La biometría para la identificación de las personas

Francesc Serratosa

PID_00195448

Universitat Oberta de Catalunya

Índice

Introducción

La biometría es una ciencia que analiza las distancias y posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas.

Hay varios rasgos biométricos que hoy en día se usan para tal fin, como las huellas dactilares, la cara, el iris, la mano, la retina o la firma. La biometría, y más en concreto las huellas dactilares, ya se estudiaban a finales del siglo XIX en aplicaciones forenses, es decir, para tratar de identificar a criminales o la identidad de las personas. En la actualidad, no solo se usa en estas aplicaciones sino en otras, como el control en los aeropuertos, en los accesos a centrales nucleares o a instalaciones militares o incluso, simplemente, para acceder a las oficinas o a la piscina municipal. Este es el motivo por el que la biometría está entrando en nuestras vidas cotidianas y es necesario que los informáticos o ingenieros en general tengan unos mínimos conocimientos sobre la materia.

Con el objetivo de aumentar la fiabilidad de los sistemas biométricos, en algunas aplicaciones se fusionan varios rasgos biométricos.

Fusión de rasgos biométricos

Se está trabajando en la fusión del reconocimiento de la oreja con el reconocimiento de la forma de andar. Esto se debe a que las dos técnicas se pueden aplicar en situaciones parecidas. Cámaras de vídeo grabando lateralmente a personas que caminan y sin colaboración por parte del usuario.

Esta fusión de métodos no siempre es trivial. Se ha publicado un libro que se dedica en exclusiva a este tema.

Reflexión

A pesar de su importancia, no vamos a comentar los métodos de fusión de sistemas biométricos por falta de tiempo.

El objetivo final de incorporar un sistema biométrico dentro de otro sistema es aumentar la seguridad de este segundo sistema. Por este motivo, es importante estudiar que el sistema biométrico en sí no tenga grietas por donde se pueda vulnerar la seguridad de todo el sistema en general.

Objetivos

Este módulo es el primero de la asignatura *Biometría*. Los objetivos son explicar los fundamentos básicos de la biometría para la identificación de las personas, así como introducir los conceptos y la terminología utilizada en los módulos posteriores para que el estudiante sea capaz de:

1. Conocer la eficacia y necesidad de la biometría en la sociedad actual.

2. Conocer las características que debe tener un rasgo biométrico para que se pueda usar en aplicaciones concretas.

3. Clasificar los rasgos biométricos que sirven para identificar y verificar a las personas.

4. Conocer las etapas o procesos internos de los tres sistemas básicos biométricos: identificación, verificación y matriculación.

5. Clasificar los errores que pueden aparecer en un sistema biométrico y detectar las condiciones en las que aparecen estos errores.

6. Evaluar una aplicación biométrica para saber su bondad. Conocer las métricas para evaluar y comparar la bondad de los sistemas biométricos.

7. Clasificar las diferentes aplicaciones donde se pueden aplicar técnicas biométricas para asegurar o ampliar su seguridad.

8. Conocer la breve historia de la biometría para identificar o verificar a las personas.

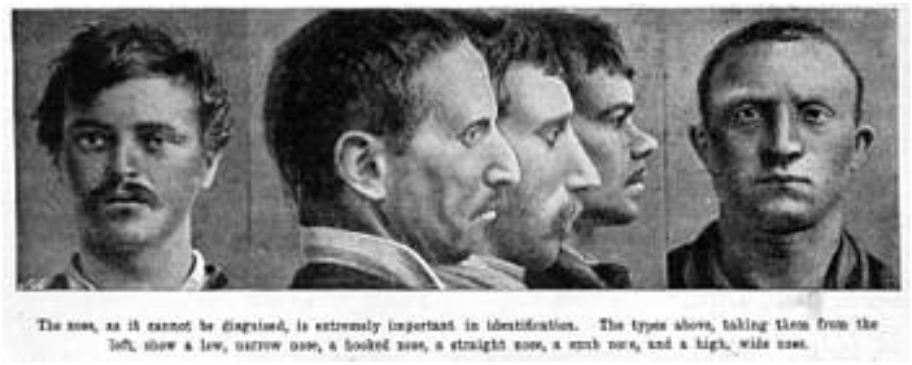
9. Comentar cómo el mundo del cine y del arte se ha hecho eco de la biometría.

10. Razonar sobre la posible vulneración de la identidad de las personas y comentar problemas de ética.

1. Los inicios de la biometría

En 1882, el policía francés **Alphonse Bertillon** (1853-1914) presentó el primer sistema de identificación de las personas basado en las características físicas, es decir en los rasgos biométricos, y lo denominó antropometría. Se considera el primer sistema científico usado por la policía para identificar a criminales. Inicialmente, se dedicó a clasificar la forma de la nariz, de la cara o del cuerpo de las personas. La figura 1 muestra una ilustración publicada en el *Pearson's Magazine* que muestra diferentes clases de narices definidas en la antropometría.

Figura 1. Ilustración publicada en el *Pearson's Magazine* (vol. XI, enero de 1901)



The nose, as it cannot be disguised, is extremely important in identification. The types above, taking them from the left, show a low, narrow nose, a hooked nose, a straight nose, a snub nose, and a high, wide nose.

En un inicio, el cuerpo de policía no quiso apoyar su investigación pero, más tarde, se dio cuenta de su enorme eficacia, puesto que en 1884 se identificó a 241 infractores reincidentes. Además de su trabajo como inspector de policía, también impartió muchas clases en las que explicaba sus métodos. La figura 2 muestra dos fotografías de estos cursos.

Figura 2. Fotografías de las clases de Bertillon (1911)

Bertillon diseñó un sistema para identificar a las personas que se basaba en guardar la información de once medidas de la cabeza y del cuerpo:

1) altura

2) anchura de los brazos extendidos

3) altura sentado

4) largura de la cabeza

5) anchura de la cabeza

6) largura de la oreja derecha

7) anchura de la oreja derecha

8) largura del pie izquierdo

9) largura del dedo corazón izquierdo

10) largura del dedo meñique izquierdo

11) largura del antebrazo izquierdo

Para conocer la similitud entre dos personas, podemos calcular la distancia euclídea entre los vectores formados por los once componentes. Si **A** y **B** son dos vectores de las once medidas de Bertillon y queremos saber si pertenecen a la misma persona, entonces calculamos:

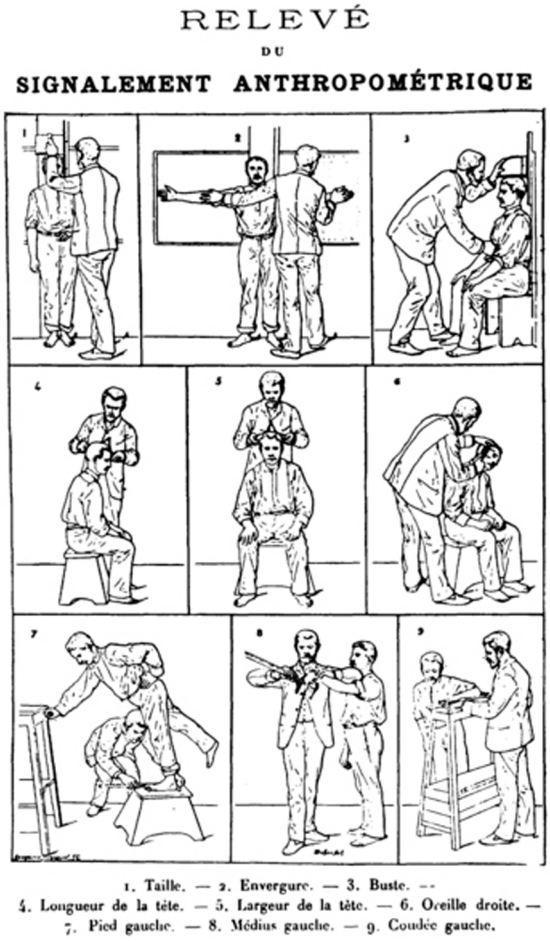
$$D_{Bertillon}(\mathbf{A}, \mathbf{B}) = \sqrt{\sum_{i=1}^{11} (A_i - B_i)^2} \qquad (1)$$

Consideramos que pertenecen a la misma persona si:

$$D_{Bertillon}(\mathbf{A}, \mathbf{B}) \leq Llindar_{Bertillon} \qquad (2)$$

La figura 3 muestra nueve dibujos hechos por el propio Bertillon donde enseña cómo se tienen que tomar las medidas. En honor a su creador, este método se denomina **bertillonaje**.

Figura 3. Imagen extraída del libro de Bertillon (1893)



La imagen muestra las once medidas que formaban la ficha de los infractores

Figura 3

Los dibujos 1 a 5 representan las medidas 1 a 5. El dibujo 6 representa las medidas 6 y 7. El dibujo 7 representa la medida 8. El dibujo 8 representa las medidas 9 y 10. El dibujo 9 representa la medida 11.

La figura 4 muestra una ficha de la policía de Nueva York donde se pueden ver las medidas de Bertillon.

Figura 4. Ficha policial de la ciudad de Nueva York

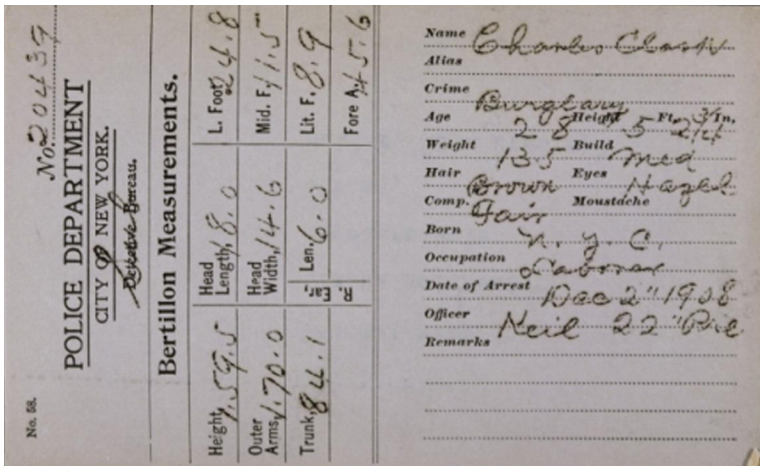


Figura 4

Se pueden ver en ella las medidas de Bertillon y la fecha del arresto, 2 de diciembre de 1908.

Las medidas de Bertillon pueden cambiar con el tiempo y, además, ser poco únicas, por eso la ciencia criminal tendió a investigar las huellas dactilares, ya que veían esta técnica con base más científica. Aunque se usó el método Bertillon durante años, fue gravemente desprestigiado por el caso de Will West y William West en 1903.

El caso de Will West y William West

En 1901, William West fue condenado y encarcelado en Kansas (Estados Unidos). Como criminal, se le tomaron las medidas de Bertillon. Dos años más tarde, en 1903, Will West fue arrestado y se le tomaron las medidas de Bertillon. Usando este método, dedujeron que Will West se había cambiado el nombre y que antes se hacía llamar William West, es decir, que era la misma persona que William y que había sido previamente condenado. Más tarde, se dieron cuenta de que William West todavía estaba en prisión y, por lo tanto, debía ser otra persona.

La tabla 2 presenta las medidas de Bertillon de Will West y William West. Se puede apreciar en dicha tabla una similitud impresionante en los once valores así como en la foto de las caras de la figura 5.

Tabla 2. Medidas de Bertillon en el caso de Will West y William West

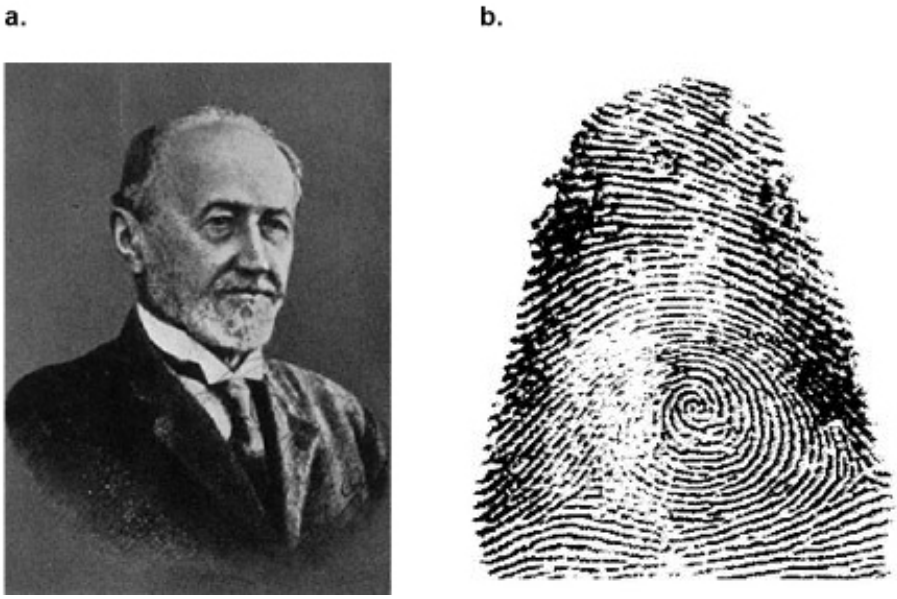
Will West	William West
178,5	177,5
187,0	188,0
91,2	91,3
19,7	19,8
15,8	15,9
14,8	14,8
6,6	6,5
28,2	27,5
12,3	12,2
9,7	9,6
50,2	50,3

Figura 5.

Fotografías de Will West y William West tomadas en su encarcelamiento, donde se puede observar la increíble similitud entre estas dos personas

Más de un siglo ha pasado desde que el jefe de la policía de Buenos Aires de nombre Juan Vucetich (1858-1925) (figura 6a) descubrió que Francisca Rojas había matado a sus dos hijos en 1892 gracias a una sanguinolenta huella dactilar (figura 6b) dejada en el buzón de su casa. Inicialmente, el criado, de nombre Velázquez, había sido condenado por error. Este trágico acontecimiento fue el percusor de la **biometría aplicada a la sociedad**.

Figura 6.



a. Fotografía de Juan Vucetich; b. la huella dactilar que Francisca Rojas dejó impresa

Un año más tarde, en 1893, el Ministerio del Interior del Reino Unido aceptó oficialmente que dos personas no podían tener exactamente las mismas huellas dactilares. Y así, muchos departamentos de policía vieron las huellas como una manera de identificar a infractores o criminales que cambiaban a menudo de nombre para evitar que se les condenara a penas superiores por el hecho de

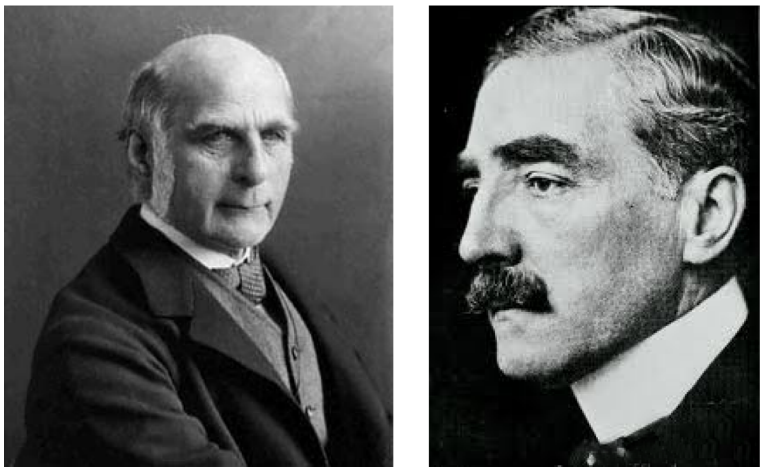
ser reincidentes. Las comisarías de policía empezaron a crear archivos de criminales con sus huellas dactilares y estos archivos se creaban o se ampliaban cuando había nuevas detenciones.

Es importante destacar que la ciencia de la biometría basada en la huella dactilar encontró una buena aplicación en los forenses y este hecho provocó grandes avances científicos. Las autoridades podían comparar las huellas dejadas en las escenas de los crímenes con las huellas introducidas en las comisarías por los criminales que habían sido arrestados previamente y así determinar o identificar a criminales reincidentes.

El enorme incremento de peticiones de comparación de huellas fue rápidamente insostenible. Por eso, apareció la necesidad de clasificar las huellas dactilares en pocas clases (de cuatro a ocho clases). Cuando se tenía que hacer una busca nueva en el archivo, las nuevas huellas solo se comparaban con los dedos que pertenecían a la misma clase. El primer método para clasificar las huellas fue ideado por **Francis Galton** (1822-1911) (figura 7a) y unos años más tarde, en el año 1900, el inspector general de la policía de Bengala (la India), de nombre **Edward Henry** (1850-1931) (figura 7b), puso en funcionamiento en Scotland Yard un método basado en esta clasificación.

Figura 7.

a. **b.**



a. Fotografía de Francis Galton; b. fotografía de Sir Edward Henry

El aprendizaje de los métodos de clasificación y comparación biométricos (huella dactilar, cara, iris, mano, forma de andar) es lento. Además, las exigencias impuestas por el hecho de que se necesite ser muy meticuloso en la busca de la similitud entre huellas, caras o iris o la clase a la que pertenecen, así como la necesidad de visualizar las huellas en tamaños diferentes (para captar la información global y también los detalles locales), ha provocado la necesidad de investigar en la adquisición y comparación automática de las huellas a través de sistemas electrónicos. Los primeros esfuerzos generaron el desarrollo de los

[(1)]Acrónimo del inglés *automatic fingerprint identification system*.

sistemas automáticos de identificación de huellas dactilares (AFIS[1]) en las últimas cuatro décadas. Más tarde, surgieron otros métodos automáticos para las caras o los iris. La policía científica fue la primera en adoptar estos métodos.

Más recientemente, las inquietudes en seguridad y en el fraude de la identidad han creado la necesidad de desplegar los métodos biométricos en otras aplicaciones sociales no forenses. Cada vez nos encontraremos más sistemas biométricos en la vida cotidiana, por eso es importante que los nuevos técnicos tengan nociones de estas tecnologías.

2. El reconocimiento biométrico

Nuestra sociedad está conectada electrónicamente y es cada vez más móvil. Las representaciones de nuestra identidad como códigos secretos (frecuentes en accesos electrónicos) y tarjetas (usadas por entidades bancarias o aplicaciones gubernamentales, como la tarjeta sanitaria) no son fiables para establecer la identidad de las personas. Los códigos secretos se pueden adivinar en muchos de los casos (sobre todo si se conoce a la persona) y las tarjetas se pueden perder o robar. Además, las tarjetas y los códigos secretos se comparten habitualmente entre amistades y compañeros de trabajo. Debido a todos estos hechos, los códigos secretos y las tarjetas no garantizan la identidad de sus usuarios.

El **reconocimiento biométrico**[2] se refiere al uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características se denominan **identificadores biométricos** o **rasgos biométricos** y sirven para reconocer automáticamente a los individuos.

(2)En inglés, *biometrics* o *biometric recogniton*.

La biometría se está convirtiendo en un factor esencial para la identificación eficaz de las personas. Esto se debe a que los rasgos biométricos no se pueden compartir o extraviar y representan intrínsecamente las formas corporales del individuo que identifica. Reconocer a una persona por su cuerpo y después enlazar este cuerpo con una identidad establecida externamente forma una herramienta muy poderosa para la gestión de la identidad con unas consecuencias potenciales enormes, tanto positivas como negativas. En consecuencia, la biometría no es solo un problema fascinante en el campo de la investigación dedicado al reconocimiento de patrones, sino una tecnología que, usada correctamente, puede permitir una sociedad más segura, reducir el fraude y proveer interfaces persona-máquina fáciles de usar.

La palabra *biometría* deriva del griego *bios* (que quiere decir **vida**) y *metria* (que quiere decir **medida**). Los rasgos biométricos son medidas extraídas del cuerpo humano vivo. Y, además, todos los rasgos biométricos son una combinación de anatomía y de comportamiento. Es importante mencionar que a menudo los rasgos biométricos son más similares en parientes próximos.

Anatomía y comportamiento

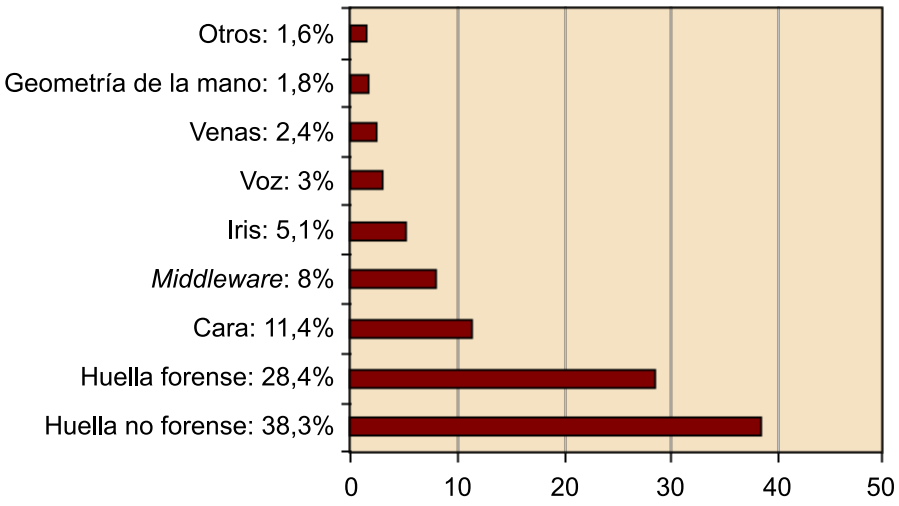
Por ejemplo, las huellas dactilares son anatómicas por naturaleza, pero el uso del sensor de entrada (es decir, cómo el usuario presenta el dedo en el sensor) depende del comportamiento del individuo.

Todos los días nos planteamos muchas preguntas relacionadas con la identidad de las personas. ¿Esta persona está autorizada a entrar en este edificio? ¿A esta persona se le puede dar esta información? ¿Esta persona está buscada por un crimen? ¿Esta persona ya ha recibido algunos beneficios sociales? Empresas privadas y gobiernos necesitan respuestas fehacientes a estas preguntas. Debi-

do a que los rasgos biométricos son difícilmente reemplazables, olvidados o compartidos, se consideran más seguros para reconocer a las personas que los clásicos códigos secretos o carnés de identidad.

El objetivo de las aplicaciones biométricas es tener sistemas más **cómodos** (extraer dinero de los cajeros automáticos sin tarjetas), más **seguros** (solo las personas autorizadas pueden tener acceso a ellos) y más **rápidos** (reducción del mantenimiento de los códigos secretos y tarjetas). El uso cada vez más extendido de las tecnologías biométricas ha hecho que los precios de los sistemas hayan bajado, que los componentes se hayan miniaturizado y que sean más fiables. Y todos estos hechos provocan que se use todavía más esta tecnología.

Figura 8. Porcentaje de los ingresos generados por los diferentes métodos biométricos

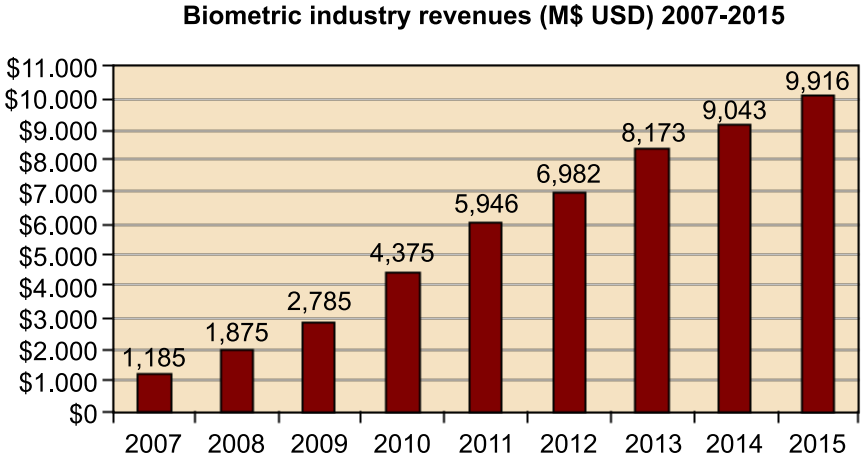


La figura 8 muestra el reparto de los rasgos biométricos respecto a los ingresos que generan. La huella dactilar es el rasgo biométrico más antiguo y sigue siendo el que genera más ingresos económicos. El siguiente rasgo biométrico es la cara, que ya está a mucha distancia porcentual.

Middleware

El ***middleware*** es un término informático que se emplea para designar a todo el conjunto de aplicaciones o rutinas de software que hacen de capas intermedias entre los dispositivos de lectura de rasgos biométricos y las aplicaciones de alto nivel que usa el usuario.

Figura 9. Ingresos generados por los sistemas biométricos desde el año 2007 hasta el año 2010. Predicción de ingresos desde el año 2011 hasta el 2015



La figura 9 muestra los ingresos de años pasados y la predicción de años futuros del sector de la biometría en millones de dólares según Acuity Market Intelligence©.

Para acabar este apartado, nos gustaría hacer un comentario sobre la realidad de las técnicas biométricas y su despliegue en sistemas aplicados reales. El uso imaginativo y adulador de la biometría en las películas y series de televisión ha provocado una percepción generalizada de la biometría como una ciencia completamente descubierta y una tecnología a prueba de fallos. Eso no es cierto. Hay gran cantidad de aspectos que son motivo de investigación, ya que se deben mejorar. El reconocimiento biométrico funciona bastante bien, hay aplicaciones biométricas funcionando con millones de usuarios, pero la investigación en este campo todavía tiene camino por recorrer.

3. Los sistemas biométricos

En función del contexto de la aplicación biométrica, podemos diferenciar dos tipos de sistemas, los sistemas de verificación y los sistemas de identificación.

Los **sistemas de verificación** (también llamados **de autentificación**) autentifican la identificación de la persona mediante la comparación del rasgo biométrico acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema.

El usuario tiene que presentar su identificación mediante un carné o clave secreta. El sistema realiza una única comparación entre el rasgo biométrico que el usuario acaba de presentar con el rasgo biométrico que hay en la base de datos con la misma identificación presentada. La salida de un sistema de verificación es normalmente binaria: es la misma persona si los rasgos biométricos coinciden (son muy similares) o son dos personas diferentes en otro caso. En algunos casos, los rasgos biométricos y la identificación de la base de datos están en la propia tarjeta del usuario en forma encriptada. En este caso, se dice que disponemos de una **base de datos distribuida** entre todas las tarjetas de los usuarios.

Los **sistemas de identificación** reconocen a la persona a través de la busca del rasgo biométrico que más se asemeja al usado para identificarlo en toda una base de datos.

El usuario no aporta ninguna información de su identificación, como era el caso del sistema de verificación. El sistema lleva a cabo una comparación uno a muchos. Esto quiere decir que el rasgo biométrico del usuario desconocido se compara con muchos rasgos biométricos de una base de datos. Hay varias salidas a este sistema. La más sencilla es devolver el nombre de la persona (identificador) cuyo rasgo biométrico se asemeja al introducido. Otra posibilidad es deducir que este rasgo biométrico no pertenece a ninguna persona de la base de datos (este caso se da cuando las distancias del rasgo biométrico con todos los rasgos biométricos de la base de datos es superior a un umbral). Finalmente, y es el caso más usual en las aplicaciones forenses, el sistema no devuelve una sola persona sino una **lista de candidatos**. Es decir, devuelve las personas cuya distancia de sus rasgos biométricos con el rasgo biométrico introducido es inferior a un umbral.

Tanto los sistemas de verificación como de identificación necesitan un proceso previo llamado **sistema de matriculación**[3]. Este proceso se encarga de recoger el rasgo biométrico (o los rasgos biométricos) junto con la identificación de la persona. Este proceso es muy importante puesto que se encarga de relacionar (¡de por vida!) la identificación de la persona con el rasgo biométrico. Normalmente, este proceso tiene lugar ante una persona autorizada que vela por la veracidad de los datos que aporta el usuario (carné de identidad, pasaporte) y controla que realmente sea este usuario el que presenta el rasgo biométrico al sistema. Además, durante el proceso de matriculado, esta persona verifica la calidad de los datos biométricos obtenidos. Si considera que los datos no tienen suficiente calidad, pide al usuario que vuelva a presentar el rasgo biométrico (huella dactilar, cara, iris) al sistema. Es fundamental que los datos que se almacenan en la base de datos tengan la máxima calidad puesto que en los procesos de identificación o verificación no siempre se puede garantizar esta calidad. Algunos sistemas piden al usuario capturar varias veces el mismo rasgo biométrico (normalmente tres veces). El sistema puede elegir la mejor imagen o fusionarlas y así reducir los errores de captura.

(3) *Enrollment*, en la bibliografía inglesa.

Los tres sistemas antes mencionados usan los procesos siguientes (ved la figura 10):

- **Captura**: La representación digital del rasgo biométrico tiene que ser capturada. El sensor biométrico es usualmente un sistema para capturar una imagen (excepto la identificación del hablador, que es una máquina de grabar voz). Normalmente, la información capturada se denomina muestra[4]. A veces, el sistema de captura también incorpora otros periféricos para introducir información no biométrica o mostrar información.

(4) En inglés, *sample*.

- **Extracción de las características**: Con el objetivo de facilitar la comparación, aumentar la información y reducir el ruido, la representación original digital (imagen digital) se procesa normalmente con un extractor de características para generar una representación compacta y más identificadora llamada registro de identificación[5] o conjunto de características[6].

(5) En inglés, *identification register*.

(6) En inglés, *feature set*.

- **Creación de la plantilla**: La plantilla[7] es una forma compacta de representar un conjunto de muestras de una sola característica biométrica (por ejemplo, se puede crear una plantilla de dieciséis muestras diferentes de la imagen de la cara de una misma persona). El proceso de creación de la plantilla recibe como entrada los registros de identificación y crea una información más compacta donde se intenta extraer la información que persiste en todas las muestras puesto que se consideran los rasgos característicos. En algunos casos, esta plantilla está formada por una única muestra y por lo tanto se puede representar como un registro de identificación.

(7) En inglés, *template*.

- **Comparación**: El proceso de comparación recibe como entrada un registro de identificación y una plantilla y calcula una distancia entre los dos. A ve-

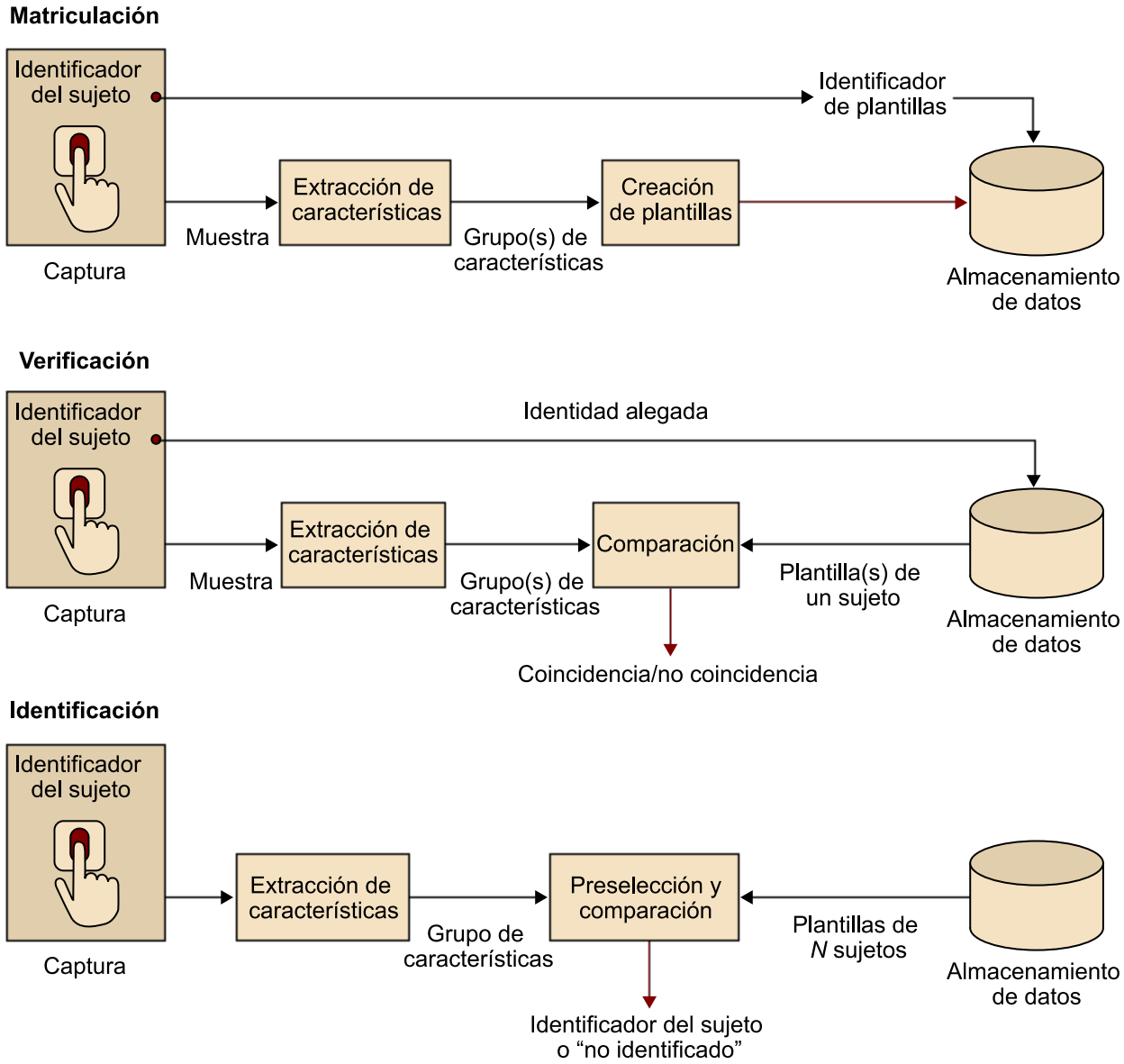
ces, en lugar de una distancia obtiene una probabilidad de que representen un mismo individuo. En el proceso de verificación, hay un umbral interno al sistema que solo lo puede modificar el administrador del sistema. Si la distancia es inferior al umbral (o la probabilidad es superior al umbral), el sistema considera que los dos datos provienen de la misma persona, de lo contrario, se considera que provienen de dos personas diferentes.

- **Selección o filtrado**: En los sistemas de identificación con muchos datos (podemos hablar de 50 millones de huellas dactilares), el filtrado es un método para aumentar el tiempo de respuesta del sistema. Con técnicas típicas de las bases de datos, logran no tener que explorar la base de datos entera y así ganar tiempo.

- **Almacenamiento de los datos**: Es el proceso para almacenar la información del usuario. Esta información está compuesta por un identificador único (por ejemplo, el número del DNI o del pasaporte), la plantilla biométrica y otros datos (por ejemplo, la dirección o la profesión). En función de la aplicación, los datos se almacenan en sistemas de almacenamiento centralizados (para poder llevar a cabo la identificación) o en tarjetas inteligentes[8] (para poder llevar a cabo la verificación). Además, se aplican técnicas de encriptación con todos los datos para que así el registro formado por el número del DNI más los rasgos biométricos sea indivisible.

[8] En inglés, *smart cards*.

Figura 10.



Etapas o procesos que componen los sistemas: a. matriculación (*enrollment*); b. verificación (*verification*); c. identificación (*identification*)

Dependiendo del dominio de la aplicación, un sistema biométrico puede operar como un sistema en línea o como un sistema fuera de línea.

a) Los **sistemas en línea** requieren que la comparación se lleve a cabo rápidamente y se requiere una respuesta inmediata, por ejemplo es el caso del permiso para iniciar una aplicación o la entrada física de una persona a unas instalaciones. Normalmente, son sistemas de verificación.

b) Los **sistemas fuera de línea** no requieren que la respuesta sea inmediata y se tolera que haya un admisible retraso en la respuesta. Normalmente, son sistemas de identificación. Los sistemas en línea suelen ser completamente automáticos, requieren que el rasgo biométrico sea capturado con un sensor electrónico y no hay control humano de la calidad de los datos. Por otro lado, los sistemas fuera de línea son usualmente semiautomáticos. La captura del rasgo biométrico puede haber sido con un sistema no electrónico (por ejem-

plo, la captura de una huella dactilar dejada en la escena de un crimen) y hay un control de la calidad de los datos por parte de un especialista. Además, este especialista dispone de herramientas informáticas para arreglar los datos o ayudar al programa a que lleva a cabo la comparación biométrica.

Dependiendo de la aplicación, se llevan a cabo dos tipos de buscas en los sistemas de identificación, que son las buscas positivas y las buscas negativas:

a) Las **buscas positivas** son aquellas por las que queremos comprobar si aquel rasgo biométrico se encuentra en la base de datos, es decir, si el usuario ha sido matriculado. Deseamos saber la identificación de aquel rasgo biométrico. El caso más típico es introducir en el sistema una huella dactilar que hemos encontrado en una escena de un crimen o una cara que hemos podido fotografiar y queremos saber a quién pertenece.

b) Por otro lado, las **buscas negativas** son aquellas por las que queremos comprobar que aquel individuo no se ha matriculado. Deseamos saber que no hay ninguna persona matriculada con aquellos rasgos biométricos. La aplicación más usual es asegurarse de que una persona no quiere usar más de una vez un servicio que solo tiene derecho a usar una sola vez, como, por ejemplo, no cobrar varias veces una ayuda estatal o no votar varias veces en unas elecciones.

4. Los rasgos biométricos

Se puede usar cualquier rasgo anatómico o de comportamiento humano como identificador biométrico para identificar o verificar a las personas si satisface los requerimientos siguientes:

- **Universalidad**: Cada persona debe poseer ese rasgo biométrico.
- **Particularidad**: Todas las personas tienen que ser suficientemente diferentes en términos del rasgo biométrico.
- **Permanencia**: El rasgo biométrico debe ser invariante en el tiempo y a cualquier otro factor desde el punto de vista de la comparación entre rasgos biométricos.
- **Medible**: El rasgo biométrico se tiene que poder medir cuantitativamente.
- **Rendimiento**: El rasgo biométrico debe garantizar precisión y robustez en diferentes factores ambientales.
- **Aceptabilidad**: Los usuarios del sistema deben aceptar el uso de ese rasgo biométrico para su identificación.
- **No falsificable**: El rasgo biométrico tiene que garantizar que su falsificación sea dificultosa.

Ved también

En el módulo "Seguridad en sistemas biométricos" de este material, se desarrolla el requerimiento de no falsificable.

Un sistema biométrico debe tener una precisión y velocidad aceptable con un número de recursos razonable. Además, no puede ser nocivo para los usuarios, debe ser aceptado por los usuarios potenciales y ser lo suficientemente robusto ante los métodos fraudulentos.

Se está usando un número bastante grande de rasgos biométricos en diferentes aplicaciones. Esto se debe a que cada rasgo biométrico tiene su propia fortaleza así como debilidad y es necesario usar un número específico de recursos. Estas características se tienen que poder adaptar a la aplicación específica para la que se diseña. Decidir qué rasgo característico se puede usar en una determinada aplicación se lleva a cabo considerando las características de la aplicación así como las propiedades del rasgo biométrico. Los principales asuntos que se tienen que considerar a la hora de seleccionar un rasgo biométrico en una aplicación concreta son los siguientes:

- ¿La aplicación necesita un sistema de verificación o identificación? En el supuesto de que la aplicación necesite la identificación de un sujeto en

una base de datos muy grande, entonces necesita un rasgo biométrico con mucha particularidad.

- ¿Cuáles son las características operacionales de la aplicación? Es decir, ¿se va a usar en un sistema semiautomático o completamente automático? ¿En el interior o en el exterior?

- ¿Los usuarios están habituados a mostrar o aceptan mostrar ese rasgo característico?

- ¿Cuál es la capacidad de almacenamiento de la aplicación? Por ejemplo, una aplicación que funciona con una tarjeta inteligente tiene unos recursos muy limitados de almacenamiento.

- ¿Es muy importante que el rasgo biométrico no sea falsificable?

A continuación, mostramos los rasgos biométricos más comunes que se han usado en sistemas comerciales o están en fase de investigación.

4.1. Rasgos biométricos de la cabeza

Los rasgos biométricos de la cabeza son los siguientes:

- **Cara**: La cara es uno de los rasgos biométricos más aceptables debido a que es el rasgo biométrico más común usado por los humanos a la hora de reconocer a las personas así como las interacciones visuales diarias. Además, el método para adquirir imágenes de la cara es no intrusivo y no hace falta ninguna interacción por parte del usuario. En fase de prototipo, encontramos algunos métodos que no solo reconocen a la persona sino su estado de ánimo según la expresión facial, la edad, el sexo y la posición. En algunas cámaras fotográficas, ya se incorpora un detector de sonrisas. La aplicación no solo detecta las caras, sino que detecta que estén sonriendo.

- **Termograma facial**: Esta tecnología se puede usar junto con el reconocimiento de la cara en los casos de seguimiento pasivo (el usuario no sabe que lo están identificando). Tiene la ventaja de que no le afecta el maquillaje, el corte de pelo o la barba. Pero tiene el inconveniente de que es muy poco permanente, puesto que le afecta un simple resfriado o si se viene de correr o de practicar deporte. Se mide con una cámara térmica a una distancia máxima de unos pocos metros.

- **Oreja**: Las características de la forma de la oreja son un rasgo biométrico muy útil para el reconocimiento pasivo de la persona. Una cámara de seguridad puede filmar con facilidad una oreja. Este rasgo biométrico se mantiene bastante estable en el tiempo, pero tiene el problema de que muchas veces las orejas quedan ocultas bajo el cabello o alguna gorra. Por tener

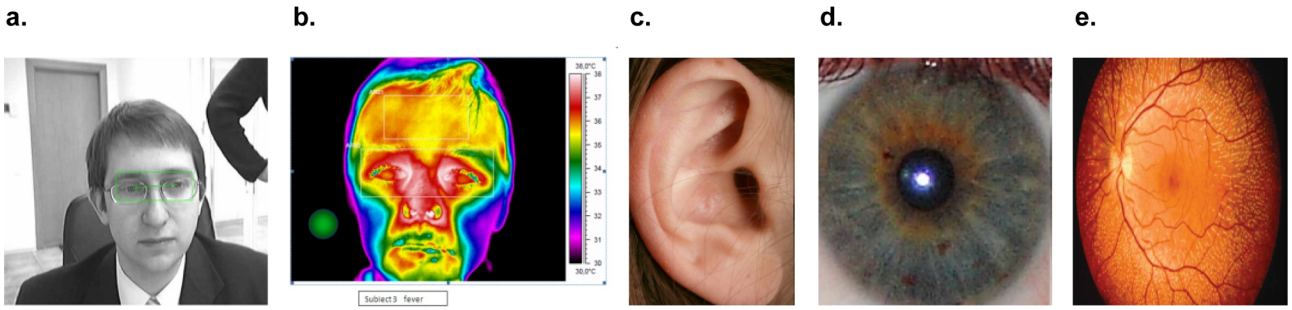
características similares de funcionamiento, normalmente se usa como un complemento al reconocimiento de las caras o de la forma de andar.

- **Iris**: La textura visual del iris humano se determina por el proceso caótico y morfogenético durante el desarrollo embrional. Se ha postulado ser distintivo para cada persona y cada ojo. Es usual que se capture una imagen del iris usando un proceso de captura sin contacto. Normalmente, la captura de una imagen del iris implica la cooperación del usuario aunque hay sistemas (en fase de prototipo en el laboratorio) para capturar la imagen del iris sin colaboración por parte del usuario. El usuario colabora ubicando la imagen en el centro del aparato de captura y asegurándose de que el iris está a una distancia predeterminada al plano focal de la cámara. La tecnología del iris ha demostrado ser muy precisa y rápida en la imagen de alta resolución y muy capturada.

- **Retina**: Este rasgo biométrico es uno de los últimos que se ha incorporado. Tiene una tecnología y aplicabilidad muy parecida a la del iris y ha demostrado ser altamente discriminatorio. Se basa en leer las pequeñas venas que hay en la retina, que es la membrana de dentro del ojo que capta la luz que estamos viendo. La captura de la imagen se realiza en luz infrarroja y esto provoca que sea una tecnología de baja aceptación.

En la figura 11, mostramos imágenes de los rasgos biométricos acabados de mencionar.

Figura 11. Rasgos biométricos de la cabeza



a. cara; b. termograma facial; c. oreja; d. iris; e. retina

La tabla 3 muestra las principales características que ha de tener un sistema biométrico en los rasgos biométricos de la cabeza.

Tabla 3. Bondad de los rasgos biométricos de la cabeza

Rasgo biométrico	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Cara	A	B	M	A	B	A	A
Termograma facial	A	A	B	A	M	A	A

Las entradas de la tabla muestran la bondad de cada característica en cada rasgo biométrico discretizada en tres valores: A (alto), M (medio) y B (bajo).

Rasgo biométrico	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Oreja	M	M	A	M	M	A	M
Iris	A	A	A	M	A	B	A
Retina	A	A	M	B	A	B	A

Las entradas de la tabla muestran la bondad de cada característica en cada rasgo biométrico discretizada en tres valores: A (alto), M (medio) y B (bajo).

4.2. Rasgos biométricos de la mano y los dedos

Los rasgos biométricos de la mano y los dedos son los siguientes:

- **Geometría de la mano y de los dedos**: La largura y anchura de los dedos, así como la relación con la anchura de la mano son rasgos biométricos bastante invariantes aunque poco distintivos. El sistema de adquisición de la geometría de la mano y de los dedos necesita colaboración con el usuario para captar la imagen frontal así como las imágenes laterales (algunos sistemas solo usan la imagen frontal). Los requerimientos de almacenamiento de esta tecnología son muy pequeños, lo que la hace muy atractiva para sistemas de memoria limitada. No obstante, debido a la poca capacidad para distinguir a diferentes usuarios, se utiliza solo en procesos de verificación y no es nada escalable en aplicaciones de identificación.

- **Huella dactilar**: La huella del dedo es el patrón de valles y cordilleras y su formación se determina durante los primeros meses de gestación. Se ha determinado empíricamente que las huellas de gemelos y las huellas de diferentes dedos de una persona son diferentes. Además, desde hace más de un siglo, se ha demostrado que es una tecnología altamente discriminatoria incluso basándose en datos de más de 50 millones de usuarios. Hoy en día, el reconocimiento de las huellas dactilares es una tecnología muy fácil de instalar y barata. Finalmente, es una tecnología útil en aplicaciones forenses así como en aplicaciones civiles y de máxima seguridad. Además, solo hay una fracción muy pequeña de la población que no puede hacer uso de esta tecnología.

Escáner de dedo

Un escáner de dedo cuesta unos 50 euros comprado a gran escala.

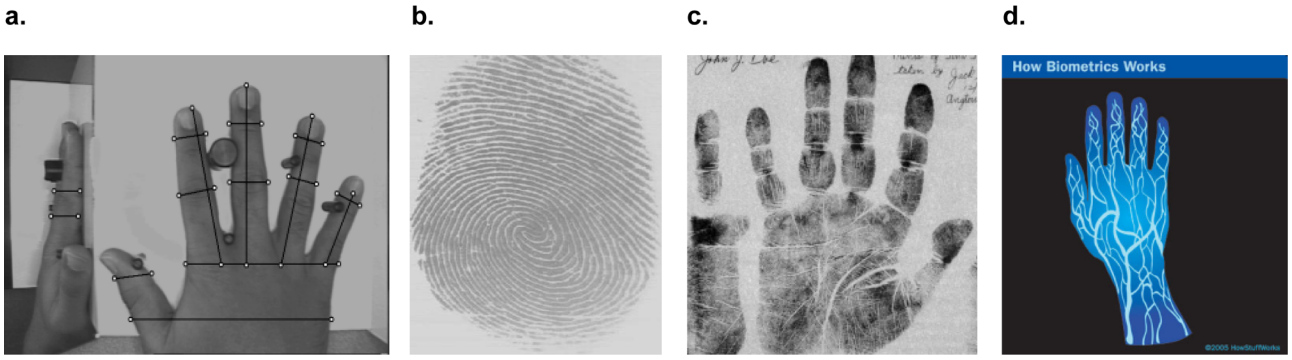
- **Huella de la mano**: La palma de los humanos contiene cordilleras y valles, igual que los dedos. La palma contiene más área y por eso se espera que pueda ser más discriminadora que los dedos. Como contrapartida, los escáneres de mano son más grandes y caros, por lo tanto, no usables en las aplicaciones donde se necesitan dispositivos reducidos. La ventaja de la palma es que contiene unas líneas más marcadas que se pueden captar con dispositivos de baja resolución (más baratos).

- **Venas de la mano y de los dedos**: La estructura de las venas de la mano y de los dedos se detecta con luz cerca del infrarrojo capturada de una imagen de la mano pulsada sobre el sistema de captura (escáner infrarrojo).

Este sistema se comercializa actualmente puesto que el escáner de infrarrojo usa diodos de tipo LED que son asequibles económicamente.

En la figura 12, mostramos imágenes de los rasgos biométricos acabados de mencionar.

Figura 12. Rasgos biométricos de la mano y de los dedos



a. geometría de la mano y de los dedos; b. dedo; c. huella de la mano; d. venas de la mano y de los dedos

La tabla 4 muestra las principales características que ha de tener un sistema biométrico en los rasgos biométricos de la mano y los dedos.

Tabla 4. Bondad de los rasgos biométricos de la mano y los dedos

Rasgo biométrico	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Geometría de la mano y de los dedos	M	M	M	A	M	M	M
Dedo	M	A	A	M	A	M	M
Huella de la mano	M	A	A	B	A	M	M
Venas de la mano y de los dedos	M	M	M	M	M	M	A

Las entradas de la tabla muestran la bondad de cada característica en cada rasgo biométrico discretizada en tres valores: A (alto), M (medio) y B (bajo).

4.3. Rasgos biométricos de todo el cuerpo

Los rasgos biométricos de todo el cuerpo son los siguientes:

- **Olor**: Cada persona exuda un olor que es característico de su composición química y se puede usar para identificar a las personas. El sistema más usual está compuesto por una matriz de sensores donde cada sensor detecta un tipo concreto de sustancia química (o componente aromático). La respuesta del sistema consiste en la cantidad de componente aromático que ha detectado cada sensor. Después de oler, se debe inicializar el sistema introduciendo aire completamente limpio. La tecnología para la identificación automática de los olores (en cualquier tipo de aplicación,

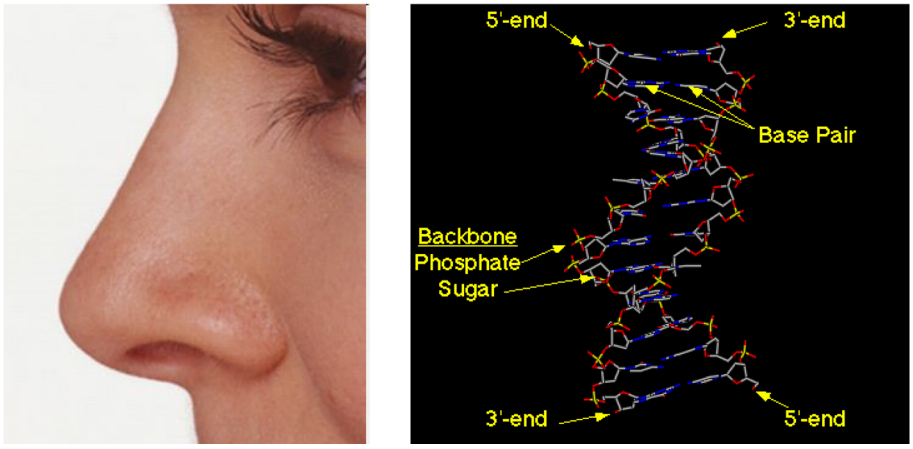
no solo identificación biométrica) está siendo investigada y hoy en día hay pocos sistemas reales (no prototipos de laboratorio) en funcionamiento y ninguno para identificar a personas.

- **ADN**: El ácido desoxirribonucleico es el código unidimensional que caracteriza al individuo por excelencia, excepto a dos gemelos idénticos, que tienen el mismo ADN. Normalmente, se usa en la identificación de personas en aplicaciones forenses, pero no se puede emplear en aplicaciones de tiempo real debido a que se necesita un tiempo de unas horas en un laboratorio para aislar correctamente el ADN y extraer la información básica. Además, el uso de la información del ADN suele preocupar a las personas porque se puede extraer el conocimiento de que una persona sufre ciertas enfermedades o es susceptible de que las sufra.

En la figura 13, mostramos imágenes de los rasgos biométricos acabados de mencionar.

Figura 13. Rasgos biométricos de todo el cuerpo

a. **b.**



a. olor; b. ADN

La tabla 5 muestra las principales características que ha de tener un sistema biométrico en los rasgos biométricos de todo el cuerpo.

Tabla 5. Bondad de los rasgos biométricos de todo el cuerpo

Rasgo biométrico	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Olor	A	M	A	B	B	M	B
ADN	A	A	A	B	A	B	A

Las entradas de la tabla muestran la bondad de cada característica en cada rasgo biométrico discretizada en tres valores: A (alto), M (medio) y B (bajo).

4.4. Rasgos biométricos de comportamiento

Los rasgos biométricos de comportamiento son los siguientes:

- **Hablador**: El reconocimiento del hablador es el sistema menos molesto, ya que el usuario no tiene que esperar a que se tome la imagen. Además, es un sistema que se puede usar a través de un teléfono sin imagen. No se espera que la voz sea suficientemente distintiva como para que se permita la identificación en una base de datos grande. Además, la voz se degrada con facilidad dependiendo del micrófono, la línea de comunicación y los sistemas de digitalización. Es importante considerar que la voz puede quedar gravemente alterada según la salud del usuario (por ejemplo, por un dolor de garganta, un resfriado, el estrés o por emociones fuertes). Además, algunas personas parece que sean muy buenas imitando la voz de otras, por lo tanto son potenciales usuarios fraudulentos.

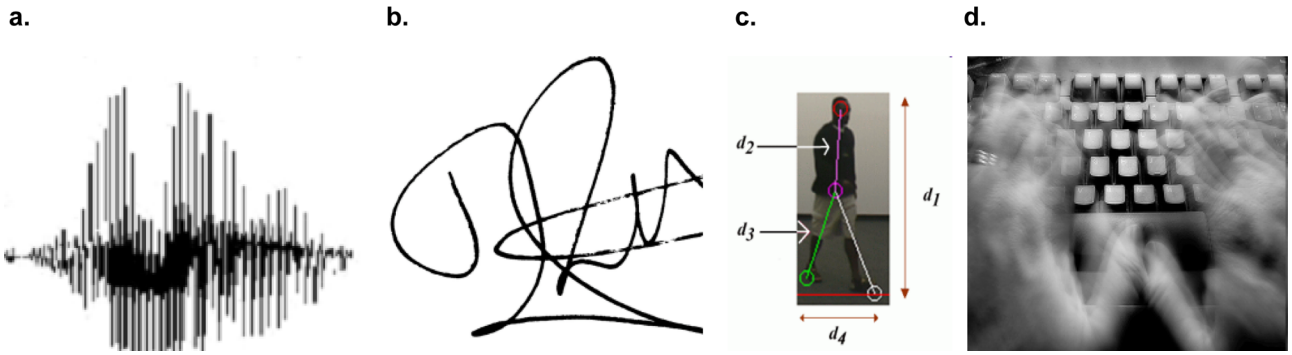
- **Firma**: Las firmas han sido aceptadas en transacciones comerciales, legales y gubernamentales desde hace siglos. La forma como las personas escriben su nombre es un rasgo biométrico de comportamiento. No obstante, es importante considerar que las firmas de algunas personas varían mucho en el tiempo, limitadas por condicionantes físicos y emocionales. Además, los falsificadores profesionales pueden reproducir firmas de forma que parezcan idénticas al ojo humano.

- **Forma de andar** (***gait***): Este rasgo biométrico se refiere a la manera de andar que tienen normalmente las personas. El ritmo y rapidez con el que mueven las piernas, si tienen un paso largo, si se balancean mucho. Tiene la ventaja de que es uno de los pocos rasgos biométricos que se puede (y se tiene que) medir a distancia, lo que provoca que sea muy adecuado en aplicaciones de seguimiento e identificación de personas. La mayoría de los algoritmos extraen la silueta de la persona que se debe identificar y deducen los atributos espacio-temporales de sus movimientos. Este rasgo biométrico tiene la desventaja de que es muy poco permanente, puesto que no solo varía con el tiempo sino que se ve afectado por ejemplo por si se llevan bolsas con peso, si se está cansado o según la ropa que se lleve.

- **Manera de teclear**: Todas las personas tienen su manera de teclear específica y repetitiva cuando encadenan una secuencia de teclas. Este rasgo biométrico no se puede usar para hacer identificación pero sí para verificar si una persona es la que está tecleando en ese momento (o tener una probabilidad de que lo sea). Normalmente, es un rasgo biométrico que se usa de manera encubierta a través de un programa instalado en el ordenador desde el que se está tecleando. Permite la verificación de que la persona que está tecleando no ha cambiado en toda la sesión de trabajo puesto que es un rasgo biométrico que se puede ir verificando continuamente.

En la figura 14, mostramos imágenes de los rasgos biométricos acabados de mencionar.

Figura 14. Rasgos biométricos de comportamiento



a. hablador; b. firma; c. forma de andar; d. manera de teclear

La tabla 6 muestra las principales características que ha de tener un sistema biométrico en los rasgos biométricos de comportamiento.

Tabla 6. Bondad de los rasgos biométricos de comportamiento

Rasgo biométrico	Característica						
	Universalidad	Particularidad	Permanencia	Medible	Rendimiento	Aceptabilidad	No falsificable
Hablador	M	B	B	M	B	A	B
Firma	B	B	B	A	B	A	B
Forma de andar	M	B	B	A	B	A	M
Forma de teclear	B	B	B	M	B	M	M

Las entradas de la tabla muestran la bondad de cada característica en cada rasgo biométrico discretizada en tres valores: A (alto), M (medio) y B (bajo).

4.5. Conclusiones

La **huella dactilar** tiene un gran equilibrio entre todas las características. Casi todo el mundo tiene dedos (excepto las personas con discapacidades en las manos). La historia ha demostrado que las huellas dactilares son muy distintivas y permanentes, aunque aparezcan cortes o quemaduras. Además, los sensores actuales captan las huellas a muy alta resolución a un precio asequible y no tienen el problema de tener que diferenciar el dedo respecto al fondo, como sucede con las caras. El principal inconveniente es que no se pueden capturar huellas dactilares a distancia y sin el conocimiento de las personas, como se puede hacer con las caras. Finalmente, las huellas dactilares y también las plantillas que generan cada vez son más difíciles de falsear gracias a los escáneres detectores de vida (detectan el flujo sanguíneo o el oxígeno que hay en la sangre) y las técnicas de encriptación, respectivamente.

Otro rasgo característico con alto rendimiento, en cuanto a las características biométricas, es el **iris**. Ha demostrado tener una gran universalidad, particularidad y permanencia. Los dos puntos flojos son la poca aceptación que tiene la sociedad actualmente a esta tecnología (relacionado con la dificultad de captar el iris) y el hecho de que no es útil para la busca de pruebas en aplica-

ciones forenses como lo son las huellas dactilares dejadas en las escenas de los crímenes. No obstante, se está empezando a imponer debido a que se ha demostrado que tiene más particularidad que las huellas.

Es interesante mencionar la **geometríade la mano**. A pesar de que solo es medible como único rasgo característico con calidad alta, es útil en algunas aplicaciones de baja seguridad debido a su rapidez, bajo coste y por ser fácil de medir.

Finalmente, hay algunos rasgos biométricos que son poco medibles. Este hecho marca claramente que no sean útiles en algunas aplicaciones donde la rapidez y sencillez del sistema sea primordial. El caso más extremo es el **ADN**, en el que se requieren horas de laboratorio para poder establecer una comparación.

5. Aplicaciones de los sistemas biométricos

Los sistemas biométricos se han desplegado en una gran variedad de entornos de aplicaciones. Las aplicaciones van desde las forenses y los controles en sistemas electorales hasta los teléfonos móviles. No obstante, el diseño y la puesta a punto de los sistemas dependen de los contextos y categorías de las aplicaciones, que a su vez definen los requerimientos de la aplicación.

5.1. Contexto de las aplicaciones

Las aplicaciones se pueden categorizar según los contextos siguientes:

- **Cooperativo frente a no cooperativo**: El sistema cooperativo es aquel por el que el usuario ha de interactuar o cooperar con el sistema para ser reconocido, por ejemplo, centrando el iris en medio de la imagen. El sistema no cooperativo es un identificador de la cara cuando se pasa por una puerta sin que el sistema solicite que la persona se detenga o que mire a la cámara.

- **Habituado frente a no habituado**: Los sistemas habituados son aquellos en los que el usuario accede al sistema de modo habitual, es decir, todos los días cuando llega a trabajar o un comercial que una vez a la semana cruza el control del aeropuerto. Un ejemplo de sistema no habituado es el que requiere la huella para la renovación del carné de conducir cada cinco o diez años. Es un factor importante en el diseño del sistema puesto que se ha demostrado que, si el usuario está habituado a interactuar con el sistema, la precisión de este aumenta claramente.

- **Supervisado frente a no supervisado**: Los sistemas supervisados son aquellos en los que en el proceso de adquisición de los datos está supervisado, observado o guiado por un humano (por ejemplo, un encargado o un funcionario de seguridad). Dentro de los sistemas supervisados, se pueden distinguir aquellos en los que la supervisión solo se lleva a cabo en la matriculación (por ejemplo, un cajero automático con sistema biométrico) o aquellos en los que la supervisión se lleva a cabo en la matriculación y la verificación (el control de los aeropuertos).

- **Entorno de funcionamiento estándar frente a no estándar**: Se considera un entorno de funcionamiento estándar a aquel al que los humanos estamos habituados en cuanto a características de temperatura, presión, luz, humedad y ruido, entre otros. Normalmente, los sistemas que funcionan en entornos cerrados (acceso al ordenador) se consideran sistemas estándares. También lo son los sistemas en entornos abiertos pero en condiciones normales. Los sistemas exteriores se pueden considerar no estándares

si las condiciones son muy especiales (como muy bajas temperaturas, nieve o viento fuerte).

- **Privados frente a públicos**: Los usuarios de los sistemas privados son los clientes directos o trabajadores de una organización que ha desarrollado o que ha desplegado un sistema biométrico. Estos usuarios se clasifican específicamente, ya que son usuarios acostumbrados a usar estos sistemas biométricos y creen en la biometría. Son usuarios potencialmente muy buenos para facilitar los procesos de matriculación, verificación o identificación y, por eso, la razón de error que generan suele ser muy baja. Los sistemas públicos son el resto de los sistemas.

- **Abierto frente a cerrado**: En los sistemas abiertos, la plantilla de un usuario almacenada en la base de datos se puede usar en varias aplicaciones. Por ejemplo, el usuario puede usar la huella dactilar para acceder al ordenador o a la banca electrónica. En los sistemas abiertos, tendremos una sola matriculación y una sola base de datos. En los sistemas cerrados, tendremos que hacer dos matriculaciones y habrá dos bases de datos. En los sistemas abiertos, necesitamos usar formatos estándares y, hoy por hoy, no es un hecho habitual, puesto que la mayoría de los vendedores emplean su propio formato.

- **Declarado frente a encubierto**: Los sistemas declarados son aquellos en los que el usuario se da cuenta y acepta la interacción con el sistema biométrico. El usuario sabe que está presentando el iris, la cara o la huella dactilar al sistema para ser reconocido. En los sistemas encubiertos, el usuario desconoce que se le está aplicando un sistema biométrico para identificarlo. Un ejemplo de esto podría ser un sistema en las salas de espera o en los pasillos de los aeropuertos. Mientras se está tranquilamente leyendo o andando, algunas cámaras ocultas podrían ir detectando a posibles personas perseguidas por la justicia.

5.2. Categorías de las aplicaciones

Se definen dos formas de categorizar las aplicaciones, la categorización horizontal y la categorización vertical.

En la **categorización horizontal**, las categorías son aplicaciones que tienen un entorno u objetivo común. En la **categorización vertical**, las categorías se basan en las necesidades de cada sector de la industria o gubernamental.

A continuación, mostramos una lista de los tipos de aplicaciones según las categorías.

1) Categorías horizontales

- **Control de acceso físico**: La biometría sirve para restringir el acceso de las personas a instalaciones tales como centrales nucleares, zonas militares o cámaras acorazadas de los bancos. Y también a zonas con una seguridad no tan alta, como clubes privados, museos o piscinas públicas.

- **Control de acceso lógico**: Acceso a ordenadores de sobremesa o servidores remotos y base de datos. Cada vez hay más programas informáticos que solo pueden usar personas autorizadas; por ejemplo, en los programas informáticos que se usan en los hospitales, los médicos están autorizados a modificar los datos, pero al personal de enfermería solo se le permite ver los datos sin modificarlos.

- **Autentificación del usuario en transacciones**: Las transacciones económicas se pueden ordenar desde cajeros automáticos o en localizaciones remotas desde ordenadores personales. La biometría añade seguridad a la transacción para reducir el fraude y también para que el ordenante de la transacción no niegue más tarde haberla ordenado.

- **Control de acceso a dispositivos**: Los dispositivos electrónicos personales como, por ejemplo, ordenadores portátiles o teléfonos móviles contienen a menudo datos personales o datos confidenciales. Estos datos se suelen proteger con un número secreto, pero cada vez más se están protegiendo con un rasgo biométrico (hoy por hoy, el más usado es la huella dactilar o la cara).

- **Tiempo y presencia**: Las aplicaciones llamadas de tiempo y presencia son aquellas que mantienen el control de la ubicación de los trabajadores o vehículos de una empresa en todo momento y también sirven para pagar las nóminas según estos parámetros. Añadir un control biométrico asegura que realmente ha sido aquel trabajador en concreto quien ha estado en una ubicación concreta.

- **Identificación civil**: Uno de los objetivos más importantes en las aplicaciones de identificación civil es prevenir múltiples matriculaciones y encontrar duplicados. Por ejemplo, duplicados de pasaportes, permisos de conducir o documentos nacionales de identidad. También se desea descubrir si una persona buscada por la policía está matriculada. La incorporación de los rasgos biométricos a estas aplicaciones es un factor crucial.

- **Identificación forense**: La comparación de las huellas dactilares latentes dejadas en escenas del crimen con una base de datos de criminales es la aplicación más antigua de la biometría. Ahora, se están incorporando tam-

bién las caras, las orejas o la forma de andar, tal como han sido filmadas en cámaras de seguridad. También se buscan marcas latentes de huellas de orejas (la persona se ha apoyado en una puerta para escuchar) o la marca de toda la mano.

2) Categorías verticales

- **Salud**: Hospitales, centros de asistencia primaria, ambulancias.
- **Finanzas**: Transacciones económicas.
- **Recepciones**: Casinos, hoteles, piscinas públicas.
- **Ventas**: Grandes superficies comerciales, gasolineras.
- **Educación**: Control de acceso a escuelas, comedores universitarios.
- **Manufactura**: Control de los trabajadores.
- **Tecnología**: Dispositivos móviles, telecomunicaciones.
- **Transporte**: Control de pasajeros, compra de billetes.
- **Instituciones públicas**: Estado, ayuntamientos, departamentos de justicia.
- **Militar**: Control de acceso a zonas restringidas.

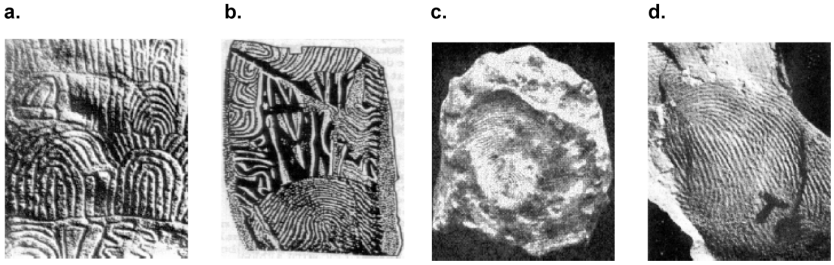
6. Historia de la biometría

Se han descubierto unos cuantos objetos históricos donde se podría deducir que hay huellas dactilares o de la palma de la mano marcadas.

Marcas históricas

Se pueden deducir marcas de huellas dactilares en las esculturas neolíticas de la isla de Gavrinis, que datan del año 3500 antes de Cristo (figura 15a). O también se pueden deducir marcas en las famosas piedras datadas 2000 años antes de Cristo de la isla de Goat (figura 15b). Es importante destacar que en estos objetos no se ha podido demostrar que realmente muestren huellas dactilares o de la palma o que haya un deseo expreso por parte del posible autor de que aquellas marcas representen realmente rasgos biométricos. No obstante, parece que hay suficientes evidencias científicas de que en realidad existe el deseo de identificar al proveedor del objeto a través de las marcas encontradas en un sello de arcilla china datada del año 300 antes de Cristo (figura 15c) y en una lámpara de origen palestino datada del año 400 después de Cristo (figura 15d).

Figura 15. Imágenes de objetos donde se puede deducir la presencia de biometría



a. escultura neolítica de la isla de Gavrinis (año 3500 a. C.); b. piedras de la isla de Goat (año 2000 a. C.); c. sello de arcilla chino (año 300 d. C.); d. lámpara palestina (año 400 d. C.).

Figura 15

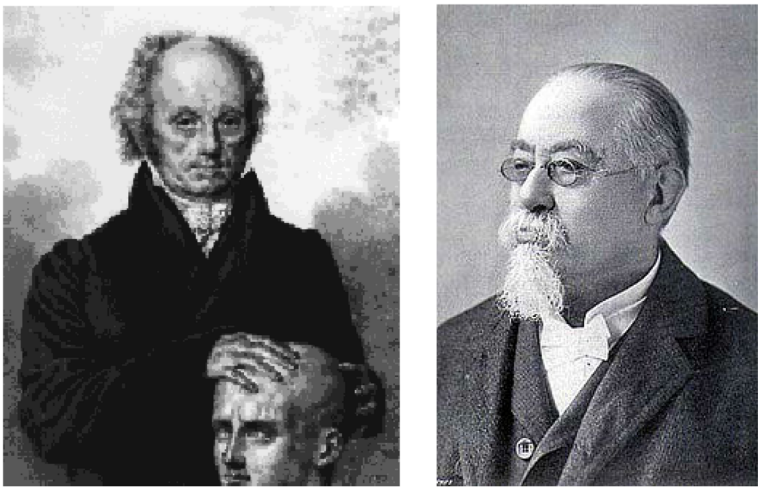
En las figuras a y b es poco probable la presencia de biometría y en las figures c y d es más probable.

Los conocimientos precedentes a la biometría fueron las pseudociencias llamadas frenología y antropometría, que sirvieron para facilitar los inicios de la misma biometría.

La **frenología** estudiaba la estructura del cráneo para determinar el carácter de la persona y su capacidad mental. Fue fundada por el alemán **Franz Joseph Gall** (1758-1828) (figura 16a) a comienzos del siglo XIX en Alemania. Gall creía que ciertas características mentales se podían relacionar con ciertas formas y características del cráneo. Este concepto fue desarrollado con más profundidad por el italiano **Cesare Lombroso** (1835-1909) (figura 16b), que unió los conceptos de la frenología con comportamientos criminales. En Estados Unidos fue donde estas creencias tuvieron más eco hasta finales del siglo XIX.

Figura 16.

a. **b.**



a. Retrato de Franz Joseph Gall; b. retrato de Cesare Lombroso

La **antropología** fue creada por el belga **Adolphe Quetelet** (1796-1874) (figura 17) en 1871. Es una ciencia que se basa en el estudio de las medidas del cuerpo humano para su clasificación y comparación. Quetelet publicó en 1871 la tesis *L'anthropométrie ou mesure des différentes facultés de l'homme*. Además de usarse para crear fichas de rasgos biométricos en las comisarías o prisiones, se utilizó para clasificar a criminales potenciales por sus características faciales. Por ejemplo, Cesare Lombroso, en el documento titulado *Criminal anthropology* y publicado en 1895, afirmaba que los criminales tienen mandíbulas prominentes y que los carteristas tienen las manos largas y la barba poco abundante. Esta parte de la antropometría se consideró con rapidez una no ciencia. No obstante, la identificación de criminales por los rasgos característicos, llamada bertillonaje, se usó en Francia durante la primera mitad del siglo XX. Tal como ya se ha indicado, se descartó por su poca particularidad y para dar paso a la tecnología de las huellas digitales.

Ved también

El bertillonaje se ha tratado en el apartado 1 del presente módulo.

Figura 17. Retrato de Adolphe Quetelet

Mientras estos acontecimientos en frenología y antropología se llevaban a cabo, también avanzaba el interés por la huella dactilar y por la geometría de la mano. En 1823, el checo **Jan Evangelista Purkinje** (1787-1869) (figura 18), mientras estudiaba las glándulas del sudor, se dio cuenta de que parecía que las crestas y los valles que tenemos en la piel de los dedos creaban siempre dibujos diferentes. Es la primera vez que se menciona este hecho pero, no obstante, en ningún momento mencionó que estas características pudieran ser usadas para la identificación de las personas.

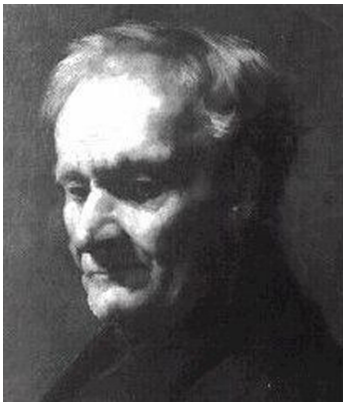


Figura 18. Retrato de Jan Evangelista Purkinje

A finales del siglo XIX, la policía de Scotland Yard puso en marcha un sistema para clasificar e identificar a las personas por sus huellas dactilares. El encargado fue el inspector de policía en Bengala **Edward Henry** (1850-1931)

(figura 7b). Este sistema se basaba en una metodología científica para clasificar las huellas en pocas clases (un máximo de seis) desarrollado por el inglés **Francis Galton** (1822-1911) (figura 7a) en 1892. Se denominaba **sistema Galton-Henry**. El número de seguidores del método Bertillon fue decayendo mientras iba aumentando el de seguidores del método Galton-Henry.

7. Biometría, cine y arte

En este apartado, tratamos la influencia de los avances biométricos en el cine. Y también se hace mención de cómo se puede usar la biometría para decidir la autoría de una obra de arte que hasta el momento se consideraba de autor desconocido.

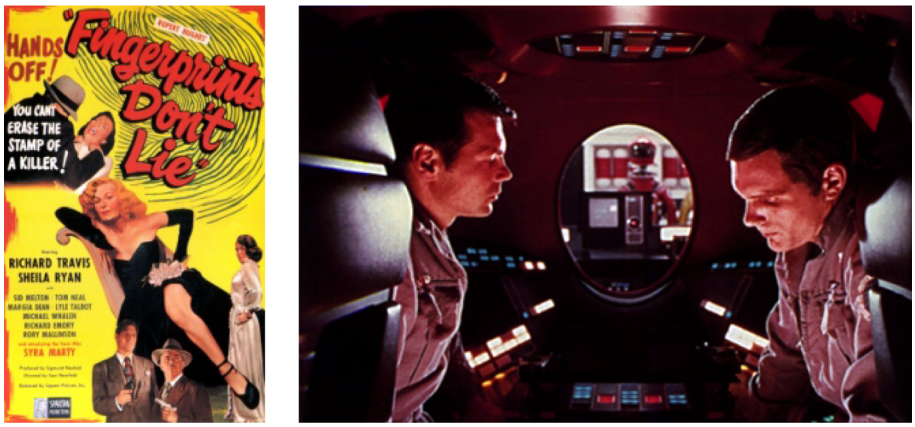
7.1. El cine de la biometría

El cine siempre ha evolucionado junto a la ciencia, a veces avanzándose a ella y prediciéndola, otras, inventando y otras, simplemente mostrando la realidad. En 1951, ya nos encontramos con la película *Fingerprints don't lie*, dirigida por Sam Newfield (figura 19a). En esta película, las huellas dactilares no solo estaban en el título sino que eran el argumento principal de la película. A pesar de parecer una prueba irrefutable, las huellas resultan ser falsas y se demuestra que el policía, quien tenía los conocimientos para falsificarlas, es el asesino.

Unos años más tarde, la ciencia sigue evolucionando y así también lo muestra el cine. En 1968, Stanley Kubrick dirige una de las películas consideradas más influyentes de la ciencia ficción como es *2001: A space odyssey* (figura 19b). El ordenador de la nave espacial, que se llama HAL, es capaz de ver las caras de las personas y deducir lo que están diciendo solo leyendo el movimiento de los labios. Kubrick, ya en 1968, pensaba que en el 2001 una máquina sería capaz de leer los labios de las personas. Hoy en día, todavía no lo hemos conseguido.

Figura 19. Primeras muestras de la biometría en el cine

a. **b.**



a. Cartel de la película *Fingerprints don't lie*; b. fotogramas de la película 2001: A space odyssey

En 1971, aparece *Diamonds are forever*, dirigida por Guy Hamilton. Tiffany Case reactiva una huella dactilar en un vaso, la fotografía, la escanea y descubre que James Bond es Peter Franks. Pero Q se hace pasar por James Bond con un dedo falso (figura 20).

Figura 20. Fotogramas de la película *Diamonds are forever*

Y ya hacia la década de 1980, aparecen los reconocedores de iris y el cine se hace eco de ellos. Dos ejemplos son *Blade runner*, 1982 (figura 21), dirigida por Ridley Scott y donde el estudio del iris sirve para identificar si la persona ha sido creada en una fábrica.

Figura 21. Fotograma de la película *Blade runner*

Y en el clásico de la ciencia ficción *Star Trek II: the wrath of Khan*, de 1982 y dirigido por Nicholas Meyer (figura 22), hay identificación de las personas por la retina.

Figura 22. Fotogramas de la película *Star Trek II: the wrath of Khan*

El 1997, se estrena *Alien: Resurrection* de Jean-Pierre Jeunet (figura 23a). En ella, un ordenador pide al comandante de la nave que se identifique, el comandante echa el aliento, la máquina responde que la identificación es correcta y abre una puerta de seguridad. En una escena posterior, una chica intenta abrir la misma puerta y, cuando la máquina le pide que se identifique, la chica saca un puñado de botellas con líquido (como un ladrón que saca un puñado de llaves), rocía el sensor con el espray de una botella, la máquina contesta que la identificación es incorrecta, lo vuelve a probar con otra botella y la máquina ya la saluda con el nombre del comandante y le abre la puerta.

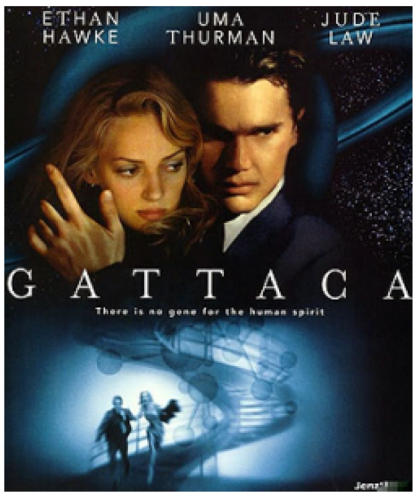
En *Gattaca*, de 1997 y dirigida por Andrew Niccol (figura 23b), se identifica el ADN para averiguar si las personas están libres de enfermedades o taras. Esta película es interesante desde el punto de vista ético puesto que muestra la biometría para la selección de las personas.

Gattaca

Palabra formada por las iniciales de las bases de las que se compone el ADN, adenina (A), guanina (G), timina (T) y citosina (C).

Figura 23. a. Fotograma de la película *Alien: Resurrection*; b. cartel de la película *Gattaca*

a. **b.**



Y ya centrándonos en el milenio actual, en *Mission: Impossible II*, del año 2000 y dirigida por John Woo (figura 24), usan un identificador de retina para leer la misión, un reconocedor facial para identificar a John McCloy y un reconocedor del hablador es falseado usando una grabación.

Figura 24. Fotogramas de la película *Mission: Impossible II*

En la película, *Minority Report*, del 2002 y dirigida por Steven Spielberg (figura 25), se usa la identificación de las personas a través del iris para llevar a cabo publicidad personalizada. Es otro ejemplo de intrusismo.

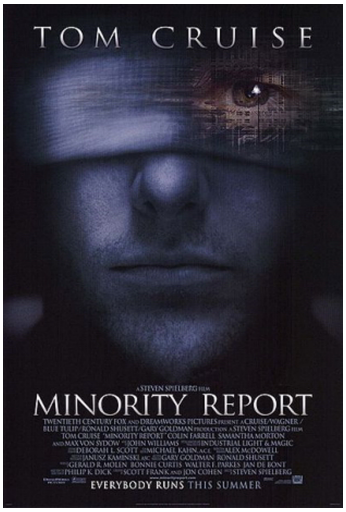


Figura 25. Fotogramas de la película Minority Report

Y también un buen clásico, *I, robot*, del 2004 y dirigida por Alex Proyas (figura 26), nos muestra un control de acceso basado en el lado del puño y un identificador del hablador para acceder a ficheros.

Figura 26. Fotogramas de la película *I, robot*

Y finalmente, en el 2009, el libro *Angels & demons*, escrito por Dan Brown (figura 27), fue llevado a la pantalla de la mano de Ron Howard. En este caso, el malhechor consigue llevarse la antimateria arrancando el ojo del científico que la custodia. Si hubieran instalado un sensor de iris con detector de vida, no habría pasado.

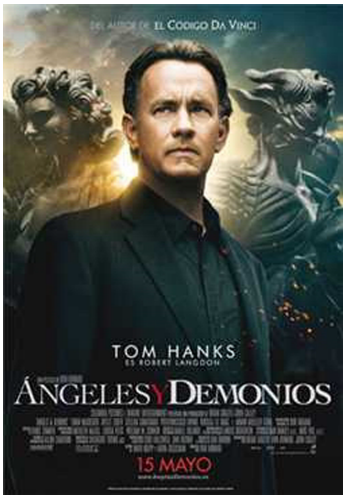


Figura 27. Fotogramas de la película Angels & demons

En la tabla 7, se muestra un resumen de las películas y el rasgo biométrico usado. Tal como puede verse, hay una variedad importante.

Tabla 7. Relación de películas con el rasgo biométrico que tratan

Año	Título	Director	Biometría
1951	*Fingerprints don't lie*	Sam Newfield	huella dactilar
1968	*A space odyssey*	Stanley Kubrick	hablador
1971	*Diamonds are forever*	Guy Hamilton	huella dactilar
1982	*Blade runner*	Ridley Scott	iris
1982	*Star Trek II: the wrath of Khan*	Nicholas Meyer	retina
1997	*Alien: Resurrection*	Jean-Pierre Jeunet	aliento
1997	*Gattaca*	Andrew Niccol	ADN
2002	*Minority Report*	Steven Spielberg	iris
2000	*Mission: Impossible II*	John Woo	retina
2004	*I, robot*	Alex Proyas	lado del puño hablador
2009	*Angels & demons*	Ron Howard	iris

7.2. Biometría y arte

En la figura 28, mostramos una imagen de un cuadro que hasta ahora se consideraba de autor desconocido y que conoce como *The beautiful Princess*. En el año 2007, lo vendió por 19.000 dólares a una galería de arte de Nueva York un coleccionista anónimo suizo. No obstante, ahora se considera que fue pintado por Leonardo da Vinci y tiene un precio superior a los 150 millones de dólares. Esto se debe a que se ha encontrado una huella dactilar de este artista en el cuadro.

Figura 28. La huella dactilar del artista

a. **b.**

a. Reproducción del cuadro *The beautiful Princess*; b. detalle de la huella que podría ser de Leonardo da Vinci

8. Reflexiones sobre una sociedad biométrica

En el Estado español, no existe una ley específica para regular el uso de la biometría. La normativa más cercana es la Ley de Protección de Datos de Carácter Personal. En Francia, y también en algún otro país, existe la Comisión Nacional de Informática y Libertad (CNIL), que autoriza el uso de la identificación biométrica solo si la finalidad de la identificación es el control de acceso de un número limitado de personas a una zona muy determinada (una zona real como, por ejemplo, una instalación nuclear o una zona virtual como, por ejemplo, unos servidores militares), cuya seguridad interesa no solo al propietario de esa zona, sino también al resto de los habitantes. Además, exige que quien instale un identificador biométrico garantice la protección de los datos.

Referencia bibliográfica

Este apartado ha sido extraído, en parte, de la publicación presentada en el diario *Avui* el 3 de julio del 2010, "Una societat biomètrica".

CNIL

En el año 2000, la CNIL prohibió un sistema de identificación de alumnos para acceder al comedor en una escuela de Niza, a pesar de que padres y alumnos estuvieran de acuerdo. La CNIL consideró que la seguridad del acceso al comedor no era lo bastante importante como para instalar un sistema tan invasivo.

En el Estado español, hay varios centros públicos o privados, por ejemplo piscinas, que están instalando sistemas de acceso basados en las huellas digitales. Siguiendo esta línea de razonamiento, en Francia no se permitirían estas instalaciones.

¿Será la biometría un factor importante en nuestras vidas en el futuro? Por supuesto. Y, por ello, el ciudadano tiene que estar informado de los aspectos más importantes relacionados con la biometría, tanto desde el punto de vista tecnológico como desde el legislativo o ético. Porque así estará capacitado para opinar y sus ideas servirán para influir en los cambios sociales que la implantación de las técnicas biométricas provoquen.

Muchos artículos marcan los tristes acontecimientos del 11 de septiembre del 2001 como el pistoletazo de salida de la biometría, si bien es cierto que la inversión en estas técnicas tuvo un punto de inflexión importante en el 2001. Los ingresos generados por los sistemas biométricos pasaron de los 400 millones de dólares de aquel año a los 5.000 millones en el 2010. No obstante, no debemos olvidar que el sistema de identificación de huellas dactilares de Scotland Yard llamado Galton-Henry se puso en marcha en el año 1900. Y sabemos que los egipcios usaban descripciones biométricas para identificar a los trabajadores. Si la biometría hace tanto tiempo que está inventada, ¿por qué ahora se habla tanto de ella? La diferencia no solo es cuantitativa, sino cualitativa. Y es que ahora, si se quiere vivir dentro de la sociedad, se está obligado a usarla. No se puede decir que algo no interesa porque si se dice eso uno acabará siendo un marginado de la sociedad y no tendrá acceso a ningún servicio que esta pueda proporcionar. Y, por eso, hay que entender qué es una sociedad con tecnología biométrica.

En la mayoría de los Estados, se están creando bases de datos con información biométrica con el objetivo de garantizar la seguridad de los ciudadanos. El FBI administra el sistema de reconocimiento de huellas dactilares denominado

Integrated Automated Fingerprint Identification System, que dispone de 50 millones de posibles criminales con su información biométrica y su historia criminal. La tendencia es clara, las bases de datos irán creciendo tanto en número de individuos como en volumen de información de cada individuo.

¿Nos tienen que preocupar estas bases de datos? Como reza el dicho, *la información es poder*, pero ¿qué información aportan esos datos? ¿Nos tiene que preocupar que la base de datos haya almacenado que yo tengo una huella dactilar de tipo lazo en el dedo índice? ¿Y si almacena el ADN? En este punto, es importante discernir entre identidad e identificación.

La **identidad** es la personalidad de cada persona, un sistema complejo en permanente construcción que extrae su riqueza de la multiplicidad de sus características físicas, psíquicas, sociales o culturales. La **identificación** son un conjunto de caracteres únicos para cada persona y asignados de una manera casi arbitraria.

Nos tendría que preocupar el almacenamiento de nuestra identidad, pero no el de nuestra identificación. De la información de las huellas dactilares podemos extraer una identificación casi única. Pero ¿se puede extraer de ellas la identidad? En el caso de la huella dactilar, hoy en día parece difícil, pero ¿que pasa con el ADN? No olvidemos la película *Gattaca* (1997), donde es posible la selección genética de modo que los hijos se vean libres de enfermedades y eso implica que solo los genéticamente correctos pueden optar a los mejores puestos de trabajo. ¿La ciencia acumulará los conocimientos necesarios para llegar a esa situación social? No está claro, pero lo que es seguro es que la humanidad tiene deseo de ciencia y que esto nos hace diferentes a los demás animales y la historia ha demostrado que es inútil intentar pararla.

DNI

Cuando el dictador Franco creó el documento nacional de identidad (DNI) en 1944 se equivocó con el nombre, puesto que se tendría que haber llamado de identificación.

La utilización de la biometría parece presentar ventajas prácticas para el ciudadano y económicas para las empresas. No obstante, la generalización de la biometría en todos los campos puede constituir un peligro real para el respeto a la vida privada. Nos encontramos en una disyuntiva que la sociedad debe ser capaz de solucionar. Por suerte, se están creando organismos independientes e internacionales que controlan el uso abusivo de la información biométrica. Un caso concreto es la ya comentada CNIL en Francia. La ciencia avanza para solucionar los problemas técnicos que aparecen. Las legislaciones se van adaptando para incorporar los conceptos biométricos. ¿Cuándo y dónde confluirán? El reto no es aceptar o no la biometría sino ser capaces de convivir en paz con ella.

Resumen

En este módulo, hemos descrito los rasgos biométricos que se usan en la actualidad y hemos descrito las características principales que deben tener para que sean útiles en ciertas aplicaciones. Hemos visto que no todos los rasgos biométricos se pueden usar en cualquier aplicación; hay rasgos biométricos que se adaptan mejor a unos tipos de aplicaciones y otros que se adaptan a otros tipos de aplicaciones.

Hemos descrito los tres sistemas biométricos básicos: identificación, verificación y matriculación. Hemos visto que tienen características que los distinguen, pero disponen de partes o procesos comunes. También hemos descrito los tipos de aplicaciones biométricas reales.

Hemos acabado el módulo explicando un poco de historia de la biometría, comentando películas de cine y reflexionando sobre el impacto que esta ciencia, antigua pero ahora muy emergente, va a tener sobre nuestra sociedad.

Actividades

1. Tomad las medidas de Bertillon a dos personas, acabad de rellenar la tabla 8 (en centímetros). Rellenad la tabla 9 con las distancias euclídeas y decidid cuál es el valor máximo que debe tener el umbral de Bertillon para que se consideren las cuatro personas diferentes. Ahora supongamos que Will West y William West eran realmente la misma persona tal como se creyó al principio. ¿Qué valor mínimo y máximo debe tener el umbral?

Tabla 8. Ficha de Bertillon

Parte del cuerpo	Will West	William West	Persona 1	Persona 2
Altura	178,5	177,5		
Anchura de los brazos	187,0	188,0		
Altura sentado	91,2	91,3		
Largura de la cabeza	19,7	19,8		
Anchura de la cabeza	15,8	15,9		
Largura de la oreja derecha	14,8	14,8		
Largura de la oreja derecha	6,6	6,5		
Largura del pie izquierdo	28,2	27,5		
Largura del dedo corazón izquierdo	12,3	12,2		
Largura del dedo meñique izquierdo	9,7	9,6		
Largura del antebrazo izquierdo	50,2	50,3		

Tabla 9. Distancias euclídeas

Distancia	Will West	William West	Persona 1	Persona 2
Will West	0			
William West		0		
Persona 1			0	
Persona 2				0

2. ¿Qué tanto por ciento de ingresos aporta el reconocimiento de la huella dactilar respecto a los demás rasgos biométricos? ¿Y cuál es el segundo rasgo biométrico?

3. Los ingresos de los sistemas biométricos entre los años 2007 y 2015 (previsión en los últimos años) respecto al tiempo es una función lineal. ¿Qué pendiente tiene? Si se mantienen las predicciones, ¿qué ingresos supondrán en el año 2020?

4. Explicad las diferencias que existen entre el sistema de verificación y el sistema de identificación. Cuándo se usa uno y cuándo el otro. Los algoritmos para comparar rasgos biométricos pueden ser muy costosos temporalmente. Por ese motivo, resulta frecuente usar algoritmos subóptimos que encuentran una distancia muy rápidamente pero puede ser que no obtengan la distancia exacta. ¿En cuál de los casos es importante usar un algoritmo subóptimo?

5. Explicad en qué consiste la matriculación. Normalmente, en los sistemas de matriculación hay un encargado que verifica los datos y todo el proceso de captura de los rasgos biométricos.

¿Por qué es tan importante comprobar que este proceso se hace correctamente? Relacionad este hecho con los tipos de errores posibles: falsas aceptaciones o falsos rechazos.

6. ¿Cuáles son los seis procesos relacionados con los sistemas de verificación, identificación y matriculación?

7. Describid una aplicación real que use un sistema fuera de línea y otra que use un sistema en línea.

8. Explicad la diferencia entre los dos tipos posibles de buscas: positivas y negativas. Describid un par de aplicaciones reales que sean de los dos tipos.

9. Describid y relacionad la universalidad y la particularidad.

10. Describid y relacionad la permanencia y que sea medible.

11. Describid y relacionad el rendimiento y la aceptabilidad.

12. Confeccionad una tabla donde se muestren todos los rasgos biométricos clasificados por la parte del cuerpo donde se encuentran. Describid su característica principal y una aplicación real donde se podrían utilizar.

13. ¿Qué diferencia hay entre los rasgos biométricos de comportamiento y los rasgos biométricos físicos?

14. Estudiad en detalle las tablas donde se muestra la bondad de los rasgos biométricos. Las valoraciones son muy sugestivas, ¿cambiaríais alguna valoración? Tened en cuenta los comentarios que hay después de todas las tablas. ¿Qué valoraciones creéis que cambiarán de aquí a diez años?

15. Describid los tipos de contexto que hay en las aplicaciones biométricas. Ejemplificad cada opción con una aplicación real.

16. Describid los tipos de categorías horizontales que hay en las aplicaciones biométricas. Ejemplificad cada opción con una aplicación real.

17. Describid los tipos de categorías verticales que hay en las aplicaciones biométricas.

18. ¿Desde cuándo se puede considerar que la biometría se aplica para la identificación de las personas? Explicad el primer caso.

19. ¿Creéis que los casos comentados sobre la existencia de posibles rasgos biométricos anteriores al siglo XIX son realmente aplicaciones biométricas para la identificación de las personas?

20. ¿En qué consistía la frenología? ¿Creéis que es una ciencia?

21. ¿En qué consistía la antropología? ¿Creéis que es una ciencia?

22. Describid el primer sistema biométrico puesto en funcionamiento. ¿Qué rasgo biométrico usaba? ¿Servía para identificar o para verificar?

23. ¿Creéis que es correcto aplicar un sistema biométrico para acceder a una escuela? ¿Y para identificar a personas en zonas conflictivas o de guerra? ¿Creéis que debe haber una comisión especial que decida si se puede implantar o no un sistema biométrico? ¿De ámbito estatal, continental o mundial?

Abreviaturas

AFIS *automatic fingerprint identification system* (sistema de identificación automático de huellas dactilares)

FVC Fingerprint Verification Competition

IVC Iris Verification Competition

Bibliografía

Bhanu, Bir; Chen, Hue (2008). *Human ear recognition by computer*. Springer.

Chen, C. H. (2010). *Handbook of pattern recognition and computer vision*. Springer.

Duda, Richard; Hart, Peter; Stork, David (2001). *Pattern classification*. Wiley.

Escolano, Francisco; Suau, Pablo; Bonev, Boyán (2009). *Information theory in computer vision and pattern recognition*. Springer.

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

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

Jebara, Tony (2004). *Machine learning. Discriminative and generative*. Kluweer Academic Publishers.

Li y otros (2005). *Handbook of face recognition*. Springer.

Maltoni, Davide; Maio, Dario; Jain, Anil; Prabhakar, Salil (2009). *Handbook of fingerprint recognition*. Springer.

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

Nixon, Mark; Tan, Tieniu; Chellappa, Rama (2006). *Human identification based on gait*. Springer.

Pekalska, Elzbieta; Duin, Robert (2005). *The dissimilarity representation for pattern recognition*. World Scientific.

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

Roy, Kaushik; Bhattacharya, Prabir (2008). *Iris recognition. A machine learning approach*. Verlag Dr. Muller.

Szeliski, Richard (2011). *Computer vision: algorithms and applications*. Springer.

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

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

Zhang, David (2004). *Palmprint authentication*. Kluweer Academic Publishers.