

Biometria a számítógépes személyazonosításban  
- vizuális módszerek

Czúni László

2015. február 7.

A jegyzetet készítette: Dr. Czúni László, egyetemi docens, Pannon Egyetem, Műszaki Informatikai Kar, Képfeldolgozás Kutatólaboratórium

Lektorálta: Dr. Várady Géza, tanszékvezető egyetemi docens, Pécsi Tudományegyetem

2. (javított) kiadás, 2015.

keplab.mik.uni-pannon.hu

A tananyag a TÁMOP-4.1.2.A/1-11/1-2011-0104 "A felsőfokú informatikai oktatás minőségének fejlesztése, modernizációja" című projekt keretében a Pannon Egyetem és a Szegedi Tudományegyetem együttműködésében készült.



# Köszönetnyilvánítás

Végtelen köszönet illeti Családomat a végtelen türelemért...



# Előszó

A Pannon Egyetemen (korábban Veszprémi Egyetem) Szirányi Tamás vezetésével kezdődött a biometria oktatása a 90-es évek második felében műszaki informatikus hallgatóknak. Tudomásunk szerint Magyarországon ez volt az első egyetemi kurzus, amelyet kimondottan ennek a tárgykörnek szenteltek. Veszprémben a bolognai rendszer bevezetése után mérnök informatikus MSc hallgatók vehetik fel választható tárgyként a Biometria a számítógépes személyazonosításban című tárgyat. Könyvünk célja elsősorban ennek a kurzusnak a támogatása magyar nyelvű írásos anyaggal, ugyanakkor reméljük, hogy más egyetemek és főiskolák informatikus, villamosmérnök vagy programozó informatikus hallgatói is szívesen veszik kezükbe és használják tanulmányaik során.

A jegyzet írása során igyekeztem azokat a tapasztalatokat és gondolatokat is beépíteni a könyvbe, amelyek az elmúlt tíz évben az egyetemi munkáim és az előadások során fogalmazódtak meg bennem. Remélem, ezzel nem csak a tankönyv szubjektivitása nőtt, hanem a jelenségek és fogalmak, ill. azok egymáshoz való kapcsolatának az érthetősége is javult.

A könyv számos irodalmi hivatkozást tartalmaz. Ezek nagy része - néhány kivételtől eltekintve - angol nyelvű anyag, így aki mélyebben szeretne megismerkedni egy adott tárgykörrel, kénytelen ezen idegen nyelvű forrásokat felhasználni, esetleg német, spanyol vagy francia nyelven kereshet megfelelő szakszöveget. A biometria nagyon gyorsan változó terület, nézzék el a szerzőnek, ha viszonylag hamar elévül néhány bemutatott technikai részlet és nem, vagy csak nagyon felületesen kerül szóba több olyan dolog, ami a tudományos kutatás kezdeti fázisaiban tart (pl. kognitív módszerek, terahertz képalkotás biometriai alkalmazása). Azonban az emberi test biológiája, fiziológiája nem változik ilyen ütemben, ezért úgy gondolom, hogy az olvasás során megszerzett tudás alapjaiban még több évtizeden keresztül felhasználható lesz a szakterületen.

A könyvben alapvetően a vizuális eszközökkel működő módszereket mutatom be eltérő részletességgel és mélységben. Ennek több oka is van: a különböző módszerek eltérnek elterjedtségükben, a gyakorlati életben betöltött fontosságukban, bonyolultságukban, előfordulnak ismétlődő technológiák, ill. a szerző ismeretei sem egyforma mélységűek az egyes esetekben. Remélem, hogy utóbbi esetén a megadott hivatkozások jó kiindulópontok azok számára, akik nem elégednek meg az itt közölt információkkal.

A képek és ábrák vagy saját készítésűek, vagy más művekből származnak, utóbbi esetben feltüntettem azok forrását, és amennyiben szükséges volt, engedélyt kértem azok felhasználásához.

Végezetül pedig bátorítani szeretném a kedves olvasókat: amennyiben hibát, pontatlanságot találnak a könyvben, vagy más javító szándékuk van, ragadjanak billentyűzetet, és írják meg azt, hogy a következő kiadás jobb minőségben kerüljön az olvasók kezébe.

Czúni László (czuni@almos.uni-pannon.hu)  
Pannon Egyetem, Képfeldolgozás Kutatólaboratórium

# Tartalomjegyzék

|                                                              |            |
|--------------------------------------------------------------|------------|
| <b>Köszönetnyilvánítás</b>                                   | <b>i</b>   |
| <b>Előszó</b>                                                | <b>iii</b> |
| <b>1. Bevezetés</b>                                          | <b>1</b>   |
| 1.1. A biometria jelentése . . . . .                         | 1          |
| 1.2. A fejlődés hajtóerői, a biometria előnyei . . . . .     | 2          |
| 1.3. Történeti háttér . . . . .                              | 7          |
| 1.4. A biometriai módszerek általános jellemzése . . . . .   | 12         |
| 1.5. Felhasználási területek, a biometria piaca . . . . .    | 15         |
| 1.6. Etikai vonatkozások . . . . .                           | 19         |
| <b>2. A biometrikus rendszerek általános modellje</b>        | <b>25</b>  |
| 2.1. Biometria, mint osztályozási feladat . . . . .          | 25         |
| 2.2. Az azonosítás általános modellje . . . . .              | 26         |
| 2.3. A biometriai módszerek pontossága . . . . .             | 27         |
| 2.4. Röviden a biológiai változatosságról . . . . .          | 32         |
| 2.5. A biometrikus rendszerek lehetséges támadásai . . . . . | 33         |
| <b>3. Szabványok</b>                                         | <b>35</b>  |
| <b>4. Bőr redőzet</b>                                        | <b>39</b>  |
| 4.1. Ujjlenyomat azonosítása . . . . .                       | 39         |
| 4.1.1. Története . . . . .                                   | 40         |
| 4.1.2. Az ujjlenyomat kialakulása . . . . .                  | 42         |
| 4.1.3. Struktúrája . . . . .                                 | 43         |
| 4.1.4. A jelfeldolgozás lépései . . . . .                    | 44         |
| 4.1.5. Eszközök . . . . .                                    | 47         |
| 4.1.6. Erősségek-gyengeségek . . . . .                       | 50         |
| 4.2. Tenyér redőinek felhasználása . . . . .                 | 51         |
| 4.3. Láb bőrredőinek felhasználása . . . . .                 | 53         |
| <b>5. A kéz alakja</b>                                       | <b>57</b>  |
| 5.1. Történeti háttér . . . . .                              | 57         |
| 5.2. A kéz geometriája és mérése . . . . .                   | 58         |

|                                                             |            |
|-------------------------------------------------------------|------------|
| <b>6. Erezet alapú módszerek</b>                            | <b>63</b>  |
| <b>7. Arc</b>                                               | <b>67</b>  |
| 7.1. Története . . . . .                                    | 68         |
| 7.2. Az arc képének jellemzői . . . . .                     | 69         |
| 7.3. Arcok detekciója és a jellemzők mérése . . . . .       | 70         |
| 7.3.1. Az arcképek készítése . . . . .                      | 70         |
| 7.3.2. Arcok detekciója . . . . .                           | 70         |
| 7.3.3. Tulajdonságok kivonása és egyezésvizsgálat . . . . . | 71         |
| <b>8. Fül alakja</b>                                        | <b>77</b>  |
| 8.1. Detekció és felismerés . . . . .                       | 78         |
| <b>9. Retina</b>                                            | <b>83</b>  |
| 9.1. Történeti háttér . . . . .                             | 83         |
| 9.2. A szem felépítése . . . . .                            | 83         |
| 9.3. Mérés és jelfeldolgozás . . . . .                      | 85         |
| 9.4. Eszközök . . . . .                                     | 86         |
| 9.5. A retina diagnosztikai felhasználása . . . . .         | 89         |
| <b>10. Írisz</b>                                            | <b>91</b>  |
| 10.1. Történeti háttér . . . . .                            | 91         |
| 10.2. Az írisz struktúrája . . . . .                        | 92         |
| 10.3. Az írisz mintázatának felismerése . . . . .           | 93         |
| 10.3.1. A kép rögzítése . . . . .                           | 93         |
| 10.3.2. Szegmentálás - az írisz lokalizálása . . . . .      | 94         |
| 10.3.3. Kép transzformációja és normalizálása . . . . .     | 95         |
| 10.3.4. Tulajdonságkinyerés és összehasonlítás . . . . .    | 95         |
| 10.4. Lehetséges problémák . . . . .                        | 97         |
| 10.5. Az írisz diagnosztikai alkalmazásáról . . . . .       | 98         |
| <b>11. Egyéb módszerek</b>                                  | <b>101</b> |
| 11.1. Aláírás . . . . .                                     | 102        |
| 11.2. Gépelés . . . . .                                     | 106        |



# 1. fejezet

## Bevezetés

### 1.1. A biometria jelentése

A biometria görög eredetű kifejezés, a *bio* életet jelent, míg a *metron* mérést. Általános értelemben tehát életfolyamatokkal kapcsolatos jellemzők mérését értjük biometria alatt. A biológusok, orvosok és a biológiai alkalmazásokkal, kutatásokkal foglalkozó statisztikusok matematikai statisztikai módszerek felhasználásával értelmezik, elemzik a biológiai jelenségeket, folyamatokat, ezért a biometria ezen részeit biostatisztikának nevezik.

Az informatika és elsősorban a biztonságtechnika területén kicsit mást értünk biometria alatt. A biometria méri és rögzíti azokat a fizikai és viselkedési jellemzőket, amelyek a vizsgált személyre egyedülálló módon jellemzőek, és ezek alapján végzi a személyek azonosítását, felismerését. Valójában mindenki biometrikus jellemzők alapján ismeri fel ismerőseit, akár találkoznak az utcán, beszéljenek telefonon vagy nézegessenek régi családi fényképeket. Azonban ma már a számítógépek is képesek arra, hogy a személyekről korábban készült és eltárolt megjelenési vagy viselkedési mintákat összevessék az aktuálisan érzékelt jelekkel és elvégezzék a személy azonosítását, felismerését. A könyvben ilyen értelemben fogjuk feldolgozni a biometria témaköreit, de természetesen más informatikai környezetben előfordulhat, hogy a tágabb értelmezést használják.

A biometriai személyazonosítási módszereket alapvetően a mért biológiai jellemzők alapján szoktuk megkülönböztetni. A lehetséges lényegesebb jellemzők abécé sorrendben: az arc tulajdonságai, a beszédhang, a DNS (deoxiribonukleinsav) mintázat, a fül alakja, a gépelés mikéntje, az illatanyagok jellemzői, az írisz mintázata, a járást jellemző mintázatok, a kéz geometriája, a kézírás képe és dinamikus jellemzői, a retina érmintázata, az ujjlenyomat vagy tenyér képe, a vénák rajzolata (például a kézen vagy a csuklón).

Biometriai jellemzőnek lehet tekinteni a billentyűzeten való gépelés mellett

más számítógépes perifériák, pl. az egér vagy egyes számítógépes programok használatának szokásokon alapuló mintázatait is. A DNS, a beszédhang és az illatanyagok optikai módon nem rögzíthető, képileg nem feldolgozható tulajdonságok, ezért könyvünkben nem tárgyaljuk őket.

## 1.2. A fejlődés hajtóerői, a biometria előnyei

Az emberi társadalom fejlődésére általában jellemző a távolságokat egyre nagyobb mértékben és sebességgel átívelő közlekedés és a kommunikációs technológiák fejlődése. Ez elsősorban a fejlettebb és kifinomultabb módszereken, eszközhasználaton alapul: egyre gyorsabb közlekedési eszközök, egyre komplexebb földi és légi úthálózatok, egyre jelentősebb kapacitás és általában nagyobb lehetőségeket jelentő mobilitás figyelhető meg. Az ipari forradalomnak köszönhetően a gépesítés jelentős lökést adott ezeknek a folyamatoknak, ami elsősorban a felhasznált technológiai színvonalban és mennyiségi növekedésben, ill. az elterjedtségben szembetűnő. A kommunikációs eszközök fejlődését ugyan ezek a jellemzők írják le, azonban talán annyi különbséget tehetünk, hogy a kommunikációt forradalmasító elektronikai eszközök tömeges elterjedése valamivel később lépett át több minőségi határt, és az ún. info-kommunikációs forradalom - különböző fázisaiban - lényegében ma is zajlik.

Mind ezek oda vezettek, hogy a modern kort megelőző időszakokban működő személyes, ill. intézményi kapcsolatokat jellemző kommunikációs, kereskedelmi, szociális mintázatok fokozatosan, de napjainkra lényegesen megváltoztak. A korábbi időszakokban a társadalom tömegei a szociális kapcsolatok során alapvetően egy kicsi környezetben léptek interakcióba egymással. Túlnyomórészt személyes kapcsolatok révén jutottak az emberek árukhoz, szolgáltatásokhoz, munkához, s mivel a társadalmi mobilitás igen kismértékű volt, ezért ezek a kapcsolatok nem voltak egyszerűen helyettesíthetők, lecserélhetők. Így természetesen a kialakuló bizalmi kapcsolatoknak fontos elemei voltak az együttműködő felek között létrejövő visszacsatolások, visszajelzések, különböző interakciók. A közlekedési és a kommunikációs eszközök fejlődése azonban a szolgáltatások és árucseré során új technikai eszközök létrejöttéhez vezetett.

Az 1.1 táblázat a társadalmi kapcsolatok különböző aspektusainak alapvető változását mutatja be a modern kort megelőző évezredek és az elmúlt néhány évtized (kb. 100 év) viszonylatában.

A hitelesség biztosítása a természetes szintről (személyesen megismerjük és felismerjük a velünk üzletelő felet) a kifinomult technológiák által körbeölelt szintre került (például egy eddig ismeretlen webáruházról árut rendelünk). Mivel az áruk, szolgáltatások egyre nagyobb értékben és egyre gyakrabban cseréltek ilyen adottságok között gazdát, ezért a minden társadalmi folyamat kohézióját jelentő hitelesség, bizalom fenntartása új eszközöket igényelt. Azonban most nem célunk bemutatni a szociális-társadalmi kapcsolatok minden aspektusát, eszközét (a különböző írásos levelektől, dokumentumoktól kezdve), elegendőnek gondoljuk, ha a tárgyunkhoz leginkább kötődő azonosítási kérdéskörre vetünk

1.1. táblázat. Társadalmi (kereskedelmi) kapcsolatok néhány jellegzetességének alapvető változása

|                        | Újkort megelőző időszakok                                           | Történelmi kései újkortól, modern kortól                                                                                                                 |
|------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Felek jelenléte        | személyes (szemtől-szembe) kapcsolat                                | a kapcsolatfelvétel hagyományos levelezéssel vagy elektronikus csatornán is történhet                                                                    |
| A kapcsolat tárgya     | az "áru" kézbe vehető, ki-próbálható                                | az "áru" (az üzletkötéskor) nem minden esetben kézzelfogható                                                                                             |
| Időtartam              | hosszan tartó ismeretség                                            | gyakori az egyszeri kapcsolatfelvétel                                                                                                                    |
| Felek azonosíthatósága | a résztvevők kiléte egyértelmű                                      | azonosítók változhatnak (pl. cím, telefonszám, weboldal), a felek nehezen vagy személyesen nem azonosíthatóak                                            |
| Elhelyezkedés          | földrajzilag jól lokalizálható                                      | globális, mindenhol jelen levő, de egyben esetleg nehezen lokalizálható partnerek és szolgáltatók (lásd felhő szolgáltatások, ill. "internet of things") |
| Egymásra utaltság      | a felek nehezen helyettesíthetők, alapvetően egymásra vannak utalva | nincs közvetlen vagy erős egymásra utaltság                                                                                                              |

egy pillantást a következőkben. Alapvetően négy esetet különböztetünk meg:

1. A kisméretű (kis hatókörű), kicsi mobilitással rendelkező társadalmi közegben a személyes megjelenés elegendő volt ahhoz, hogy az adott üzletet nyélbe üssük. Az üzletet kötő felek (pl. vevő és eladó) már régóta ismerték egymást, korábban is volt kapcsolatuk, ha esetleg valamelyik fél halasztást kért, a problémás ügyeket személyesen lehetett a későbbiekben rendezni. A személyes ismeret lényegileg az érzékszervekből származó információkon alapult.
2. Abban az esetben, ha a szereplők el akartak érni valamilyen korlátozott hozzáférésű erőforrást, és a hozzáférést ellenőrző nem ismerte magát az igénylőt, a jogosultság bizonyításához valamilyen igazoló dokumentumot használtak. Az igazoló dokumentum - vagy általánosabban a hozzáférést lehetővé tevő eszköz - lehet egy okirat, kulcs, vagy akár egy elektronikus kártya. (Lényegileg a pénz is hasonló szerepet tölt be, azonban ott a vásárlási jog könnyen átruházható a pénzürmék vagy bankók átadásával.)
3. Harmadik eset, ha az azonosítás nem egy kézzel fogható eszközzel, hanem jelszóval történik, akár például, amikor a felhasználóhoz tartozó jelszót adunk meg egy számítógéphez való hozzáférés során. Természetesen az előző esettel való kombináció is lehetséges: a bankkártyánkat tipikusan PIN (Personal Identification Number) kóddal használjuk.
4. A biometria azonosítás lényegileg az első eset gépi megoldásán alapul: a partnerek nem közvetlenül az érzékszerveik alapján ismerik fel egymást, hanem különböző elektronikus szenzorok (korábban mechanikus mérések) elemzik a személy tulajdonságait, és valójában nem is biztos, hogy a kapcsolat egyik fele egy konkrét személy (hanem például egy elektronikus szolgáltatás vagy "robot").

Napjainkban az első eset egyértelműen nem elegendő, hiszen az áruforgalom, a szolgáltatások és általában az emberek közti kapcsolatok jelentősen globalizálódtak. Az igazolást végző eszközök is számos hátránnyal bírnak: legkézenfekvőbb hiányosságuk, hogy előfordulhat, hogy elvesznek, eltulajdoníthatják azokat, vagy el is romolhatnak. Ha jelszót használunk, akkor más problémák adódhatnak: elfelejthetjük azt, vagy ha valahova leírjuk - elkerülendő az elfelejtést - mások is könnyen megtudhatják. Emellett az is gyakori, hogy a különböző hozzáférésekhez azonos vagy nagyon hasonló jelszót használunk, így az egyiknek a felfedése egyszerre vezet több rendszer biztonságának csökkenéséhez. Mind a fizikai eszközök, mind a jelszavak használata esetén a jogosultság könnyen átadható egy másik személynek, megsértve az alapvető biztonsági protokollt.

Tegyük egy pillantást néhány olyan felmérésre, amely a jelszó alapú azonosítás gyakorlatáról ad átfogó képet. [63] az Amerikai Egyesült Államokban végzett online felmérések alapján mutat be érdekes adatokat. A 2012 nyarán végzett felmérésekbe 2208 18 évnél idősebb személyt vontak be. A kutatás néhány fontosabb eredménye a következőkben foglalható össze:

- A felnőttek 58%-a több mint 5 egyedi online jelszóval rendelkezett,
- 30%-uknak 10 vagy több,
- 8%-uknak 21 vagy még több jelszava volt.
- Az idősebb felhasználóknak tipikusan több jelszava volt, mint a fiataloknak (55 év felett átlagosan 8,2, míg 18 és 34 év között 6,7).
- A 45 és 54 év közötti férfiaknak van a legtöbb online jelszava, átlagosan 9,8.

A jelszóhasználat általános gyakorlatáról, ill. a jelszók "újrahasznosításáról" [41] is értékes információkat közöl. A nagyszabású felmérés során a felhasználók gépeire - beleegyezésükkel - egy speciális programot telepítettek, amely az adatgyűjtést végezte. Három hónap alatt több mint félmillió felhasználót vontak be a felmérésbe, amelyek során többek között kiderült:

- A felhasználók átlagosan 25 db, jelszót igénylő webhelyet látogattak,
- naponta átlagosan 8 jelszót kellett begépelniük.
- Az átlagos felhasználónak 6,5 különböző jelszava volt,
- átlagosan 3,9 webhelyen használtak egy-egy (azonos) jelszót.
- Évente átlagosan a felhasználók 0,4%-a adja meg jelszavát ún. adathalász weboldalakon,
- gyakran történik meg az is, hogy a felhasználók elfelejtenek egy-egy jelszót, pl. a Yahoo felhasználóinak 1,5%-a havonta.

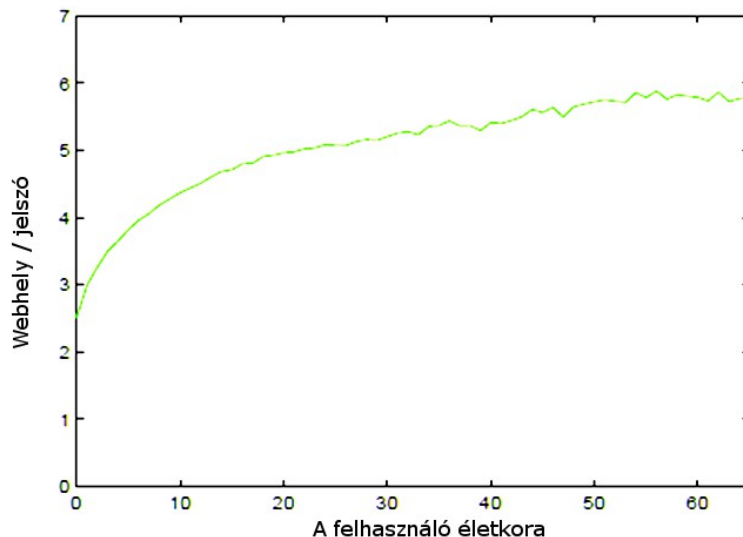
Az 1.1 ábra az egy jelszóra jutó webhelyek számát mutatja a felhasználók évkorának függvényében. Átlagosan 6 alatti értékeket találunk, de az évkor növekedésével az átlagos újrahasznosítása a jelszavaknak egyértelműen nő.

Mindezen problémákkal szemben a biometria rendszereknek a következő előnyeit tudjuk megállapítani:

- a biometria jellemzőket nem hagyhatjuk vagy felejtethetjük el,
- az azonosító nem ruházható át,
- nehéz a jeleket hamisítani, nem lehet "kitalálni" azokat,
- könnyű a használatuk, és nő a rendszer által létrejött biztonság.

Természetesen vannak hátrányai is a biometria rendszereknek, mint például a következők:

- erősek a félelmek a személyes információknak és a magánélet titkosságának védelmével kapcsolatosan,



1.1. ábra. Az egy jelszóra jutó webhelyek száma az életkor függvényében [41] szerint

- az azonosítás során született döntés (azonos - nem azonos) nem 100%-os, mindig számolhatunk a rendszer döntésének hibájával,
- az egyéb biztonsági rendszerekhez hasonlóan - rendszer szinten - támadható,
- bizonyos esetekben (pl. betegség, sérülések) - egyes módzatoknál - nő a döntési hiba valószínűsége.

Az azonosítási módszerek áttekintő képét (a biztonsági és technológiai szint függvényében) az 1.2 ábra szemlélteti.

Fontos nem elfeledkezni a biometria eszközök működését biztosító elektronikai és informatikai ipar fejlődéséről sem. Moore törvénye szerint a számításokat végző áramkörök teljesítménye durván 18 havonta megduplázódik. A Gordon Bell-ről elnevezett Bell törvénye az ezekre az integrált áramkörökre épülő rendszerekről tesz általános érvényű megállapítást: a félvezetők, memóriák, interfészek és hálózati eszközök fejlődése révén körülbelül tízévenként újfajta igényeket kiszolgáló, új számítógéposztályok jönnek létre, amelyek ráadásul egyre olcsóbban, és egyre nagyobb körben érhetők el a felhasználók számára. Ennek a folyamatnak a mérföldkövei a következőképpen sorolhatók fel:

- 1960-as évek: nagyszámítógépek (mainframes),
- 1970-es évek: miniszámítógépek (minicomputers),



1.2. ábra. A személyazonosítás technológia fejlődésének főbb szintjei

- 1980-as évek: hálózatra kötött munkaállomások és személyi számítógépek,
- 1990-es évek: böngésző-webkiszolgáló struktúrák, kézisámítógépek,
- 2000-es évek: webes szolgáltatások (Web2),
- 2003: mobiltelefonok és számítógépek egybeolvadása,
- 2004: vezeték nélküli szenzorhálózatok (motes).

Bell korábbi becslése szerint 2010-től várható az otthoni és a viselhető (ill. testközel) hálózatok elterjedése. Valójában ez a jóslata is beteljesült, hiszen elsősorban a Bluetooth, Wifi és infra kommunikáció révén a környezetünkben lévő észlelő és jelprocesszáló gépek ma már igen hatékonyan tudnak együttműködni. Igencsak valószínű, hogy ez a folyamat nem áll meg, és a jövőben megjelenő eszközök révén az ember-gép kapcsolat szorosabbá válik, így az emberi jellemzők digitalizálására is új utakat találunk. (Gondoljunk csak a könyv írása közben megjelenő Google Glassra és más hasonló kiterjesztett valóság eszközre, amelyekhez minden valószínűség szerint hamarosan elérhetővé válnak olyan alkalmazások, amelyek a személyek azonosítására is képesek lesznek.)

### 1.3. Történeti háttér

A biometria jellemzők azonosításban való felhasználása az emberi civilizáció számtalan korszakában megfigyelhető volt, így a történeti háttérnek áttekintése akár egy önálló könyv terjedelmét is elérné. Ebben a fejezetben tehát néhány főbb mérföldkövet ill. érdekességet mutatunk csak be.

Egy 31000 évesnek becsült barlangban a történelem előtti idők embere által készített barlangrajzokat találtak, ahol a rajzokat számos *kézlenyomat* vette körül. Feltételezések szerint az alkotók aláírás gyanánt használták kezük mintáját [89]. Természetesen ez csak egy a lehetséges teóriák közül, hiszen igen sok másik barlangban is fedeztek fel ezrével kéznyomatokat. Történtek próbálkozások arra is, hogy a kéznyomatokból utólag rekonstruálják a személyek nemét [111]. Az 1.3. ábra tipikus, negatív kézmintákat mutat egy franciaországi barlangrajzon. A test geometriájának mérését a modern korban (az 1800-as évek végén) Bertillon alkalmazta elsőként, de az első kereskedelmi, kimondottan *kézzalak* felismerő rendszerek majd csak az 1970-es években jelentek meg. 1996-ban az olimpiai játékokon már nagy tömegeken végeztek használtak kéz alapú azonosítást, az olimpiai faluban több mint 65000 ember fizikai hozzáférését szabályozták vele. A 28 napos időszak alatt több mint 1 millió ellenőrzést hajtottak itt végre.



1.3. ábra. Negatív kéznyomatok foltos lovak körül, barlangrajz, Pech-Merle, Franciaország

Az első - bizony állíthatóan - tudatosan azonosításra használt *ujjlenyomatok* az ókori Babilón területéről kerültek elő, ahol kereskedelmi adásvétel során rögzítették azokat agyagtáblán i.e. 500 környékén. Egyiptomban szintén a kereskedelemben tűntek fel ujjlenyomatok: segítségükkel tudták a már korábbról ismert, megbízható kereskedőket megkülönböztetni a piacon megjelenő új kereskedőktől [77]. Kínából is számos példát találhatunk az ujjlenyomat használatára, itt már a bűnüldözésben is használták azokat pl. i.e. 221-206 között a Qin dinasztia idejében [84].

A modern korban az első jelentős továbblépés az 1850-es években történt: Sir William James Herschel kezdeményezte az ujjlenyomat alkalmazását Indiában. Akkoriban Indiában komoly problémát jelentett az aláírások használatának megbízhatósága, ezért a szerződéseken és okiratokban bevezette az ujjlenyoma-





1.4. ábra. Alphonse Bertillon "önarcképe", 1900. augusztus 22. A kép megfelel egy tipikus rendőrségi felvételnek (mug shot). Bertillont tartják a modern biometria atyjának.

tok használatát. Például a nyugdíjfolyósítás során azt kellett megakadályozni, hogy a rokonok felvegyék az elhalálozott nyugdíját, vagy hogy a letöltendő börtönbüntetést különböző csalásokkal kerüljék el az elítéltek.

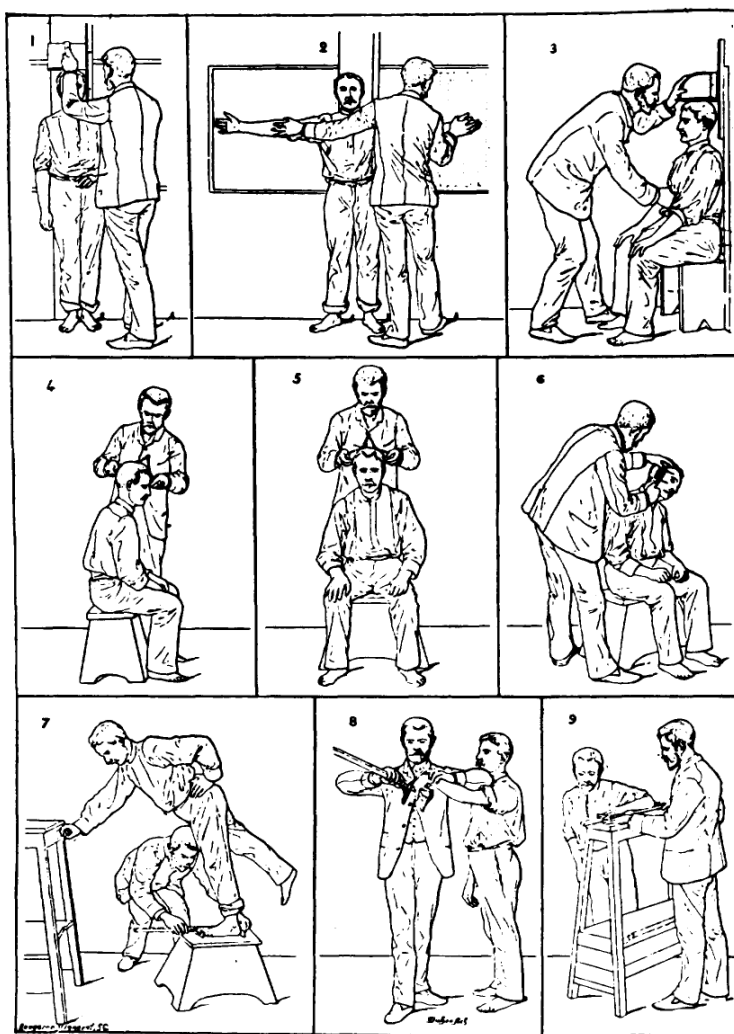
A modern Európában az első jelentős biometria alkalmazás Alphonse Bertillon (1853. április 24. - 1914. február 13.) francia rendőrségi alkalmazott nevéhez fűződik. Ő használta először a bűnügyi arcképet, a fej és test főbb jellemzőinek adatait, ill. az olyan egyedi jellegzetességeket, mint pl. a sebhelyek, tetoválások. Bertillon arcképét a 1.4. ábra, a mérési procedúra illusztrációját pedig a 1.5. ábra illusztrálja. Azonban problémák merültek fel a Bertillon rendszerrel kapcsolatban, miután két különböző személy esetén a leíróik közel azonosnak mutatkoztak. Mint később kiderült ikrekről volt szó [84].

Az 1890-es években Sir Francis Galton egy új osztályozási módszert dolgozott ki a kéz tíz ujjára, az ujjlenyomat apró sajátosságos pontjaira ("minutiae", minucia) támaszkodva. Valójában ezt a megközelítést használják a mai modern módszerek is.

Angliában és Írországból 1901-től kezdték el használni az ujjlenyomatot a Scotland Yard speciális hivatalában, valójában Galton módszerére támaszkodva, de Henry-féle osztályozási rendszer néven. Az európai alkalmazásokat megelőzte Juan Vucetich rendőrségi felhasználása Argentínában.

Az USA-ban az ujjlenyomatok első használata Gilbert Thompson nevéhez fűződik, aki a US Geological Survey munkatársaként használta ujjlenyomatát, hogy hitelesítsen egy általa kiállított dokumentumot 1882-ben. Az első szisztemati-

# RELEVÉ DU SIGNALEMENT ANTHROPOMÉTRIQUE



1. Taille. — 2. Envergure. — 3. Buste. —  
4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. —  
7. Pied gauche. — 8. Madius gauche. — 9. Coudée gauche.

1.5. ábra. Ábrák Bertillon "Identification anthropométrique" című művéből (1893). A rajzok az azonosító rendszer méréseit illusztrálják.

kus tesztek 1902-ben kezdődtek, 1903-tól pedig a New Yorki Állami Börtönben bevezették az ujjlenyomat alapú azonosítást. 1924-ben az FBI (Federal Bureau of Investigation) külön részleget hozott létre az ujjlenyomatok feldolgozására. 1946-ra már kb. 100 millió ujjlenyomat kártyát dolgoztak fel itt, nagyrészt kézi módszerekkel. Az automatikus felismerési módszerek bevezetésére a 60-as évekig kellett várni, amikor az FBI megbízta a National Institute of Standards and Technology-t (NIST) a kérdéskör alapos tanulmányozásával. 2010-ben az FBI "Integrated Automated Fingerprint Identification System" (IAFIS) rendszerében már 70 millió bűnüggyel kapcsolatos, 31 millió civil és 73000 terrorizmussal kapcsolatosan nyilvántartott lenyomatot tároltak.

Fontos lépés volt az ujjlenyomat azonosítás megjelenése a hétköznapi alkalmazásokban: a Compaq számítógépekhez egy kiegészítő kártyán már 1998-ban elérhető volt az ujjlenyomat beolvasás, az IBM ThinkPad T42 hordozható gépébe 2004-ben került bele az ujjlenyomat szkennel: az engedélyezett felhasználók beregisztráltak mintáit az integrált szkennel biztonsági áramkörei tárolták.

Az ujjlenyomat-felismeréssel ellentétben a többi biometrikus azonosítási mód jóval lassabb fejlődésen ment keresztül. Az első ismert *tenyérlenyomatot* használó rendszer a magyar Recoware Kft. nevéhez kötődik 1994-ből, a technológiát később a Lockheed Martin Information Systems vásárolta meg 1997-ben.

Az *írisz* alapú azonosítás alapelveit 1936-ban Frank Burch fektette le, míg az első jelentősebb szabadalmat (Leonard Flom és Aran Safir két szemész professzortól) 1987-ben fogadták el "Iris Recognition Technology" címen [40]. Az egyik legelterjedtebb módszer kidolgozása John Daugman nevéhez fűződik, akinek az algoritmus 1994-ben kapott szabadalmat.

A *fület* egyedi geometriai jellemzői szintén alkalmassá teszik a biometrikus felhasználásra. A viszonylag ritkán alkalmazott módszert Iannarelli már az 1940-es évek vége óta alkalmazta, igaz, annak automatizálása sokat váratott magára. Az első gépi *arcfelismeréssel* kapcsolatos eredmények Bledsoe [12] nevéhez kapcsolódnak az 1960-as évekből, azonban csakúgy, mint a későbbi Goldstein és Lesk [50] munkáiban, eleinte alapvetően az operátor kézügyességén múlt az arc jellegzetes geometriai jellemzőinek pontos meghatározása (mivel az nem automatikus, gépi módon történt).

Bár a *kézírásfelismeréssel* kapcsolatos első eredmények már a 20. század első felében megjelentek, az első automatikus aláírás ellenőrző rendszert 1965-ben a North American Aviation fejlesztette ki [76]. A Veripen Inc. 1977-es szabadalma által leírt módszer lehetővé tette, hogy a kézírás során a nyomásértékeket is felhasználják. Az ezen alapuló technológiát kezdte el használni nem sokkal később az Egyesült Államok Légierője (United States Air Force - USAF) is.

Az első *hang alapú* azonosítási rendszer prototípusát a Texas Instruments fejlesztette ki 1976-ban, ezt szintén a USAF kezdte el használni elsőként nagy méretekben.

A *DNS alapú* biometriában 1998 fontos időpont: az FBI elindítja a CODIS-t (Combined DNA Indexing System), ami a DNS mintázatok tárolását, keresését teszi lehetővé. A kód előállítását végző laboratóriumi folyamat akkoriban minimum 40 percet, de akár több órát is igénybe vehetett (ez az idő napjainkra

lényegesen lerövidült) [21].

## 1.4. A biometriai módszerek általános jellemzése

A biometria fejlődését ösztönző hajtóerők igen sokrétűek, az élet legkülönbözőbb területein találkozhatunk a biometria használatával, óriási sokféleség jellemzi a biometriai alkalmazásokat. Természetesen a különböző módszerek jellemzése és összehasonlítása is igen sokféle szempont szerint történhet. Magukat a biometriai jellemzőket alapvetően két nagy csoportba sorolhatjuk:

1. statikus fizikai jellemzők mérésén alapuló módszerek, ill.
2. viselkedési jellemzőkön alapuló eljárások.

Az első kategóriába tartoznak: az arc (látható vagy infra tartományban), a vér érhalózat, a DNS, a fül, az illatanyagok, a kéz geometria, a szem (írisz és retina), az ujjlenyomat. Léteznek speciális, az orvosi képalkotás által előállított jellemzőket használó technikák is, vagy pl. akár a fogazat állapota, formája is használható bizonyos esetekben. A viselkedési jellemzők közül jól használható: a gépelés, a beszédhang, a járás, a kézírás, a számítógépes szoftverhasználat. Könyvünkben (mint ahogy a címe is utal rá) csupán a vizuális módszereket tárgyaljuk.

A biztonságtechnikában dolgozó rendszerfejlesztők első alapvető gondolata, kérdése, hogy a rengeteg megközelítés közül mikor melyiket érdemes választani. Az optimális döntés meghozatala érdekében számos szempontot kell mérlegelni:

- **Skálázhatóság:** Szinte minden informatikai rendszernél felmerül a skálázhatóság kérdésköre. Esetünkben azonban nem csak maguk az alkalmazott informatikai technológiák döntőek a skálázhatóság szempontjából, hanem a biometriai jellemzők is. Adott körülmények között egy kicsi populáción (pl. ha csak néhány tucat munkavállaló van egy cégnél) igen jól működhet egy arc vagy egy hang alapú biometriai beléptető rendszer. Azonban ha a felhasználók száma néhány száz vagy ezer közelébe emelkedne, akkor könnyen meglehet, hogy bár fizikailag a rendszer bővíthető lenne és képes lenne kezelni a megnövekedett igényeket, de az addig jól működő rendszer által generált hibás elfogadások vagy elutasítások mértéke elfogadhatatlan mértéket öltene és a rendszer használhatatlannak bizonyulna.
- **Társadalmi elfogadottság:** A személyes jellemzőket mérő informatikai rendszerek számos etikai problémát vetnek fel (amelyeket később külön is számba veszünk). Ezen etikai problémák hozománya, hogy sok esetben erőteljes a társadalmi elutasítása alkalmazásuknak. Például az ujjlenyomat alapú azonosítás - köszönhetően történeti előzményeinek - a társadalmi megítélés szerint leginkább a bűnüldözéssel, ill. magával a bűnözés fogalmával hozható összefüggésbe. A kéz alakjának felismerése sokkal kevésbé jellemző a bűnügyi nyomozásokban, ezért az emberek nem érzik megalázónak, lehetséges kompromittáló tényezőnek annak alkalmazását

a hétköznapi életben. Ezzel szemben az ujjlenyomat szkennerek korlátozott felhasználása a hordozható számítógépeken a felhasználók jelentős részének elfogadható "kockázatot" jelent csupán. Természetesen idővel a társadalmi elfogadottság mértéke változhat, pl. a felhasználók újabb generációinak megjelenésével, főleg, ha a technikák alkalmazásának vélt hátrányaival szemben mind több kézzel fogható kényelmi előny is jelentkezik.

- **Pontosság:** A pontosság általános jelentését valójában többféle mérőszámmal lehet konkrétan definiálni, gyakorlatilag a statisztikában, az alakfelismerésben használt osztályozási fogalmak használata a célravezető. A biometriai rendszerek modell szintű bemutatásánál fogunk kitérni ezekre a definíciókra. Az egyes módszerek tárgyalásánál pedig nagyságrendi becslést adunk a legfontosabb mutatók értékeire.
- **Interakció mértéke:** A különböző biometriai megoldások a felhasználók más és más mértékű és jellegű hozzájárulását igénylik a hatékony működés érdekében. Egyes mérések semmiféle speciális tevékenységet nem igényelnek, s még akár észrevétlenek is maradhatnak. Más módszerek jelentős odafigyelést, esetleg bizonyos utasítások végrehajtását is igényelhetik (pl. előre megadott szöveg elmondását a hangot rögzítő mikrofonhoz odahajolva).
- **Költségek:** Ez vonatkozhat a beszerzésre és az üzemeltetésre is, összességében vagy a felhasználókra vetítve is kalkulálhatunk. Érdekes azonban nem csak a közvetlenül felmerülő kiadásokat figyelembe venni. Szélesebb körben, pl. vállalati vagy társadalmi szinten elemezve egy rendszer bevezetését egy sokfelhasználós, hatékonyan működő azonosító rendszer rengeteg időt és fáradságot takaríthat meg, ami összességében jelentős költségmegtakarítást jelenthet.

A biometriai módszerek jellemzése során természetesen ezen fő szempontokon kívül sok egyéb speciális szempont is felvethető, amelyek egyébként valamilyen módon és mértékben meghatározzák a rendszerről alkotott általános képet. Ilyen szempontok például:

- megtéveszthetőség: milyen könnyű csalással más személyazonosságát "elbitorolni",
- felhasználói élmény: mennyire kényelmes, kézenfekvő a használat,
- általánosság: a potenciális felhasználók mekkora hányada esetében nem alkalmazható,
- állandóság: hogyan képes a rendszer követni a felhasználók tulajdonságainak változásait,
- egyediség: a mért jellemző mennyire különböző személyenként (ez szoros kapcsolatban van a pontossággal),

- integrálhatóság: szükség esetén milyen módon kapcsolódhat más - akár biometriai - rendszerekhez,
- robosztusság: a rendszer mennyire zavartűrő (pl. környezeti hatásokkal szemben).

A fő cél olyan rendszerek létrehozása, ahol a költséghatékonyság, használhatóság, pontosság az adott méretben maximumát éri el. Természetesen nem lehet a különböző modalitásokat általánosan összehasonlítani, ugyanis az egyedi tényezők mindig torzíthatják a képet. Ha csak a költséget és a pontosságot vesszük számba, akkor az 1.6 ábrát vehetjük kiindulási alapnak a leggyakrabban használt biometriai módszerek esetén.



1.6. ábra. Néhány elterjedtebb biometriai módszer hozzávetőleges pontossága és költsége

Ahogy az ábráról leolvasható, az ujjlenyomat, a retina és írisz képének felhasználása egyértelműen a legpontosabb megoldást jelenti, de utóbbi kettő esetében a költségek is viszonylag magasak. A képkötő, feldolgozó és tároló eszközök árának esése, a nagy gyártási példányszámok azonban az ujjlenyomat alapú eszközök esetén már az árakban is érződnek. A beszédhang rögzítésével és feldolgozásával azonban a költségek szempontjából nehéz versenyezni: a mikrofonok a telefonok milliárdjaiban jelen vannak, a hangok feldolgozása is lényegileg megoldott a digitális telefonokban alkalmazott áramkörök segítségével. A kéz alakjának felismerésének viszonylagos drágasága valószínűleg a nagy eszközméretnek köszönhető: a képbeviteli eszközökben el kell tudni helyezni az emberi kezét.

A tömegtermelés korában azonban a költségek közti különbségek, esetleg az árak is könnyen megváltozhatnak (lásd Moore törvénye), így a fenti jellemzés nem tekinthető örökérvényűnek.

## 1.5. Felhasználási területek, a biometria piaca

A korábban tárgyalt tömeg-, ill. fogyasztói kultúrára jellemző hitelességi deficit (lásd 1.1 táblázat) természetszerűleg fenntartja, ill. erősíti a szereplőkben ébredő biztonság iránti vágyat. Így az élet számtalan területén jelennek meg az ellenőrző, azonosító rendszerek. Ugyanakkor a modern emberre szintúgy jellemző a kényelem iránti vágy, ezért a környezetben már rendelkezésre álló intelligens, ma már hálózatba kötött eszközöktől elvárja, hogy tegyék egyszerűbbé és gyorsabbá az egyes hitelesítő procedúrákat, ill. a személyazonosság megállapításával legyenek a különböző rendszerek vagy kereskedelmi szolgáltatások személyre szabottak. A felhasználás jellegét tekintve az alkalmazások a következő főbb csoportokba sorolhatók:

- Kereskedelmi szolgáltatások:
  - Pénzfelvétel automatákból
  - Hozzáférés számítógépekhez, egyéb műszaki eszközökhöz, berendezésekhez (pl. személygépjármű vezetésekor [55])
  - Hozzáférés számlázási, pénzügyi adatokhoz
  - Vásárlás (online v. offline)
  - Kényelmi szolgáltatások: VIP beléptetés, klubtagság
- Hatósági (állami) alkalmazások:
  - Személyazonosság igazolása
  - Szociális támogatások folyósítása
  - Jogosítványok (gépkocsivezetés, választási szavazások)
  - Határátlépés (útlevelék) <sup>1</sup>
  - Fegyverhasználat
  - Katonai programok
  - Társadalmi és egészségügyi biztosítások
  - Adathozzáférések (pl. ingatlan)
- Bűnügyi, bírósági felhasználás:
  - Halottak azonosítása
  - Bűnözők felderítése, azonosítása
  - Vérváladék, családi kapcsolatok meghatározása

---

<sup>1</sup>A 2001-es amerikai terrortámadások ürügyén az Egyesült Államok a beutazó, külföldi állampolgárok esetén két ujjlenyomat és fénykép rögzítését tette kötelezővé. Néhány év alatt közel 100 milliós adatbázis jött létre. Később - 2008-tól - 10 ujjas mintavételt vezettek be, így becslések szerint évente 20-23 millió ujjlenyomattal nő az adatbázis mérete. A DHS (United States Department of Homeland Security) nyilatkozata szerint az ujjlenyomatokat 75 évig fogják tárolni.

- Elveszett személyek felkutatása
- Büntetés végrehajtás: börtönök, javítóintézetek, házi őrizet, próbára bocsátások

Ezekon kívül az élet számos területén találkozhatunk különböző alkalmazásokkal, melyeket nehéz lenne a fenti besorolás szerint osztályozni:

- Videófelügyelet: Igen sok helyen vannak jelen a videokamerák, amelyekkel nem csak rögzíteni lehet a különböző eseményeket, hanem sok esetben automatikusan követni is lehet egyes személyeket, vagy a rögzített felvételek alapján elemezni, hogy ki látható a képen. Itt a statikus megjelenésen kívül pl. a járásminta is segítheti a személy felismerést, követést.
- Egészségügy: Mivel az egészségügyben sok személyes adatot tárolnak, ill. a kezelések erősen személyfüggőek, ezért kulcsfontosságú a betegek gyors és megbízható azonosítása. Emellett a bizalmas adatok elérése, biztonságos kezelése erős ellenőrzési, beléptetési szintet igényel.
- Munkaidő nyilvántartás: A munkahelyre való belépésnél, ill. kilépésnél gyorsan, kényelmesen és pontosan kell elvégezni az azonosítást, ellenkező esetben vagy a munkavállalók lesznek elégedetlenek vagy könnyen kijátszható lesz az ellenőrző rendszer (és természetesen a hasznos munkaidő is jelentősen csökkenhet).

A biometriai módszerekhez hasonlóan az alkalmazásokat is lehet jellemezni működési sajátosságuk alapján, ami természetesen erősen függ a mért jellemzőktől. Így beszélhetünk: nyílt - zárt, rejtett - nyilvános, alacsony - magas biztonsági szintű, skálázható - kevésbé skálázható, egyénileg - segédszemélyzet-tel használható, kooperatív - nem kooperatív rendszerekről.

A biometria felhasználása tehát napjainkban már igen széleskörű, csupán ízelítőül tekintsük át néhány érdekes alkalmazását:

- Az EU tagállamok nagy részénél a személyi igazolvány a fényképen kívül is tartalmaz biometrikus azonosítót. A német személyi igazolványban - egyebek mellett - chipen tárolásra került a fénykép és az ujjlenyomat is, amelyet csak egyes hatóságok tudnak kiolvasni.
- A Hitachi cég által kifejlesztett ujj érhálózat alapú azonosítási módszer kártya nélküli fizetést tesz lehetővé. A rendszer első nagyobb tesztjét a cég éttermében végezték Shin-Kawasaki-ban 2007-ben. Később a cég lényegileg azonos megoldását gépkocsikban való felhasználásra is bemutatták, itt a gépjárművet csak az arra jogosult személy indíthatja, ennek ellenőrzése a kormány mellé beépített érellenőrző szenzor feladata [55] (lásd 1.7. ábra).
- A BRASKA cég többféle biometrikus széfet forgalmaz. AX11650 azonosítójú terméke (lásd 1.8. ábra) 120 felhasználó adatait tudja kezelni, a széf tartalmához való hozzáféréshez ujjlenyomat azonosítást használ.





1.7. ábra. A Hitachi által kidolgozott érhálózat alapú gépjárművezetőt azonosító rendszer [Hitachi2007]



1.8. ábra. A BRASKA cég ujjlenyomat azonosítás alapú széfje

- 2008 óta a Japánban működő cigaretta-automaták egy részét (4800-at, ami valójában kevesebb, mint az összes cigaretta-automata 1%-a) életkor ellenőrző kamerával látták el. (A többi készülék egy ún. Taspo életkor ellenőrző kártyával használható.) A berendezés csak akkor engedi a cigaretta vásárlását, ha az arcképe alapján legalább 20 évesnek véli a vásárlót. Azonban többen észrevették, hogy a gép átverhető egyszerű fotókkal, sőt a fizetés során elfogadott ezres vagy tízezres bankókon levő arcképek is jól használhatók erre a célra (lásd 1.9. ábra).
- A biometria azonosítás talán egyik legfontosabb területe lenne a lőfegyverekhez való hozzáférés szabályozásának biztosítása. Azonban a könyv írásáig ilyen fegyver nem került kereskedelmi forgalomba. Az igények fontosságát azonban jelzi, hogy mind az EU-ban, mind az USA-ban valószínűleg a jogi szabályozásba is beépül a technológia, amennyiben nagy tömegekben és nagy megbízhatósággal elérhető lesz. 2013 októberében az Európai Bizottság kiadott egy dokumentumot, amely szerint a Bizottság a fegyvergyártókkal együttműködve olyan technológiák után kutat, amely biometrikus szenzorokkal és a személyes adatok fegyverben való tárolásá-



1.9. ábra. A japán bankókon lévő portrék is alkalmasnak bizonyultak az arc alapú életkorellenőrző rendszer megtévesztésére a japán cigaretta-automatákban.

val biztosítani tudja azt, hogy csak a fegyver vásárlója használhassa azt [37].



1.10. ábra. Amerikai tengerészgyalogosok ujjlenyomatokat, írisz képeket és egyéb adatokat gyűjtenek be iraki civilektől Fallujah-ban egy iraki rendőrségi övezetben (2007. július 19., [97])

A biometriával kapcsolatos piaci elemzések egyértelmű dinamikus emelkedést mutatnak már hosszú évek óta. Általában az elmúlt évtizedben kb. 100 millió dolláros éves piacról beszélhettünk. A biztonsági kérdések fontosságának felerősödése, a médiában megjelenő terrorcselekményektől való félelem óriási növekedést indukált. Csak a biometrikus olvasóberendezések piaca 2011-ben 50 millió dolláros volt, miközben az elkövetkező évekre átlagosan 48%-os bővülést prognosztizálnak. Egyes becslések szerint [90] a globális biometria piaca az évtized közepére tízmilliárd dolláros méretű lesz.

Ebből a piacból az automatikus ujjlenyomat azonosító rendszerek hasítják ki a legnagyobb szeletet, és várhatóan a közeljövőben sem lesz ez másként. Ezt a szektort még 2,8 milliárd dollárosnak becsülték 2010-ben, de évi közel 20%-os növekedést prognosztizálva közelébe kerülhet a 7 milliárd dollárnak 2015-re. Az arc, írisz, véna és hang alapú felismerő rendszerek alkotják a második nagy szegmenst, szintén 20% körüli éves növekedési rátával. Ez a terület a 2010-es 1,4 milliárdos szintről várhatóan kb. 3,5 milliárd dollárra emelkedik 2015-re [104]. 2010-es adatok alapján a biometria piaci mérete Észak-Amerikában volt a legnagyobb, közel 1,64 milliárd dollárral. Ezután következik Ázsia és a közeli Csendes-óceáni területek (1,160Mrd USD), Európa és Ausztrália (820M USD), Közel-Kelet és India (716M USD), Dél Amerika (516M USD), Afrika (416M USD) [112].

Az elektronikai termékek területén évtizedek óta tapasztalt ár- és méretcsökkenés ill. teljesítménynövekedés, az egyre olcsóbb és jobb képességekkel bíró szenzorok megjelenése természetesen hatással van a biometria eszközök képességeire, árára és elterjedésükre. Várhatóan az otthoni alkalmazások területén új piaci lehetőségek nyílnak meg a következő években. Ezt erősítheti, hogy a tehetős és az új technológiákra fogékony emberek száma világszerte növekszik, különösen a fejlődő világban, így a biztonsági fejlesztésekre várhatóan további igények jelentkeznek.

## 1.6. Etikai vonatkozások

A különböző kultúrákban, társadalmakban a személyes és gazdasági kapcsolatok jellemrajzát igen nagy változatosság jellemzi. Ennél fogva könyvünkben nem törekedhetünk a biometria etikai vonatkozásait nemzetközi viszonylatban bemutatni, kizárólag a magyarországi helyzet tömör értékelésére vállalkozunk.

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (általánosan: adatvédelmi törvény) alapján a következőképpen definiáljuk a személyes adat fogalmát:

"Személyes adat bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;". . .

A biometria információk nagymértékben személyesek, hiszen a legtöbb esetben egyértelműen azonosítják a személyeket. Ugyanakkor speciális adatokról van szó, hiszen a biometria mérések révén közvetetten egyéb személyes adatokat és jellemzőket is meg lehet állapítani (pl. betegségek, életkor, nemiség, faji

hovatartozás). Ezen kívül fontos kiemelni, hogy a testünket azonosító jellemzők nem cserélhetők le, nem módosíthatók, röviden ezek a jellemzők visszavonhatatlanok, állandók. Bár néhány esetben egy-egy jellemzőt lehet helyettesíteni (pl. másik ujjat használni egy beléptető rendszerben), de a már használt jellemző továbbra is a sajátunk marad.

Az egyre több helyen előforduló elektronikus szenzorok, informatikai rendszerek és ezek integrációja lehetővé teszi, hogy az egyes személyekről folyamatosan gyűjtsünk adatokat, ill. ezek az adatok szinte automatikusan rendszerezésre, elemzésre kerüljenek és pillanatok alatt a Föld tetszőleges pontján lekérdezhetővé válnak. A személyünket érintő nagyfokú kiszolgáltatottság és visszaélések elvi lehetősége rengeteg etikai és jogi problémát vet fel, ami sok esetben társadalmi ellenérzést vált ki. A különböző ellenérvek között a leggyakoribbak a következők:

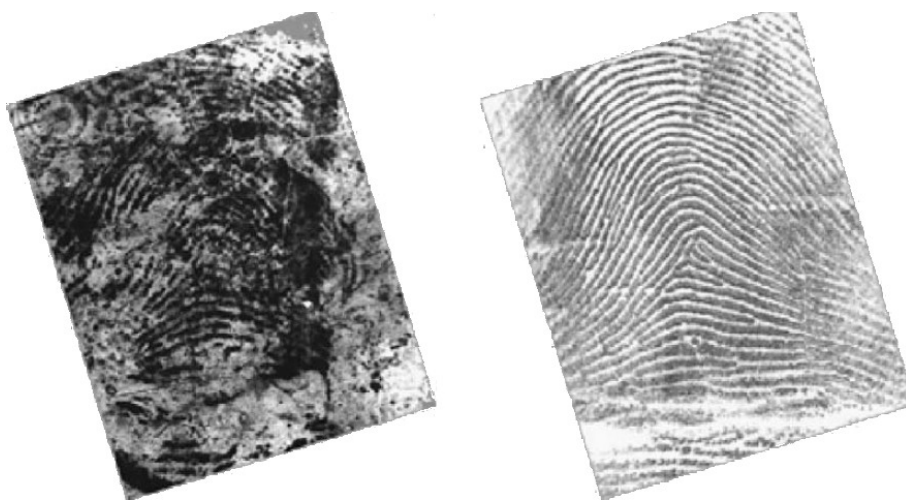
- A begyűjtött információk alapján alapvető személyes, magánjellegű adataink kerülnek be elektronikus adatbázisokba - sokszor automatikus módon - , ahol nem ismert az információ áramlásának útja, illetve a további felhasználás módja és célja.
- A rögzített adatok a rendszerből nem feltétlenül törlődnek, sőt akár harmadik fél irányába ki is szivároghatnak, ami sokféle visszaélésnek lehet az alapja.
- A kiszivárgott - személyt egyértelműen azonosító biometria - adatok nem generálhatók újra. Bár lehet másik ujjat, másik szemet használni a továbbiakban, de másik arcunk, hangunk nem lehet, így a véges biometria jellemzőink egyszerűen "elhasználódhatnak".
- Illetéktelen, rosszindulatú személyek birtokába kerülve vissza lehet élni jellemzőinkkel, pl. meg lehet figyelni napi szokásainkat, vagy akár kompromittáló események szereplőjévé lehet tenni egyeseket.
- Gazdasági, kereskedelmi értelemben is léteznek visszaélések: pl. a vásárlási szokások gyűjtése és elemzése révén egyre kifinomultabb és rafináltabb módszerekkel lehet a vevőket rávenni újabb vásárlásokra, gyakorlatilag a tudtukon kívül lehet az embereket befolyásolni.
- Egészségre vonatkozó adatok kerülnek mások kezébe.
- A mérési folyamat esetleg egészségügyi károsodást okozhat (pl. fertőzések által).
- A biometria rendszerek személyes adatokat gyűjtenek és automatikus döntéseket hoznak. Az így meghozott döntés értelemszerűen függhet magának a felismert személynek a kilététől (ill. annak valamely tulajdonságától), így az egyenlő bánásmód elve akár rejtett módon is sérülhet.

Az itt felsorolt szempontok alapvetően felvetések, de mindenesetre mérlegelendő kockázatokat jelentenek. Talán a lehetséges egészségügyi mellékhatások

tartoznak leginkább abba a kategóriába, amit középtávon, független mérésekkel lehet igazolni vagy cáfolni. Azonban gondoljunk az elmúlt néhány évtized rengeteg a mobiltelefon egészségügyi hatásaival kapcsolatos kutatására, a nagyfeszültségű távvezetékekkel, vagy a terahertz képalkotó berendezésekkel kapcsolatosan felmerülő kockázatokra. Ezen rendszerek egészségügyi kockázatainak megállapítása igen nehézkes, költséges, több évtizedet is igénybe vehet, és az eredmények értékelése sok esetben szubjektív.

Több példa is ismert, amikor látszólag szofisztikált biometria rendszert ért sikeres támadás. Amennyiben egy támadás sikeres, akkor a fenti félelmek jelentős része már egyáltalán nem nevezhető alaptalannak. A biometria rendszerek támadásaival a későbbiekben külön fejezetben foglalkozunk (lásd a 2.5 fejezetet).

A bűnügyi minták elemzése során különös óvatossággal kell eljárni. A szakértői értékelések során is előfordulhatnak súlyos tévedések, függetlenül a biometria módszertől. Nevezetes példa, amikor az FBI szakértői pozitívnak értékelték egy ujjlenyomat egyezést a 2004-ben történt madridi robbantásos terrortámadások<sup>2</sup> nyomozása során. Azonban később kiderült, hogy az FBI által gyanúsított személy ártatlan, a több szakértő által biztosnak mondott egyezés hibáját az FBI elismerte. Az előbbi példában a helyszínen talált szennyezett és az azonosnak ítélt ujjlenyomatot az 1.11. ábrán láthatjuk.



1.11. ábra. Bal oldalon a madridi robbantásnál talált "szennyezett" minta, jobb oldalon az ártatlannak bizonyult gyanúsítottól vett ujjlenyomat minta látható.

---

<sup>2</sup>2004. március 11-én - három nappal a spanyolországi parlamenti választások előtt - összehangolt pokolgépes merénylesorozat történt a madridi helyiérdekű vasúti hálózaton. A robbantásokban 191 ember meghalt és 1800 ember megsérült. A hivatalos nyomozás szerint a támadás mögött egy, az al-Kaidával közvetlen kapcsolatban nem lévő, de a vonzókörébe tartozó terrorcsoport állt.

A témához szorosan kapcsolódik a [36] tanulmány, amely érdekes eredményekről számol be ujjlenyomatok kontextus-függő kiértékelésével kapcsolatban. Több szakértőtől olyan ujjlenyomat párokat gyűjtöttek, ahol korábban saját maguk egyértelmű egyezéseket találtak, az egyezések helyességét független szakértő által is leellenőriztették. (Az egyik minta bűnügyi helyszínről származott.) Később ugyanezen minták kiértékelését kérték tőlük, azzal a hamis háttérinformációval, miszerint a most mutatott képeket még nem ismerik, de ezeket az FBI korábban **hibásan** egyezőnek minősítette. A kérés szerint azonban rutinszerűen kellett eljárniuk, a szokásos módszereiket lehetett használniuk, a minták egyezését cáfoló háttérinformációt tehát hivatalosan nem vehették számításba. Az öt felkért szakértő közül most azonban csak egy állította, hogy a minták egyeznek. Egy úgy nyilatkozott, miszerint nem tudja eldönteni az esetleges egyezőséget, míg hárman egyértelműen azt mondták, hogy a minták nem egyeznek. Azaz a háttérinformáció nagymértékben befolyásolta a szakértők munkáját, a szakértői véleményeket, hiszen ötből hárman megváltoztatták korábbi döntésüket. Ezen példákból azt a következtetést tudjuk levonni, hogy a modern biometria rendszerek sem tévedhetetlenek, illetve a szakértői vélemények sem feltétlenül korrektek, a több éves gyakorlattal rendelkező szakértők is befolyásolhatók akár félrevezető információkkal. Ezek alapján tehát nem teljesen alaptalanok azok a félelmek, miszerint hiba lenne teljes bizonyossággal bízunk a biometria rendszerekben, sőt azok számos szándékos vagy nem szándékos visszaélésnek lehetnek a tárgyai és eszközei.

Szabó Máté Dániel (jogász, adatvédelmi szakértő) a Biometrikus azonosítás és adatvédelem című írásában foglalkozik a kérdéskörrel [102]. Összegzőként a következő javaslatokat teszi:

"A nyers biometria adatokat (például képeket) használó biometrikus azonosító rendszerek sok veszélyt hordoznak magukban, ezért velük szemben előnyben részesítendőek azok, amelyek az ilyen adatokból visszafordíthatatlanul képzett sablonok alkalmazásán alapulnak.

1. Azok a biometrikus azonosító rendszerek, amelyek nem járnak a biometria adatok vagy sablonok adatbázisban történő kezelésével, adatvédelmi szempontból sokkal kevésbé lehetnek aggályosak, ezért az olyan megoldások fogadhatók el adatvédelmi szempontból, amelyek esetében a biometria adat vagy sablon az érintett birtokában van, olyan adathordozó eszközön, amelyhez kizárólag ő férhet hozzá, és az adatokat sehol máshol nem tárolják.
2. Ha elengedhetetlen az adatbázisok használata, mert az adatkezelés célja a személyazonosság megállapítása, vagy ha a biometria adatokat az érintett által hagyott nyomokból gyűjtik össze, esetleg ha az érintett tudta nélkül történik az adatok felvétele, akkor az adatkezelés alapvető jogot érint, ezért csak olyan körülmények között lehetséges, ahol az érintettek valóban önkéntes hozzájárulásával történik mindez, vagy pedig a szükségesség és az arányosság követelményének figyelembevételével törvény rendeli el a

biometria adatok használatát. Ilyen, törvény alapján kötelező biometria adatkezelést csak különleges biztonsági célok indokolhatnak.

3. Az általánosan használható személyazonosító adattá válás elkerülése érdekében népesség-nyilvántartásba biometria adatot kötelezően felvenni nem szabad.
4. Ugyanezen cél érdekében nem szabad megengedni, hogy az egyes biometria kus azonosító rendszerek ugyanazon fizikai jellemzőből ugyanazt a sablont állítsák elő."

A biometria rendszerek alkalmazása tehát nem csak műszaki, hanem jogi, etikai, gazdasági és politikai kérdés is egyben. Mindenképpen figyelemmel kell lenni a törvényi szabályozásra, és a legnagyobb mértékben tekintettel kell lenni a személyiségi jogokra.



1.12. ábra. Kézi írisz olvasó az amerikai hadsereg iraki használatában [9]

A magánélettel kapcsolatos félelmek az internet kiterjedt használatból eredően ma már igencsak jogosak, hiszen az ott megjelenő információk a kézzel fogható valóság olyan kiterjesztései, amelyek a nagyteljesítményű adatfeldolgozó mechanizmusok révén könnyen és nagy mennyiségben felfedezhetők és összefüggésbe hozhatók egymással. Acquisti és munkatársai több olyan kísérletet folytattak, ahol azt mutatták be, hogyan lehetséges egyes személyazonosságokat az internet által felfedni, sőt ún. érzékeny személyi adatokat megszerezni [1]. Tanulmányukban bemutatták, hogyan lehet a gépi arcfelismerést, a felhő számítási technológiát és az online közösségi hálózatokat együttesen felhasználni személyek azonosításához, még hozzá oly módon, hogy csak nyilvánosan, a

kereskedelmi forgalomban elérhető eszközöket használták fel. Az első kísérletükben az interneten talált arcképekből indultak ki és kerestek azokhoz - az azonosítást egyértelműsítő - releváns információkat. A második kísérletükben egy észak amerikai egyetemi campuson gyűjtöttek arcképeket webkamera segítségével, majd pedig a továbbiakban lényegileg az előző kísérlethez hasonló módon eljárva, a személyek 30%-a esetében tudták az azonosítást megtenni. A harmadik vizsgálat arra terjedt ki, hogy a második kísérletben sikeresen azonosított személyek esetén hogyan lehetséges az ún. SSN-t (Social Security Number - társadalombiztosítási azonosító) meghatározni. Az Amerikai Egyesült Államokban ez a szám igen sok szolgáltatáshoz szükséges, és ismerete bár önmagában nem jelenti a személyazonosság tulajdonlását, mégis az egyénre nézve igen nagy biztonsági kockázatot jelent.

Valójában a fenti tanulmánynak nem a könnyen elvégezhető automatikus arc alapú azonosítás a lényege, újdonság értéke, hanem a számítógépes technológiák együttes használata esetén felmerülő személyiségi ill. jogi kérdések. Fontos észrevenni, hogy míg szükség esetén néhány a személyhez lazán kötődő adatot meg tudunk változtatni (pl. hálózati azonosítót, nevet, jelszót), addig az arcunkat és egyéb biometria azonosítóinkat nem. A fenti példák pedig azt illusztrálják kitűnően, hogy akár ezekből az egyedi, megváltoztathatatlan jellemzőkből kiindulva, a különböző rendszerekben tárolt ránk vonatkozó információk együttes felhasználásával, elemzésével egészen részletes képet lehet alkotni rólunk - és mindezt tudtunkon kívül.



## 2. fejezet

# A biometrikus rendszerek általános modellje

### 2.1. Biometria, mint osztályozási feladat

A biometrikus rendszerek lényegileg azonosítási feladatot végeznek, aminek alapvetően többféle módja van. Minden esetben van egy vagy több lekérdezés, azaz az aktuálisan ellenőrizendő személy valamely jellemzőjéről gyűjtünk be adatokat, amelyeket összevetünk korábban rögzített egy vagy több biometriaival ("template"). Alapvetően két fő működési módot különböztetünk meg:

- **Ellenőrzés** ("positive identification", "verification"): Ebben az esetben a vizsgálat során vett mintát csak egy adott lehetséges személy korábban rögzített mintájával vetjük össze. Ilyenkor egy azonosító begépelésével, kártya használatával vagy más módon adjuk meg, hogy konkrétan ki a jelölt személy, tehát elegendő a hozzá tartozó mintával való összevetés. Ebből következik, hogy az összehasonlítás gyorsan meg tud történni. Abban az esetben, ha a személyhez tartozó kártya tartalmazza a biometrikus template-et, akkor nincs is valójában szükség egy központi adatbázisra, elegendő valamilyen módon a kártya érvényességét ellenőrizni, ill. összehasonlítani a kártyán tárolt adatokat a felhasználóval (azaz biometrikus jellemzőivel).
- **Azonosítás** ("identification"): Ha a személyazonosság megállapításához nincs konkrét jelöltünk, akkor az adatbázisban szereplő összes személy mintáját össze kell vetni az aktuálisan látott személy éppen mért adataival. Az adatbázis tartalmazhat néhány tucát, néhány száz, ezer, de akár több százmillió mintát is, ezért az ilyen rendszereknek a működése a valós idejű alkalmazásoktól az ún. offline jellegű esetekig terjedhet.

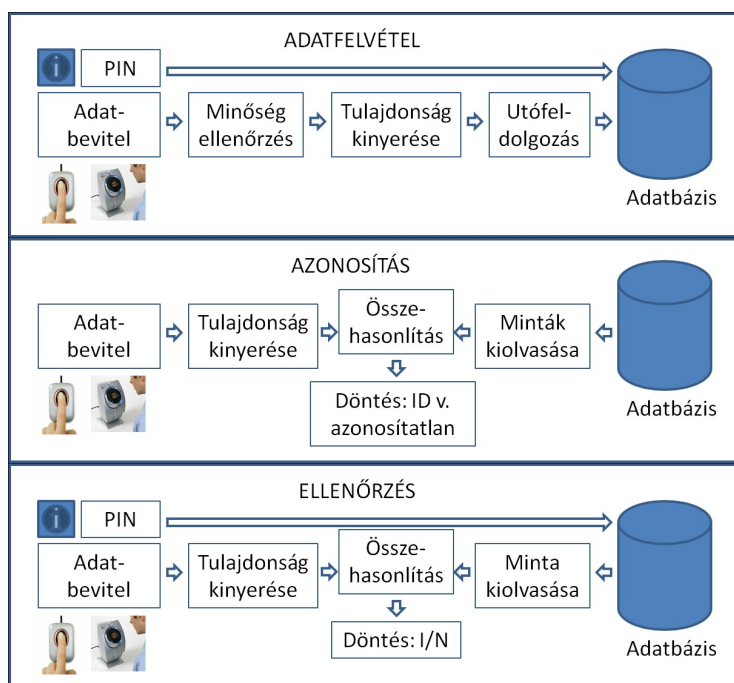
A biometria vizsgálatok során valójában statisztikai alakfelismerésről van szó, miszerint ahány személy van az adatbázisban, mindegyik egy-egy objektum osztálynak felel meg. Azonosítás során az ismeretlen mintát kell besorolni

valamelyik korábban "betanított" osztályba. Természetesen innen adódik, hogy a statisztikai osztályozásban használt klasszikus módszerek nagy része kiválóan alkalmazható a biometriai összehasonlítások során, mint pl. a legközelebbi szomszéd (Nearest Neighbor - NN), k legközelebbi szomszéd (k-NN), neurális hálózatok vagy éppen a támasztóvektor gépek (Support Vector Machine - SVM).

## 2.2. Az azonosítás általános modellje

Függetlenül attól, hogy milyen biológiai jellemzőket mérünk, az azonosítás folyamata kisebb eltérésektől eltekintve minden esetben megegyezik: a rendszert adatokkal kell feltölteni (adatfelvétel és template előállítása), ellenőrzés vagy azonosítás során pedig az aktuálisan mért adatokat hasonlítjuk az adatfelvétel során rögzített mintákhoz. Tekintsük át a folyamat főbb pontjait (a 2.1 ábra grafikusán illusztrálja az egyes lépéseket):

- **Adatfelvétel** ("enrollment"):
  1. Egy vagy több személyes jellemző adatot rögzítünk.
  2. Ellenőrizzük, hogy a nyers adatok megfelelnek-e bizonyos minőségi követelményeknek. Ezt az ellenőrzést esetleg a biometriai jellemző kivonása után is el lehet végezni.
  3. Tulajdonság kivonása (képi jellemzők detekciója és mérése).
  4. Ha több felvétel is volt, akkor lehet átlagolással, középérték kiválasztással egy megfelelő reprezentánst előállítani. Bizonyos rendszerek több értéket is tárolnak egy-egy személyhez.
  5. Minta tárolása.
- **Ellenőrzés** ("verification"):
  1. Azonosító meghatározása.
  2. Azonosítónak megfelelő tárolt minta kiolvasása (pl. adatkártyából).
  3. Felvétel készítése.
  4. Tulajdonság kivonása a felvételtől (képi jellemzők detekciója és mérése).
  5. A tulajdonságot reprezentáló minták összehasonlítása.
  6. Döntési szabály alkalmazása.
- **Azonosítás** ("identification"):
  1. Felvétel készítése.
  2. Tulajdonság kivonása a felvételtől (képi jellemzők detekciója és mérése).
  3. Adatbázisból lehetséges minták kiolvasása.
  4. 1:N-hez való összevetések elvégzése.



2.1. ábra. Az adatfelvétel, azonosítás és ellenőrzés folyamatai

#### 5. Döntési szabály alkalmazása.

Megemlítjük, hogy a tulajdonság kivonása során az első lépések egyikeként az értékes információ hordozó jelet le kell határolni a környezetétől, pl. egy arc-képet szegmentálni kell a háttértől; ezt ebben a konkrét esetben arcdetekciónak hívjuk. Önmagában ez a szegmentálás sem mindig egyszerű feladat, különösen akkor, ha nem akarunk a felhasználóknak feladatot adni, azaz nem várunk el tőlük túl sok interakciót és támogatást. Más esetekben, pl. ujjlenyomat esetén az ujj elhelyezése a szenzoron lényegesen leegyszerűsíti a feldolgozandó terület behatárolását, de a kép normalizációjára, standardizálására így is ügyelni kell (pl. az ujjlenyomat képet a megfelelő irányba kell forgatni).

Mind az ellenőrzés, mind az azonosítás során minták összehasonlítását kell végezni, aminek a kimenete egy hasonlósági mutató lesz. Mivel a végeredmény igen/nem jellegű kell hogy legyen, így a hasonlósági érték küszöbölésével tudjuk ezt a döntést meghozni.

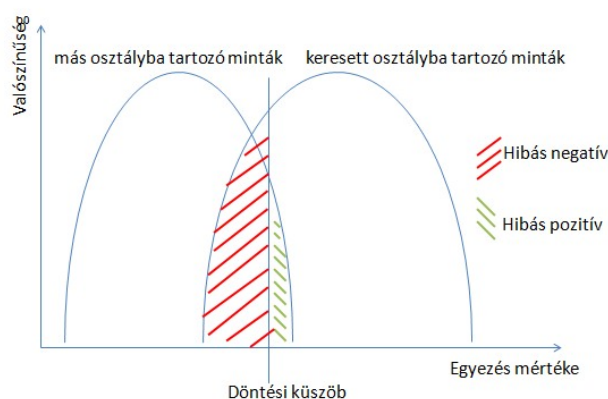
## 2.3. A biometriai módszerek pontossága

A felhasználók számára nagyon fontos kérdés, hogy egy adott biometriai módszer mennyire pontos, mennyire megbízható. Nos, ezt a kérdést nem egyszerű

## 282. FEJEZET. A BIOMETRIKUS RENDSZEREK ÁLTALÁNOS MODELLJE

megválaszolni, ugyanis először tisztázni kell, hogy mit értünk pontosságon. A következőkben a különböző lehetséges hibafajtákról lesz szó, majd pedig azokról a mutatókról, amelyek jellemzik a rendszerek hibázásra való hajlamát. Minden osztályozás során felmerülhet, hogy hibát követ el a módszer, például nem minden esetben sorolja be a felismerendő személy mintáját a megfelelő, korábban látott minta által definiált osztályba. Ha nem követünk el hibát, akkor egyezés esetén a minta pozitív (megtaláltuk a keresett személyt), ha nincs egyezés, akkor az aktuális vizsgált mintára a negatív kifejezést használjuk. Kétféle döntési hibát lehet megkülönböztetni:

- hibás/fals pozitív (elsőfajú hiba, false positive, FP): ebben az esetben egyezést jelzett a rendszer, holott nem kellett volna, ténylegesen az összehasonlított minták más-más személytől származnak.
- hibás/fals negatív (másodfajú hiba, false negative, FN): a ténylegesen egyező minták párosítása során sem talált egyezést a rendszer.



2.2. ábra. Különböző egyezések valószínűsége azonos és más osztályba tartozó minták esetén

Értelemszerűen - helyes döntések esetére - definiálhatjuk a TP (true positive) és TN (true negative) kifejezéseket is. Az elsőfajú hiba és a másodfajú hiba gyakorisága összefügg egymással: ha az egyik csökken, a másik szükségszerűen nőni fog, a kettő arányát - felhasználó szinten, a legegyszerűbben - a döntési küszöb állításával tudjuk befolyásolni. Azaz ha a küszöb alatti egyezést mérünk, akkor elvetjük a jelöltet, ellenkező esetben elfogadjuk. Ezt a jelenséget illusztrálja a 2.2 ábra, ahol az egyezés mértékének valószínűségét ábrázoltuk, attól függően, hogy a jelöltek a keresett osztályba, vagy más osztályba tartoznak. Jól látszik, hogy ha a két görbe erősen átlapolódik, akkor számottevő lesz a hiba mértéke, ha viszont nem metszenek egymásba, akkor található olyan küszöbszám, amivel hiba nélkül tud a módszer működni. Tehát a döntési hiba erősen függ a különböző osztályokat jellemző tulajdonságok eloszlásától. Később - néhány biometria

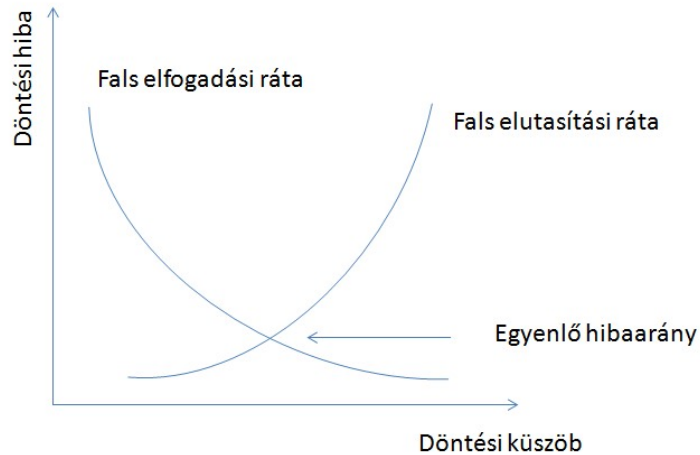
jellemző tárgyalásánál - konkrétan látni fogjuk, hogy a biometria leírók egyik legfontosabb jellemzője, hogy hogyan alakul az osztályokon belüli és az osztályok közötti szórás, azaz mennyire hasonlóak az egy azonos személyhez tartozó leírók, és mennyire térnek el azok egymástól, ha különböző személyekhez tartozó mintákat vizsgálunk.



2.3. ábra. Francois Brunelle kanadai fotóművész évek óta kutatja a hasonló arcokat. "I'm not a look-alike!" című projektjének célja összegyűjteni 200 hasonmást (akik nem állnak közeli genetikai kapcsolatban egymással). A kép forrása <http://www.francoisbrunelle.com>.

Biometria rendszereknél általában a hibás elfogadási arány/ráta (HER) és hibás elutasítási arány/ráta (HEUR) kifejezéseket használják a hibás pozitív és hibás negatív helyett. Ezek az arányok azt mondják meg, hogy mi a valószínűsége a tévedésnek adott feltételek esetén (avagy 100 esetből hányszor fogunk átlagosan hibázni). A rendszer szigorúságát a döntési küszöb adja meg, így azt az alkalmazás jellegének függvényében tudjuk állítani. Egy fokozottan védett létesítmény esetén (pl. atomerőmű) érdemes a döntési küszöböt magasra állítani, így nagyon kicsi az esélye annak, hogy illetéktelenek jutnak be, azonban viszonylag relatíve gyakran fordul elő olyan eset, hogy egy ott dolgozó nem tud bejutni, csak esetleg egy újabb ellenőrzés után. Ezzel szemben egy teniszkлубban túl zavaró lenne, ha gyakran kellene blokkolni a tagok bejutását, viszont kicsi a kockázata, ha esetleg egy illetéktelen személy is bemegy a létesítménybe. Így a döntési küszöböt érdemes alacsonyabb szinten megállapítani.

A hibás elfogadási ráta és hibás elutasítási ráta függvények alakja jól jellemzi egy biometria rendszer pontosságát. Ha a görbék alacsonyan futnak, akkor ala-



2.4. ábra. A döntési küszöb hatása a döntési hibákra

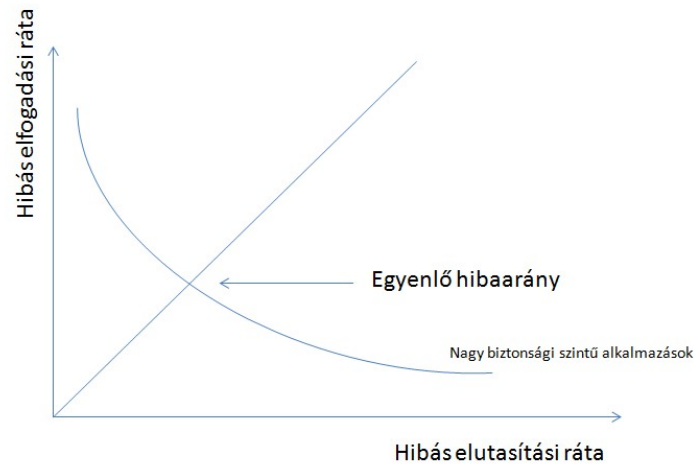
csongyan metszik egymást, így kevés hibával számolhatunk (lásd 2.4 ábra). Sok rendszer ismertetése során nem adják meg a függvényalakokat, hanem csak azt specifikálják, hogy milyen értéken metszi egymást a két görbe. Ezt az értéket egyenlő hibaarányának (Equal Error Rate - EER) vagy keresztező hibaarányának (Crossover Rate) nevezik. A Receiver Operating Characteristics Curve (ROC Curve, "vevő működési karakterisztikus görbe"<sup>1</sup>) szintén helyettesítheti a két függvény megadását, ebben az esetben a két hibát egymás függvényében ábrázoljuk, erre a 2.5. ábra mutat példát.

A biometriában még három másik számszerű mutatót is gyakran használnak, amelyek a hibafüggvények mellőzésekor jöhetnek szóba:

- Nulla hibás egyezés arány (Zero False Match Rate - ZeroFMR, ): a legalacsonyabb hibás elutasítási érték, amikor a hibás elfogadási érték nulla.
- Nulla hibás elutasítási arány (Zero False Non-Match Rate - ZeroFNMR): a legalacsonyabb hibás elfogadási érték, ahol a hibás elutasítási érték nulla.
- Minimális fél teljes hiba arány (Minimum Half Total Error Rate - MinH-TER): a következő kifejezés minimális értéke:  $HTER(t) := (HER(t) + HEUR(t))/2$ , ahol  $t$  a küszöbérték.

Abban az esetben, ha egy szűrés ("screening") típusú lekérdezést hajtunk végre egy biometrikus adatbázison, a szokásos információ-visszakeresés mutatókat lehet használni (itt a TP, TN, stb. jelölések az esetek számára vonatkoznak):

<sup>1</sup>A kifejezés eredete a 2. Világháborúba nyúlik vissza. A radar jelek feldolgozásával foglalkozó mérnökök kezdték el használni ezt az osztályozást jellemző mutatót. A feladatuk annak a jellemzése volt, milyen pontossággal tudják meghatározni a vett radarjelekből, hogy a bemért jel ellenséges vagy baráti objektumról származik, esetleg csupán zajról van szó.



2.5. ábra. A "Receiver Operating Characteristics Curve"

- Precizitás (precision):  $TP/(TP+FP)$ , azaz az összes találatok között vesszük a helyes találatok arányát.
- Felidézés (recall):  $TP/(TP+FN)$ , a teljes keresés alatt lévő adatbázisból a valóban megfelelő objektumok hány százalékát sikerült megtalálni.
- Pontosság (accuracy):  $(TP+TN)/(TP+TN+FP+FN)$ , azaz a keresés során hányszor hoztunk helyes döntést, legyen az pozitív vagy negatív.
- F-mérték (F-score):  $2 \times (\text{felidézés} \times \text{precizitás}) / (\text{felidézés} + \text{precizitás})$ , a precizitás és a felidézés harmonikus közepe.

Nem szabad elfelejtenünk, hogy nem csak a felismerés során fordulhatnak elő hibák. Adatfelvételkor, amennyiben nem felel meg a minta az előzetesen definiált minőségi kritériumoknak, el kell utasítani a bevitelt (Failure to Enroll). Ha felismerés során készül rossz mintarögzítés, akkor is hasonlóan kell eljárni (Failure to Acquire v. Failure to Capture).

Végezetül elmondhatjuk, hogy egy módszer pontossága nagyban függ a mérési feltételektől, a minták szennyeződésétől, a konkrét minták eloszlásától és a kiértékelési módszertől. Természetesen messze nem csak arról a trivialitásról van szó, hogy a tesztelést nem a betanítás során felvett mintákon kell kiértékelni, hanem arról, hogyan reagál egy rendszer a változó körülményekre. Példának okáért ha arc alapján szeretnénk személyeket azonosítani, akkor nem mindegy, hogy milyen felbontással állnak rendelkezésre az arcképek, és az sem, hogy sikerült-e minden esetben szemből elkészíteni a fotókat.

Egy adott termék kiértékelését ezért célszerű valamilyen független szervezetre bízni, a reklámokban szereplő minőséget jellemző adatok sok esetben megkérdőjelezhetőek, főként akkor, ha nem tudjuk a tesztadatbázis méretét, jellegét és az adatgyűjtés és tesztelés pontos körülményeit.

## 2.4. Röviden a biológiai változatosságról

Ahogy pl. már a 2.4. ábra is illusztrálta, ha az egyes személyeket a biológiai tulajdonságuk szerint szeretnénk megkülönböztetni, akkor előfordulhat, hogy a mért jellemzők alapján a megkülönböztetés nem lesz sikeres. Ennek igen sokféle oka lehet: ilyen például a rossz objektumdetekció, a rossz tulajdonságkinyerés, különböző zajok megléte. Az is alapvető kérdés, hogy a mért tulajdonságok alapján (függetlenül az egyéb zavaró tényezőktől) a személyek egyáltalán megkülönböztethetők-e. Azaz nagy fontossága van annak, hogy az osztályon belüli és az osztályok közti változatosság, szórás hogyan alakul. Ideális esetben az előbbi kicsi, míg az utóbbi relatív nagy. Ezeket a változatosságokat több tényező határozza meg:

- a genetikai adottságok (genotípussal azonosítható),
- fejlődésbeli és környezeti hatások (a fenotípussal azonosítható): az egyed specifikus megjelenésére gondolunk itt, ami változatos lehet egy adott populáción belül, együttesen függ a génektől, a fejlődési folyamattól és a környezeti hatásoktól,
- genetikai penetráció: valamely tulajdonság milyen mértékben van elterjedve, ill. milyen mértékben öröklhető (ezzel kapcsolatos statisztikai adatokat az írisz alapú biometriai módszerek tárgyalásánál mutatunk be).

A genetikai értelemben azonos személyek genotípusos jellemzői megegyeznek (pl. vércsoport, DNS), a megjelenő biológiai tulajdonságaik azonban valamilyen mértékben sorolhatók a genotípusos vagy fenotípusos kategóriába.

Mivel néhány biometriai jellemzőnk időben változik (pl. a hangunk vagy az arcunk) ezért az ebből adódó döntési hiba (hibás negatív) esetén beszélhetünk fenotípus hibaarányról is. Az emberi populációra az jellemző, hogy közel 1% az ikerpárok aránya, akik genetikailag azonosnak tekinthetők. Ennek a következménye lesz egy alap szintű hibás pozitív döntési ráta, ami valójában egyfajta genotípus hibaarány.

Pontosabban vizsgálva az utóbbi esetet azt találjuk, hogy minden 80 szülésre 1 ikerszülés jut, aminek a harmada tartozik az egypetéjű ikrek közé. Azaz 240 szülés esetén 243 gyermek születik, akik közül ketten fognak azonos genetikai kódcsellettal rendelkezni. Ez alapvetően meghatározza a DNS alapú biometria elvi hibáját is.

Valójában ennél kicsit bonyolultabb a valós helyzet: az egypetéjű ikrek genetikai kódja sem teljesen azonos, ennek az okai többek között azok a genetikai



változások, melyek a magzati fejlődés korai szakaszában alakulhatnak ki (úgynevezett "másolási hibák"), de mivel az X vagy az Y kromoszómákban ezek az eltérések nem jelentkeznek, így nem öröklődnek tovább.

## 2.5. A biometrikus rendszerek lehetséges támadásai

A biometrikus rendszereket érő támadásokat alapvetően kétféle csoportba lehet sorolni:

- **Közvetlen támadás ("direct attack"):** Közvetlenül a szenzort éri a támadás, méghozzá olyan módon, hogy hamis, szintetikus mintákat rögzít a szenzor. Ezt könnyen el lehet érni korábban rögzített, majd reprodukált 2D-s vagy 3D-s mintákkal (nyomtatott arcképpel, írisz képpel, előre felvett hangmintával vagy pl. gumi ujjlenyomattal). A támadás előnye, hogy a támadónak nem kell előzetesen részletes technikai információval rendelkezni a megtámadott rendszerről. Természetesen az ilyen esetek ellen is vannak védekezési módok: leggyakrabban valamilyen tevékenységet várnak el az ellenőrzött személytől, például meg lehet vizsgálni a pislogásokat, lehet kérni kicsit változtatott hangmintát, meg lehet vizsgálni az ujj hőmérsékletét vagy lehet kérni egy másik ujjat az ellenőrzés céljára.
- **Közvetett támadás ("indirect attack"):** A támadás az informatikai rendszer valamelyik részét éri, például az eltárolt mintákat vagy a különböző kommunikációs csatornákat. Természetesen ez jóval nagyobb technikai felkészültséget igényel, annál is inkább, mivel az informatikai rendszert jól fel lehet készíteni az ilyen támadásokra (pl. titkosítással, vízjelezéssel).

A 2.6. ábrán számokkal jelöltük meg egy általános rendszer lehetséges támadási pontjait. Az első pont kivételével mindegyik támadás az indirekt kategóriába tartozik. Vegyük most ezeket sorba:

**1:** Hamis ujjlenyomatot vagy egyéb biometriai jellemzőt használnak.

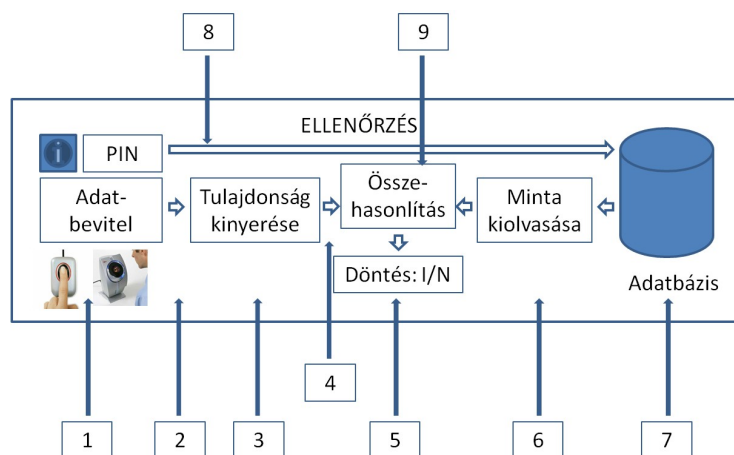
**2:** A rögzített jelet (pl. képet) ellopják, kicserélik.

**4,6,8:** A kommunikációs csatornát éri támadás, adatlopás vagy adatcsere történhet.

**3,7,9:** Trójai programmal a rendszerbe jutva módosítani lehet annak működését.

**5:** A rendszer kimenetén avatkoznak be, csak magát a döntést módosítja a támadó.

Ismertek esetek, amikor egyszerű fényképekkel kijátszották a kereskedelemben kapható biometrikus rendszereket. Kiváló példa erre a [92] cikk, ahol azt mutatják be, hogyan lehet kereskedelmi nyomtatóval készített írisz képekkel 50%-os valószínűséggel becsapni egy azonosító rendszert.



2.6. ábra. Egy azonosító rendszer lehetséges támadási pontjai

[46] arról számol be, hogy az ún. IrisCode-ból (amelyet sok rendszer az összehasonlítás során használ) sikeresen állítottak vissza olyan írisz képeket, melyek alkalmasak voltak az ellenőrző rendszer megtévesztésére kb. 85%-os valószínűséggel. Valójában több megfelelő írisz képet is elő tudtak állítani erre a célra (osztályon belüli variációk). Mindez azt jelenti, ha egy indirekt támadással megszerezzük valakinek az írisz kódját, akkor egy közvetlen támadással sikeresen csaphatnánk be az azonosító rendszert. (Megjegyezzük, hogy a nagyfelbontású kamerák korszakában nincs szükség a leíró kód megszerzésére, valójában sokkal egyszerűbben meg lehet szerezni az írisz jó minőségű fényképét.)

## 3. fejezet

# Szabványok

A nemzetközi szabványok jelentősége az elektronikai és informatikai ipar globalizációjával természetesen nő. Sőt, egyre nyilvánvalóbb az is, hogy a vállalatok növekedésében is egyre nagyobb a jelentősége a szabványoknak a szabadalmakkal körbeágyazott technológiákkal szemben [33].

A 2001. szeptember 11-i ikertornyokat ért támadások előtt kevés biometria szabvány létezett. Az egységesítés területén az egyik legfontosabb eredmény az ANSI/NBS-ICST 1-1986 szabvány volt, ami az ujjlenyomatokat kezelő rendszerek közti adatok átadásával foglalkozott. A szabvány létrehozásának motivációja alapvetően rendészeti területéről volt meghatározó. Az egyik legjelentősebb, nem szabványügyi testület által vezetett törekvés az ún. BioAPI Consortium [10] volt, amit 1998-ban hoztak létre, hogy megfelelő platformfüggetlen API (Application Programming Interface) álljon rendelkezésre biometrikus alkalmazások fejlesztéséhez. A konzorcium eredményeit később nemzetközi szabványok is felhasználták.

A 2001-es események után egyre inkább felerősödött az igény, hogy a biometria módszereket ne csak a bűnüldözésben, hanem a civil szférában is - nemzeti és nemzetközi szinten egyaránt - egységesebb jogi és technikai körülmények között használhassák. 2001 végén az ANSI (American National Standards Institute) által akkreditált INCITS-en (International Committee for Information Technology Standards) belül azzal a céllal hozták létre az M1 műszaki testületet (M1 Technical Committee on Biometrics), hogy koordinálja az ipari, akadémiai és kormányzati szervezetek konszenzusán alapuló fejlesztéseket.

Ezzel párhuzamosan - az USA kezdeményezésére - a nemzetközi szabványosítás érdekében 2002. júniusában létrejött az ISO-n belül a 37-es altestület (SC37), amihez már a kezdetekkor 17 ország csatlakozott [103]. Az SC37-en belül alapvetően hat főirányt lehet megkülönböztetni, amelyekkel külön munkacsoportok foglalkoznak:

1. elnevezések és elvek harmonizációja;
2. biometria adatok átvitele, API-k;
3. interoperabilitást biztosító adatformátumok szabványosítása;
4. szabványnak megfelelő alkalmazás profilok;
5. teljesítményleszték és jelentések;
6. tesztelési módszertanok kidolgozása, jogi és társadalmi aspektusok vizsgálata.

A szabványok kidolgozása jól elkülöníthető lépésekben nyilvánul meg, az ISO esetén ezek a fázisok a következők:

1. Új munkajavaslat kidolgozása.
2. Munkaverziók, előterjesztések, vázlatok.
3. Bizottság szintű előterjesztések.
4. Nemzetközi szabvány előterjesztések.
5. A végleges nemzetközi szabvány előterjesztése.
6. Az elfogadott nemzetközi szabvány publikálása.

A munkacsoportok több tucat szabványt hoztak létre az elmúlt években, néhányat említünk meg ezek közül (az egyértelműség kedvéért itt az eredeti angol elnevezést használjuk):

- Fingerprint minutiae 19794-2;
- Fingerprint image 19794-4;
- Face image 19794-5;
- Iris image 19794-6;
- Hand geometry image 19794-10;
- Testing and reporting fundamentals 19795-1.

Más szabványosító testületek is aktívak még a biometria területen, úgy mint az International Telecommunication Union (ITU-T), az International Civil Aviation Organization (ICAO), valamint az Organization for the Advancement of Structured Information Standards (OASIS) és az Open Group is végez kapcsolódó munkákat. Az ANSI is több szabványt specifikált a témában, amelyek sok esetben - bár nem mindig - megfelelnek a nemzetközi szabványoknak.

Egyre több közigazgatási vagy kereskedelmi területen jelennek meg a különböző nemzetközi szabványoknak megfelelő alkalmazások. Egyik példája ennek

a Unique Identity Authority of India (UIDAI) szervezet ún. Aadhaar projektje, ahol a tervek szerint 1,2 milliárd állampolgárról gyűjtenek be biometrikus adatokat [107]. Az ICAO is követ bizonyos biometrikus ISO szabványokat, például az arcaazonosítás során keletkező adatokat szabványos módon tárolják.



## 4. fejezet

# Bőr redőzet

A bőr redőzete az egyénekre egyedileg jellemző mintázattal bír, legyen szó az ujjról, tenyerről vagy akár a talpról. Könyvünkben legfőképpen az ujjakon megfigyelhető mintázatokkal ill. azok biometria feldolgozásáról fogunk részletesen beszámolni, mivel döntőrészt azok használata jellemző a biometria rendszerekben. Természetesen a leírt információkat jelentős részt adaptálhatjuk a többi említett testrész esetén is.

A bőr redőzetének személyazonosítás céljából való kriminalisztikai vizsgálatát **daktiloszkópiának** nevezik, természetesen ez vonatkozik a talpra és a tenyérre is az emberi ujjakon kívül. A szó görög eredetű, jelentése: daktilo - ujjakat, szkópia - nézni.

Az orvosi tudományokban a bőr mintázatának vizsgálatát antropológiai **dermatoglífiának** nevezik (dermato - bőr, glífia - rajzolat, véset). Feladata a mintázatok öröklődésével, genetikai rendellenességek (pl. Down kór) rajzolatból való kimutatásával kapcsolatos, vagy különböző népcsoportoknak, etnikumoknak a bőrredőkben megjelenő sajátosságainak kutatása. Míg a daktiloszkópia a személyek egyedi azonosításával foglalkozik, a dermatoglífia statisztikai alapon vizsgálja a populációt vagy annak egy részét.

A **kiromantia** a tenyér mintázatával foglalkozik, korábban az orvosképzés része volt. Ma azonban elsősorban az áltudomány kategóriájába sorolt tenyérjólást értjük alatta.

### 4.1. Ujjlenyomat azonosítása

Egyes irodalmi források megkülönböztetik az ujjnyomot, ujjlenyomatot és az ujjnyomatot [67]. Ezek szerint az **ujjnyomok** azok a mintázatok, amiket az ujj véletlenszerűen hagy bizonyos tárgyakon. Ezeknek a minősége nem túl jó, sokszor az ujj teljes mintázatának csak egy részletét tartalmazzák, többé-kevésbé szennyezettek és speciális fizikai, kémiai ill. elektronikus módszerekkel kell feljavítani őket, hogy a felismerésben használhatóak legyenek. Angolul "**latent fingerprint**"-nek nevezik ezeket. Egyes esetekben ezek a nyomok igen jól lát-

hatók szabad szemmel is, mivel valamilyen anyag (pl. por, liszt, agyag) kenődik az adott felületre, ezeknek a neve **"patent print"**. Az ún. **"plastic print"** olyan ujjnyom, amit valamilyen puha anyagban, pl. műanyagban, agyagban, gittben hagy az emberi kéz.

Az **ujjlenyomatok** a rendőrség által is készített, az ujj körbenyomásával készülő, jó minőségű képek. Ezeket angolul **"exemplar"**-nak, azaz **mintapéldánynak** nevezik.



4.1. ábra. Rendőrségi ujjlenyomat (Anna Vasilievna Timiriova orosz költő rendőrségi ujjlenyomata, amit 1950-ben a szovjet rendőrség készített a letartóztatása során)

Az **ujjnyomatok** az előbbiek csak egy részét jelentik, tipikusan sík felületen keletkeznek, és jó minőségű képek. A 2D-s biometria szkennernek tipikusan ilyen képeket készítenek. Angolul ezeket is fingerprint-nek nevezik.

Az angol biometria szakirodalom, a hazai köznyelv, sőt a hazai szakmai irodalom sem fektet valójában hangsúlyt ezekre a specifikus elnevezésekre, általában használhatjuk az ujjlenyomat (fingerprint) kifejezést. Elsősorban akkor érdemes a különbségeket kihangsúlyozni, ha rendészeti környezetben, az egyes esetek megkülönböztetésére van szükség. A jelen könyvben is a széles körben elterjedt ujjlenyomat kifejezést használjuk.

#### 4.1.1. Története

Ujjlenyomatokat találtak már többek között ókori babiloni agyagtáblákon, pecséteken, agyagedényeken, téglákon, egyiptomi sírkamrák falain, kínai és görög vázákon, edényeken, római cserepeken, téglákon. Természetesen ezek jó része az elkészítés során véletlenszerűen került fel a tárgyak felületére, de jelentős részük díszítésként, illetve minden bizonnyal a személyazonosság jeleként. Erre többek között onnan lehet következtetni, hogy ezekben az esetekben az ujjlenyomatokat nagyon mélyen nyomták bele az anyagba. Kínában selymen és papíron is talál-



tak ókori ujjlenyomatokat, sőt egy Kínába utazó arab kereskedő, Abu Zayd Hasan szemtanúja volt annak, hogy kínai kereskedők a kölcsön-megállapodásokat ujjlenyomatokkal hitelesítették [88].

Minden bizonnyal az ókoriaknak nem voltak tudományos igényű információi az ujjlenyomatok egyediségéről, mégis Hammurabbi (i.e. 1792-1750) babiloni király idejéből ismert tény, miszerint a letartóztatott személyektől ujjlenyomatot vettek [5]. A kínai Qin dinasztia [i.e. 221-206] idejében a bűnügyi helyszínekről kéz, láb és ujjlenyomatokat vettek, i.sz. 650-ben pedig Kia Kung-Yen kínai történész javasolta az ujjlenyomatok használatát személyazonosítás céljára.

Európában az angol orvos-botanikus Nehemiah Grew (1641-1712) közölte az első cikket, ami a kéz és tenyér redőit írta le [52]. Nem sokkal később már különböző szerzők anatómiai műveiben tárgyalták a redők meglétét (például Gobard Bidloo holland és Marcello Malpighi itáliai orvosok). 1788-ban - kb. egy évszázad elmúltával - a német anatómus Johann Christoph Andreas Mayer (1747-1801) már azt vélte felfedezni, hogy az ujjlenyomat minden személy esetében más és más.

Az 1800-as években több európai tudós is tett fontos észrevételeket az ujjlenyomatokkal kapcsolatban, mint például a cseh Jan Evangelista Purkyně, a német Georg von Meissner, az angol Sir William James Herschel vagy a francia Paul-Jean Coulier.

1880-ban Dr. Henry Faulds, skót sebész a Nature-ben publikálta eredményeit, illetve javaslatot tett tintával való adatrögzítésre és azonosításra. Ötletét a londoni Metropolitan Police elvetette, így Charles Darwinhoz fordult ötletével. Darwin unokatestvéréhez, Galtonhoz továbbította az információkat, ő maga már túl öreg és beteg volt, hogy a témával foglalkozzon.

Galton 1892-ben "Finger Prints" címmel jelentette meg írását, ami az első témával foglalkozó könyv volt [47]. Galton dolgozta ki az első osztályozási módszert: azt állította, hogy két ujjlenyomat nem lehet azonos ill. a valószínűségét két ujjlenyomat egyezésének 1:65 000 000 000-hoz becsülte. (Itt jegyezzük meg, hogy Galton tudományos munkássága igen sok és változatos területre terjedt ki a földrajztól kezdve a meteorológiáig, lásd <http://galton.org/>.)

Galton művének hatására Sir Edward Henry - Indiában dolgozó főfelügyelő - figyelme az ujjlenyomatok alkalmazásának irányába fordult. Galton rendszerét munkatársaival (Azizul Haque és Hem Chanda Bose) továbbfejlesztette az 1896 és 1925 közötti időszakban. 1899-ben már világszerte elfogadták a módszerüket, mivel 1897-ben a bevezetőben említett Bertillon-féle azonosítási módszerrel (Anthropometry) való összehasonlításból egyértelműen győztesen került ki.

A Henry-féle módszer a 10 ujjlenyomat mintázatát előre meghatározott osztályokba sorolja, és így a további feldolgozás, az apró sajátos mintázatok (mint redő végződések és elágazások - azaz a minuciák) azonosítása jelentősen felgyorsulhat. A módszer az osztályozás során felhasználja az ujjak sorszámát, illetve a globális mintázatot (örvény, ív, hurok). Valójában a Henry-féle módszer nagyon sokáig több helyen használatban volt, sőt, a mai modern rendszereknek is az alapját adja.

### 4.1.2. Az ujjlenyomat kialakulása

A bőrünk az egyik legnagyobb kiterjedésű szervünk, amit különböző típusú, de szorosan együttműködő szövetek alkotnak, több millió szenzorral és kiterjedt érhálózattal. A bőr rugalmas, folyamatosan cserélődő védelmező fedőrétege a testnek, amely alapvetően sima, kivéve az ujjakat, tenyereket és talpakat. Az ezeken a felületeken megfigyelhető redők (bőrlérendszer vagy bőrfodorszál struktúra) feladata a csúszásgátlás, a biztos fogás, tapadás biztosítása.

A bőrlérendszer megtalálható bizonyos alsóbbrendű emlősöknél (pl. mókus, sün) és főemlősöknél is (lásd a csimpánz kezét vagy a selyemmajom farkát), anatómiai magyarázata a bőr rétegeinek egymáshoz kapcsolódása. Maga a jól látható mintázat a bőr felső rétegén, az ún. felhámon (epidermisz) található, amelyet csapszerű kinövések (dermális papillák) kötnek az alatta levő irharéteghez (dermisz) (lásd 4.2. ábra). A csapszerű kinövések felszíni leképeződései a bőr redői, kiemelkedései, a bőrfodorszálok.



4.2. ábra. Felhám és irharéteg összetett sávja ill. két réteg kapcsolódását biztosító dermális papillák. (A kép eredeti forrása Deborah S. Dempsey weboldala, Department of Biological Sciences, Northern Kentucky University, a Creative Commons Attribution-Share Alike 3.0 Unported license.)

Embriológiai kutatások során kimutatták, hogy a hámrétegen lévő redők kifejlődését ún. voláris párnák kialakulása előzi meg, ezek növekedése 6,5-10,5 magzati hét között a legintenzívebb. Harold Cummins már 1929-es tudományos cikkében [25] leírta a bőrlérendszer kifejlődésének fontos lépéseit, különös tekintettel ezekre a padocskákra. Eleinte ezek alakja nagyjából hasonló, lekerékített, majd a magzat 9. hetétől a méretük és alakjuk elkezd megváltozni. Ezeknek a párnáknak a kialakulását befolyásolhatják külső fizikai tényezők,

genetikai okok, ill. akár mindkettő is. Mindenesetre ezek alakja, mérete és elhelyezkedése befolyással van a bőrlécrendszer kinézetére. Testvéreknél, iker-testvéreknél a globális mintázat nagymértékben hasonló, de az apró részletek (minuciák) eltérnek.

A 10-11. hét során még az epidermisz egy alapvetően sima, vékony réteg mind a felszínen, mind a mélyebb dermális találkozásnál. Ekkor azonban már az epidermisz mélyebb, jól lokalizálható pontjaiban egyes sejtburjánzásoknál megjelennek az első redőmintázatok, miközben a voláris párnák visszafejlődnek (valójában nincs szó zsugorodásról, a többi rész növekedése előzi meg a párnák fejlődését). A redők kialakulására több elmélet is létezik, az epidermális és dermális rétegek találkozása, illetve idegi befolyások is szóba kerülnek [39]. Míg a végleges dermális papillák kialakulása csak a 24. héttől kezdődik, ekkorra már az epidermális redők morfológiája megfelel a felnőttkorinak.

A kialakult bőrlécrendszer ezek után méretében még igen, struktúrájában azonban már nem változik. Egyedül a különböző sérülések (vágások, sebek, hiányosságok), szennyeződések, ill. a bőr extrém kiszáradása okozhat problémát a biometria azonosításban.

#### 4.1.3. Struktúrája

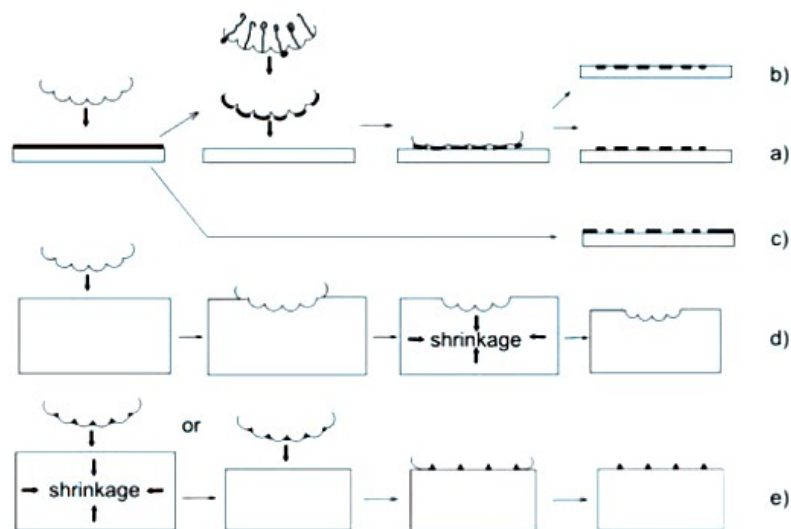
Az ujjlenyomat mintázatát völgyek és hegyek egymás mellett futó vonulatai adják. A feldolgozásra kerülő ujjlenyomatok valójában a redőmintázat két-dimenziós képei, amelyek a kéz lenyomásával a 3D-s felületi mintából készülnek, így kicsit a felvétel során torzulnak. A mintavétel lehetséges módjait a 4.3. ábra szemlélteti.

Ha a vonalakat egy relatív nagyobb felületen szemléljük, akkor különböző globális mintázatokat vélhetünk felfedezni. A három irányból összefutó élek ún. **triráduszt** alkotnak. Ezeknek több típusát lehet felismerni, attól függően, hogy mi van a találkozási pontban (lásd 4.4. ábra).

A jellemző minták területe jól körülhatárolható a nagyjából párhuzamosan induló **típusvonalak** által körülzártan. A mintázat közepe a **mag**. A **delta** az az elágazási pont, amit az élek számlálásánál referencia pontként használnak.

A három legalapvetőbb globális, az ujjbegyen megfigyelhető mintázat az **ív**, a **hurok** és az **örvény** (lásd 4.6. ábra). Az ívek között megkülönböztethetjük az egyszerű és a sátras/tornyos ívet. Előbbinek nincs trirádusza. A hurokmintázatok egy trirádussal rendelkeznek, két fajtájuk van: az ulnaris és a radiális hurkok. Az ulnaris esetben a kisujj felől indulnak a redők és oda is térnek vissza, míg radiális esetben a hüvelykujj felől indulnak és oda is érkeznek. Az örvények alapvető fajtái pedig a spirális, a koncentrikus örvények, ill. különböző összetett mintázatokban is gyakran szerepelnek, hurkokkal és ívekkel kombinálva.

Bár a globális mintázatok alkalmasak az ujjlenyomatok osztályozására, azonban pontos egyezést nem lehet általuk végezni, de az utóbbit jelentősen felgyorsíthatják előzetes szűréssel. A pontos egyezéshez apróbb részletek megfigyelésére van szükség. Ezeket az apróbb jellemzőket **minuciáknak** nevezzük, a két legfontosabb minucia a **végződés** és az **elágazás**. Többféle minuciát mutat a 4.7. ábra.



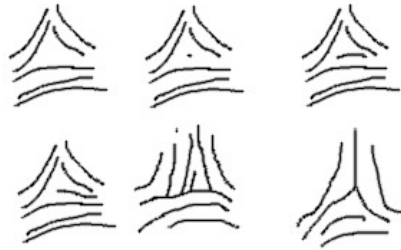
4.3. ábra. Az ujjlenyomat kialakulása különböző anyagokon: a) az ujjon lévő festékanyag megtapad egy tárgyon; b) a kézen lévő festék beleszívódik egy papírlapba; c) a megérintett felületről az ujj eltávolít festékanyagot; d) puha anyagban keletkezik lenyomat; e) az ujj redőiben lévő anyag megtapad egy felületen. (A kép forrása [68].)

Ezeknek a lokális mintázatoknak kucsfontosságú a helye a személyek megkülönböztetésében, de már az ujjlenyomat irányultságának meghatározásához is használhatóak. Megfelelő minőségű felvételek esetén a bőr pórusai is jól kivehetők. A hegyeken elhelyezkedő pórusok nyitottak vagy zártak lehetnek (lásd 4.7. ábra), ezek is lokalizálható jellemzői az ujjlenyomatoknak.

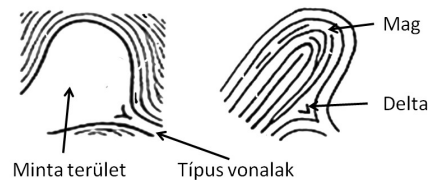
#### 4.1.4. A jelfeldolgozás lépései

A feldolgozandó kép dinamika tartománya általában 8 bit, azaz 256 szürkeségi árnyalat megfelelő a mintázatok elemzéséhez. A kép felbontása nagyban függ a szkennelő készüléktől (a lehetséges szkennelési módszerekkel a következő fejezetben foglalkozunk). Az alkalmazott feldolgozási módszertől függően minimum 250 képpont szükséges inchenként (250 dpi, azaz 100 pont centiméterenként), a 625 dpi (250 pont per centiméter) általában az elfogadott mintavételi sűrűség. A szükséges feldolgozandó ujjterület kb. 2,5 cm élhosszúságú négyzet, így utóbbi esetben egy kb. 600x600 pixel felbontású kép feldolgozásával számolhatunk. A feldolgozás során a következő lépéseket kell megtenni: *előfeldolgozás, tulajdonságkinyerés, egyezés vizsgálat*.

**Előfeldolgozás:** Az előfeldolgozás során a célunk a kép lényegi részeinek ki-



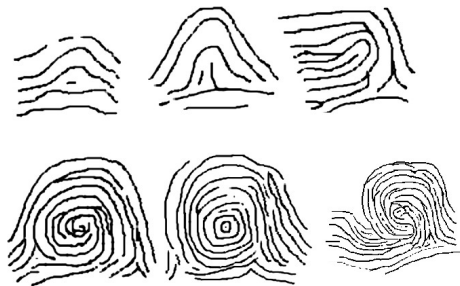
4.4. ábra. A trirádusok tipikus fajtái



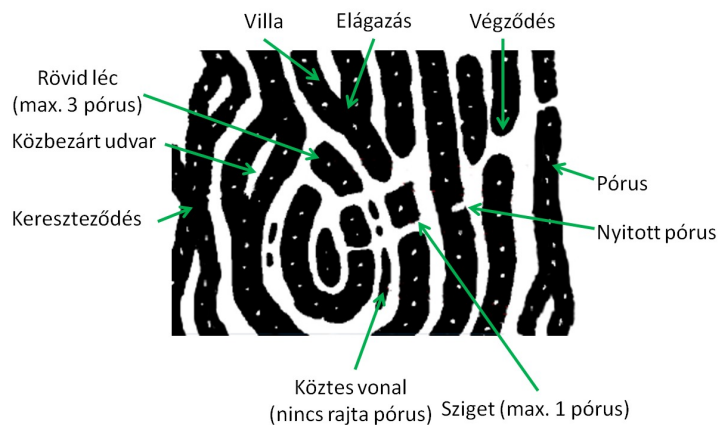
4.5. ábra. A típusvonalak által körülhatárolt mintaterület és az utóbbin lévő redőzet számlálásához használt mag és delta pontok.

jelölése és a képi minőség feljavítása. Az előbbit szegmentálásnak nevezzük, az ún. ROI (Region Of Interest) kijelölése a feladata, azaz azon képterületé, amivel a feldolgozás további lépéseiben foglalkozni kell. A bőr redőin a legapróbb részleteket kell megtalálni, azonban az "ideális" mintázatok képét torzíthatják szennyeződések, a nedves, gyűrődött vagy éppen kiszáradt bőr. Ezen hatások miatt szükség lehet a kép minőségének javítására, aminek célja három probléma kezelése: szakadt vonalak összekötése, a szennyeződések által összekötött vonalak szétválasztása és a kontraszt javítása. Az első kétfajta hiba kezelésére alapvetően kétféle megközelítést szoktak használni: pixel-térbeli adaptív szűrőket vagy frekvencia-térbeli szűrőt. Az előbbi többnyire lokális minták vizsgálatát jelenti, alapvetően az élek párhuzamos futásának kihasználásával. A kontraszt javítása adaptív hisztogram-transzformációkkal lehetséges.

**Tulajdonságkinyerés:** A tulajdonságkinyerés vonatkozhat a globális jellemzőkre, illetve a lokális jellemzők detekciójára. A globális mintázatok detekcióját a redőzet irányultságának lokális eloszlása árulja el. Ehhez éldetektációt kell végezni, majd pedig az élek irányát kell meghatározni. Az élek területi eloszlása alapján be lehet sorolni a képet a megfelelő globális kategóriába. A lokális jellemzők detekcióját ill. magukat a leírásukat úgy tudjuk elvégezni, ha az ujjlenyomatok képét azonos irányba hozzuk. Ehhez fel lehet használni a globális jellemzés során mért irányultságokat. Néhány nem túl gyakran előfor-



4.6. ábra. Az ujjlenyomat jellemző globális mintái: Első sor: egyszerű ív, sátras ív, hurok. Második sor: spirál, koncentrikus örvény és egy összetett alakzat



4.7. ábra. Az ujjlenyomat minuciái

duló jellemzőt, mint a magokat és deltákat is fel lehet használni ebből a célból. A minuciák detekcióját bináris, vékonyított képeken végzik el. A binarizálást adaptív küszöböléssel érdemes elvégezni, míg a vékonyításra morfológiai vékonyítást lehet használni [85]. A vékonyítás hatására a képen lévő bináris objektumok 1 pixel vastag vonalakká, ill. pontokká zsugorodnak, de topológiai értelemben nem történik változás: hurok, objektumok nem törlődnek, a vonalak nem rövidülnek, nem szakadnak szét.

**Egyezés vizsgálata:** A minuciák típusának és pozíciójának meghatározása után az aktuális lekérdezés adatainak és a jelöltek leíróinak összevetését kell elvégezni. Mivel a különböző szennyezések és az ujj alakjának lenyomáskor szenvedett torzulása miatt nem várhatunk pontos egyezést, olyan módszert kell alkalmazni, amely egy bizonyos fokig tolerálja ezeket a bizonytalanságokat. A minuciák összehasonlítása során a jellemzőket a szomszédságukkal együtt kell

megvizsgálni. Egy-egy pontot (minuciát) jellemez a típusa, pozíciója, irányultsága, illetve néhány szomszédjának az iránya, távolsága. Nem várunk feltétlenül pontos egyezést a korábban említett lehetséges problémák miatt, tehát ha egy minucia kellően hasonló jellemzőkkel bír, akkor egyezést állapítunk meg.

Előfordul, hogy az ujjlenyomatokat egyszerű korrelációs módszernek vetik alá, ami elvégezhető a pixel és a frekvencia térben is. Az ujjlenyomat nemlineáris torzulásai, az előforduló szennyeződések, ill. az apró minuciákban való különbségek egy korrelációs módszerrel nehezen kezelhetők. Egy gyors korrelációs számítás azonban egy durva szűréssel felgyorsíthatja a keresést, ami különösen akkor lehet hasznos, ha több tízezer, esetleg milliós nagyságrendű összevetésről van szó.

Az ujjlenyomatok jellemzéséhez az eddig említett globális mintázatokon és a lokális minták, minuciák elhelyezkedésén kívül használhatunk egyéb szám- szerű jellemzőket is. Ilyen viszonylag robusztusan meghatározható ujjlenyomat jellemzők pl.:

- mag és trirádusz közti egyenes által metszett bőrlécek száma,
- bőrlécek száma adott területen belül,
- bizonyos hosszúságot elérő bőrlécek száma adott területen belül.

#### 4.1.5. Eszközök

A tinta alapú ujjlenyomat elkészítéséhez ("off-line" módszer) fehér papírlapot, erre a célra kapható tintát, tinta hengert, ill. tintázó lemezt használnak. Az ujjra közvetlenül a hengerrel, vagy a lemez által hordják fel a festéket. Ebben az esetben a számítógépes azonosításhoz a képek digitalizálása szükséges. A lenyomatokat általában nem üres lapra, hanem erre a célra rendszeresített nyomtatványra készítik. A nyomtatványokat ahhoz, hogy hatékonyan lehessen keresni köztük, célszerű digitalizálni, és elektronikus rendszerben kereshetővé tenni. Természetesen az ujj mintázatának közvetlen elektronikus beolvasása ("on-line" vagy "live-scan" módszer) a leghatékonyabb, amire többféle céleszközt fejlesztettek ki.

A szenzorok kialakítása alapvetően kétféle lehet: a teljes felületen leképező (érintős) vagy az ujj végighúzásán alapuló változatok léteznek. Az érintős módszer hátrányai:

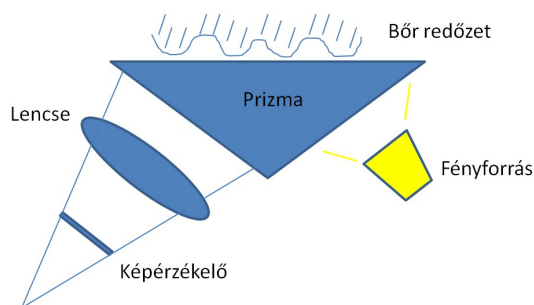
- a szenzor könnyen összekoszolódhat,
- a korábbi használatból látható ujjlenyomatok maradhatnak rajta,
- az ujjlenyomat elfordulását az algoritmusnak kompenzálnia kell,
- a szenzor mérete jelentős hatással van az előállítási költségekre.

A végighúzó szenzor esetén a fentiekkel szemben:

- a szenzor nehezebben koszolódik,
- nincsenek maradvány ujjnyomok,
- az ujj kisebb valószínűséggel fordul el,
- a hőmérséklet a mozgás közben ingadozhat.

### Optikai beolvasó

Az egyik legkorábban alkalmazott és legjobban elterjedt módszert Optical Frustrated Total Internal Reflection (OFTIR)-nek nevezik. Az ujjat egy üvegprizmára kell helyezni, amit lézerrel világítanak meg (lásd 4.8. ábra). Az ujjról visszavert fényt CCD (Charge Coupled Device) vagy CMOS (Complementary Metal Oxide Semiconductor) képérzékelővel rögzítik (ilyen érzékelők vannak a hagyományos digitális kamerákban is). A módszer alapvető hátránya, hogy a prizma és a képérzékelő között egy bizonyos távolságnak meg kell lennie, ezért a miniatürizálásnak korlátai vannak.



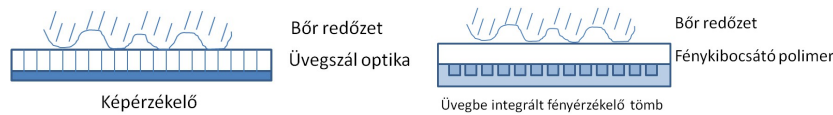
4.8. ábra. Optikai elvű ujjlenyomat szkennel felépítése (Optical Frustrated Total Internal Reflection - OFTIR)

Az OFTIR elven kívül léteznek más optikai megoldások is, pl. a [35] által bemutatott módszer, ahol üvegszálak által történik az ujj megvilágítása és a visszavert fény elvezetése is a szenzorokig (4.9 ábra, bal oldal). Így ez a hagyományos OFTIR rendszernél jóval helytakarékosabb. Másik kisméretű megoldás, amikor egy rugalmas anyag hátoldalára helyeznek el mikroprizmákat, amik a fény visszaverésével, eltérítésével vesznek részt a képalkotásban [20] (4.9 ábra jobb oldal).

### Piezoelektromos beolvasó

Ebben az esetben egy mátrix szerkezetű nyomásérzékelőről van szó, amely nyomás hatására áramot hoz létre (lásd piezoelektromos effektus). A nyomás ereje





4.9. ábra. Bal oldal: Optikai szál optika ujjlenyomat szkennel. Jobb oldal: Elektro-optikai ujjlenyomat érzékelő.

meghatározza az áram nagyságát, így a redőt alkotó kitüremkedések és mélyedések megfelelő képet alkotnak a mátrix áram leképezése után. (Tipikusan az ilyen szenzorok alacsony érzékenysége miatt az általuk generált kép minősége általában elmarad az OFTIR szenzorokétól.)

### Ultrahang beolvasó

Az ultrahang eszközökben az ujj irányába kibocsátott, majd az onnan visszaverődött hanghullámok segítségével mérünk távolságot, ami tükrözni fogja a bőrléc-struktúrát. A módszer érzékeny az ujj szennyeződéseire, ill. az alkalmazott technológia viszonylag relatív költséges ahhoz, hogy tömegesen elterjedjen.

### Kapacitív beolvasó

A kapacitív érzékelők meglehetősen elterjedtek, mert kisméretűek és olcsó az előállításuk. Ennek köszönhetően a beágyazott rendszerek (lásd laptop ujjlenyomat érzékelők) kedvelt beviteli módját jelentik. Az érzékelő egy vagy több félvezető chipből áll, apró cellákat tartalmazva. Minden cellán egy szigetelő réteggel ellátott kondenzátor lemez található. Amikor az ujjat a szenzorra helyezzük, az ujj mintázata adja a kondenzátor másik felét. A bőrfelület távolsága - amit a bőr mintázata határoz meg - fogja befolyásolni a kialakuló feszültséget, amelyet az eszköz a kiolvasás során digitális jellé alakít (lásd 4.10. ábra).



4.10. ábra. Kapacitív ujjlenyomat szkennel: a bőrfelület és a kondenzátor lemezek távolsága kódolja a bőrredőzet mintázatát.

### Hőszkenner

Ezekben az eszközökben ún. piro-elektromos anyagok generálnak áramot a hőmérséklet különbségeknek megfelelően. A szenzor felületéhez hozzáérő bőrredők a távolabb fekvő mélyedésekhez képest más hőmérsékletet hoznak létre, ennek

megfelelően áll elő az ujjlenyomatot ábrázoló kép.



4.11. ábra. A három oszlopban három különböző ujjlenyomatról származó kép látható. Első sor: kapacitív, második sor optikai, harmadik sor hőszensor által alkotott kép. (kép forrása: [3])

#### 4.1.6. Erősségek-gyengeségek

Mint röviden bemutattuk, az ujjlenyomat használatának jelentős történelmi hagyományai vannak, számtalan, több száz algoritmusról beszélhetünk, ill. azok összehasonlítása is sokféle szempont szerint történhet. A különböző módszerek összevetésére ún. ujjlenyomat összehasonlító versenyeket (FVC - Fingerprint Verification Competition) rendeztek több alkalommal is (2000-ben, 2002-ben, 2004-ben és 2006-ban). A 2006-os FVC szervezését négy egyetem laboratóriu-

mai végezte (University of Bologna, Michigan State University, San Jose State University, Universidad Autonoma de Madrid). A verseny legfontosabb céljait a következő pontokban lehet összefoglalni:

- ujjlenyomat ellenőrzés, összehasonlítás,
- kézlenyomat ellenőrzés,
- ujjlenyomat indexelés, az orientáció becslése,
- biztonságos ujjlenyomat ellenőrző módszerek tesztelése.

Külön eljárásban vizsgálták a kis erőforrás igényű, ún. könnyű (lightweight) megoldásokat. A versenyen - ahol 53 résztvevő csapat 70 algoritmusát szerepelt - négy új adatbázist hoztak létre. Jelenleg az ún FVC-onGoing (on-line evaluation of fingerprint recognition algorithms) projekt keretében szerveznek összehasonlító versenyeket, ahol a könyv készítésének idejében már 2439 algoritmus értékelése történt meg.

Más biometriaival összehasonlítva az ujjlenyomat alapú megközelítés előnyei:

- Nagy pontosság, precizitás (jó minőségű képek esetén akár 100% pontossággal működik).
- Könnyű használni a beviteli eszközöket.
- A kis méretnek köszönhetően sok helyre beépíthető.
- Könnyen helyettesíthető másik ujjal (pl. sérülés esetén).

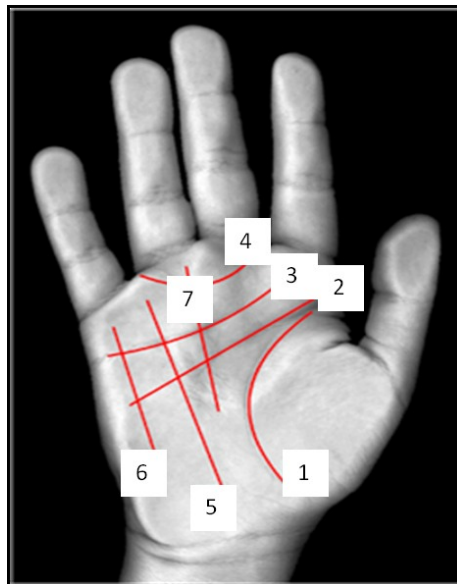
A módszer használatának korlátai:

- A populáció mérhető része (kb. 2%) esetében nem használható az ujjlenyomat gyenge minősége miatt (pl. bizonyos fizikai munkavégzés során sérül a bőrfelület).
- Időben változhat a mintázat (főleg sérülés miatt), ezért időszakonként a minták frissítése szükséges.
- Társadalmi elfogadottsága mérsékelt, mivel használata elsősorban a bűnüldözéshez kapcsolódik.
- Speciális eszközt igényel, amelyek elterjedtsége kisebb, mint a mikrofonoké vagy kameráké.

## 4.2. Tenyér redőinek felhasználása

A kézolvasás, tenyérjósítás (kirológia, kiromantia) ősidők óta misztikus tudomány, ami a vizsgált illető jellemét, érzelmeit, jövőbeli sorsát állítja felismerni. A tenyérnyomatok tenyérjósításban, ill. egészséggel kapcsolatos diagnózisban

való kínai felhasználásáról már i.e. 1000-ból vannak információink [115]. A 19. században még német egyetemeken tanították a tenyérjósást, azonban a mai ismereteink szerint nincs tudományos igényű bizonyíték a kézolvásban alkalmazott módszerek igazolására. A tenyérjósás szerint a tenyéren lévő vonalak és dombok különböző jelentéssel bírnak erősségük, hosszuk, metszéspontjaik szerint. A 4.12. ábra a tenyér fővonalait mutatja, mint 1. Életvonal, 2. Fejvonal, 3. Szívvonal, 4. Vénusz öve, 5. Nap-vonal, 6. Merkúr-vonal, 7. Sorsvonal.



4.12. ábra. A tenyér fővonalai: 1. Életvonal, 2. Fejvonal, 3. Szívvonal, 4. Vénusz öve, 5. Nap-vonal, 6. Merkúr-vonal, 7. Sorsvonal.

A tenyér redőinek változatossága és egyedisége természetesen lehetővé teszi a biometria felhasználást, azonban sokkal kevesebb helyen alkalmazzák, mint az ujjlenyomatokat. Ennek feltehetően legfőbb oka az, hogy az ujjlenyomatokat sokkal kézenfekvőbb rögzíteni, mint a tenyér (vagy akár a láb) képét. Az első tenyérnyomatot használó azonosító rendszert a KFKI-ban (Központi Fizikai Kutató Intézet) kezdték el fejleszteni 1990-ben. Az ún. RECOderm rendszert a Magyar Rendőrség 1992-től már alkalmazta, majd egy éves gyakorlati tapasztalatok alapján annak országos bevezetéséről döntöttek. A rendszerben alkalmazott ujj- és tenyérnyomat azonosító technológiát - a szabadalmával együtt - 1997-ben a Lockheed Martin Information Systems vásárolta fel.

Napjainkban jóval kevesebb tenyérnyomatot tárolnak a bűnüldöző szervezetek, mint ujjlenyomatot, bár a két technika felhasználásnak aránya a jövőben valószínűleg valamelyest változni fog: az FBI Újgenerációs Azonosítás nevű rend-

szerének (Next Generation Identification [82]) egyik fontos célkitűzése a tenyér-nyomatok tárolása és visszakeresése.

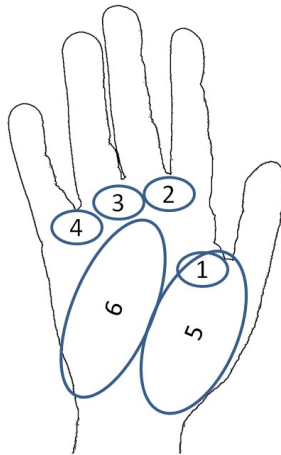
A tenyérnyomat rögzítése kissé nehezebb feladat, mint az ujjlenyomaté: egyrészt a tenyér nagyobb felület, és így nagyobb eszközt igényel, másrészt nehezebben érhető el, hogy a nagyobb felületről sík állapotában kapjunk szkennelt képet. Az azonosítás alapjait adhatják a bőr jelentősebb redői, ill. minuciák is. Azonban míg egy ujj esetén nem több mint kb. 80 minuciáról beszélhetünk, addig egy tenyér esetén több száz, akár 800 minucia is lehet. A vastagabb hajlatok kialakulása az embrionális fejlődés során megelőzi a finom (tapadást segítő) redők kialakulását; mindkét mintázat egyedinek és állandónak tekinthető. A három legjelentősebb hajlat jól látszik a tenyéren, és megfelel az előző ábrán szereplő 1-es, 2-es és 3-mas fővonalaknak ("radial", "proximal" és "distal"). Míg ezek a vonalak akár 100 dpi mellett is jól megfigyelhetők, a vékony redőkhöz kb. 500 dpi mintasűrűség szükséges, a pórusok pedig jóval ezen felbontás fölött digitalizálhatók. A minuciáknak a nagyobb száma miatt normál (nem bűnügyi) felhasználás során nem szükséges a teljes tenyér képének feldolgozása, tárolása. Nyilvánvaló, hogy ha szennyezett a minta, akkor a több sajátosságos pont jelentősen javítja a helyes felismerés valószínűségét.

A tenyér fontosabb régióit mutatja a következő 4.13. ábra: négy ún. interdigitális (1-4), egy thenar (5) és egy hypothenar régióról (6) beszélhetünk, utóbbi kettő között az ún. axiális trirádus helyezkedik el. A hypothenaron megtalálható a minták mindegyik fő típusa, sőt helyenként ezek bonyolultan kombinálódnak. Leggyakoribb minta az ív és a legritkább az örvény. Az ívek és a hurkok gyakorisága nemenként eltérő. A thenaron leggyakrabban előforduló minták a hurkok, örvények, a minta nélküli területek és ezek kombinációi. Ezen a területen a férfiaknál gyakrabban fordulnak elő rajzolatok, mint a nőknél.

A kézen található minuciák feldolgozása gyakorlatilag megfelel az ujj mintázatainak feldolgozásához, természetesen a fővonalat fel lehet használni az orientáció megállapításához. Mivel a kéz kiterjedése jóval nagyobb az ujjnál, ezért az optikai eszközök alapvetően alkalmasak akár a kéz és az ujj együttes beolvasására. A következő ábrán (4.14. ábra) a Crossmatch cég 1000dpi-s kéz- és ujjlenyomat olvasóját láthatjuk.

### 4.3. Láb bőrredőinek felhasználása

Az ujj, tenyér vagy kéz biometriához képest a láb képén alapuló kereskedelmi rendszerek használata egyáltalán nem elterjedt. Ennek az oka magyarázható a testrészek nehezebb hozzáférhetőségével, illetve higiéniai és kulturális okokkal is. A bűnüldözésben azonban kiválóan alkalmazható biometriai jellemzőről van szó. Természetesen előfordulhatnak olyan területek (csecsemő gondozás, fürdők, egészségügyi szolgáltatások), ahol a hétköznapi gyakorlatban is kiváló eszköznek bizonyulhat a láb bőrredőinek biometriai felhasználása. Példának okáért mivel a csecsemők ösztönösen összezárnak tenyerüket, ezért esetükben egyszerűbb láb-



4.13. ábra. A tenyér interdigitális (1-4) és thenar (5) és hypothenar régiói (6)

mintát rögzíteni, mint a kéz alakját vagy redőzetét használni.

Az egyik első tanulmány, ami a lábnyomatok bűnügyi felhasználásáról szól Kennedytől jelent meg 1996-ban [66]. Ő még tintával készült lenyomatokat vizsgált, és a láb lenyomatának alapvető geometriai adatait használta fel. [81] már automatikus felismerő rendszert mutatott be 2000-ben, amiben egy nyomás érzékeny matracot alkalmaztak. Az általa elért 85%-os pontosság messze elmaradt a kéz, ill. ujj alapú módszerektől. [64] és [65] már jobb - szintén nyomásérzékelős matracral elért - eredményekről számolt be néhány évvel később. Azonban a 98% körüli felismerési pontosság is aránylag kicsi populációra vonatkozik (kevesebb, mint egy tucat személyre vonatkoznak a közölt adatok). Fontos megjegyezni, hogy ezek a fenti módszerek - ellentétben az ujj vagy tenyér alapú megközelítésekkel - nem vizsgálták a talp finom mintázatát, hanem annak alapvető geometriáját, ill. nyomástérképét használták fel.

A láb alapú módszereket alapvetően két nagyobb csoportba lehet sorolni: statikus és dinamikus. Az előbbi esetében a mintát a vizsgált személy álló pozíciójában, stabil testtartás mellett rögzítik, míg a második esetben sétálás közben veszik fel az egyénre jellemző vonásokat. Utóbbi tehát nem igényel jelentős odafigyelést a felhasználóktól. Valójában a járást feltételező módszerek nem szigorúan, ill. nem minden esetben a lábnyomat alapú biometriai módszerek halmazába, hanem pl. a járás alapú módszerekhez sorolhatóak be. Az adatfeldolgozás folyamata nem tér el a többi biometriai rendszer általános modelljétől, ezért lényegileg két sajátos területre, az adatok rögzítésére és a vizsgált tulajdonságokra térünk csak ki:



4.14. ábra. A Crossmatch cég 1000dpi-s olvasója, mely ujj és tenyérnyomatok készítésére is alkalmas (<http://www.crossmatch.com>)

1. **Adatok rögzítése:** A lábról származó információk származhatnak nyomásérzékeny matracokról vagy valamilyen optikai eszközből. Az előbbi kisebb felbontással rendelkezik, így a talp egyfajta nyomástérképét tudják előállítani. Ilyen megközelítést választott [66] is. A szakirodalom többféle matracról is beszámol, mint pl. a Nitta Big Mat [81] vagy az ún. TechStorm Foot Analyzer [65]. Amennyiben ennél részletesebb adatokat szeretnénk kapni a bőr redőzetéről, akkor alapvetően optikai eszköz használata célszerű, amely hasonló a tenyérhez vagy ujjakhoz használt beviteli eszközökhöz. Természetesen a megfelelő teherbírásról gondoskodni kell.
2. **Adatok előfeldolgozása:** Az előfeldolgozás célja a kép minőségének javítása, a pozíció és irány meghatározása, kompenzálása, azért, hogy a további adatfeldolgozás ezektől független lehessen.
3. **Tulajdonságok kinyerése a normalizált képből:** Most bemutatunk néhány ilyen jellemző, viszonylag könnyen kinyerhető tulajdonságot:  
*Nyomástérkép középpontja* (Center of Foot Pressure - COP): Kiszámítható a mért nyomásértékek értékéből és eloszlásából. A mozgás során a COP pozíciója változik és az egyénekre jellemző elmozdulást mutat. Valójában még álló pozícióban is kismértékű mozgás jellemzi. Idős korban a pozíciója nagyobb mértékben változhat.  
*Nyomástérkép:* Statikus esetben a nyomástérkép is jól jellemzi a személyt, azonban a testsúly áthelyezése miatt az értékei viszonylag nagy eltérést mutathatnak. Ezért több egymás utáni mérés szükséges, és minden pozícióban a maximális vagy átlag érték már jól jellemezhet egy-egy pozíciót.

A nyomástérkép értelmezhető egy szürkeskálás képként, amivel akár korrelációs összehasonlítást is végezhetünk.

*Geometriai jellemzők:* A kéz geometriai vizsgálatához hasonlóan a kép geometriai formája is viszonylag könnyen mérhető. Így a láb, a lábujjak hossza, a sziluett íve, az ujjak hossza és alakja, az ujjak közti szögek, és a láb különböző helyein mért szélessége a célja ezeknek a méréseknek.

*A láb texturális jellemzői:* Szintén a kéz mintázatának feldolgozásához hasonlóan járhatunk el a redőzet lokális és globális mintázatának meghatározásában.

4. **Minta összehasonlítás:** Az alkalmazott metrika kimenete egy hasonlósági mérték lesz.
5. **Döntés:** A felismerésről, azonosításról a szükséges döntést a hasonlósági érték alapján küszöböléssel lehet megtenni.



## 5. fejezet

# A kéz alakja

### 5.1. Történeti háttér

Bár Bertillon - mint ahogy korábban bemutattuk - nagyrészt sikeresen alkalmazta az emberi test alakjának mérését biometria céljára, azonban érdekes módon magának a kéz alakjának a mérését nem használta. Valójában az emberi kéz igen sokrétűen, többféle módon is alkalmas az azonosításra:

- az ujjak mintázatának lenyomata,
- a tenyér mintázatának lenyomata,
- az ujjak vagy a kezek geometriája,
- a vénák által alkotott mintázat.

A kéz geometriáját használó első szabadalom 1971-ben jelent meg: Miller találmánya kimondottan a kéz ujjainak alakját használja fel személyazonosításra [78]. Az eszköz mechanikus működésű volt, de később hamar egyértelmű lett az optikai eszközök előnye, amelyek több szabadalomban és eszközben is megjelentek [59],[101].

A kéz alakján alapuló módszerek felhasználása eleinte különböző állami és nagy biztonságot igénylő nukleáris intézményekben merült fel, de hamar igen népszerűvé vált egyéb, kereskedelmi felhasználási területeken is. Mivel a potenciális felhasználók nem tekintik annyira egyedinek (és egyben bűnözéshez kapcsolódónak), mint az ujjlenyomatot, ill. kevésbé tartanak esetleges káros egészségügyi mellékhatásoktól (mint pl. a retina leolvasást végző berendezések esetén), ezért a kéz alapú biometria viszonylag elfogadott és népszerű módszernek számít.

A technika egyik korai nagyléptékű felhasználása az 1996-os Atlantában megrendezett Olimpiai Játékokhoz kötődik, ahol az olimpiai faluba való belépési jogosultság ellenőrzésére használták. A sikeres alkalmazás méretére jellemző

volt, hogy kb. 65000 felhasználót kellett a rendszernek kezelnie, és 28 nap alatt több mint egymillió azonosítás történt.

## 5.2. A kéz geometriája és mérése

Az embereknek születésükkor a két kezük alakja általában csaknem teljesen egyforma. Később a kéz formájában lassú változás kezdődik, ami különösen a serdülőkorra jellemző. Az alakváltozás legfőbb oka, hogy az egyik kezünket gyakrabban használjuk, mint a másikat, így a különböző szövetek vastagsága eltérő lesz, illetve előfordulnak kezenként eltérő sérülések is. Másik jelentős változást indukáló korszak az öregedéskor figyelhető meg.

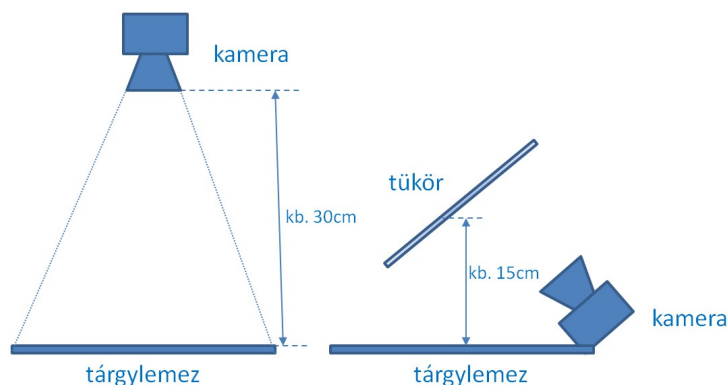
A kézgeometria biometriai jellemzőit a következőképpen foglalhatjuk össze:

- A kéz formája egyénekre jellemző, egyedi mintázatot mutat, de nem zárható ki jelentős hasonlóság két különböző személy keze esetén.
- A kéz geometriája kevés paraméterrel jól jellemezhető.
- A kéz biometriai használata viszonylag kényelmes, nem kötődik általános ellenérzéshez, a felhasználók nem idegenkednek tőle (pl. lehetséges egészségkárosodástól való félelmekre hivatkozva), ellenérzést egyedül az eszközök lehetséges szennyezettsége jelenthet.

A kéz alakjának jellemzéséhez elegendő arról bináris fényképet készíteni. Ehhez használhatók hagyományos, vagy infra megvilágító fényforrások (a korszerű eszközökben LED-eket alkalmaznak), a képeket CCD vagy CMOS optikai szenzorok rögzítik. A bináris kép kb. 25x25 cm-es területről készül kb. 200x200 pixeles minimális felbontáson, azaz kb. milliméteres fizikai felbontás elegendő a biometriai azonosításhoz. Amennyiben a kéz vastagságát is mérni szeretnénk, akkor sok eszközben egy tükör segítségével a kép szélére vetítik a kéz oldalsó képét, amelynek az oldalnézeti alaktani jellemzői is feldolgozhatók lesznek. Ezt a leképezést ortografikus leolvasásnak nevezik ("orthographic scanning").

Ahhoz, hogy a kézről torzításmentes képet kapjunk, a kamerát viszonylag távol kell a kéztől elhelyezni, emiatt a készülék viszonylag nagy helyet foglal el. Erre a problémára ad megoldást, ha egy tükör segítségével fényképezzük le a kezet, a kétféle elrendezésre mutat vázlatos példát az 5.1. ábra. (Megjegyezzük, hogy a célnak megfelelő képet el lehet készíteni akár egy síkágvas szkennelvel is, azonban fokozott igénybevétel esetén nem célszerű mozgó alkatrészeket alkalmazni.) A kéz, ill. ujjak elhelyezését a leolvasó készülékben kis pálcikák segítségével lehet befolyásolni, általuk érhető el az, hogy a pozíció minden esetben közel azonos legyen, a kéz alakja ne torzuljon. Azonban így is előfordulhat - például, ha eltérő testhelyzetben használjuk a leolvasót - hogy a kéz időnként más pozíciót foglal el, és szignifikánsan eltérő mérési eredmények születnek. Ezért célszerű a szkennel használatát betanulni: a testhelyzet legyen mindig hasonló, a kéz feküdjön fel a szkennelő felületre, és azonos irányba tartsuk a kezünket.

Az elkészült kép feldolgozása három lépésben történik:



5.1. ábra. Kéz szkennerek lehetséges változatai. Bal oldal: Torzításmentes képhez a tárgytávolságnak viszonylag nagyoknak kell lennie. Jobb oldal: Tükör közbeiktatása által a készülék mérete csökkenthető.

1. a kéz képének szegmentálása,
2. tulajdonságok kivonása,
3. tulajdonság leírók összehasonlítása.

**A kéz képének szegmentálása:** Az első lépés a kéz területének az automatikus kijelölését jelenti, amit gyakorlatilag egy bináris kép előállításával érünk el a bemeneti kép küszöbölésével. A bináris képeken szükség esetén bináris morfológiai lépésekkel tudunk szűréseket végezni, hogy a kéz képe zajmentes legyen. Sok rendszer speciális képfeldolgozó eljárásokat alkalmaz ahhoz, hogy eliminálja az ujjakat irányító pálcikák hatását, vagy kiszűrje a gyűrűk vagy belógó ruhadarabok hatását. Az előbbi kiszűrése meglehetősen egyszerű, mivel a kamerához képest fix pozícióban vannak a tüskék (így a képből egyszerűen kivonhatók), míg az utóbbi torzító tényezők okozta alakváltozás formai elemzését kell elvégezni ahhoz, hogy ruhát vagy gyűrűt detektálva az adott területet kivonhassuk a kezlet jellemző adataiból. Mivel a kéz mindig azonos pozíciója nem garantálható, ezért néhány egyszerűbb transzformációval (eltolás, elforgatás, affin transzformációk) célszerű a kéz képét egységes formába hozni. Mivel az ujjak egyenkénti elmozdulását a kép egységes transzformációjával nem lehet kompenzálni, ezért abban az esetben, ha a kezlet jellemző tulajdonság-leírók nem invariánsak ezekre a hatásokra, az egyes ujjakat külön kell szegmentálni és feldolgozni.

**Tulajdonságok kivonása:** A kéz alakjához viszonylag egyszerű mérésekkel is jól lehet paramétereket rendelni, sok könnyen mérhető jellemzőt definiálhatunk:

- az ujjak hossza, szélessége, vastagsága (átlagosan, vagy bizonyos pozíciókban),

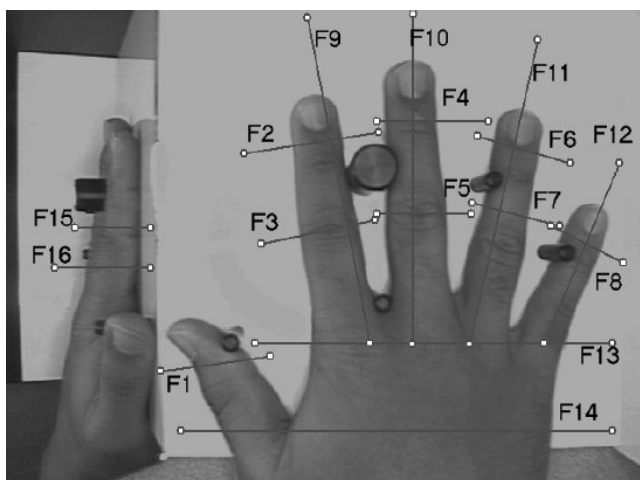
- a tenyér szélessége és vastagsága (átlagosan, vagy bizonyos pozíciókban),
- ujjak ívének vonalvezetése, az ujjak területének jellemzése.

Természetesen ehhez arra van szükség, hogy a kézen jól azonosítsunk bizonyos tájékozódási pontokat. Ilyen pontok lehetnek az ujjak végződésai, az ujjak tövei vagy a tenyér legszélesebb pontja. Ezeknek a megtalálása és a mérések elvégzése a bináris képeken nem okoz nehézséget (lásd 5.2). A kontúr teljes hosszának jellemzésére jól bevált módszer az ún. Fourier leírók használata [87]. A mérési bizonytalanságot úgy a legegyszerűbb csökkenteni, hogy az adatfelvitel során legalább három mérést készítünk és azoknak az átlaga, vagy az együttese jelenti a tárolandó mintát (template-et, template-eket). Ha a kéz képének egészét szeretnénk jellemezni, akkor a kéz kontúrja mentén kell a pontok koordinátáit tárolnunk. Megfelelően sok ilyen pont esetén (esetleg a teljes bináris kép felhasználása esetén) erősebb a minták megkülönböztető képessége, mivel az egész kép alakját modellezzük, nem pedig csak a kép alakjának néhány jellemző méretét.

**Minták összehasonlítása:** A kéz képen mért adatokat egy vektorban tárolva azok összehasonlítására számos metrika alkalmas. Míg az euklideszi távolság nem veszi figyelembe az egyes komponensek változékonyságát, addig a Mahalanobis távolság normalizál a szórás (ill. kovariancia) szerint. Másik lehetséges megközelítése a minták összehasonlításának, ha a statisztikai alakfelismerésben már bevált módszereket alkalmazunk (pl. SVM-et [23]).

A kéz alapú rendszerek teljesítménye általában igen jónak mondható. Egyrészt nincs szükség sok adat tárolására, másrészt a tapasztalatok szerint a döntési hibák is alacsony szinten tarthatók. A Sandia Laboratories egy kereskedelmi rendszer 1991-ben készített vizsgálata során az ún. egyenlő hibaarányt (Equal Error Rate - EER) 0,1%-nak mérte [94], más cikkekben is ehhez hasonló adatokat lehet találni (pl. 0,3% alatti EER-t jelentett [109]). A gyártók oldalain ezeknél kisebb értékeket publikálnak, pl. a Handyman elnevezésű rendszer weboldalán 0,01% EER-rel jellemzik a bemutatott rendszert. Természetesen ezek az adatok nagymértékben függenek a tesztminta jellegétől, célszerű független laboratóriumok méréseire alapozni véleményünket.

Természetesen előfordulhatnak problémák a kézalak-felismerő rendszerek használata közben is. Tipikus eset, hogy kisgyerek felhasználóknál az ujjak pozicionálására szolgáló tüskék túl távol vannak, így a kéz helyzete bizonytalan, esetenként más és más. Ez oly mértékű torzulást okozhat, ami a mérendő tulajdonságokat túlzott mértékben változtatja meg. Hasonló problémát okozhatnak műkörmök, hiányzó ujjak, gyűrűk (időszakosan különböző helyeken, különböző gyűrűket viselve) ill. egészségügyi okokból használt kötszerek. Ügyelni kell a készülék elhelyezésére, hogy a mozgássérültek is kényelmesen használhassák, ill. ha több helyen is el van helyezve leolvasó terminál, akkor azok elhelyezkedése (magassága, iránya) nagyjából megegyezzen, elkerülve az eltérő testtartásból adódó bizonytalanságokat. Elsősorban kültéri felhasználáskor fordulhat elő, hogy a kéz



5.2. ábra. Kéz felülnézeti és oldalnézeti képe a 16 tengellyel, amelyek mentén a mérések történnek. (Kép forrása [60].)

melegéből adódó párasodás rontja a képminőséget, vagy a rendszerbe besugárzó napfény teszi tönkre a feldolgozandó képet.

A készülékek elterjedését elősegíti, hogy több szabványban is foglalkoznak a kéz geometriai adatainak kezelésével. Az ANSI INCITS 396-2005 Hand Geometry Interchange Format megadja a mérés, tárolás és átvitel adatainak formátumát a kéz sziluettjéhez, foglalkozik az adattartalommal és a mértékegységekkel. Ez az amerikai szabvány egyébként megfelel az ISO/IEC CD (Committee Draft) 19794-10 Biometric Interchange Format - Part 10, Hand Geometry Silhouette Data nemzetközi szabványnak, amelynek első verziója már 2007-ben megjelent.



## 6. fejezet

# Erezet alapú módszerek

Mivel az emberi szervezet sejtjeinek tápellátásában az érhalózat nélkülözhetetlen szerepet tölt be, így az erek az egész emberi testet átszövik. Az egyes egyedek alapvető genetikai hasonlósága miatt természetes az is, hogy azonos helyeken hasonló érstruktúrák vannak jelen. Azonban ezek az érmintázatok részleteikben eltérőek. Ha tehát a test olyan területeit választjuk, ahol az erek nagyságrendileg hasonló sűrűséggel találhatók és valamilyen berendezéssel feltérképezhetők, akkor az erek alkalmassá válnak az egyedek azonosítására.

A leggyakrabban alkalmazott erezet alapú módszer a retinát tápláló ereken alapuló azonosítás, azonban a köznyelvben ezt retina biometriának hívják, erezet alapú módszer alatt inkább a kéz, az ujjak és csukló érhalózatának képalkotását és képfeldolgozását értik.



6.1. ábra. Kéz színes felvétele, a kéz infra felvétele, az azonosításhoz detektált érhalózat [45]

Az erezetet jól vizualizáló képalkotó technikák működési elve a következő módon foglalható össze: A vérben lévő hemoglobin a tüdőben oxigént vesz fel, amit az artériákon keresztül a sejtekhez szállít, majd pedig az oxigéntől megsza-

badult hemoglobin a vénákon keresztül áramlik a szív irányába. A hemoglobin e két állapotában másként nyeli el az elektromágneses sugárzást: az oxigén nélküli állapotában elnyeli a közeli infra tartományban a kb. 760nm-es sugárzást. Ennek köszönhetően, ha a tenyeret közeli infravörös fénnel világítjuk meg, az oxigénben szegény vért sötétnek látjuk, és így kirajzolódik az érhálózat egy része. Ezeknek az ereknek a detekcióját és fontosabb paramétereinek leírását kell megoldani a biometrikus azonosításhoz.

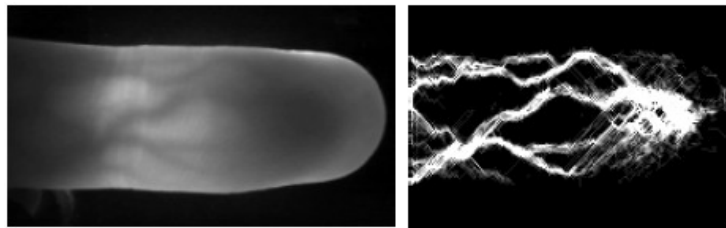
Az első kéz érhálózatának biometriai elemzését bemutató cikkek az 1990-es években jelentek meg [73], [26]. Az ujjak is alkalmasak erezet alapú azonosításra, mint ahogy [79] bemutatja. Az utóbbi cikkben az ujjat világítják át infra LED-ekkel, egy újról 240x180 pixel felbontású 8 bites kép elkészítése megfelelő (lásd 6.2. ábra). A módszer nehézségét az jelenti, hogy az átvilágítás során az útban lévő csontok és az izmok is árnyékot vetnek a keletkezett képen, így nem feltétlenül csak a hemoglobint szállító erek lesznek sötétek, hanem más területek is. A feldolgozás fontosabb lépései:

1. **Pozíció normalizálás:** A művelet célja, hogy olyan képpel dolgozzunk, amelyen az ujj helye és iránya mindig megegyező. A legegyszerűbb, ha az ujj képének a körvonalát vagy az ujj bináris képét használjuk fel ebből a célból, például a középtengely pozícióját és irányát állítjuk be. A középtengely meghatározható bináris morfológiai lépésekkel, pl. vázositással vagy vékonyítással is [85], majd ezek után a kép elforgatását kell elvégezni szükség szerint.
2. **Erek detekciója:** A detekciós mechanizmus lényege, hogy az erek helyén a kép intenzitás profilja tipikusan egy nagyjából meghatározható szélességű völgygel jellemezhető. Ha a követő algoritmus benne van egy völgyben, akkor meghatározható az az irány, ahol a völgyben - az ér mentén - a legmélyebb irányban haladhatunk tovább. Ha már nem található olyan újabb szomszédos pont, amely megfelel a feltételeknek, akkor elértünk a völgy végéig, a követő algoritmus nem halad tovább. Több pontból indítva az algoritmust, a valódi érponthoz nagyobb valószínűséggel fogjuk többször bejárni, mint az esetleges zajhoz tartozó sötét területeket. Sok véletlen indítás után tehát készíthetünk egy térképet, ahol az adott pontok bejárás gyakoriságát jegyezzük fel. Ennek a térképnek a további feldolgozása (újra-mintavételezése, küszöbölése) után kapjuk meg az érpixelet.
3. **Összehasonlítás:** Az újról készült és a mintaként használt érkép összevetése egyfajta regisztrációs algoritmussal történik, ahol a bináris pontok egyezését számszerűsítik.

A fenti módszer pontosabb leírása a [79]-es cikkben található, az ott bemutatott több mint 600 képen végzett tesztek szerint az egyenlő hibaarány (EER) 0,145%. Ez a jónak mondható hibaarány azonban hideg időben valamelyest romolhat, amikor az erek láthatósága csökken.

A Hitachi kereskedelemben kapható érszenzora alapvetően a [79] szerinti elvet követi (lásd 6.3. ábra bal oldalát). A Fujitsu viszont a tenyér érhálózatára





6.2. ábra. Egy ujj infra képe és a lehetséges érponatok: minél többször járt egy pontban a követő algoritmus, annál világosabb egy pont képe a jobb oldali térképen [79].

fejlesztett ki egy biometriai szenzort, aminek a képét az előző ábra jobb oldala mutatja. Ezzel az eszközzel könnyebben megvalósítható, hogy a mintavétel érintésmentes legyen, hiszen a készülék nem fogja közre a kezét, a megvilágítás és az érzékelés azonos irányból történik. Egy a Fujitsu által 70000 személyen elvégzett felmérés szerint az általuk készített rendszer esetén a hibás elfogadási ráta 0,00008% volt, miközben a hibás elutasítást 0,01%-on tudták tartani [45].



6.3. ábra. Balra és középen: A Hitachi cég egyik érhálózatot vizsgáló ujjlenyomat szenzora [56]. Jobbra: A Fujitsu érintésmentes egyoldali tenyér érhálózat szenzora [45].

Összefoglalásként elmondható, hogy a kéz érhálózata kiválóan alkalmas biometriai felhasználásra. Ennek a megközelítésnek több előnye is van:

- a mért jellemző védett helyen van, aminek következménye, hogy
- a mintázat normál esetben nehezen sérül meg, és
- stabilnak tekinthető (nem számolva sérülésekkel, betegségekkel),
- nehezen vehető illegálisan minta (szemben az ujjlenyomatokkal),
- a módszer nem igényel feltétlenül közvetlen kontaktust,
- kombinálható a tenyér bőrfelületével,
- elhasználódás esetén másik ujj is használható.



## 7. fejezet

# Arc

Az arc a hétköznapi emberek számára a legkézenfekvőbb és legnyilvánvalóbb biometria azonosító: egymást leginkább az arc alapján ismerjük fel, és a személyek identitását is az archoz kötjük. Ennek megfelelően a különböző - hagyományos, papír alapú - hitelesítő rendszerekben is igen gyakran használják az arcot, mint például jogosítványokban, igazolványokban, útlevelekben. Annak ellenére egyeduralkodó az arc alapú azonosítás elterjedtsége, hogy az arc igen változékony "képet mutat": az arc formája, színe változik a kor haladtával, az érzelmek, a megvilágítás hatására, befolyásolja a szőrzet és a különböző viselt tárgyak (ékszerek, szemüvegek). A hétköznapi tapasztalat szerint úgy tűnik, az emberek igen jók az arcfelismerésben a sok nehezítő tényezőnek fittyet hányva. Valójában nem teljesen van így: a testalkat, a testtartás, a mozgás jellegzetességei, a ruhaviselet, a hang, a megjelenéskor tapasztalt szituációs helyzet igen nagymértékben hatással van felismerési képességünkre.

Az arc biometria felhasználása a gépi rendszerekben - a felismerés nehézségeinek ellenére - több jelentős előnnyel is jár más módszerekhez képest. Egyrészt távolról is jól rögzíthető az arc képe, a mérés nem igényel fizikai kontaktust, másrészt sok esetben a szereplők tényleges hozzájárulása sem kell a felvételekhez, így a nagyszámban alkalmazott videómegfigyelő rendszerek is felhasználhatók azonosítás céljára. Mindemellett az arc segítségével jó eséllyel meghatározható a személy neme, az életkora, az etnikai hovatartozása és bizonyos érzelmi állapotok is. Az ember-gép kapcsolatban (Human Computer Interface - HCI) is jól használható az arc, akár mint a számítógép működését befolyásoló, vezérlő "eszköz" is.

Az emberi viselkedésben az arcfelismerésnek kitüntetett szerepe van, mivel az agnak bizonyos területe - vagy területei - specializálódtak a feladatra. Az egyik leginkább erre utaló jelenség az ún. arcvakság (prosopagnosia) nevű betegség, amikor is a betegek nem tudnak felismerni másokat vagy archoz kapcsolódó jelenségeket (pl. a személy neme, kora, érzelme), míg más tárgyak felismerésével nincs problémájuk. A betegséget - mely az ún. temporális kéreg alsó részterüle-

teinek szelektív diszfunkciójából vagy sérüléséből ered - Oliver Sacks neurológus - több népszerű könyv szerzője - tette sokak által ismertté. Egyik könyvében arról számolt be, hogy egyik betege a feleségét és a diákjait sem ismerte fel, csak a hangjuk és a mozgásuk alapján [93].

Mielőtt a gépi rendszerek működését elkezdenénk vizsgálni, az olvasóban felmerülhet, hogy az emberek valójában milyen pontossággal ismerik fel egymást, ha csupán az arcra vagyunk hagyatkozva. [69] tartalmaz erre a kérdésre vonatkozó releváns adatokat. Az Amazon cég Mechanikus Török szolgáltatása segítségével annotáltak arcokat, összesen 240000 válaszadatot gyűjtöttek be az internetes szolgáltatás segítségével, a tesztadatbázis valamivel több, mint 5000 arcot tartalmazott. A feladat során egy kép-párról kellett eldönteni, hogy mindkét kép ugyanazt a személyt ábrázolja-e. (A két kép tipikusan más időben és helyszínen készült, még ha ugyanazt a személyt ábrázolta is.) Amikor a személyek a teljes arcot látták (beleértve a fejet és a test környezetét), 99,2%-os volt a felismerés, ha csak az arcot (a fej legtetejét, ill. a nyakat már nem), akkor 97,53%-ra csökkent a pontosság. Érdekes módon, ha ennek a képnek az inverzével végezték a kísérletet (azaz maga az arc ki volt takarva, a fejnek csak kicsi része látszódott) akkor is 94,27%-nak adódott az eredmény.

## 7.1. Története

Az első ismert számítógépes fejlesztések az arcfelismerés területén Woodrow Wilson Bledsoe-hoz, Helen Chanhoz és Charles Bissonhoz kötődnek a 60-as évekből [11], [13]. Az általuk kifejlesztett rendszer bár a beszámolók szerint kielégítően működött, azonban nem volt automatikus működésű, kézzel kellett meghatározni a képeken az arc egyes jellemző pontjait: egy operátor kb. 40 arc pontjait tudta kijelölni egy óra alatt. Később Bledsoe elhagyta a korábbi munkahelyét (a Panoramic Research, Inc. céget) és 1966-tól a Stanford Research Institute-nál kezdett el dolgozni folytatva az arcfelismeréssel kapcsolatos munkáját. Több mint 2000 képet tartalmazó adatbázison elért felismerési eredményeik jobbakk voltak, mint amit az emberek produkálni tudtak [14]. Később mások is hasonló, nem teljesen automata módszert dolgoztak ki, pl. [50] szerint 21 tulajdonság meghatározására volt szükség az azonosításhoz.

A statisztikai adatfeldolgozásban már korábban használt főkomponens elemzés felhasználását az arcok jellemzésére a 80-as évek végén kezdték el alkalmazni. Az egyik első ilyen cikk Sirovich és Kirby nevéhez kötődik [96]. Turk és Pentland 1991-es cikkében már - bár még kevés számú kép esetén - a felismerési tesztek során a zajok hatását is vizsgálták a felismerés pontosságára, az ún. sajátképek által kifeszített térben való kódolás során [106].

A nemek és az arckifejezések felismeréséről már a 90-es években jelentek meg eredmények [24], [51], hasonló módszerek piaci alkalmazásával a közeljövőben várhatóan egyre gyakrabban találkozhatunk.

Arcfelismerő rendszer első tömeges - de nem túl sikeres - alkalmazása a 2001-es tampa Super Bowl mérkőzéskor történt. A stadionba érkező arcokat vizsgálták körözött személyeket keresve. Azonban nem találtak egy keresett személyt sem,

viszont egy tucat ártatlan nézőt tartóztattak fel a rendszer jelzései alapján... Valójában a korszerű arcfelismerő rendszerek ma már igen nagy hatékonysággal működnek, a felismerés pontossága 80-100% közötti, természetesen mindez a körülmények függvénye. A valódi kihívást három problémakör jelenti: több milliós adatbázisokban való keresés; az arc változásai okozta bizonytalanságok; ill. a képpel kapcsolatos megszorítások hiánya. Utóbbi az jelenti, hogy nem csak jó minőségű, beállított arcképeken (ang. "mug shot", lásd 1.4. ábra) kell a felismerésnek működni, hanem változatos körülmények (pl. fényviszonyok, látószög) között. ("Labeled Faces in the Wild"-nak [108] hívják azt a képi adatbázist, amit ilyen képek felismerésének széleskörű tesztelésére hoztak létre.)

A különböző módszerek összehasonlítására 2000-ben egy komplex teszt kezdődött el a NIST vezetésével és több amerikai állami hivatal támogatásával. A Face Recognition Vendor Test (FRVT) néven futó teszteket később továbbfejlesztették és megismételték 2002-ben és 2006-ban [44]. Az utóbbi teszten 10 országból 22 szervezet vett részt, a módszertan alapján dolgozták ki az írisz és ujjlenyomat összehasonlító széleskörű nemzetközi teszteket is. Az események folytatásának tekinthető a 2004-től 2006-ig futó ún. Face Recognition Grand Challenge (FRGC), ahol az arcfelismerés aktuális problémáival foglalkoztak (pl. 3D-s technikák, nagyfelbontású képek) [43].

## 7.2. Az arc képének jellemzői

Az arc bőre az arckoponya csontjain, a homloki területeken a homlokcsont pikelyrészein, ill. a koponya többi részéhez ízülettől kapcsolódó állcsonton feszül. A bőr alatt található arcizomzat részben a csontokon eredve belesugárzik az arcbőrbe, részben az arcbőrben ered és tapad. Az ajkak izmos alapját és a szemhéjak izmos borítását önmagukba visszatérő izmok adják, az arc oldalsó területének alakját részben egy rágóizom határozza meg.

Az arc jellemzőit három szinten lehet csoportosítani:

- Könnyen megfigyelhető globális jellemzők. Ilyen jellemző az arc általános formája, geometriája: pl. kerek vagy hosszúkás arc, a bőr színe, férfias vagy nőies arc, különböző rasszokra jellemző globális vonások.
- Jól lokalizálható jellemzők. Az arc egyes szerveinek, részeinek alakja, az egyes részek egymáshoz való viszonya, vagy textúrája.
- Az arc apró részletei. Sajátos vonásai az arcnak a különböző sebek, ráncok, elszíneződések, szemölcsök, szeplők vagy anyajegyek. Ezeknek a szerepe elsősorban akkor jelentős, ha ikreket akarunk megkülönböztetni.

Az arcfelismerés szempontjából fontosabb, vizuálisan jól felismerhető rész: a homlok, az orrtő, a szemöldök, a felső/alsó szempilla, a felső/alsó szemhéj, az alsó szemhéj ránc, a szemgödör alatti ránc, az orrcimpa, a háromszög pálya, az orr alatti ránc, az ajakbarázda, az állcsúcs.

### 7.3. Arcok detekciója és a jellemzők mérése

#### 7.3.1. Az arcképek készítése

Az arcfelismerés pontosságát alapvetően határozza meg, hogy milyen minőségű képek állnak rendelkezésre. Lényeges tényező az arc irányultsága, a kép felbontása, a fényviszonyok, ill. a jel-zaj viszony. Utóbbi alatt itt most azt is értjük, hogy az esetleges tömörítés során jelentkező hibák jelentősen ronthatják a feldolgozás hatékonyságát, különösen akkor, ha kicsi az arc mérete és jelentős a tömörítés mértéke. Ez elsősorban a biztonsági kamerák archív felvételeinek elemzése során jelent komoly problémát.

Arcfelismerés céljából az arcról készülhet színes vagy szürkeárnyaltos fénykép, infra vagy közel-infra tartományú felvétel, ill. 3D-s pontfelhő. Utóbbiból a további feldolgozás céljából a legtöbb módszer háromszöghálót állít elő. Valójában az arcról nem szükséges teljes 3D-s modell készítése, elegendő csupán egy irányból (tipikusan szemből) egy mélységi térkép generálása. Több ilyen ún. 2,5D-s képből elő lehet állítani a 3D-s modellt, de a felismeréshez erre alapvetően nincs szükség. Természetesen a különböző modalitású képek kombinációjával jobb felismerési aránnyal bíró módszerek alakíthatók ki.

#### 7.3.2. Arcok detekciója

Mivel egy biometria ellenőrző rendszerben a felhasználóktól nehezen várható el, hogy megfelelően tudják pozícionálni az arcukat a kamera képén, ezért a felismerő rendszernek kell első lépésként automatikusan lehatárolnia az arcot befoglaló négyzetet, amely a teljes kép gyakorlatilag tetszőleges területén előfordulhat. Az egyik - ma már klasszikusnak nevezhető - alpmódszer az arcok detekciójára a kép mintázatát, szerkezetét elemző Viola és Jones munkáján alapuló bináris osztályozó [110]. A módszer tetszőleges objektumra betanítható, széles körű elterjedtségét annak köszönheti, hogy meglehetősen jó pontossággal működik, és gyorsan futó implementációját tartalmazza az igen népszerű OpenCV függvénykönyvtár. Mivel ezt a detektort jól lehet használni a biometria más területein is, pl. a fülnek, vagy a szemnek a detekciójára, ezért röviden ismertetjük működését.

*Viola és Jones detektor:* Az eljárás különböző méretű négyzetekkel pásztázza végig a képet és keres a korábban megtanult mintázatoknak megfelelő területeket. A négyzetekkel ún. Haar-szerű szűrőket lehet kiszámolni különböző helyeken és különböző konfigurációkban. Ilyen szűrőkre mutat példát a 7.1. ábra. A szűrőnek előnye, hogy egy ún. integrált kép segítségével gyorsan számítható:

$$IntI(x, y) = \sum_{1 \leq i \leq x, 1 \leq j \leq y} I(i, j). \quad (7.1)$$

Egy blokk értéke pedig:

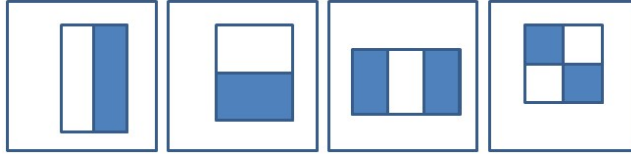
$$I_{blokk} = IntI(BR_x, BR_y) - IntI(TR_x, TR_y) - IntI(BL_x, BL_y) + IntI(TL_x, TL_y), \quad (7.2)$$

ahol az  $IntI$  indexei sorrendben az integrált kép jobb alsó, jobb felső, bal alsó és bal felső sarkait jelentik. A szűrők elhelyezkedése a vizsgálati ablakon belül rengeteg pozíciót vehet fel, a szűrők kimenete a sötét és világos területek összegének különbsége. Ahhoz, hogy bonyolult mintázatokat is meg tudjunk különböztetni, igen sok ilyen szűrőre van szükség, amelynek a kiszámítása, ill. osztályozásban való használata sok időt igényel a tanítás és a felismerés során egyaránt. Az előbbire az ún. AdaBoost [42] algoritmus ad megoldást, az utóbbira az, hogy a felismerés során vízesésszerűen kell a szűrőket alkalmazni, és amennyiben valamelyik kimenete negatív, tovább már nem kell vizsgálni az adott mintázatot (lásd 7.2. ábra), a többi szűrőt már nem kell alkalmazni rengeteg erőforrást megtakarítva.

Az AdaBoost <sup>1</sup> algoritmus a boosting tanuló algoritmusok családjába tartozik, az egyike az első adaptív megoldásoknak. Az eljárás lényege, hogy nagy számú, de gyorsan kiszámítható osztályozót (pl. a Haar-szerű szűrőket) súlyoz úgy, hogy végül egy bináris döntést hozzon egy osztályozási feladatban. Az egyes osztályozók súlya arányos a megkülönböztető képességükkel, az algoritmus kimenete a súlyozott gyenge osztályozók kombinációja:

$$H(\omega) = \text{sign} \sum_{t=1 \dots T} \alpha_t h_t(\omega) \quad (7.3)$$

ahol  $h_t$  egy  $w$  tulajdonságot kiértékelő gyenge osztályozó (melyből  $T$  darab van), az  $\alpha$ -k pedig a súlytényezők.



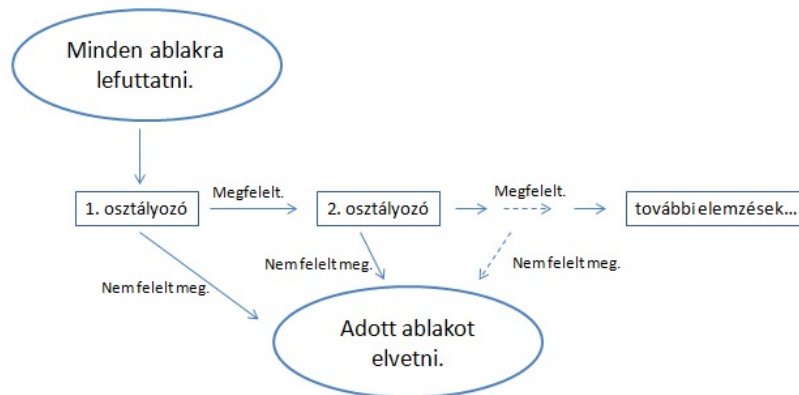
7.1. ábra. A Viola és Jones detekciós módszer által alkalmazott négy különböző elrendezésű Haar-szerű szűrő mintázata. A sötét és a világos területek összegének különbsége a szűrő kimenete.

A Viola és Jones objektum-felismerési módszert - megfelelő betanítás után - lehet alkalmazni az arc egyéb részeinek a felismerésére is, mint pl. szemek, orr, ajak.

### 7.3.3. Tulajdonságok kivonása és egyezésvizsgálat

A tulajdonságkinyerő és feldolgozó módszereket alapvetően három nagy csoportba lehet sorolni:

<sup>1</sup>Robert Schapire korábbi megoldása ("recursive majority gate formulation") és Yoav Freund korábbi algoritmusai ("boost by majority") nem voltak megfelelően adaptív. Közös munkájuk eredménye az AdaBoost, amely már igen jó adaptivitással tudja a gyenge osztályozók együttes hatékonyságát kihasználni. Ezért az eredményükért elnyerték az igen nagy elismerést jelentő Gödel Prize kitüntetést.



7.2. ábra. A vízesés felismerési modell előnye, hogy gyorsan - már részleges vizsgálatok után - elveti a nem megfelelő mintákat, így jó eséllyel csak akkor fut le nagyszámú vizsgálat, ha a vizsgált minta megfelel a kritériumoknak. Ennek megfelelően a hibás pozitív minták aránya eleinte igen nagy - de folyamatosan csökken -, míg a hibás negatív arány kicsi, majd növekedni kezd.

- **Látszat alapú:** A teljes arcot reprezentáló adattömbön statisztikai tömörítést hajtanak végre, a hasonló arcok keresése a csökkentett dimenziójú vektorok összehasonlításán alapul.
- **Modell alapú:** Az arc kitüntetett pontjait (áll csúcsa, ajak sarka, stb.) jelölik ki, ezek lokális tulajdonságán és egymáshoz való geometriai viszonyán alapul.
- **Lokális leíró alapú:** Az arcon sok lokális jellemző pontot keresnek, amelyek lehetőleg különböző körülmények között is jól detektálhatók és a leírásuk (tulajdonság vektoruk) invariáns több nem kívánt hatásra, mint pl. fényviszonyok változása, geometriai torzulások.

*Látszat alapú módszerek:* Ezek az eljárások nem választanak ki kitüntetett részeket az arcon, hanem az egész arcterületet, mint bittérképet veszik az összehasonlítás alapjául (miután a 2D-s mátrix struktúra pixeleit egyszerűen sor- vagy oszlop-folytonosan végigjárva vektorba fejtették). Ez azonban egyrészt több tíz vagy százezer képpontot jelent, aminek a feldolgozása alapvetően túl lassú lenne, másrészt számos lényegtelen terület van az arcon, amelyek - az osztályozás szempontjából - nem hordoznak lényeges információt. Ezért olyan dimenziócsökkentő módszert kell használni, ami jelentősen csökkenti az adattömbök méretét, de a lényeges, arcra jellemző információkat nem torzítja számottevően. A lényeges információk kiválasztására több megoldás is létezik. A főkomponens elemzés (Principal Component Analysis - PCA) olyan általános adattranszformáció, amely során a transzformálandó vektorok



jó eséllyel korreláló komponensei közti korreláció megszűnik. A transzformált vektorok komponensei sorrendben egyre kisebb szórással rendelkeznek, így azok diszkriminatív tulajdonsága is jó eséllyel egyre kisebb lesz. Ezért ezeknek jelentős részét elhagyva (az adattömb méretét jelentősen csökkentve) az adatok még jól használhatók a különböző osztályozási módszerekben [106]. A PCA olyan transzformációt hajt végre az adatokon, amely a kiindulási vektorok halmazának statisztikai elemzésén alapul, a kovariancia mátrix legnagyobb sajátértékéhez tartozó sajátvektorok adják a transzformáció bázisait.

A transzformáció után az arcok vektoriális leírása az új bázisfüggvényekhez való hasonlóságot írja le (hasonlóan a Fourier transzformáció együtthatóihoz). Így ha a tanító arcokból (pl. a felismerni kívánt személyekről készült adatbázison) számítjuk ki az új bázisokat és végrehajtjuk a transzformációt, akkor viszonylag kevés együttható elegendő lehet az arcok jellemzéséhez. Bár a PCA alapú modellek törekszenek a minimális információ veszteségre (adott komponensszám mellett), de nem veszik figyelembe, hogy a vektorok különböző osztályokhoz (különböző arcokhoz) tartoznak, ezért előfordulhat, hogy nem nagy szórású, de diszkriminatív vektorkomponensek is a transzformációt követő dimenziócsökkentés áldozatául válnak.

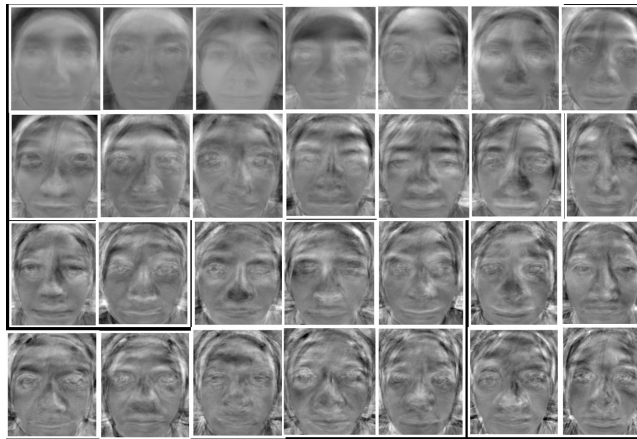
Ezzel szemben a lineáris diszkriminancia elemzés (Linear Discriminant Analysis - LDA) a transzformáció bázisképeinek meghatározása során nem csak a teljes tanító képhalmaz szórását vizsgálja, hanem arra törekszik, hogy az osztályokon belüli szórás minimális, az osztályok közti szórás maximális legyen a transzformáció után. Természetesen ezzel a megközelítéssel jobb osztályozási eredmények érhetők el [6].

A PCA során kapott ún. bázisfüggvények - amelyek referenciaként szolgálnak az új együtthatók előállításához - elnevezésére a sajátarcok (eigenfaces) kifejezést használjuk. Az LDA azonos funkcióját betöltő függvényeket Fisher arcoknak nevezzük (lásd Fisher lineáris diszkriminánsok [6]).

*Modell alapú technikák:* A modell alapú megoldások 3D-s vagy 2D-s modellt alkotnak az arcról vagy a fejről és a modell paramétereinek összehasonlításával végzik a felismerést. A legegyszerűbb modellek nem képesek kezelni a paraméterek torzulását olyan esetekben, amikor a fej elfordul, míg másokat pózfüggetlennek lehet tekinteni, legalábbis egy bizonyos mértékig. A modell alapú módszerek komplexitása meghaladja a látszat alapú módszerekét, mivel fontos - és egyben viszonylag időigényes lépésük - az egyes jellemző pontok megkeresése, mint pl. az orr hegye, a szemek vagy az ajkak sarka.

Az egyik leggyakrabban hivatkozott modell alapú technikát, az ún. Face Bunch Graphs (FBG) módszert [114] ismertetjük tömören, bár több hasonló megoldás is létezik (pl. az Active Appearance Model (AAM) [22]). Az FBG az arcot egy gráfként kódolja, ahol a csomópontok megfelelnek az arc valamely jellemző kulcspontjának. A csomópontok jellemzésére ún. Gabor együtthatók halmazát használják, amelyek a pont környéki terület texturális jellemzőit írják le. Az együtthatók előállítása különböző irányú és frekvenciájú Gabor szűrőkkel számított konvolúcióval történik.

A gráf modell létrehozása - a módszer betanítása - alapvetően két lépéssel tör-

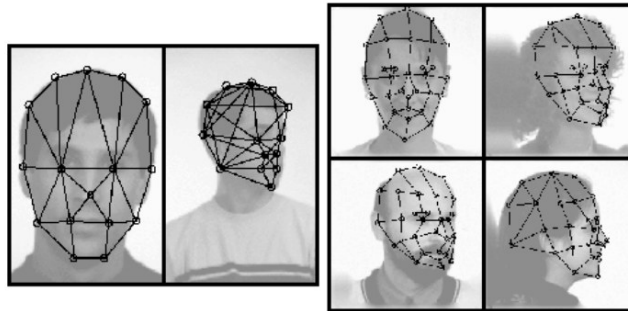


7.3. ábra. 40 arckép segítségével előállított 28 sajátkép (készítette Brian Harding és Cat Jubinski, Cornell University)

ténik. Először az operátornak kézzel kell kijelölnie a jellemző pontokat (egy vagy néhány kép alapján) és meg kell határoznia a gráf alapvető struktúráját. Ezek után a tanítóhalmaz többi képén már nagyrészt automatikusan lehet végezni a tanítást, kézi beavatkozás csak akkor szükséges, ha egy újabb tanító képen rossz helyre került volna a csúcspont. Mivel azonban az egyes pózokhoz (a fej különböző irányultságához) külön tanítást végzünk (és ezekhez eltérő gráf struktúra fog létrejönni), ezért ilyen ritkán fordul elő. Második lépésként a több képből kivont Gabor leírókat összegyűjtjük, így csomópontonként egy egész csoport (bunch) áll majd rendelkezésünkre a keresés során. Ezek a csoportok tehát egyfajta póz, egy arcrészletének a változatos megjelenését tudják jellemezni: pl. csukott, vagy nyitott szájakat, szemeket, a különböző fényviszonyok hatásait, a különböző kortól vagy nemtől függő megjelenési mintákat. Két csomópont távolsága a gráfon a tanítóhalmazra jellemző adott pontok átlagos távolsága. Arcfelismerés során az ún. Elastic Bunch Graph Matching algoritmust lehet alkalmazni a következő lépésekkel:

1. Egy közelítő keresés során a feldolgozandó kép diszkrét helyein a Gabor szűrőket alkalmazzuk, majd a generált leírókat összevetjük a tanítóhalmaz leíróival. Ilyenkor a tanítóhalmaz leíróinak csomópontonkénti átlagát is használhatjuk.
2. A keresést pontosítjuk, most már bizonyos csomópontok összes halmazát használjuk és a legjobb egyezéseket keressük meg csomópontonként.
3. A feldolgozandó arcon a csomópontok pozícióit finomhangoljuk úgy, hogy a tanítóhalmaz valamely Gabor halmazával a legjobb egyezést érjük el, a feldolgozás eredménye egy olyan képgráf lesz, amely a meglévő FBG modellhez legjobban illeszkedik.

4. Két arc hasonlóságát úgy számítjuk ki, hogy az egymásnak megfelelő csomópontok hasonlóságát átlagoljuk. Mivel ismertek a csomópontok pozíciói, két arc összehasonlítását úgy is el tudjuk végezni, hogy ha hiányoznak bizonyos csomópontok. Így a módszer kevésbé érzékeny a fej pozíciójára, takarásokra vagy jelentősebb fényhatásokra.



7.4. ábra. A bal oldali gráfok az arc megkeresésére lettek meghatározva, a jobb oldali, valamivel részletesebb gráfok pedig arcfelismerésre. Kép forrása: [114].

*Lokális leíró alapú módszerek:* Olyan jellemző pontok keresését, leírását és összehasonlítását végzik el, amelyek robusztus módon detektálhatók az arcokon változatossághoz viszonyított körülmények között. Ilyen leíró pl. az LBP (Local Binary Patterns) [83] vagy a SIFT (Scale Invariant Feature Transform) [70]. Utóbbi módszer igen nagy népszerűségnek örvend a képvisszakeresésben, kategorizálásban, s mivel a biometria más területén is jól lehet használni, ezért tömören ismertetjük.

A transzformáció első lépéseként Gauss konvolúciós szűrővel végzünk simítást több lépésben, hogy egy ún. képpiramist hozzunk létre (a simítás során a kép méretét is csökkentjük különböző lépésekben, ún. oktavokat hozva létre). Ezt követően a szomszédos konvolúciós szintek különbségével az ún. DOG (Difference of Gaussians) képeket számítjuk ki, amelyeken lokális szélsőérték pontokat (minimum és maximum) keresünk. A lokális szélsőérték feltétele, hogy a pontnak a szomszédos 8 pixel értékénél, és a piramis szomszédos szintjein található 9-9 közvetlen szomszédjának értékénél is kisebbnek (minimum), illetve nagyobb-nak (maximum) kell lennie. A különböző skálaszinteken detektált pontok koordinátáinak pontos meghatározásához interpoláció szükséges. Mivel ennek a feltételnek túl sok instabil pont felel meg, ezért csökkenteni kell a kulcspontok számát, a következő lépés az instabil pontok törlése: az alacsony kontrasztú, és a nem elég magas sarkossági jellemzővel rendelkezőket el kell távolítani (előbbihez a Laplace operátort, utóbbihoz a Hesse mátrixot vesszük segítségül). A szűrési feltételeknek megfelelő kiugró szélsőérték pontok lesznek a továbbiakban a SIFT kulcspontok.

Ezek után ezen pontok invariáns jellemzését kell elvégezni. A kulcspontok képi pozícióját, és a hozzájuk tartozó skálát ismerjük, a feldolgozás következő lépése irányok rendelése a pontokhoz, amelyeket a lokális gradiens jellemzők

alapján határozzuk meg Az elforgatás invariancia biztosításához relatív koordináta rendszert kell kijelölni, melyet a kulcsponthoz tartozó fő gradiens irányhoz (a kulcspont orientáció) rögzítjük. A súlyozott irány-hisztogram minden csoport azon gradiens-magnitúdók súlyozott összegét tartalmazza, amelyek iránya a csoportba esik. Az irányokat 10 fokként tekintjük egy csoportnak. A domináns irányok a hisztogram kiemelkedő értékei lesznek. Alapvetően a legnagyobb ilyen csúcsot tekintjük fő iránynak, de ha előfordul még olyan érték, mely a maximális érték 80%-án belül van, akkor létre kell hozni vele egy új kulcspontot ugyanazon a helyen.

A SIFT leíró a súlyozott irány-hisztogramokból generáljuk, minden SIFT pont környezetében  $4 \times 4$  hisztogramot hozunk létre, egyenként 8 iránnyal. Összességében egy 128 elemű vektort kapunk, amely értékeit normalizáljuk. Két SIFT pont hasonlóságát az L2 távolság alapján mérjük, egyezés meghatározásánál általában figyelembe vesszük az egyezés egyediségét (jellemezhető a (1.legjobb megfeleltetés hasonlósága)/(2.legjobb megfeleltetés hasonlósága) arányszámmal).

A SIFT általában jó hatásfokkal alkalmazható képi egyezések keresésére, egyetlen hátránya a magas számításigény. Az algoritmus csak a leírók generálását, annak matematikai módszereit definiálja. A leírók egyezésének vizsgálata többféleképpen is megoldható.

A modell alapú módszerrel összevetve a fő különbség abból adódik, hogy sokkal több jellemző pontról van szó, amelyek kiválasztása teljesen automatikusan történik, ill. az invariancia a leíró technikában különös hangsúlyt kapott.

## 8. fejezet

# Fül alakja

Míg az arc természetesen az egyik legkézenfekvőbb tárgya a személyazonosításnak, a fejen oldalt található fül használata már kevésbé nyilvánvaló módszer. Azonban a fül alakja is elegendően részletgazdag és egyénenként eltérő ahhoz, hogy biometrikus azonosításhoz felhasználható legyen. Ráadásul a fül alakját nem befolyásolják olyan tényezők, amelyek az arc esetében megnehezítik a felismerést (pl. különböző arckifejezések).

A fül alapú azonosítás egyik legismertebb szakértője szerint nincs két azonos alakú fül: több évtizedes kutatási és felhasználói gyakorlatában - több ezer minta vizsgálatáról beszélünk - nem találkozott ilyen esettel, még kettes, ill. hármas ikrek esetén sem [58].

A fül az archoz képest oldalról látszik, így arcképekről az alakja általában nem határozható meg, azonban ha nem pont oldalról fotózzuk a fejet, a kisebb torzulásokat kompenzálni lehet, és a megfelelő geometriai jellemvonások elegendő pontossággal lemérhetők.

A fül alakját a vázát alkotó rugalmas porc és a hozzá szorosan tapadó bőr határozza meg. A fülkagyló általában 25-30 fokos szöget zár be a koponya felszínével. A fül alakja nagyrészt az 5. életévig kialakul, ezek után lineárisan változik, később már csak öregkorban jellemző szignifikáns alakváltozás az arányok megváltozásával. Formája meglehetősen bonyolult, három jól elkülöníthető részből épül fel:

- külsőfül (elasztikus porcos fülkagyló, csontos és porcos külső hallójárat),
- középfül,
- belsőfül.

Kívülről csak a külső fül látható, a kezelőorvos is csak a középfület és külső fület elválasztó dobhártyáig tud betekinteni, az azonosításban csak a fülkagyló alakjának az elemzésével foglalkozunk. A fülkagyló fontos funkciója, hogy a hangrezgéseket felfogja és a hallójáratba irányítsa.



8.1. ábra. A fül külső részei

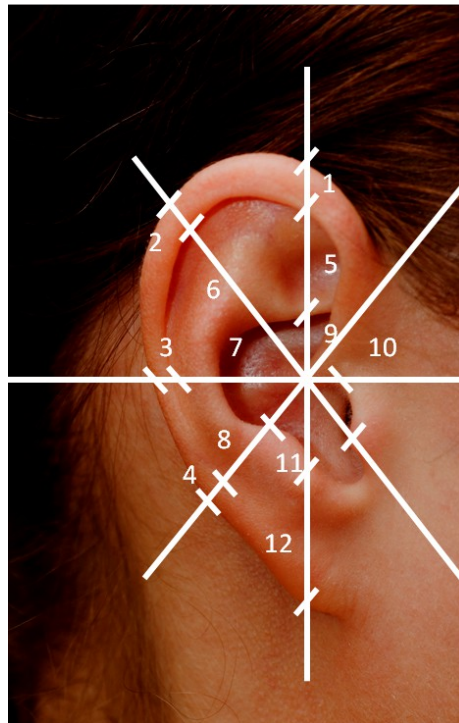
## 8.1. Detekció és felismerés

A fül mérete viszonylag nagy, ezért relatív könnyen fényképezhető (ellenben az írisszel vagy retinával). A fül képének feldolgozása alapvetően három lépésben történik: 1. detekció, 2. tulajdonságok kinyerése, 3. tulajdonságok összevetése. Mivel a 3. lépés az előzőktől nagymértékben függ és belőlük következik, ezért csak az első két pontot tárgyaljuk.

1. **Detekció:** A detekcióra többféle módszer is alkalmazható. A legkézenfekvőbb egy általános fül mintával való egyezést vizsgálni, ahol a minta tartalmazhat éleket, vagy akár valamilyen szűrőkre adott választ is. Utóbbi megközelítésnek tipikus esete a Viola és Jones (korábban már bemutatott) általános detekciós mechanizmusának [110] alkalmazása. A keresést gyorsíthatja, ill. leegyszerűsítheti, ha a bőrszín vagy az íves fülszegély, ill. a fülcimpa lokalizációjával kezdjük a keresést.
2. **Tulajdonságok kinyerése:** A tulajdonságok kinyerésére számos különböző módszer létezik, ezek közül most néhány alapvető megközelítést tekintünk át: geometriai jellemzők mérése; kép alapú direkt összevetés; jellemző pontok felhasználása; 3D-s módszerek.
  - Geometriai tulajdonságok: A fül alakját jellemző módszerek közül a legkorábbi megoldást Iannarelli dolgozta ki [58]. A megoldása nem automatikus, a fül pozícionálását, méret szerinti normalizálását és

a jellemző szakaszok kijelölését kézzel kellett elvégezni. A módszer illusztrációja a 8.2. ábrán látható a megjelölt szakaszokkal, amelyeket csak 3 mm-es pontossággal rögzítettek a személy neme és rassza mellett. A fül lehetséges méretét is figyelembe véve könnyen belátható, hogy az így meghatározott paraméterterben csak néhány millió eltérő minta tárolható. A módszer másik fő hátránya a koordináta rendszer origójának meghatározása. Ez a lépés nehezen automatizálható, azonban nagyban befolyásolja a mérések kimenetét. Mindezekkel szemben Burge és Burger módszere jól automatizálható [17]. A teljes fejről (oldalnézetből) elegendő egy 300x500-as felbontású képet készíteni, amin a fül detekcióját kell először elvégezni. (A módszer néhány fontosabb képi kimenetét a 8.3. ábra illusztrálja.) Ezek után a Canny [18] éldetektor alkalmazásával a fontosabb élek kijelölése történik meg. A rövidebb éleket - amelyek feltehetőleg nem fontosak az azonosítás szempontjából - törölni lehet. Alapjában véve a megmaradó élek már alkalmasak lennének a fül azonosítására, de sajnos ezek pontos pozíciója erősen függ a megvilágítástól, ezért ezen élek egymáshoz való viszonyát kell valamilyen módon felhasználni. Ebből a célból az élpontok körül ún. voronoi cellákat kell létrehozni (ahol a cellák minden pontja ahhoz az élhez tartozik, amelyhez a legközelebb van). Ezek után minden cellát a középpontja, mint gráf csúcspont reprezentál, az egymással szomszédos cellákat pedig élek kötik össze. Két fül összehasonlítása ezek után a gráfok összevetésén alapul: a csúcspont a Canny detektor által meghatározott élek tulajdonságát jellemzi, a gráf éle pedig két cella viszonyát.

- Kép alapú dimenziócsökkentő módszerek: Hasonlóan az arcfeldolgozás egyik fő irányához, ebben az esetben a fül képét, mint bittérképet dolgozzák fel. Mivel több tízezer - köztük sok lényegtelen, homogén területet kódoló - pixelről van szó, ezért a lényegi információ kiemelését - azaz a dimenziócsökkentést - valamilyen általános statisztikai módszerrel érdemes elvégezni. Ilyen lehet az ún. főkomponens elemzés (Principal Component Analysis), vagy a lineáris diszkriminancia elemzés (Linear Discriminant Analysis) [75]. A módszerről bővebben az Arc fejezetben olvashatunk.
- Jellemző pont alapú módszerek: Két fül összehasonlítását elvégezhetjük jellemző pontok detektálásával és ezen jellemző pontok pozíciójának és/vagy környezetének összehasonlításával. Valójában a korábban említett Iannarelli módszer is hasonló volt, de a jellemző pontokat egy nehezen lokalizálható középponthoz képest határozta meg, nem pedig a pontok maguk voltak jól detektálható jellemző mintázatok. A célra talán a legalkalmasabb módszer az ún. Skála Invariáns Tulajdonság Transzformáció (Scale Invariant Feature Transform - SIFT), amely eljárás módszert ad a megfelelő pontok detektálására, leírására és összehasonlítására [70]. A SIFT fő előnye, hogy az általa generált leírók nagymértékben invariánsak az affin geometriai

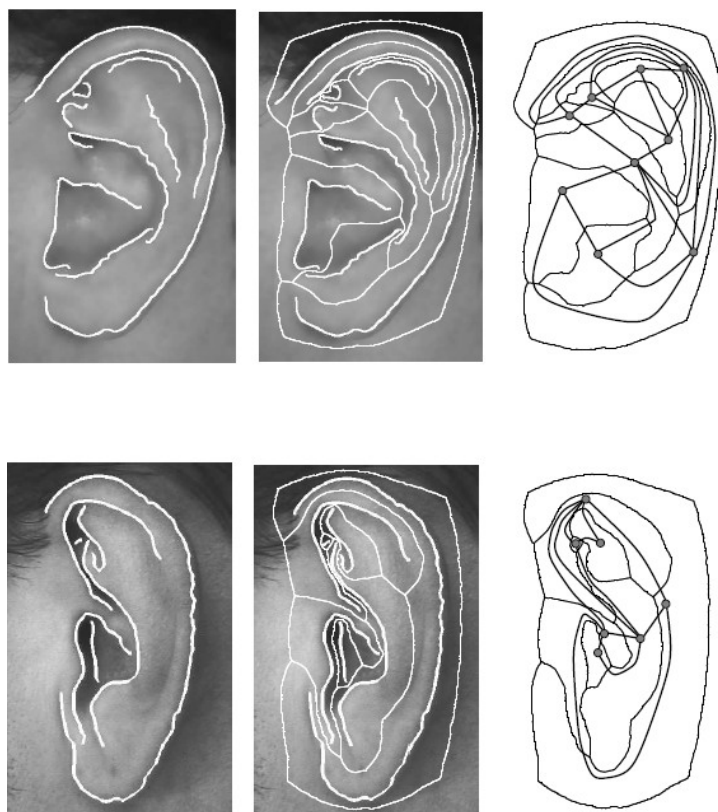


8.2. ábra. Az Iannarelli módszer által kijelölt azonosítási pontok

transzformációkra és az átlagos intenzitás változásokra, amelyek a fényképfelvételek esetén gyakran fordulnak elő. Léteznek a SIFT-nél jóval gyorsabb, bár kevésbé robusztus módszerek (pl. SURF, FAST), amelyek szintén alkalmasak lehetnek a célra.

- 3D módszerek: Egyre több eszköz alkalmas 3D-s objektumok pontjainak, formáinak rögzítésére. Ebben az esetben a fülről korábban eltárolt minta is 3D-s, és magát a detekciót és összehasonlítást is 3D-ben kell elvégezni. Az illesztés során kompenzálni kell a fül 3D-ben értelmezett pozícióját és irányát (előbbi a méretre is hatással van). Egy jól használható módszer az ún. Iteratív Legközelebbi Pont algoritmus (Iterative Closest Point - ICP) [8]. Az illesztés hibájának a mértékét lehet használni az azonosítás során.
- Hang alapú megközelítés: Akkermans és munkatársai akusztikus módszert alkalmaztak a külső hallójáratból visszaverődő hanghullámok mérésével [2]. Eljárásuk szerint adott frekvenciájú mérőjelet kell a fülbe sugározni, majd a visszaverődő hanghullámok spektrális jellemzőit mérni. Ezzel a megközelítéssel 1,7%-7% közötti EER-t tudtak elérni, attól függően, hogy fejhallgatót vagy mobiltelefont használtak a kísérletek során.





8.3. ábra. A Burge és Burger-féle módszer alkalmazása két fülre. Balról jobbra: a fülön a Canny detektor által kijelölt élek, az élek által meghatározott voronoi diagrammok, a régiók reprezentációja gráfokkal. Kép forrása: [16].

Bár kiterjedt felmérésről nincs tudomásunk a fül alapú azonosító rendszerek megbízhatóságával kapcsolatban, több irodalmi példa is igazolja a fül ilyen célból való megbízható felhasználhatóságát [16]. Azonban van néhány nyilvánvaló tény, amely megnehezíti az alkalmazhatóságot: alapvetően a haj általi takarás okozza a legtöbb problémát. Ezt a kérdést a haj detekciójával, és az általa takart területek összehasonlításból való kivonásával tudjuk kezelni. A detekció történhet a látható vagy pedig az infra tartományban. Utóbbi azon az elven alapul, hogy a haj hőmérséklete valamivel alacsonyabb, mint a fülé, tehát egy infra kép nagyban megkönnyíti a haj eliminációját a képről.

A másik probléma a bűnügyi felhasználás során jelentkezik: ha nem közvetlenül fényképezéssel rögzítjük a fül alakját, hanem valamilyen lenyomat alapján végezzük az összehasonlítást, jelentősen megnőhet a bizonytalanság. Ennek az az oka, hogy ha különböző erővel nyomjuk a fület a felülethez, torzul annak az

alakja. Egyik híres példája a fül alapú azonosítás bűnügyi alkalmazásának a David Wayne Kunze által elkövetett gyilkosság felderítése és pere volt, amikor is a fül alakja perdöntő bizonyítékként szolgált Kunze bűnösségének kimondásában [99]. A per során - egyéb szakértők mellett - tanúként hallgatták ki Alfred V. Iannarellit és Cornelius Van der Lugt amatőr, de elismert holland szakértőt. Van der Lugt addigra már több száz esetben vizsgált füllenymat azonosságokat és hat esetben bírósági perben is szakértőként szolgált.

Az említett két hátrány ellenére a fül több előnnyel is bír más hasonló (pl. arc alapú) megközelítésekkel szemben. Az archoz hasonlóan itt sincs higiéniai kockázat (kontaktusmentes az adatrögzítés), de a fülnek, mint objektumnak a detekcióját segíti, hogy jól becsülhető a fül hátttere. Emellett a fül alakját nem lehet szándékosan torzítani, a hangulat, és egyéb befolyásoló tényezők minimálisak, eltekintve a már említett hajtól és ékszerektől.

Chang és társai [19] a tanulmányukban összehasonlítják az arc és a fül alapú azonosítást. A cikkükben bemutatott kísérlet szerint a felismerési pontosságot a fül esetében találták magasabbnak: 72,7% a 69,3%-kal szemben. Az arc és a fül együttes felhasználásával lényegesen jobb eredményt, 90,9%-ot tudtak elérni hasonló körülmények között.

## 9. fejezet

# Retina

A retina (más néven az ideghártya vagy recehártya) a gerincesek szemének a látásért felelős fényérzékeny rétege. Feladata, hogy a szembe érkező fényt elektromos jelekké alakítsa, amelyek az agyba jutva létrehozzák a látás komplex funkcióját. Mivel az embrionális fejlődés során az agyból nő ki (és neurális feldolgozást is végez), ezért a központi idegrendszer egy kihelyezett részének tekinthetjük.

A biometriai azonosítással kapcsolatban a legfontosabb, amivel tisztában kell lenni, hogy jelen esetben nem magát a retina fényérzékeny látósejtjeit vizsgáljuk, hanem a retina vérellátásért felelős érhálózat képi mintázatát.

### 9.1. Történeti háttér

Annak ellenére, hogy a szem belső felülete szabad szemmel nem látható, a retina felhasználása a személyazonosításban viszonylag korai elvi megoldásnak számít, Legelőször 1935-ben két szemész Carleton Simon és Isodore Goldstein vélte felfedezni - szembetegségek tanulmányozása során - hogy a szemben lévő érhálózat teljesen egyedi. Hamarosan publikálták is megfigyelésüket, miszerint a retina-fényképek segítségével lehetséges az egyedek személyazonosítása [95].

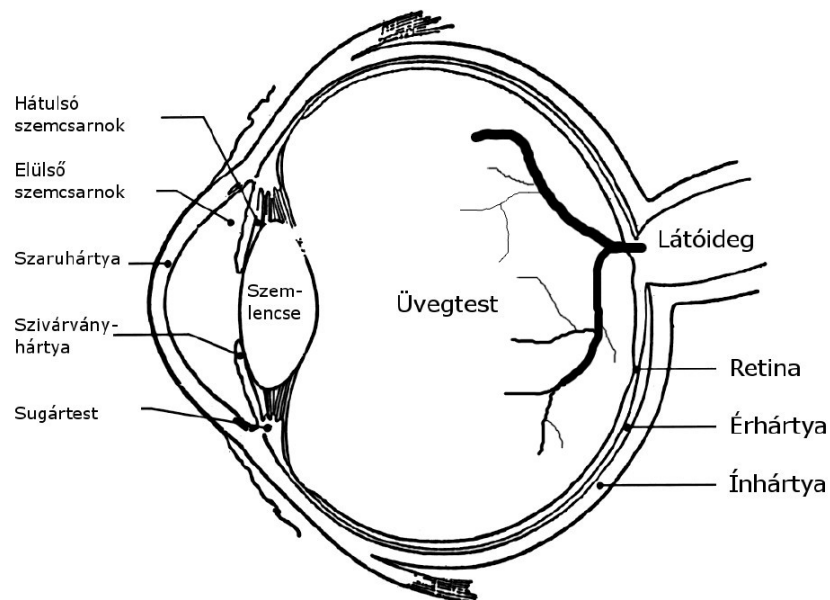
Az ötvenes években Dr. Paul Tower tett értékes megfigyeléseket ikrek tanulmányozása során, miszerint a sokmindenben nagyon hasonló ikrek esetén is eltér a retina érhálózatának struktúrája [105].

1976-ban Robert "Buzz" Hill azzal a céllal hozta létre az EyeDentify Inc. nevű céget, hogy retinaazonosításra alkalmas rendszert fejlesszen ki. 1978-ban szabadalmaztatták a kifejlesztett speciális szkennerkészüléket. Kereskedelmi modellek a 80-as évek első felében jelentek meg a piacon.

### 9.2. A szem felépítése

A szem felépítését a 9.1. ábra szemlélteti. Az egyes részek magyar és angol elnevezései:

- szaruhártya - cornea
- elülső csarnok - anterior chamber
- szivárványhártya - iris
- hátsó szemcsarnok - posterior chamber
- sugártest - ciliary body
- szemlencse - lens
- üvegtest - vitreous body
- látóideg - optical nerve
- ínhártya - sclera
- érhártya - choroid
- ideghártya - retina



9.1. ábra. Az emberi szem felépítése. A retina kettős érhálózata az érhártyából, és a retina belső felületén futó erekből áll (az ábrán középen látható erek).

Az optikai leképezést a szem minden olyan része befolyásolja, amelyen áthalad a fény, tehát a szaruhártya, az elülső csarnok, a szemlencse, az üvegtest

és maga a retina is. Így, ha ennek a rendszernek valamelyik része nem funkcionál megfelelően, akkor az befolyásolja a retináról kapott képet. Azonban az érhálózatról elegendő egy relatív kisfelbontású kép az azonosításra, így a kép kismértékű homályosodása nem jelent lényegi problémát. Gyakorlatilag, ha valakinek nem túl rossz a látása (pl. alkalmas gépjárművezetésre), akkor a retinája megfelel a biometriai azonosítás céljaira. Azonban a pupilla (a szivárványhártya által határolt nyílás a szemlencse előtt) mérete lényegileg meghatározza a szembe jutó fény mennyiségét, így hatással van a retina érhálózatáról alkotott képre.

Maguk a fényt érzékelő receptorok (csapok és pálcikák) igen kicsik, így normál eszközökkel távolról nem tudjuk azokat azonosításra használni, viszont a retinát belülről tápláló érhálózat - mivel a szem belső felületén helyezkedik el - jól látható és használható, különösen infra tartományban (lásd ezezt alapú módszerek).

A retina belső rétegeinek vérrel való ellátását a retina központi erei végzik, amelyek szemtükörzéssel és különböző (fundus) kamerákkal is jól megfigyelhetők. Ezek az erek a látóideg becsatlakozásánál (vakfolt) lépnek be a szembe, az állapotuk fontos diagnosztikai információforrás az ideghártyát, a központi idegrendszert és az érrendszert érintő kórképek felismerésében. Az ideghártya véráramlásában az érhártya is fontos szerepet tölt be, főleg a mélyebben fekvő rétegek esetén. A retinával határos érhártyaréteg az emberi szervezet legsűrűbb hajszálérhálózata.

### 9.3. Mérés és jelfeldolgozás

A mérés és jelfeldolgozás alapját a retina egy körkörös sávokra osztott területe adja. A vizsgált terület kiterjedését (a határoló külső és belső körök sugarát) úgy célszerű meghatározni, hogy az adott készülékkel különböző környezeti hatások (pl. pupilla átmérő) mellett is megfelelő világossággal és kontraszttal rendelkezzen a terület. Ahhoz, hogy mindig azonos területen történjen a mérés, a kamerának és a szem tengelyének egy vonalba kell esnie. Ezt úgy lehet elérni, hogy ún. fixációs pontokat kell a nézőnek takarásba hozni. Szemüveg viselése két okból is problémát jelenthet: egyrészt tükröződések keletkezhetnek, másrészt a szemüveg más és más módon torzíthatja a képet attól függően, hogy milyen szögben viselik.

A kép világosságának egyfajta normalizációját lehet elérni, ha egy pont világosság értékét a körülötte lévő régió átlagos világosságához hasonlítjuk. Ezzel kompenzálhatjuk a vizsgált terület esetleges egyenetlen világosságeloszlását, ill. a pupilla esetenként eltérő méretéből adódó hatást. [54] szerint 96db 4 bites normalizált kontrasztértéket tárolnak el szemenként, azaz 2x48 byte alapvetően elég a mintázat jellemzésére. A mintázat tárolását tér ill. frekvencia tartományban is megfelelően lehet kódolni.

Az adatfelvitel (enrollment) során is könnyen előfordulhat, hogy nem a célterületről készül kép vagy erősen torzult a retina képe, ezért itt szűrést, majd

több mintahalmaz átlagolását kell elvégezni. Mindez azt jelenti, hogy csak jól korreláló (0,75-0,8 korrelációs együtthatók) képeket használhatunk fel az átlagolás során.

A felismerés során a rögzített mintát összevetjük a korábban tárolt mintákkal, ami két lépésből áll:

1. Fázis korrekció: A vizsgált személyek a fejüket (az optikai tengely körül) az egyes mérések során elfordíthatják, ezért szükséges a megfelelő pozíció normalizálása. A korrekció során a rögzített adatokat a különböző lehetséges elforgatásoknak megfelelően transzformálják, és a maximális korrelációt adó elforgatást fogadják el.
2. Mintaegyezés vizsgálata: A diszkretizált mintákat tároló vektor és a tárolt template hosszát egységesre kell alakítani. Az értékeket is normalizálni szükséges. Ezek után korrelációt kell számítani, ahol -1 jelenti a lehetséges legkevésbé korreláló és +1 az elvileg legjobban korreláló jeleket. Esetünkben kb. 0,7-es korrelációs érték már egyezést jelent, természetesen felismerés során a legjobb egyezést (legerősebb korrelációt) választjuk, mint azonosított mintát.

A mérési eredményeket több tényező is torzíthatja: nem megfelelő pupillaméret, rossz szentávolság, rossz fixáció, szennyezett kamera lencse, szemüveg torzító/tükröződő hatása, zavaró külső fény. Utóbbi kétszeresen is gondot okozhat: egyrészt erős fény esetén lecsökken a pupilla mérete nagy veszteséget okozva a retinára eső fényben, másrészt ez a külső fény közvetlenül a kamerába is bevilágíthat és elronthatja a retináról alkotott képet.

Az itt tömören felvázolt módszerre jellemző, hogy a Sandia National Laboratory tesztjei szerint a vizsgált ún. EyeDentify rendszer egyszer sem produkált hibás elfogadást, míg 1%-os valószínűséggel fordult elő, hogy három próbálkozás után is hibásan utasított el mintát [94]. A retina alapú azonosítás előnyeit és hátrányait a 9.1 táblázat foglalja össze.

## 9.4. Eszközök

Az orvosi alkalmazásokban ún. szemtükör (ophthalmoscope) készülékeket használnak a szemfenék optikai vizsgálatához. A készülék célja, hogy megvilágítsa a szem belsejét és lehetővé tegye a megvilágított részek vizsgálatát.<sup>1</sup> A szemtüköröknek alapvetően két fajtája ismert:

- A direkt szemtükör körülbelül egy kisebb zseblámpa méretű készülék, amely több lencse segítségével kb. 15-szörös nagyítást tud elérni. A rutin szemészeti vizsgálatoknál általában ilyen készüléket használnak, a szemhez

<sup>1</sup>Hermann Ludwig Ferdinand von Helmholtz (1821. augusztus 31. - 1894. szeptember 8.) német orvos és fizikus találta föl az 1850-es évek elején, és ezáltal a modern szemészet egyik megalapítója lett.

9.1. táblázat. A retina alapú azonosítás előnyei és hátrányai

| Előnyök                                                                                                                                                                                                                                                                                                                                  | Hátrányok                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• alacsony döntési hibaarány</li> <li>• ikrek esetén is eltérő mintázat</li> <li>• gyors feldolgozás</li> <li>• nehezen hamisítható (szemben az íriszszel)</li> <li>• a minta nehezen szennyeződik, védett helyen van</li> <li>• nem változik az időben (kivéve néhány szembetegséget)</li> </ul> | <ul style="list-style-type: none"> <li>• szürkehályog és súlyos optikai hiba (pl. asztigmatizmus) csökkentheti a pontosságot</li> <li>• sokan invazívnak tekintik és félnek egészségügyi káros mellékhatásoktól</li> <li>• közel kell lenni a szkennnerhez, nem túl felhasználóbarát</li> <li>• szemüveg problémát jelenthet</li> <li>• drága készülékek</li> </ul> |

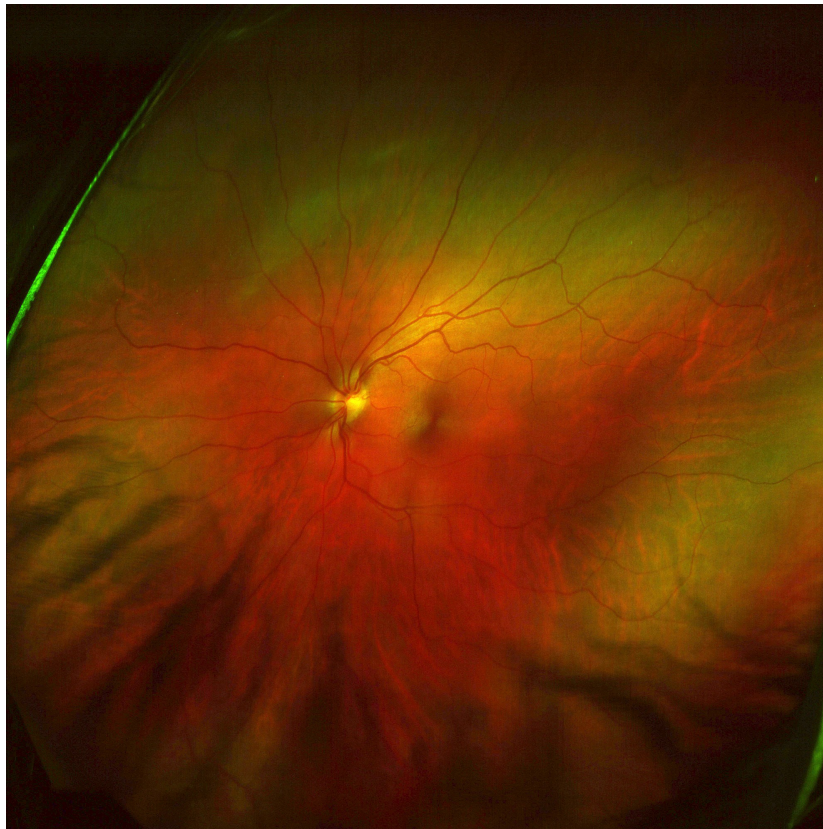
közel kell helyezni, és viszonylag kicsi látómezővel, egyenes állású képpel rendelkezik.

- Az indirekt szemtükör fordított állású képet alkot, nagyobb látómezővel és kisebb nagyítással. A periférikus részek vizsgálatára is alkalmas, a páciensről távolabb tartva, ill. szürkehályog esetén is használható.

A világos kép érdekében kitágult pupillánál érdemes a készülékeket használni. Az orvosi gyakorlatban ebből a célból pupillatágítót alkalmaznak (pl. tropikamidot), amely kb. 20-25 percig maximális pupillatágulatot hoz létre, hatása 4-5 óra múlva teljesen megszűnik. Az újabban, lézerrel működő berendezések nem igénylik a pupilla tágítását, akár 2 mm-es résen keresztül is jó képet adnak. Az ún. Scanning Laser Ophthalmoscope a konfokális lézer mikroszkóp elvének megfelelően készít a retináról képet (lásd 9.2. ábra). Ezekkel a készülékekkel a retináról nagyfelbontású, mikroszkópikus, valós idejű képalkotás is lehetséges [15].

A funduskamerák az indirekt szemtükör továbbfejlesztésének tekinthetők, 30-140 fokig képesek a retinát lefényképezni. Fő előnyük, hogy mivel a megvilágítás és az érzékelés külön optikai úton történik, ezért minimális nem kívánt reflexiók lépnek fel. A funduskamerák viszonylag bonyolultak, kevés gyártó foglalkozik előállításukkal, drágák, és szakszemélyzet szükséges a megfelelő beállításukhoz, használatukhoz.

A szemfenék képének előállításához az eszközök eleinte a látható tartományban



9.2. ábra. Optomap szkennelvel Doctor Martin Lindower által készített kép - Michael Judge Brislin tulajdona

működtek, de az olcsó CCD/CMOS kamerák jól érzékelnek a közeli infra tartományban is. A szükséges nagy fényerő miatt a látható tartományban működő készülékek használata a felhasználók számára kellemetlennek bizonyulhat, ez a probléma a közeli infra tartomány esetén elkerülhető, mivel az emberi szem nem érzékel ebben a sávban.

Az első jól működő azonosításra készült prototípus eszközt 1981-ben kezdték el tesztelni az USA-ban, infra megvilágítást használt, az adatok elemzésére pedig személyi számítógépet. Az ezzel szerzett tapasztalatok alapján 4 évvel később került gyártásba az EyeDentify Inc. cég EyeDentification Rendszer 7.5-ös verziója, ami már megbízhatóan képes volt ellenőrzésre és felismerésre (azonosításra) is. A készülék körkörösén szkennelte a retinát, 256 12 bites logaritmusos mintát dolgozott fel és alakított át 40 byte-os leírókká mindkét szem esetén. Alapvetően a frekvencia térben kódolta az információt, de azért, hogy a felismerés gyorsan működjön, külön tárolt 32 byte-ot szemenként a tér tartományban.





9.3. ábra. Bal oldal: Az EyeDentify Biometric Retinal Identification Scanner (EyeDentification System 7.5) Jobb oldal: Az amerikai hadsereg egy katonája retina azonosítást végez Afganisztánban (kép forrása: defenseimagery.mil). A készülékhez közel kell hajolni, ez alapvető hátrány az írisz szkennerekhez képest.

## 9.5. A retina diagnosztikai felhasználása

Röviden megemlíjtjük, hogy a retináról alkotott kép többféle betegséggel kapcsolatos diagnózis felállításában játszhat szerepet. A teljesség igénye nélkül néhány olyan betegség (ill. egészségi állapot), amely a retina vizsgálatának segítségével diagnosztizálható:

- időskori sárgafolt-degeneráció;
- cukorbetegség okozta retinasérülés;
- glaucoma (zöldhályog);
- retinaleválás;
- melanoma;
- ocularis hipertenzió (lehetséges okok: krónikus vesebetegségek, pajzsmirigy hibás működése, terhesség, alkoholizmus).



## 10. fejezet

# Írisz

Az írisz (latinosan Iris) a görög mitológiában a szivárvány istennője, az istenek hírnöke. Szárnyakat és tarka ruhákat viselt, kezében hírnöki pálcát és korsót tartott. Az emberi szem szivárványhártyáját szintén írisznek nevezik. Ez valójában egy lapos, lemezszerű réteges szerkezet, melynek kerek nyílású fényrekesz funkciója van: a nyílás méretének szabályozásával több vagy kevesebb fényt enged a szembe. Az írisz által meghatározott nyílás átlagos átmérője kb. 4 milliméter, magának a nyílásnak a neve szembogár vagy pupilla. A fényképezőgépek által alkalmazott lamella rendszerek is hasonlóak működésükben és funkciójukban.

### 10.1. Történeti háttér

Az írisz alapú azonosítás alapötletét 1936-ban Frank Burch vetette fel, de ennek dokumentálása meglehetősen szegényes, az irodalmi források James Doggart szemészeti tankönyvére hivatkoznak [34] igazolásul. Az első jelentősebb témával kapcsolatos szabadalmi bejelentés Leonard Flomtól és Aran Safirtól, két szemész professzortól származik 1987-ből "Iris Recognition Technology" címen [40]. Az egyik legelterjedtebb jelfeldolgozási módszer kidolgozása John Daugman nevéhez fűződik, akinek az algoritmus 1994-ben kapott szabadalmat, az íriszfelismeréssel kapcsolatos első publikációkat is Daugman írta [28].

A technika egyik híres alkalmazása szintén az ő munkájának eredménye [31]. Az "Afgán lány" egy híres portré kép a National Geographic 1985. júniusi kiadásának borítóján. A fénykép 1984-ben készült egy pakisztáni menekülttáborban egy 12 éves lányról - a kép annyira elragadó volt, hogy az újság címlapjára került. 2002-ben a National Geographic Television munkatársai a kép készítőjével felkerekedtek, hogy megkeressék a lányt, hogy megtudják, hogyan alakult a sorsa az eltelt 17 év alatt. Mivel a nevét sem tudták, a helyiek a fénykép alapján próbálták azonosítani, először sikertelenül. Később Afganisztánban találták meg (Sharbat Gula néven), az azonosítása során felhasználták a nagyfelbontású képet a szeméről, azaz annak írisz mintázatát. A Daugmann-féle ún. IrisCode

összehasonlítása során a bal szemre 0,24, a jobb szemre 0,31 Hamming távolság adódott. Ez azt jelenti, hogy a jobb szem esetén 1 a 6 millióhoz az esélye a véletlen egyezésnek, a bal szem esetén ez a szám 1 a  $10^{15}$ -hez.



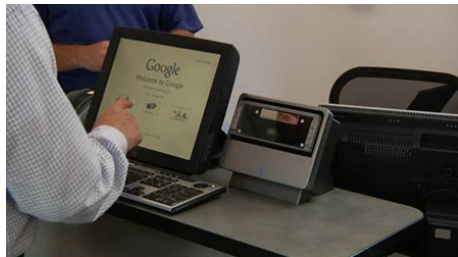
10.1. ábra. Az afgán lányról 1984-ben és 2002-ben készült képek (Steve McCurry felvételei)

A módszer ma már a legelterjedtebb biometria megoldások közé tartozik, és piaci szereplése igen nagy növekedésnek néz elébe a 2010-es években [48], ami több mint évi 25%-os piaci bővülést jelent. Ennek egyik fő oka talán az, hogy az ujjlenyomathoz hasonló megbízhatóságra képes, azonban nincs szükség közvetlen kontaktusra a szenzor és a személy között, így az ellenőrzés igen gyorsan megtörténhet, akár nagyobb távolságból is (néhány méterről). Az SRI International Sarnoff 2013-ban mutatta be "Move PassThru" elnevezésű ellenőrző rendszerét, amellyel akár percenként 10 gépkocsivezető azonosítását is el tudják végezni anélkül, hogy a sofőrnek ki kéne szállnia a gépjárműből [98].

## 10.2. Az írisz struktúrája

A szivárványhártya az ínhártyára tapad, alapját egy finom kötőszövetes állomány képezi, amelyben a pupilla szűkítéséért és tágításáért felelős izmok találhatók. A szivárványhártya külső felszíne egyénre jellemző redőzöttséget mutat. Színét - örökletes módon - a benne található festékanyagot (pigmentet) tartalmazó sejtek száma, pigment tartalma és elrendeződése határozza meg. A szivárványhártya szerkezetének rétegződése a következő:

- a hátsó rétege csak kettő sejtnyi vastagságú (epithelialis sejtek), de az ott található festékanyagok miatt ez a rész nem áttetsző;



10.2. ábra. A Google adatközpontjai is használnak írisz azonosítást a fokozott fizikai biztonság érdekében (kép forrása: <http://irisid.com>)

- e felett található egy izomréteg, ami a pupilla nyitását vagy zárását végzi;
- izmok feletti kötőszöveti réteg, amely kollagén (zselészerű), boltív formájú alakzatokat alkot, ill. erezetet tartalmaz sugárirányban;
- az elülső rétegben sok festékanyagot tartalmazó sejtek találhatók.

Valójában az elülső három réteg látható jól, a hagyományos vagy a közeli infra tartományban érzékelő kamerák által alkotott képet lehet használni a biometria alkalmazásokban.

Az írisz mintázatának kialakulása a fogantatás után kb. 8 hónappal fejeződik be, bár annak a színe kb. a csecsemő 1 éves koráig megváltozhat. Az írisz komplex textúrája valójában fenotípusos tulajdonság (lásd a 2.4 fejezet), ennél fogva ikrek esetén is jól használható a személyek megkülönböztetésére. Az írisz mintázata rendkívül gazdag információban, a British Telecom Research Laboratories több mint 200000 mintán végzett elemzése szerint négyzetmilliméterenként 3,4 bit információt tartalmaz [29].

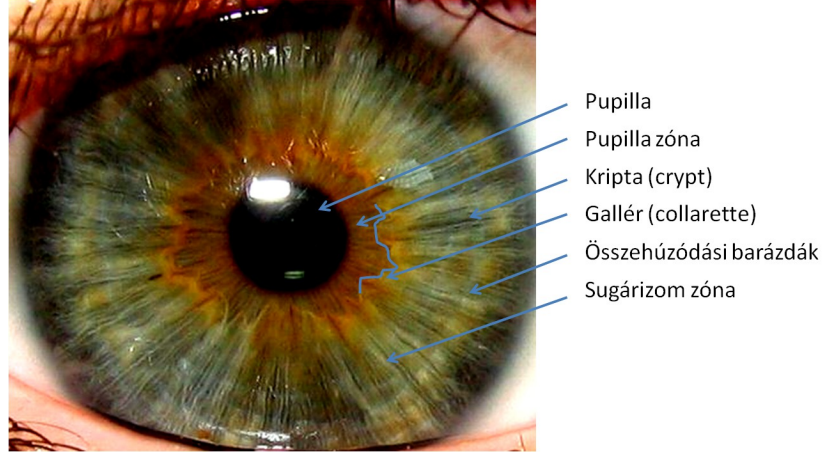
### 10.3. Az írisz mintázatának felismerése

A szakirodalomban igen sokféle módszert találhatunk az írisz detekciójára és mintázatának jellemzésére. A teljesség igénye nélkül csupán néhány ismertebb megközelítést, ill. cikket sorolunk itt fel: textúra elemzés [71], fraktál dimenzió [113], wavelet transzformáció [30], lokális intenzitás változás [72], diszkrét koszinusz transzformáció [80].

Részletesebben a Daugman féle ún. wavelet alapú megközelítést mutatjuk be, ez volt az egyik első olyan módszer, amely a gyakorlati életben is jól bizonyított és viszonylag elterjedtnek mondható [30]. A következő ábra az algoritmus képtranzformációs lépéseit tekinti át.

#### 10.3.1. A kép rögzítése

Mint ahogy az afganisztáni lány példájából is láttuk, az íriszről a látható tartományban készített képek is alkalmasak a személyazonosításra, ennek ellenére a



10.3. ábra. Az írisz részei (Matthew Goldthwaite képe alapján, licenz: GFDL)

kereskedelemben kapható azonosító rendszerek a közeli infra tartományban működnek (NIR - Near Infra Red). Ez az elektromágneses spektrum kb. 700-900 nm-es tartományát jelenti, a kép készítéséhez segédfényt használnak. A NIR tartományban való képrögzítésnek több előnye is van:

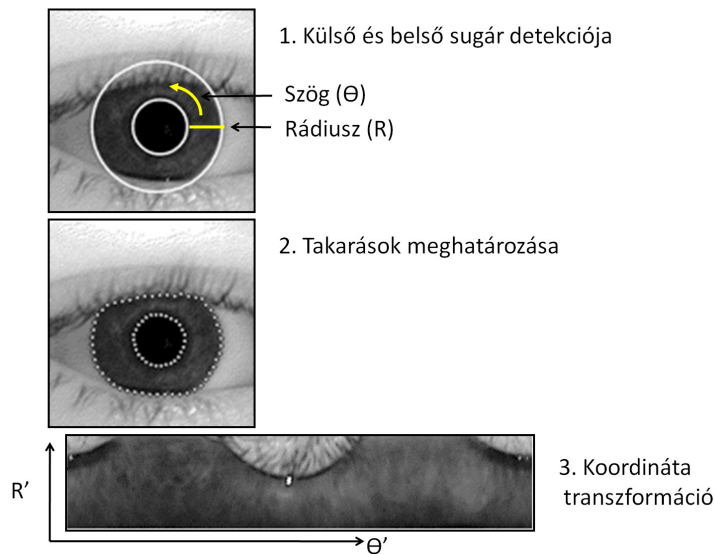
- a környezeti fénynek a tükröződése a szemén jóval kevésbé okoz problémát,
- a legtöbb embernek sötétbarna szeme van, amelynek a struktúrája jobban látszik ebben a tartományban.

### 10.3.2. Szegmentálás - az írisz lokalizálása

Az első lépés az írisz megkeresése a képen. Feltételezzük, hogy a személy a kamerába néz, és megfelelő nagyítás esetén a szem egésze a képen látható, ugyanakkor a kép kiterjedése nem nagyobb a szem kb. kétszeresénél. Ilyenkor az írisz lokalizálása már lehetséges annak belső és külső kontúrjának megkeresésével. Ennek egyik módja egy célfüggvény maximalizálása a következő módon:

$$\arg_{r, x_0, y_0} \max \left| G_\delta(r) * \frac{\partial}{\partial r} \oint_{r, x_0, y_0} \frac{I(x, y)}{2r\pi} ds \right|, \quad (10.1)$$

ahol  $I(x, y)$  maga a kép,  $r$  a lehetséges sugara az írisz kontúrjának,  $x_0$  és  $y_0$  jelenti a középpontot,  $G_\delta$  pedig egy simító függvény ( $\delta$ -val jellemezhető Gauss konvolúciós kernel), ami a maximalizálandó célfüggvény simaságát segíti elő. A függvény 2 legnagyobb helyének megkeresésével tehát azt a két középpontot és két sugarat találhatjuk meg, ahol a körív mentén, a vonal menti integrál sugár szerinti változása a legnagyobb. A  $2r\pi$  a kör kerülete szerinti normalizációért felelős.



10.4. ábra. Az IrisCode generálásának első lépései, a koordináta transzformáció egyben a normalizálás célját is szolgálja

Problémát okozhat a szemhéj és a szempillák takarása az íriszen. Ezek eliminálása sem különösebben nehéz feladat, hiszen színükben eltérnek az írisztől, tehát akár egy viszonylag egyszerű, szín alapú szegmentálás által is lehet egy olyan maszkot generálni, ahol az érintett területek vannak jelölve. Hasonlóan a tükröződő részek eliminációja is elvégezhető.

### 10.3.3. Kép transzformációja és normalizálása

Az írisz képe valójában egy gyűrű alakú képi objektum egy külső és egy belső körív által határolva. Megjegyezzük, hogy a két kör középpontja nem feltétlenül esik egybe, de az ebből adódó pontatlanságoktól most eltekintünk (valójában ez a probléma is megfelelően kezelhető a kép normalizálása során). A kép elemzését azonban hagyományos négyzet alakú képen végezzük, tehát szükség van egy polár-koordináta transzformációra (lásd 10.4. ábra). A transzformáció során olyan képet állítunk elő, amely fix mérettel rendelkezik, azaz egyben a képméret normalizálása is megtörténik.

### 10.3.4. Tulajdonságkinyerés és összehasonlítás

A tulajdonságkinyerés kimente egy ún. IrisCode lesz, ami egy bináris jelszekvencia. Két írisz összehasonlítása pedig a bináris mintázatok egyszerű gyors összevetésén alapul Hamming távolság kiszámításával. A 256 byte-os bináris

kód generálása komplex 2D-s Gabor waveletek segítségével történik:

$$h_{\{Re, Im\}} = sgn_{\{Re, Im\}} \int_{\rho} \int_{\phi} I(\rho, \phi) e^{-i\omega(\theta_0 - \phi)} e^{-(r_0 - \rho)^2 / \alpha^2} e^{-(\theta_0 - \phi)^2 / \beta^2} d\rho d\phi, \quad (10.2)$$

ahol  $I(\rho, \phi)$  az írisz képe polár-koordináta rendszerben (a lokalizálás és normalizálás miatt eltolás- és skálafüggetlenül),  $\alpha$  és  $\beta$  2D-s wavelet méret paraméterek,  $\omega$  a wavelet frekvencia,  $r_0$  és  $\theta_0$  a pozíciók, amikre  $h$ -t kiszámoljuk.  $h$  valójában egy komplex, bináris értékű függvény, aminek az értékeinek a sorozata jelenti az IrisCode-ot. A komplex kettős integrál értékét (amplitúdóját) valójában nem használjuk fel, csupán a fázisát binárisan kódolva (erre szolgál az  $sgn$  előjel függvény), így az intenzitás változásokra nem lesz a módszer különösebben érzékeny. Másik előnye, hogy ha a fázisban hiba történik, akkor jó eséllyel csak az egyik bit változik meg (a valós vagy képzetes rész), ahhoz ellentétes fázisba kell, hogy kerüljön az integrál, hogy a kód teljesen megváltozzon (a valós és a képzetes bit is).

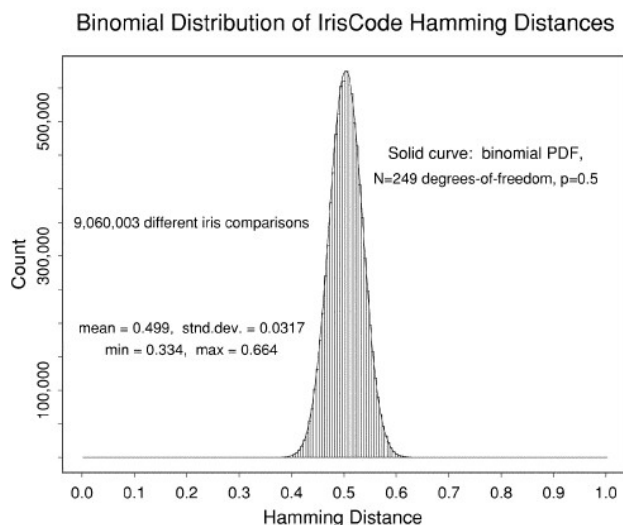
A módszert később kibővítették egy maszkkal, ami az eltakart területeket binárisan reprezentálja, ezeket így ki lehet hagyni az összehasonlításból. Az ennek megfelelően módosított Hamming távolság a következőképpen alakul:

$$HD = \frac{\|IrisCode_{Query} \oplus IrisCode_{Candidate} \cap mask_{Query} \cap mask_{Candidate}\|}{\|mask_{Query} \cap mask_{Candidate}\|}, \quad (10.3)$$

ahol  $\oplus$  a kizáró VAGY,  $\cap$  az ÉS,  $\|\cdot\|$  pedig az 1-es biteket számláló operátor. Azaz a két összehasonlítandó IrisCode csak azon biteinek vesszük a Hamming távolságát, ahol egyik maszk sem jelöl eltakart területet. Bár magának a kódnak a kiszámítása nem túl gyors művelet, de íriszenként csak egyszer kell elvégezni. Ezzel szemben az összehasonlítás - amit nagyobb adatbázisok esetén sok milliószor kell megtenni - igen gyors bináris művelet.

Alapvető kérdésként merül fel az IrisCode osztályon belüli és osztályok közötti változatossága. Erről adnak némi információt a 10.5 és 10.6 ábrák. A kódok távolságának az eloszlása a binomiális mintát követi. Az első esetben közel 9,1 millió összevetés alapján az átlag 0,499-nek, a szórás 0,0317-nek adódott. Tehát a bináris kód kb. 50%-os valószínűséggel egyezik, azaz szinte teljesen véletlenszerű az egyezés a két minta között. Szemléltetésképpen: Az eloszlás megfelel egy olyan pénzfeldobási kísérletnek, ahol egymás után 249 fejet dobtunk ( $p=0$ ,  $N=249$ ). A következő ábra már jóval kevesebb összehasonlítás során született: 648 egyetű ikerhez tartozó szem alapján készült. Mégis, a két eloszlás szinte teljesen azonos. Összehasonlításul: abban az esetben, ha változó fényviszonyok és távolság mellett azonos íriszekről készültek statisztikák, az átlag 0,110-nek, a szórás 0,065-nek adódott. A módszer az egyenlő hibaarányt ( $HD=0,342$  küszöbnél) 1:1200000 döntési hibánál éri el.





10.5. ábra. A Hamming távolság eloszlása 9,1 millió írisz összehasonlítása alapján. A kép forrása: <http://www.cl.cam.ac.uk/~jgd1000/binomdata.html>

## 10.4. Lehetséges problémák

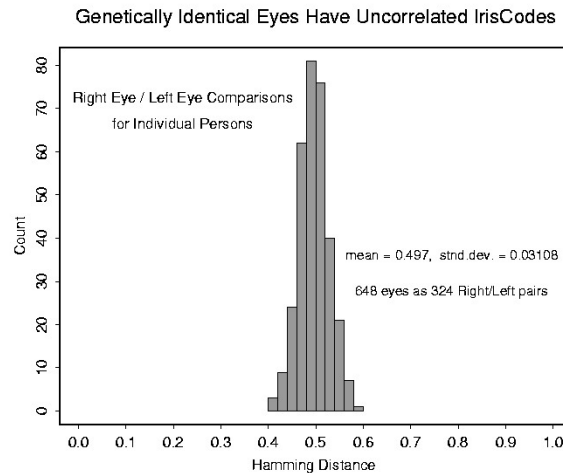
Bár az írisz alapú felismerés az egyik legnagyobb biztonsággal (legkisebb hibarárányal) működő biometria módszer, mégis előfordulhatnak esetek, amikor bizonytalanná válik a működése. Az egyik problémát az alkohol fogyasztása okozhatja: ebben az esetben a pupilla erős kitágulása vagy szűkülése torzíthatja a mintázatot oly mértékben, ami ronthatja a különböző algoritmusok hatékonyságát [4].

[91] arról számol be, hogy modern szürkehályog műtétek során bizonyos mértékben megváltozhat az írisz mintázata, és ez érzékelhetően befolyásolja a műtét utáni - a korábbi minták alapján működő - biometria azonosítást, azaz jelentősen növeli a hibás elutasítások valószínűségét. A 10.7 ábra műtét előtti és műtét utáni íriszképet mutat a látható és infra tartományban.

A módszer feltételezi, hogy a szemről megfelelő felbontású kép áll rendelkezésre, ezért viszonylag közelről alkalmazható és a személyek megfelelő viselkedését igényli, túl alacsony vagy túl magas embereknel, ill. szemüveg használatánál előfordulhatnak azonosítási problémák.

A hamisítás egyik legegyszerűbb módja nyomtatott írisz kép használata (ter-

<sup>1</sup>CopyRight: 2004 Roizenblatt et al; license BioMed Central Ltd. This is an Open Access article: verbatim copying and redistribution of this article are permitted in all media for any purpose, provided this notice is preserved along with the article's original URL:<http://www.biomedical-engineering-online.com/content/3/1/2>



10.6. ábra. A Hamming távolság egypetűjű ikrek IrisCode-ja esetén. A kép forrása: <http://www.cl.cam.ac.uk/~jgd1000/genetics.html>

mérszentesen csak akkor, ha nem személyzet működteti az azonosító rendszert, lásd [92]). Ez ellen többféle ellenőrzési módszerrel is lehet védekezni:

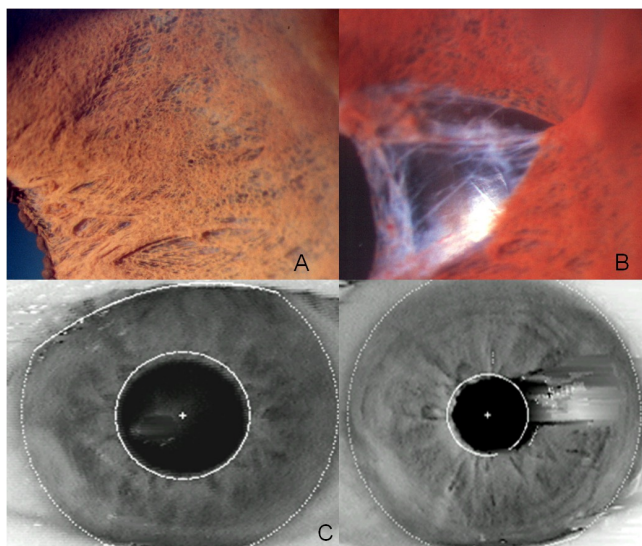
- A "vörös szem" effektus észlelhető-e?
- Fény hatására a pupilla összehúzódik-e?
- A szem apró rezgésének, ill. a pupilla akaratlan véletlenszerű mozgásának (tágulások-összehúzódások, hippus) meglétének vizsgálata.
- 3D-s leképezéssel a szem alakjának vizsgálata.

Ezekkel a megoldásokkal kizárható a 2D-s nyomtatott hamisítvány használata.

Korábban, a 2.5 fejezetben röviden ismertettük a [46] cikk észrevételeit, miszerint bizonyos esetekben az IrisCode-ból vissza lehet állítani azonosításra alkalmas írisz mintázatokat.

## 10.5. Az írisz diagnosztikai alkalmazásáról

Fontos megemlíteni az ún. íriszdiagnosztikát (más néven iridiológiát) amely olyan, az alternatív gyógyászat körébe tartozó diagnosztikai módszer, amely az írisz, az ínhártya és a szem egyéb jellegzetességei alapján ad információt a páciens egészségi állapotáról, ill. egyes betegségekre való hajlamairól (természetesen



10.7. ábra. Szürkehályog műtét során sérülhet az írisz mintázata. Bal oldal: műtét előtt. Jobb oldal: műtét után. Első sor: színes kép. Második sor: közeli infra fénykép. <sup>1</sup>

nem értjük ide a retina korábban említett diagnosztizálását). A módszer szerint a megfigyeléseket úgynevezett írisztérképekkel vetik össze, melyek a szivárványhártyát az egyes testrészeknek és szerveknek megfelelő területre osztják.

Az íriszdiagnosztikát a modern tudomány nem ismeri el, mint megalapozott módszert, és inkább veszélyesnek tartja alkalmazását (szemben a retina alapú diagnosztikával). Edzard Ernst 2000-ben 77 íriszdiagnosztikával foglalkozó cikket vizsgált meg [38]. Legfontosabb megállapítása az volt, hogy azok a cikkek találták jó diagnosztikai eszköznek az íriszdiagnosztikát, amelyek nem használtak kontrollcsoportot és nem alkalmaztak kettős vak-próbákat. Az általa vizsgált, négy kontrollált, kettős vak módszertannal dolgozó kutatás közül egyik sem találta hasznavehetőnek az iridiológiát. Természetesen mindez nem jelenti azt, hogy bizonyos betegségek esetén nem jelentkeznének törvényszerűen jelek a szem különböző részein. Például a szivárványhártya részleges vagy teljes hiánya (aniridia) gyakran együtt jár az ún. Wilms-tumorról (ami egy gyermekkorban előforduló daganat). 1964-ben fedezték fel, hogy egy a szivárványhártyáért és egy másik ezért a betegségért felelős gén a 11-es kromoszóma karján egymáshoz közel helyezkednek el. Így érthető, hogy sérülésük gyakran egyszerre történik.



## 11. fejezet

# Egyéb módszerek

Könyvünk a vizuális szenzorokkal működő biometria módszerekkel foglalkozik, így természetesen nem kerül sor sokféle módszerre, mint pl. a DNS, a beszédhang, az illatanyag, az egér vagy szoftverhasználat, EKG jelek, GPS koordináták, gépjárművezetés, internet használat, és más kognitív "ujjlenyomat" alapú megközelítések. Szintén nem kerül sor néhány speciális képalkotási technikára sem, mint az infra, a terahertz vagy a 3D-s kamerák alkalmazása.

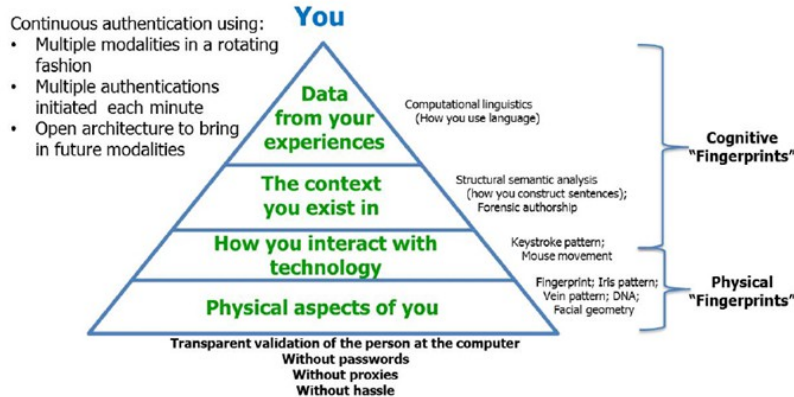
Az eddig tárgyaltakon kívül számos egyéb, többé-kevésbé sikeresen felhasználható vizuális biometria módszer létezik. Ezek alkalmazása - egy kivétellel - jelenleg általában meglehetősen korlátozott, az eddig ismertetteken túl a kézírás tekinthető elterjedt módszernek. Ebben a fejezetben röviden bemutatjuk a kézírás és a gépelés mintázatán alapuló személyazonosítás alapjait. Nem kerülnek bemutatásra a következő vizuális megközelítések: ajak felismerés, arcjegyek elemzése, bőr spektroszkópia, fogászati módszerek [62], a járás, a köröm, a szem körüli területek (periocular) vizsgálata és a tetoválások.

Szintén nem foglalkozunk adatfúzióval, amikor is több módszer adatainak vagy osztályozási eredményeinek az együttes feldolgozásával növelhető a megbízhatóság. Ennek az iránynak a jövőbeli alkalmazása egyre valószínűbb, hiszen az olcsó szenzorok és az egyre aktívabb szoftverhasználat megteremti a szükséges feltételeket. A 11.1. ábra az amerikai DARPA (Defense Advanced Research Projects Agency) egyik 2012-ben induló projektjének fő filozófiai elgondolását foglalja össze. Ezek szerint a számítógép felhasználók személyének ellenőrzése gyakorlatilag egy folyamatos monitorozást jelent, ami figyelembe veszi a fizikai adottságokat, a viselkedést, a kontextust és a felhasználók kifejezéseit (pl. nyelvi megnyilvánulásokat) [27].

Az olvasót - érdeklődésének megfelelően - a megadott hivatkozások segíthetik ezen területek feltárásában.

### Solution: **Active Authentication**

An open solution that provides **meaningful** and **continual** authentication to DoD's computer systems leveraging that which makes up **you**



11.1. ábra. Az amerikai Fejlett Védelmi Kutatási Projektek Ügynökségének (Defense Advanced Research Projects Agency - DARPA) elképzelése a biometria jövőjéről: az aktív autentikáció [27]

## 11.1. Aláírás

Az aláírás mintázata (csak úgy, mint a gépelése) az egyénre jellemző egyedi sajátosság és a viselkedés alapú biometria kategóriájába tartozik. A kézírás egyediségét számos cikk tárgyalja [53], [57]. A kézzel írott szöveg feldolgozásának több célja is lehet: a szöveg felismerése (az OCR egy speciális változata), ill. az író felismerése hosszabb szöveg vagy az aláírás alapján.

Az aláírás, mint hitelesítő eszköz már több ezer éve ismert, Rómában már i.sz. 400 környékén törvénybe iktatták használatát egyes dokumentumok hitelének igazolására. A kézírás gépi felismerése már több mint száz éve foglalkoztatja a kutatókat, az első szabadalom 1914-ben jelent meg a témában, igaz az csak számok felismerése vonatkozott [49]. (A gépi kézírás felismerés kezdetét általában 1938-tól, Hansel szabadalmától datálják - erre a szerző nem talált közvetlen utalást). Az első on-line kézírás felismerésről szóló cikk T. L. Dimondtól jelent meg [32]: a Stylator nevű eszköz Descartes koordináta rendszerben volt képes a kézírás felismerésére. Napjainkban az online kézírásfelismerés gyakorlatilag megoldottnak tekinthető [86], azonban az offline kézírás felismerés és az aláírás hitelesítés offline módja még jelentős hibákkal bír. Az első automatikus aláírás ellenőrző rendszert 1965-ben a North American Aviation fejlesztette ki [76]. A Veripen Inc. vállalat 1977-es szabadalma által leírt módszer a kézírás során mért nyomásértékeket is felhasználja, az ezen alapuló technológiát kezdte el használni

nem sokkal később az Egyesült Államok légereje is.

Az aláírás hitelesítés módozatait két nagy csoportra lehet osztani: online és offline. Az online felismerés során az aláírást folyamatában rögzítjük, ez vonatkozhat a toll hegyének pozíciójára, a toll nyomására, dőlésszögére és az ezekből számolt egyéb paraméterekre. Ezzel szemben az offline felismerés csupán a leírt szöveget, mint képet dolgozza fel. Mindezekből adódik, hogy napjaink legjobb offline rendszerei elmaradnak az online módszerek eredményeitől, minimum 8-10%-os hibával működnek (ami természetesen nagyban függ attól is, milyen képességű hamisítóval van dolgunk).

A különböző módszerek összehasonlítására több nemzetközi versenyt is szerveztek, mint pl. a 2004-es Signature Verification Contest-et (SVC2004) [100] vagy a 2009-es International Conference on Document Analysis and Recognition (ICDAR2009) konferencia felismerési versenyét. Az előbbin a legjobb algoritmusnak kb. 3% volt az egyenlő hibaaránya (EER) online felismerés esetén, míg a második említett versenyen ez a hiba online esetben szintén kb. 3%-nak, offline esetben azonban kb. 9%-nak adódott.

A 11.1. táblázat a kézírás alapú hitelesítés előnyeit és hátrányait veszi számba.

### A kézírás feldolgozása

A célra igen sokféle megközelítés létezik, pl. Fourier tartományú módszerek, Rejtett Markov Modellek (Hidden Markov Models - HMM), dinamikus idővetémités (Dynamic Time Warping - DTW) alapú, csak idő és pozíció, vagy a toll szögét és a nyomás erősségét is feldolgozó, ill. külső kamera képét felhasználó eljárások. A következőkben az online időbeli feldolgozás főbb lehetséges lépéseit tekintjük át (tárgyalásunk alapját a [61] cikk adja). Megjegyezzük, hogy az offline módszerek is hasonló elveket követnek, természetesen az időbeliségről akkor nincsen információ.

**Előfeldolgozás:** Az előfeldolgozás célja az esetleges zajok kiszűrése, ill. az adatok normalizálása. Előbbi adódhat az eszköz működéséből, a sebesség ingadozásából és az írás bizonytalanságából is. A normalizálás érintheti a szó méretét és méretarányait, a szó pozícióját. Az időben egyenletesen mintavételezett jelet a síkon újrámintavételezik és simítják, így egy kevésbé zajmentes képet kapunk, megfelelő arányokkal. Ilyenkor természetesen az időbeli jellemzők torzulnak, így azok kivonatolását, tárolását korábban kell megtenni. Szintén elmentésre kerülnek a fontosabb jellemző pontok adatai, mint a vonalak kezdő- és végpontjainak koordinátái, és a vonalhúzások száma, mint globális paraméter. Mivel az aláírás egyes különálló darabjait előfeldolgozás során összekötik, így ennek a lépésnek a végén egy összefüggő sztring (ill. vektor) áll elő az x,y koordinátákkal.

**Tulajdonság kinyerés:** Az aláírás képének lokális tulajdonságait két cso-

11.1. táblázat. Az aláírás biometria használatának előnyei és hátrányai

| Előnyök                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Hátrányok                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Társadalmilag elfogadott, sok helyen jól bevált.</li> <li>• Hosszú távú felhasználási tapasztalatok a manuális vizsgálatok területéről.</li> <li>• Felhasználó barát, megszokást nem igényel.</li> <li>• Nem invazív, egészségügyi ártalomtól nem kell tartani.</li> <li>• Offline módban nincs különösebb hardver igénye.</li> <li>• Online módban olcsó, meglévő eszközök is használhatók (pl. tablet).</li> <li>• Le lehet cserélni, azaz az aláírást meg lehet változtatni szükség esetén.</li> </ul> | <ul style="list-style-type: none"> <li>• Egy személy aláírása igen nagy változatosságot mutathat, akár az érzelmi vagy fizikai állapotának függvényében.</li> <li>• Viszonylag könnyen hamisítható.</li> <li>• Offline esetben nagy hibaarány.</li> <li>• Fizikai kontaktust igényel.</li> <li>• Nem túl gyors.</li> </ul> |



portra lehet osztani: mint térbeli, és mint időbeli adatok. Az előbbi csoportba tartozók alapvetően az alakra vonatkoznak, mint pl.:

- az egymást követő pontok  $x, y$  koordinátáinak különbsége,
- az  $y$  koordináta értéke a tömegközépponthoz képest,
- a vonalvezetés tengelyekkel bezárt szöge,
- a vonalvezetés görbülete,
- adott pont környékén a kép pixeleinek értéke.

Az időbeli adatokat az abszolút és az átlagsebesség segítségével normalizált relatív sebesség jelenti.

**Összehasonlítás:** A tulajdonságkinyerés után az egyes mintapontokban különböző adataink lesznek, ezeknek a rendezett sorozata tehát adatvektornak tekinthető. Két aláírás összevetése ezen vektorok távolságán alapul. Mivel az aláírások esetén nagyon gyakran fordul elő, hogy az alapvonal mentén a szöveg megnyúlik vagy tömörödik, így ennek kompenzációja célszerű. Megoldás az ún. idővetemítés (DTW - Dynamic Time Warping) alkalmazása, amely két vektor koordinátáinak oly összerendelését adja meg (bizonyos megszorítások mellett), amely esetén a két vektor leginkább hasonlónak bizonyul [74]. Két szó összehasonlítására [61] a következő függvényt használja:

$$Dissim(T, I) = \frac{Dist(T, I)}{NormFact(N_T, N_I)} + SP|S_T - S_I|, \quad (11.1)$$

ahol  $T$  és  $I$  a két összehasonlított szöveg leíró vektora,  $Dist(T, I)$  a kettő leíró távolsága,  $SP$  egy büntető konstans a különböző vonalszámokra,  $|S_T - S_I|$  a vonaldarabok számának különbsége,  $NormFact(N_T, N_I)$  két  $N_T$  és  $N_I$  hosszú szöveg maximális lehetséges távolsága. A fenti függvény eredményét küszöbölni kell, így lehet meghozni a döntést az azonosságról vagy különbözőségről. Ha globális döntési küszöböt alkalmazunk, akkor annak értékét úgy kell meghatározni, hogy egy adott tesztadatbázison a minimális döntési hibával járjon. Ha személyfüggő küszöböt használunk, akkor ennek meghatározására érdemes a közös teszten alapuló globális küszöbből kiindulni és minden felhasználó esetén olyan módon változtatni, hogy a döntési hiba csökkenjen.

Az olvasóban jogosan merül fel, hogyan lehet azonosítani az igen jó minőségű szkennelést és nyomtatóval előállított hamisított aláírások képét. Triviális megoldás, ha a lézer fénymásológépek/nyomtatók által kinyomtatott speciális miniatűr rejtett kódokat keresünk a képen. Ehhez természetesen igen nagyfelbontású szkennelés szükséges. Más módszerek szerint a tintasugaras és lézer eszközök esetén eltér a festék szóródásának a mintája a különböző tollaktól, ill. a papír benyomódása (ill. annak hiánya) is árulkodó lehet.

## 11.2. Gépelés

Bár jegyzetünk alapvetően a vizuális módszerekkel foglalkozik, és a gépelés jellemzői lényegileg nem értelmezhetők vizuális jelként biometria szempontból, nagyon röviden kitérünk a gépelés alapú felismerés alapelveire is.

A billentyűzet leütésének ritmusán alapuló azonosítás kezdete a 2. Világháborúig nyúlik vissza, amikor is a távíró operátorok felfedezték, hogy a jelek ritmusából fel lehet ismerni a küldő személyét. A számítógépek tömeges elterjedésével azonban magától értetődik ennek a technikának a használata, mivel külön eszközt nem igényel és könnyen implementálható. A biometria rendszerekben két esetet különböztetünk meg:

- Egyik esetben hosszabb szöveg gépelésének elemzését végezzük el, mint például egy elektronikus levél begépelése. Valójában egy felhasználó hosszabb időszak alatt vizsgált gépelése, billentyűzet használata folyamatos megfigyelést tesz lehetővé.
- Máskor egy rövid kifejezést, tipikusan csak egy jelszót vizsgálunk.

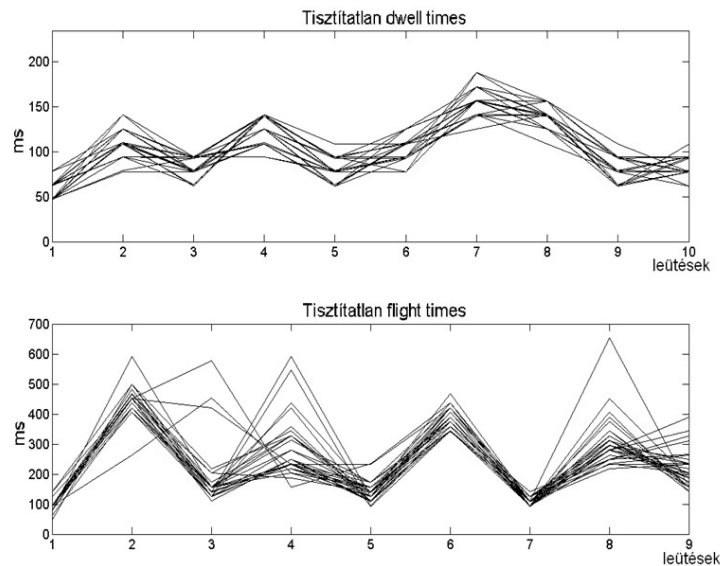
Mindkét esetben maga a vizsgálat a háttérben történhet, valójában a személyeknek nem is kell feltétlenül a tudatában lenniük az ellenőrzésnek (természetesen nem etikus, ha nem hívjuk fel erre a felhasználók figyelmét). A gépelés jellemzése a következő adatokkal lehetséges:

- két billentyűleütés közben eltelt idő (miután az egyik billentyűt felengedték és a másik le lett nyomva);
- billentyű nyomvatartásának ideje;
- az ujjak elhelyezkedése;
- nyomóerő;
- gépelési sebesség.

Bár ezek a jellemzők jól begyakorolt szöveg esetén igen jól jellemzik az adott személyt, változó körülmények között (pl. jelentősen eltérő testhelyzet, eltérő billentyűzet geometria) nagy szórást mutathatnak.

A személy felismerése alapvetően adott szóhoz tartozó tulajdonságvektorának összevetésén alapul. A tapasztalatok szerint használhatunk egyszerű metrikákat is, mint az euklideszi távolság vagy  $l_1$  norma.

Más megközelítések is léteznek két gépelési minta összehasonlítására, [7] ún. trigráfok időbeli sorrendiségén alapuló módszert ismertet. Kettő egymás után lenyomott billentyűt bigráfoknak, három egymás után lenyomott billentyűt trigráfoknak nevezünk. Egy bigráf vagy trigráf tartama alatt azt az időt értjük, ami az első elemének lenyomása és utolsó elemének felengedése között telik el. A trigráfokat (bigráfokat) ezek szerint növekvő sorrendbe lehet helyezni. Példának



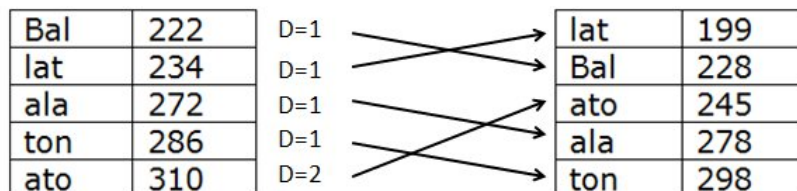
11.2. ábra. Egy felhasználó 10 betűs jelszavának begépelésének adatai. Első sor: nyomvatartási idő (dwell time), második sor: két leütés közti idő (flight time)

vegyük a "Balaton" jelsorozatot, ennek trigráfjai: bal, ala, lat, ato, ton. Két mintavétel eltérő adatokkal fog szolgálni, erre mutat példát a 11.3. ábra.

Két begévelt jelsorozat ( $T_1, T_2$ ) távolságát úgy kapjuk meg, hogy össze adjuk az egyes trigráfok pozíciójának esetleges átrendeződését ( $D_i$ ), majd elosztjuk a lehetséges legnagyobb távolsággal ( $D_{maxsum}$ ):

$$D(T_1, T_2) = D(T_2, T_1) = \frac{\sum_i (D_i)}{D_{maxsum}} = \frac{1 + 1 + 1 + 1 + 2}{12}. \quad (11.2)$$

Utóbbi módszert 154 személlyel és egy valamivel hosszabb, mint 600 karakteres szövegen tesztelve a hibás elutasítások aránya 4%-nak ("jogosult sikertelen belépése"), a hibás elfogadások aránya ("illetéktelen belépések") 0,01%-nak adódott. Ezek meglepően jó adatok figyelembe véve a technika egyszerűségét. Megjegyezzük, hogy 7 betűs jelszavak esetén 1:120 az esélye azonos sorrendiségnek, azaz ha valakinek a jelszavát tudjuk is, de gépelés ritmusát nem, ennyi az esélye, hogy sikerül a jelszával visszaélni. A módszer előnyeinek és hátrányainak összevetését a 11.2. táblázat tartalmazza.



11.3. ábra. A Balaton jelsorozat sorrendbe rakott trigráfjainak időtartama (ms) és a sorrendiség egyenkénti eltérései

11.2. táblázat. A gépelés alapú biometria előnyei és hátrányai

| Előnyök                                                                                                                                                                                                                                                                                                  | Hátrányok                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• könnyű felhasználói befogadás</li> <li>• természetes módszer számítógépes, ill. hálózati belépéseknél</li> <li>• folyamatos monitoringot tesz lehetővé</li> <li>• minimális betanulást igényel</li> <li>• nincs szükség speciális hardver eszközökre</li> </ul> | <ul style="list-style-type: none"> <li>• magas hibás elutasítási ráta</li> <li>• érzékeny a felhasználó fizikai kondíciójára és a billentyűzet geometriájára</li> <li>• korlátozott alkalmazhatóság (billentyűzetet igényel), fizikai kontaktust igényel</li> </ul> |

# Irodalomjegyzék

- [1] Alessandro Acquisti, Ralph Gross, Fred Stutzman Faces of Facebook: Privacy in the Age of Augmented Reality, <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/> meglátogatva: 2014. február 8.
- [2] A. H. M. Akkermans, T. A. M. Kevenaar, D. W. E. Schobben, Acoustic Ear Recognition for Person Identification, Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05) pp. 219-223
- [3] Alonso-Fernandez, Fernando, et al. "A comparative study of fingerprint image-quality estimation methods." Information Forensics and Security, IEEE Transactions on 2.4 (2007): 734-743.
- [4] Arora, S.S.; Vatsa, M.; Singh, R.; Jain, A. "Iris recognition under alcohol influence" (Conference Publications). 978-1-4673-0397-2. Biometrics (ICB), 2012 5th IAPR International Conference on. pp. 336-341
- [5] Ashbaugh, David (1999). Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. Boca Raton, Florida: CRC Press. pp. 15.
- [6] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman. Eigenfaces vs. fsher-faces: recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7):711-720, 1997.
- [7] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi, User Authentication through keystroke, ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002, Pages 367-397.
- [8] Besl, Paul J.; N.D. McKay (1992). "A Method for Registration of 3-D Shapes". IEEE Trans. on Pattern Analysis and Machine Intelligence, 14 (2): 239-256.
- [9] [http://www.biometrics.dod.mil/Newsletter/issues/2008/Oct/v4issue4\\_-pm.html](http://www.biometrics.dod.mil/Newsletter/issues/2008/Oct/v4issue4_-pm.html) meglátogatva: 2014. február 8.
- [10] <http://www.bioapi.org/> meglátogatva: 2014. február 8.

- [11] Bledsoe, W. W., and Chan, H. 1965. A Man-Machine Facial Recognition System-Some Preliminary Results, Technical Report PRI 19A, Panoramic Research, Inc., Palo Alto, California
- [12] Bledsoe, W. W. 1966. Some Results on Multicategory Pattern Recognition. *Journal of the Association for Computing Machinery* 13(2):304-316.
- [13] Bledsoe, W. W. 1966. Man-Machine Facial Recognition: Report on a Large-Scale Experiment, Technical Report PRI 22, Panoramic Research, Inc., Palo Alto, California
- [14] Bledsoe, W. W. 1968. Semiautomatic Facial Recognition, Technical Report SRI Project 6693, Stanford Research Institute, Menlo Park, California. Faculty Council, University of Texas at Austin, In Memoriam Woodrow W. Bledsoe <http://www.utexas.edu/faculty/council/1998-1999/memorials/Bledsoe/bledsoe.html>
- [15] <http://www.bostonmicromachines.com/aoslo.htm> meglátogatva: 2014. március 1.
- [16] Burge, M., and W. Burger. "Using ear biometrics for passive identification." *Proceedings of the IFIP TC11 14th International Conference on Information Security, SEC*. Vol. 98. 1998.
- [17] Burge, M., and Burger, W., Ear biometrics in computer vision, *Proc. ICPR 2000*, pp. 822-826, 2002
- [18] J. Canny (1986): A computational approach to edge detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 8(6): pp. 679-698
- [19] Chang, K., Bowyer, K.W., Sarkar, S., Victor, B. Comparison and Combination of Ear and Face Images in Appearance-Based Biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, September 2003, pp. 1160-1165.
- [20] W. S. Chen and C. L. Kuo, "Apparatus for Imaging Fingerprint or Topographic Relief Pattern on the Surface of an Object," US Patent 5448649, 1995.
- [21] <http://www.fbi.gov/about-us/lab/biometric-analysis/codis> meglátogatva: 2014. február 8.
- [22] Cootes, T. F., Edwards, G. J., and Taylor, C. J. (2001). Active appearance models. *IEEE Transactions on pattern analysis and machine intelligence*, 23(6), 681-685.
- [23] Cortes, Corinna; and Vapnik, Vladimir N.; "Support-Vector Networks", *Machine Learning*, 20, 1995
- [24] G. W. Cottrell and J. Metcalfe. Empath: face, emotion, and gender recognition using holons. In *NIPS*, pages 564-571, 1990.

- [25] Cummins, Harold. The Topographic History of the Volar Pads (walking Pads; Tastballen) In the Human Embryo. Washington, 1929.
- [26] CROSS, J. M.; SMITH, C. L. Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification. In: Security Technology, 1995. Proceedings. 29th Annual 1995 International Carnahan Conference on. IEEE, 1995. p. 20-35.
- [27] Broad Agency Announcement: Active Authentication, DARPA-BAA-12-06, January 12, 2012
- [28] Daugman, J., "High confidence visual recognition of persons by a test of statistical independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, 15 (11), pp 1148-1161 (1993)
- [29] Daugman, John. "Recognizing people by their iris patterns." Information Security Technical Report 3.1 (1998): 33-39.
- [30] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 21-30, 2004.
- [31] <http://www.cl.cam.ac.uk/~jgd1000/afghan.html>
- [32] Dimond, T.L. "Devices for reading handwritten characters", Proceedings of Eastern Joint Computer Conference, pp 232-237, December 1957.
- [33] Economic benefits of standardization - Summary of results, DIN, 2000
- [34] J. H. Doggart. Ocular Signs in Slit-lamp Microscopy. Kimpton, London, 1949.
- [35] R. F. Dowling Jr. and K. L. Knowlton, "Fingerprint Acquisition System With a Fiber Optic Block," US Patent 47851 71, 1988
- [36] Dror, I. E., Charlton, D., Peron, A. E. (2006). Contextual information renders experts vulnerable to making erroneous identifications. Forensic Science International, 156, 74-78.
- [37] European Commission: Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking, published October 10, 2013
- [38] Ernst E. (2000. Jan). "Iridology: not useful and potentially harmful". Arch. Ophthalmol. 118 (1), 120-1.
- [39] The Fingerprint Sourcebook, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, [www.nij.org](http://www.nij.org)
- [40] Leonard Flom, Aran Safir, "Iris recognition system", US4641349 A, Közzététel dátuma 1987. febr. 3.
- [41] Dinei Florencio and Cormac Herley, A Large-Scale Study of Web Password Habits, Proc. WWW 2007, Banff, BC

- [42] Freund, Yoav; Schapire, Robert E. A Decision-Theoretic Generalization of on-Line Learning and an Application to Boosting, *Journal of Computer and System Sciences*, Vol 55, Issue 1, 119-139 (1997)
- [43] <http://face.nist.gov/frgc/> meglátogatva: 2014. március 14.
- [44] <http://face.nist.gov/frvt/> meglátogatva: 2014. március 14.
- [45] Palm Vein Pattern Authentication Technology, Whitepaper, 2006 [http://www.fujitsu.com/downloads/COMP/ffna/palm-vein/palmsecure\\_wp.pdf](http://www.fujitsu.com/downloads/COMP/ffna/palm-vein/palmsecure_wp.pdf) meglátogatva: 2014. február 8.
- [46] Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., and Ortega-Garcia, J. (2012). From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems. Paper presented at the Black Hat USA, Las Vegas, 2012.
- [47] Francis Galton, *Finger Prints*, London, Macmillan and Co., 1892
- [48] Global Biometrics Technology Market (2010-2015) - Market Forecast by Products, End-User Application and Geography, Publishing Date: January 2011, Report Code: SE 1302, forrás: <http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html> meglátogatva: 2014. február 22.
- [49] Hyman Eli Goldberg, U.S. Patent 1,117,184, On-line recognition of hand-written numerals to control a machine in real-time.
- [50] A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces," *Proc. IEEE*, May 1971, Vol. 59, No. 5, 748-760.
- [51] B. A. Golomb, D. T. Lawrence, and T. J. Sejnowski. SexNet: A neural network identifies sex from human faces. In *NIPS*, pages 572-577, 1990.
- [52] Grew, Nehemiah (1684). "The description and use of the pores in the skin of the hands and feet". *Philosophical Transactions of the Royal Society* 14: 566-567.
- [53] Diana Harrison, Ted M. Burkes, Danielle P. Seiger, *Handwriting Examination: Meeting the Challenges of Science and the Law*, *Forensic Science Communications*, October 2009, Volume 11, Number 4
- [54] Robert "Buzz" Hill, *Retina Identification*, in book *Biometrics, Personal Identification in Networked Society*, editors A. K. Jain, R. Bolle, S. Pankanti, Kluwer, 2002
- [55] <http://pinktentacle.com/2007/10/steering-wheel-finger-vein-authentication-system/> meglátogatva: 2014. február 8.
- [56] [http://www.hitachi.co.jp/products/it/veinid/global/products/embedded\\_devices.html](http://www.hitachi.co.jp/products/it/veinid/global/products/embedded_devices.html) meglátogatva: 2014. február 8.



- [57] R. A. Huber and A. M. Headrick, *Handwriting Identification: Facts and Fundamentals*, CRC Press, LCC, 1999.
- [58] A. Iannarelli, *Ear Identification*. Forensic Identification Series. Paramount Publishing Company, Fremont, California, 1989.
- [59] H. Jacoby, A. J. Giordano, and W. H. Fioretti, "Personnel Identification Apparatus," US Patent No. 3648240, 1972.
- [60] A.K. Jain, A. Ross and S. Pankanti, "A Prototype Hand Geometry-based Verification System", *Proc. of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)* , Washington D.C., pp.166-171, March 22-24, 1999.
- [61] Anil K. Jain, Friederike D. Griess, Scott D. Connell, On-line signature verification, *Pattern Recognition* 35 (2002) 2963 - 2972
- [62] Anil K. Jain, Hong Chen, Silviu Minut, *Dental Biometrics: Human Identification Using Dental Radiographs, Audio- and Video-Based Biometric Person Authentication*, *Lecture Notes in Computer Science* Volume 2688, 2003, pp 429-437
- [63] <http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/> meglátogatva: 2013. április 21.
- [64] J.-W. Jung, K.-H. Park, and Z. Bien. Unconstrained Person Recognition Method using Static and Dynamic Footprint. In *Proceedings of the 18th Hungarian-Korean Seminar*, Budapest, Hungary, pages 129-137, 2002.
- [65] J.-W. Jung, T. Sato, and Z. Bien. Dynamic Footprint-based Person Recognition Method using Hidden Markov Model and Neural Network. *International Journal of Intelligent Systems*, 19(11):1127-1141, 2004.
- [66] R. Kennedy. Uniqueness of bare feet and its use as a possible means of identification. *Forensic Science International*, 82(1):81-87, 1996.
- [67] Kovács Tibor, Milák István, Otti Csaba: A biztonságstudomány biometriai aspektusai, *Pécsi Határőr Tudományos Közlemények*, XIII., 2012
- [68] Miroslav Králík, Ladislav Nejman, Fingerprints on artifacts and historical items: examples and comments, *Journal of Ancient Fingerprints*, pp. 5-15, nr. 1. 2007
- [69] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar, "Attribute and Simile Classifiers for Face Verification," *IEEE International Conference on Computer Vision (ICCV)*, Oct, 2009
- [70] Lowe, David G. (1999). "Object recognition from local scale-invariant features". *Proceedings of the International Conference on Computer Vision* 2. pp. 1150-1157.

- [71] L. Ma, T. Tan, Y. Wang and D. Zhang, "Personal Identification based on Iris Texture Analysis", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 25, No. 12, pp. 1519-1533, 2003.
- [72] L. Ma, T. Tan, Y. Wang and D. Zhang, "Efficient Iris Recognition by Characterizing Key Local Variations", *IEEE Transactions on Image Processing*, Vol. 13, No. 6, pp. 739-750, 2004.
- [73] P. MacGregor and R. Welford, (1991) *Veincheck: Imaging for security and personnel identification*, *Adv. Imaging* 6 (7), 52-56.
- [74] R. Martens, L. Claesen, Dynamic programming optimization for on-line signature verification, in: *Proceedings of the International Conference on Document Analysis and Recognition*, 1997, pp. 653-656.
- [75] Martinez, A. M.; Kak, A. C. (2001). "PCA versus LDA". *IEEE Transactions on Pattern Analysis and Machine Intelligence* 23 (2): 228-233
- [76] Mauceri, A.J. "Feasibility Study of Personnel Identification by Signature Verification", North American Aviation Inc Downey Calif Space and Information Systems Div., Defense Technical Information Center, 1965
- [77] Z. McMahon, *Biometrics: History*, Indiana University, Computer Science Department, 24 January 2005.
- [78] R. P. Miller, "Finger dimension comparison identification system," US Patent No. 3576538, April, 1971.
- [79] Miura, Naoto, Akio Nagasaka, and Takafumi Miyatake. "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification." *Machine Vision and Applications* 15.4 (2004): 194-203.
- [80] Donald M.Monro, Soumyadip Rakshit, and Dexin Zhang, "DCT-Based Iris Recognition", *IEEE Transactions on Pattern analysis and Machine Intelligence*, Vol.29, No.4, pp.586-595, 2007.
- [81] K. Nakajima, Y. Mizukami, K. Tanaka, and T. Tamura. Footprint-based personal recognition. *IEEE Transactions on Biomedical Engineering*, 47(11):1534-1537, 2000.
- [82] [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi) meglátogatva: 2014. február 8.
- [83] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7):971-987, 2002.
- [84] <http://onin.com/fp/fphistory.html> meglátogatva: 2014. február 8.

- [85] Palágyi Kálmán: Képfeldolgozás haladóknak, Typotex, 2011
- [86] Pittman, J.A.: Handwriting recognition: tablet PC text input. *IEEE Comput.* 40(9), 49-54 (2007)
- [87] William K. Pratt. 2001. *Digital Image Processing: PIKS Inside* (3rd ed.). John Wiley & Sons, Inc., New York, NY, USA.
- [88] Reinaud, Joseph Toussaint (1845). *Relation des voyages faits par les Arabes et les Persans dans l'Inde et la Chine dans le IX Siecle.. I.* Paris: Imprimerie royale. p. 42. quoted in: Laufer (1912)
- [89] Janeen Renaghan, *Etched in Stone*, Zoogoer, August, 1997
- [90] Global Biometric Systems Market Forecast & Opportunities, 2017 <http://www.reportlinker.com/p0937502/Global-Biometrics-Market-Forecast-and-Opportunities.html> meglátogatva: 2014. február 8.
- [91] R. Roizenblatt, P. Schor et al. Iris recognition as a biometric method after cataract surgery. *Biomed Eng Online*. 2004; 3: 2
- [92] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. Direct Attacks Using Fake Images in Iris Verification. In *Biometrics and Identity Management, Lecture Notes In Computer Science*, Vol. 5372. Springer-Verlag, Berlin, Heidelberg 181-190. 2008
- [93] Oliver Sacks: *A férfi, aki kalapnak nézte a feleségét (és más orvosi történetek)*, Park Kiadó, 2008
- [94] A Performance Evaluation of Biometric Identification Devices, Technical Report SAND9 1-0276, UC-906, Sandia National Laboratories, Albuquerque, NM and Livermore, CA for the United States Department of Energy under Contract DE-AC04-76DP00789, 1991.
- [95] C. Simon and I. Goldstein, "A New Scientific Method of Identification," *New York State Journal of Medicine*, Vol. 35, No. 18, pp. 901-906, September, 1935.
- [96] Sirovich, Lawrence, and Michael Kirby. "Low-dimensional procedure for the characterization of human faces." *JOSA A* 4.3 (1987): 519-524.
- [97] Herschel Smith: *Operation Alljah and the Marines of 2nd Battalion, 6th Regiment*, *The Captain's Journal*, <http://www.captainsjournal.com>
- [98] SRI International Sarnoff launches iris biometric vehicle access control system". *Biometric Update*. 2013-04-10
- [99] *STATE v. David Wayne KUNZE*, Court of Appeals of Washington, Division 2. 97 Wash. App. 832, 988 P.2d 977, 1999

- [100] <http://www.cse.ust.hk/svc2004> meglátogatva: 2014. március 14.
- [101] J. Svigals, "Low Cost Personal Identification Verification Device Based on Finger Dimensions," IBM Technical Disclosure Bulletin, Vol. 25, No. 4, September 1982.
- [102] Szabó Máté Dániel: Biometrikus azonosítás és adatvédelem. Megjelent: Acta Humana, 2004/1.
- [103] Catherine J. Tilton: Standards - Getting Started, Planet Biometrics, September 2011.
- [104] Transparency Market Research (TMR): Biometrics Market - Global Industry Size, Market Share, Trends, Analysis And Forecasts, 2012 - 2018 <http://www.transparencymarketresearch.com/biometrics-market.html> meglátogatva: 2014. február 8.
- [105] P. Tower, "The fundus Oculi in monozygotic twins: Report of six pairs of identical twins," Archives of Ophthalmology, Vol. 54, pp. 225-239, 1955.
- [106] Turk, Matthew A., and Alex P. Pentland. "Face recognition using eigenfaces." Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on. IEEE, 1991.
- [107] <http://uidai.gov.in/> meglátogatva: 2015. február 7.
- [108] <http://vis-www.cs.umass.edu/lfw/> meglátogatva: 2014. március 14.
- [109] Veldhuis, Raymond, Asker Bazen, Wim Booij, and Anne Hendrikse. "A comparison of hand-geometry recognition methods based on low-and high-level features." (2004): 326-330.
- [110] Viola, Paul, and Michael Jones. "Robust real-time object detection." International Journal of Computer Vision 4 (2001).
- [111] Wang, James Z., et al. "Determining the sexual identities of prehistoric cave artists using digitized handprints: a machine learning approach." Proceedings of the international conference on Multimedia. ACM, 2010. pp. 1325-1332
- [112] <http://www.wenturedigital.com/component/content/article/35-latest-headlines/46-fingerprint-biometric-market-growth.html> meglátogatva: 2013. április 21.
- [113] Wen-Shiung Chen, and Shang-Yuan Yuan, "A Novel Personal Biometric Authentication Technique using Human Iris Based on Fractal Dimension features", Proceedings of ICASSP, Vol.3, pp. 201-204, 2003.
- [114] Wiskott, L., Fellous, J. M., Kuiger, N., and Von Der Malsburg, C. (1997). Face recognition by elastic bunch graph matching. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 19(7), 775-779.

- [115] D. Zhang. Palmprint authentication. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.