Biometria

Carles Fernández Tena

PID_00194171

UOC
Universitat Oberta de Catalunya

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca

Índex

1. Introducció. Fonaments de la biometria. Antecedents històrics 5
1.1. Definició i objectius de la biometria 6
1.2. Conceptes bàsics 8
1.3. Classificació i comparació de biometries 10

2. Operativa d'un procés biomètric 13
2.1. Selecció de característiques 15
2.2. Classificació 18
2.3. Fusió de biometries 21
2.4. Mètriques d'avaluació 23

3. Anàlisi de les biometries principals 27
3.1. Reconeixement facial 27
3.1.1. Normalització 28
3.1.2. Dificultats del reconeixement facial 28
3.1.3. Mètodes de reconeixement facial 30
3.2. Reconeixement de l'iris 33
3.3. Reconeixement dactilar 36
3.4. Reconeixement del parlant 40
3.5. Altres biometries 44

4. Aplicacions principals 48

5. Conclusions i reptes futurs 51

Bibliografia 53

1. Introducció. Fonaments de la biometria. Antecedents històrics

La biometria se sol concebre popularment com un camp totalment modern i innovador, amb idees sortides de novel·les i cinema de ciència-ficció. Tot i això, al llarg de la història de la humanitat, incloent-hi civilitzacions antigues, hi ha hagut un gran nombre d'esdeveniments on apareix repetidament la idea d'**identificar persones** o bé **verificar-ne les identitats**, basant-se únicament en trets físics o de comportament.

Des del 6000 aC, i de manera repetida, es té constància de l'ús d'empremtes dactilars i manuals per a la identificació personal per part de diverses civilitzacions, com per exemple assiris, babilonis, japonesos i xinesos. No ha estat fins a finals del segle XX que s'ha presenciat de manera conjunta l'aparició i la consolidació de noves biometries, entre les quals destaquen la **facial**, la de l' **iris** i la de la **veu**. A continuació detallem alguns esdeveniments importants de la història de la biometria.

- Cap al 3000 aC, a l'antic Egipte eren rutinaris els enregistraments de trets i mesures corporals per a transaccions comercials i oficials. Els faraons certificaven decrets per mitjà d'empremtes dactilars. Els treballadors de les piràmides eren identificats per mitjà de nom, procedència, mida, complexió, trets facials i de comportament, i altres característiques particulars com ara cicatrius. Aquest va ser el cas durant la construcció de la piràmide de Kheops, per tal d'evitar el falsejament d'identitat dels treballadors en recollir les racions mensuals d'aliments.
- També a l'antiga civilització babilònica es té constància de l'ús d'empremtes del palmell de la mà per a provar l'autenticitat de certes obres d'artesania, com ara gravats.
- S'han trobat empremtes dactilars provinents de l'antiga Xina, datades entre el 610 i el 910 dC. Joao de Barros, explorador i escriptor, va enregistrar històricament un dels primers usos de la biometria, en què els marxants xinesos, gràcies a l'ús de la tinta, imprimien el palmell de la mà i del peu dels nens en papers per verificar-ne la identitat. També es feien servir per a la compravenda de terrenys, contractes i pagarés.
- Al segle VII dC, Suleiman, marxant àrab, feia servir empremtes dactilars com a prova de validesa entre prestataris i prestadors.
- Vers l'any 1000 dC, Quintilià, un advocat de l'Imperi Romà procedent d'Hispània, va aconseguir exculpar un home cec per l'assassinat de la seva mare, demostrant que les empremtes de sang dels palmells de la mà trobades a l'escena es van utilitzar per a incriminar-lo.
- S'han trobat diversos documents oficials de la Pèrsia del segle XIV amb impressions d'empremtes dactilars. Un doctor oficial del govern va observar que no hi havia dues empremtes completament iguals.
- Ja en època moderna, el fisiòleg txec Jan Evangelista Purkyně va incidir de nou en aquesta idea, en descobrir el 1823 que les excrecions de suor a la mà d'una persona produïen patrons únics, fet que el va portar a concebre la possibilitat d'identificar persones a partir de les empremtes dactilars.
- El 1858 Sir William James Herschel, governador anglès a l'Índia, va marcar els contractes de funcionaris amb impressions digitals del palmell de la mà, per identificar-los i evitar casos de suplantació en dies de pagament. Herschel, que va dirigir la policia científica de Bengala, conclou que totes les empremtes de la mà són diferents, i que no canvien substancialment amb el temps.
- L'any 1870 Alphonse Bertillon, oficial de la policia francesa, proposa el sistema antropomètric (*bertillonage*) per a la identificació de criminals. Aquest sistema es basava en l'enregistrament de mesures corporals, descripcions físiques i característiques distintives com ara tatuatges, per a evitar el falsejament de la identitat durant les detencions. Aviat es va desestimar en veure que persones diferents podien compartir les mateixes mesures.
- A la dècada dels anys noranta del segle XIX, Sir Francis Galton crea el primer sistema de classificació d'empremtes mitjançant característiques discriminatòries (minúcies

o detalls de Galton, encara utilitzades avui dia) dels deu dits de la mà, influenciat per la feina de Bertillon, Herschel i Purkyně. Vucetich implementa el sistema de Galton a l'Argentina, i Henry ho fa al Regne Unit, el qual a més proposa un sistema per a agilitzar l'eficàcia de les cerques que substitueix el sistema antropomètric.

- El 1924 l'oficina federal d'intel·ligència dels Estats Units crea una divisió d'identificació personal, amb una base de dades inicial de 810.000 empremtes. La recerca de coincidències es feia de manera manual.
- L'any 1936, l'oftalmòleg Frank Burch proposa utilitzar l'iris per a la identificació biomètrica.
- El 1960 es publica el primer model fisiològic de producció acústica de la parla, de la mà de Gunner Fant (KTH, Suècia). Durant els anys següents es dugué a terme el primer pas important per a la verificació d'identitat mitjançant la parla, de la mà de Lawrence Kersta (Bell Labs), qui va introduir el terme *voiceprint* (empremta de veu) per referir-se a la unicitat dels espectrogrames de senyal de la parla. Inicialment els patrons de veu es comparaven visualment, i tot i que l'anàlisi d'espectrogrames no va obtenir els resultats esperats, va desencadenar la investigació posterior en el reconeixement del parlant, i el naixement d'aquesta biometria.
- El 1965 la North American Aviation desenvolupa el primer sistema de reconeixement de signatura.
- A partir del 1965 es van començar a implementar procediments automàtics per a la comparació i la codificació d'empremtes dactilars, coneguts com a *AFIS* (*automated fingerprint identification system*). L'any 2000 la base de dades d'empremtes dactilars de l'FBI contenia mostres dels deu dits de la mà de 47 milions d'individus.
- A la dècada dels ans seixanta del segle XX, Bledsoe, Chan i Bisson proposen el primer sistema semiautomàtic de reconeixement facial, en què un administrador ha de localitzar manualment punts de referència de la cara (ulls, nas, orelles, boca) i el sistema calcula i compara distàncies i proporcions entre ells. A la dècada dels setanta aquests marcadors es van ampliar, afegint característiques com el color dels cabells o el gruix dels llavis. En tots els casos els resultats van ser molt limitats.
- El 1970 es modelitzen per primera vegada les característiques de comportament de la parla. El primer prototip de sistema de reconeixement del parlant arriba el 1976.
- L'any 1974 es desenvolupen fortament les biometries de reconeixement de la signatura (Stanford Research Institute, EUA, i National Physical Laboratory, RU) i de geometria de la mà (Universitat de Geòrgia).
- El terme *biometria* comença a popularitzar-se a la dècada dels anys vuitanta del segle XX, per a referir-se als sistemes automàtics d'identificació personal.
- L'any 1988, Sirovich i Kirby publiquen el mètode de les *eigenfaces* per al reconeixement facial, basat en tècniques de reducció de dimensionalitat (anàlisi de components principals, PCA). Es demostra que amb 100 valors numèrics es pot representar convenientment una cara ben alineada i normalitzada. El 1991, Turk i Pentland descobreixen que l'error residual d'aquesta tècnica es pot aplicar per a la detecció facial, cosa que possibilita l'aparició de sistemes de reconeixement facial en temps real.
- El 1987, els oftalmòlegs Safir i Flom patenten el concepte general d'identificar persones a partir de l'iris, i el 1989 demanen a John Daugman (Universitat de Harvard) desenvolupar un algorisme per a aconseguir-ho. El 1994, Daugman patenta el seu algorisme, conegut com a *IrisCode*. La patent genèrica del reconeixement de l'iris va expirar el 2005, i la de l'algorisme d'IrisCode el 2011.
- Comencen a sorgir competicions i programes d'avaluació de diferents biometries, com ara FERET per al reconeixement facial (1993), IAFIS per a l'empremta dactilar (1994, 1999), avaluacions NIST per al parlant (anuals des de 1996), FRVT per a la cara, l'empremta i l'iris (2000, 2003, 2006 respectivament), FRGC per a la cara (2004), etc.
- El 2000 es publica el primer treball sobre reconeixement biomètric a partir de patrons vasculars, concretament els del palmell de la mà.
- El 2005 es presenta la tecnologia *iris-on-the-move* , que permet el reconeixement de l'iris a distància i en moviment.

1.1. Definició i objectius de la biometria

Una gran quantitat de sistemes actuals no podrien proveir els seus serveis sense disposar de mecanismes fiables capaços d'autentificar la identitat dels usuaris que hi accedeixen. La finalitat d'aquests mecanismes és assegurar-se que els serveis proporcionats pel sistema només són accessibles a usuaris legítims, i a ningú més.

Alguns exemples d'aquests sistemes inclouen controls d'accés a edificis i zones segures, caixers automàtics, telèfons mòbils, ordinadors i sistemes informatitzats.

Tots ells serien vulnerables a impostors si no existís aquest tipus de mecanismes.

La manera tradicional de restringir l'accés a aquests sistemes ha estat la utilització de **paraules de pas** i de **targetes d'identitat**, és a dir, seguretat basada, respectivament, en el coneixement d'una determinada informació i en la possessió d'un determinat objecte. Aquests mètodes, que fem servir diàriament per a la validació electrònica i per a fer operacions bancàries, comporten riscos importants de seguretat:

- Les paraules de pas poden ser divulgades a usuaris no autoritzats.
- Si són massa senzilles els impostors poden esbrinar-les fàcilment mitjançant tècniques d'enginyeria social o força bruta.
- Si són massa complexes els mateixos usuaris poden oblidar-les.
- I de la mateixa manera, les targetes d'identitat poden ser utilitzades per tercers.

En aquestes condicions, el **camp de la biometria** esdevé una manera més adequada d'enfocar les aplicacions d'autentificació per a evitar els riscos de seguretat dels mètodes tradicionals.

La biometria és la ciència que tracta d'establir la identitat d'una persona a partir d'una sèrie d'atributs físics[1] o atributs de comportament[2].

(1)Per exemple, cara, iris, veu, empremta dactilar, o geometria de la mà.

(2)Com ara la signatura, la dinàmica de tecleig, o l'anàlisi biomecànica de la marxa mentre es camina.

Així doncs, la biometria fa possible l'establiment de la identitat d'una persona basant-nos en "qui és", més que no pas "què posseeix" o "què recorda" (Beardsley, 1972). Concretament, els sistemes biomètrics comparen un conjunt de característiques extretes d'un individu amb aquelles prèviament obtingudes del mateix individu.

Etimologia de la paraula *biometria*

Etimològicament, la paraula *biometria* denota tot allò relacionat amb el mesurament d'éssers vius.

L' **avantatge** immediat dels sistemes biomètrics és que els trets personals no poden ser robats, compartits o perduts fàcilment. A més a més, els sistemes biomètrics normalment assoleixen nivells de precisió molt alts, i el balanç entre precisió i exhaustivitat es pot ajustar per a optimitzar una determinada aplicació.

Com a **contrapartida**, presenten una sèrie de limitacions, com per exemple el possible increment en el cost d'instal·lació i d'execució, les dificultats tècniques afegides al reconeixement en entorns molt incontrolats, o la possible variació significativa dels trets biomètrics al llarg del temps.

A part d'aspectes beneficiosos purament relacionats amb les aplicacions de **seguretat**, la biometria aporta un component addicional important d' **usabilitat** per als usuaris finals, que no necessiten recordar paraules de pas complexes i potencialment diferents per a cada sistema, ni portar a sobre estris identificatius en tot moment. D'altra banda, una crítica que habitualment es fa als sistemes biomètrics és el fet d'atemptar en més o menys mesura contra la **privacitat** de les persones, atès el caràcter altament sensible de les dades amb què es treballa. En aquest sentit, cal destacar les millores recents que actualment s'han dut a terme en el camp de l'encriptació biomètrica.

1.2. Conceptes bàsics

Al llarg d'aquest mòdul s'empren regularment una sèrie de termes biomètrics que cal definir i saber diferenciar correctament. Es tracta dels conceptes de *mostra*, *característica* (o *patró*) i *plantilla biomètrica*.

Les **mostres biomètriques** són aquelles dades relatives a una persona que els sistemes biomètrics obtenen per mitjà de sensors.

Per exemple, una fotografia de la cara o de l'iris, una gravació de veu o de vídeo, o una empremta dactilar.

Quan parlem de **característiques biomètriques** o patrons biomètrics[3], ens referim a aquelles característiques distingibles de l'individu que poden ser mesurades o estimades a partir d'una mostra biomètrica, i que cal extreure per al procés d'identificació.

(3) Idealment, aquests patrons haurien de ser únics i invariants per a cada persona.

Per exemple, són característiques biomètriques d'una persona la distància entre els ulls, la grandària del nas, els patrons irregulars de l'iris, la distribució de vasos sanguinis a la retina o la manera de caminar.

Una **plantilla biomètrica** és un recull d'informació compilat a partir d'una sèrie de característiques biomètriques, que serveix com a resum dels trets més significatius d'una persona. Una plantilla recopila informació única de l'individu de manera eficient, per tal de poder comparar les unes amb les altres ràpidament.

Una possible plantilla biomètrica podria estar formada per l'*IrisCode* de l'ull dret, les minúcies dactilars de la mà esquerra i la freqüència fonamental de la veu.

Els sistemes biomètrics empren sensors per a capturar mostres biomètriques d'una persona, extreuen una sèrie de característiques a partir d'aquestes mostres i les recopilen en forma de plantilla biomètrica. Posteriorment, la informació continguda en les diferents plantilles pot ser comparada per tal d'establir la identitat de l'individu.

Les característiques biomètriques han de complir una sèrie de **condicions necessàries** per a poder-se utilitzar de manera efectiva com a identificadors personals. Aquestes condicions són:

- **Universalitat**. Totes les persones han de posseir naturalment aquesta característica.

- **Unicitat**. Una mateixa característica no pot presentar-se de la mateixa manera en dos individus diferents.

- **Perdurabilitat**. La característica ha de restar inalterable al llarg del temps.

- **Mesurabilitat**. La característica ha de poder-se mesurar físicament i de manera senzilla per mitjà d'un sensor.

A més d'aquestes condicions necessàries, és positiu que les característiques biomètriques també presentin un seguit de **propietats desitjables** que facin més adequada la seva implantació real a la societat.

Una de les propietats més òbvies són les **prestacions** de la biometria en qüestió, que engloba no solament la precisió del reconeixement i el nivell de seguretat consegüent que se'n deriva, sinó també la rapidesa de funcionament i el baix cost de la solució, amb els quals se'n possibilita la implementació a gran escala.

Una altra vessant de requisits té més relació amb l' **acceptació** del sistema per part de la societat, on la facilitat d'ús de la solució i la reduïda necessitat d'invasió exerceixen papers destacats, però on també és imprescindible considerar qüestions culturals i possibles connotacions negatives de la tecnologia.

Finalment, també cal tenir en compte la **facilitat d'elusió** de la tecnologia fent servir pràctiques fraudulentes; per exemple, una persona pot utilitzar sense autorització fotografies d'un altre usuari que estigui registrat, o motlles artificials d'empremtes dactilars d'una altra persona. Per a evitar aquestes pràctiques se solen afegir mòduls de *liveness detection*, és a dir, detecció de "part viva" sobre la fisiologia presentada (cara viva, ull viu, dit viu, etc.), que determinen de diverses formes possibles si la mostra biomètrica prové d'una persona viva, o bé es tracta d'un intent de frau.

D'altra banda, si ens concentrem en les **funcionalitats** que la identificació biomètrica pot oferir a la societat, en podem destacar tres de principals:

- **Identificació positiva** o "és aquesta persona qui diu ser?". Aquest tipus d'identificació permet verificar amb un alt grau de fiabilitat si la presumpta identitat d'una persona, per exemple a través d'un nom d'usuari (*login*), està relacionada amb la mostra biomètrica adquirida pel sensor que fa de paraula de pas. Les aplicacions derivades d'aquest tipus d'identificació s'utilitzen especialment per a controls d'accés, validació de transaccions i autenticació en dispositius electrònics.

- **Identificació a gran escala** o "aquesta persona es troba present a la base de dades?". Se'ns permet determinar si una característica biomètrica concreta està associada a alguna de les moltes identitats inscrites al sistema, que poden ser de l'ordre de milions, mantenint la supervisió externa tan reduïda com sigui possible. Entre les aplicacions que necessiten identificació a gran escala hi figuren els controls fronterers, la identificació de votants, els carnets electrònics (d'identitat, de conduir), la investigació criminal i la identificació de cossos o de nens perduts.

- **Vigilància (*screening*)** o "aquesta persona forma part de la llista negra?". En aquest cas es determina si l'individu en qüestió pertany a una llista negra (o blanca) d'identitats d'interès. Són exemples d'aquesta tipologia els sistemes de seguretat per videovigilància biomètrica, com ara els utilitzats en aeroports, estacions o esdeveniments multitudinaris. Per la naturalesa que tenen, les aplicacions de vigilància biomètrica poden no tenir accés a processos d'entrenament d'usuaris en el sentit tradicional; poden no tenir control sobre tots els factors relacionats amb la captura, com ara les condicions d'il·luminació o l'orientació correcta de les mostres obtingudes; i han de processar una gran quantitat de dades amb la mínima supervisió possible.

1.3. Classificació i comparació de biometries

Les tecnologies biomètriques solen classificar-se en dos grans grups: les **físiques** i les de **comportament**, sovint també anomenades *estàtiques* i *dinàmiques*, respectivament.

- El primer grup es basa en **característiques anatòmiques del cos**, que varien poc o gens al llarg de la vida, com per exemple el color dels ulls, les empremtes dactilars, el codi genètic o els patrons de l'iris.

- En canvi, el segon grup de tecnologies analitza **característiques de comportament de l'individu**, i aquestes característiques presenten molta més variabilitat, com succeeix amb la manera de caminar o d'escriure.

Biometria de veu

El cas de la biometria de veu sol tractar-se de manera especial, ja que incorpora característiques d'ambdós grups a la vegada.

La manera en què s'adquireixen les característiques també és una manera habitual de classificar les biometries, que poden ser **actives** o **passives**.

- Les actives necessiten la col·laboració de l'individu per a adquirir les mostres (tal com passa amb l'empremta dactilar o el reconeixement de retina).

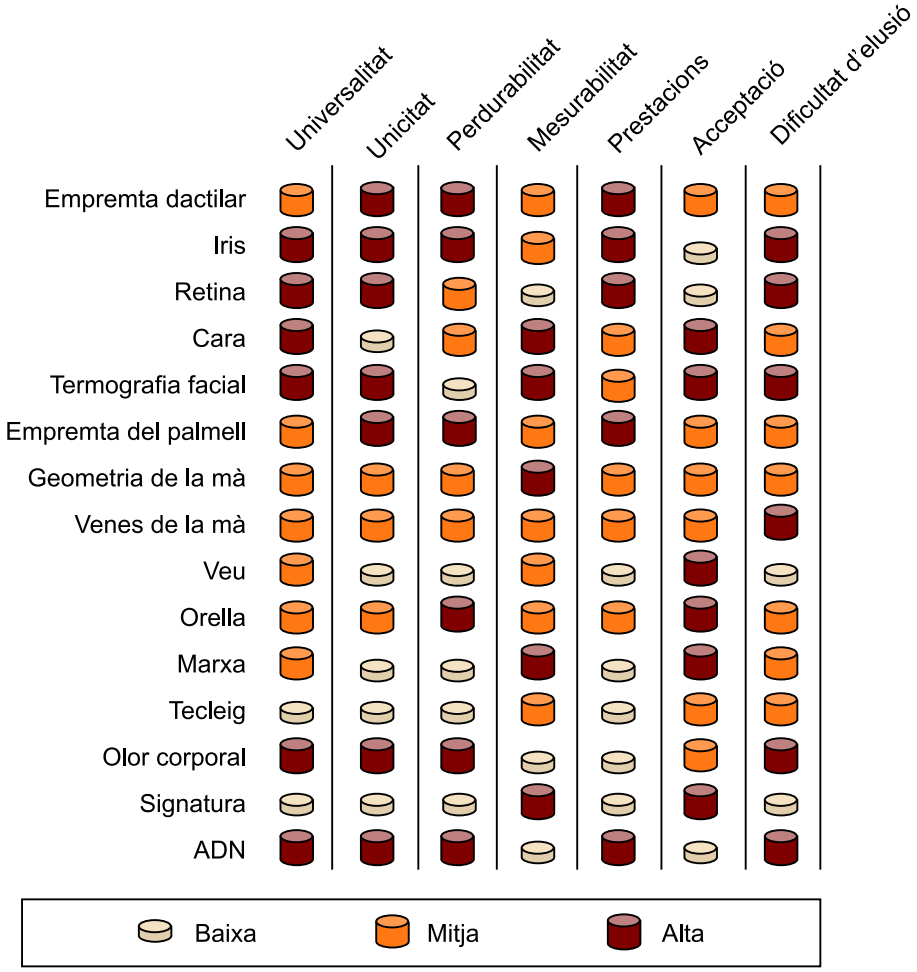
- En canvi, a les passives la invasió pot ser pràcticament nul·la. L'individu no ha de prendre part activament en el procés de reconeixement, no cal que toqui cap dispositiu ni que faci cap acció específica. De fet, ni tan sols és necessari que l'individu sàpiga que el procés de reconeixement està duent-se a terme.

Exemple

Un exemple clar de biometria passiva és la facial, especialment en el cas de videovigilància, on les càmeres cobreixen grans àrees, se situen per a captar vistes frontals de la gent que circula per la zona, i aquestes persones sovint no s'adonen de la presència d'aquestes càmeres.

La taula següent mostra la comparació d'un seguit de tecnologies biomètriques respecte de les set propietats necessàries i desitjables esmentades a la secció anterior, on es qualifica cada biometria amb un valor baix, mitjà o alt d'acord amb estadístiques dutes a terme per diferents institucions científiques i per organismes especialitzats en el sector biomètric. Una biometria ideal hauria de tenir valors alts per a totes les propietats.

Comparació de les tecnologies biomètriques més habituals segons les propietats biomètriques que posseeixen en major o menor grau



Com es pot observar, les biometries **de l'iris** i **de l'empremta dactilar** han demostrat oferir molt bones prestacions i ser considerablement robustes al soroll de les dades, tot i que el seu nivell d'intrusió sol estar per sobre del desitjat. En el cas de l'empremta genètica o **ADN**, aquestes característiques es porten al límit i se n'obtenen taxes de reconeixement gairebé òptimes però són completament intrusives per a l'usuari que s'ha d'identificar. D'altra banda, altres biometries com el reconeixement **facial** i el reconeixement del **parlant** són especialment poc intrusives i poden ser mesurades fàcilment i a distància; no obstant això, tot i que generalment ofereixen bons resultats, solen estar per sota dels resultats oferts per les biometries anteriors, entre altres motius a causa que són més variables i més sensibles al soroll a interferències externes. Biometries com ara la **signatura** o la **dinàmica de tecleig** mostren més debilitats pel fet que poden esdevenir molt semblants entre individus diferents, i, per tant, poden ser falsificades amb facilitat, i a més es poden veure naturalment alterades al llarg del temps. Altres tecnologies com ara el reconeixement de la **retina** o de l' **olor corporal** han demostrat oferir bones prestacions pel que fa a la identificació, però són molt complicades de mesurar, ja sigui per una intrusió molt alta (que també comporta un baix nivell d'acceptació) o per la facilitat amb què es contaminen les mostres analitzades.

Biometries de la cara, de l'iris, de l'empremta dactilar i de la veu

Cal esmentar que, tot i que al llarg dels darrers vint anys s'han portat a terme una gran quantitat d'experiments per a avaluar individualment les biometries contingudes a la taula, únicament hi ha hagut quatre biometries que han estat exhaustivament analitzades per mitjà de grans iniciatives internacionals a gran escala: es tracta de les biometries de la cara, de l'iris, de l'empremta dactilar i de la veu. Aquest fet també ha originat un salt qualitatiu molt més important en la recerca i la millora d'aquestes quatre tecnologies que el que s'ha pogut observar a la resta.

2. Operativa d'un procés biomètric

Els sistemes biomètrics són exemples de **sistemes de reconeixement automàtic**, on les característiques emprades per a classificar poden extreure's d'imatges de la cara o de l'iris, d'empremtes dactilars, de senyals de la veu, etc., i les classes que s'han de reconèixer són les possibles identitats de l'individu. Qualsevol sistema biomètric consta típicament de quatre **mòduls** ben diferenciats:

1) Un **sensor**, que captura el conjunt de dades biomètriques de l'individu que es presenta al sistema. Per exemple, un sensor d'empremta dactilar que genera imatges en forma de crestes a partir dels relleus de les puntes dels dits.

2) Un **mòdul d'extracció de característiques**, que processa les dades capturades pel sensor i n'extreu una plantilla biomètrica en forma de vectors de característiques. Seguint el mateix exemple, aquest mòdul analitza la imatge de l'empremta i extreu posicions i orientacions de les bifurcacions i dels punts terminals de les crestes, anomenades *minúcies*, que representen la part fonamental i distintiva de les dades.

3) Un **mòdul de comparació**, en què es confronta la plantilla biomètrica extreta de l'individu amb plantilles guardades a la base de dades i es quantifica la similitud entre elles per mitjà de puntuacions.

4) I finalment, un **mòdul de decisió**, en què a partir de les puntuacions obtingudes pel mòdul anterior el sistema verifica o estableix la identitat de l'individu. Per exemple, una possible estratègia per a determinar identitats seria la d'assignar a la persona en qüestió aquella identitat de la base de dades amb la qual s'obté una puntuació més elevada, sempre que aquesta puntuació superi un llindar d'acceptació mínim.

Qualsevol sistema biomètric necessita disposar prèviament de mostres biomètriques de les persones que es volen identificar. El **procés d'inscripció** o **entrenament** és, doncs, un pas inicial imprescindible.

Al llarg d'aquest procés s'obtenen, mitjançant un sensor, unes mostres biomètriques de la persona que es vol incorporar al sistema, se n'extreuen característiques biomètriques i finalment es crea una plantilla biomètrica, a la qual s'assigna externament la identitat de l'individu.

La plantilla etiquetada queda així enregistrada a la base de dades, preparada per a comparacions posteriors. Mitjançant aquest procés d'enregistrament és possible tant incorporar com actualitzar la informació biomètrica dels usuaris, i depenent de l'aplicació, pot no ser necessària la intervenció humana per a etiquetar la identitat de l'individu.

D'altra banda, un sistema biomètric té dos possibles modes de funcionament, anomenats **verificació** i **identificació**. Tot i que puguin semblar equivalents, aquests processos segueixen en realitat plantejaments diferents que tenen associats nivells de complexitat diferents.

1) En el cas de la **verificació** o autenticació, s'ha de confirmar una identitat que es presenta de manera explícita al sistema. Cal, doncs, respondre la pregunta "és cert que aquesta persona és qui diu ser?", o dit d'una altra manera, "és cert que aquestes dades biomètriques corresponen a aquesta identitat?".

En aquest cas, l'usuari presenta la seva identitat (per exemple, per mitjà d'un nom d'usuari al sistema) i la confirma amb un senyal biomètric que faria de paraula de pas. Aquest tipus de plantejament s'anomena *comparació one-to-one* (1:1).

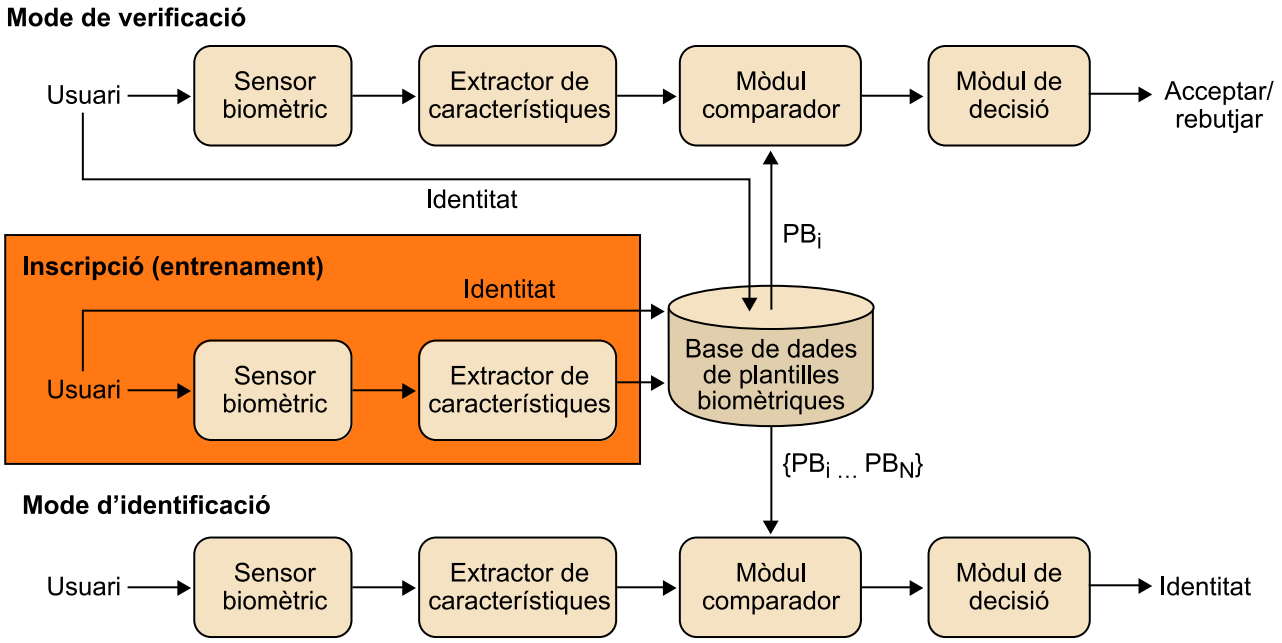
2) D'altra banda, durant un procés d' **identificació**, el sistema ha de determinar la identitat de l'individu d'entre totes les possibles identitats enregistrades a la base de dades. La pregunta que ha de respondre aquest procés és "qui és aquesta persona?", o "quina identitat de les emmagatzemades es correspon amb aquestes dades?".

Un possible exemple consistiria a determinar la procedència d'una empremta dactilar trobada en un escenari policial. En aquest cas la comparació es fa exhaustivament i s'anomena *one-to-many* (1:N).

One-to-few

Existeix una alternativa intermèdia entre ambdós modes de funcionament, que s'anomena *comparació one-to-few*. En aquest cas, l'accés al procés d'identificació està restringit a un nombre molt limitat d'usuaris, típicament menys de 10, i no és necessari presentar explícitament la identitat que s'ha de verificar.

Arquitectura dels dos possibles modes de funcionament d'un sistema biomètric: verificació i identificació



2.1. Selecció de característiques

Una de les tasques que poden resultar més complicades en un procés de reconeixement biomètric, i en qualsevol procés de reconeixement automàtic en general, és la **selecció de les característiques** que s'extrauran de la mostra inicial de dades i que s'utilitzaran al procés final de classificació i decisió.

> Les característiques escollides han de ser relativament fàcils de mesurar, i han de permetre discriminar les classes en què es poden classificar.

Les característiques seleccionades condicionen completament la resta d'etapes del procés de reconeixement, des de la captura de la mostra fins al tipus de classificador.

Per posar-ne un exemple concret, imaginem que volem dissenyar un classificador per diferenciar de manera automàtica entre dos bolets com el fredolic (*Tricholoma atrosquamosum*) i el *lepiota* (*Lepiota brunneoincarnata*), mostrats a la figura següent. Ambdós són molt semblants entre si i comuns a l'àrea de Barcelona, però el segon d'ells és altament tòxic i mortal.

Esquerra: fredolic (*Tricholoma*) (http://ca.wikipedia.org/wiki/Fitxer:Tricholoma_terreum.jpg). Dreta: *lepiota* (http://en.wikipedia.org/wiki/File:Lepiota_brunneoincarnata_060823w.jpg)

Sempre que ens plantegem abordar un problema de reconeixement cal passar necessàriament per una sèrie d'etapes, incloses a l'anomenat ***cicle de disseny***, que es presenta a continuació.

Cicle de disseny d'un procés de reconeixement

En primer lloc, cal **recollir la informació** que utilitzarem per a classificar, per exemple mesurant-la mitjançant un sensor que ens proporcioni dades per a cada observació.

En l'exemple proposat, podríem obtenir dades com ara l'altura total, la longitud de la cama o la longitud de la circumferència del barret. Però aquestes mesures semblen força similars entre ambdues espècies de bolets, de manera que haurem de plantejar la captura d'altres dades, com ara fotografies de la part inferior del barret i del contorn de perfil de cada bolet. Qualsevol característica escollida té problemàtiques inherents: les fotografies són sensibles a condicions d'il·luminació i a la posició dels bolets en el moment de la captura, i els contorns poden presentar grans variacions (fins i tot per a un mateix bolet) i poden ser difícils de comparar entre si.

El pas següent és **seleccionar i extreure les característiques** que farem servir per al classificador. Aquesta selecció depèn de la informació que tinguem *a priori*, del cost d'adquirir les característiques, de la invariància d'aquestes característiques (a la translació, rotació, escala, distorsió, oclusió, deformació...) i, especialment, del poder discriminant que tinguin. És a dir, cal que les característiques siguin similars per a classes iguals, i diferents per a classes diferents.

Fent un estudi més exhaustiu de les dades de l'exemple anterior, o utilitzant coneixement *a priori* sobre micologia, es pot comprovar que les diferències principals entre els dos bolets són la textura escamosa de la part inferior de la cama (present al *lepiota* i no al fredolic), el color de les làmines sota el barret (més clar als *lepiotes*), i l'estructura laminar de sota el barret (que als *lepiotes* no sol tocar la cama, i als fredolics sí). Per raons logístiques, pot resultar més senzill mesurar la textura de la cama que les làmines del barret, ja que per a les altres dues opcions hauríem de girar el bolet i obtenir una imatge inferior, que quedaria sempre amagada parcialment per la cama. En canvi, obtenir una fotografia de la cama és senzill: la textura no varia circularment, i la direcció clara de la cama ens possibilita l'alineament automàtic de les imatges.

Existeixen tècniques de visió per a aïllar els objectes d'interès del fons de la imatge (segmentació d'objectes), i d'altres per a detectar l'angle i la posició de les rectes més notòries d'una imatge (transformada de Hough), amb la qual cosa podem obtenir les imatges normalitzades següents, més preparades per a la classificació. Aquestes tasques preparatives s'anomenen *etapes de* ***preprocessament***, i són habituals durant l'extracció de característiques.

Preprocessament

El preprocessament sovint és una part molt important dins l'algorisme final de reconeixement, i pot arribar a ser força complex en alguns casos.

Imatges alineades i segmentades del final de la cama en quatre mostres de bolets

Les dues primeres corresponen a fredolics, les dues darreres a *lepiotes*.

En aquest exemple, podem refinar encara més les característiques seleccionades mitjançant tècniques de visió, per preparar-les per al reconeixement. La visió per computador és un dels camps més utilitzats per a l'extracció de característiques per l'enorme potencial que ofereix, i les tecnologies biomètriques en són un exemple clar: són poques les biometries que no fonamenten els seus algorismes en la captura, el processament i la classificació de característiques visuals. Per a aquest exemple podem utilitzar tècniques clàssiques de morfologia que detectin els contorns principals de la imatge, per exemple, els **mètodes de Sobel** o de **Canny**, que també solen utilitzar-se per a les biometries de l'iris i de l'empremta dactilar.

Processament de les característiques discriminants a partir d'imatges on s'ha aplicat un mètode de detecció de contorns

Cal trobar una nova representació de les característiques que deixi constància clara de la diferència entre classes.

Les imatges binàries obtingudes semblen estar més a prop d'una quantificació numèrica que ens permeti discriminar les classes. Poden existir multitud de característiques vàlides per a ajudar-nos a resoldre un problema de reconeixement concret.

En aquest cas, se'ns acudeixen dues:

- Utilitzar morfologia d'imatge per a comptar el nombre de regions connexes en imatges de bolet normalitzades a la mateixa àrea.
- Calcular el percentatge de variació vertical de píxels. Es pot estimar prenent la imatge de contorns $I_C(x, y)$, fent-ne la derivada vertical, sumant les contribucions en valor absolut i dividint-ho entre el nombre de píxels totals $\|I_C(x, y)\|$:

$$\% = \frac{\sum_{\forall x,y} \left| \frac{\partial I_C(x,y)}{\partial y} \right|}{\| I_C(x, y) \|}$$

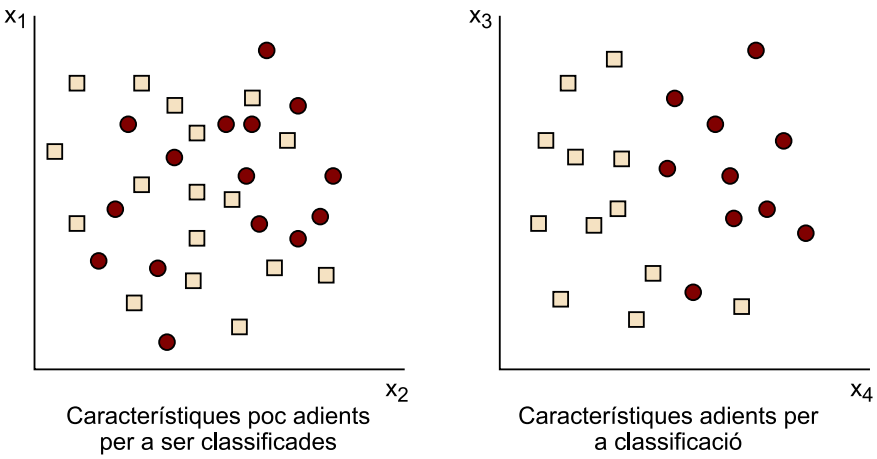
Agafant com a exemple les quatre observacions de bolets anteriors, cadascuna etiquetada com a classe *fredolic* o classe *lepiota*, el valors numèrics per a les dues característiques seleccionades són els següents.

	Fredolics		***Lepiotes***	
	Imatge 1	**Imatge 2**	**Imatge 3**	**Imatge 4**
Nre. regions connexes	33	38	192	262
% variació vertical	0,012	0,011	0,065	0,060

Podem observar que les dues característiques seleccionades semblen separar correctament les classes *fredolic* i *lepiota* a l'espai de característiques. Segurament ens decidiríem pel segon model, que té més coherència estadística en presentar propietats de probabilitat.

Tot i que hem aconseguit trobar característiques que discriminen entre les classes, a la pràctica aquest pas pot arribar a ser molt difícil d'assolir. Generalment, els algorismes de classificació que es veuran a continuació poden ser més robustos utilitzant diverses característiques combinades, i buscant models de decisió més adients a espais multidimensionals.

A l'exemple anterior es podria dibuixar la mesura escollida de *variació vertical de contorns* a l'eix horitzontal i, per exemple, una mesura de *croma* (color) *de les làmines* a l'eix vertical. Si les característiques no fossin gaire discriminants, per exemple, longituds i amplades en el cas dels bolets, ens trobaríem amb el cas de l'esquerra de la figura següent, on les observacions de cada classe queden barrejades a l'espai de característiques. En canvi, si són discriminants, l'espai resultant ens facilitarà separar entre classes en general (gràfic de la dreta de la figura següent).



No totes les característiques tenen el mateix poder discriminant, ni són igualment adients per a la classificació. A més, l'ús de diferents característiques combinades pot beneficiar la classificació.

2.2. Classificació

Seguint el cicle de disseny d'un procés de reconeixement, un cop escollides les característiques discriminatives (en l'exemple dels bolets, la *variació de píxels verticals*), cal **seleccionar un model de classificació** que primer aprengui regles a partir de les observacions disponibles, i que després decideixi de manera automàtica quina és la classe més adient per a una nova observació, desconeguda fins ara. En el nostre exemple, en observar la fotografia d'un nou bolet, el classificador decidirà si pertany a la classe *lepiota* o a la classe *fredolic*.

A grans trets, un **classificador** serveix per a trobar de manera òptima quina és la frontera entre les possibles classes a l'espai de característiques.

Exemple

Per exemple, en el cas anterior, si prenem com a característica la variació de píxels verticals, podríem escollir a ull un llindar proper a 0,040 per a decidir si ens trobem davant d'un *lepiota* o d'un fredolic, segons si el nou valor observat és més gran o més petit que aquest llindar.

No obstant això, per a crear models robustos, en primer lloc cal treballar amb un conjunt més gran d'observacions, de l'ordre de centenars o milers d'exemples etiquetats. A més, és molt més raonable escollir els llindars o les fronteres de classificació mitjançant mètodes d'aprenentatge automàtic, que generen models de decisió matemàticament òptims a partir del conjunt d'observacions.

Existeixen molts **mètodes de classificació** que ens permeten desenvolupar sistemes de reconeixement automàtic. Aquests mètodes es divideixen en tres grans tipus, segons com aprenguin a partir de les observacions:

- **Aprenentatge supervisat.** És el més comú. Es disposa d'un conjunt de dades d'entrenament, és a dir, a cada observació del conjunt s'ha assignat manualment una etiqueta de classe o un cost. Es poden enumerar moltes tècniques de classificació basades en aprenentatge supervisat, algunes d'elles són: els *k*-veïns més propers, les xarxes neuronals que utilitzen *back-*

propagation, les màquines de suport vectorial (SVM), els algorismes de *boosting*, o l'algorisme ID3 per a la construcció d'arbres de decisió.

- **Aprenentatge no supervisat.** El sistema agrupa les dades de manera automàtica (*clustering*), a partir de com estiguin distribuïdes a l'espai de característiques. Cada grup localitzat esdevé una classe, i aquesta assignació de classes es fa de manera automàtica. Alguns exemples d'aprenentatge no supervisat són l'algorisme *k-means*, les mixtures gaussianes (GMM) o les xarxes neuronals autoorganitzatives (SOM).

- **Aprenentatge per reforç.** No es dóna cap informació de classes de manera explícita, però un agent extern va comunicant al sistema si cada decisió presa és correcta o incorrecta, informació que el sistema utilitza per a millorar-ne les regles de decisió. Dos exemples clàssics d'aprenentatge per reforç són els mètodes de Montecarlo i l'aprenentatge per diferència temporal.

La selecció del tipus de classificació depèn de la naturalesa de cada problema, però en general, i particularment en el cas del reconeixement biomètric, ens trobarem majoritàriament davant de casos d'aprenentatge supervisat, on ens és possible "etiquetar" cada observació amb la classe que li correspon. Un cop escollit el tipus, un mateix problema es pot resoldre fent servir diferents models concrets.

Per exemple, en el cas del reconeixement facial (aprenentatge supervisat) és comú fer servir SVM, xarxes neuronals o *boosting*.

Tot seguit es descriuen molt breument alguns dels models de classificació supervisada més habituals:

- **Classificador lineal.** És un classificador binari que parteix l'espai de característiques en dues zones (per exemple, *lepiota* o fredolic), d'acord amb una sèrie de característiques observades (per exemple, textura del peu i color de les làmines). En un espai de característiques $\mathbb{R}^2$ es tractaria d'una recta, en $\mathbb{R}^3$ d'un pla, etc.

- ***k*-veïns més propers** (*k-nearest neighbors*, kNN). És un dels mètodes més simples de classificació a partir d'un conjunt d'entrenament etiquetat. Un objecte nou es classifica d'acord amb el vot de la majoria: se li atorga la classe/etiqueta més comuna entre els *k* veïns etiquetats que li són més propers a l'espai de característiques.

- **Regressió logística**. Descriu les relacions entre una sèrie de variables independents, com ara alçada, pes, sexe, etc., i una resposta binària de sortida, expressada en forma de probabilitat (per exemple, "té problemes de

sobrepès?"). S'utilitza la funció logística $f(x) = 1/(1+e^{-x})$ per a modelitzar la probabilitat de sortida com a combinació lineal dels paràmetres d'entrada.

- **Classificador bayesià ingenu (*naive*)** . És un classificador basat en el teorema de Bayes, on el model se simplifica suposant independència entre totes les variables. D'aquesta manera, les probabilitats condicionals es transformen en productes de probabilitats que resulten en càlculs molt més senzills.

- **Arbres de decisió** (o de classificació). Prediuen la classe a la qual pertany una observació en funció dels atributs observats. A partir d'un node inicial el model es pregunta sobre algun dels atributs en particular, i depenent de la resposta, condueix a través de les branques a un node de sortida (cadascuna de les fulles), que correspon a la classe assignada. Les "preguntes" que cal fer sobre els atributs s'escullen seqüencialment fent servir criteris com ara mínima entropia. **Xarxes neuronals (artificials).** Aquest model de classificador s'inspira en la naturalesa de les xarxes neuronals biològiques. Cada neurona es modelitza com una funció senzilla de resposta no lineal, i un nombre considerable d'aquestes neurones s'organitzen en una xarxa de capes interconnectades massivament. La fase d'entrenament consisteix a estimar el pes assignat a cada connexió, a partir dels atributs d'entrada i els valors de sortida. Per a fer-ho s'utilitzen algorismes com ara *backpropagation*.

- **Màquines de suport vectorial** (*support vector machines*, SVM). Són mètodes de classificació binària que, com els classificadors lineals, busquen la frontera que maximitza la separació entre dues classes. Els SVM, però, es basen únicament en els punts més propers a la frontera (els anomenats *vectors de suport*), que són els més crítics a l'hora de decidir-se per una categoria o una altra. Els SVM permeten transformar les dades inicials en nous espais on les classes siguin més separables, per mitjà de les anomenades *funcions de nucli* (*kernel*).

Exemple

En l'exemple dels bolets, com que en principi faríem servir una única característica per a classificar, serien models adequats el classificador lineal, els *k*-veïns més propers o els SVM.

Per a **entrenar** i **avaluar el classificador** obtingut, el més habitual és tenir un gran conjunt de dades etiquetades, i separar-les en una part destinada a l'aprenentatge del classificador (*training*) i una part destinada a verificar-les (*test*). Les proporcions de *training-test%* solen anar del 50-50 % al 70-30 % del total de dades etiquetades. L'aprenentatge es realitza fent servir el conjunt de *training*, però cada model de classificació segueix un procediment propi per a entrenar-se. Posteriorment, el classificador après s'utilitza per a classificar les mostres de *test*, de les quals ja tenim etiquetes vertaderes. Finalment, es comparen les etiquetes vertaderes amb els valors decidits pel classificador. Aquest procés ens informa de com de bé generalitza el classificador que s'ha escollit.

Utilitzar moltes característiques no sempre millora els resultats de la classificació. Al contrari, en tenir més característiques és més possible (i) que algunes d'elles no siguin confiables, (ii) que hi hagi dependències entre elles i només

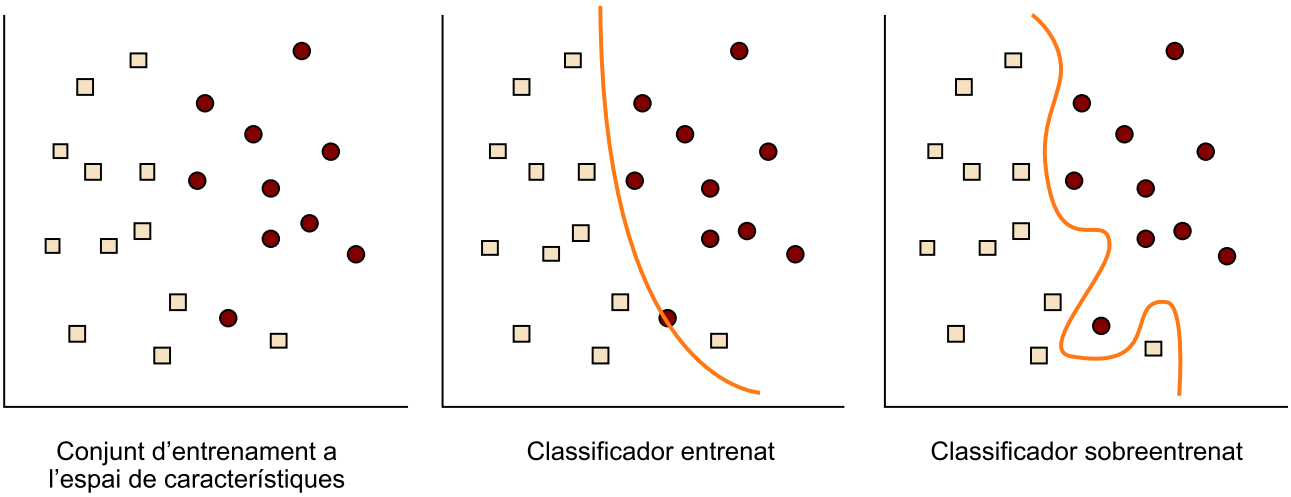
creïn complexitat (per exemple, l'alçada d'una persona i la longitud de la seva mà solen ser informacions redundants), (iii) que s'incrementin els costos d'adquisició de les dades, (iv) o que hi hagi més soroll a les dades mesurades.

En general, el nombre de mostres necessàries per a entrenar correctament un classificador creix exponencialment amb la dimensionalitat (nombre de característiques escollides). Això es coneix com a ***maledicció de la dimensionalitat*** o *efecte Hughes*.

Si es fan servir regles de decisió més sofisticades les fronteres entre classes s'adaptaran millor a les dades, com s'observa a la figura següent. No obstant, això pot conduir a l'efecte conegut com a ***sobreajustament*** (*overfitting*): el classificador s'adapta excessivament a les dades etiquetades, de manera que quan se li presenten noves dades per classificar, s'equivoca molt més que si hagués utilitzat regles més simples, que generalitzen millor.

Evitar el sobreajustament

El sobreajustament pot evitar-se amb tècniques com la regularització de dades o el *cross-validation*.



L'adaptació excessiva al conjunt de dades d'entrenament acaba produint sobreajustament, perjudicial per a la classificació.

2.3. Fusió de biometries

Els sistemes biomètrics unimodals, és a dir, basats en una única modalitat biomètrica, es veuen considerablement limitats per defectes d'unicitat, d'universalitat i per la presència de soroll a les dades, i sovint no assoleixen els nivells desitjats de precisió en aplicacions reals.

Diversos estudis coincideixen en el fet que els **sistemes multimodals**, que combinen adequadament diverses biometries, poden millorar-ne els resultats ostensiblement.

D'aquesta manera, combinant diverses biometries ens és possible aconseguir millors resultats conjunts i que el sistema final sigui més robust a interferents unimodals.

Per exemple, combinant biometries de cara i de veu es poden mitigar problemes de l'un i de l'altre, com efectes d'il·luminació adversos o soroll ambiental intens.

Cal dir, però, que les limitacions d'una de les biometries pot perjudicar les bonances que aportin les altres biometries al sistema final.

Per exemple, si combinéssim cara, veu i iris, la intrusió d'aquesta última tecnologia faria que es desaprofités la poca intrusió de les dues primeres.

Finalment, la multimodalitat millora clarament la resistència de l'aplicació davant la falsificació d'identitats per part d'impostors.

La fusió de biometries pot tenir lloc en diferents punts de l'arquitectura presentada, segons si es duu a terme a nivell de característiques (després de l'extracció), a nivell de puntuació (després de la comparació) o a nivell de decisió (després de la decisió final). A continuació es descriuen aquests tres tipus de fusió.

1) S'anomena **fusió a nivell de característiques** la consolidació de diversos vectors de característiques provinents de diferents captures biomètriques en un únic conjunt de dades, abans de passar-lo al classificador. Els vectors de característiques d'entrada poden provenir de diferents algorismes i modalitats, i no sempre és possible fusionar-los.

Per exemple, no es poden fusionar minúcies dactilars i coeficients d' *eigenfaces*, ja que les primeres tenen longitud variable que depèn de cada imatge, mentre que els segons tenen longitud definida. En canvi, sempre es poden fusionar vectors homogenis; per exemple, es pot fer la mitjana aritmètica de diverses mesures de la geometria de la mà, i també és possible concatenar vectors de geometria facial amb vectors de geometria de la mà.

Cal normalitzar els espais de característiques dels vectors que s'han de fusionar, fent que els seus rangs siguin similars. A més, és habitual recórrer a tècniques de reducció de dimensionalitat, especialment en el cas de concatenar múltiples vectors, ja que sovint tenir excessives característiques empitjora les prestacions del sistema.

2) D'altra banda, parlem de **fusió a nivell de puntuació** quan el que es combinen són les mesures de similitud, és a dir, les puntuacions obtingudes pels classificadors, per a cadascuna de les modalitats considerades.

Per exemple, la mesura global de similitud d'un sistema cara + veu podria ser la mitjana entre la mesura de similitud de cara i la de veu.

3) Finalment, la **fusió a nivell de decisió** consisteix a fusionar les decisions binàries (acceptar / refusar) de cadascuna de les biometries seguint una regla concreta.

En l'exemple del sistema cara + veu anterior, la regla podria consistir a acceptar l'individu sempre que la identificació de cara i la de veu siguin ambdues positives, és a dir, totes dues hagin reconegut l'usuari com a genuí.

Si bé és cert que els sistemes multimodals poden millorar les taxes de reconeixement en general, se sol **criticar** la fusió de biometries que incorporen biometries de tipus molt diferenciats, argumentant que una biometria robusta és més eficient utilitzada individualment que unida a altres biometries més febles. Per acabar, la creació de bases de dades multimodals és molt més complicada i costosa que la de modalitats úniques, i normalment consta d'un nombre molt limitat d'individus.

2.4. Mètriques d'avaluació

En condicions ideals, la fiabilitat dels processos biomètrics pot arribar a ser molt alta. No obstant això, les diferències entre modalitats biomètriques posen en relleu una sèrie d'avantatges i deficiències que les fan més adequades per a una o altra aplicació. En general, ens cal disposar de paràmetres que indiquin com de fiable pot ser una determinada biometria i que alhora ens permetin comparar una biometria amb les altres, per tal d'escollir la més adequada per a cada aplicació.

Una de les components d'error a què estan exposats els sistemes biomètrics és la **variabilitat intraclasse**, que fa que dues mostres biomètriques del mateix individu semblin força diferents i no s'apreciï una clara coincidència entre elles.

Els canvis d'entorn, la presència de soroll, un posicionament diferent del sensor o una mala interacció de l'usuari amb el dispositiu poden provocar variacions importants.

Per exemple, les diferents condicions d'il·luminació, orientació i expressió facial amb què es capturen diverses imatges de la cara d'una mateixa persona poden fer molt difícil la correspondència entre les característiques facials extretes.

D'altra banda, l'altra font fonamental d'errors és la **similitud interclasse** o entre membres de classes diferents, és a dir, la possibilitat que els patrons biomètrics de dos individus diferents presentin un alt grau de semblança.

Exemple

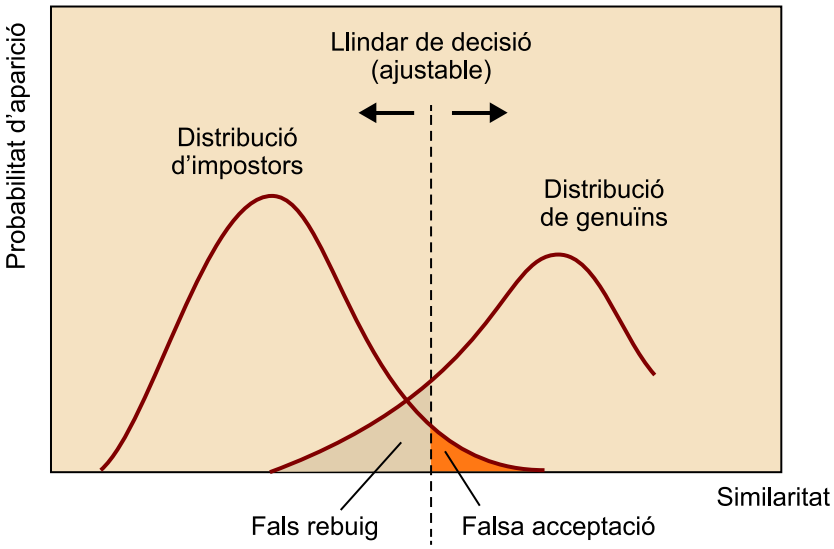
Seria el cas de persones amb cares similars, o fins i tot imatges sotmeses a condicionants similars, com per exemple portar un mateix tipus d'ulleres o mirar cap a una mateixa direcció, cosa que augmentaria falsament el grau de coincidència entre les identitats.

Per les raons esmentades, és molt difícil que dues mostres biomètriques d'un mateix individu, fins i tot adquirides en condicions similars, siguin completament idèntiques. Per aquest motiu, els sistemes biomètrics estimen la coincidència de dues mostres biomètriques fent servir una **mesura de similitud**, generalment expressada per mitjà d'un sol número que quantifica com s'assembla la mostra biomètrica analitzada a la plantilla emmagatzemada a la

base de dades. Com més elevat és el valor d'aquesta mesura, més seguretat es té a afirmar la identitat de l'individu, i com més baix, més certesa es té per a rebutjar-la.

Si fem un nombre prou elevat d'experiments per a una determinada biometria, on extraiem característiques biomètriques d'una població i les comparem amb plantilles prèviament entrenades, obtindrem histogrames de puntuacions semblants als de la figura següent, on s'observen dues corbes. La de la dreta correspon als experiments de **genuïns**, és a dir, comparacions entre mostres d'un mateix individu, que resulten en alts graus de similitud. La corba de l'esquerra correspon als experiments d' **impostors**, on es creuen mostres de dos individus diferents que generen puntuacions habitualment molt baixes. La regió central de puntuacions correspon a casos on el sistema ho té més difícil per a decidir si la identitat és genuïna o impostora, per les fonts d'error abans esmentades. Per a forçar una decisió s'estableix un **llindar d'acceptació**, de manera que en aquells casos on la mesura de similitud superi aquest llindar, s'acceptarà la identitat de l'individu, i es rebutjarà en cas contrari. En fixar un llindar estem assumint una certa quantitat d'error (vegeu les zones ombrejades), on tractem impostors d'altes puntuacions com a genuïns (falsa acceptació o *false matching rate,* FMR), i els genuïns de baixa puntuació com a impostors (fals rebuig o *false non-matching rate,* FNMR). Aquest llindar es fa servir al mòdul de decisió.

Distribucions de mesures de similitud obtingudes en comparar parells de plantilles de la mateixa identitat (genuïns) i d'identitats diferents (impostors).



Depenent de l'aplicació, ens pot convenir fixar el llindar d'acceptació a valors més baixos o més alts.

Per exemple, en el cas d'instal·lar controls d'accés per a centrals nuclears (alta seguretat) ens interessa restringir fortament l'entrada a persones alienes i evitar falses autoritzacions, motiu pel qual establirem un llindar molt alt. En aquest cas, acceptaríem que en un moment donat el sistema invalidés un usuari autèntic i li fes repetir el procés per corroborar-ne la identitat. En canvi, si la intenció fos trobar una cara particular entre moltes hores de gravació de multituds (cerca forense), podem assumir un cert nombre de falsos positius als resultats, sempre que no es passi per alt la identitat que cerquem; en aquest cas escollirem un llindar força baix.

Els nivells de fals rebuig i falsa acceptació depenen de diversos factors, com ara la qualitat de les mostres rebudes pels sensors, el tipus de característiques biomètriques utilitzades, les prestacions de la biometria escollida, i el llindar d'acceptació establert. Com es pot veure a la figura anterior, amb el llindar es poden balancejar les proporcions de falsos rebutjos i falses acceptacions:

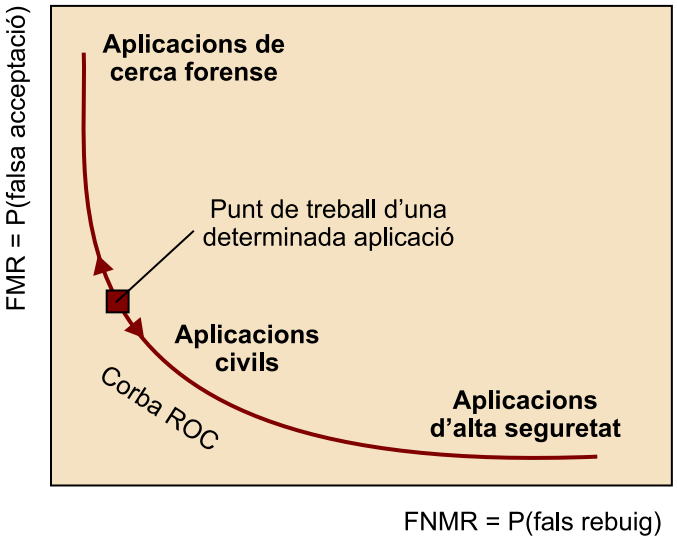
- Si abaixem el llindar per fer que el sistema sigui mes tolerant al soroll i a les variacions, la falsa acceptació creixerà.

- Per contra, si apugem el llindar per fer el sistema més segur, el que creixerà seran els falsos rebutjos.

Una opció molt comuna és situar aquest llindar al punt en què els histogrames de genuïns i impostors es tallen:

Aquest punt de treball s'anomena **EER** (*equal-error rate*), ja que té com a particularitat que les ràtios de falsa acceptació i de fals rebuig són idèntics.

La manera més comuna d'avaluar el nivells d'error d'una determinada tecnologia biomètrica és representar la seva **corba ROC** (*receiver-operator characteristic*). Aquesta corba s'obté dibuixant el fals rebuig del sistema en funció de la falsa acceptació, FNMR contra FMR, com es pot observar a la figura següent. També és habitual veure corbes ROC on es representa l'FNMR contra 1-FMR, i es veuria la corba capgirada verticalment. Com que ambdós errors depenen del llindar d'acceptació escollit, cada punt d'aquesta corba també correspon a un determinat llindar. Tal com es comentava anteriorment, l'elecció d'un o altre llindar es fa depenent del tipus d'aplicació final que es vol.



La corba ROC representa els possibles punts de treball del sistema, corresponents a diferents llindars d'acceptació. L'elecció del llindar depèn del tipus d'aplicació buscada.

Es poden comparar sistemes biomètrics visualment, dibuixant les corbes ROC de cada sistema als mateixos eixos de coordenades. Per a aplicacions convencionals, els punts òptims de treball són aquells que ofereixen baixes taxes d'ambdós errors al mateix temps. En cas de voler comparar sistemes biomètrics a partir d'una sola mesura, és habitual utilitzar el valor d'EER com a indicador per a resumir la fiabilitat del sistema. No obstant això, com que l'EER correspon a un únic punt de treball, aquesta pràctica fa que es perdi informació del comportament del sistema amb altres llindars d'acceptació.

És per aquest motiu que darrerament s'ha estès la utilització d'una altra mètrica, l'anomenada **AUC** (*area under curve*), que consisteix a calcular l'àrea sota la corba ROC com a indicador de l'error total comès pel sistema. De tota manera, és obvi que utilitzar una sola mesura de comparació sempre comporta una pèrdua d'informació respecte a la representació completa de les corbes ROC.

3. Anàlisi de les biometries principals

3.1. Reconeixement facial

L'observació de les cares és la forma més natural d'identificació personal a què estem acostumats en la nostra vida diària. Per tant, no és d'estranyar que, tot i les conegudes limitacions del reconeixement facial, aquesta sigui una de les biometries a les quals s'han destinat més iniciatives i recursos per a aconseguir sistemes que emulin o millorin la nostra capacitat biològica. Aquest fet ha potenciat enormement la **tecnologia d'identificació facial automàtica** durant els darrers anys i l'ha feta evolucionar des de l'ús de simples models geomètrics fins a la dependència amb processos complexos matemàtics de representació i classificació de dades.

La biometria facial és molt menys acurada que altres biometries com l'ADN, el reconeixement de l'iris, de la retina o de l'empremta dactilar. Encara que bàsicament tothom té una cara, la similitud entre cares de persones diferents pot arribar a ser molt alta[4], i hi ha diversos factors[5] que poden fer canviar substancialment dues observacions de la mateixa cara. Tot i així, és una biometria de gran utilitat per a una gran quantitat d'aplicacions, perquè entre els **avantatges principals** figuren:

(4)Per exemple entre bessons.

(5)Canvis d'edat, d'il·luminació, d'expressió, d'orientació o la variació de complements com ara cabells, barba o ulleres.

- És mínimament intrusiva.
- Pot fer identificacions a distància considerable.
- No requereix la col·laboració explícita de l'individu.

En resum, té una alta universalitat, les propietats d'unicitat i perdurabilitat són limitades, i la mesurabilitat pot passar de ser raonablement alta (en absència de dificultats) a força baixa (en cas de factors externs adversos).

Un dels **inconvenients principals** d'aquesta biometria és la facilitat d'elusió. La manera més senzilla d'evitar una identificació en aplicacions de videovigilància és la simple ocultació de la cara. A més, en aplicacions de verificació d'identitat, es poden aconseguir falses acceptacions amb l'ús de màscares o, en aquells sistemes sense detecció de cara viva, per mitjà de fotografies d'un individu validat. El fet que aquesta biometria tingui múltiples fonts de variabilitat també la fa més adequada per a aplicacions amb entorns controlats, com ara

controls d'accés, que no pas per a sistemes d'alta seguretat. No obstant això, entre les seves aplicacions també s'inclou la identificació en escenaris multitudinaris, com ara aeroports o estadis.

Finalment, la **percepció** d'aquests sistemes per part de la població sol ser més dolenta que la d'altres sistemes com ara l'iris o l'empremta, per la sensibilitat de la informació que representa una fotografia facial, i pel sentiment d'inseguretat que provoca a la població el poder sentir-se vigilat sense tenir-ne coneixement.

3.1.1. Normalització

La normalització facial és un pas important i sovint imprescindible, pel qual es localitzen un conjunt de punts prominents de la cara[6] que es fan servir per a transformar geomètricament les imatges de cara rebudes, i així col·locar-les en la mateixa posició i comparar-les posteriorment. Habitualment, aquestes transformacions es limiten a translacions, rotacions i escalats.

(6)Per exemple, els extrems dels ulls, les comissures de la boca, les narius o els cornets nasals, o la punta del nas entre altres possibilitats.

En tot cas, qualsevol preprocés o tasca de normalització facial comença per la **detecció automàtica de la cara** a la imatge de partida.

Els mètodes més adequats per a tal finalitat són les **cascades de classificació**. Aquestes cascades incorporen un conjunt molt gran de classificadors simples o "dèbils", com per exemple la diferència de dues àrees rectangulars de la imatge, que ens diuen quines regions són relativament més clares o fosques que d'altres. S'agrupen molts d'aquests classificadors dèbils en etapes seqüencials, de manera que si un sol dels classificadors falla, es descarta la presència d'una cara a la imatge. Quan es processen tots aquests classificadors dèbils de manera seqüencial al llarg de les etapes donen lloc a un classificador fort, que informa amb precisió de la presència o absència de la cara en una posició de la imatge. El procés es repeteix de manera exhaustiva per a totes les possibles posicions i escales considerades a la imatge d'entrada i dóna a conèixer totes les regions on és altament probable que hi hagi una cara.

3.1.2. Dificultats del reconeixement facial

A la pràctica, les imatges facials no es capturen en condicions ideals, sinó sotmeses a una gran quantitat de variabilitats, que inclouen:

- **Il·luminació.** Les condicions d'il·luminació són un dels problemes principals per al reconeixement facial, ja que suposen l'aparició de patrons que degraden les imatges originals, sobreposant-hi fortes ombres i reflexos depenent de la posició de la font o fonts de llum. Les característiques facials

subjacents són, doncs, o bé difícils de captar o bé es troben massa emfatitzades per culpa d'aquests patrons artificials.

- **Variacions posturals.** Com que les cares són objectes tridimensionals, és possible obtenir imatges d'una mateixa cara sota diferents vistes possibles, cosa que crea dificultats importants per traslladar la informació d'una vista a l'altra (per exemple, en comparar una cara frontal amb una de lateral). Sovint, aquest problema també comporta oclusions de certes parts de la cara.

- **Expressió.** El canvi d'expressió degut a la contracció d'alguns dels molts músculs facials dificulta l'alineament d'un conjunt de cares i la comparació, ja que es creen diferents aparences. Per exemple, no és trivial comparar cares amb expressions de sorpresa i de tristesa.

- **Oclusions.** L'altra causa principal de dificultat per al reconeixement facial és l'aparició d'elements que impossibiliten tenir una visió completa de la cara, ja sigui per elements externs a la persona o per peces de roba o complements (bufandes, ulleres normals i de sol, gorres), cabells llargs, etc. Aquests elements fan que la informació facial no estigui completament disponible per a l'algorisme de reconeixement, i que de vegades els continguts aliens de la imatge s'interpretin com a informació facial.

A més d'aquestes dificultats, el reconeixement facial també es veu fortament afectat per la variabilitat de la persona **al llarg del temps**: la presència de barba, el guany o la pèrdua de pes, la pèrdua de cabell, o l'aparició d'arrugues. Per fer front a totes aquestes limitacions, els sistemes actuals més sofisticats de reconeixement facial sovint incorporen tot un seguit d'etapes de preprocessament destinades a aconseguir invariància en termes d'il·luminació, rotació i expressió facial. Així doncs, s'empren les tècniques següents:

- **Tècniques fotomètriques** per a reil·luminar cares. Redueixen l'efecte d'ombres i reflexos i simulen millors condicions d'il·luminació.

- **Tècniques de projectivitat** per a transformar cares amb rotacions en vistes frontals.

- **Tècniques que transformen** cares amb expressions facials en cares d'expressió neutra.

Malgrat tot, és difícil que una solució que sigui capaç de resoldre tots els problemes a la vegada i per a tot tipus d'escenaris variables. En comptes d'això, és més habitual ajustar el sistema a condicions particulars d'ús, segons l'escenari que s'estigui tractant.

3.1.3. Mètodes de reconeixement facial

Principalment hi ha dos tipus de tècniques per al reconeixement facial.

- En primer lloc, les basades en l' **anàlisi local**, és a dir, en la posició i la forma de certs atributs facials (ulls, nas, boca, celles...) i com es relacionen entre ells.

- D'altra banda, trobem les tècniques basades en l' **anàlisi global** de la cara, que es representa com a combinació lineal d'elements d'una certa base que compleix determinades condicions.

Els primers mètodes de reconeixement facial daten del començament dels anys setanta, i es basen en la detecció automàtica de certs marcadors facials, com ara ulls, nas i barbeta, dels quals posteriorment s'extreuen **característiques geomètriques** creuades com distàncies, angles i àrees. Aquestes propietats esdevenen descriptors que posteriorment es comparen estre si per a establir la identitat de l'individu. Els mètodes estrictament geomètrics han demostrat no ser especialment acurats per al reconeixement facial. La informació extreta de marcadors facials no sembla ser per si mateixa suficientment discriminant per a aquesta tasca, i sovint es necessita explotar addicionalment l'aparença facial. Amb poques paraules: no n'hi sol haver prou amb dimensions i distàncies, sinó que també cal analitzar formes i textures.

Al començament dels anys noranta es van produir avenços significatius, especialment deguts a mètodes d'àlgebra lineal basats en l'**aparença global**, com ara *eigenfaces* i *fisherfaces*. Aquests mètodes operen sobre imatges de la cara de dimensions exactament iguals i perfectament alineades, és a dir, amb posició, rotació i escala iguals. Aquestes imatges se solen alinear de manera que els ulls i la boca dels usuaris coincideixin en posició espacial. Cada cara analitzada esdevé un llarg vector on s'inclouen ordenadament les intensitats lluminoses de cada píxel de la imatge; per exemple, concatenant totes les columnes d'una mateixa imatge en escala de grisos. D'aquesta manera, una imatge de 200 × 250 píxels en escala de grisos a 8 bits generaria un llarg vector de 50.000 elements, cadascun dels quals pren valors entre 0 i 255. Per aquest motiu diem que les imatges de la cara tenen una gran dimensionalitat, i que mostren informació redundant. En construir un conjunt suficientment gran de cares, l'ús de tècniques algebraiques de reducció de dimensionalitat com PCA (anàlisi de components principals, usat per a *eigenfaces*) i LDA (anàlisi linear discriminant, usat per a *fisherfaces*) ens permet trobar subespais vectorials de moltes menys dimensions.

Bàsicament, aquestes tècniques permeten convertir aquests llargs i redundants "vectors de la cara" en vectors equivalents que poden representar aquella mateixa cara amb molts menys elements, emfatitzant les característiques més significatives de cada cara.

Així doncs, tant la tècnica de PCA com la d'LDA tenen com a objectiu reduir les dimensions dels vectors facials expressats amb intensitats, tot i mantenint la informació particular de cada cara.

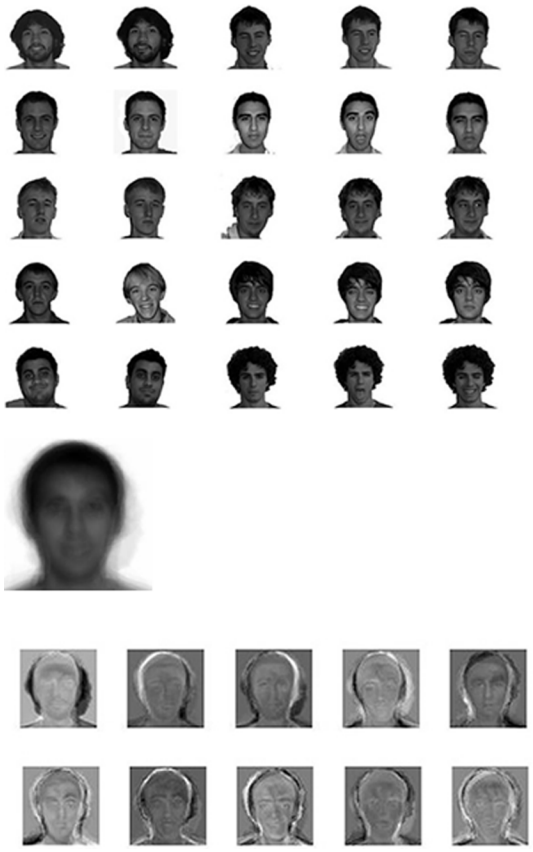
No obstant això, les dues tècniques operen de manera diferent: el **PCA** es concentra a trobar elements que representin òptimament (comprimeixin) les característiques facials, derivant en l'algorisme *eigenfaces*, que resulta molt adient per a comprimir informació facial. D'altra banda, la tècnica **LDA** no busca la representativitat, sinó la discriminabilitat de les dades; és a dir, es concentra a trobar els elements que siguin òptims per a distingir entre les cares de persones diferents.

LDA i PCA

Tot i que, per definició, LDA hauria de ser molt més valuós que PCA per al reconeixement facial, a la pràctica s'ha demostrat que això només succeeix quan es té un conjunt molt gran de dades d'entrenament, i que en entorns amb dades molt limitades és millor fer servir PCA.

Eigenfaces

Podem veure amb més detall el cas concret de les *eigenfaces* (mètode de PCA). Aquesta tècnica es desfà de la informació considerada inútil als vectors de la cara inicials i troba una nova base de vectors, les *eigenfaces*, que és ortogonal, és a dir, on els vectors es troben incorrelats entre si. D'aquesta manera, parlant a grans trets, aconseguim representar una cara inicial com a combinació lineal d' *eigenfaces*, on cada *eigenface* és un vector. A més, podem utilitzar els pesos d'aquesta combinació lineal (anomenats *coeficients d'eigenfaces*) com a representació comprimida de la informació facial. Per a fer-se'n una idea, comprimir acuradament una imatge facial per mitjà d'aquesta tècnica suposa una compressió de factor 1.000, aproximadament. Així doncs, en l'exemple anterior de la cara de 50.000 píxels, aconseguiríem una imatge qualitativament molt similar amb només 50 coeficients. A més, es pot comparar qualsevol imatge facial amb les cares presents a la base de dades, a partir de la distància existent entre aquests coeficients d' *eigenfaces*. Com més *eigenfaces* es consideren per a la nova base, més acurada serà la representació facial, però a la pràctica s'observa que per a més de 100 *eigenfaces* la diferència entre la imatge original i la reconstrucció és molt difícil de percebre.



Superior: exemples d'imatges facials alineades i normalitzades de la base de dades Rice. **Centre:** cara mitjana d'aquesta base de dades. **Inferior:**

les 10 primeres *eigenfaces* obtingudes, que caracteritzen els detalls més notoris de grups de cares característics respecte de la imatge mitjana. Font: Kochelek, Krueger, Robinson, Escarra, http://www.oercommons.org/courses/obtaining-the-eigenface-basis/view)

No-linealitat del reconeixement facial

Tot i el funcionament acceptable d'aquestes tècniques d'àlgebra lineal en condicions controlades, el problema de reconeixement facial és altament no lineal a causa del gran nombre de variacions d'entorn possibles com ara la il·luminació, l'orientació i l'expressió facial. El comportament de mètodes lineals és molt limitat quan apareixen aquests problemes. Per a solucionar-ho s'han proposat variacions d'aquests mètodes basats en mètodes de nuclis (*kernels*), que apliquen transformacions no lineals a l'espai de característiques per intentar linealitzar-les, i així s'han aconseguit tècniques com el *kernel PCA* i el *kernel LDA*.

Seguint la idea dels mètodes no lineals, trobem una altra família de mètodes molt populars per al reconeixement facial, els **EBGM** (*elastic bunch graph matching*).

L'EBGM consisteix a considerar la cara com una malla, on s'identifiquen una sèrie de marcadors de referència, com ara els ulls, el nas, la boca o el contorn de la cara, entre molts possibles.

La raó d'escollir aquests punts és que són relativament fàcils de localitzar, tot i que hi hagi canvis d'expressió o lleugeres variacions posturals. Aquests marcadors constitueixen nodes d'un graf, i per a cada node s'extrauen descriptors de la regió espacial on es troba el marcador en qüestió. Es pretén descriure la regió propera a cada marcador: els contorns, els canvis i els detalls que poden observar-se prop de cada marcador. Per a extreure aquesta informació és comú fer servir transformades *wavelet*, que són similars a la transformada de Fourier, però no solament produeixen dades en el domini freqüencial, sinó també en l'espacial; d'aquesta manera s'obté informació molt valuosa de la textura de cada zona, tant en amplitud com en fase. La similitud de dues cares s'avalua comparant la informació local de cada marcador, per a tots els marcadors localitzats.

Variants del mètode EBGM

Hi ha moltes variants d'aquest mètode, depenent dels marcadors escollits, del filtre o filtres *wavelet* utilitzats, del nombre d'escales freqüencials i espacials escollides, de la mètrica triada per a comparar les respostes dels filtres, i moltes més opcions pel que fa al disseny.

Finalment, una altra possible estratègia per a tractar les variacions no lineals de l'entorn i per a augmentar la capacitat de generalitzar dels algorismes de reconeixement és utilitzar models de classificació més sofisticats. Diverses tècniques de classificació s'han utilitzat per a aquesta finalitat amb resultats positius, com ara les **xarxes neuronals** i els **SVM** (màquines de suport vectorial), que es dissenyen específicament per a tenir en compte les propietats de les característiques facials. Des dels anys noranta han sorgit, i continuen sorgint, multitud de propostes diferents que utilitzen sistemes de classificació generalment molt complexos des d'un punt de vista matemàtic, dissenyats específicament per a solucionar problemes concrets d'aquesta biometria. A diferència d'altres biometries com l'iris o la veu, no sembla haver-hi un mètode clarament preferit per a la biometria facial, i el més normal és trobar variacions dels mètodes globals i locals descrits en aquesta secció que es diferencien per la manera precisa de tractar les dades.

El reconeixement facial ha experimentat una gran evolució durant els darrers anys, potenciat per les diverses avaluacions tecnològiques que han tingut lloc els darrers anys (FERET, 1993-1997, FRVT, 2000, 2002 i 2006, FRGC, 2004). Tot i això, encara requereix una millora important pel que fa a precisió d'identificació per a poder competir amb altres biometries com l'iris o l'empremta dactilar. La majoria dels sistemes comercials actuals de reconeixement facial es basen en la imposició d'un gran nombre de restriccions pel que fa a l'obtenció d'imatges, com la necessitat de cares molt frontals o d'il·luminació molt regular, cosa que fa que encara quedin passos per fer fins a aconseguir un sistema invariant a les causes principals de degradació d'identificació. Tot i això, aquesta biometria és enormement popular per la facilitat de captar les mostres biomètriques dels individus. D'altra banda, la seva implementació es veu afavorida pels avenços tecnològics en capacitat de processament i perquè en l'actualitat es poden adquirir fàcilment càmeres de qualitat cada vegada superior.

3.2. Reconeixement de l'iris

El reconeixement de l'iris ha esdevingut una de les modalitats biomètriques més populars i útils de les darreres dècades, especialment pel seu alt nivell de precisió per a la identificació personal.

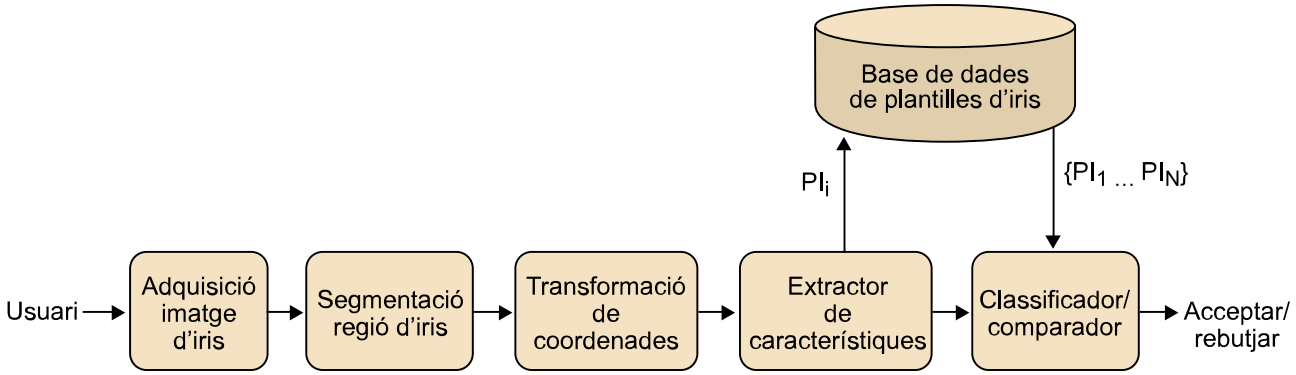
> Les característiques biomètriques utilitzades en aquest cas són els patrons texturals trobats a cadascun dels iris d'una persona.

L'aleatorietat dels patrons musculars de l'iris fa que es redueixi moltíssim la probabilitat de trobar dues persones que comparteixin les mateixes característiques, que alguns autors estimen d'una entre 10^{72}. D'altra banda, els patrons de l'iris es desenvolupen al vuitè mes de gestació, i romanen estables al llarg de la vida de la persona a partir d'aquest moment. La pròpia fisiologia de l'iris també contribueix a aquesta estabilitat, ja que l'iris es troba aïllat de factors externs gràcies a la còrnia. Tot això fa que la biometria de l'iris mostri millors propietats d'unicitat i perdurabilitat que la cara o la veu, i a més es consideri adequada per a utilitzar-se com a modalitat única. Addicionalment, tothom amb almenys un ull pot utilitzar aquesta biometria, fins i tot les persones cegues, de manera que la universalitat és destacable, i no és fàcil aconseguir enganyar un sistema d'aquestes característiques.

La mesurabilitat és lleugerament més complexa: tot i que el procés d'adquisició és senzill, ràpid i realitzable a certa distància, requereix una col·laboració mínima dels usuaris. Un dels inconvenients més importants d'aquesta biometria és l'alt cost que poden arribar a tenir els aparells de captura, tot i que amb els anys els costos segueixen decreixent. A més, els patrons de l'iris consten

d'estructures molt riques i complexes, que dificulten la tasca de dissenyar algorismes alternatius de reconeixement. L'elusió és difícil d'aconseguir, motiu pel qual generalment es considera una tecnologia segura en aquest sentit.

Arquitectura modular d'un sistema de reconeixement de l'iris



L'arquitectura típica d'un sistema de reconeixement de l'iris comença per l' **adquisició d'imatges** de l'ull on siguin clarament observables els patrons de l'iris.

Inicialment, la captura es feia a distàncies curtes i amb la participació de l'usuari, que havia d'evitar moure's durant el procés d'adquisició per assegurar la qualitat de les imatges obtingudes. La tecnologia recent, però, possibilita que aquestes imatges puguin capturar-se en moviment i a distàncies de fins a més d'un metre.

Generalment, les imatges no es capturen en **espectre visible**, sinó fent servir llum a freqüències properes a l'infraroig (*near-infrared spectrum*, **espectre NIR**), que és invisible a l'ull humà, i per tant més còmode per als usuaris. L'ús d'espectre NIR també permet veure estructures texturals molt més riques en els iris de colors foscos, i a més s'elimina en gran mesura la presència molesta de reflexos especulars a les imatges, que dificulten l'extracció d'informació. Tot i això, aquesta banda freqüencial no pot capturar certa informació cromàtica que prové de la melanina de l'iris, i a més els sensors infrarojos són molt més cars. Per aquests motius, i pel fet que les càmeres d'espectre visible han millorat molt durant els darrers anys, a l'actualitat encara coexisteixen els dos mètodes de captura, tant en espectre visible com en espectre NIR.

Els aparells de captura poden incorporar mecanismes per a detectar la presència d'ull viu; per exemple, variant la quantitat de llum projectada per l'escàner de l'iris i detectant la resposta de la pupil·la en dilatar-se. D'aquesta manera s'assegura que no es pugui falsejar l'accés mitjançant imatges de l'iris d'alta qualitat.

Un dels passos fonamentals per a l'extracció de plantilles biomètriques de l'iris és la **segmentació** de la imatge.

Aquest pas consisteix a analitzar la imatge capturada de l'ull per tal de localitzar la regió anular que conté l'iris, i alhora descartar la resta de zones.

Per a aconseguir-ho, el més habitual és tractar de localitzar les circumferències interior i exterior de l'iris, anomenades respectivament **contorn pupil·lar** i **contorn límbic**. Generalment, el contorn pupil·lar és més fàcil de trobar, ja que el contrast de la pupil·la és molt alt. Encara que hi ha diverses tècniques per a localitzar aquestes zones, les més comunes amb diferència són les següents:

- **El mètode integral-diferencial de Daugman.** Per a detectar circumferències a la imatge es fa una cerca exhaustiva, provant tots els orígens i tots els radis possibles, i veient si els continguts de la imatge coincideixen aproximadament amb la circumferència que es dibuixaria en cada cas. Així s'identifiquen les circumferències més clares de la imatge. També hi ha una variació d'aquesta tècnica per a detectar parpelles.

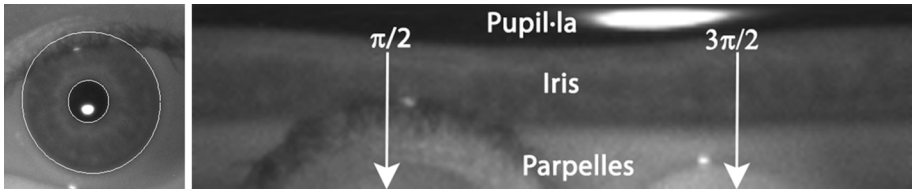
- **La transformada circular de Hough.** El mètode original de la transformada de Hough es fa servir per a localitzar les línies rectes predominants d'una imatge. En el cas de l'iris es fa servir una variació d'aquest mètode per a localitzar les circumferències més notòries de la imatge. També es pot fer servir per a detectar les parpelles, considerant radis molt més grans.

- **Els mètodes de contorns actius.** Tot i que els contorns de l'iris són pràcticament circulars, no tenen perquè ser cercles perfectes, especialment si l'ull no s'observa de manera completament frontal. Els mètodes basats en contorns actius o *snakes* situen inicialment una corba paramètrica a la imatge (en aquest cas, un cercle), i la van adaptant iterativament als contorns de la imatge. El resultat és que el cercle inicial es va apropant progressivament als contorns de l'iris fins a adaptar-s'hi perfectament. El problema principal d'aquesta tècnica és que depèn en gran mesura d'una bona posició inicial de la corba; altrament, pot convergir a resultats erronis. També és aplicable per a detectar les parpelles.

Partint del resultat de qualsevol d'aquestes tècniques, els contorns interior i exterior de l'iris i les parpelles superior i inferior poden localitzar-se de manera molt precisa. La segmentació pot millorar-se encara més trobant les parts de la regió anular envaïdes per altres elements, com ara reflexos lluminosos i pestanyes. Aquestes parts que amaguen la regió anular de l'iris es descarten durant l'extracció de característiques i es pren només la part d'imatge que ens interessa.

Un cop s'assoleix la segmentació de l'iris, la resta de passos fins a arribar a la identificació sol ser molt convencional i d'ús generalitzat. En primer lloc, s'acostuma a fer una **transformació dels eixos de coordenades** de la imatge, de cartesianes a polars, de manera que la regió anular s'acaba desplegant en una zona rectangular on l'eix horitzontal està format per angles i el vertical per radis.

Transformació de la imatge de l'iris, de coordenades cartesianes (esquerra) en polars (dreta).



L'eix vertical del nou espai representa el radi (incremental de dalt a baix) i l'eix horitzontal, els angles. La regió de l'iris és la banda central de contrast mitjà. S'hi pot observar la invasió de la parpella superior a $\pi/2$, que cal emmascarar.

Per a l'extracció de característiques se sol utilitzar encara avui la **tècnica d'*IrisCode*** proposada per Daugman, que caracteritza l'individu a partir de la informació de fase trobada a la banda de l'iris, que és molt més discriminant i invariant que la informació d'amplitud.

Per a obtenir la fase s'utilitzen les anomenades *wavelets de Gabor*, que localitzen informació tant al domini freqüencial com a l'espacial amb resolució òptima.

Transformada

Podem pensar en una transformada *wavelet* com una transformada de Fourier on el senyal que s'ha de transformar es multiplica per una funció harmònica i per una funció gaussiana. La informació de fase es guarda de manera binària (00, 01, 10, 11) d'acord amb el signes de les parts real i imaginària de la transformada *wavelet* i així es crea un mapa binari que es coneix com a *IrisCode*, i s'estandarditza a 256 bytes (2.048 bits d'informació de fase, partint de 1.024 píxels de la regió de l'iris). Aquests codis constitueixen en si mateixos una plantilla biomètrica de l'iris (PI).

Les plantilles biomètriques obtingudes són fàcils d'emmagatzemar, pel seu petit volum d'informació, i també es comparen entre elles de manera fàcil i ràpida. La **classificació** es pot dur a terme amb una simple instrucció XOR (OR exclusiu) sobre els dos codis binaris que s'han de comparar, amb la qual s'obté el nombre de bits diferents (distància de Hamming). Els bits diferents entre els totals donen una mesura de la similitud entre codis.

Fins a l'actualitat, el reconeixement de l'iris s'ha utilitzat principalment per a aplicacions de control fronterer, en substitució de passaports, i aplicacions d'alta seguretat, tot i que governs, aeroports i empreses privades n'estan incrementant i normalitzant l'ús progressivament. En l'actualitat s'estan posant en marxa diversos projectes de seguretat nacional a gran escala, com ara el projecte Aadhaar a l'Índia, que planeja recollir prop de 600 milions de plantilles facials, dactilars i de l'iris fins al 2014 per a documents nacionals d'identitat.

3.3. Reconeixement dactilar

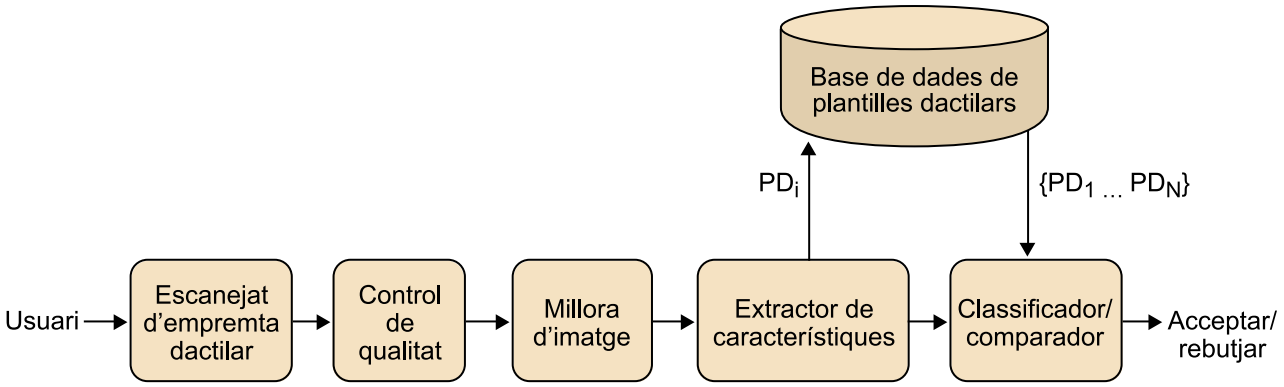
El reconeixement dactilar consisteix a identificar o verificar la identitat d'una persona a partir de l'anàlisi de les crestes dermals trobades a la punta d'un o més dels dits.

Aquestes crestes es troben representades per mitjà d' **empremtes dactilars**. A més de ser un dels procediments biomètrics més antics per a la identificació personal, el reconeixement dactilar és també el **mètode biomètric més implementat arreu del món** en l'actualitat.

La formació de les crestes i valls a l'epidermis de les puntes dels dits depèn tant de factors genètics com ambientals, i té lloc durant el desenvolupament embrional de qualsevol persona fins al setè mes de gestació, característica que fa que compleixi l'atribut d'universalitat. És igualment acceptada la unicitat d'aquesta biometria: circumstàncies com ara la posició del fetus durant aquests mesos condicionen aquestes característiques biomètriques, i fins i tot fan que les empremtes dactilars de dos bessons iguals siguin diferents. La perdurabilitat és molt més discutible: tot i que en principi les configuracions d'aquestes crestes es mantenen invariants durant la vida de la persona, els dits són molt més sensibles a alteracions físiques que altres parts del cos (iris, retina), en estar més exposats a marques d'accidents, com per exemple cicatrius o cremades.

Quant a **atributs desitjables**, hi ha hagut moltes discussions entorn de les possibilitats d'elusió dels mètodes de reconeixement dactilar. Hi ha diversos mètodes per a confeccionar falsos models de crestes dactilars en diversos materials (gelatina, plàstic, silicona) a partir de motlles, i fins i tot s'han donat casos molt més violents, en què bandes de lladres han arribat a seccionar un dit a persones autoritzades per accedir a automòbils de classe alta o zones d'alta seguretat. D'altra banda, l'acceptació de la tecnologia és limitada pel fet de ser una tecnologia de contacte, amb les reticències higièniques conseqüents.

Arquitectura modular d'un sistema d'identificació personal a partir de l'empremta dactilar



L'arquitectura d'un sistema de reconeixement d'empremtes dactilars conté els mòduls propis de qualsevol sistema biomètric, amb algunes variacions particulars.

En primer lloc, el dit de l'individu que s'ha d'identificar és escanejat mitjançant un sensor que **captura** una imatge digital de l'empremta dactilar. Aquesta imatge es codifica típicament en mapes de grisos a 8 bits de resolució, suficient per a poder contrastar adequadament els detalls de les crestes i valls de l'epidermis, que serviran per a caracteritzar l'individu.

Adquisició d'empremta dactilar de tipus espiral

Font: NIST (CC).

És molt habitual que els dispositius utilitzats per a la captura inicial incorporin mecanismes per a detectar intents de frau, fent servir tècniques com ara la **detecció de dit viu**. Aquests mètodes no solament són capaços de rebutjar imatges impreses d'empremtes i motlles sintètics de diversos materials; a més, poden arribar a detectar amb un alt grau de certesa que el dit presentat hagi estat tallat, pertanyi a una persona difunta o, fins i tot, que l'individu que intenta accedir es trobi sota una pressió emocional important. Per a fer-ho, poden mesurar-se diverses variables com ara la calor superficial, el moviment, la circulació sanguínia o la quantitat de proteïnes o de molècules odoroses presents a la mostra analitzada.

Mètodes més utilitzats per a detectar intents de frau

Els mètodes possiblement més utilitzats són la mesura de conductivitat i impedància elèctriques de la pell, i l'estimació de l'oxigenació sanguínia a partir de transmissions lluminoses (*oximetria de pols*).

La imatge de l'empremta dactilar adquirida pel sensor pot veure's fàcilment degradada per diversos motius.

> La mala col·locació del dit al sensor, un contrast d'imatge insuficient, la presència de brutícia, una humitat ambiental excessiva o l'aparició de distorsions de diversos tipus poden comprometre enormement la qualitat de la imatge obtinguda, i conseqüentment, deteriorar-ne el reconeixement.

En aquestes circumstàncies resulta indispensable incorporar un mòdul de **control de qualitat**, per a garantir que les imatges analitzades estan en condició de ser processades. La mesura de qualitat de la imatge s'obté a partir de l'estimació automàtica de paràmetres com ara la continuïtat i la uniformitat de l'estructura de crestes i valls, o el contrast de la imatge. Si la imatge analitzada no té suficient qualitat, es descarta i s'insta l'usuari a repetir la captura. D'altra banda, les imatges que passen el control s'envien a un mòdul de **millora d'imatge**, que filtra el soroll local de les regions que ho necessitin i incrementa la claredat de l'estructura global.

En segon lloc, el mòdul d' **extracció de característiques** analitza la imatge millorada resultant, en què l'estructura de crestes i valls ja és visiblement clara, i n'extreu les característiques biomètriques que s'utilitzaran per a caracteritzar l'individu. Generalment, les característiques que es poden extreure d'una empremta dactilar se situen a tres possibles nivells:

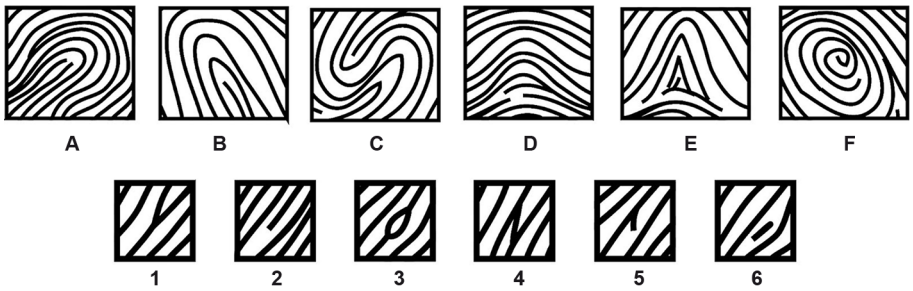
- Els patrons de flux macroscòpics formats per l'estructura de crestes.

- Les minúcies, punts singulars en què l'estructura de crestes i valls perd localment la regularitat. Els dos tipus bàsics de patrons minucials són la bifurcació i la finalització de crestes.

- Els porus de les glàndules sudorípares, i atributs de contorn de les crestes.

Els **patrons de flux** són determinats per la manera en què les crestes d'un dit s'agrupen les unes amb les altres i formen determinades estructures. La figura següent mostra les categories de patrons de flux més habituals (A-F): bucles, que poden estar orientats cap a la dreta (A), cap a l'esquerra (B), o ser dobles (C); arc normal (D) i arc en tenda (E); i espirals (F).

Categories principals de patrons de flux



(A) bucle dret, (B) bucle esquerre, (C) doble bucle, (D) arc, (E) arc en tenda, i (F) espiral. Les minúcies o irregularitats de cresta més habituals són: (1) bifurcació, (2) terminació, i altres tipus derivats d'ús comú: (3) llacuna o trau, (4) creuament, (5) agulló, (6) illa.

D'altra banda, les **minúcies** són les característiques més utilitzades en biometria dactilar, i formen el 80% dels punts singulars d'una empremta. Les dues categories bàsiques de minúcies són les bifurcacions i les terminacions de cresta, tot i que les aplicacions biomètriques solen utilitzar moltes més categories segons la topologia específica. S'han arribat a definir 52 tipus de minúcia diferents, dels quals els 6 presentats a la figura anterior solen ser els més utilitzats per experts en comprovacions manuals (1-6). Per a cada minúcia localitzada, l'extractor de característiques guarda el tipus i la posició i orientació relatives respecte de les altres minúcies de la mateixa empremta; per tant, les plantilles biomètriques de minúcies tenen mida variable. La interrelació geomètrica entre el conjunt de minúcies de dues mostres que s'han de comparar permet validar la identitat d'un individu, en cas de coincidència. A part d'aquestes minúcies, també se solen guardar el nombre de crestes tallades per la recta que

connecta dues minúcies, i els punts *core* i *delta*, punts de referència centrals i separadors respectivament, definits d'acord amb els patrons de flux anteriorment esmentats.

Finalment, a un nivell encara més detallat, trobem els **porus** i altres **atributs de contorn**. Els porus tenen una mida considerablement més reduïda que les minúcies, i no són apreciables en empremtes dactilars en tinta, sinó que es requereix l'ús d'escàners òptics. Entre els atributs de contorn se sol incloure informació relativa al gruix o la forma de determinades crestes, l'orientació o la freqüència local de crestes a cada regió de la imatge, o la localització de crestes incipients (aquelles molt primes i discontínues en alguns trams).

En tercer lloc, un cop extretes, les característiques dactilars escollides s'incorporen a una plantilla dactilar (PD_i), que caracteritza l'individu a partir d'aquests patrons. Tal com succeïa amb la resta de biometries analitzades fins ara, aquesta plantilla s'emmagatzema a la base de dades únicament en el cas d'enregistrar l'individu al sistema de reconeixement. En la resta de casos, aquesta plantilla obtinguda s'envia al **classificador**. Allà es compara o bé directament amb la plantilla de la identitat proposada, prèviament emmagatzemada, per tal de confirmar aquesta identitat (verificació), o bé amb cadascuna de les plantilles de la base de dades per a esbrinar la identitat de l'individu en qüestió (identificació).

Pel fet de ser la tecnologia biomètrica més implementada arreu del món, hi ha moltíssimes aplicacions que utilitzen reconeixement dactilar, des d'anàlisi forense fins a control d'accés per a treballadors, aeroports o agències governamentals. També es poden destacar els lectors d'empremta dactilar per a l'inici de sessions d'ordinador, control d'accés d'estudiants a escoles de primària al Regne Unit, préstec de biblioteques i virtualment qualsevol situació de verificació d'identitat.

3.4. Reconeixement del parlant

Les tecnologies de reconeixement del parlant[7] s'ocupen de reconèixer les persones a partir de les característiques de la seva parla.

(7)No s'ha de confondre amb el reconeixement de la parla, que no reconeix el parlant sinó allò que s'ha dit, independentment de qui ho hagi dit, i per tant no participa de la definició de biometria.

El reconeixement del parlant extreu i modelitza característiques acústiques de la parla per a diferenciar individus.

Observació

Per tant, és una de les poques biometries que no es basa en el processament d'imatge.

Les característiques de la parla d'un individu són condicionades per aspectes intrínsecs a la fisiologia, com ara la forma del tracte vocal, les cavitats nasals, la boca o els llavis, i per la manera en què tots plegats són utilitzats per l'individu per a generar un so (és a dir, l'estil de la parla i altres trets de comportament). Els condicionants fisiològics són invariants per a cada persona, cosa que no succeeix amb la vessant de comportament, que pot variar amb l'edat, l'estat

de salut, i fins i tot l'estat emocional de la persona en el moment de l'anàlisi. És per aquest motiu que la biometria de veu se sol considerar **a mig camí** entre les biometries físiques i les de comportament.

La precisió del reconeixement del parlant es considera mitjana, generalment no tan bona com la d'altres biometries. Això es deu a tres raons fonamentals:

- La presència habitual de soroll ambiental durant l'anàlisi del senyal sonor.
- L'alta variabilitat intraclasse: un mateix parlant canvia la veu per raons d'edat, malaltia o emoció.
- La baixa variabilitat interclasse: dues persones diferents poden tenir una veu molt semblant, especialment dins d'una mateixa família.

Així doncs, tot i que l'atribut d'universalitat és clar, els atributs de mesurabilitat, perdurabilitat i unicitat són més febles que el primer.

No obstant això, aquesta tecnologia té **altres punts forts** que la fan molt interessant per a determinades aplicacions biomètriques. La parla és una acció molt natural i senzilla, d'alta acceptació entre tota la població. A més, no és gens invasiva, ja que no es requereix contacte físic; de fet, es permet la identificació a distància dels usuaris per via telefònica. Finalment, el cost de la implantació és molt més barat que el d'altres biometries, punt que incrementa les seves prestacions tecnològiques. Es tracta d'una biometria que ha experimentat avenços científics constants durant els darrers 25 anys i per tant ha adquirit un alt grau de maduresa tecnològica. D'altra banda, es tracta d'una biometria cooperativa, ja que l'individu que s'ha d'identificar ha de produir activament els sons que l'identifiquin.

Hi ha dues **modalitats bàsiques** de reconeixement del parlant: amb **dependència** i amb **independència textual**, segons si el sistema coneix o desconeix *a priori* el text parlat per l'individu. Tot i que el contingut textual també es pot rebre mitjançant sistemes de reconeixement automàtic de parla, aquest procés està sotmès a errors, i se sol evitar quan es requereixen nivells més alts de seguretat. D'altra banda, es pot afegir un extra de seguretat a la modalitat dependent, fent que el text parlat per l'individu variï per a cada usuari del sistema (per exemple, usant com a text el número de carnet d'identitat, el codi d'usuari, o una paraula de pas).

La **parla** es produeix a partir de l'aire expulsat pels pulmons, que provoca la vibració de les cordes vocals quan aquestes es tensen, i posteriorment es modela per acció del tracte vocal (formada per les cavitats faríngia i bucal) i el tracte nasal (cavitat nasal). Particularment, el tracte vocal modela la parla a partir de la posició de la llengua, els llavis, el paladar i la mandíbula. La

vibració de les cordes vocals, localitzades a la laringe, produeix els anomenats *sons vocàlics*, formats per combinacions de senyals periòdics a determinades freqüències, que després ressonen als espais creats per les diferents cavitats. Quan les cordes vocals no es troben tenses en expirar l'aire, es creen els sons consonàntics, tant els fricatius com els oclusius. La concatenació progressiva de sons produïts per les diferents configuracions vocals al llarg del temps és el que genera el senyal de la parla.

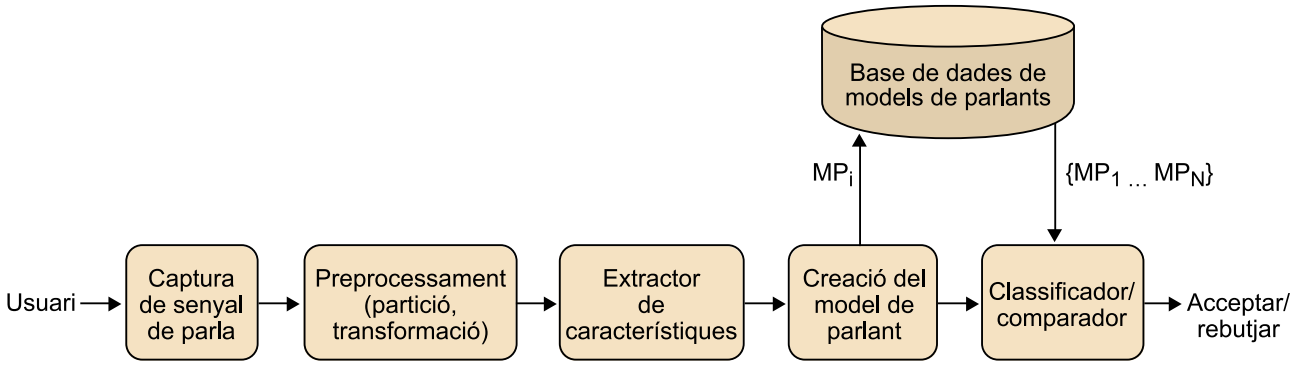
Així doncs, les **característiques pròpies del parlant** queden reflectides en aquest senyal de dues maneres diferents.

- D'una banda, a partir dels trets anatòmics, és a dir, la geometria i les dimensions de les cavitats i dels elements implicats en els tres tractes vocals, que determinen passivament els sons que es generen.

- D'altra banda, els trets de comportament com la velocitat i el ritme de parla, la prosòdia (variació de l'entonació), la dicció, les expressions utilitzades i les falques, entre moltes altres, determinen de manera activa la parla produïda.

En general, una característica robusta hauria de ser comuna i fàcil de trobar al senyal de parla, invariant durant la parla i difícil de falsificar. Però no es coneix cap característica de la parla que compleixi perfectament aquestes propietats, de manera que la informació que habitualment s'utilitza és l'anatòmica, que sol ser més fàcil d'extreure i de modelitzar. Concretament, se solen estimar paràmetres a partir de l' **espectre de la veu**.

Arquitectura modular d'un sistema de reconeixement del parlant



La **captura** d'un senyal de parla és fàcil de dur a terme utilitzant un micròfon convencional, o convertint a àudio digital el senyal rebut per via telefònica. Com és habitual amb qualsevol tecnologia biomètrica, abans de l'extracció de característiques cal dur a terme un preprocessament del senyal capturat. En el cas del reconeixement de parlant, es talla i enfinestra el senyal de la parla en finestres d'uns 20 mil·lisegons, i cadascun dels fragments es transforma en

(8)Aquest pas és similar al que fa l'algorisme de compressió JPEG sobre imatges, per a conservar la informació que millor es percep i descartar la resta.

domini freqüencial. També se sol filtrar cada fragment[8] fent servir un banc de filtres, per a ponderar els components freqüencials de manera que s'ajustin a l'escala de percepció humana (escala de Mel).

Finalment, pot ser necessari dur a terme algun processament addicional d'acord amb les imposicions del canal.

Exemple

Per exemple, la parla rebuda per via telefònica suposa alta variabilitat deguda al canal i una amplada de banda limitada.

La fase d' **extracció de característiques** sol emprar tècniques d'anàlisi cepstral, que també són molt utilitzades pels sistemes de reconeixement automàtic de la parla.

(9)És habitual obtenir coeficients cepstrals mitjançant tècniques com MFCC (*Mel frequency cepstrum coefficients*) o LPC (*linear predictive coding*).

A grans trets, cada fragment de senyal de veu enfinestrat es transforma en domini freqüencial, i l'envolupant de l'espectre s'aproxima per mitjà dels anomenats *coeficients cepstrals*[9].

Aquests coeficients es poden considerar similars als coeficients de les sèries de Fourier, que permeten aproximar funcions qualssevol, i on l'aproximació serà més precisa com més coeficients es facin servir. La diferència principal és l'ús de l'escala logarítmica per a tenir en compte el factor de percepció humana, descrit anteriorment.

A resultes de l'extracció, a partir d'un senyal de la parla s'obté una seqüència temporal de vectors de coeficients, on cada fragment ha originat un vector de coeficients cepstrals de mida fixa. Aquests conjunts de coeficients són les característiques biomètriques que serviran per a comparar i classificar els parlants.

Posteriorment a l'extracció, les característiques extretes es processen per tal de generar un **model de parlant** propi de cada usuari que participi al sistema.

Aquestes tècniques poden ser molt simples, com per exemple quantificacions vectorials o estadístiques de segon ordre, però és normal utilitzar mètodes d'aprenentatge automàtic més sofisticats i robustos, com mixtures gaussianes (GMM), xarxes neuronals, models ocults de Markov (HMM) o màquines de suport vectorial (SVM).

La tècnica més utilitzada per a aquest problema són sens dubte les **mixtures gaussianes**, que permeten aproximar qualsevol funció de densitat de probabilitat mitjançant un nombre predefinit de mixtures gaussianes, cadascuna definida únicament pel vector de mitjanes i la matriu de covariàncies corresponents. Això fa que el model resultant sigui senzill i fàcil d'emmagatzemar.

La **classificació** final del parlant es fa comparant la funció de probabilitat del model obtingut amb cadascun dels models ja enregistrats a la base de dades. Es fa servir un criteri de màxima versemblança, és a dir, s'escull quin dels models

de probabilitat guardats explica millor les observacions d'entrada. Els models de parlant guardats poden ser fàcilment actualitzats a partir de noves mostres biomètriques de parla, cosa que és molt convenient si tenim en compte la variabilitat temporal de la veu.

Les aplicacions del reconeixement automàtic del parlant són principalment quatre:

- Identificació
- Verificació
- Seguiment
- Diarització

Les dues primeres són les pròpies de qualsevol tecnologia biomètrica, però tenen l'avantatge de poder garantir la verificació d'identitats pràcticament des de qualsevol lloc, amb l'ajuda d'un telèfon mòbil o d'Internet. Són aplicacions comunes l'accés a comptes bancaris i sistemes financers, la compra telefònica, o el reinici periòdic de paraules de pas per a treballadors. D'altra banda, les dues darreres aplicacions tenen sentit en casos de múltiples parlants en una mateixa gravació. El seguiment de parlant consisteix a identificar els moments en què una determinada persona està parlant dins del grup. De manera més general, la diarització de parlants identifica i segmenta els moments d'una gravació en què parlen cadascun dels integrants d'una conversa de grup.

3.5. Altres biometries

Hi ha tot un seguit de tècniques biomètriques diferents de les ja descrites. Aquestes, ja sigui pel fet d'estar encara en fase experimental o bé perquè resulten molt més inaccessibles que les anteriors, encara són lluny de la comercialització, i no són considerades estàndards pels experts del sector. Destaquem les següents:

1) Empremta genètica (ADN)

Cada cèl·lula del cos humà conté una còpia de la cadena d'ADN que codifica la informació d'una persona. Tot i que la majoria d'aquest ADN és idèntic entre dues persones qualssevol, un 10% de la cadena és únic per a cada individu (excepte en el cas de bessons idèntics), altament variable i s'anomena *seqüència minisatèl·lit*. La tècnica d'anàlisi d'ADN, també anomenada *empremta genètica*, consisteix a comparar directament dues mostres d'ADN d'un mateix individu, de manera que per a aquesta biometria no s'extreuen plantilles biomètriques. Com que no totes les etapes del procés estan automatitzades, i alguns dels passos necessaris requereixen processos químics complexos, en l'actualitat l'anàlisi genètica es restringeix a aplicacions forenses. Tot i que possiblement és la biometria més robusta en l'actualitat, també presenta els greus inconvenients de ser altament intrusiva, de no operar en temps real,i de ser molt susceptible a qüestions de privacitat, ja que revela condicions genètiques dels usuaris. A més, és relativament fàcil aconseguir mostres genètiques d'altres usuaris amb finalitats fraudulentes. Per exemple, simplement obtenint un cabell de la persona, sempre que incorpori el fol·licle capil·lar de l'arrel.

2) Retina

La retina és un teixit fotosensible que se situa a la superfície interna de l'ull, on es projecta la llum provinent de l'exterior. Després d'una sèrie de processos electroquímics, la retina transmet al nervi òptic informació per recrear la imatge que li ha estat projectada. La retina humana està coberta per una gran quantitat de vasos sanguinis que estan disposats de manera diferent a cada persona, característica que esdevé la clau d'aquesta biometria. Els escàners de retina apliquen una font de llum coherent de baixa intensitat per il·luminar aquests vasos sanguinis i obtenir-ne una fotografia de la distribució, que posteriorment es compara amb altres plantilles d'imatges emmagatzemades a la base de dades. Els sistemes de reconeixement de retina s'utilitzen des de la dècada dels anys setanta, especialment per a aplicacions d'alta seguretat com ara les de caire militar, a causa de l'alta precisió que proporcionen per a tasques de verificació d'identitats. Com a contrapartida, l'anàlisi de la retina és extremadament invasiva i més lenta que no pas altres tecnologies com ara l'anàlisi de l'iris o l'empremta dactilar.

3) Termografia facial

S'empren càmeres infraroges per a detectar els patrons de calor creats per les ramificacions de les venes sanguínies pròpies de cada persona, anomenats *termogrames*. Aquesta biometria no invasiva té molts paral·lelismes amb el reconeixement facial, tot i que, al contrari d'aquest, la termografia facial és independent de les sovint difícils condicions d'il·luminació ambiental. Malgrat això, la comercialització inicial no ha estat possible pel cost tan elevat de la implementació, principalment per l'alt preu de les càmeres tèrmiques o termogràfiques que s'hi empren.

4) Geometria de la mà

La base d'aquesta biometria és la comparació d'un conjunt de distàncies i dimensions mesurades a partir d'una imatge de la mà, com ara la mida global, la longitud de cada dit, la posició de les unions o la forma. La simplicitat la fa una tecnologia barata i fàcil d'aplicar, i a diferència de l'empremta dactilar, no es veu perjudicada pels canvis de temperatura o humitat de la pell. Tot i això, les característiques biomètriques emprades no són gaire distintives, la geometria és variable durant l'etapa de creixement, i les imatges poden contenir elements de distorsió com ara anells o polseres. En conseqüència, es poden obtenir alts nivells d'error en conjunts grans d'usuaris.

5) Signatura

Està generalment acceptat que la manera en què una persona signa el nom és una característica pròpia d'aquesta persona. Es tracta d'una biometria de comportament, i per tant es veu afectada per condicionants externs de l'individu a l'hora de fer la signatura, tant físics com emocionals. A més, es requereix la

cooperació de l'usuari, a diferència d'altres biometries com ara el reconeixement facial. Un altre dels punts febles és la possible variabilitat de la signatura al llarg de la vida d'una persona. Un sistema de reconeixement de la signatura és capaç de mesurar altres paràmetres a més del nom signat i la rúbrica, com per exemple la pressió exercida i la velocitat instantània amb què l'usuari l'executa, si es disposa d'un sensor adequat.

6) Patrons cutanis

La pell d'una persona es caracteritza i distingeix pel gruix de les diferents capes, la pigmentació, la densitat de col·lagen i d'altres proteïnes, l'estructura subjacent de capil·lars, etc. El reconeixement de patrons cutanis analitza l'espectre característic de la pell d'un individu per mitjà de tècniques espectroscòpiques, treballant amb llum visible i infraroja reflectida per la pell. Es tracta d'una biometria emergent.

7) Anàlisi de la marxa

L'estudi espaciotemporal de la manera en què una persona camina és complex, ja que la marxa pot modificar-se al llarg del temps a causa de lesions, canvis de pes o alteracions temporals de la conducta, i no és excessivament distintiva entre individus. Tot i això, aquesta biometria de comportament és acceptable per a la verificació en condicions de baixa seguretat, principalment perquè pot operar a distància i les mostres de vídeo són fàcils i barates d'obtenir. Per a fer la verificació s'arriben a tenir en compte diversos factors, com ara la velocitat, la cadència, la longitud i l'amplada del pas, o les mitjanes dels angles a les diferents articulacions. El seu ús també arriba a aplicacions no biomètriques, com ara diagnòstic mèdic o modelització virtual de moviment humà.

8) Olor corporal

Aquesta biometria es basa a capturar substàncies químiques volàtils emeses pels porus cutanis. Encara es troba en fase experimental per la gran quantitat de dificultats associades, com ara la presència de contaminants externs (per exemple, olors intensos de perfum o tabac), el fet que l'olor d'una persona pot ser molt menys distintiu que el d'una altra, i la possibilitat que aquesta olor variï significativament al llarg del temps per factors dietètics o fisiològics, entre d'altres.

9) Llit unguial

El llit unguial és una estructura longitudinal formada per fileres de pell pràcticament paral·leles i riques en patrons vasculars, unides a estructures dèrmiques per mitjà de canals molt estrets. La biometria de llit unguial escaneja aquestes

estructures presentades per la pell sota les ungles dels dits, i posteriorment es tracten aquestes dades de manera similar a com operen la resta de biometries basades en patrons vasculars.

4. Aplicacions principals

Les aplicacions industrials, comercials i quotidianes de la biometria continuen estenent-se dia rere dia arreu del món. Actualment, podem classificar les aplicacions principals de la biometria en el seguit de blocs temàtics que trobem a continuació.

1) Control d'accés físic

Engloba tots els mecanismes destinats a autenticar la identitat d'una persona en una localització de control mitjançant l'anàlisi de les característiques biomètriques. Per a aquestes aplicacions, la falsa acceptació i fals rebuig s'ajusten a nivells especialment baixos, i per a aconseguir-ho es treballa en entorns controlats d'il·luminació i distància. Entre les biometries més utilitzades per al control d'accés es poden destacar l'empremta dactilar, la cara i les venes del palmell de la mà, i les aplicacions típiques inclouen zones segures de bancs, hospitals, edificis policials o militars i caixers automàtics. No obstant això, la ràpida adopció de les tecnologies biomètriques permet fer pensar a curt i mitjà termini en nous escenaris de control d'accés, com ara identificar alumnes a l'entrada de les escoles o engegar de manera personalitzada un automòbil.

2) Control fronterer i aeroports

Aquesta aplicació utilitza tecnologies biomètriques d'autenticació per a regular o monitorar el trànsit massiu de persones que entrin o surtin de les fronteres d'un país. Generalment, aquests sistemes de base biomètrica van lligats a sistemes de reconeixement de documents (per exemple, passaports i carnets d'identitat). També se sol treballar amb sistemes globals distribuïts capaços d'identificar individus inscrit en bases de dades internacionals. Les tecnologies més utilitzades solen ser l'iris, l'empremta dactilar i la verificació vascular.

3) Videovigilància

El reconeixement facial pot fer-se a distància, sobre múltiples usuaris i sense intervenció ni coneixement d'aquests, fets que el converteixen en una tecnologia idònia per a la identificació d'individus en espais multitudinaris. Tot i que se sol connectar la videovigilància amb la identificació de llistes negres (individus sospitosos o amb altres connotacions negatives), també és habitual utilitzar aquests sistemes per a la identificació de llistes blanques, com ara el reconeixement instantani de clients importants o personalitats d'interès. D'altra banda, són importants les aplicacions d'anàlisi forense, que permeten

rastrejar fora de línia (*offline*) hores de contingut audiovisual i metratge capturat amb càmeres de vigilància, per exemple per a la identificació d'individus lligats a actes vandàlics o la cerca massiva de persones.

4) Control d'accés lògic

Es busca restringir electrònicament l'accés a arxius de dades i l'execució de determinades aplicacions a aquells usuaris que tinguin l'autoritat per a accedir a tals serveis. D'aquesta manera s'elimina la dependència tradicional de mots de pas o PIN i a més es possibilita l'enregistrament dels intents d'accés i la informació biomètrica de qui ha intentat accedir. Té una aplicació especial en el camp de seguretat a la Xarxa, ja sigui per a compres en línia (*online*) o per a transaccions bancàries.

5) Justícia i ordre públic

La biometria té clares aplicacions legals i policials, d'entre les quals podem emfatitzar els programes nacionals de gestió de la identitat (és el cas de passaports i documents d'identitat biomètrics), la investigació d'escenes de crim, l'accés a documents oficials i l'administració de presons. Les tecnologies biomètriques més comunes per a aquestes aplicacions són l'empremta dactilar, la cara i la veu.

6) Registre d'entrada

L'ús de la biometria és també comú en empreses d'envergadura, especialment per al control d'assistència al lloc de treball, amb vista a agilitzar el procés de registre i evitar el préstec, el robatori o l'ús fraudulent de targetes d'identificació. Es tracta d'un tipus de control d'accés físic, que sol incloure restriccions horàries (per exemple, deixant entrar personal només en horari d'oficina), i sol proporcionar informació estadística, com ara quantes hores de feina setmanals porta cada treballador, quines són les hores de trànsit més alt, o bé quanta gent encara roman a l'interior de l'edifici en cas d'una evacuació d'emergència. El mètode més utilitzat és l'empremta, tot i que també s'empren el reconeixement facial, de l'iris, de la veu i de patrons vasculars de la mà.

7) Sanitat / assistència sanitària

Les aplicacions sanitàries de la biometria inclouen l'accés a historials i diagnòstics mèdics personals (un tipus de control d'accés lògic), i l'associació de nadons amb les mares, per a evitar intercanvis accidentals d'infants.

8) Seguretat en finances i transaccions (telecompra)

Les transaccions financeres i la compra d'articles per via telefònica o per Internet, mitjançant veu sobre IP, també poden beneficiar-se de capes addicionals de seguretat durant el procés de verificació d'aquest tipus d'operacions. La bi-

ometria més adequada en aquest cas és la de veu, que resulta molt barata ja que tots els telèfons i la majoria d'ordinadors incorporen micròfons. Aquesta tecnologia sol complementar-se amb altres tipus de protecció com ara paraules de pas o codis d'identificació.

9) Biometria mòbil

De la mateixa manera que algunes biometries (cara, empremta dactilar) s'han introduït amb facilitat al mercat dels ordinadors portàtils per a proveir serveis de control d'accés lògic, també s'està observant aquesta tendència en el cas de telèfons intel·ligents (*smartphones*) i altres dispositius mòbils. També hi ha importants aplicacions per a la identificació a distància mitjançant la biometria de veu. Per tant, aquest conjunt d'aplicacions és un tipus de control d'accés lògic que sol estar preparat per a transaccions comercials segures.

10) Màrqueting i anàlisi de mercat

Les tecnologies d'anàlisi facial poden utilitzar-se no solament per a la identificació personal, sinó també com a mitjà per a seleccionar automàticament els anuncis en funció del tipus d'audiència observada (basant-se en paràmetres com el sexe o l'edat), per a identificar l'interès dels clients davant de certs productes, i per a proveir estadístiques dels diferents segments de població observats en localitats concretes dels comerços o botigues.

A banda d'aquestes aplicacions genèriques, hi ha un gran nombre de grans projectes biomètrics en diferents països d'arreu del món, especialment pel que fa a programes nacionals de gestió identitària (a Alemanya, Austràlia, el Brasil, el Canadà, els Estats Units, l'Índia, l'Iraq, Israel, Holanda, Nova Zelanda, Noruega i el Regne Unit, entre d'altres). La iniciativa biomètrica més important a l'actualitat és l'anomenat *Aadhaar* o *India's Unique Identification Project*, que pretén recollir 600 milions de registres d'empremtes dactilars, cares i iris de la majoria dels 1.200 milions d'habitants de l'Índia fins a finals del 2014.

5. Conclusions i reptes futurs

El fet de poder reconèixer la identitat d'una persona de manera confiable esdevé un problema de summa importància per a multitud d'escenaris de la societat actual: Finances, assistència sanitària, xarxes de transport, espectacles, seguretat i ordre públic, control d'accés, control fronterer, òrgans de govern o comunicació.

En aquest sentit, la biometria, que permet establir la identitat d'una persona a partir de trets personals distintius i de manera automàtica, té potencial per a convertir-se en una part essencial i irreemplaçable de les nostres vides.

Les característiques biomètriques no poden compartir-se ni traspaperar-se, i representen de manera íntegra la identitat de l'individu a partir de la fisiologia o el comportament. La connexió d'aquests trets a identitats establertes de manera externa comporta indubtablement enormes conseqüències, tant positives com negatives. Però utilitzades de manera prudent i racional, aquestes tecnologies poden conduir la societat a augmentar la seguretat, reduir el frau i millorar l'experiència d'usuari.

Les tecnologies biomètriques han de complir una sèrie de **condicions imprescindibles** per a poder ser implementades amb garanties:

- Universalitat
- Unicitat
- Permanència
- Mesurabilitat
- Dificultat d'elusió

No obstant això, hi ha **altres atributs desitjables** que reforcen la utilitat d'unes biometries sobre unes altres, com ara el baix cost, la usabilitat o l'intrusisme, la rapidesa i la senzillesa, la facilitat per a localitzar i consultar les dades emmagatzemades, el fet de gaudir d'acceptació i no tenir connotacions negatives, i el fet d'estar en mans d'organitzacions confiables, ja que les dades són susceptibles de ser utilitzades per a finalitats dubtoses. La comparació de característiques entre possibles biometries ens facilita la tasca d'escollir aquelles que millor s'adapten a determinades aplicacions o necessitats específiques.

Finalment, tot i que des de l'entrada a l' **era del processament digital** s'han efectuat enormes progressos en el camp de la biometria, encara a dia d'avui hi ha un nombre de reptes importants que innegablement en condicionen

l'evolució i la implantació futures, com assolir invariància de les característiques biomètriques amb les condicions de l'entorn, o aconseguir sistemes més robustos de detecció de vida en mostres biomètriques, per tal d'evitar casos de frau identitari (conegut com a *spoofing*).

Respecte a reptes de caire més sociològic, els problemes principals de les institucions relacionades amb la biometria són garantir la privacitat personal dels individus, i sensibilitzar la societat cap al vertader coneixement de les tecnologies biomètriques, per a facilitar-ne així la implantació.

Bibliografia

Ashbourn, J. (2000). *Biometrics: Advanced Identity Verification*. Lodres: Springer.

Beardsley, C. T. (1972). "Is your computer insecure?". *IEEE Spectrum* (vol. 9, núm. 1, pàg. 67-78).

Daugman, J. (2004). "How iris recognition works". *IEEE Trans. On Circuits and Systems for Video Technology* (vol. 14, núm. 1, pàg. 21-30).

Delac, K.; Grgic, M. (2004). "A survey of biometric recognition methods". *Proc. of the 46th IEEE Int. Conf. of Electronics in Marine* (pàg. 184-193).

Jain, A. K.; Pankanti, S.; Prabhakar, S.; L. Hong, Ross, A.; Wayman, J. (2004). "Biometrics: A Grand Challenge". *Proceedings of the 17th ICPR* (vol. 2, núm. 1, pàg. 935-942). IEEE.

Jain, A. K.; Ross, A.; Prabhakar, S. (2004, gener). "An Introduction to Biometric Recognition". *IEEE Trans. on Circuits and Systems for Video Technology* (vol. 14, núm. 1, pàg. 4-19).

Proença, H.; Alexandre, L. A. (2006, abril). "Iris segmentation methodology for non-cooperative recognition". *IEEE Proc. Vis. Image Signal Process*. (vol. 153, núm. 2).

Ross, A.; Jain, A. K. (2003). "Information fusion in biometrics". *Pattern Recognition Letters* (vol. 24, núm. 13, pàg. 2115-2125). Elsevier.

S. Z. Li; Jain, A. K. (2009). *Encyclopedia of Biometrics*. Springer-Verlag.

Sinha, P.; Balas, B.; Ostrovsky, Y.; Russell, R. (2006). "Face recognition by humans: Nineteen results all computer vision researchers should know about". *Proceedings of the IEEE* (vol. 94, núm. 11, pàg. 1948-1962). IEEE.

Sirovich, L.; Kirby, M. (1987). "A low-dimensional procedure for the characterization of human faces". *Proceedings of the IEEE* (vol. 59, núm. 5, pàg. 748-760).

The NSTC Subcommittee on Biometrics. http://www.biometrics.gov

Turk, M. A.; Pentland, A. (1991). "Face recognition using Eigenfaces". *Proc. IEEE* (pàg. 586-591).

Viola, P.; Jones, M. (2001). "Rapid object detection using a boosted cascade of simple features". *Proceedings of the IEEE*. CVPR.