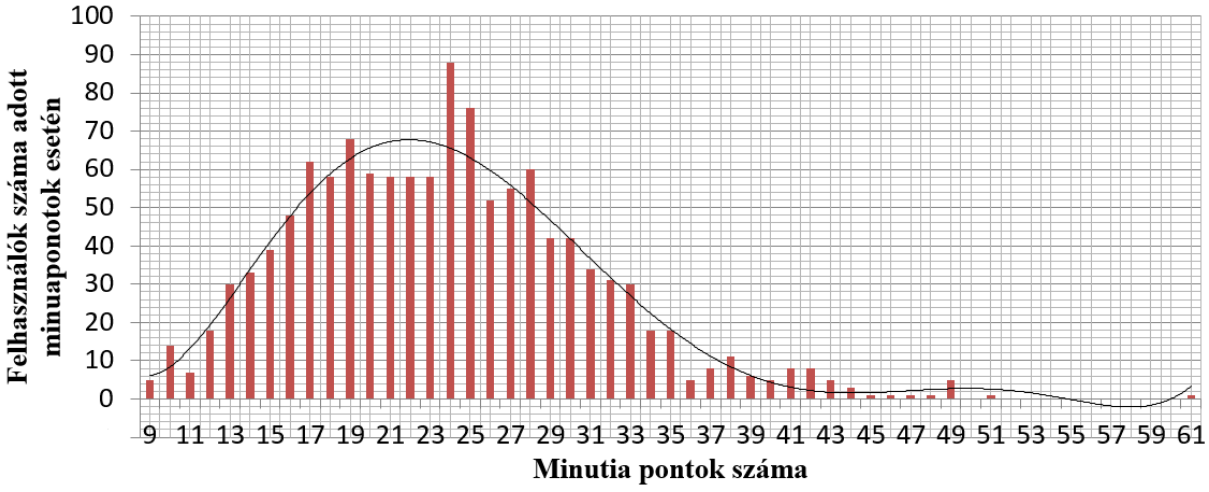
ahogyan a kézmosás megváltoztatja a bőr felszínének állapotát, és a mintázat képét időlegesen azonosításra alkalmatlanná teszi.

A B C D

(A) Normál állapotú ujj. (B) 1ml body lotion. (C) 3ml body lotion. (D) 6ml body lotion

24. ábra: Az ujjnyomat mintázata különböző mennyiségű kézkrém használata után

A 24. ábrán látható a kézkrém hatása az ujjnyomat mintázatára. A méréshez 280 mérést végeztem el különböző tesztalanyokon. Az eredményt egyértelműen mutatja, hogy 1 ml kézkrém esetén javult az ujjnyomat felismerhetősége, 3 és 6 ml esetén pedig jelentősen romlott. A tesztek elvégzéséhez Balea Body Lotion Milch & Honig kézkrémet használtam.



25. ábra: Minutia pontok száma egy ujjon

A 25. ábra elkészítéséhez 1232 felhasználó ujjnyomatát vettem alapul Suprema Bio Entry Plus készüléken regisztrálva. Az ábrán hatodfokú polinomiális trendvonal figyelhető meg (fekete takaró görbe). Jellemzően 15-30 minutia pontot regisztrált a rendszer, szélsőséges esetben 61-et illetve 5 alkalommal 9-et.

Összefoglalva elmondható, hogy a sikeres ujjnyomat azonosításnak számos előfeltétele van. Kísérletekkel bizonyítottam, hogy a képminőséget alapvetően befolyásolja az ujjbegy természetestől eltérő fizikai, biológiai állapota, illetve minőségi és szennyezettségi foka.

3.1.2 Írisz

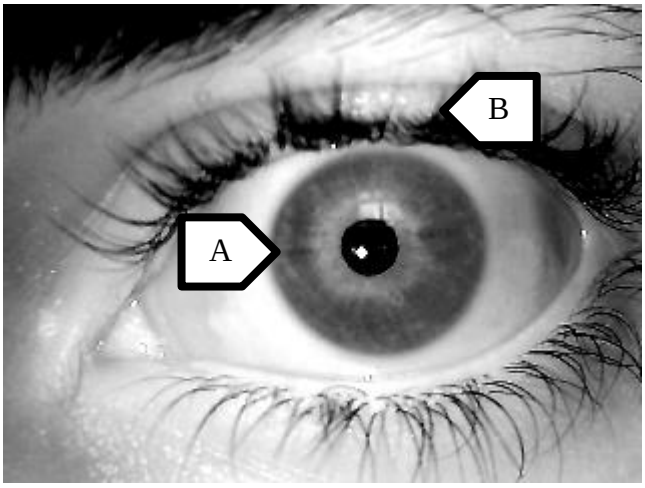
Az általam végzett kísérletek feltételezik, hogy a vizsgált személy írisze alkalmas a regisztrációra.

Az írisz vizsgálata során három fő esetleges sérülékenységet okozó elemet találtam, nevezetesen:

1. A szem nyitottságának mértéke.
2. Fényviszonyok.
3. A kamera pozíciója.

Részleteiben:

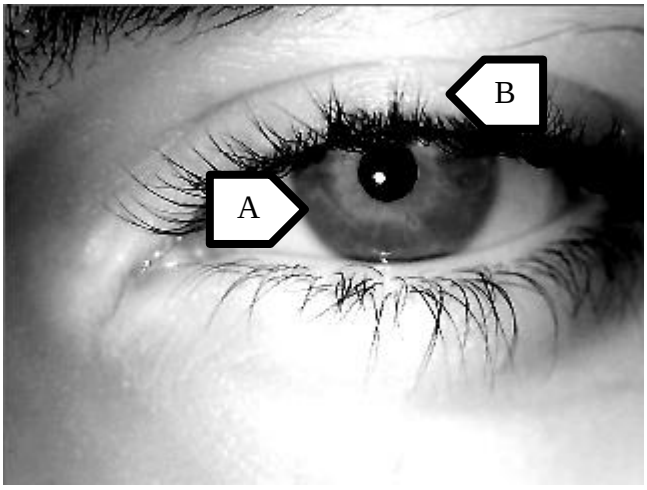
A *szem nyitottságának mértéke* kiemelkedően fontos szempont. Tesztjeim alapján megállapítottam: ha a szemhéj részben takarja az íriszt, akkor a téves elutasítási arány jelentősen növekszik.



26. ábra: Az írisz teljesen nyitott szem esetében

A 26. ábra egy teljesen nyitott szemet mutat be. Az A-val jelölt írisz felett látható a B-vel jelölt szemhéj. Ilyenkor a sikeres azonosítás valószínű.

A 27. ábrán a szem nincs teljesen nyitva, itt az A-val jelölt íriszt részben eltakarja a B-vel jelölt szemhéj. Ebben az állapotban a Ni-Eye Mirrorkey MKC-Module 500 már képtelen azonosítani az íriszmintázatot: a téves elutasítás mértéke 100 %-os volt (10 személyen vizsgálva, személyenként 10 azonosítási kísérletet végezve).



27. ábra: Az írisz részben nyitott szem esetében

A *fényviszonyok* szerepe szintén jelentős az azonosítás sikerességében. Ennek fő oka, hogy a szem felületén tükröződnek a világítótestek és fényforrások fényei.

A tükröződő fényeket két csoportba oszthatjuk. Az egyik az írisz azonosító eszköz által kibocsájtott infra tartományú fény. Léteznek olyan azonosító eszközök is, amelyek passzívak és nincs beépítve fényforrás. Azok, amelyek beépített fényforrással rendelkeznek, általában infratartományban világítják meg a szemet. Mivel a kamera is ugyanebben a tartományban működik, ezért a szemen jól látható az eszköz által kibocsájtott fény visszaverődése. Ez általában a pupilla területére esik, tehát az íriszben nem hoz létre foltot.

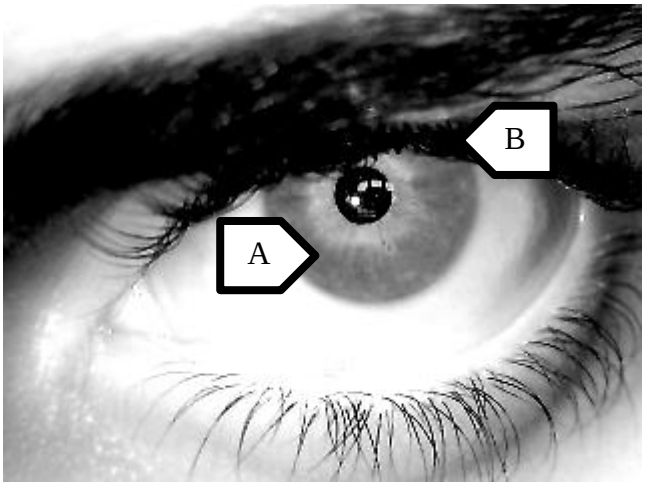
A másik csoportba a kívülről érkező fények tartoznak. Ezek lehetnek természetesek és mesterségesek. Az ilyen típusú tükröződések is megjelenhetnek tehát az íriszen, amely az azonosítás sikerességét csökkenti.

Az az eset is előfordulhat, hogy a kamera által „látott” terület egy része túlzottan megvilágított, így a képnek csak egy része értékelhető. Ekkor az írisznek csak egy részét használhatja az eszköz azonosításra: következésképpen a téves elutasítás értéke drasztikusan megnövekszik. Lényeges tehát, hogy a megvilágítás optimális legyen.

A *kamera pozíciója* szintén kiemelt fontosságú. A kamerának közelről kell a szemet vennie, azzal a lehető leginkább szemben pozícionálva. Ez nem egyszerű feladat, mert kis látószögű kamerát alkalmaznak és a szemnek is közel kell lennie az eszközhöz.

Rögzített helyre beépített eszközök esetén a testmagasság alapvetően meghatározza az azonosítás sikerességét. Számos tesztet végeztem ennek a bizonyítására. Végeredményben igazoltam a sejtést, hogy akkor a leghatékonyabb az írisz azonosítása, amikor a kamera és a szem ugyanabban a magasságban helyezkedik el.

Abban az esetben, ha a kamera elhelyezkedése olyan, hogy az íriszre mintegy lefelé, vagy felfelé néz akkor a Ni-Eye Mirrorkey MKC-Module 500 azonosító 90 %-os téves elutasítást produkált (28. ábra).



28. ábra: A szemhéj eltakarja az írisz jelentős részét, a szem síkja 60°-os szöget zár be az eszközhöz húzható egyenessel

Tapasztalataim szerint arra mindenképpen figyelni kell, hogy az arc síkja merőleges legyen a szemközépből a kamerára húzott képzeletbeli egyenesre. Tehát, amennyiben a kamera a szem magassága alatt helyezkedik el, akkor a fejet előre kell billenteni.

Amennyiben a szem az eszköz magassága felett helyezkedik el, akkor az azonosítási sikeresség csak csekély mértékben romlik.

Abban az esetben, ha a szem az eszköz magassága alatt helyezkedik el, akkor minél nagyobb az eltérés, annál nagyobb lesz a FRR[3] érték is.

29. ábra: Írisz azonosítás pozícionálásának egy lehetséges megoldása repülőtéren [44]

A 29. ábrán látjuk a felvetett probléma egy másik megoldási módját. Ebben az esetben az íriszt (A) fényképező kamera (B) függőlegesen képes elmozdulni, így állítható be az adott személyhez viszonyított optimális magasságba.

3.2 A minta másolatának elkészítése

A biometrikus azonosítás lényeges eleme lehet az élőminta-felismerés. Amennyiben az eszköz nem rendelkezik ilyen technikai tulajdonsággal, akkor szinte minden esetben elérhető, hogy egy, a valódi biometrikus mintáról készült másolatot az eszköz úgy azonosítson, mintha az aktuális minta valóságos (élő) lenne. Itt az általam vizsgált technológiák voltak: az ujjnyomat, az arc, a tenyérérhálózat és az íriszazonosítás.

Nem humán biometrikus mintát minden említett biometrikus azonosító készülékhez létre lehetetett hozni, ezek összetettsége és időigénye eszközönként eltérő volt.

[3] Az angol „False Rejection Rate” (téves elutasítási arány) kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban utasítja el a rendszer a jogosult felhasználót.

Kétféle mesterséges mintát tudtam előállítani:

1. Regisztrálható és azonosítható.
2. Egy regisztrált (létező) személy valamilyen biometrikus mintájának másolata.

A regisztrált személy közreműködésének vonatkozásában:

1. A személy közreműködésével készített (működő) másolat.
2. A személy tudta nélkül készített (működő) másolat.

Megítélésem szerint a mintamásolással kapcsolatosan a biometrikus eszközökre négy különböző biztonsági fokozatot vezethető be, nevezetesen:

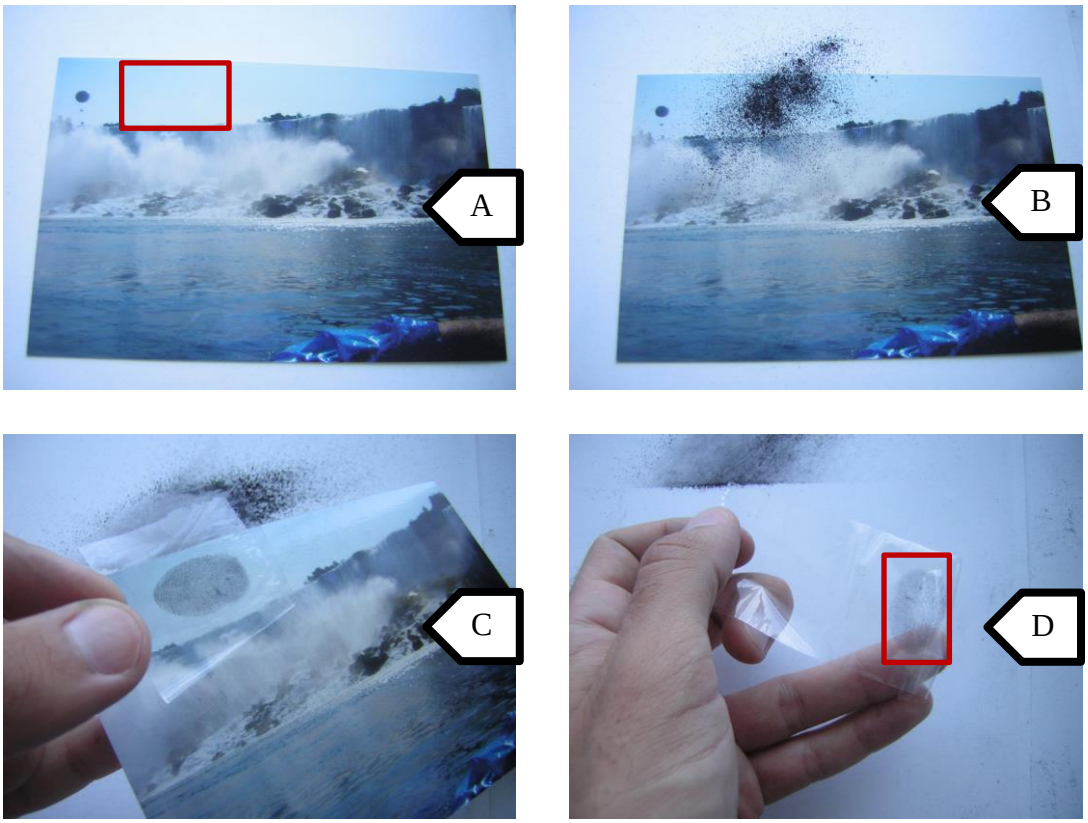
1. fokozat: Nem készíthető működő biometrikus másolat az adott eszközhöz (a legerősebb fokozat).
2. Egy regisztrált személy biometrikus mintájáról annak közreműködésével készíthető működő biometrikus másolat (a másolatot létező mintaként fogadja el az eszköz).
3. Egy regisztrált személyről annak tudta nélkül készíthető működő másolat.
4. Készíthető olyan tárgy, amely biometrikus mintaként regisztrálható és azonosítható (leggyengébb biztonsági fokozat).

3.2.1 Ujjnyomat

A tulajdonos számos helyen „hagyhatja ott” az ujjnyomatát: például poháron, fényképen, számítógép egéren, kilincsen, ajtón, asztalon, gépjárművön. Ez pedig alkalmat ad másolat készítésére. [45] Jómagam az így megszerzett mintát egy rugalmas anyagra hívtam elő. Ezt követően már - például egy laptopon lévő ujjnyomat olvasón keresztül - elérhető minden ezzel az ujjnyomattal védett adat, információ, hozzáférés.

Az ujjnyomat-másolat elkészítésére két metódust dolgoztam ki.

Az elsőt általában akkor alkalmaztam, amikor a másolatot a felhasználó tudta nélkül készítettem (ezt követően természetesen azonnal tájékoztattam az illetőt). A módszer sikeressége mindig felület és anyagfüggő. A rendőrség által is alkalmazott eljárás a legegyszerűbb és leggyorsabb, ennek menetét mutatja be a következő, 30. ábra. A tiszta felületet (A) grafitporral szórjuk meg (B), majd egy ecsettel lesöpörjük a felesleget. Ezután egy átlátszó, „cellux”-szerű fóliával lehúzzuk a mintát (C). A pirossal megjelölt területen található az „A” képen még a tárgyon, a „D”-n pedig már a fólián lévő ujjnyomat.



30. ábra: Az ujjnyomat előkészítése klónozásra

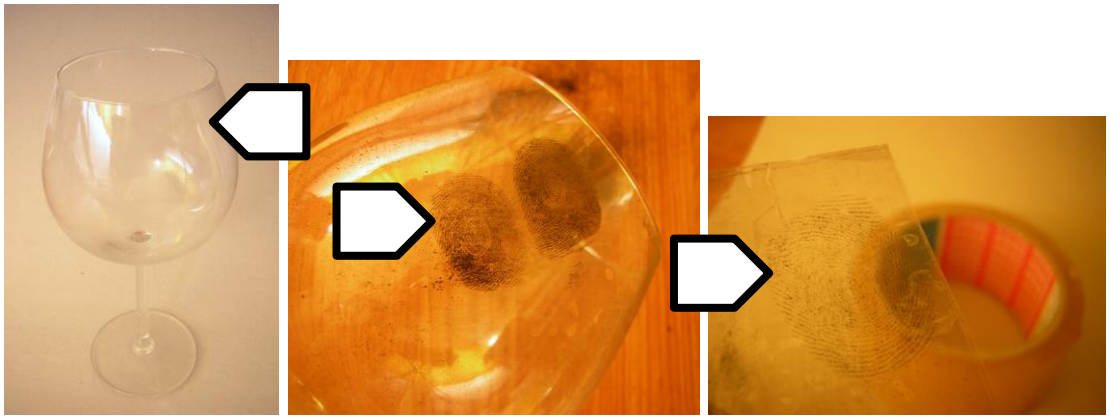
Ezt a mintát számítógép segítségével javítottam, eltüntettem a zajokat, és elkészítettem a nyomtatásra alkalmas képet. A javítás során növeltem a kontrasztot. A folyamat a 31. ábrán látható: A képet digitalizálom (A), majd a kontrasztot manuális módon növelem (B), ezután lokálisan kiválasztom a minimum és maximum értékeket (C), majd kivágom a kép információ hordozó részét (D).

31. ábra: Az ujjnyomat digitalizálásának folyamata

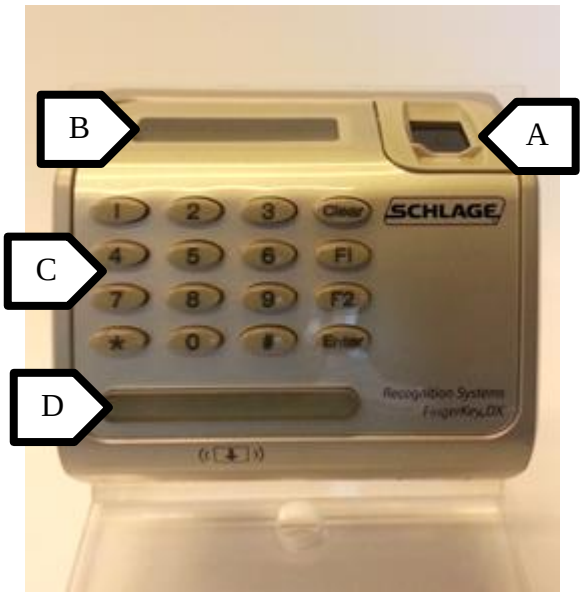
Az utolsó lépés a rugalmas másolat (32. ábra) elkészítése. Ez készülhet CNC marással vagy 3D nyomtatással is. Az első esetben a felesleges anyagot távolítjuk el a munkadarabról, a másik esetben a mintázatnak megfelelően építjük fel a másolatot.

32. ábra: Ujjnyomatról készített háromdimenziós másolat

Ujjnyomat nagyon jó hatásfokkal vehető le pl. borospohárról (33. ábra). Az ujjnyomatra finom grafitport szórva a minta kirajzolódik, amit egy átlátszó ragasztószalaggal könnyedén levehetünk.



33. ábra: Borospoháron található ujjnyomat levétele (nyíllal jelölve a minta)

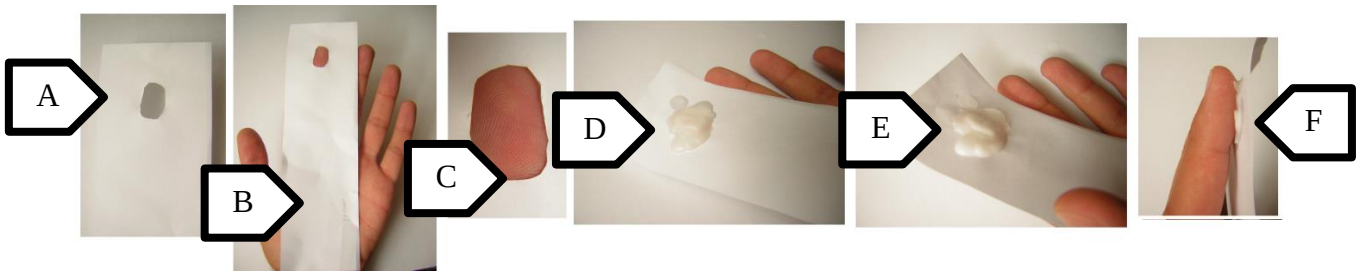


34. ábra: Fingerkey DX ujjnyomat azonosító eszköz

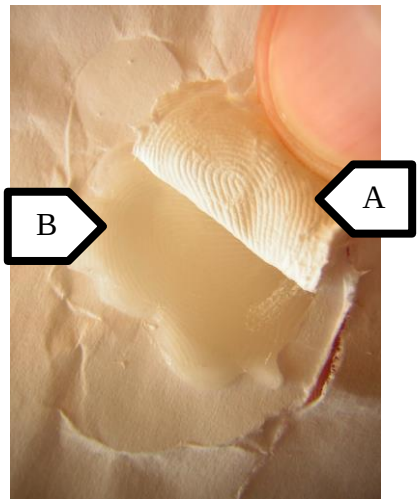
Az elkészített másolatot a Fingerkey DX ujjnyomat azonosító eszközön (34. ábra) teszteltem. A műszer 3 mm-el sülyesztett szenzorral rendelkezik (A), így a bőrnek vagy a guminak rugalmasnak kell lennie, hogy a felületre fel tudjon feküdni. Az eszköz kétsoros kijelzővel (B), nyomógombokkal (C) és egy visszajelző LED-el (D) rendelkezik. A Fingerkey DX 90 % valószínűséggel sikeresen működik az általam elkészített másolattal.

Ezt a klónt ezen kívül még négy különböző ujjnyomat azonosítón is teszteltem - mindegyiken sikerrel. Ezek rendre a Suprema által gyártott Bio Entry Plus, a D-Station, az iEvo Ultimate és az iEvo Micro ujjnyomat azonosító műszerek voltak, ráadásul az utóbbi kettő élőminta-felismeréssel is rendelkezik.

A másik eljáráshoz a felhasználó (minta-tulajdonos) aktív hozzájárulása szükséges. Ekkor - nyilvánvalóan - az előzőhöz képest pontosabb másolat készíthető. A másolás két lépésben zajlik, ezeket a 35. ábra mutatja be. Először egy negatív mintát készítettem az ujjbegyről. Ehhez egy papíron lyukat vágtam az ujjnyomat méretének megfelelően (A), ezután ezt a papírt az ujjra helyeztem (B) úgy, hogy az ujjnyomat pontosan a kivágott területre essen (C), majd ebbe öntöttem gumiszerű anyagból egy vékony réteget (D). Ezt a megszilárdulása után tovább vastagítottam (E), így az stabilabbá vált (az F képen látható, hogy csak az ujjnyomatról készül másolat, nem az egész ujjról).

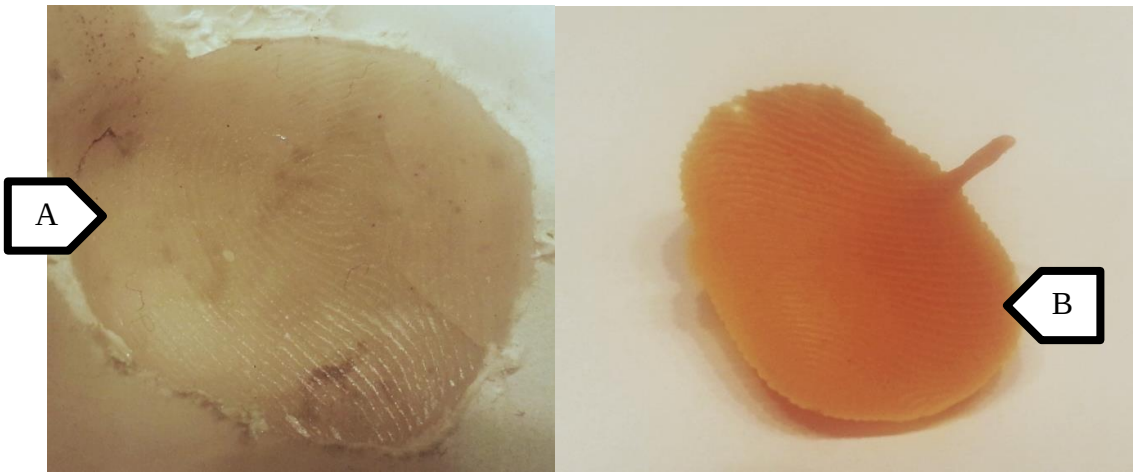


35. ábra: Az ujjnyomat másolása



36. ábra: Az ujjnyomat másolatának leválasztása a negatív formáról

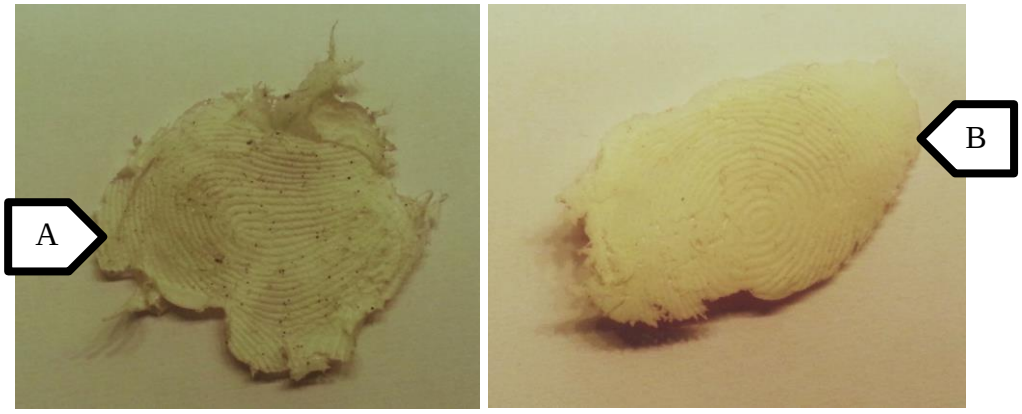
A 36. ábrán látjuk az ujjnyomat másolatának (A) leválasztását a negatív formáról (B), miután a másolat teljes mértékben megszilárdult.



37. ábra: Az ujjnyomatról készült viasz és gumi negatív

A 37. ábrán A-val jelölve látható az ujjnyomatról, viaszból, B-vel - egy hasonló eljárással, de más anyagból - szintén általam készített negatív minta. Mind a negatív, mind a pozitív elkészítéséhez számos vegyület alkalmazható, erre egy példa a 38. ábrán látható kétkomponensű Aquasil Ultra, amely az A és a B részben tárolt folyékony anyagok összekeveredése után szilárdul meg.

38. ábra: Az ujjnyomat másolására alkalmas plasztikus anyag

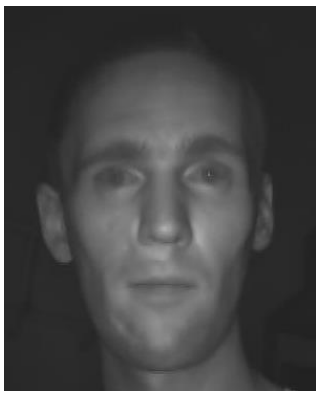


39. ábra: Az ujjnyomat nyers másolata

A 39. ábrán egy általam készített ujjnyomat nyers másolata látható (A), amelyről a széleken elhelyezkedő felesleges anyag például ollóval levágható (B).

Tapasztalataim szerint ujjnyomat viszonylag egyszerűen, speciális eszközök, anyagok, vegyületek igénybe vétele nélkül klónozható.

3.2.2 Arcazonosítás



40. ábra: Az arcról infratartományban készült fénykép

A kifejezetten arcazonosításra készített biometrikus eszközök döntő többsége infratartományban készít felvételt. A megoldás előnye, hogy a kép kevésbé érzékeny a külső fényviszonyok zavaró hatásaira (40. ábra). Jól látható, hogy a fejen kívüli részek igen sötétek, tehát jól kizárja a környezet zavaró objektumait. Jellemző még, hogy néhány esetben a szem közepén megcsillan az infra-megvilágító LED fénye.

Az arcazonosító eszközök esetében két különböző eljárás segítségével találtam sérülékenységet. Az első egy síkbeli, a második egy térbeli felületen alkotja az arc másolatát.

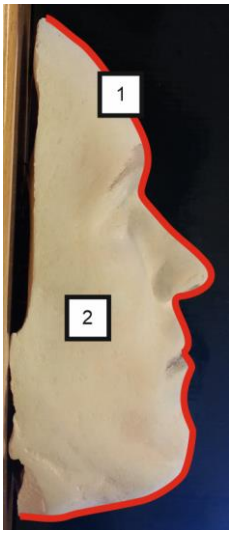
Az első esetben sík felületen hoztam létre tehát a képet. Erről az eszköz által használt infratartományú kamera ugyanolyan felvételt alkot, mint amilyet a valós arcról is kapna.

A második esetben az arcról egy 3D-s másolatot készítettem. Ez után ezt úgy színeztem, hogy infratartományban ugyanolyan textúrával, színnel és kontraszttal rendelkezzen, mint a valós arc (41. ábra).

41. ábra: Színes felvétel az arc 3D színezett másolatáról

Ehhez először el kellett készítenem az arc három dimenziós negatív lenyomatát. Ennek a menete a következő volt: az arcra formaleválasztó anyagot hordtam fel (erre a

feladatra például a kézkrém is alkalmas). Ezután vizes gipszes gézpólya darabokkal fedtem be az arcot (szabadon csak az orrnyílás maradt a légzés biztosítására). A megfelelő rétegvastagság elérése után meg kell várni a gipsz kötését. Amikor ez megtörtént, akkor le kell választani az arcról a körülbelül egy centiméter vastagságú maszkot (a 42. ábrán 1-es számmal és piros színnel jelölve), ami a tökéletes illeszkedésnél fellépő vákuumhatás miatt egy lassú folyamat. Ezután a negatív formát ismét formaleválasztó anyaggal kellett megfesteni, majd gipszet kitöltöttem (pozitív nyomat, a 42. ábrán 2-es számmal jelölve). Ekkor érdemes gézt vagy dróthálót tenni a pozitív formába, hogy a szerkezetben fellépő esetleges húzó irányú igénybevételeket az fel tudja venni - így meggátolva a gipsz darabokra törését.



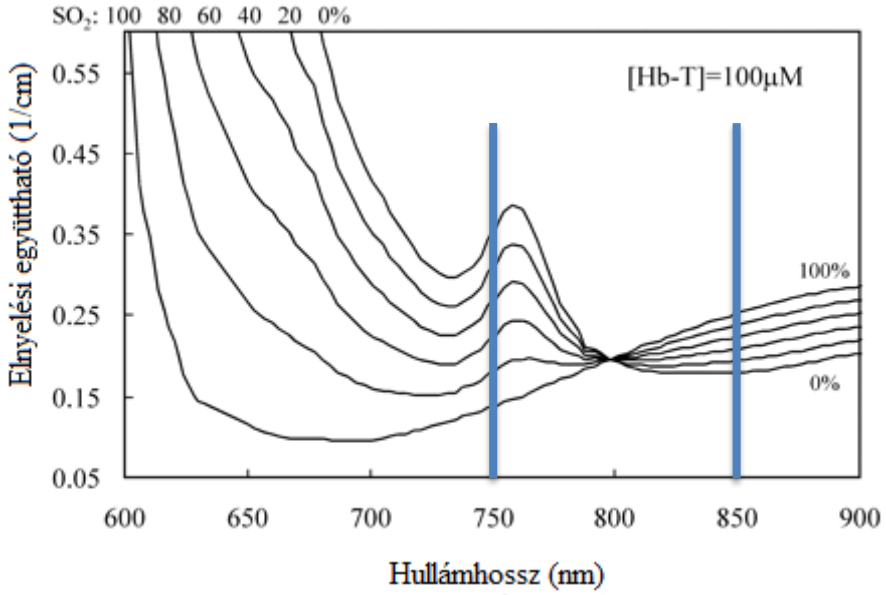
42. ábra: A gipszmásolat elkészítése

A kész gipszmintát ezután színezni kell. A maszk színezését úgy kell elvégezni, hogy infratartományban egyezzen meg a képe a valós arc infratartományú képével. Amennyiben ez sikerül, akkor az arcfelismerő rendszer valóságos mintának fogja „látni” a legyártott maszkot.

3.2.3 Tenyérérhálózat

A tenyérérhálózat-azonosítás esetén infratartományban készül felvétel a tenyérről. Ezen jól megfigyelhető a tenyérerezet, amelyet szabad szemmel általában nem lehet látni. Az egyes erek különböző mértékben nyelik el a fényt annak függvényében, hogy mennyi a bennük lekötött oxigén, illetve milyen hullámhosszúságú fénnyel történik a megvilágítás.

Amennyiben az erezet mintázatának lemásolása a feladat, akkor mindenképpen ugyanolyan hullámhosszúságú infrafénnyel kell a felvételt elkészíteni, mint amilyennel az eszköz dolgozik, amely majd azonosítani fogja a személy kezét és a másolatot is. Ez azért szükséges, mert a különböző hullámhosszúságú fények különböző mélységre tudnak behatolni a bőr alá, így az elkészült infraképen jelentős különbségek jelenhetnek meg. Azt is figyelembe kell venni, hogy a vénák és az artériák a fény hullámhosszától függően más és más arányban nyelik el a fényt.



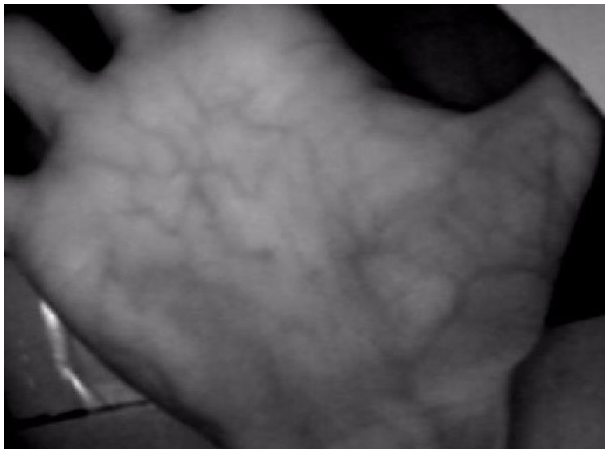
43. ábra: A vér fényelnyelő képessége a fény hullámhosszának függvényében különböző lekötött oxigénmennyiség esetén.([46] alapján készített ábra.)

A 43. ábrán látható, hogy a bejelölt 750 nm-es hullámhosszon a vénák nagyobb kontraszttal jelennek meg a képeken, mint az artériák (amennyiben azonos az átmérőjük és azonos mélységben helyezkednek el): a vénás SO_2 – szaturációs oxigén - indexe 70 %, az artériáknál ez az érték 100 %. Az azonosító algoritmusok az erek síkra vetített helyzetét rögzítik, azok vastagságát és mélységi adatait nem. A tenyérerezet-azonosításra alkalmazott LED-ek hullámhossza tipikusan 750 és 850 nm közé esik. 800 nm alatti hullámhossz esetén a vénás erek detektálása nagyobb hatásfokú. Ugyanekkor határozottan nem lehet kijelenteni, hogy az a kép, amit látunk, az csak vénákat tartalmaz.

A felvétel készítésénél ugyanazokat a megvilágítási körülményeket kell előállítani, mint amelyekkel a biometrikus eszköz is dolgozik, ezzel biztosítva, hogy a felvétel ugyanolyan jellegzetességekkel rendelkezzen, mint az eredeti kép. Ezt a 44. ábrán láthatjuk.

Az elkészített képet ezután megfelelően kell nyomtatni: olyan tintát kell választani, amely ugyanolyan kontrasztú képet jelent a szenzor számára, mint amilyet egy személy tenyere is ad.

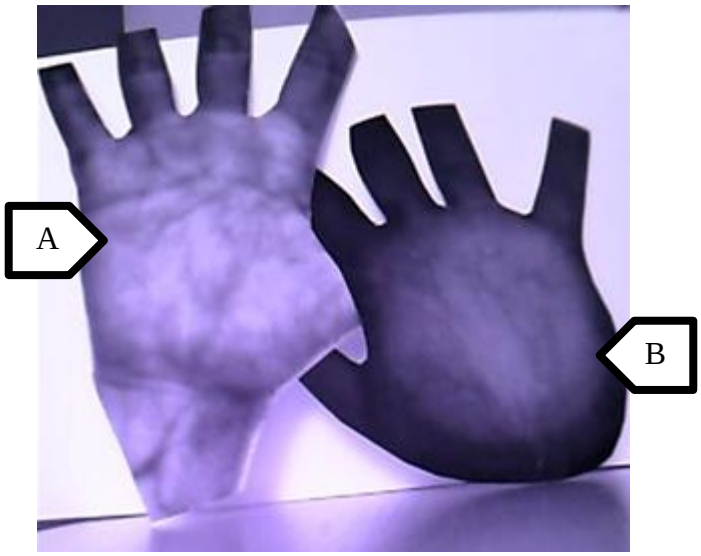
Az így elkészített képet papírlapra lehet nyomtatni, amelyet a kéz alakjának megfelelően körülvágva még megkísérelhető a belépés.



44. ábra: A tenyér erezete

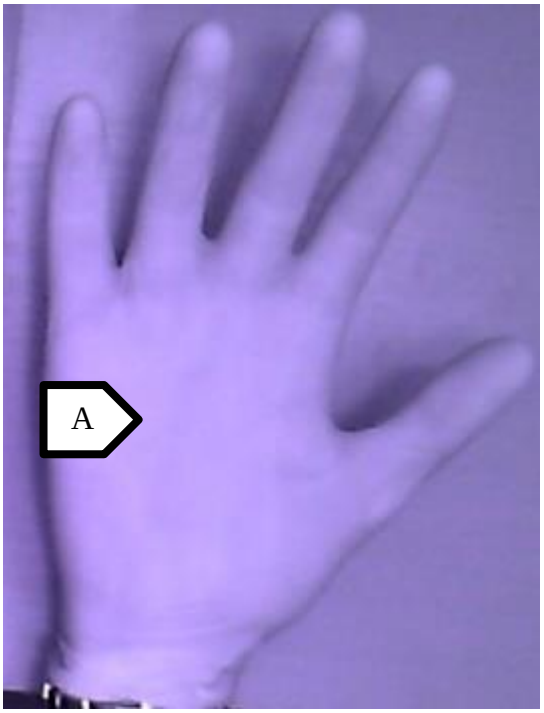
Egy másik módszer szerint a képet gumikesztyűre lehet másolni, amelyet kézre felhúzva végrehajtható az azonosítás.

A 45. ábrán a kinyomtatott kézerezet képe látható infrakamera előtt. Megfigyelhető, hogy a kinyomtatott kép teljesen visszaadja az eredeti rajzolatot. Vizsgálati tapasztalataim azt mutatják, hogy a különböző nyomtatók tintái teljesen eltérő mértékben látszódnak sötétnek, illetve világosnak. Az A-val és B-vel jelölt kép kölönböző tintával nyomtatott tenyér képét mutatja be.



45. ábra: A kinyomtatott kézerezet infrakamera előtt

A 46. ábrán látható, hogy egy orvosi latex gumikesztyű képes eltakarni a kéz erezetét az infratartományban. Azonban a gumikesztyűre filctollal rárajzolható vagy rányomtatható egy másik személy tenyérerezete. Filctoll alkalmazása esetén fontos ellenőrizni, hogy a rajzolt vonalak miként látszódnak infratartományban. Nem csak az egyes vonalak geometriai elhelyezkedése lényeges, de azok vastagsága és árnyalata is.



46. ábra: Egy gumikesztyű az infratartományban

3.2.4 Írisz azonosítás

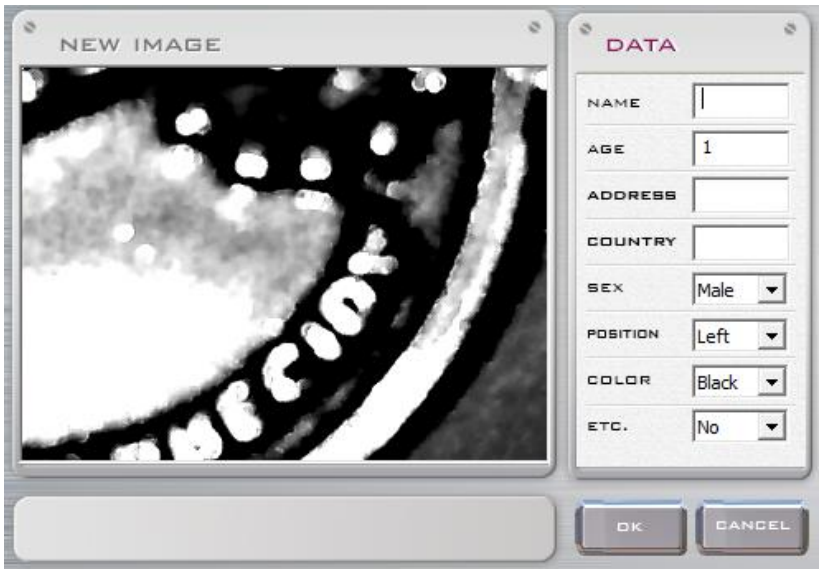
Az arcazonosítás című fejezetben bemutatott módszerek segítségével létrehozható az írisz 2D másolata is. Az íriszazonosítókat úgy tervezték, hogy képesek élőmintafelismerésre (a pupilla tágulását és összehúzódását vizsgálja az eszköz), tehát fényképekkel nem „működnek”.

Méréseim tapasztalata, hogy különböző hullámhosszúságú infrafénnyel megvilágított szem esetén az elkészült képekben jelentős eltérés látható. Ezért kiemelten fontos, hogy a felvételt a másolandó szemről ugyanolyan áteresztő spektrummal rendelkező kamerával készítsük el.

47. ábra: Mi-Eye Mirrorkey írisz azonosító

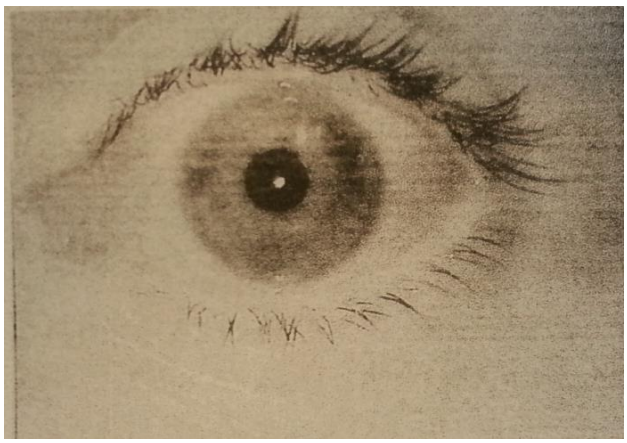
Méréseimet a 47. ábrán látható, USB-porton kommunikáló Ni-Eye Mirrorkey MKC-Module 500 írisz azonosítóval végeztem. Az eszköz tartalmaz egy infrafényvetőt (A) egy nagy látószögű színes kamerát (B) valamint egy infrakamerát (C). Az eszköz előnye, hogy kicsi, mobil és egyszerű a használata.

A kép feldolgozását és az azonosítást a hozzá kapcsolt számítógép végzi el. A berendezés infrafénnyel (A) világítja meg az íriszt, majd egy kamerával (C) alkot képet róla. A kamera előtt egy olyan speciális üveg található, amely az infratartományú fényt átengedi a mögötte található kamera számára, a látható fényt pedig visszatükrözi - ezzel segítve a felhasználót, hogy a szemére irányítsa a kamerát. Amennyiben a saját szemét látja a tükörben, akkor a kamera is az ő íriszére néz.



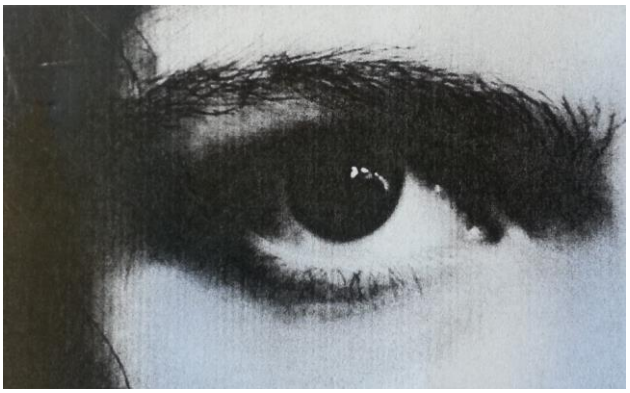
48. ábra: Írisz azonosítóval regisztrált érmerészlet

A 48. ábrán egy sikeres regisztráció látható, amely ebben az esetben egy érme részlete. Megállapítható tehát, hogy nem csak az íriszt, de az arra részben hasonlító tárgyakat is íriszként kezeli az adott eszköz.



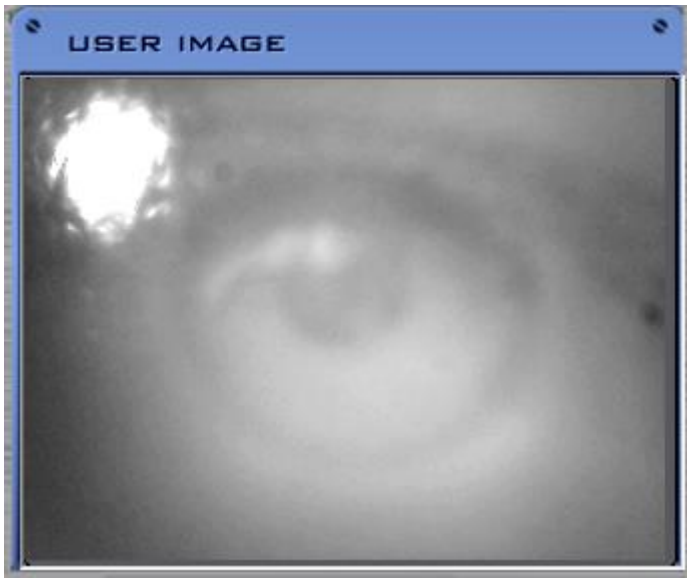
49. ábra: Az írisz működő másolata

A 49. és 50. ábrákon látható papírra nyomtatott képeket a tesztek alatt alkalmazott írisz azonosító élő (valóságos) mintának ismerte fel (az azonosítást sikeres volt)..



50. ábra: Írisz működő másolata

Az 51. ábrán a szoftver képernyőképe látható, amint az írisz azonosító elé egy fényképet helyeztem. A kapott kép nem volt elegendő kontrasztos az azonosításhoz. Megfigyelhető az eszközbe épített infra LED visszatükröződése is a felvételen.



51. ábra: Fénykép az írisz azonosító előtt

Az 52. ábra egy sikeres regisztrációt mutat, ezen az íriszazonosító egy olyan alakzatot látott írisznek, ami – a külső szemlélőként megfigyelve – egyáltalán nem tűnik annak.

Az e-kereskedelemben alkalmazható biometrikus azonosítók jó eséllyel olyan eszközök lesznek, amelyek valamilyen infratartományú képalkotást alkalmaznak. Ezért fontos az ilyen eszközök továbbfejlesztésének kérdése a jövőben.

52. ábra: Íriszazonosító által tévesen írisznek azonosított alakzat

A biometrikus azonosítás sérülékenységeit a 5. táblázat mutatja be.

Technológia	Módszer	Sérülékenység	Megjegyzés
Ujjnyomat	Grafitpor	Ujjnyomat otthagyása tárgyakon	Általában csak részleges minta található
Ujjnyomat	Viasz	Külső a biometrikus jegy	A személy beleegyezik, vagy tud a másolat készítéséről
Arc	Infra fotó	Külső a biometrikus jegy	Nehéz a megfelelő fotó elkészítése
Arc	3D maszk	Külső a biometrikus jegy	A személy beleegyezik, vagy tud a másolat készítéséről
Tenyérérhálózat	Infra fotó	Az eljárás publikus	Nehéz a megfelelő fotó elkészítése
Írisz azonosítás	Érme	Hibás algoritmus	Nehéz a megfelelő fotó elkészítése
Írisz azonosítás	Fotó	Élőminta felismerés hiánya	Nehéz a megfelelő fotó elkészítése

5. táblázat: A biometrikus technológiák sérülékenységei

3.3 Az eszközök fejlesztési lehetőségei

A biometrikus azonosítás lehetséges hiányosságait laboratóriumi mérések végzésével kutattam az infravörös tartományban végzett képalkotó módszerekkel. Ezen mérések jelentősebb eredményeit foglalja össze, elemzi és szintetizálja a fejezet.

3.3.1 Mérés az infrakamerával

A gyakorlatban a 780 nm és az 1 mm közötti elektromágneses sugárzást nevezzük infravörös sugárzásnak (IR). Az 1. számú melléklet az infra-tartomány elhelyezkedését ábrázolja az elektromágneses spektrumban.

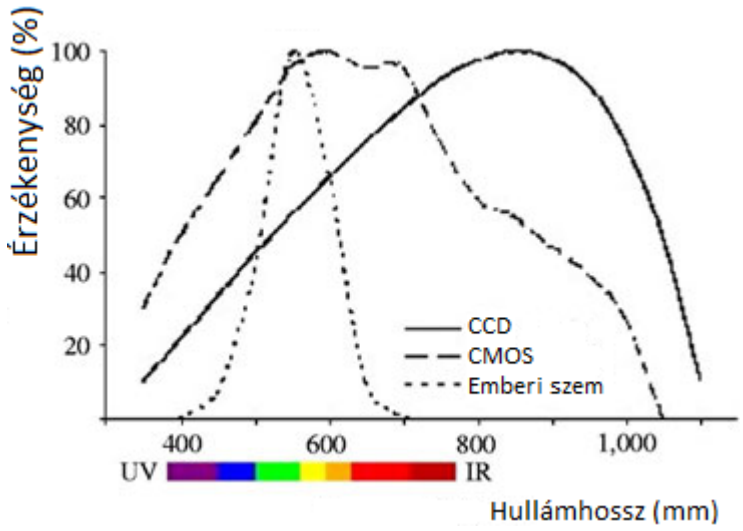
Az infravörös sugárzást William Herschel fedezte fel 1799-ben. Tanulmányai során megállapította, hogy a spektrumban az ibolyától a vörös felé haladva a színek hőmérséklete növekszik. Ezután megmérte a spektrum azon részének a hőmérsékletét, amelyik „túl van" a vörösön. Azt tapasztalta, hogy ez a terület melegebb volt, mint az emberi szemmel látható színek esetében. Ezzel bizonyította, hogy a nap nem csak olyan elektromágneses sugárzást tartalmaz, amely az emberi szem számára látható. [47]

Az infratartomány felosztása:

- A közeli infravörös sugárzás (NIR, IR-A) 0,75-1,4 μm hullámhosszúságú, amelyet az optikai kommunikációban használnak, mert csak enyhén gyengül üvegen keresztül haladva. A képi intenzivitás erős ebben a tartományban, ezért az éjjellátó szemüvegek is itt működnek.
- A rövid hullámhosszúságú infravörös sugárzás (SWIR, IR-B) a 1,4-3 μm. Gyengülése 1450 nm-nél következik be. az 1530-tól 1560 nm-ig tartó hullámhosszúságú fényt a telekommunikációban alkalmazzák.
- A közepes hullámhosszúságú infravörös sugárzás (MWIR, IR-C) 3-8 μm. Az infravörös önirányítású rakétáknál alkalmazzák. A rakéta fejére infraérzékelőt tesznek, ami azt az infravörös sugárzást észleli, ami sugárhajtóművek lángjánál tapasztalható.
- A hosszú hullámhosszúságú infravörös sugárzás (LWIR, IR-C) a 8-15 μm, melyet gyakran hőérzékelőként emlegetnek, mert egy passzív hőképet alakít ki, melyhez nem kell külső fényforrás, vagy hő.
- A távoli infravörös sugárzás (FIR) a 15-1000 μm-es hullámhosszok közé eső tartomány. [48]

A mérés célja, hogy elemezni tudjuk a biometrikus azonosítás legelső elemét, vagyis a képalkotást infra tartományban.

A mérésekhez saját készítésű kamerát építettem.



53. ábra: A CCD, CMOS és az emberi szem érzékenysége a hullámhossz függvényében ([49] alapján)

Az 53. ábrán látható, hogy maga a fényérzékelő elem, akár CCD, akár CMOS, az infratartományban is érzékeny. Ebből következik, hogy a leírt technológiát alkalmazva a képeken az emberi szem számára nem látható spektrumú összetevők is megjelennek, ami rontja a fénykép színhűségét. Ahhoz, hogy a színek színhelyesen jelenjenek meg a digitális képen, az infratartományt egy szűrővel levágják. Ez a szűrő a CCD vagy CMOS felületén található, vagy az az előtti lencserendszer része.

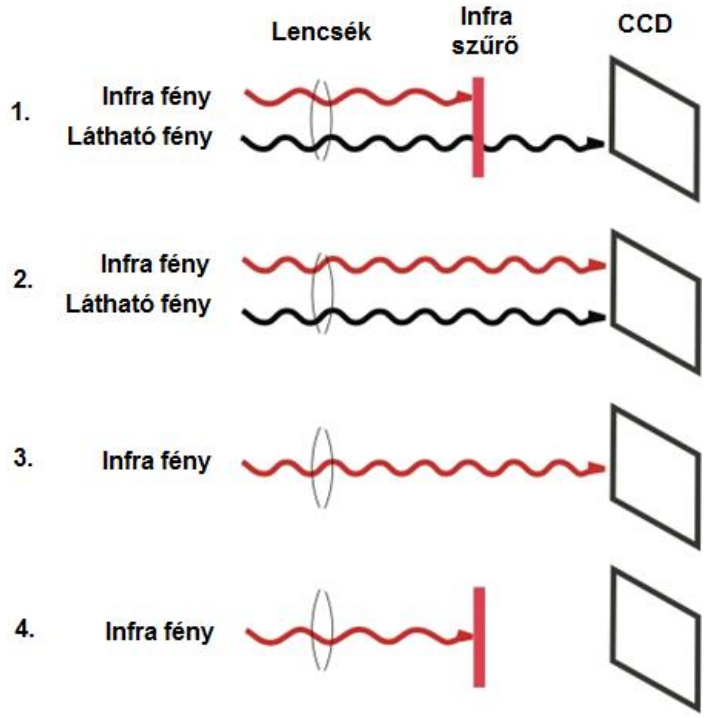
A saját méréseim során egy Hama gyártótól származó USB webkamerát alkalmaztam, amely egy manuális fókusszal rendelkező színes kamera. A gyártó a felbontást több módon is közli:

- 2 MP
- 720p HD
- 1600 · 1200 Pixel (interpolált felbontás: 3200 · 2400 Pixel).

Ahhoz, hogy egy kamera az infratartományban tudjon működni, számos lehetőség áll rendelkezésre. A következőkben egy lehetséges megoldást ismertetek.

Az 54. ábrán, az 1. számmal jelölt esetében a kamera normál működése tanulmányozható: a látható fény eljut a fényérzékelő elemig, az infratartományú fény azonban a lencsék mögött lévő infraszűrőn tud keresztül haladni. A 2. számmal jelölt esetben nincs a rendszerben infraszűrő. Ekkor a fény teljes spektrumban eljut a fényérzékelő elemig. Az általam alkalmazott megoldás esetében kizárólag infrafénnyel történik a vizsgált tárgy

megvilágítása, így a képalkotó elemen az infrafény jelentkezik (3. számmal jelölve). A 4. számú eset azt mutatja be, hogy az általam alkalmazott elrendezés a hagyományos, infraszűrővel rendelkező kamerák esetén nem alkalmazható.



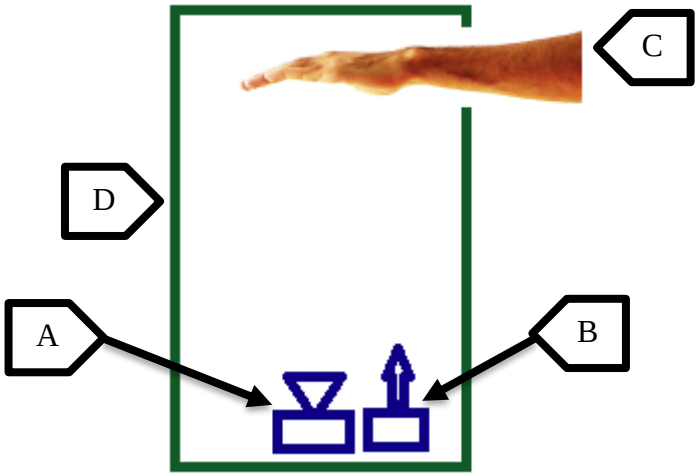
54. ábra: Az infrafény és a CCD képérzékelő elem

A méréseimhez eltávolítottam az infraszűrőt az optikából. Ehhez szétszereltem a webkamerát, majd a lencsét lecsavarva eltávolítottam a lencserendszerről az infraszűrő lapkát, amely egy teljesen sík, élénk zöld színű, vékony üveglap. Arra gondosan kellett figyelni, hogy a lencse a művelet során sértetlen maradjon, mert az a kép minőségét drasztikus mértékben rontaná. A mérés alatt alkalmazott kamera esetében ez a lencsesor legutolsó tagja, amely a képérzékelő elem oldalára esik.

Az 55. ábra a kamera által készített felvételt mutatja, amely a kéz tenyér felőli oldaláról készült. Jól megfigyelhető az érhálózat.

55. ábra: A kamera által készített felvétel a kéz tenyér felőli oldaláról

A mérés egy mérőkamrában (az 56. ábrán „D”-vel jelölve) zajlik, amely megfelelő vastagságú és feketére festett annak érdekében, hogy ne engedjen be a fényt a környezetből. A kamra felső részénél kivágás található, amely a tenyér (az ábrán „C”-vel jelölve) behelyezésére szolgál. A mérőkamra belsejében, alul foglal helyet az átalakított kamera (az ábrán „A”-vel jelölve). A tenyér megfelelő infratartományú megvilágítása a kamera mellett elhelyezett infra LED-el (az ábrán „B”-vel jelölve) történik. A tenyér és a kamera távolsága 70 cm. A mérőkamra szélessége 40 cm, mélysége pedig 40 cm. A mérések során több különböző infra LED-et is teszteltem, mindig egyszerre csak egyet. Az így kapott képek egymással összevethetők.



56. ábra: Az infra mérőkamra elvi rajza

A mérés során felhasznált infratartományban működő LED-ek a következők voltak:

LED megnevezése	**Hullámhossz [nm]**	**Sugárzási szög [°]**	**Sugárzás intenzitása [mW/sr]**
LED8	950	30	20
LED7	940	34	30 @ 20mA
LED6	890	10	140
LED5	880	30	20
LED4	860	30	40~100
LED3	850	10	230~420
LED2	850	30	40~100
LED1	850	50	18~45

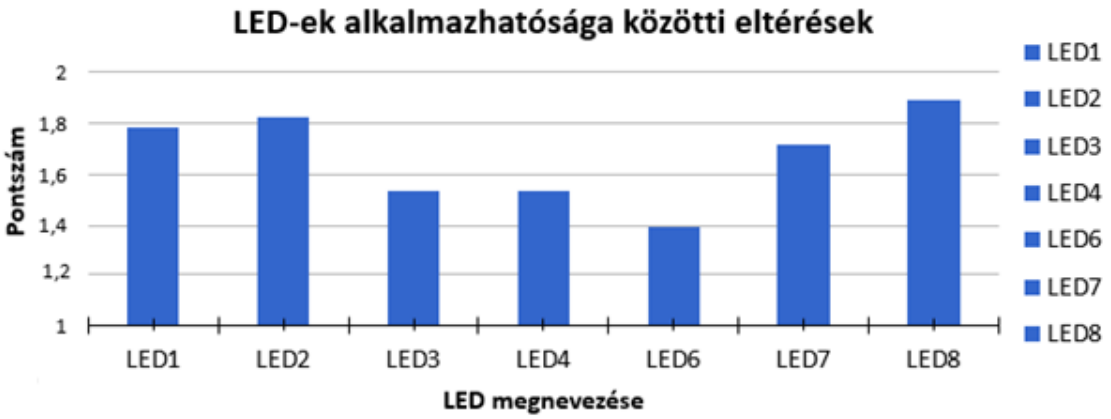
6. táblázat: A mérések során alkalmazott LED-ek

A mérések során 336 képet készítettem összesen 14 tenyérről (7 személy) 8 különböző LED-el (ezek paramétereit a 6. táblázat mutatja be). A méréseket háromszor ismételtem. Felvettem referenciaképeket is, melyek közül az erezetet nem mutató mintát 1 pontra értékeltem, míg a legkontrasztosabb képet 3 pontra (az alkalmazott skálát lásd a 2. számú mellékletben!). A LED5-el sajnos nem sikerült minden mérést elvégezni, ezért ez hiányzik az eredmények közül.

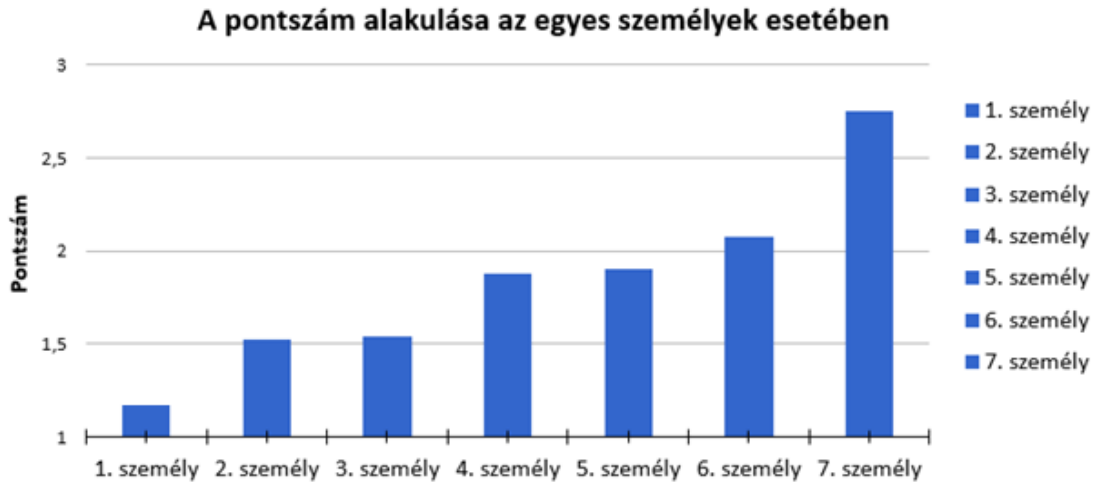
A tesztek során bebizonyosodott, hogy a 850 nm hullámhosszúságú LED-ek korlátozottan alkalmasak arra, hogy láthatóvá tegyük vele a tenyérérhálózatát. A konkrét mérési eredményeket az 57. és az 58- ábra mutatja be.

A mérést megismételtem más típusú LED-ekkel is. Ezek:

- LD271, 130 mA, 950 nm (sötét burkolattal);
- SF 484-2, 100 mA, 880 nm, (világos burkolattal).



57. ábra: A LED-ek alkalmazhatósága közötti eltérések



58. ábra: A pontszám alakulása az egyes személyek esetében

Tehát fontos szempont a megfelelő hullámhossz kiválasztása, mert az erek kontrasztos képe alapvetően ettől függ. A mérésekből kiderült, hogy az általam használt LED-ek hullámhosszúsága közül a 850 nm, és a 950 nm a legalkalmasabb a tenyér megvilágítására, így ezek ajánlottak az esetleges további mérések folytatására.

Szintén lényeges, hogy a LED egyenletes fényerősséggel világítson minden irányszögben.

A fény erősségének beállításánál mindenképpen figyelembe kell venni a kamera érzékenységét.

3.4 A Feladatorientált Biztonsági Küszöb (MOST) fogalmának bevezetése

A fejezet az általam kidolgozott szempontrendszert mutatja be annak megállapításához, hogy az egyes biometrikus technikák, illetve eszközök alkalmazhatók-e az e-kereskedelemben.

Az e-kereskedelmet számos biometrikus azonosítási módszerrel lehet biztonságosabbá tenni, amelyek azonban eltérő mértékben felelnek meg a feladatnak.

Néhány szempont triviális, így ezek szükséges feltételek: ilyen például az, hogy azonos eredménnyel reprodukálható legyen az azonosítás eltérő helyszíneken, napszaktól, megvilágítástól és a hőmérsékleti viszonyoktól függetlenül. [31, p. 80.]

3.4.1 A szempontrendszer alapja

Az egyes biometrikus azonosító eljárásokat különböző, e-kereskedelem orientált módon kialakított szempontok szerint szükséges vizsgálni.

A biometrikus eszközök vonatkozásában követelmény, hogy a megoldás legyen képes a fizető személyét egyértelműen és megbízhatóan azonosítani. A tenyérerezet és az írisz alapú azonosításról például elmondható, hogy olyan tulajdonságon alapulnak, amely nem változik az ember élete során. Technikailag mindkettő az infratartományban dolgozik, működésükhöz egy infra LED (panel) és egy infratartományban látó kamera szükséges.

Az E-kereskedelemben alkalmazható eszközöket – megítélésem szerint - 12 szempont alapján szükséges és elégséges vizsgálni, ezek a következők:

1. **Mindenkinél alkalmazható**. A lehetséges biometrikus minták az emberi test geometriai vagy viselkedéstani jellemzőiből származnak. Vannak, akiknél hiányzik ezek közül néhány, például az emberek öt százalékának nem rögzíthető az ujjnyomata. Ők azok a személyek (felhasználók), akik nem tudnak ujjnyomatra regisztrálni. A szempontot a failure to enroll (FTE) skaláris mennyiséggel jellemezzük. [25, pp. 29-30] [31, p. 80.] [50, pp. 6-7]

2. **Egyediség**. A biometrikus minta egyedisége biztosítja azt, hogy minden ember a világon megkülönböztethető. Tartalmazzon bármilyen nagyszámú elemet (felhasználót) egy adatbázis az egyes biometrikus minták egymástól határozottan el kell, hogy térjenek. Amennyiben a minták nagyon hasonlóak, az elfogadhatatlanul magas FAR-t és FRR-t fog eredményezni. [50, pp. 6-7] [25, pp. 29-30.]

3. **Eszköz mérete**. Mivel az e-kereskedelem nagyrészt mobil eszközökben használja a biometrikus eszközöket, ezért fontos, hogy az eszköz geometriai méretei ne legyenek kezelhetetlenül nagyok. Az alkalmazott eszközöknek kényelmesen el kell férniük egy íróasztalon (egérméretnél nem nagyobb), esetleg olyan technológiát kell alkalmaznia, ami a közeli jövőben okoselefonokba is integrálható lesz.

4. **Megbízhatóság**. A legfontosabb feladata a rendszernek, hogy a biometrikus mintát a lehető legnagyobb biztonsággal azonosítsa be. Minimálisan két indexet kell figyelembe vennünk, ezek a téves elfogadás (FAR), valamint a téves elutasítás (FRR). [51]

Néhány biometrikus rendszer FAR mutatója:

- hangazonosítás: 500 : 1,
- arcazonosítás (2D): 2.000 : 1,
- ujjnyomat-azonosítás: 1.000.000 : 1,
- íriszazonosítás: 10.000.000 : 1,
- retinaazonosítás: 10.000.000 : 1. [52]

Az adatbázisban tárolt mintáknak egymástól szignifikánsan el kell térniük. Ezen túlmenően az azonosításkor beolvasott mintának magas százalékkal hasonlítania kell a már eltárolt biometrikus mintára. Ezeknek a kritériumoknak minimálisan fenn kell állniuk, hogy nagy biztonsággal lehessen az adott felhasználót beazonosítani.

A FAR és az FRR jellemzőkből származtatható az EER[4] érték. Miután a FAR és az FRR értékek befolyásolhatók egy azonosítási küszöb beállításával (például egy ujjnyomat azonosnak tekinthető, ha a 30 minutia pontból 20 megegyezik, de akár 10-et is beállíthatunk küszöbnek – bár ez meglehetősen kockázatos) akár eszközönként is, ezért javasolt alapul venni az EER mutatót. [50, pp. 6-7] [53, pp. 567-571.]

[4] Az angol „Equal Error Rate” kifejezés kezdőbetűiből származik. Azt a pontot adja, ahol a FAR és az FRR értékei egyenlők egymással. [29] [53, pp. 567-571.]

5. **Változatlanság**. Sok biometrikus jellemző változik az idő múlásával, ilyen például a hang vagy az arc. Az írisz és az ujjnyomat ebből a szempontból stabilitást mutat. A hosszú távon jól működő biometrikus azonosítás feltétele, hogy olyan jellemzőt válasszunk, amely évtizedes intervallumot tekintve is változatlan marad. Amennyiben ez nem áll fenn (és nem történik meg a letárolt minta rendszeres aktualizálása), akkor magas lesz az FRR érték. [25, pp. 29-30.] [50, pp. 6-7]

6. **Elérhetőség**. Meghatározza, hogy a mintáról mennyire egyszerű elkészíteni az azonosításhoz szükséges képet. Nem minden biometrikus jellemző érhető el egyszerűen. Például retina azonosítás esetén közelről kell erős fénnyel a szembe világítani és közben képet készíteni a retináról. Ehhez képest például az arcfelismerés esetén a biometrikus minta elérhetősége jobb, hiszen ebben az esetben egy hétköznapi környezetben készül fénykép az arcról. [50, pp. 6-7]

7. **Elfogadottság**. Néhány eszköz érzelmi ellenállást, akár félelmet is kiválthat a felhasználó részéről. Az elfogadottság azt mutatja meg, hogy a rendszert használó személy mennyire hajlandó együttműködni az azonosítóval. A retina azonosítás például (ahol nagyon közel kell a szemet helyezni az eszközhöz) kevésbé számít közkedveltnek a felhasználók körében. [25, pp. 29-30.] [50, pp. 6-7]

8. **Belső biometrikus jellemző**. A belső biometrikus jellemzők kevésbé sérülékenyek (a másolat készítése nehéz, vagy lehetetlen), mint a külsők. A test felületén található biometrikus jellemzők könnyen leolvashatatlanná válhatnak külső fizikai vagy kémiai behatások révén. Ez rontja a biometrikus minta rendelkezésre állását. [31, p. 80.]

9. **A technológia kiforrottsága**. Néhány biometrikus technológia fejlődő fázisban van, tömeges elterjedésük még nem valósult meg. A kevésbé kiforrott technológiákat még nem tesztelték egymástól független kutatóhelyeken és a gyakorlatban, így előfordulhat, hogy olyan hiányosságai vannak az alkalmazott verziónak, amelyek miatt a megoldás nem működik megfelelő hatékonysággal.

10. **Élőminta felismerés**. A legtöbb biometrikus minta lemásolható valamilyen módszerrel. Fontos az, hogy a másolatokkal ne lehessen elérni sikeres azonosítást. Ennek érdekében valamilyen egyedi módszerrel meg kell győződni arról, hogy a biometrikus minta nem másolat. A technológia akkor jöhet számításba az e-kereskedelemben, amennyiben

a biometrikus mintáról lehetetlen készíteni működő másolatot (vagy legalábbis nagyon bonyolult). [50, pp. 6-7] [53, pp. 567-571.]

11. **Érintés nélküli technika**. A biometrikus eszközök megérintése a felhasználókban gyakran ellenállást vált ki. Ezért előny, ha a berendezés úgy képes az azonosításra, hogy a felhasználónak ahhoz nem kell hozzáérnie. [31, p. 80.]

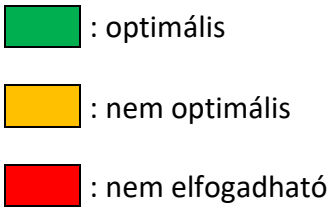
12. **Azonosítási idő**. Az azonosítási idő a technológiától függően változhat, azonban a DNS azonosítást leszámítva ezen intervallumok a célnak megfelelőek, mivel másodperc nagyságrendbe esnek. [31, p. 80.]

A 7. táblázatban az e-kereskedelemben alkalmazható biometrikus technológiák értékelésének 12 szempontja összegezve tekinthetőek át korrelációba hozva az egyes biometrikus azonosítási módszerek értékelésével.

	Szempontok	Írisz	Ere-zet	Arc	Ujj-nyo-mat	DNS	Alá-írás	Hang	Re-tina	Kéz geo-met-ria
1.	Mindenkinél alkalmazható									
2.	Egyediség									
3.	Eszköz mérete									
4.	Megbízhatóság									
5.	Változatlanság									
6.	Elérhetőség									
7.	Elfogadottság									
8.	Belső biometrikus jellem-zőt használ									
9.	A technológia kiforrottsága									
10.	Élőminta felismerés									
11.	Érintés nélküli									
12.	Azonosítás idő									

7. táblázat: A biometrikus módszerek alkalmazhatósága azonosításra az e-kereskedelemben – adott szempontrendszer alapján (A táblázatot a szerző készítette a fejezet szöveges részében hivatkozott irodalmak alapján)

Valamennyi szemponthoz három értékelési kimenet (válasz) rendelhető, nevezetesen:



A biometrikus eszközök jelentős része azonosítja a valóságos mintáról készült klónokat, illetve kvázi-mintákat kezel valóságosként. Ez az e-kereskedelemben túlzott, elfogadhatatlan kockázattal bír, ezek tehát nem alkalmazhatók erre a feladatra.

A fejezet alapján bevezethető (és célszerű is bevezetni) az adott feladathoz rendelt feladatorientált biztonsági küszöb (Mission Oriented Security Threshold: MOST) fogalma, amely azt adja meg, hogy egy adott biometrikus megoldás alkalmas-e egy meghatározott feladat ellátására.

Tehát adott esetben a biztonsági küszöböt az erezet, írisz, arc és ujjnyomat érik el. Látható az is, hogy az erezet és írisz jobban alkalmas a feladatra, mint az utóbbiak.

A „nem elfogadható” értékelést kapott technológiákat kizárjuk. Ezután a szempontok újra vizsgálatánál a megfelelő és az elfogadható válaszok száma szerint kiválasztjuk a legmegfelelőbb technológiát. A 7. táblázat alapján megállapítható, hogy a követelményeknek leginkább az erezet azonosítás fele meg.

BEFEJEZÉS

Az értekezés összegezi a több éves laboratóriumi kutatómunkám során összegyűjtött eredményeket, rendszerezi a tapasztalataimat és megadja az eredmények hasznosítási lehetőségeit.

Kiindulásképpen elemeztem a tudományterületen fellelhető irodalmakat, majd a hiányos területeken kutatásokat végeztem.

A munkám során célul tűztem ki, hogy elemzem az e-kereskedelem jelenlegi helyzetét, megállapítom annak gyenge pontjait. Kimutattam, miként lehet hatékonyan növelni az elektronikus kereskedelem biztonságát a biometrikus azonosítás integrálásával.

Elemeztem és értékelem az egyes biometrikus technikákat, technológiákat, hogy eldönthető legyen, melyik alkalmas a biztonságos e-kereskedelmi tranzakciók lebonyolításának feladatára. Elkészítettem az eszköz azonosítási folyamatba illesztési protokollját. Végső soron: egy olyan alkalmazást alkottam meg, amely alkalmas rá, hogy a jövőben a jelenlegi azonosítási módszereket kiváltja.

Munkámban bemutattam az e-kereskedelem felfutását, majd jelenlegi helyzetét. Ezt követően az e-kereskedelem technikai felépítéséről írtam. A biztonságot úgy növelem, hogy megvizsgálom a rendszer sérülékeny pontjait, amelyre megoldást javaslok. Ezt követően az e-kereskedelemben alkalmazott biometrikus azonosítási módokat mutatom be, kitérve az egyes technikák jellemzőire. Vizsgáltam az eszközözket és a köztük zajló kommunikációt is.

Meghatároztam a szempontrendszert az e-kereskedelem vásárlói oldalán alkalmazható biometrikus azonosítókhoz. Ezen belül vizsgáltam a minta megfelelőségét, a másolt minta elkészítésének lehetőségét. A fejezetben kitértem a lehetséges fejlesztési irányokra is.

Meghatároztam a Feladatorientált Biztonsági Küszöböt (MOST), amely megadja, hogy egy adott eszköz alkalmas-e a megadott feladat ellátására vagy sem. Ennek folyamán 12 e-kereskedelemre specifikus szempontot fogalmaztam meg, melyet 9 különböző technikán vizsgáltam.

A vizsgálat eredményeképpen meghatároztam, hogy az erezet és az írisz azonosítás az, amelyek az e-kereskedelemben történő alkalmazásnak megfeleltek.

A kutatásaimat 2019. március 13-án zártam.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Új tudományos eredmények (tézisek)

1. tézis: Megalkottam a „feladatorientált biztonsági küszöb” (Mission Oriented Security Threshold - MOST) fogalmát biometrikus eszközökre.

2. tézis: Elsőként adtam meg vizsgálati szempontrendszert az egyes biometrikus technikák, illetve eszközök alkalmazhatóságára az e-kereskedelemben.

3. tézis: Elsőként dolgoztam ki háromszintű értékelési eljárást a biometrikus eszközök, módszerek biztonsági megfelelőségének meghatározására.

További gondolatok

Jelenleg ahhoz, hogy az e-kereskedelmi rendszerek a jövőben is olyan piaci sikereket érhessenek el, mint a múltban és fenn tudják tartani ezt a töretlen fejlődést, arra van szükség, hogy a biztonságukat folyamatosan fejlesszük. Erre nyújt egy lehetőséget a biometrikus azonosítás bevezetése a fizető személy minden kétséget kizáró megnevezésére.

Várható, hogy a meglévő biometrikus módszerek változni fognak, valamint a jövőben új, eddig nem létezők fognak megjelenni. Ezek kockázatait és alkalmazási lehetőségeit folyamatosan érdemes nyomon követni.

Látható, hogy az eddigi asztali számítógép alapú e-kereskedelmet a mobil alapú kezdi felváltani, amelyen már nem csak böngészőből, hanem a kereskedő által fejlesztett alkalmazásokból is elérhető. Ezen új felületek új vizsgálandó területet képeznek. Az okostelefon felületekre fejlesztett alkalmazások már használhatják a biometrikus azonosítást, ennek a területnek a vizsgálata is javasolt.

Napjainkban egyre több mesterséges intelligenciával rendelkező eszközt mutatnak be. Csak idő kérdése, hogy ezek mikor terjednek el az e-kereskedelemben. Ezen terület kutatása soha nem volt egyszerű, várhatóan a jövőben ennek a területnek a feltérképezésére is nagy igény várható.

FELHASZNÁLT IRODALOM

[1] Kovács Tibor: A biometrikus azonosítás alkalmazhatósága napjainkban, Nemzetközi Gépész és Biztonságtechnikai Szimpózium, Budapesti Műszaki Főiskola, 2007. november 14., CD ISBN 978-963-7154-68-3.

[2] Khalid Saeed and Tomosana Nagashima, Biometrics and Kansei Engineering, Springer, 2012, ISBN 978-1-4614-5607-0.

[3] Krebs, Brian. Hanging Up on Mobile in the Name of Security. Krebs on Security, 16 Aug. 2018, https://krebsonsecurity.com/2018/08/hangingup-on-mobile-in-the-name-of-security/.

[4] Horváth Attila: Az elektronikus pénz, mint az elektronikus kereskedelmet támogató speciális fizetési rendszer, Ph.D. értekezés, Budapest, 2007.

[5] Varga Diána: Az internetes kereskedelem történelme, jeletősége és fejlődése, BGF szakdolgozat, Kereskedelmi és Szakmenedzser szak, 2011.

[6] Statista: Retail e-commerce sales worldwide from 2014 to 2021 https://www.statista.com/ statistics/ 379046/ worldwide-retail-e-commerce-sales/ Letöltés: 2017.10-hó.

[7] World Bank. 2017. World Development Indicators 2017. Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/26447 License: CC BY 3.0 IGO.

[8] http:// www.nfh.hu/ magyar/ informaciok/ vizsgalati/ 2012_ellenorzes/ jelentes_eker_2023.html, Letöltés ideje: 2012. december.

[9] http://www.nfh.hu/ informaciok/ hirek/ nap_111117_1.html, Letöltés ideje: 2012. december.

[10] Simon Kemp: Digital trends 2019: Every single stat you need to know about the internet, Singapore, https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/.

[11] Worldometers: World Population http://www.worldometers.info/world-population/.

[12] Verizon Data Breach Investigations Report 2016, Elérhetőség: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, Letöltés ideje: 2016 július.

[13] http://www.bankrate.com, Letöltés ideje: 2015. január.

[14] Military Standard - Reliability Program for Systems and Equipment Developement and Production, Washington D. C. MIL-STD- 785B.

[15] 2013 Data breach investigations report – North American Industry Classification System, Verizon enterprise DBIR Insider document.

[16] Őszi Arnold, Kovács Tibor: Sérülékenységi vizsgálatok az e-kereskedelem és a biometria területén, Tavaszi Biztonságtechnikai Szimpózium 2013, ÓBUDAI EGYETEM, Budapest, 2013. április 10. ISBN 978-615-5018-53-4.

[17] Ms. Ruchi Oberoi, Ms. Sharmistha Dey, Shourabh Sholliya: Privacy and Security Issues in E-Commerce: A Survey, National Institute of Technical Teachers Training & Research, Chandigarh, India (MHRD, Govt. of India), 2017. május 21, ISBN: 978-81-934083-0-8.

[18] International Conference on New Frontiers of Engineering, Science, Management and Humanities (ICNFESMH-2017).

[19] Biztonságpiac évkönyv 2015, Felelős kiadó: Radványi Róbert, ISSN 2061-6082.

[20] Őszi Arnold: Személyes adatok korszerű informatikai védelmének elmélete, Securinfo magazin, megjelenés: 2013. január 30. http://securinfo.hu/termekek/it-biztonsag/923-titkositas-1.html, Letöltés ideje: 2016. július.

[21] Őszi Arnold: Személyes adatok korszerű informatikai védelme a gyakorlatban, Securinfo magazin, megjelenés: 2013. február 10. http://securinfo.hu/termekek/it-biztonsag/929-szemelyes-adatok-vedelme-gyakorlatban.html, Letöltés ideje: 2016. július.

[22] Őszi Arnold: A PayPass bankkártyás fizetési módszer biztonságtechnikai elemzése, Bolyai szemle folyóirat, 2011. XX.évf. 1.szám, ISSN 1416-1443.

[23] Harshit Jhaveri, Hardik Jhaveri, Dhaval Sanghavi: Biometric security system and its applications inhealthcare, International Journal of Technical Research and Applications, Volume 2, Issue 6 (Nov-Dec 2014), e-ISSN: 2320-8163.

[24] Gyarmati Ervin, Kreisz Gábor: Az informatikai biztonság helyzete Magyarországon, Taksony, 2006.

[25] A. K. Jain, A. A. Ross and K. Nandakumar: Introduction to Biometrics, New York: Springer, 2011, ISBN : 978-0-387-777326-1.

[26] Nermin K. Negied: Human Biometrics: Moving Towards Thermal Imaging, International Journal of Recent Technology and Engineering (IJRTE),Volume-2, Issue-6, January 2014, ISSN: 2277-3878.

[27] Balla József: Biztonság növelése a határforgalom-ellenőrzésben. (Határrendészeti Tanulmányok HU ISSN 1786-2345 /nyomtatott, HU ISSN 2061-3997 /online/ 2010., VII. évfolyam 1. szám - p. 97-105).

[28] Feng, J. & Jain, A. K.: Fingerprint Reconstruction: From Minutiae to Phase, IEEE Trans. On Pattern Analysis And Machine Intelligence, Vol. 33, No. 2, FEB. 2011.

[29] Őszi Arnold: Az e-kereskedelem elvárásai a biometriával szemben, MEB 2014, 12th International Conferenceon Management, Enterprise and Benchmarking, Budapest, Hungary, 2014. Május 30-31, HU ISSN 2061-9499.

[30] R. Cappelli, D. Maio, D. Maltoni, J.L.Wayman, and A.K. Jain.: Performance evaluation of fingerprint verification systems. IEEE Transactionson Pattern Analysis and Machine Intelligence, 28(1):3–18, 2006.

[31] Balla József rendőr alezredes: A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- és közbiztonság alakulására, Doktori (PhD) értekezés, NKE, Hadtudományi Doktori Iskola, Budapest, 2013.

[32] Anil K. Jain, PatrickFlynn, Arun A. Ross: Handbook of Biometrics, Springer kiadó, 2008, ISBN-13: 978-0-387-71040-2.

[33] Árendás - Bachraty - Jeges - Körmöczi - Molnár - Barczikay - Demcu - Csurgay - Szász - Máté - Nehéz - Posony - Tizedes - Veresegyházi: Integrált biometrikus azonosító rendszerek. Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, 2005.

[34] Otti Csaba, Őszi Arnold, Nagy Attila Lajos: iEvo ujjnyomat olvasó gyorstesztje, Securinfo, http://securinfo.hu/tesztek/158-teszt/819-ievo-ujjnyomat-olvaso-gyorstesztje.html Megjelent: 2012. szeptember 06. Letöltés ideje: 2012. október.

[35] Rathgeb Christian, Uhl Andreas, Wild Peter, Iris Biometrics: From Segmentation to Template Security, Springer, 2012, ISBN: 978-1-4614-5570-7.

[36] Csercsa Richárd, Lombai Ferenc, Szilágyi Tünde: Biometrika, Írisz alapú személyazonosítás, PPKE-ITK, 2004. december 16.

[37] Fénykép, http://media.t3.com/img/resized/lu/xl_Lumia950XL-03-650-80.JPG.

[38] Sean Cameron: Microsoft Lumia 950 XL review: a top phone if it wasn't for Windows 10 Mobile, 2015. december 17, http://www.t3.com/reviews/microsoft-lumia-950-xl-review, Letöltés ideje: 2016. július.

[39] Őszi Arnold: A biometria alapú munkaidő-nyilvántartás elmélete és gyakorlata, Hadmérnök, ZMNE, Budapest, 2011. VI. évf. 1. szám, ISSN 1788-1919.

[40] C. Simon and I. Goldstein, “A new scientific method of identification,” New York State Journal of Medi-cine, vol. 35, no. 18, 1935..

[41] DNS-ujjlenyomatok, 1999. szeptember, http://www.kfki.hu/~cheminfo/hun/hir/cikk/dns.html Letöltés ideje: 2012. december.

[42] Dr. Husi Géza, Dr. Szemes Péter Tamás, Bartha István Ákos: Épületfelügyelet és biztonságtechnika, TERC Kft. Budapest, 2013, ISBN 978-963-9968-65-3.

[43] Kovács Tibor, Őszi Arnold, Leung Yuen Ting: Dependence on tecnical parameters of the conditions of application of biometrical identification devices, Bánki Közlemények, Óbudai Egyetem, Budapest, 2011. november 15. ISBN 978-615-5018-27-5.

[44] https://www.moi.gov.qa/site/arabic/departments/pad/resources/images/2012/12/08_27247.jpg, Letöltés ideje: 2016. július.

[45] Otti Csaba, Őszi Arnold: Fingerprint security, IESB 2011, International Engineering Symposium at Bánki, Bánki Kari Tudományos Konferencia, Óbudai University, 2011. november 15-16. ISBN 978-615-5018-15-2.

[46] http://jap.physiology.org/content/92/1/372, Letöltés ideje: 2014. október.

[47] Az infrasugárzásról, http://www.infrafilm.hu/technologia.html, Letöltés ideje: 2016. július.

[48] R. Paschotta: Infrared light, Encyclopedia of Laser Physics and Technology, 1. edition October 2008, Wiley-VCH, ISBN 978-3-527-40828-3.

[49] CCD spektrum, http://gitthailand.com/image/ccd-spectrum.jpg, Letöltés ideje: 2014. december.

[50] David Zhang Guangming Lu: 3D Biometrics - Systems and Applications. Springer, Hong Kong, 2013, ISBN 978-1-4614-7399-2.

[51] Shuo Wang and Jing Liu: Biometrics on mobile phone, Recent Application in Biometrics, Dr. Jucheng Yang (Ed.), InTech, 2011, ISBN: 978-953-307-488-7.

[52] Kovács Tibor: A biometrikus azonosítás alapjai, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Alkalmazott Biometria Intézet (Applied Biometrics Institute – ABI), Digitális jegyzet, Budapest 2014.

[53] Őszi Arnold, Kovács Tibor: Theory of the Biometric-based Technology in the field of e-commerce, CINTI 12th IEEE International Symposium, Óbuda University, 2011. november 21-22, ISBN: 978-1-4577-0043-9.

[54] Sánta Imre: Optika és látórendszerek, EDUTUS Főiskola,TÁMOP-4.1.2, 2012 https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0017_45_optika_es_latorendszerek/ch01s03.html Letöltés ideje: 2018.11-hó.

[55] Zeitz, C., Scheidat, T., Dittmann, J., Vielhauer, C., Agulla, E., Muras, E., Mateo, C. & Alba Castro, J.: Security issues of internet-based biometric authentication systems, Electronic Imaging, 2008.

[56] Kovács Tibor: Személyazonosítás biometriai lehetőségei, Magyarországi Biztonsági Vezetők Egyesülete, 17. konferencia, Lillafüred, 2016. május 11.

[57] Az elekromágneses tartomány, http://arekold.amk.uni-obuda.hu/opto/2_EM_Spektr_files/TeljesEMS.png, Letöltés: 2014. november 25.

[58] Dr. Erdődi László: Exploit írás, http://nik.uni-obuda.hu/exploitwriting/ Letöltés ideje: 2016. augusztus.

[59] Global B2C E-commerce Report 2016, Ecommerce Foundation, Amsterdam, www.ecommercefoundation.org/reports.

[60] C. Simon and I. Goldstein, “A new scientific method of identification,” New York State Journal of Medi-cine, vol. 35, no. 18, pp. 901–906, 1935..

RÖVIDÍTÉSJEGYZÉK

DNS: az elnevezés a dezoxiribonukleinsav szóból származik. Elnevezése az angol nyelvű szakirodalomban DNA vagy teljes nevén deoxyribonucleic-acid.

FAR: Az angol „False Acceptance Rate" (téves elfogadás) kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a nem jogosult felhasználót jogosultként.

FRR: Az angol „False Rejection Rate" (téves elutasítás) kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a jogosult felhasználót nem jogosultként.

EER: Az angol „Equal Error Rate" kifejezés kezdőbetűiből származik. Azt a pontot adja, ahol a FAR és az FRR értékei egymással egyenlők. [53, pp. 567-571.] [29]

TCP/IP: Az internet protokoll, a TCP/IP betűszó angol rövidítésből keletkezett: Transmission Control Protocol / Internet Protocol (átviteli vezérlő protokoll/internet protokoll). A TCP/IP egy olyan protokollkészlet, amely arra lett kidolgozva, hogy hálózatba kapcsolt számítógépek egymás között megoszthassák erőforrásaikat.

A TCP/IP protokoll két alrendszere az alábbi feladatokat látja el:

- A **TCP** a küldő számítógépen a továbbítandó adathalmazt darabolja fel adatcsomagokra, és az adatcsomagokat címkézi. Az adatokat fogadó számítógépen a kapott adatcsomagokat összerakja, és így előállítja az eredeti adathalmazt.

- Az **IP** (internet protokoll) az adatcsomagokat irányítja, a kommunikációban résztvevőket azonosítja. Az IP állapotmentes protokoll, nem garantálja a csomagok megérkezését a célzotthoz, és azt sem, hogy az elküldött csomagok ugyanolyan sorrendben érkeznek meg, mint ahogyan elküldésre kerültek. [16, pp. 1-7.]

MOST: Mission Oriented Application

ÁBRAJEGYZÉK

A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

Sorszámozott lista a szerzők, a cím, valamint a megjelenés helyének feltüntetésével.

Tudományos és szakmai folyóirat megjelenések

1. PHUOC DAI HUU NGUYEN, Lourdes Ruiz, Arnod Őszi: „**Biometrics Acquisition in a Hungarian University: The Óbuda University Case - Bánki Donát Faculty**", BÁNKI KÖZLEMÉNYEK 1 : 1 pp. 30-33. , 4 p. (2018) Közlemény:3381961 Őszi Arnold, Lourdes Ruiz S: „**Biometric uses in occupational safety and health",** Hadmérnök folyóirat, pp. 1-9. Lektorált, magyar nyelvű folyóiratcikk – ISSN 1788-1919 (2016) Nyelv: Angol
2. Őszi Arnold, Lourdes Ruiz S: BIOMETRIC USES IN OCCUPATIONAL SAFETY AND HEALTH, HADMÉRNÖK 11 : 4 pp. 1-9. , 9 p. (2016), Közlemény:3152611 Nyelv: Angol
3. Dr. Horváth Sándor, Dr. Kovács Tibor, Dr. Szűcs Endre, Őszi Arnold, Vetési Vivien, Bartus Attila, „**Sikeres múlt, bíztató jelen, impozáns jövőkép – 20 éves a biztonságtechnikai mérnökképzés,**" *Detektor plusz szakmai szakfolyóirat,* 2014. 21. évfolyam 1. szám, pp. 10-12., ISSN 1217-9175, Kiadó: Typon International Kft.
4. Kovács T., Őszi A.: „**Positioning: the common problem of biometrical identification devices: Fingerprint, handgeometry, iris and palm vein**" Tavaszi Biztonságtechnikai Szimpózium 2014: Bánki Közlemények. Konferencia helye, ideje: Budapest, Magyarország, 2014.04.04 Budapest: Óbudai Egyetem, 2014. pp. 1-9. (ISBN:978-615-5460-03-6) Nyelv: Angol
5. Otti Csaba, Őszi Arnold, „**Sérülékenységi vizsgálatok az arcazonosítás terén,**" *Detektor plusz szakmai szakfolyóirat*, 2013. 20. évfolyam. 6. szám, pp. 10-11., ISSN 1217-9175, Kiadó: Typon International Kft. http://www.detektorplusz.hu/
6. Őszi Arnold, „**Személyes adatok korszerű informatikai védelme a gyakorlatban,**" 2013. február 10. - magyar nyelvű lektorált folyóiratcikk - http://securinfo.hu/termekek/it-biztonsag/929-szemelyes-adatok-vedelme-gyakorlatban.html
7. Őszi Arnold, „**Személyes adatok korszerű informatikai védelmének elmélete"** *Securinfo magazin* 2013. január 30. - http://securinfo.hu/termekek/it-biztonsag/923-titkositas-1.html - magyar nyelvű lektorált folyóiratcikk
8. Otti Csaba, Őszi Arnold, Nagy Attila Lajos, „**iEvo ujjnyomat olvasó gyorstesztje**" 2012. szeptember 06. - - Securinfo - http://securinfo.hu/tesztek/158-teszt/819-ievo-ujjnyomat-olvaso-gyorstesztje.html
9. Őszi Arnold, „**Identivision ICR-E42 és ICR-163 DVR-ek**" *Securitymag – Szakmag - Tesztek (Security Magazine)* 2012. március 12. - Óbudai Egyetem - Link:

http://www.securitymag.hu/szakmag/tesztek/140-identivision-icr-e42-es-icr-163-dvr-ek

10. Őszi Arnold, „**A biometria alapú munkaidő-nyilvántartás elmélete és gyakorlata**” Hadmérnök folyóirat: 2011. március - VI. évf. 1. szám:. - Lektorált, magyar nyelvű folyóiratcikk – ISSN 1788-1919 - p. 90-95
11. Őszi Arnold, „**A PayPass bankkártyás fizetési módszer biztonságtechnikai elemzése**” Bolyai szemle folyóirat: 2011. - XX. évf. 1. szám: - p. 153-162. Lektorált, magyar nyelvű folyóiratcikk ISSN 1416-1443

Konferenciák

1. Őszi Arnold, „**Az e-kereskedelem elvárásai a biometriával szemben”** *MEB 2014 – 12th International Conference on Management, Enterprise and Benchmarking,* Budapest, Hungary, 2014 Május 30-31, pp. 1-10., HU ISSN 2061-9499, Magyar nyelvű konferencia előadás, konferencia kiadványban lektorált magyar nyelvű tudományos cikk
2. Otti Csaba, Fehér András, Őszi Arnold, „**Face recognition systems**” *Hacktivity* 2013. október 11. – Budapest – Kiadványban megjelent, előadás magyar nyelven
3. Őszi Arnold, Kovács Tibor, „**SÉRÜLÉKENYSÉGI VIZSGÁ-LATOK AZ E-KERESKEDELEM ÉS A BIOMETRIA TERÜLETÉN**” 2013. április 10. TAVASZI BIZTONSÁGTECHNIKAI SZIMPÓZIUM 2013, ÓBUDAI EGYETEM - Budapest - - Magyar nyelvű konferencia előadás, konferencia kiadványban lektorált magyar nyelvű lektorált tudományos cikk megjelent: 1-7 oldal - ISBN 978-615-5018-53-4
4. Őszi Arnold (PhD aspiráns, Óbudai Egyetem), Kovács Tibor (CSc/PhD, Óbudai Egyetem), „**A jelen kor titkosítási módszerei az informatikában** (Encrypting methods of the information technology in the present)”– *Magyar Tudomány Ünnepe 2012 Konferencia az Óbudai Egyetemen, Biztonságtechnikai szekció,* 2012. november 26. 15:30 ISBN: 978-615-5018-46-6
5. Otti Csaba, Fehér András, Őszi Arnold, Milák István – „**A biometria biztonsága és sérülékenysége**” *Hacktivity* 2012. október 12. – Budapest – Kiadványban megjelent, előadás magyar és angol nyelven - ISBN 978-963-08-4920-3
6. Kovács Tibor, Őszi Arnold, Leung Yuen Ting, „**Biometrikus eszközök műszaki paramétereinek függése az alkalmazási körülményektől** (Dependence on tecnical parameters of the conditions of application of biometrical identification devices)”, *BÁNKI KÖZLEMÉNYEK 2011 - Óbudai Egyetem, Plenáris ülés*, Budapest, Népszínház út 8. - 2011. november 15. - pp. 1-10. - dokumentum típusa: Folyóiratcikk/Szakcikk - magyar nyelvű előadás, angol nyelvű lektorált konferencia-kiadvány és tudományos cikk - ISBN 978-615-5018-27-5
7. Őszi Arnold, Kovács Tibor, „**Theory of the Biometric-based Technology in the field of e-commerce**” *Óbuda University – CINTI 2011 – 12th IEEE International Symposium on Computational Intelligence and Informatics* -2011. november 21-22. - ISBN: 978-1-4577-0043-9- Konferencia kiadvány és lektorált tudományos cikk angol nyelven megjelent

8. Otti Csaba, Őszi Arnold, „**Fingerprint security**” *Óbudai University - IESB 2011 - International Engineering Symposium at Bánki - Bánki Kari Tudományos Konferencia,* 2011. november 15-16 - ISBN 978-615-5018-15-2., Konferencia kiadvány és lektorált tudományos cikk magyar nyelven megjelent.
9. Otti Csaba, Őszi Arnold, **„Fingerprint Identification Systems, Security or Security Leak**,” 2011. szeptember 17-18, Hacktivity The Largest Hacker Conference in Central and Eastern Europe. Budapest, Előadás és konferencia kiadvány magyar és angol nyelven
10. Őszi Arnold, „**Mohi atomerőmű biztonságtechnikai felülvizsgálata (a TDK munka továbbdolgozása)”** *Jánossy Ferenc Szakkollégium (JFSZK)* 2011. március 18. Magyar nyelvű konferencia kiadványban megjelent.
11. Őszi Arnold (Biztonságtechnikai mérnök szak, MSc, I. évfolyam), „**Mohi atomerőmű biztonságtechnikai felülvizsgálata**” *Budapesti Műszaki Főiskola - Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar - Gépszerkezettani és Biztonságtechnikai Intézet - TUDOMÁNYOS DIÁKKÖRI DOLGOZAT (TDK),* 2009.11.12. Konzulens: Dr. habil Kovács Tibor, MSc, BSc szakirány felelős – pp.: 1-49

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném megköszönni mindazoknak, akik önzetlenül segítettek az értekezésem megírásában. Név szerint Prof. Dr. Kovács Tibor egyetemi docensnek, hogy vállalta a témavezető szerepét és hogy részt vehettem mellette számos kutatásban, hasznos ötleteivel támogat engem és alapos odafigyeléssel ellenőrzi és segíti a munkámat.

Köszönöm az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának, Prof. Dr. Rajnai Zoltánnak. Továbbá az Alkalmazott Informatikai és Alkalmazott Matematikai Doktori Iskolájának, valamint az Alkalmazott Biometria Intézetének, hogy megteremtették az inspiráló kutatáshoz és tudományos munkához a szükséges feltételeket.

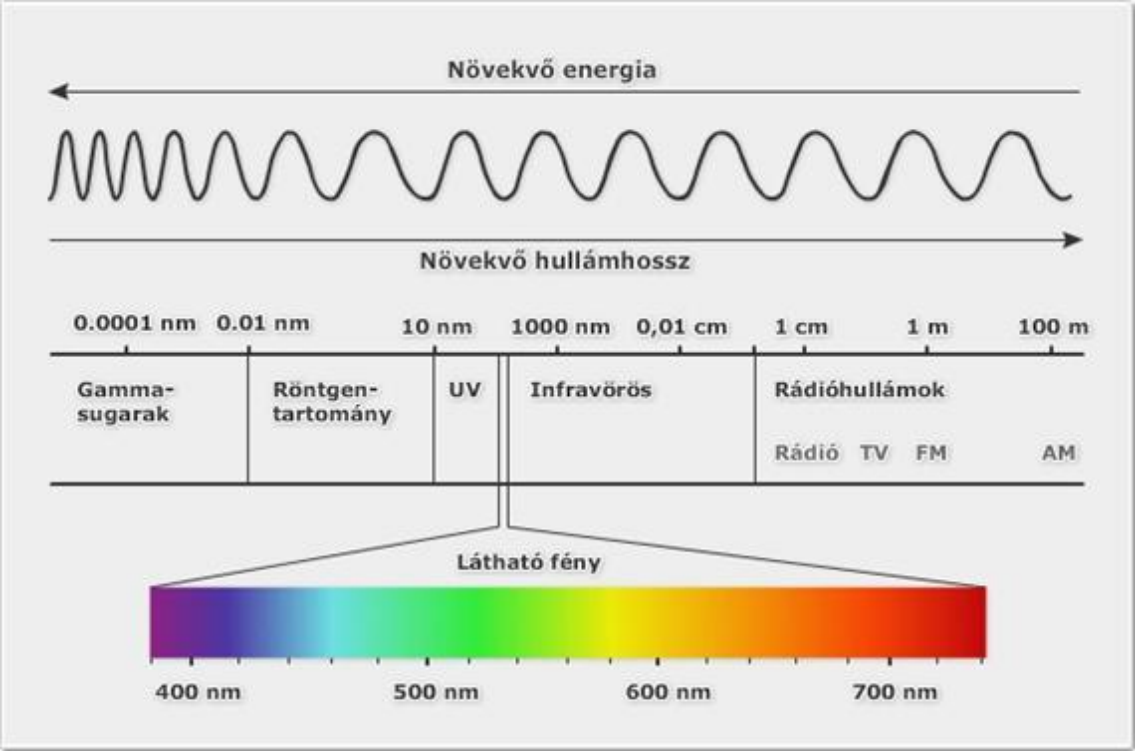
Rajtuk kívül az értekezésem megírásában igen sok támogatást kaptam számos PhD hallgatótól, ezúton köszönöm nekik is mindennapi értékes segítségüket.

Köszönöm továbbá családomnak, barátaimnak és ismerőseimnek mindennemű segítségét, támogatását – nélkülük biztosan nem jutottam volna el idáig.

Legvégül, de nem utolsó sorban köszönettel tartozom az Óbudai Egyetemen dolgozó valamennyi kedves munkatársamnak, kollégámnak, akik egy nagyon jó hangulatú munkahelyi környezetet kialakítva segítettek át a nehéz pillanatokon.

1. SZÁMÚ MELLÉKLET

Az elektronmágneses tartomány. [54]



2. SZÁMÚ MELLÉKLET

 1 – Legrosszabb minőség: egy ér sem látható

 2 – Elfogadható minőség: Az erek részben láthatóak.

 3 – Kiváló minőség: A tenyéren lévő erek jól láthatóak