Avaluació dels sistemes biomètrics en aplicacions reals

Francesc Serratosa

PID_00195431

Universitat Oberta de Catalunya

Índex

Introducció

L'objectiu final dels sistemes biomètrics és augmentar la seguretat d'altres sistemes.

Augmentar la seguretat d'altres sistemes

Si s'aplica un sistema d'identificació de persones per l'iris als aeroports és per augmentar la seguretat en un país. En aquest cas, "la seguretat al país" és el sistema en si del qual es vol augmentar la seguretat.

Per aquest motiu, és imprescindible garantir que el sistema biomètric en si sigui tan segur com sigui possible i tenir eines per a avaluar aquesta seguretat. En aquest mòdul explicarem les eines que s'han desenvolupat per mostrar la qualitat del sistema biomètric.

En aquest mòdul hem posat conjuntament l'avaluació dels sistemes biomètrics i l'exposició de diversos sistemes biomètrics reals. Això ha estat així per mostrar la importància que té aquesta avaluació amb els grans desplegaments. Aquestes aplicacions biomètriques de gran transcendència social, econòmica o política amb milions de persones involucrades no es podrien portar a terme si no fos per uns baixíssims errors biomètrics.

És clar que s'accepta basar la seguretat d'un sistema (per exemple, unes eleccions d'un president) amb un mètode biomètric si els errors del mateix sistema biomètric són molt inferiors a altres mètodes clàssics no automatitzats o semiautomatitzats.

Objectius

Els objectius d'aquest mòdul són explicar els errors que poden aparèixer en un sistema biomètric i també explicar els mecanismes que s'han plantejat per avaluar la bondat dels sistemes biomètrics. També es volen mostrar uns quants exemples d'aplicacions biomètriques reals i a gran escala, perquè pugueu assolir els objectius següents:

1. Classificar els errors que poden aparèixer en un sistema biomètric. I determinar en quines condicions apareixen aquests errors.

2. Avaluar una aplicació biomètrica per saber-ne la bondat. Conèixer les mètriques per avaluar i comparar la bondat dels sistemes biomètrics.

3. Conèixer uns quants exemples de grans sistemes biomètrics.

1. Errors dels sistemes biomètrics

La promesa en què es basa el reconeixement biomètric és que donada una mostra nova, el sistema biomètric ofereix sempre la decisió correcta, tant sigui en verificació (és o no és la persona) com en identificació (retorna la identificació de la persona). A la pràctica, un sistema biomètric és un sistema de reconeixement de patrons que inevitablement pren decisions incorrectes. Per això és fonamental entendre per què un sistema biomètric comet errors i modelar aquests errors per poder-ne conèixer la magnitud. I després discutir sobre quins tipus d'errors ens podem trobar.

Referència bibliogràfica

El tractament comprensiu del sistemes biomètrics està detallat en ISO/IEC 19795-2 (2007).

1.1. Raons dels errors dels sistemes biomètrics

Les raons dels errors dels sistemes biomètrics són degudes a una sèrie de limitacions, les quals es detallen a continuació:

- **Limitació de la informació**: la informació invariant i distintiva continguda en una mostra biomètrica està inherentment limitada a causa de la capacitat intrínseca del senyal de l'identificador o sensor biomètric. Per exemple, la informació distintiva en la geometria de la mà és inferior que en les ditades. Conseqüentment, les mostres de la geometria de la mà poden distingir menys identificacions que les ditades encara que sigui en condicions ideals. La limitació de la informació també pot provenir d'una presentació pobra del tret biomètric al sensor per part dels usuaris o de l'adquisició del senyal inconsistent. Mostres adquirides de manera diferent d'un tret biomètric limiten la invariància al llarg de diferents mostres del mateix usuari.

- **Limitació de la representació**: la representació ideal hauria de ser dissenyada de manera que retingués tota la invariància i també la informació discriminatòria de les mostres preses. Els mòduls actuals d'extracció de característiques, típicament basats en models simplistes del senyal biomètric, fallen a l'hora de capturar tota la riquesa de la informació en un senyal biomètric real. Així, s'hi inclouen característiques errònies i se n'exclouen característiques vertaderes. En conseqüència, una fracció de l'espai legítim de les mostres no pot ser representat pel sistema biomètric, i així apareixen errors de representació.

- **Limitació en la invariància**: finalment, donat un esquema representatiu, el disseny d'un comparador ideal hauria de modelar perfectament la relació d'invariància al llarg de diferents mostres del mateix usuari (mateixa identificació), encara que les mostres hagin estat adquirides en diferents condicions. Un altre cop, a la pràctica (a causa de la incapacitat d'adquirir un nombre prou gran de mostres o la variància en les condicions de la

captura de les mostres) el comparador pot ser que no modeli les relacions d'invariància i així apareixen errors en el comparador.

El repte és poder arribar a una representació realista i invariant del tret biomètric provinent de mostres noves en condicions no controlades (o quasi no controlades). Llavors, estimar formalment la informació discriminatòria en el senyal de les mostres. Aquesta tasca és realment difícil en un sistema d'identificació a gran escala en què el nombre d'usuaris matriculats pot ser enorme (més de cinquanta milions).

1.2. Tipus d'errors en els sistemes biomètrics

En aquest apartat es detallen els errors que apareixen en les diferents etapes d'un sistema biomètric.

Vegeu també

Vegeu la figura 10 del mòdul "La biometria per a la identificació de les persones" d'aquesta assignatura.

1) Errors en el mòdul de captura: en els sistemes completament automàtics, les dades són capturades sense supervisió de cap expert. Aquests sistemes biomètrics típicament usen un dispositiu tipus *live-scan* que automàticament detecta la presència d'un tret biomètric quan apareix en el punt de mira del dispositiu. Aquests tipus de captura poden produir dos tipus d'errors: **fallada en la detecció (FD)** i **fallada en la captura (FC)**. La fallada en la detecció apareix quan el tret biomètric s'acosta al sensor però el sensor no és capaç de detectar-ne la presència. La fallada en la captura apareix quan el sistema s'ha adonat que hi ha un tret biomètric però no pot capturar la mostra. Normalment, la raó entre aquestes dues fallades és inversament proporcional.

2) Errors en l'extractor de característiques: després de capturar la mostra, el sistema l'envia a l'extractor de característiques. Si la imatge té molt poca qualitat (atenció, en cas de veu seria el senyal acústic), l'extractor no és capaç d'extreure'n cap característica coherent. Aquest error es coneix com a **fallada de procés (FP)**. Com que el mòdul de captura i l'extractor de característiques s'usen en els tres processos bàsics (matrícula, verificació i identificació), normalment s'ajunten en una sola mesura anomenada **fallada d'adquisició (FA)**. Un percentatge de fallades d'adquisició alt respecte del nombre de vegades que s'han adquirit mostres provoca una baixada important del rendiment del sistema i també frustració dels usuaris, que a la vegada genera rebuig al sistema biomètric (reducció d'acceptabilitat). Una manera d'augmentar aquest percentatge de fallades d'adquisició és permetre que el sistema generi un conjunt de característiques encara que la imatge sigui dolenta, és a dir, que la qualitat d'aquestes característiques sigui baixa. El problema és, llavors, que el mòdul de comparació pateix una càrrega addicional i les comparacions poden retornar sortides errònies.

3) Errors en el mòdul de creació de la plantilla: el mòdul de creació de la plantilla també pot fallar, atès un conjunt de característiques de diferents mostres. Aquestes fallades apareixen quan les característiques han estat extretes en una situació molt sorollosa i per tant hi ha poca coherència entre les

mostres. Aquesta fallada s'anomena **fallada de matriculació (FM)**, ja que la plantilla només es genera en el procés de matriculació. Semblant a la fallada d'adquisició, si la fallada de matriculació es desactiva o es posen uns límits de qualitat molt baixos, llavors apareixen molts més errors en la comparació.

4) Errors en el mòdul de comparació: el mòdul de comparació genera un resultat donades una mostra i una plantilla. Aquest resultat acostuma a tenir un valor dins del rang de 0 a 1 i representa una probabilitat o una distància. Les possibles fallades del mòdul de comparació depenen de si ens trobem en un procés de verificació o identificació. Les descriurem a continuació.

En un **procés de verificació**, després de calcular la distància o probabilitat, s'aplica un llindar, modificable externament, per prendre una decisió final. Si la distància (o probabilitat) és inferior (o superior) al llindar, llavors es considera que la plantilla i la mostra provenen del mateix individu. Altrament, es considera que són de diferents individus. En aquest procés ens trobem davant de quatre combinacions, dues de les quals generen errors:

a) L'usuari s'identifica correctament i presenta al sistema els seus trets biomètrics:

- El sistema retorna correctament que hi ha etiquetatge, és a dir, que els trets biomètrics pertanyen a la identificació presentada. No hi ha error i s'anomena **acceptació correcta**[1] **(AC)**.

(1)En anglès, *correct acceptance*.

- El sistema retorna erròniament que no hi ha etiquetatge, és a dir, que els trets biomètrics no són de la persona amb la identificació presentada al sistema. Aquest és un **error de no-etiquetatge**[2] **(ENE)**.

(2)En anglès, *false rejection* o *false non-match*.

b) L'usuari s'identifica de manera fraudulenta (per exemple, introdueix la identificació d'una altra persona que sap que té uns permisos especials) i presenta al sistema els seus trets biomètrics:

- El sistema retorna correctament que no hi ha etiquetatge, és a dir, que els trets biomètrics pertanyen a una altra identificació. No hi ha error i s'anomena **rebuig correcte**[3] **(RC)**.

(3)En anglès, *correct rejection*.

- El sistema retorna erròniament que sí que hi ha etiquetatge, és a dir, que els trets biomètrics són de la persona amb la identificació presentada al sistema. Aquest és un **error d'etiquetatge**[4] **(EE)**.

(4)En anglès, *false acceptance* o *false match*.

En un **procés d'identificació**, a l'hora de definir els errors, ens trobem davant de sis combinacions, tres de les quals generen errors i una no és possible.

a) La persona de la qual se cerquen els trets biomètrics s'havia matriculat al sistema (la seva plantilla és a la base de dades).

- El sistema retorna la identificació de la persona de qui es fa la cerca. No hi ha error: **acceptació correcta (AC)**.

- El sistema retorna una altra identificació: **error d'identificació positiu**[5] **(EIP)**. El que ha passat és que hi ha una plantilla d'una altra persona que per error ha retornat una distància més petita que la plantilla correcta.

(5)En anglès, *false positive identification*.

- El sistema retorna que no hi ha cap plantilla amb aquests trets biomètrics: **error de rebuig**[6] **(ER)**. Aquest cas només pot aparèixer quan el sistema d'identificació disposa d'un llindar com en la verificació. Podria ser que aquest error desaparegués si el llindar de la distància fos menys restrictiu, és a dir, si n'augmentem el valor.

(6)En anglès, *false rejection*.

b) La persona de la qual se cerquen els trets biomètrics no s'havia matriculat al sistema (la seva plantilla no és a la base de dades).

- El sistema retorna la identificació de la persona de qui es fa la cerca. Aquesta combinació no és possible. Si la identificació no ha estat mai entrada perquè l'usuari no s'ha matriculat, llavors no en pot retornar mai la identificació.

- El sistema retorna una altra identificació: **error d'identificació negatiu**[7] **(EIN)**.

(7)En anglès, *false negative identification*.

- El sistema retorna que no hi ha cap plantilla amb aquests trets biomètrics: **rebuig correcte (RC)**. Semblant a l'error de rebuig, només pot aparèixer aquesta situació si hi ha un llindar d'acceptació. Cap plantilla no ha retornat una distància inferior al llindar d'acceptació. Si s'augmentés el llindar d'acceptació per intentar que desapareguessin els errors de rebuig, llavors ens podríem trobar que alguns rebutjos correctes desapareixerien.

1.3. Modelització dels errors

En l'apartat anterior hem detallat quina mena d'errors poden aparèixer en un sistema biomètric, i també les causes que els generen. A continuació, farem un estudi més científic d'aquests errors en cas que ens trobem en un sistema de verificació i en un sistema d'identificació.

1.3.1. Sistema de verificació

Suposem que la plantilla emmagatzemada a la base de dades d'una persona és T i la mostra que volem verificar és I. A més, suposem que tenim una funció de similitud (es defineix com la inversa d'una distància) entre una mostra i una plantilla $S(I,T)$. S pren valors dins del rang de 0 a 1. Com més gran és S, més s'assembla la mostra a la plantilla, és a dir, més probabilitat hi ha que pertanyin a la mateixa persona. Llavors tenim dues possibles hipòtesis:

- $\boldsymbol{H_0}$: $I \neq T$: la mostra que volem verificar no pertany a la mateixa persona amb la qual s'ha generat la plantilla.

- $\boldsymbol{H_1}$: $I = T$: la mostra que volem verificar és de la mateixa persona amb la qual s'ha generat la plantilla.

Les possibles respostes del sistema biomètric són:

- $\boldsymbol{D_0}$: no hi ha etiquetatge. El sistema considera que pertanyen a persones diferents.

- $\boldsymbol{D_1}$: hi ha etiquetatge. El sistema considera que provenen de la mateixa persona.

Considerant les hipòtesis i les sortides del sistema, ens trobem amb els errors que hem mencionat anteriorment:

- **Error d'etiquetatge (EE)**: també anomenat *error de tipus I*. El sistema retorna D_1 quan la hipòtesi era H_0.

- **Error de no-etiquetatge (ENE)**: també anomenat *error de tipus II*. El sistema retorna D_0 quan la hipòtesi era H_1.

La **probabilitat d'error d'etiquetatge (FMR[8])** és la probabilitat d'un error tipus I. Matemàticament:

$$FMR = Probabilitat(D_1|H_0)$$

La **probabilitat d'error de no-etiquetatge (FNMR[9])** és la probabilitat d'un error tipus II. Matemàticament:

$$FNMR = Probabilitat(D_0|H_1)$$

[8] Sigla de l'anglès *false match rate*.

[9] Sigla de l'anglès *false non-match ratio*.

Per a poder avaluar la precisió d'un sistema de verificació biomètric és necessari recollir un nombre molt elevat de comparacions entre mostres i plantilles de la mateixa persona i també un nombre molt elevat de comparacions entre mostres i plantilles de persones diferents. El conjunt de les primeres mostres

s'anomena **distribució genuïna** i matemàticament es representa amb la distribució $p(s|H_0)$. El conjunt de les segones mostres s'anomena **distribució impostora** i matemàticament es representa amb la distribució $p(s|H_1)$. D'aquesta manera, podem definir les raons dels errors amb les funcions següents:

$$FNMR = \int_0^t p(s|H_1)ds \qquad (1)$$

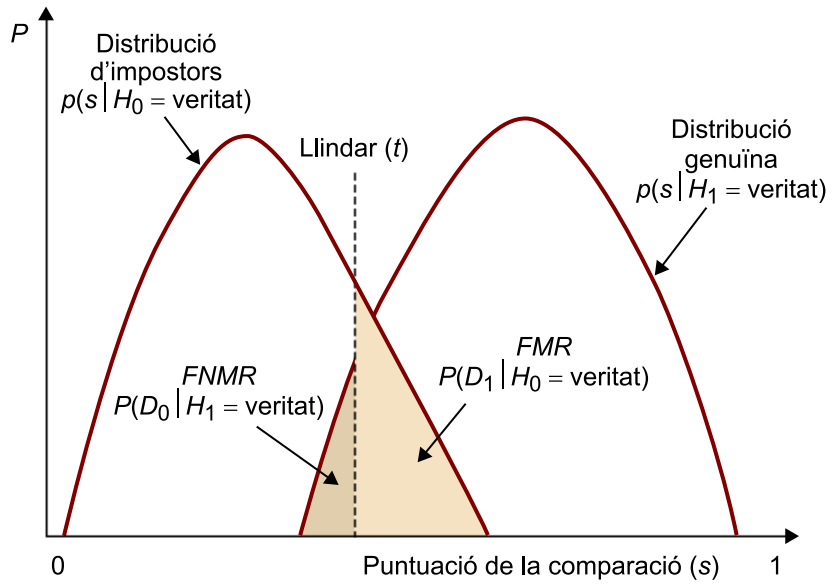
i

$$FMR = \int_t^1 p(s|H_0)ds \qquad (2)$$

en què t és el llindar d'acceptació imposat per l'administrador del sistema.

La figura 1 mostra les distribucions impostores i genuïnes respecte al valor de la similitud de comparació (*matching score*). En un sistema real, les mostres que pertanyen a la distribució genuïna acostumen a tenir una similitud més gran (o distància inferior, més a la dreta en la figura) que les mostres que pertanyen a la distribució impostora (amb distància superior, més a l'esquerra de la figura).

Figura 1. Distribució de les poblacions impostores i les genuïnes respecte de la similitud



Hi ha una disjuntiva molt important entre l'*FMR* (o també *false acceptance rate*, *FAR*) i l'*FNMR* (o també *false rejection rate*, *FRR*) en cada sistema biomètric. De fet, tal com es veu en les fórmules, els dos depenen del llindar d'acceptació t. Per això, en realitat, hauríem d'escriure $FMR(t)$ i $FNMR(t)$. Com es veu en la figura, FNMR(t) (o $FRR(t)$) és l'àrea marcada per la distribució genuïna i el llindar t. I $FMR(t)$ (o $FAR(t)$) és l'àrea marcada per la distribució impostora i també pel llindar t. Si es redueix t perquè el sistema sigui més tolerant a les variacions

d'entrada i al soroll, llavors *FMR*(*t*) augmenta. D'altra banda, si augmentem *t* perquè el sistema sigui més segur llavors augmentem *FNMR*(*t*). L'administrador del sistema no pot saber anticipadament on es desplegarà el sistema ni quina resposta tindran els usuaris. Per aquest motiu, és difícil imposar inicialment el llindar *t*. Per poder mostrar la bonança d'un sistema de verificació independentment del llindar s'han definit les dues funcions següents:

- ***Receiver operating characteristic* (ROC)**: el ROC és una corba en un pla bidimensional marcada pels punts *FMR*(*t*) i 1 – *FNMR*(*t*) per a diversos valors de *t*. El valor 1 – *FNMR*(*t*) s'anomena *el poder del test*. Aquesta gràfica mostra FMR respecte de la bondat del test.

- ***Detection-error trade-off* (DEC)**: el DEC és una corba semblant al ROC però marcada pels punts *FMR*(*t*) i *FNMR*(*t*). El DEC és interessant per a mostrar la relació entre els dos tipus d'errors ja que l'objectiu és rebaixar al màxim els dos errors.

A més d'aquestes gràfiques, quan es vol analitzar un sistema biomètric, s'acostumen a donar tres índex globals. Quan rebem informació d'un sistema biomètric per part d'una persona de l'empresa, és important usar o considerar aquests índex amb cautela, ja que sovint han estat portats a terme científicament, però amb bases de dades controlades pels mateixos desenvolupadors del sistema. Els índex són:

- **Probabilitat d'error equivalent (EER[10])**: indica la probabilitat d'error per a tots els valors del llindar en què *FMR* és igual a *FNMR*:

$$EER = FMR(t) \text{ tal que } FMR(t) = FNMR(t) \text{ per a tot } t.$$

(10)Sigla de l'anglès *equal-error rate*.

- **Zero FNMR**: es defineix com el valor més petit d'*FMR* en el qual no hi ha errors d'etiquetatge.

- **Zero FMR**: es defineix com el valor més petit d'*FNMR* en el qual no hi ha errors de no-etiquetatge.

- **Separabilitat**: si assumim que la població genuïna i impostora generen distribucions normals (distribucions de Gauss), llavors podem analitzar com de separades estan, o dit d'una altra manera, com de petit és el solapament que trobem entre les dues poblacions. Com més solapament, més errors es generaran en el procés de reconeixement.

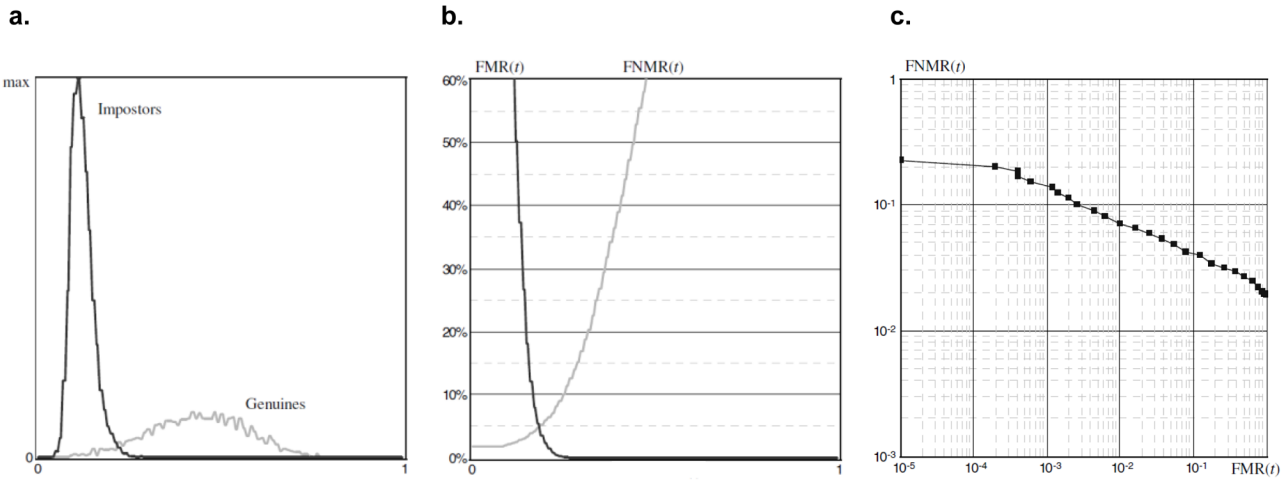
$$S = \frac{\| \hat{x}_{impostors} - \hat{x}_{genuins} \|}{\sqrt{\frac{\sigma^2_{impostors} + \sigma^2_{genuins}}{2}}} \qquad (3)$$

La figura 2 mostra els resultats d'un algorisme de comparació de ditades presentat en la Fingerprint Identification Competition (FVC) de l'any 2002. Les dades que es mostren van ser calculades amb 2.800 parelles de ditades genuïnes (que pertanyien al mateix dit) i 4.950 parelles impostores (que pertanyien a individus diferents).

FVC

L'**FVC** és una competició en què empreses o centres de recerca poden enviar els algorismes ja compilats (no s'envia el codi font) per comprovar-ne el funcionament i la bondat.

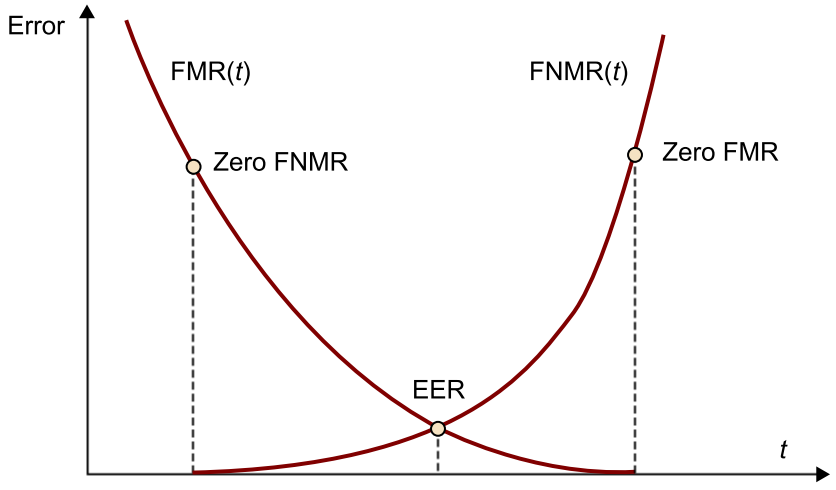
Figura 2. Alguns resultats de l'algorisme de comparació FVC



a. Distribucions genuïnes i impostores respecte de la simitud. **b.** Evolució del percentatge d'error dels errors FMR i FNMR respecte del llindar. **c.** La corba DEC obtinguda amb les mateixes dades que s'ha computat la figura b

La figura 3 mostra el percentatge dels errors *FMR* i *FNMR* respecte del llindar. També es mostra el punt en què es defineix l'EER, i també els valors zero *FNMR* i zero *FMR*. Fixeu-vos que el valor zero *FNMR* (o *zero FMR*) s'ubica exactament en el punt en què la gràfica de l'*FNMR* (o *FMR*) passa a valdre 0.

Figura 3. Exemple d'obtenció dels valors globals *zero FNMR*, *zero FMR* i EER amb les corbes de la probabilitat dels errors respecte del llindar de similitud



Els requeriments de precisió d'un sistema de verificació biomètric depenen molt de l'aplicació.

Exemple

En aplicacions forenses com la identificació de criminals, el que volem és no deixar d'identificar un criminal encara que hi hagi el risc d'haver d'examinar manualment un munt de potencials falsos etiquetatges identificats pel sistema. Això implica que el que ens preocupa és que l'*FNMR* sigui alt i, per tant, posarem un llindar de similitud baix. Un altre extrem seria un control d'accés d'alta seguretat. El principal objectiu és que no entrin impostors. En aquest cas, ens preocupa que l'*FMR* sigui alt. Clarament, si imposem que el llindar de similitud sigui molt alt, llavors farem baixar l'*FMR*, però això implicarà que algunes vegades hi haurà persones autoritzades a qui no es permetrà l'accés. Visualitzant la figura 3 es veu molt clar aquest concepte.

1.3.2. Sistema d'identificació

Suposem que una mostra que es vol identificar és comparada amb N plantilles de la base de dades i també suposem que aquestes comparacions són independents entre elles. En els sistemes d'identificació, com hem vist, es defineixen tres tipus d'errors que estan relacionats amb els errors d'etiquetatge i de no-etiquetatge:

- **Error d'identificació positiu (EIP)**: es relaciona directament amb l'error d'etiquetatge. Tenim la mostra correcta i la plantilla existeix, però el sistema no és capaç de trobar l'etiquetatge correcte.

- **Error de rebuig (ER)**: és semblant a l'error d'identificació positiu, per tant, també es relaciona directament amb l'error d'etiquetatge, ja que tenim la mostra correcta i la plantilla existeix però el comparador retorna una similitud inferior al llindar (o una distància més gran al llindar).

- **Error d'identificació negatiu (EIN)**: es relaciona amb l'error de no-etiquetatge. En aquest cas, no tenim la plantilla correcta i el sistema retorna un etiquetatge incorrecte i la similitud és més gran que el llindar de similitud.

La **probabilitat d'error d'identificació positiu (*FPIR*[11])** engloba la probabilitat d'error dels dos primeres errors esmentats: **error d'identificació positiu** i **error de rebuig**. Aquest error depèn del nombre de plantilles N i es defineix de la manera següent:

(11)Sigla de l'anglès *false positive identification-error rate*.

$$FPIR_N = 1 - (1 - FMR)^N$$

Aquests errors apareixen quan la mostra s'etiqueta erròniament amb una o més plantilles de la base de dades. Per això, $FPIR_N$ es calcula com u menys la probabilitat que no es faci cap etiquetatge fals amb cap de les plantilles. L'expressió $(1 - FMR)$ és la probabilitat que la mostra no s'etiqueti falsament amb una de les plantilles de la base de dades. Si *FMR* és molt petita, llavors aquesta expressió general es pot aproximar per $FPIR_N \approx N \cdot FMR$. I d'aquesta manera podem establir que la probabilitat dels errors d'etiquetatge positius s'incrementa linealment amb la mida de la base de dades. Aquesta aproxima-

ció es basa a considerar només el primer terme del binomi de Newton. Si volguéssim una aproximació més acurada, podríem usar els dos primers termes del binomi de Newton i l'expressió quedaria:

$$FPIR_N \approx N \cdot FMR - \frac{N \cdot (N-1)}{2} \cdot FMR^2 \qquad (4)$$

Amb aquesta segon aproximació, el valor que s'obté és una mica més petit, ja que té un terme més restant.

La **probabilitat d'error d'identificació negatiu (*FNIR*[12])** és més senzill de calcular, ja que es considera exactament igual a *FNMR*; *FNIR* = *FNMR*. Això es deu al fet que la probabilitat d'un error d'identificació negatiu quan s'està cercant la plantilla en les *N* plantilles de la base de dades és el mateix que l'*FNMR* en el mode de verificació.

(12)Sigla de l'anglès *false negative identification-error rate*.

2. Avaluació d'un sistema biomètric

La bondat d'un sistema biomètric depèn dràsticament d'un munt de variables: la composició de la població (ocupació, edat, sexe, demografia, raça...), l'entorn, la manera de fer les proves, i també altres restriccions específiques de l'aplicació. En una situació ideal, es voldria caracteritzar el rendiment en un model independent a l'aplicació. Així es podria predir el rendiment en una aplicació real.

S'han aplicat tècniques de modelatge rigoroses per caracteritzar l'adquisició de les dades i el procés de comparació. Amb aquestes tècniques s'ha aconseguit extrapolar els resultats obtinguts al laboratori com si fossin aplicacions reals i s'han obtingut força bons resultats. Avui en dia s'estan duent a terme avaluacions comparatives en bases de dades reduïdes. Els exemples més clars són la Fingerprint Verification Competition (FVC) (ja comentat) o l'Iris Verification Competition (IVC). Dels resultats obtinguts en aquestes competicions, en pot dependre que un sistema es pugui portar al mercat comercial o no. A causa de la importància de poder avaluar la precisió dels sistemes biomètrics, es poden definir tres tipus d'avaluacions:

1) Avaluació de la tecnologia: l'objectiu és avaluar la qualitat dels algorismes donada una tecnologia específica. No s'avalua tot el sistema, sinó algorisme per algorisme. Tots els algorismes es comparen atesos els mateixos sensors, bases de dades i qualsevol aspecte que en pugui afectar els resultats. La base de dades es divideix en dues parts. Normalment, totes les dades es generen a la vegada i la partició es porta a terme d'una manera aleatòria. La primera part compon la **base de dades d'aprenentatge** (***learning database***). Forma la part de les dades que els usuaris poden usar per a poder fer la posada a punt de l'algorisme i extreure'n el màxim rendiment. La segona part compon la **base de dades de test** (***test database***). Forma la part de les dades que els avaluadors usen per a fer les proves finals. Els participants no l'han pogut usar ni visualitzar abans de fer les proves. Com que les dades queden disponibles a tota la comunitat científica, després els experiment es poden repetir. Alguns llibres de biometria incorporen DVD amb aquestes dades. És una **avaluació repetible**.

2) Avaluació de l'escenari: l'objectiu d'aquest tipus d'avaluació és determinar el rendiment complet de tot el sistema en un prototip de laboratori o en un simulador d'aplicacions. El test es porta a terme en un sistema complet però en unes condicions controlades, encara que intenta simular una situació del món real. La comparació sempre es duu a terme amb els mateixos sensors biomètrics i la mateixa població. És una **avaluació repetible**.

3) Avaluació del funcionament: l'objectiu d'aquesta avaluació és determinar el rendiment del sistema complet en una situació real d'entorn específic i una població específica. És una **avaluació no repetible** perquè hi pot haver paràmetres no documentats o desconeguts. No hi ha una base de dades inicial.

3. Primeres grans aplicacions reals

La llista següent mostra uns quants exemples d'aplicacions desenvolupades a gran escala. No pretén ser una llista exhaustiva, sinó uns quants exemples per a mostrar que la biometria s'està aplicant i ja fa un temps que s'aplica a problemes reals i arreu del món. A més, s'han seleccionat les aplicacions que no estan relacionades amb el control d'accés ni la seguretat, que són a les que estem més habituats.

1) Sud-àfrica; verificació d'empremtes: La primera aplicació a gran escala de la biometria utilitzant empremtes digitals va ser la distribució de pensions a àrees rurals de Sud-àfrica. El 1990 cada pensionista tenia les seves empremtes digitals registrades. Van ser emmagatzemades en una targeta personal i verificades abans de lliurar la pensió per tal de garantir que qui portava la targeta n'era el propietari. Aquest sistema va reduir el frau considerablement.

2) Mèxic; verificació d'empremtes: L'Institut Electoral Federal de Mèxic va instal·lar 2.000 aparells de control biomètric per a la verificació de les targetes d'identitat dels votants. El propòsit no era identificar el votant pel nom, sinó comprovar que ell o ella, malgrat el nom, tingués dret a votar. Aparentment, l'operació va ser un èxit.

3) Uganda; verificació de cares: Per lluitar contra el frau electoral, el president d'Uganda va decidir tenir un sistema de reconeixement de cares instal·lat als centres electorals per a les eleccions generals del juny del 2001. En dos mesos, 11 milions de votants van ser fotografiats per crear una base de dades només per a les votacions. Aquest sistema es troba encara en vigor.

4) Malàisia; verificació d'empremtes: Des del 2001, a cada habitant de Malàisia de més de dotze anys li ha estat expedida una targeta d'identificació biomètrica, la *MyKad*, que conté dades com la data i el lloc de naixement, el sexe, el nom dels pares, l'ètnia d'origen, la religió, una fotografia i les empremtes. És una targeta amb múltiples propòsits, ja que serveix com a carnet de conduir, passaport, targeta de pagament electrònic i també conté informació mèdica d'emergència.

5) L'Afganistan; verificació de l'iris: L'Alt Comissionat per als Refugiats (HCR) va utilitzar la biometria el 2003 per a ajudar les famílies afganes a tornar al seu país després d'una llarga estada al Pakistan. El personal de l'HCR va fotografiar l'iris de les possibles persones que tornarien. Quan van estar preparades per tornar, la seva identificació es va fer abans que els donessin els

diners per al transport, per als cupons del menjar i per a les necessitats bàsiques. L'agència sosté que es va estalviar d'aquesta manera milions de dòlars prevenint fraus d'identitat.

6) Austràlia; verificació de l'iris: El 2003, es va provar a Austràlia un sistema biomètric per dispensar metadona. Als drogoaddictes que van triar participar en el programa se'ls va fotografiar l'iris per a la seva identificació posterior a les farmàcies que participaven en l'estudi, on els pacients rebrien la dosi exacta prescrita pel metge. La utilització d'aquest sistema de control és particularment útil en grans farmàcies on els farmacèutics no coneixen tots els pacients.

7) Europa; verificació d'empremtes: En un intent de reduir les múltiples sol·licituds d'asil polític als diferents països d'Europa, la Comunitat Europea ha establert una base de dades centralitzada, *Eurodac*, que conté les empremtes de tota persona que demana asil. Abans del gener del 2003, quan el sistema va esdevenir operatiu, s'estimava que un 80% de 500.000 sol·licituds anuals es demanaven a diversos països, mentre que ara s'ha reduït a un 11% de 280.000 sol·licituds. La base de dades *Eurodac* no es pot emparellar amb altres bases de dades.

8) L'Índia; verificació d'empremtes: Algunes cerimònies religioses al temple de Tirumala a l'Índia poden atraure 150.000 peregrins al dia. Les autoritats han adoptat un sistema biomètric per facilitar la gestió de la multitud. Els peregrins registren les seves empremtes digitals amb antelació. El dia de les cerimònies són identificats per les empremtes i autoritzats a entrar al temple.

9) El Japó; verificació de la cara, de les empremtes: A Kyoto es va dur a terme un experiment per permetre a la gent gran beneficiar-se dels serveis socials sense sortir de les seves llars. Les persones inscrites connecten amb treballadors de l'Ajuntament i s'identifiquen mostrant la cara a una càmera web i posant el dit en un sensor d'empremtes.

10) Indonèsia, Tailàndia; verificació d'ADN, empremtes: Per identificar els cossos després del tsunami del desembre del 2004, els experts van recopilar mostres d'ADN que després es van comparar amb l'ADN de les famílies que buscaven un familiar desaparegut i rastres d'empremtes digitals amb les empremtes de persones desaparegudes que les tenien registrades en documents d'identificació.

11) Texas, EUA; verificació d'empremtes: *Medicaid* és un programa americà que dóna prestacions sanitàries a les persones amb ingressos baixos. Per oferir una millor protecció de la informació mèdica dels pacients i reduir el frau, l'estat de Texas ha estat provant un projecte pilot des del 2004. Les empremtes digitals de les persones aptes per a Medicaid són emmagatzemades en la seva targeta Medicaid per comprovar-les abans de rebre prestacions.

Resum

En aquest mòdul hem descrit com s'avaluen els sistemes biomètrics. Primer de tot, hem estudiat quins errors poden aparèixer en els sistemes biomètrics. Després, hem vist que hi ha mètriques globals i que hi ha mètriques que són gràfiques com la ROC o la DEC. L'avaluació dels sistemes biomètrics és fonamental, ja que sempre hem de veure la biometria com una ciència molt aplicada.

També hem descrit exemples de grans desplegaments. Aquests exemples s'han de veure simplement com una mostra de les possibilitats que té la biometria per al reconeixement de les persones. S'han posat en funcionament altres sistemes i n'apareixen de nous.

Activitats

1. Les probabilitats dels errors en els sistemes biomètrics es classifiquen en tres tipus diferents de limitacions. Descriviu-les i resumiu-les.

2. Donades les limitacions anteriors, apareixen quatre tipus d'erros en els mòduls (o processos) d'un sistema biomètric. Descriviu els mòduls i també els possibles errors.

3. Els sistemes biomètrics disposen d'un llindar (normalment no és visible per l'usuari, ni tan sols per l'administrador del sistema) a partir del qual es considera que, donada una comparació, les dues mostres provenen del mateix individu o no. Relacioneu aquest llindar amb els errors generals dels sistemes biomètrics de verificació: error d'etiquetatge i error de no-etiquetatge.

4. Feu el mateix exercici que en el punt 3 però per als sistemes biomètrics d'identificació amb els errors: error d'etiquetatge positiu, error de rebuig i error d'identificació negatiu.

5. Expliqueu què és la distribució genuïna i què és la distribució impostora i com es modelen matemàticament.

6. Donats els valors de similitud genuïns: {3, 3, 5, 5, 6, 6, 6, 7, 9} i els valors de similitud impostors: {1, 2, 2, 3, 3, 3, 4, 4, 5}. Dibuixeu la funció de distribució de *FNMR* i de *FMR* (figura 1). Quin és el valor del llindar que fa que l'error general (*FNMR* + *FMR*) sigui mínim? Quin és el valor del llindar mínim perquè *FNMR* = 0? En aquest llindar, quin valor pren *FMR*? Quin és el valor del llindar màxim perquè *FMR* = 0? En aquest llindar, quin valor pren *FNMR*?

7. Dibuixeu el ROC i el DEC amb les distribucions de població de l'exercici 6. Suposeu els deu llindars següents: {0,5, 1,5, 2,5, 3,5, 4,5, 5,5, 6,5, 7,5, 8,5, 9,5}.

8. Donades les poblacions dels dos exercicis anteriors, digueu quin és l'EER, el zero *FNMR*, el *zero FMR* i la separabilitat de les poblacions.

9. Descriviu els tres tipus d'avaluacions: tecnologia, escenari i funcionament.

10. Dibuixeu la figura de la DEC i de la ROC seguint la taula 1 de l'annex.

11. Cerqueu aplicacions reals en què s'apliquin tècniques biomètriques i agrupeu-les per trets biomètrics específics.

Abreviatures

AC Acceptació correcta

DEC *Detection-error trade-off*

EE Error d'etiquetatge

EER *Equal-error rate* ('probabilitat d'error equivalent')

EIN Error d'identificació negatiu

EIP Error d'identificació positiu

ENE Error de no-etiquetatge

ER Error de rebuig

FA Fallada d'adquisició

FC Fallada de captura

FD Fallada de detecció

FM Fallada de matriculació

FMR *False match rate* ('probabilitat d'error d'etiquetatge')

FNIR *False negative identification-error rate* ('probabilitat d'error d'identificació negatiu)

FNMR *False non-match rate* ('probabilitat d'error de no-etiquetatge')

FP Fallada de procés

FPIR *False positive identification-error rate* ('probabilitat d'error d'identificació positiu')

RC Rebuig correcte

ROC *Receiver operaring characteristic*

Bibliografia

Jain, Anil; Bolle, Ruud; Pankanti, Sharath (1999). *Biometrics. Personal identification in networked society*. Editorial Kluweer Academic Publishers.

Jain, Anil; Flynn, Patrick; Ros, Arun (editors) (2008). *Handbook of biometrics*. Editorial Springer.

Nanavati, Samir; Thieme, Michael; Nanavati, Raj (2002). *Biometrics. Identity verification in a networked world*. Editorial Wiley Computer Publishing.

Ross, Arun; Nandakumar, Karthik; Jain, Anil (2006). *Handbook of multibiometrics*. Editorial Springer.

Wayman, James; Jain, Anil; Maltoni, Davide; Maio, Dario (editors) (2005). *Biometric systems. Technology, design and performance evaluation*. Editorial Springer.

Zhang, David (2000). *Automated biometrics. Technologies and systems*. Editorial Kluweer Academic Publishers.

Annex. Obtenció de les acceptacions falses, rebutjos falsos i la DEC a partir de la matriu de similitud

En aquest apartat es descriu com es pot obtenir la DEC a partir de la matriu de similitud. És a dir, la matriu en què les files i les columnes representen registres concrets de trets biomètrics i les cel·les són la similitud entre els trets biomètrics. La taula 1 mostra un exemple de la matriu de similitud.

Suposem que tenim una base de dades amb tres persones i cada persona ha fet tres enregistraments. És usual que us demanin tres enregistraments a l'hora de matricular-vos per garantir tenir més informació dels vostres trets biomètrics. Aquests nou enregistraments queden representats per les columnes. D'altra banda, suposem que cinc persones han mostrat els seus trets biomètrics per intentar accedir a la base de dades. Les tres primeres persones són les mateixes que s'han matriculat, però les dues últimes no s'han matriculat. Aquests cinc intents de verificació es representen en les cinc files.

Taula 1. Matriu de similitud: tres persones enregistrades tres vegades; cinc intents de verificació

	Persona 1			**Persona 2**			**Persona 3**		
Persona 1	**3**	**3**	**4**	3	2	3	3	0	1
Persona 2	3	2	4	**1**	**3**	**4**	2	3	6
Persona 3	1	4	1	2	1	2	**3**	**8**	**5**
Persona 4	3	1	9	2	6	3	5	0	7
Persona 5	2	1	3	3	0	0	1	2	2

Els intents d'identificació genuïns són els valors marcats en negreta. La persona 1 o la persona 2 o la persona 3 diuen que són qui realment són i es porta a terme la comparació amb els seus trets biomètrics. Fixeu-vos que s'ha de considerar que només hi ha tres intents genuïns i no nou, malgrat s'hagin fet nou comparacions. La resta de valors són intents d'identificació fraudulents. La persona presenta els seus trets biomètrics al sistema però diu que és una altra persona. Hi ha 3 × 5 identificacions menys 3 de genuïnes = 12.

El resultat d'una verificació és binari: "S'accepta que la persona és qui diu que és" o "No s'accepta que la persona és qui diu que és". Aquesta decisió es pren aplicant un llindar (imposat per l'administrador del sistema) i comprovant els tres enregistraments de la persona que l'usuari diu que és. Només que una de les tres comparacions sigui per sobre del llindar, llavors ja considerem que tenim una petició correcta: "S'accepta que és la persona que diu que és". D'altra

banda, fa falta que les tres comparacions siguin per sota del llindar perquè considerem que la petició no és correcta: "No s'accepta que és la persona que diu que és".

Suposem que el llindar és 4,5. Llavors, la taula 2 mostra el resultat de la verificació.

Taula 2. Resultat de la verificació tenint en compte la matriu de similitud de la taula 1 i el llindar 4,5

Llindar 4,5	**Persona 1**	**Persona 2**	**Persona 3**
Persona 1	**Persona diferent**	Persona diferent	Persona diferent
Persona 2	Persona diferent	**Persona diferent**	**Mateixa persona**
Persona 3	Persona diferent	Persona diferent	Mateixa persona
Persona 4	**Mateixa persona**	**Mateixa persona**	**Mateixa persona**
Persona 5	Persona diferent	Persona diferent	Persona diferent

Els errors estan marcats en negreta. Les acceptacions falses són les cel·les amb valors en negreta i subratllats. És a dir, impostors un dels tres resultat de la comparació dels quals era per sobre del llindar de similitud. Els rebutjos falsos són les cel·les amb valors en negreta i guixats. És a dir, verificacions genuïnes que el llindar és per sobre dels tres valors.

La probabilitat d'error d'etiquetatge (*FMR*) es calcula com el nombre d'acceptacions falses (cel·les en negreta i subratllades) dividit per la població impostora. Amb llindar 4,5 pren el valor:

$$FMR = 4/12 = 1/3.$$

La probabilitat d'error de no-etiquetatge (*FNMR*) es calcula com el nombre de rebutjos falsos (cel·les en negreta i guixades) dividit per la població genuïna. Amb llindar 4,5 pren el valor:

$$FNMR = 2/3.$$

Per tal de dibuixar la DEC, hauríem de calcular el valor de l'*FMR* i de l'*FNMR* per a diversos valors del llindar, per exemple, en aquest cas: 0,5; 1,5; 2,5; 3,5; 4,5; 5,5; 6,5; 7,5; 8,5; 9,5. Amb els deu parells de valors de l'*FMR* i de l'*FNMR* obtinguts, dibuixaríem la gràfica de la DEC.