Biometría

Carles Fernández Tena

PID_00194177

UOC
Universitat Oberta de Catalunya

Índice

1. Introducción. Fundamentos de la biometría. Antecedentes históricos

La biometría se suele concebir popularmente como un campo totalmente moderno e innovador, con ideas salidas de las novelas y el cine de ciencia ficción. No obstante, a lo largo de la historia de la humanidad, en todas las civilizaciones antiguas ha habido un gran número de acontecimientos en los que aparece repetidamente la idea de **identificar a las personas** o de **verificar sus identidades**, basándose únicamente en sus rasgos físicos o de comportamiento.

Desde el 6000 a. C., y de forma repetida, se tiene constancia del uso de huellas dactilares y manuales para la identificación personal por parte de diversas civilizaciones, como por ejemplo la asiria, la babilónica, la japonesa y la china. No fue hasta finales del siglo XX cuando se presenció de forma conjunta la aparición y consolidación de nuevas biometrías, entre las que destacan la **facial**, la de **iris** y la de **voz**. A continuación detallamos algunos acontecimientos importantes de la historia de la biometría.

- Hacia el 3000 a. C., en el antiguo Egipto eran rutinarias las grabaciones de rasgos y medidas corporales para las transacciones comerciales y oficiales. Los faraones refrendaban los decretos por medio de huellas dactilares. Los trabajadores de las pirámides eran identificados por su nombre, procedencia, estatura, complexión, rasgos faciales y de comportamiento y otras características particulares, como por ejemplo cicatrices. Este fue el caso durante la construcción de la pirámide de Keops, para evitar que se falseara la identidad de los trabajadores con ocasión del reparto de las raciones mensuales de alimentos.
- También en la antigua civilización babilónica se tiene constancia del uso de huellas de la palma de la mano para probar la autenticidad de ciertas obras de artesanía, como la de los grabados, por ejemplo.
- Se han encontrado huellas dactilares provenientes de la antigua China, datadas entre el 610 y el 910 d. C. Joao de Barros, explorador y escritor, registró históricamente uno de los primeros usos de la biometría por parte de los mercaderes chinos, quienes imprimían con tinta la huella de la palma de la mano y del pie de niños en papeles para verificar su identidad. El mismo procedimiento utilizaban para la compraventa de terrenos, contratos y pagarés.
- En el siglo VII d. C., Suleyman, mercader árabe, usaba huellas dactilares como prueba de validez entre prestatarios y prestamistas.
- Hacia el año 1000 d. C., Quintiliano, un abogado del Imperio romano, procedente de Hispania, consiguió exculpar a un hombre ciego del asesinato de su madre tras demostrar que las huellas de sangre de las palmas de la mano encontradas en la escena del crimen se utilizaron para incriminarlo.
- Se han encontrado varios documentos oficiales de la Persia del siglo XIV con impresiones de huellas dactilares. Un doctor oficial del gobierno observó que no había dos huellas completamente iguales.
- Ya en época moderna, el fisiólogo checo Han Evangelista Purkyně incidió de nuevo en esta idea al descubrir en 1823 que las excreciones de sudor en la mano de una persona producían patrones únicos, hecho que le llevó a concebir la posibilidad de identificar a las personas a partir de sus huellas dactilares.
- En 1858, sir William James Herschel, gobernador inglés en la India, marcó los contratos de los funcionarios con impresiones digitales de la palma de la mano para identificarlos y evitar casos de suplantación en los días de pago. Herschel, que dirigió la policía científica de Bengala, concluye que todas las huellas de mano son diferentes y no cambian sustancialmente con el tiempo.
- En el año 1870, Alphonse Bertillon, oficial de la policía francesa, propone el sistema antropométrico (*bertillonage*) para la identificación de criminales. Este sistema se basaba en el registro de medidas corporales, descripciones físicas y características distintivas, como por ejemplo tatuajes, para evitar el falseamiento de la identidad durante

las detenciones. Pronto se desestimó al ver que personas diferentes podían compartir las mismas medidas.

- En la década de 1890, sir Francis Galton crea el primer sistema de clasificación de huellas mediante características discriminatorias (minucias o detalles Galton, todavía utilizados hoy en día) de los diez dedos de la mano, influenciado por el trabajo de Bertillon, Herschel y Purkyně. Vucetich implementa el sistema de Galton en Argentina y Henry lo introduce en el Reino Unido, donde además propone un sistema para agilizar la eficacia de las buscas, que sustituye así al *bertillonage*.
- En 1924, la Oficina Federal de Inteligencia de Estados Unidos crea una división de identificación personal, con una base de datos inicial de 810.000 huellas. La busca de coincidencias se hacía de forma manual.
- En el año 1936, el oftalmólogo Frank Burch propone utilizar el iris para la identificación biométrica.
- En 1960 se publica el primer modelo fisiológico de producción acústica del habla, desarrollado por Gunner Fant (KTH, Suecia). Durante los años siguientes se lleva a cabo el primer paso importante para la verificación de identidad mediante el habla, realizado por Lawrence Kersta (Laboratorios Bell), quien introduce el término *voiceprint* (huella de voz) para referirse a la unicidad de los espectrogramas de señal de habla. Inicialmente, los patrones de voz se comparaban visualmente, y a pesar de que el análisis de espectrogramas no obtuvo los resultados esperados, desencadenó la posterior investigación en reconocimiento de hablante y el nacimiento de esta biometría.
- En 1965 se desarrolla el primer sistema de reconocimiento de firma por parte de la North American Aviation.
- A partir de 1965 se empezaron a implementar procedimientos automáticos para la comparación y codificación de huellas dactilares, conocidos como AFIS (*automated fingerprint identification system*). En el año 2000, la base de datos de huellas dactilares del FBI contenía muestras de los diez dedos de las manos de 47 millones de individuos.
- En la década de 1960, Bledsoe, Chan y Bisson proponen el primer sistema semiautomático de reconocimiento facial, en el que un administrador ha de localizar manualmente puntos de referencia de la cara (ojos, nariz, orejas, boca) y el sistema calcula y compara distancias y proporciones entre ellos. En la década de los setenta, estos marcadores se ampliaron con la incorporación de características como el color de los cabellos o el grueso de los labios. Los resultados fueron muy limitados en todos los casos.
- En 1970 se modelan por primera vez las características de comportamiento del habla. El primer prototipo de sistema de reconocimiento de hablante llega en 1976.
- En el año 1974 se desarrollan fuertemente las biometrías de reconocimiento de firma (Stanford Research Institute, en Estados Unidos, y National Physical Laboratory, en el Reino Unido) y de geometría de la mano (Universidad de Georgia).
- El término *biometría* empieza a popularizarse, en la década de 1980, para referirse a los sistemas automáticos de identificación personal.
- En el año 1988, Sirovich y Kirby publican el método de las *eigenfaces* para reconocimiento facial, basado en técnicas de reducción de dimensionalidad (análisis de componentes principales, PCA). Se demuestra que con 100 valores numéricos se puede representar convenientemente una cara alineada y normalizada. En 1991, Turk y Pentland descubren que el error residual de esta técnica se puede aplicar para la detección facial, ya que posibilita la aparición de sistemas de reconocimiento facial en tiempo real.
- En 1987, los oftalmólogos Safir y Flom patentan el concepto general de identificar a personas a partir del iris y, en 1989, piden a John Daugman (Universidad de Harvard) que desarrolle un algoritmo para conseguirlo. En 1994, Daugman patenta su algoritmo, conocido como IrisCode. La patente genérica del reconocimiento de iris expiró en el 2005 y la del algoritmo IrisCode, en el 2011.
- Empiezan a surgir competiciones y programas de evaluación de diferentes biometrías, como por ejemplo, FERET para reconocimiento facial (1993), IAFIS para huella dactilar (1994, 1999), evaluaciones NIST para hablante (anuales desde 1996), FRVT para cara, huella e iris (2000, 2003, 2006, respectivamente), FRGC para cara (2004), etc.
- En el 2000 se publica el primer trabajo sobre reconocimiento biométrico a partir de patrones vasculares, concretamente los de la palma de la mano.
- En el 2005 se presenta la tecnología *iris-on-the-move*, que permite el reconocimiento de iris a distancia y en movimiento.

1.1. Definición y objetivos de la biometría

Una gran cantidad de sistemas actuales no podrían proveer sus servicios sin contar con mecanismos fiables capaces de autentificar la identidad de los usuarios que acceden a los mismos. La finalidad de dichos mecanismos es asegurarse de que los servicios proporcionados por el sistema solo son accesibles a usuarios legítimos, y a nadie más.

Algunos ejemplos de estos sistemas incluyen controles de acceso a edificios y zonas seguras, cajeros automáticos, teléfonos móviles, ordenadores y sistemas informatizados.

Todos ellos serían vulnerables a los impostores, de no existir este tipo de mecanismos.

La forma tradicional de restringir el acceso a estos sistemas ha sido la utilización de **contraseñas** y de **tarjetas de identidad**, es decir, seguridad basada, respectivamente, en el conocimiento de una determinada información y en la posesión de un determinado objeto. Estos métodos, que usamos diariamente para la validación electrónica y para hacer operaciones bancarias, comportan riesgos importantes de seguridad:

- las contraseñas pueden ser divulgadas a usuarios no autorizados;
- si son demasiado sencillas, los impostores pueden averiguarlas fácilmente mediante técnicas de ingeniería social o ataques de fuerza bruta;
- si son demasiado complejas, los mismos usuarios pueden olvidarlas;
- y, de igual forma, las tarjetas de identidad pueden ser utilizadas por terceros.

En estas condiciones, el **campo de la biometría** constituye la forma más adecuada de enfocar las aplicaciones de autentificación, lo que evita los riesgos de seguridad de los métodos tradicionales.

La biometría es la ciencia que trata de establecer la identidad de una persona a partir de una serie de atributos físicos[1] o de comportamiento[2].

[(1)]Por ejemplo, cara, iris, voz, huella dactilar y geometría de la mano.

[(2)]Como la firma, la dinámica de tecleado y el análisis biomecánico de la marcha mientras se anda.

Así pues, la biometría hace posible el establecimiento de la identidad de una persona, basándose más en "quién es" que en "qué posee" o "qué recuerda" (Beardsley, 1972). Concretamente, los sistemas biométricos comparan un conjunto de características extraídas de un individuo con las obtenidas previamente del mismo individuo.

Etimología de la palabra *biometría*

Etimológicamente, la palabra *biometría* denota todo lo relacionado con la medición de seres vivos.

La **ventaja** inmediata de los sistemas biométricos es que los rasgos personales no se pueden robar, compartir ni perder fácilmente. Además, los sistemas biométricos alcanzan normalmente niveles de precisión muy altos, y el balance entre precisión y exhaustividad se puede ajustar para optimizar una determinada aplicación.

Como contrapartida, presentan una serie de **limitaciones**, entre las que cabe citar el posible incremento en el coste de instalación y de ejecución, las dificultades técnicas añadidas al reconocimiento en entornos muy incontrolados o la posible variación significativa de los rasgos biométricos a lo largo del tiempo.

Aparte de los beneficiosos aspectos estrictamente relacionados con las aplicaciones de **seguridad**, la biometría aporta un importante componente adicional de **usabilidad** para los usuarios finales, que no necesitan recordar contraseñas complejas y potencialmente diferentes para cada sistema, ni llevar consigo los instrumentos identificativos en todo momento. Por otro lado, a los sistemas biométricos se les hace habitualmente la crítica de que atentan en mayor o menor medida contra la **privacidad** de las personas, dado el carácter altamente sensible de los datos con los que se trabaja. En este sentido, hay que destacar las recientes mejoras que se han llevado a cabo en el campo de la encriptación biométrica.

1.2. Conceptos básicos

A lo largo de este módulo se emplean regularmente una serie de términos biométricos que hay que definir y saber diferenciar correctamente. Se trata de los de *muestra*, *característica* (o *patrón*) y *plantilla biométrica*.

Las **muestras biométricas** son aquellos datos relativos a una persona que los sistemas biométricos obtienen por medio de sensores.

Por ejemplo, una fotografía de la cara o del iris, una grabación de voz o de vídeo o una huella dactilar.

Por lo que respecta a las **característicasbiométricas** o **patrones biométricos**[3], nos referimos a las características distinguibles del individuo que se pueden medir o calcular a partir de una muestra biométrica que hay que extraer para el proceso de identificación.

Por ejemplo, son características biométricas de una persona la distancia entre sus ojos, el tamaño de su nariz, los patrones irregulares del iris, la distribución de los vasos sanguíneos en la retina o su forma de andar.

[3] Idealmente, estos tendrían que ser únicos e invariantes para cada persona.

Una **plantilla biométrica** es una compilación de información recopilada a partir de una serie de características biométricas, que sirve como resumen de los rasgos más significativos de una persona. Una plantilla recopila información única del individuo de forma eficiente para poder compararla con otras rápidamente.

Una posible plantilla biométrica podría estar formada por el IrisCode del ojo derecho, las minucias dactilares del dedo anular de la mano izquierda y la frecuencia fundamental de la voz.

Los sistemas biométricos emplean sensores para capturar muestras biométricas de una persona, extraen una serie de características a partir de dichas muestras y las recopilan en forma de plantilla biométrica. Posteriormente, la información contenida en las diferentes plantillas se puede comparar para establecer la identidad del individuo.

Las características biométricas tienen que cumplir una serie de **condiciones necesarias** para que se las pueda utilizar de manera efectiva como identificadores personales. Estas condiciones son:

- **Universalidad**. Todas las personas tienen que poseer naturalmente esta característica.

- **Unicidad**. Una misma característica no puede presentarse de una forma idéntica en dos individuos diferentes.

- **Perdurabilidad**. La característica tiene que permanecer inalterable a lo largo del tiempo.

- **Mensurabilidad**. La característica se ha de poder medir físicamente y de forma sencilla por medio de un sensor.

Además de estas condiciones necesarias, es conveniente que las características biométricas también presenten una serie de **propiedades deseables** que hagan más adecuada su implantación real en la sociedad.

Una de las propiedades más obvias de la biometría en cuestión es la de sus **prestaciones**, que engloban no solo la precisión del reconocimiento y el consecuente nivel de seguridad que se deriva de la misma, sino también su rapidez de funcionamiento y el bajo coste de la solución, lo que posibilita su implementación a gran escala.

Otra vertiente de requerimientos tiene más relación con la **aceptación** del sistema por parte de la sociedad, donde la facilidad de uso de la solución y la reducida necesidad de invasión juegan un papel destacado, pero donde también es imprescindible considerar cuestiones culturales y posibles connotaciones negativas de la tecnología.

Finalmente, se debe tener en cuenta asimismo la **facilidad de burlar** la tecnología usando prácticas fraudulentas; por ejemplo, una persona puede utilizar sin autorización fotografías de otro usuario que esté registrado o moldes artificiales de huellas dactilares de otra persona. Para evitar esas prácticas se suelen añadir módulos de *liveness detection*, es decir, de detección de "parte viva" sobre la fisiología presentada (cara viva, ojo vivo, dedo vivo, etc.), que determinan de varias formas posibles si la muestra biométrica proviene de una persona viva o bien se trata de un intento de fraude.

Por otro lado, si nos concentramos en **las funcionalidades** que la identificación biométrica puede ofrecer a la sociedad, cabe destacar las tres siguientes, entre las más importantes:

- **Identificación positiva**, o "¿es esta persona quien dice ser?". Este tipo de identificación permite verificar con un alto grado de fiabilidad si la presunta identidad de una persona, por ejemplo a través de un *login*, está relacionada con la muestra biométrica adquirida por el sensor que hace de contraseña. Las aplicaciones derivadas de este tipo de identificación se utilizan especialmente para controles de acceso, validación de transacciones y autenticación en dispositivos electrónicos.

- **Identificación a gran escala**, o "¿se encuentra presente esta persona en la base de datos?". Se nos permite determinar si una característica biométrica concreta está asociada a alguna de las muchas identidades inscritas en el sistema, que pueden ser del orden de millones, manteniendo la supervisión externa tan reducida como sea posible. Entre las aplicaciones que necesitan identificación a gran escala figuran los controles fronterizos, la identificación de votantes, los carnés electrónicos (de identidad, de conducir), la investigación criminal, la identificación de cuerpos o de niños perdidos.

- **Vigilancia (*screening*)**, o "¿forma parte esta persona de la lista negra?". En este caso, se determina si el individuo en cuestión pertenece a una lista negra (o blanca) de identidades de interés. Se incluyen en esta tipología los sistemas de seguridad por videovigilancia biométrica, como los utilizados en aeropuertos, estaciones o acontecimientos multitudinarios. Debido a su naturaleza, las aplicaciones de vigilancia biométrica pueden no tener acceso a procesos de entrenamiento de usuarios en el sentido tradicional, carecer de control sobre todos los factores relacionados con la captura, como por ejemplo los relativos a las condiciones de iluminación o la correc-

ta orientación de las muestras obtenidas; y tienen que procesar una gran cantidad de datos con la menor supervisión posible.

1.3. Clasificación y comparativa de biometrías

Las tecnologías biométricas suelen clasificarse en dos grandes grupos: las **físicas** y las **de comportamiento**, a menudo también llamadas estáticas y dinámicas, respectivamente.

- El primer grupo se basa en las **características anatómicas del cuerpo**, que varían poco o nada a lo largo de la vida; entre ellas figuran el color de los ojos, las huellas dactilares, el código genético o los patrones del iris.

- En cambio, el segundo grupo de tecnologías analiza las **características de comportamiento del individuo**, que presentan mucha más variabilidad, como sucede con la forma de andar o de escribir.

Biometría de voz

El caso de la biometría de voz suele tratarse de forma especial, puesto que incorpora características de ambos grupos a la vez.

La forma en que se adquieren las características también es una manera habitual de clasificar las biometrías, que pueden ser **activas** o **pasivas**.

- Las activas necesitan la colaboración del individuo para adquirir las muestras (tal como ocurre con la huella dactilar o el reconocimiento de retina).

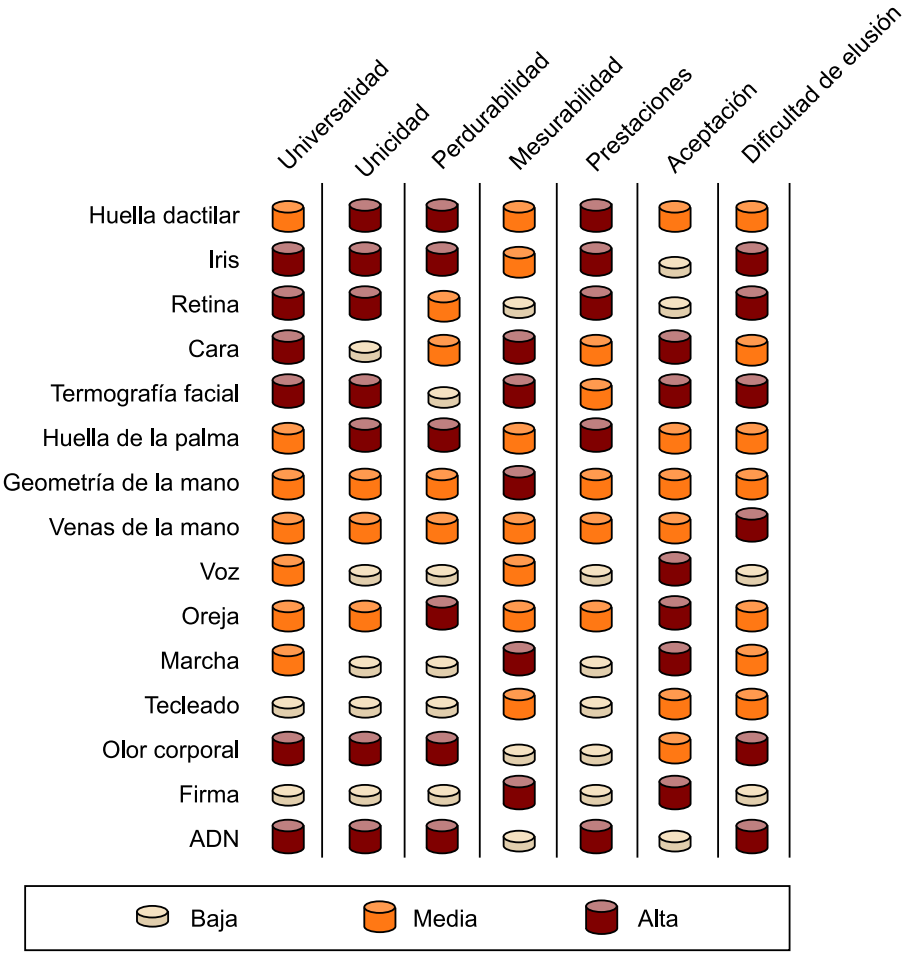
- En cambio, en las pasivas la invasión puede ser prácticamente nula. El individuo no tiene que tomar parte activa en el proceso de reconocimiento, no hace falta que toque ningún dispositivo ni que realice ninguna acción específica. De hecho, ni siquiera es necesario que el individuo sepa que se está llevando a cabo el proceso de reconocimiento.

Ejemplo

Un claro ejemplo de biometría pasiva es la facial, especialmente en el caso de la videovigilancia, en el que las cámaras cubren grandes áreas, se sitúan para capturar vistas frontales de la gente que circula por la zona, y estas personas a menudo no se dan cuenta de la presencia de estas cámaras.

La siguiente tabla muestra la comparativa de una serie de tecnologías biométricas respecto de las siete propiedades necesarias y deseables mencionadas en la sección anterior, en la que se califica cada biometría con un valor bajo, medio o alto de acuerdo con estadísticas llevadas a cabo por diferentes instituciones científicas y organismos especializados en el sector biométrico. Una biometría ideal tendría que tener valores altos para todas las propiedades.

Comparativa de las tecnologías biométricas más habituales, según las propiedades biométricas que poseen en mayor o menor grado.



Como se puede observar, las biometrías **de iris** y **huella dactilar** ofrecen muy buenas prestaciones y han demostrado ser considerablemente resistentes al ruido de los datos, a pesar de que su nivel de intrusión suele estar por encima del deseado. En el caso de la huella genética o de ADN, estas características se llevan al límite, con lo que se obtienen tasas de reconocimiento casi óptimas, aunque resultan completamente intrusivas para el usuario a identificar. Por otro lado, hay biometrías, como la de reconocimiento **facial** y la de reconocimiento de **hablante**, que son especialmente poco intrusivas y se pueden medir fácilmente a distancia; no obstante, a pesar de que generalmente ofrecen buenos resultados, estos suelen estar por debajo de los ofrecidos por las biometrías anteriores, debido, entre otros motivos, a su variabilidad y mayor sensibilidad al ruido y a las interferencias externas. Algunas biometrías, como por ejemplo la de **firma** o la de **dinámicade tecleado**, muestran mayores debilidades por el hecho de que sus resultados pueden resultar muy parecidos entre individuos diferentes, y, por tanto, se pueden falsificar con facilidad, además de que es posible que se vean naturalmente alterados a lo largo del tiempo. Otras tecnologías, entre las que figuran las de reconocimiento de **retina** o de **olor corporal**, han demostrado ofrecer buenas prestaciones en lo referente a

Biometrías de cara, iris, huella dactilar y voz

Cabe mencionar que, a pesar de que a lo largo de los últimos veinte años se han llevado a cabo una gran cantidad de experimentos para evaluar individualmente las biometrías contenidas en la tabla, únicamente se han analizado exhaustivamente cuatro biometrías por medio de importantes iniciativas internacionales a gran escala: se trata de las biometrías de cara, iris, huella dactilar y voz. Este hecho también ha originado un salto cualitativo en la investigación y mejora de estas cuatro tecnologías, mucho más importante que el que se ha podido observar en el resto.

la identificación, pero son muy complicadas de medir, ya sea por una intrusión muy alta (que también comporta un bajo nivel de aceptación), ya por la facilidad con que se contaminan las muestras analizadas.

2. Operativa de un proceso biométrico

Los sistemas biométricos son ejemplos de sistemas **de reconocimiento automático**, en los que las características empleadas para clasificar pueden extraerse de imágenes de cara o de iris, de huellas dactilares, de señales de voz, etc., y las clases a reconocer son las posibles identidades del individuo. Cualquier sistema biométrico consta típicamente de cuatro **módulos** claramente diferenciados:

1) Un **sensor**, que captura el conjunto de datos biométricos del individuo que se presenta al sistema. Por ejemplo, un sensor de huella dactilar que genera imágenes en forma de crestas a partir de los relieves de las puntas de los dedos.

2) Un **módulo de extracción de características**, que procesa los datos capturados por el sensor y extrae una plantilla biométrica en forma de vectores de características. Siguiendo el mismo ejemplo, este módulo analiza la imagen de la huella y extrae posiciones y orientaciones de las bifurcaciones y puntos terminales de crestas, llamadas minucias, que representan la parte fundamental y distintiva de los datos.

3) Un **módulo de comparación**, en el que se confronta la plantilla biométrica extraída del individuo con plantillas guardadas en la base de datos y se cuantifica la similitud entre ellas por medio de puntuaciones.

4) Y, finalmente, un **módulo de decisión**, en el que, a partir de las puntuaciones obtenidas por el módulo anterior, el sistema verifica o establece la identidad del individuo. Por ejemplo, una posible estrategia para determinar identidades sería la de asignar a la persona en cuestión la identidad de la base de datos con la que se obtiene una mayor puntuación, siempre que esta puntuación supere un mínimo umbral de aceptación.

Cualquier sistema biométrico necesita disponer previamente de muestras biométricas de las personas que se quiere identificar. El **proceso de inscripción** o **entrenamiento** es, pues, un paso inicial imprescindible.

A lo largo de dicho proceso se obtienen, mediante un sensor, unas muestras biométricas de la persona que se pretende incorporar al sistema, se extraen sus características biométricas y, finalmente, se crea una plantilla biométrica a la que se asigna externamente la identidad del individuo.

La plantilla etiquetada queda así registrada en la base de datos, preparada para posteriores comparaciones. Mediante este proceso de registro se puede tanto incorporar como actualizar la información biométrica de los usuarios, y dependiendo de la aplicación, es posible que no sea necesaria la intervención humana para etiquetar la identidad del individuo.

Por otro lado, todo sistema biométrico tiene dos posibles modos de funcionamiento, denominados **verificación** e **identificación**. A pesar de que puedan parecer equivalentes, estos procesos siguen en realidad planteamientos diferentes, que tienen asociados distintos niveles de complejidad.

1) En el caso de la **verificación** o autenticación, se tiene que confirmar una identidad que se presenta de forma explícita al sistema. Hace falta, pues, responder a la pregunta "¿es cierto que esta persona es quien dice ser?" o, dicho de otra forma, "¿es cierto que estos datos biométricos corresponden a esta identidad?".

En este caso, el usuario presenta su identidad (por ejemplo, por medio de un *login* al sistema) y la confirma con una señal biométrica que haría de contraseña. Este tipo de planteamiento se denomina comparativa *one-to-one* (1:1).

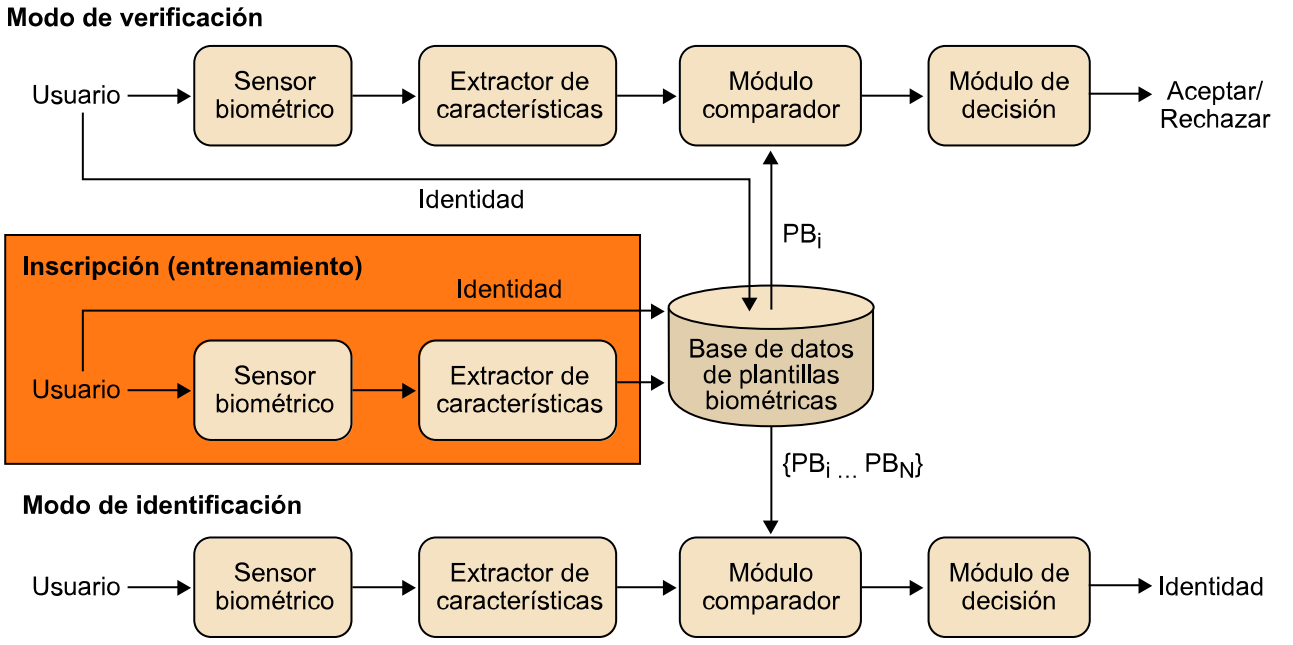
2) Por otro lado, durante el proceso de **identificación**, el sistema tiene que determinar la identidad del individuo entre todas las posibles identidades registradas en la base de datos. La pregunta a responder por este proceso es "¿quién es esta persona?" o "¿qué identidad de las almacenadas corresponde a estos datos?".

Un posible ejemplo consistiría en determinar la procedencia de una huella dactilar encontrada en un escenario policial. En este caso, la comparación se realiza exhaustivamente y se denomina *one-to-many* (1:N).

One-to-few

Existe una alternativa intermedia entre ambos modos de funcionamiento, que se denomina comparativa *one-to-few*. En este caso, el acceso al proceso de identificación está restringido a un número muy limitado de usuarios, típicamente menor de diez, y no es preciso presentar explícitamente la identidad a verificar.

Arquitectura de los dos posibles modos de funcionamiento de un sistema biométrico: verificación e identificación.



2.1. Selección de características

Una de las tareas que pueden resultar más complicadas en un proceso de reconocimiento biométrico, así como en cualquier proceso de reconocimiento automático en general, es la selección **de las características** que se extraerán de la muestra inicial de datos y se utilizarán en el proceso final de clasificación/decisión.

> Las características escogidas han de ser relativamente fáciles de medir y tienen que permitir discriminar entre las clases que queremos diferenciar.

Las características seleccionadas condicionan completamente el resto de las etapas del proceso de reconocimiento, desde la captura de la muestra hasta el tipo de clasificador.

Por poner un ejemplo concreto, imaginemos que queremos diseñar un clasificador para diferenciar de forma automática dos setas tales como la negrilla (*Tricholoma atrosquamosum*) y la lepiota (*Lepiota brunneoincarnata*), mostradas en la siguiente figura. Ambas son muy parecidas entre sí y comunes en el área de Barcelona, pero la segunda de ellas es altamente tóxica y mortal.

Izquierda: Negrilla (*Tricholoma*) (http://ca.wikipedia.org/wiki/Fitxer:Tricholoma_terreum.jpg). Derecha: Lepiota (*Lepiota*) (http://en.wikipedia.org/wiki/File:Lepiota_brunneoincarnata_060823w.jpg)

Siempre que nos planteemos abordar un problema de reconocimiento habremos de pasar necesariamente por una serie de etapas, incluidas en el llamado **ciclo de diseño** que se presenta a continuación.

Ciclo de diseño de un proceso de reconocimiento.

En primer lugar, hay que **recoger la información** que utilizaremos para clasificar los datos proporcionados por un sensor mediante una serie de observaciones.

En el caso propuesto, podríamos obtener datos, como por ejemplo la altura total, la longitud del tallo o la longitud de la circunferencia del sombrero. Pero estas medidas parecen ser bastante similares en ambas especies de setas, de forma que tendremos que plantear la captura de otros datos, como los proporcionados por fotografías de la parte inferior del sombrero y del contorno de perfil de cada seta. Cualquier característica escogida tiene problemáticas inherentes: las fotografías son sensibles a las condiciones de iluminación y a la posición de las setas en el momento de la captura, y los contornos pueden presentar grandes variaciones (incluso para una misma seta) y ser difíciles de comparar entre sí.

El siguiente paso es **seleccionar y extraer las características** a utilizar por el clasificador. Esta selección depende de la información a priori que tengamos, del coste de adquirir las características, de la invariancia de dichas características (a traslación, rotación, escala, distorsión, oclusión, deformación...) y, especialmente, del poder discriminante que tengan. Es decir, hace falta que las características sean similares para clases iguales y diferentes para clases distintas.

Realizando un estudio más exhaustivo de los datos del ejemplo anterior, o utilizando conocimientos previos sobre micología, se puede comprobar que las principales diferencias entre las dos setas son la textura escamosa de la parte inferior del tallo (presente en la lepiota, pero no en la negrilla), el color de las láminas debajo del sombrero (más claro en las lepiotas) y la estructura laminar de debajo del sombrero (que en las lepiotas no suele tocar el tallo, y en las negrillas sí). Por razones logísticas, puede resultar más sencillo medir la textura del tallo que las láminas del sombrero, puesto que para las otras dos opciones tendríamos que girar la seta y obtener una imagen inferior, que siempre quedaría escondida parcialmente por el tallo. En cambio, obtener una fotografía del tallo es sencillo: la textura no varía circularmente, y la clara dirección del tallo nos posibilita el alineamiento automático de las imágenes.

Existen técnicas de visión para aislar los objetos de interés del fondo de la imagen (segmentación de objetos) y otras para detectar el ángulo y posición de las rectas más notorias de una imagen (transformada de Hough), con lo que podemos obtener las siguientes imágenes normalizadas, más preparadas para la clasificación. Estas tareas preparatorias, que se denominan etapas de **preprocesamiento**, son habituales durante la extracción de características.

Preprocesamiento

El preprocesamiento suele constituir una parte muy importante dentro del algoritmo final de reconocimiento y puede llegar a ser bastante complejo en algunos casos.

Imágenes alineadas y segmentadas del final del tallo en cuatro muestras de setas.

Las dos primeras corresponden a negrillas, las dos últimas a lepiotas.

En este ejemplo, podemos refinar todavía más las características seleccionadas mediante técnicas de visión para prepararlas para el reconocimiento. La visión por ordenador es uno de los campos más utilizados para la extracción de características, debido al enorme potencial que ofrece, y las tecnologías biométricas son un claro ejemplo de ello: son pocas las biometrías que no fundamentan sus algoritmos en la captura, procesamiento y clasificación de características visuales. Para este ejemplo podemos utilizar técnicas clásicas de morfología que detecten los contornos principales de la imagen; entre ellas, las de los métodos de **Sobel** o los de **Canny**, que se suelen utilizar también para las biometrías de iris y de huella dactilar.

Procesamiento de las características discriminantes a partir de imágenes en las que se ha aplicado un método de detección de contornos.

Hay que encontrar una nueva representación de las características que deje clara constancia de la diferencia entre clases.

Las imágenes binarias obtenidas parecen estar más cerca de una cuantificación numérica que nos permita discriminar las clases. Pueden existir multitud de características válidas para ayudarnos a resolver un problema de reconocimiento concreto.

En este caso, se nos ocurren dos:

- Utilizar morfología de imagen para contar el número de regiones conexas en imágenes de seta normalizadas en la misma área.
- Calcular el porcentaje de variación vertical de píxeles. Se puede estimar tomando la imagen de contornos $I_C(x, y)$, haciéndole la derivada vertical, sumando las contribuciones en valor absoluto y dividiéndolo entre el número total de píxeles $\|I_C(x, y)\|$:

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

Tomando como ejemplo las cuatro observaciones de setas anteriores, cada una etiquetada como clase “negrilla” o clase “lepiota”, los valores numéricos para las dos características seleccionadas son los siguientes.

	Negrillas		**Lepiotas**	
	Imagen 1	**Imagen 2**	**Imagen 3**	**Imagen 4**
n.º regiones conexas	33	38	192	262
% variación vertical	0,012	0,011	0,065	0,060

Podemos observar que las dos características seleccionadas parecen separar correctamente las clases negrilla y lepiota en el espacio de características. Seguramente nos decidiríamos por el segundo modelo, que tiene más coherencia estadística al presentar propiedades de probabilidad.

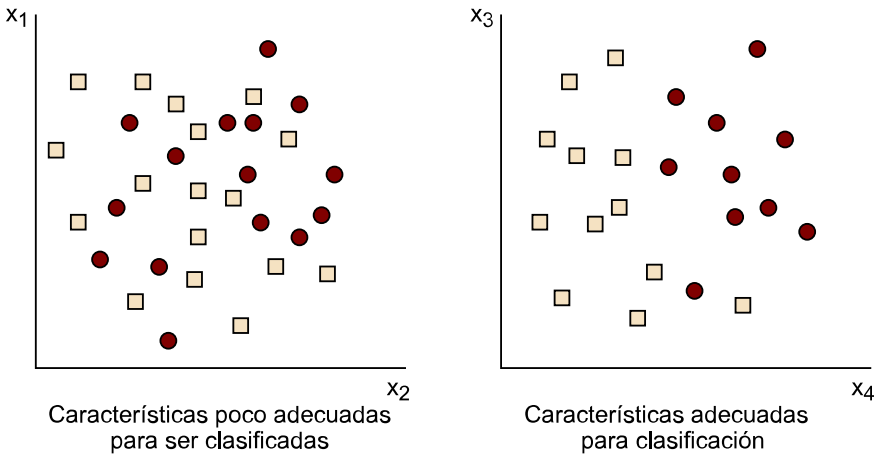
Continguts

Continguts

Continguts

A pesar de que hemos conseguido encontrar características que discriminan entre las clases, este paso puede llegar a ser muy difícil de lograr en la práctica. Generalmente, los algoritmos de clasificación que se verán a continuación pueden ser más robustos si se utilizan varias características combinadas y se buscan modelos de decisión más adecuados para espacios multidimensionales.

En el supuesto anterior se podría dibujar la medida escogida de "variación vertical de contornos" en el eje horizontal y, por ejemplo, una medida de "croma (color) de las láminas" en el eje vertical. Si las características escogidas, pongamos por caso las de longitudes y anchuras en el ejemplo de las setas, no fueran muy discriminantes, nos encontraríamos con el caso de la izquierda de la figura siguiente, donde las observaciones de cada clase quedan mezcladas en el espacio de características. En cambio, si fueran discriminantes, el espacio resultante nos permitiría separar fácilmente las clases en general (gráfico de la derecha de la siguiente figura).



No todas las características tienen el mismo poder discriminante, ni son igualmente adecuadas para la clasificación. Además, el uso de diferentes características combinadas puede beneficiar al sistema final.

2.2. Clasificación

Siguiendo el ciclo de diseño de un proceso de reconocimiento, una vez escogidas las características discriminativas (en el ejemplo de las setas, la "variación de píxeles verticales"), hay que **seleccionar un modelo de clasificación** que, primero, aprenda reglas a partir de las observaciones disponibles y, después, decida de forma automática cuál es la clase más adecuada para una nueva observación, desconocida hasta ahora. En nuestro caso, al observar la fotografía de una nueva seta, el clasificador decidirá si pertenece a la clase "lepiota" o a la clase "negrilla".

A grandes rasgos, un **clasificador** sirve para encontrar de forma óptima cuál es la frontera entre las posibles clases en el espacio de características.

Ejemplo

Por ejemplo, si tomamos como característica la variación de píxeles verticales, podríamos escoger a primera vista un umbral cercano a 0.040 para decidir si nos encontramos ante una lepiota o una negrilla, dependiendo de si el nuevo valor observado es mayor o menor que dicho umbral.

No obstante, para crear modelos robustos hay que trabajar, en primer lugar, con un conjunto más grande de observaciones, del orden de centenares o miles de ejemplos etiquetados. Además, es mucho más razonable escoger los umbrales o fronteras de clasificación mediante métodos de aprendizaje automático, que generan modelos de decisión matemáticamente óptimos a partir del conjunto de observaciones.

Existen muchos **métodos de clasificación** que nos permiten desarrollar sistemas de reconocimiento automático. Estos métodos se dividen en tres grandes tipos, según como aprendan a partir de las observaciones:

- **Aprendizaje supervisado.** Es el más común. Se dispone de un conjunto de datos de entrenamiento, es decir, que a cada observación del conjunto se le ha asignado manualmente una etiqueta de clase o un coste. Se pueden enumerar muchas técnicas de clasificación basadas en aprendizaje supervisado, entre las que figuran las de los *k*-vecinos más cercanos, las redes neuronales que utilizan *backpropagation*, las máquinas de apoyo vectorial (SVM), los algoritmos de *boosting* o el algoritmo ID3 para la construcción de árboles de decisión.

- **Aprendizaje no supervisado.** El sistema agrupa los datos de forma automática (*clustering*), según cómo estén distribuidos en el espacio de características. Cada grupo localizado constituye una clase, y esta asignación de clases se hace de forma automática. Algunos ejemplos de aprendizaje no supervisado son el algoritmo *k-means*, los modelos de mezclas de gaussianas (GMM) o las redes neuronales autoorganizativas (SOM).

- **Aprendizaje por refuerzo.** No se da ninguna información de clases de forma explícita, pero un agente externo le va comunicando al sistema si cada decisión tomada es correcta o incorrecta, información que el sistema utiliza para mejorar sus reglas de decisión. Dos ejemplos clásicos de aprendizaje por refuerzo son los métodos de Montecarlo y el aprendizaje por diferencia temporal.

La selección del tipo de clasificación depende de la naturaleza de cada problema, pero en general, y particularmente en el caso del reconocimiento biométrico, nos encontraremos mayoritariamente ante casos de aprendizaje supervisado, en los que nos es posible "etiquetar" cada observación con la clase que le corresponde. Una vez escogido el tipo, un mismo problema se puede resolver utilizando diferentes modelos concretos.

Per ejemplo, en el caso del reconocimiento facial (aprendizaje supervisado) es común usar SVM, redes neuronales o *boosting*.

A continuación se describen muy brevemente algunos de los modelos de clasificación supervisada más habituales:

- **Clasificador lineal.** Es un clasificador binario que divide el espacio de características en dos zonas (por ejemplo, lepiota o negrilla), según una serie de características observadas (en este caso, podrían serlo la textura del pie y el color de las láminas). En un espacio de características $\mathbb{R}^2$ se trataría de una recta, en $\mathbb{R}^3$ de un plano, etcétera.

- ***k*-vecinos más cercanos** (*k-nearest neighbors*, kNN). Es uno de los métodos más simples de clasificación a partir de un conjunto de entrenamiento etiquetado. Un objeto nuevo se clasifica según el voto de la mayoría: se le otorga la clase/etiqueta más común entre los *k* vecinos etiquetados que le son más cercanos en el espacio de características.

- **Regresión logística**. Describe las relaciones entre una serie de variables independientes, como altura, peso, sexo, etc., y una respuesta binaria de salida, expresada en forma de probabilidad (por ejemplo, "¿tiene problemas de sobrepeso?"). Se utiliza la función logística $f(x) = 1/(1+e^{-x})$ para modelar la probabilidad de salida como combinación lineal de los parámetros de entrada.

- **Clasificador bayesiano ingenuo (*naive*)**. Es un clasificador basado en el teorema de Bayes, en el que el modelo se simplifica suponiendo independencia entre todas las variables. De esta forma, las probabilidades condicionales se transforman en productos de probabilidades, con lo que los cálculos resultan mucho más sencillos.

- **Árboles de decisión** (o de clasificación). Predicen la clase a la que pertenece una observación en función de los atributos observados. A partir de un nodo inicial, el modelo se pregunta sobre alguno de los atributos en particular y, dependiendo de la respuesta, conduce a través de las ramas a un nodo de salida (cada una de las hojas) que corresponde a la clase asignada. Las "preguntas" que hay que hacer sobre los atributos se escogen secuencialmente utilizando diferentes criterios, como el de mínima entropía.

- **Redes neuronales (artificiales)**. Este modelo de clasificador se inspira en la naturaleza de las redes neuronales biológicas. Cada neurona se modela como una función sencilla de respuesta no lineal, y un número considerable de estas neuronas se organizan en una red de capas interconectadas masivamente. La fase de entrenamiento consiste en calcular el peso asignado a cada conexión a partir de los atributos de entrada y los valores de salida. Para hacerlo se utilizan algoritmos como, por ejemplo, el de *back-propagation*.

- **Máquinas de vectores de soporte** (*support vector machines*, SVM). Son métodos de clasificación binaria que, como los clasificadores lineales, buscan la frontera que maximiza la separación entre dos clases. Sin embargo, los SVM se basan únicamente en los puntos más cercanos a la frontera (los llamados vectores de soporte), que son los más críticos a la hora de decidirse por una categoría u otra. Los SVM permiten transformar los datos iniciales en nuevos espacios en los que las clases sean más separables por medio de las llamadas funciones de *kernel*.

Ejemplo

En el ejemplo de las setas, dado que en principio usaríamos una única característica para clasificarlas, serían modelos adecuados el clasificador lineal, los *k*-vecinos más cercanos y los SVM.

Para **entrenar** y **evaluar el clasificador** obtenido, lo más habitual es contar con un gran conjunto de datos etiquetados y separarlos en una parte destinada al aprendizaje del clasificador (*training*) y otra dedicada a su examen (*test*). Las proporciones de *training-test*% suelen ir del 50-50% al 70-30% del total de datos etiquetados. El aprendizaje se realiza usando el conjunto de *training*, pero cada modelo de clasificación sigue un procedimiento propio para entrenarse. Posteriormente, el clasificador aprendido se utiliza para clasificar las muestras de test, de las que ya tenemos etiquetas verdaderas. Finalmente, se comparan las etiquetas verdaderas con los valores decididos por el clasificador. Este proceso nos informa de cómo de bien generaliza el clasificador que se ha escogido.

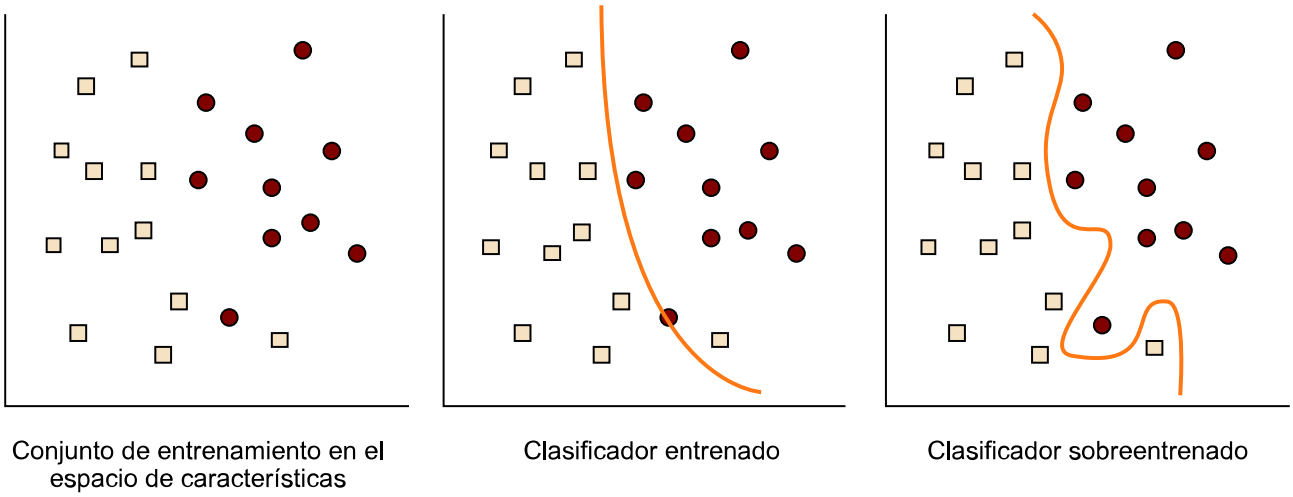
Utilizar muchas características no siempre mejora los resultados de la clasificación. Al contrario, al tener más características es posible que: a) algunas no sean confiables; b) haya dependencias entre ellas y solo creen complejidad (por ejemplo, la estatura de una persona y la longitud de su mano suelen ser informaciones redundantes); c) se incrementen los costes de adquisición de los datos, o d) haya más ruido en los datos medidos.

En general, el número de muestras necesarias para entrenar correctamente un clasificador crece exponencialmente con la dimensionalidad (número de características escogidas). Esto se conoce como **maldición de la dimensionalidad** o efecto Hughes.

Si se utilizan reglas de decisión más sofisticadas, las fronteras entre clases se adaptarán mejor a los datos, como se observa en la figura siguiente. No obstante, ello puede conducir al efecto conocido como **sobreajuste** (*overfitting*): el clasificador se adapta excesivamente a los datos etiquetados, de forma que, cuando se le presentan nuevos datos para clasificar, se equivoca mucho más que si hubiera utilizado reglas más simples, que generalizan mejor.

Evitar el sobreajuste

El sobreajuste se puede evitar con técnicas como la de regularización de datos o la *cross-validation*.



La excesiva adaptación al conjunto de datos de entrenamiento acaba produciendo sobreajuste, perjudicial para la clasificación.

2.3. Fusión de biometrías

Los sistemas biométricos unimodales, es decir, basados en una única modalidad biométrica, se ven considerablemente limitados, debido a defectos de unicidad y de universalidad y a la presencia de ruido en los datos, y a menudo no logran los niveles deseados de precisión en aplicaciones reales.

Varios estudios coinciden en señalar que los **sistemas multimodales**, que combinan adecuadamente varias biometrías, pueden mejorar ostensiblemente sus resultados.

De esta forma, combinando varias biometrías nos es posible conseguir mejores resultados conjuntos, de forma que el sistema final sea más robusto frente a interferentes unimodales.

Por ejemplo, combinando biometrías de cara y de voz se pueden mitigar problemas de una y otra, tales como efectos de iluminación adversos o ruido ambiental intenso.

Sin embargo, se ha de tener en cuenta que las limitaciones de una de las biometrías puede perjudicar los resultados que aporten las demás biometrías al sistema final.

Per ejemplo, si combináramos cara, voz e iris, la intrusión de esta última tecnología haría que se desaprovechara la escasa intrusión de las dos primeras.

Finalmente, la multimodalidad mejora claramente la resistencia de la aplicación a la falsificación de identidades por parte de impostores.

La fusión de biometrías puede tener lugar en diferentes puntos de la arquitectura presentada, según si se realiza en el ámbito de características (después de la extracción), en el de puntuación (después de la comparación) o en el de decisión (después de la decisión final). A continuación se describen estos tres tipos de fusión.

1) Se denomina **fusión en cuanto a las características** a la consolidación de varios vectores de características provenientes de diferentes capturas biométricas en un único conjunto de datos, antes de pasarlo al clasificador. Los vectores de características de entrada pueden provenir de diferentes algoritmos y modalidades, y no siempre es posible fusionarlos.

Por ejemplo, no se pueden fusionar minucias dactilares y coeficientes de *eigenfaces*, puesto que las primeras tienen una longitud variable que depende de cada imagen, mientras que los segundos tienen una longitud definida. En cambio, siempre se pueden fusionar vectores homogéneos; es el caso, por ejemplo, de realizar una media aritmética de varias medidas de la geometría de la mano; también es posible concatenar vectores de geometría facial con vectores de geometría de la mano.

Es necesario normalizar los espacios de características de los vectores a fusionar, haciendo que sus rangos sean similares. Además, es habitual recurrir a técnicas de reducción de dimensionalidad, especialmente en el caso de concatenar múltiples vectores, puesto que, a menudo, contar con excesivas características empeora las prestaciones del sistema.

2) Por otro lado, hablamos de **fusión en cuanto a la puntuación** cuando lo que se combina son las medidas de similitud, es decir, las puntuaciones obtenidas por los clasificadores para cada una de las modalidades consideradas.

Por ejemplo, la medida global de similitud de un sistema cara + voz podría ser una media entre la medida de similitud de cara y la de voz.

3) Por último, la fusión **a nivel de decisión** consiste en fusionar las decisiones binarias (aceptar/rechazar) de cada una de las biometrías siguiendo una regla concreta.

En el caso del sistema cara + voz anterior, la regla podría consistir en aceptar al individuo siempre que la identificación de cara y la de voz sean ambas positivas, es decir, que las dos hayan reconocido al usuario como genuino.

Si bien es cierto que los sistemas multimodales pueden mejorar las tasas de reconocimiento en general, se suele **criticar** la fusión de biometrías de tipos muy diferenciados, argumentando que una biometría robusta es más eficiente utilizada individualmente que unida a otras más débiles. Por último, la creación de bases de datos multimodales es mucho más complicada y costosa que la de modalidades únicas, y normalmente constan de un número muy limitado de individuos.

2.4. Métricas de evaluación

En condiciones ideales, la fiabilidad de los procesos biométricos puede llegar a ser muy alta. No obstante, las diferencias entre modalidades biométricas ponen de relieve una serie de ventajas y deficiencias que las hacen más o menos adecuadas para una u otra aplicación. En general, es preciso disponer de parámetros que indiquen hasta qué punto puede ser fiable una determinada biometría y al mismo tiempo nos permitan comparar una biometría con las demás para escoger la más adecuada para cada aplicación.

Uno de los componentes de error a que están expuestos los sistemas biométricos es el de la **variabilidad intraclase**, que hace que dos muestras biométricas del mismo individuo parezcan muy diferentes y no se aprecie una clara coincidencia entre ellas.

Los cambios de entorno, la presencia de ruido, un posicionamiento diferente del sensor o una mala interacción del usuario con el dispositivo pueden provocar variaciones importantes.

Por ejemplo, las diferentes condiciones de iluminación, orientación y expresión facial con que se capturan varias imágenes de la cara de una misma persona pueden hacer muy difícil la correspondencia entre las características faciales extraídas.

Por otro lado, la otra fuente fundamental de errores es la **similitud interclase** o entre miembros de clases diferentes, es decir, la posibilidad de que los patrones biométricos de dos individuos distintos presenten un alto grado de semejanza.

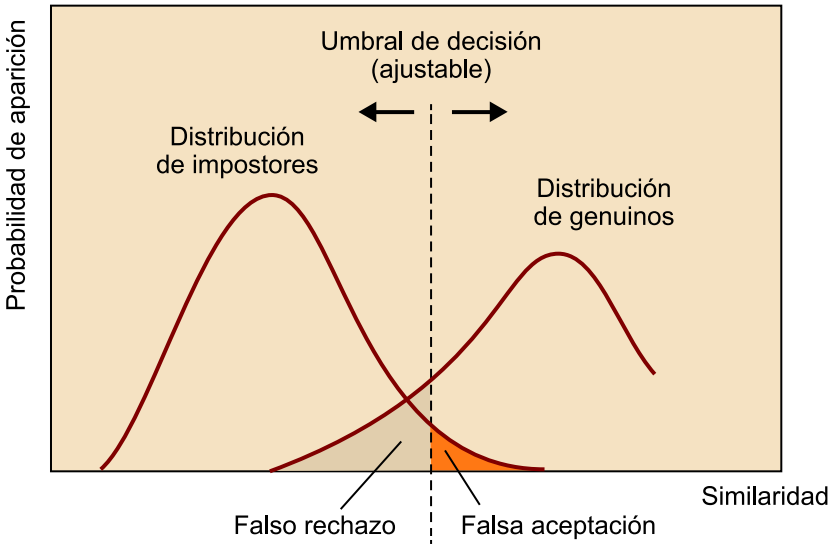
Ejemplo

Sería el caso de personas con caras parecidas o incluso de imágenes sometidas a condicionantes similares, como por ejemplo llevar el mismo tipo de gafas o mirar en una misma dirección, cosa que aumentaría falsamente el grado de coincidencia entre las identidades.

Debido a las razones mencionadas, es muy difícil que dos muestras biométricas de un mismo individuo, incluso adquiridas en condiciones similares, sean completamente idénticas. Por este motivo, los sistemas biométricos estiman la coincidencia de dos muestras biométricas usando una **medida de similitud**, generalmente expresada por medio de un solo número que mide cuánto se asemeja la muestra biométrica analizada a la plantilla almacenada en la base de datos. Cuanto más elevado es el valor de dicha medida, más seguridad se tiene al afirmar la identidad del individuo, y cuanto más bajo es, más certeza se tiene para rechazarla.

Si realizamos un número suficientemente elevado de experimentos para una determinada biometría, en la que extraemos características biométricas de una población y las comparamos con plantillas previamente entrenadas, obtendremos histogramas de puntuaciones parecidos al de la figura siguiente, donde se observan dos curvas. La de la derecha corresponde a los experimentos de **genuinos**, es decir, comparaciones entre muestras de un mismo individuo que resultan en altos grados de similitud. La curva de la izquierda corresponde a los experimentos de **impostores**, donde se cruzan muestras de dos individuos diferentes que generan puntuaciones habitualmente muy bajas. La región central de puntuaciones corresponde a casos en los que el sistema lo tiene más difícil para decidir si la identidad es genuina o impostora, y debido a las fuentes de error antes mencionadas. Para forzar una decisión se establece un **umbral de aceptación**, de forma que en los casos en los que la medida de similitud supere este umbral se aceptará la identidad del individuo, y se rechazará en caso contrario. Al fijar un umbral estamos asumiendo una cierta cantidad de error (ver las zonas sombreadas), donde tratamos a impostores de altas puntuaciones como genuinos (falsa aceptación o *false matching rate*, FMR), y a los genuinos de baja puntuación como impostores (falso rechazo o *false non-matching rate*, FNMR). Este umbral es el que se utiliza en el módulo de decisión.

Distribuciones de medidas de similitud obtenidas al comparar pares de plantillas de la misma identidad (genuinos) y de identidades diferentes (impostores).



Dependiendo de la aplicación, nos puede convenir fijar el umbral de aceptación en valores más bajos o más altos.

Por ejemplo, en el caso de instalar controles de acceso para centrales nucleares (alta seguridad) nos interesa restringir fuertemente la entrada a personas ajenas y evitar falsas autorizaciones, motivo por el cual estableceremos un umbral muy alto. En este caso, aceptaríamos que en un momento dado el sistema invalidara a un usuario auténtico y le hiciera repetir el proceso para corroborar su identidad. En cambio, si la intención fuera encontrar una cara particular entre muchas horas de grabación de multitudes (busca forense), podemos asumir un cierto número de falsos positivos en los resultados, siempre que no se pase por alto de ninguna forma la identidad que buscamos; en este caso, escogeremos un umbral bastante bajo.

Los niveles de falso rechazo y de falsa aceptación dependen de varios factores, entre los que cabe citar la calidad de las muestras recibidas por los sensores, el tipo de características biométricas utilizadas, las prestaciones de la biometría escogida y el umbral de aceptación establecido. Como se puede ver en la figura anterior, con el umbral se pueden equilibrar las proporciones de falsos rechazos y falsas aceptaciones:

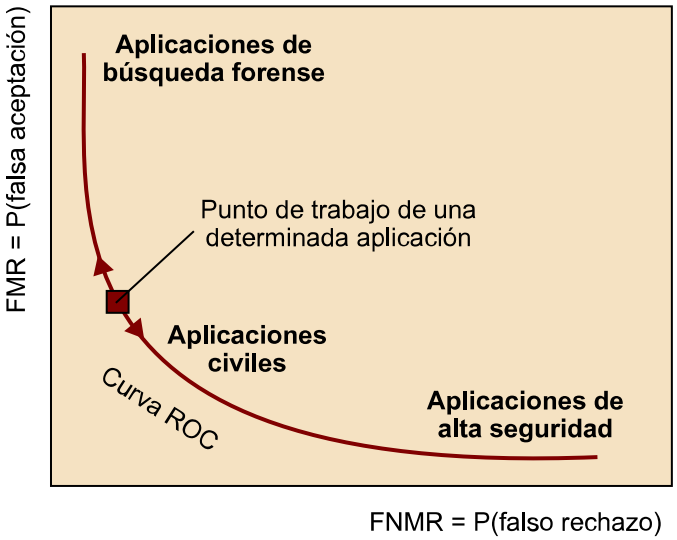
- si bajamos el umbral para hacer que el sistema sea más tolerante al ruido y a las variaciones, crecerá la falsa aceptación.

- Por el contrario, si subimos el umbral para hacer el sistema más seguro, lo que crecerá serán los falsos rechazos.

Una opción muy común es situar este umbral en el punto en que los histogramas de genuinos y de impostores se cortan:

Este punto de trabajo se denomina **EER** (*equal-error rate*), puesto que tiene como particularidad que las ratios de falsa aceptación y de falso rechazo son idénticas.

La forma más común de evaluar los niveles de error de una determinada tecnología biométrica es representar su **curva ROC** (*receiver-operator characteristic*). Esta curva se obtiene dibujando el falso rechazo del sistema en función de la falsa aceptación, FNMR contra FMR, como se puede observar en la siguiente figura. También es habitual ver curvas ROC en las que se representa la FNMR contra 1-FMR, viéndose la curva reflejada verticalmente. Como ambos errores dependen del umbral de aceptación escogido, cada punto de esta curva también corresponde a un determinado umbral. Tal como se comentaba anteriormente, la elección de uno u otro umbral se hace dependiendo del tipo de aplicación final que se desee.



La curva ROC representa los posibles puntos de trabajo del sistema, correspondientes a diferentes umbrales de aceptación. La elección del umbral depende del tipo de aplicación perseguida.

La comparación de sistemas biométricos se puede realizar visualmente, dibujando las curvas ROC de cada sistema en los mismos ejes de coordenadas. Para aplicaciones convencionales, los puntos óptimos de trabajo son los que ofrecen bajas tasas de ambos errores al mismo tiempo. En caso de querer comparar sistemas biométricos a partir de una sola medida, es habitual utilizar el valor de EER como indicador para resumir la fiabilidad del sistema. No obstante, como el EER corresponde a un único punto de trabajo, esta práctica hace que se pierda información del comportamiento del sistema con otros umbrales de aceptación.

Este es el motivo de que últimamente se haya extendido la utilización de otra métrica, la llamada **AUC** (*area under curve*), que consiste en calcular el área bajo la curva ROC como indicador del error total cometido por el sistema. De todas formas, es obvio que utilizar una sola medida de comparación siempre comporta una pérdida de información respecto a la representación completa de las curvas ROC.

3. Análisis de las principales biometrías

3.1. Reconocimiento facial

La observación de las caras es la forma más natural de identificación personal a que estamos acostumbrados en nuestra vida diaria. Por tanto, no es de extrañar que, a pesar de las conocidas limitaciones del reconocimiento facial, sea esta una de las biometrías a las que más iniciativas y recursos se han destinado para conseguir sistemas que emulen o mejoren nuestra capacidad biológica. Este hecho ha potenciado enormemente la **tecnología de identificación facial automática**, que durante los últimos años ha evolucionado desde el uso de simples modelos geométricos a la utilización de complejos procesos matemáticos de representación y clasificación de datos.

La biometría facial es mucho menos precisa que otras biometrías, como las de ADN, reconocimiento de iris, retina o huella dactilar. Aunque básicamente todo el mundo tiene una cara, la similitud entre caras de personas diferentes puede llegar a ser muy alta[4]. Además hay varios factores[5] que pueden hacer cambiar sustancialmente dos observaciones de la misma cara. No obstante, es una biometría de mucha utilidad para gran cantidad de aplicaciones, debido a que entre sus **principales ventajas** figuran:

(4) Por ejemplo, entre gemelos.

(5) Cambios de edad, de iluminación, de expresión, de orientación, además de los debidos a determinados complementos, como por ejemplo cabellos, barba u gafas.

- ser mínimamente intrusiva,
- poder realizar identificaciones a distancia considerable, y
- no requerir colaboración explícita por parte del individuo.

En resumen, tiene una alta universalidad, sus propiedades de unicidad y perdurabilidad son limitadas, y la mensurabilidad puede pasar de ser razonablemente alta (en ausencia de dificultades) a muy baja (en caso de factores externos adversos).

Uno de los **mayores inconvenientes** de esta biometría es la facilidad con que puede eludirse. La forma más sencilla de evitar una identificación en aplicaciones de videovigilancia es la simple ocultación de la cara. Además, en aplicaciones de verificación de identidad se pueden conseguir falsas aceptaciones con el uso de máscaras o, en los sistemas sin detección de cara viva, por medio de fotografías de un individuo validado. El hecho de que esta biometría tenga múltiples fuentes de variabilidad también la hace más adecuada para aplicaciones como las de control de acceso en entornos controlados, no para siste-

mas de alta seguridad. No obstante, entre sus aplicaciones también se incluye la identificación dinámica en escenarios multitudinarios, como aeropuertos o estadios, entre otros.

Finalmente, la percepción de estos sistemas por parte de la población suele ser peor que la del iris, la huella y otros sistemas por la sensibilidad de la información que representa una fotografía facial, así como por el sentimiento de inseguridad que le provoca a la población poder sentirse vigilada sin tener conocimiento de ello.

3.1.1. Normalización

La normalización facial es un paso importante y a menudo imprescindible, por el cual se localizan un conjunto de puntos prominentes de la cara[6] y se usan para transformar geométricamente las imágenes de cara recibidas, y así colocarlas en la misma posición para su posterior comparación. Habitualmente, estas transformaciones se limitan a traslaciones, rotaciones y escalados.

(6)Por ejemplo, los extremos de los ojos, las comisuras de la boca, los orificios nasales, o la punta de la nariz, entre otras posibilidades.

En todo caso, cualquier preproceso o tarea de normalización facial empieza por **la detección automática de la cara** en la imagen de partida.

Los métodos más adecuados para esta finalidad son las **cascadas de clasificación**. Estas cascadas incorporan un conjunto muy grande de clasificadores simples o "débiles", como por ejemplo, los que realizan la diferencia de dos áreas rectangulares de la imagen, dando a conocer qué regiones son relativamente más claras u oscuras que otras. Se agrupan muchos de estos clasificadores débiles en etapas secuenciales, de forma que, si falla por lo menos uno de ellos, se descarta la presencia de una cara en la imagen. Cuando todos estos clasificadores débiles se procesan de forma secuencial a lo largo de las etapas dan lugar a un clasificador fuerte, que informa con precisión de la presencia o ausencia de la cara en una posición de la imagen. El proceso se repite de forma exhaustiva para todas las posibles posiciones y escalas consideradas en la imagen de entrada, dando a conocer todas las regiones donde es altamente probable que haya una cara.

3.1.2. Dificultades del reconocimiento facial

En la práctica, las imágenes faciales no se capturan en condiciones ideales, sino sometidas a una gran cantidad de variabilidades, que incluyen:

- **Iluminación.** Las condiciones de iluminación son uno de los problemas más importantes para el reconocimiento facial, puesto que suponen la aparición de patrones que degradan las imágenes originales, sobreponiendo fuertes sombras y reflejos dependientes de la posición de las fuentes de luz. Las características faciales subyacentes, pues, pueden ser difíciles de

capturar o encontrarse demasiado enfatizadas por culpa de estos patrones artificiales.

- **Variaciones posturales.** Como las caras son objetos tridimensionales, es posible obtener imágenes de una misma cara bajo diferentes vistas, lo que origina importantes dificultades para trasladar la información de una vista a otra (por ejemplo, al comparar una cara frontal con una lateral). A menudo, este problema también supone oclusiones de ciertas partes de la cara.

- **Expresión.** El cambio de expresión debido a la contracción de algunos de los muchos músculos faciales dificulta el alineamiento de un conjunto de caras y su comparación, dado que se crean diferentes apariencias. Por ejemplo, no es trivial comparar caras con expresiones de sorpresa y de tristeza.

- **Oclusiones.** La otra causa principal de dificultad para el reconocimiento facial es la aparición de elementos que impiden tener una visión completa de la cara, ya sea por elementos externos a la persona, ya por prendas de ropa o complementos (bufandas, gafas normales y de sol, gorras), cabellos largos, etc. Estos elementos hacen que la información facial no esté completamente disponible para el algoritmo de reconocimiento y que, a veces, los contenidos de la imagen ajenos al rostro se interpreten como información facial.

Además de estas dificultades, el reconocimiento facial también se ve fuertemente afectado por la variabilidad de la persona **a lo largo del tiempo**, manifestada por la presencia de barba, el aumento o la pérdida de peso, la caída del cabello o la aparición de arrugas. Para hacer frente a todas estas limitaciones, los sistemas actuales más sofisticados de reconocimiento facial incorporan a menudo una serie de etapas de preprocesamiento destinadas a conseguir invariancia en términos de iluminación, rotación y expresión facial. Así pues, se emplean:

- **técnicas fotométricas** para reiluminar caras, que reducen el efecto de sombras y reflejos y simulan mejores condiciones de iluminación;

- **técnicas de proyectividad** para transformar caras con rotaciones en vistas frontales; y

- técnicas que transforman caras con expresiones faciales en caras de expresión neutra.

A pesar de todo, es difícil contar con una solución que sea capaz de resolver todos los problemas a la vez y para todos los tipos de escenarios. En vez de eso, es más habitual ajustar el sistema a condiciones particulares de uso, según el escenario que se esté tratando.

3.1.3. Métodos de reconocimiento facial

Existen principalmente dos tipos de técnicas para el reconocimiento facial.

- En primer lugar, las basadas en **análisis local**, es decir, en la posición y forma de ciertos atributos faciales (ojos, nariz, boca, cejas...) y en cómo se relacionan entre sí.

- Por otro lado, encontramos las técnicas basadas en **el análisis global** de la cara, que se representa como combinación lineal de elementos de una cierta base que cumplen determinadas condiciones.

Los primeros métodos de reconocimiento facial datan del comienzo de los años setenta y se basan en la detección automática de ciertos marcadores faciales, como por ejemplo ojos, nariz y barbilla, de los que posteriormente se extraen **características geométricas** cruzadas, tales como distancias, ángulos y áreas. Estas propiedades constituyen descriptores que posteriormente se comparan entre sí para establecer la identidad del individuo. Los métodos estrictamente geométricos han demostrado no ser especialmente minuciosos para el reconocimiento facial. La información extraída de marcadores faciales no parece ser por sí misma lo suficientemente discriminante para esta tarea, por lo que a menudo se necesita explotar la apariencia facial adicionalmente. En pocas palabras, no basta con disponer de dimensiones y distancias, sino que también se han de analizar formas y texturas.

A comienzos de los años noventa se produjeron adelantos significativos, debido especialmente a los métodos de álgebra lineal **basados en la apariencia global**, tales como los de las *eigenfaces* y las *fisherfaces*. Estos métodos operan sobre imágenes de cara de dimensiones exactamente iguales y perfectamente alineadas, es decir, con igual posición, rotación y escala. Estas imágenes se suelen alinear de forma que los ojos y la boca de los usuarios coincidan en posición espacial. Cada cara analizada constituye un largo vector en el que se incluyen ordenadamente las intensidades luminosas de cada píxel de la imagen; por ejemplo, concatenando todas las columnas de una misma imagen en escala de grises. De esta forma, una imagen de 200x250 píxeles en escala de grises a 8 bits generaría un largo vector de 50.000 elementos, cada uno de los cuales toma valores entre 0 y 255. Por este motivo, decimos que las imágenes de cara tienen una gran dimensionalidad y muestran información redundante. Al construir un conjunto suficientemente grande de caras, el uso de técnicas algebraicas de reducción de dimensionalidad, como PCA (análisis de componentes principales, usado para *eigenfaces*) y LDA (análisis lineal discriminante, utilizado para *fisherfaces*), nos permite encontrar subespacios vectoriales de muchas menos dimensiones.

Básicamente, estas técnicas permiten convertir los largos y redundantes "vectores de cara" en vectores equivalentes que pueden representar la misma cara con muchos menos elementos, enfatizando las características más significativas de cada cara.

Así pues, tanto la técnica de PCA como la de LDA tienen como objetivo reducir las dimensiones de los vectores faciales expresados con intensidades, aunque manteniendo la información particular de cada cara.

No obstante, las dos técnicas operan de forma diferente: la de **PCA** se concentra en buscar elementos que representen óptimamente (compriman) las características faciales, derivando en el algoritmo *eigenfaces*, que resulta muy adecuado para "comprimir" información facial. Por otro lado, la técnica de **LDA** no busca la representatividad, sino la discriminabilidad de los datos; es decir, se concentra en buscar los elementos que sean óptimos para "distinguir" las caras de personas diferentes.

LDA y PCA

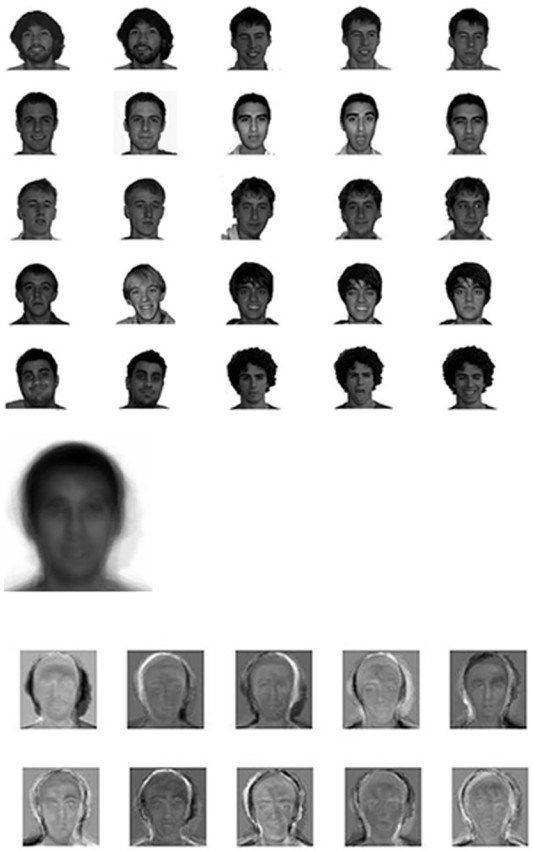
A pesar de que, por definición, LDA tendría que ser mucho más eficaz que PCA para reconocimiento facial, en la práctica se ha demostrado que eso solo sucede cuando se tiene un conjunto muy grande de datos de entrenamiento, y que en entornos con datos muy limitados es mejor usar PCA.

Eigenfaces

Podemos ver con más detalle el caso concreto de las *eigenfaces* (método de PCA). Esta técnica se deshace de la información considerada inútil en los vectores de cara iniciales, encontrando una nueva base de vectores, las *eigenfaces*, que es ortogonal, es decir, donde los vectores se encuentran incorrelados entre sí. De esta forma, hablando a grandes rasgos, conseguimos representar una cara inicial como combinación lineal de *eigenfaces*, donde cada *eigenface* es un vector. Además, podemos utilizar los pesos de esta combinación lineal (llamados coeficientes de *eigenfaces*) como representación comprimida de la información facial. Para hacerse una idea, comprimir cuidadosamente una imagen facial por medio de esta técnica supone una compresión de factor 1.000, aproximadamente. Así pues, en el ejemplo anterior de la cara de 50.000 píxeles, conseguiríamos una imagen cualitativamente muy similar con solo 50 coeficientes. Además, se puede comparar cualquier imagen facial con las caras presentes en la base de datos a partir de la distancia existente entre estos coeficientes de *eigenfaces*. Cuantas más *eigenfaces* se consideren para la nueva base, más minuciosa será la representación facial, pero en la práctica se observa que, para más de 100 *eigenfaces*, la diferencia entre la imagen original y la reconstrucción es muy difícil de percibir.

No linealidad del reconocimiento facial

A pesar del aceptable funcionamiento de estas técnicas de álgebra lineal en condiciones controladas, el problema de reconocimiento facial es altamente no lineal, debido al gran número de variaciones de entorno posibles, como las provocadas por la iluminación, la orientación y la expresión facial. Cuando aparecen estos problemas, el comportamiento de los métodos lineales es muy limitado. Para solucionarlo se han propuesto variaciones de dichos métodos, basadas en los *kernels*, que aplican transformaciones no lineales en el espacio de características para intentar linealizarlas, consiguiendo así técnicas como las del *kernel* PCA y el *kernel* LDA.



Arriba: ejemplos de imágenes faciales alineadas y normalizadas de la base de datos Rice. **Centro:** cara media de esta base de datos. **Abajo:** las diez primeras *eigenfaces* obtenidas, que caracterizan los detalles más notorios de grupos de caras característicos respecto de la imagen media. Fuente: Kochelek, Krueger, Robinson, Escarra. http://www.oercommons.org/courses/obtaining-the-eigenface-basis/view)

Siguiendo la idea de los métodos no lineales, encontramos otra familia de métodos muy populares para reconocimiento facial, la del **EBGM** (*elastic bunch graph matching*).

El EBGM consiste en considerar la cara como una malla en la que se identifican una serie de marcadores de referencia, como por ejemplo los ojos, la nariz, la boca o el contorno de la cara, entre otros muchos posibles.

La razón de escoger estos puntos es que son relativamente fáciles de localizar, a pesar de que haya cambios de expresión o ligeras variaciones posturales. Estos marcadores constituyen nodos de un grafo, y para cada nodo se extraen descriptores de la región espacial donde se encuentra el marcador en cuestión. Se pretende describir la región cercana a cada marcador: los contornos, los cambios y los detalles que se pueden observar en su vecindad. Para extraer esta información es común utilizar transformadas *wavelet*, similares a la transformada de Fourier, pero que no solo producen datos en el dominio frecuencial, sino también en el espacial; de esta forma se obtiene información muy valiosa

Variantes del método EBGM

Hay muchas variantes de este método, dependiendo de los marcadores escogidos, el filtro o filtros *wavelet* utilizados, el número de escalas frecuenciales y espaciales elegidas, la métrica seleccionada para comparar las respuestas de los filtros y otras muchas opciones en el ámbito del diseño.

de la textura de cada zona, tanto en amplitud como en fase. La similitud de dos caras se evalúa comparando la información local de cada marcador, para todos los marcadores localizados.

Finalmente, otra posible estrategia para tratar las variaciones no lineales del entorno y aumentar la capacidad de generalizar los algoritmos de reconocimiento es utilizar modelos de clasificación más sofisticados. Con esta finalidad se han utilizado con resultados positivos varias técnicas de clasificación, como por ejemplo las **redes neuronales** y las **SVM** (máquinas de vectores de soporte), que se diseñan específicamente para tener en cuenta las propiedades de las características faciales. Desde los años noventa han surgido, y continúan aparecidendo, multitud de propuestas que utilizan sistemas de clasificación generalmente muy complejos en el ámbito matemático, diseñados específicamente para solucionar problemas concretos de esta biometría. A diferencia de lo que ocurre en otras biometrías, como la del iris o la de voz, no parece que exista un método claramente preferido para la biometría facial, y lo más normal es encontrar variaciones de los métodos globales y locales descritos en esta sección, donde lo que se diferencia es la forma precisa de tratar los datos.

El reconocimiento facial ha experimentado una gran evolución, potenciado por las diversas evaluaciones tecnológicas que han tenido lugar en los últimos años (FERET 1993-1997, FRVT 2000, 2002, 2006, FRGC 2004). No obstante, todavía requiere una importante mejora en lo que respecta a la precisión de identificación para poder competir con otras biometrías, como la de iris o la de huella dactilar. La mayoría de los sistemas comerciales de reconocimiento facial actuales se basan en la imposición de un gran número de restricciones en cuanto a la obtención de imágenes, tales como la necesidad de caras muy frontales o de iluminación muy regular, lo que explica que todavía queden pasos por realizar hasta conseguir un sistema invariante a las principales causas de degradación de identificación. No obstante, esta biometría es enormemente popular por su facilidad para capturar las muestras biométricas de los individuos, y su implementación se ve favorecida por los adelantos tecnológicos en capacidad de procesamiento y la posibilidad actual de adquirir más fácilmente cámaras de una calidad cada vez superior.

3.2. Reconocimiento de iris

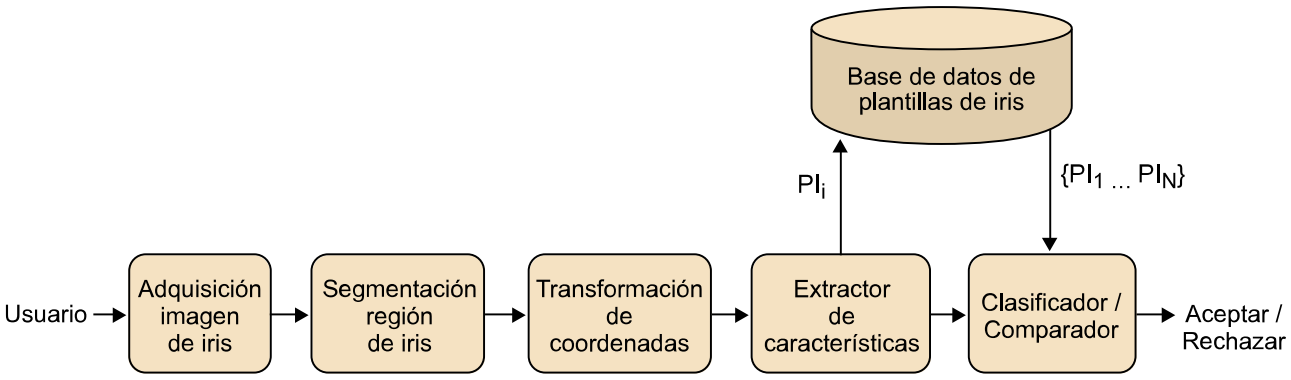
El reconocimiento de iris constituye una de las modalidades biométricas más populares y útiles de las últimas décadas, especialmente debido a su alto nivel de precisión para la identificación personal.

Las características biométricas utilizadas en este caso son los patrones texturales encontrados en cada uno de los iris de una persona.

La aleatoriedad de los patrones musculares del iris hace que se reduzca muchísimo la probabilidad de encontrar dos personas que compartan las mismas características, que algunos autores estiman de una entre 10 72. Por otro lado, los patrones del iris se desarrollan en el octavo mes de gestación y, a partir de ese momento, permanecen estables a lo largo de la vida de la persona. La propia fisiología del iris también contribuye a dicha estabilidad, dado que esta membrana se encuentra aislada de factores externos gracias a la córnea. Todo ello hace que la biometría de iris muestre mejores propiedades de unicidad y perdurabilidad que la de cara o la de voz y que, además, se considere adecuada para utilizarse como modalidad única. Adicionalmente, todo el mundo con un ojo al menos, o incluso un ciego, puede utilizar esta biometría, de forma que su universalidad es destacable, y no es fácil conseguir engañar a un sistema de estas características.

La mensurabilidad es ligeramente más compleja: a pesar de que el proceso de adquisición es sencillo, rápido y realizable a cierta distancia, requiere una mínima colaboración por parte de los usuarios. Uno de los inconvenientes más importantes de esta biometría es el alto coste que pueden llegar a tener los aparatos de captura, a pesar de que su precio ha ido decreciendo con el paso de los años. Además, los patrones de iris constan de estructuras muy ricas y complejas que dificultan la tarea de diseñar algoritmos alternativos de reconocimiento. La elusión es difícil de conseguir, motivo por el cual se considera generalmente que es una tecnología segura en este sentido.

Arquitectura modular de un sistema de reconocimiento de iris.



La arquitectura típica de un sistema de reconocimiento de iris empieza por **la adquisición de imágenes** del ojo en las que sean claramente observables los patrones de iris.

Inicialmente, la captura se realizaba a distancias cortas y con la participación del usuario, quien había de evitar moverse durante el proceso de adquisición para asegurar la calidad de las imágenes obtenidas. Sin embargo, la tecnología más reciente posibilita que dichas imágenes se puedan capturar en movimiento y a distancias de hasta más de un metro.

Generalmente, las imágenes no se capturan en **espectro visible**, sino utilizando luz en frecuencias cercanas al infrarrojo (*near-infrared spectrum*, **espectro NIR**), que es invisible al ojo humano y, por lo tanto, más cómodo para los usuarios. El uso del espectro NIR también permite ver estructuras texturales mucho más ricas en los iris de colores oscuros, y además se elimina en gran medida la molesta presencia en las imágenes de reflejos especulares que dificultan la extracción de información. No obstante, esta banda frecuencial no puede capturar cierta información cromática que proviene de la melanina del iris, y además los sensores infrarrojos son mucho más caros. Por estos motivos, y por el hecho de que las cámaras de espectro visible han mejorado mucho durante los últimos años, en la actualidad todavía coexisten los dos métodos de captura, tanto en espectro visible como en espectro NIR.

Los aparatos de captura pueden incorporar mecanismos para detectar la presencia de ojo vivo; por ejemplo, variando la cantidad de luz proyectada por el escáner de iris y detectando la respuesta de la pupila al dilatarse. De esta forma se asegura que no pueda falsearse el acceso mediante imágenes de iris de alta calidad.

Uno de los pasos fundamentales para la extracción de plantillas biométricas del iris es la **segmentación de la imagen**.

> Este paso consiste en analizar la imagen capturada del ojo para localizar la región anular que contiene el iris y, a la vez, descartar el resto de zonas.

Para conseguirlo, lo más habitual es tratar de localizar las circunferencias interior y exterior del iris, denominadas **contorno pupilar** y **contornolímbico**, respectivamente. Por regla general, el contorno pupilar es más fácil de encontrar, dado que el contraste con la pupila es muy alto. Aunque existen diversos métodos para localizar dichas zonas, los más comunes con diferencia son los siguientes:

- **El método integro-diferencial de Daugman.** Para detectar circunferencias en la imagen se realiza una busca exhaustiva, probando todos los orígenes y radios posibles y viendo si los contenidos de la imagen coinciden aproximadamente con la circunferencia que se dibujaría en cada caso. Así se identifican las circunferencias predominantes de la imagen. También existe una variación de esta técnica para detectar párpados.

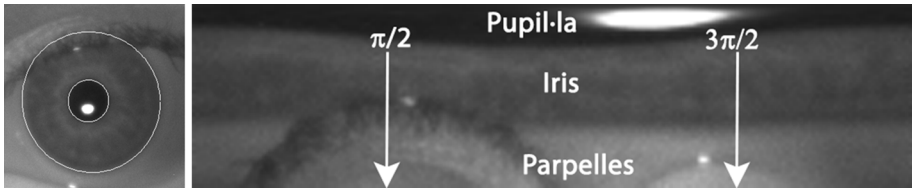
- **La transformada circular de Hough.** El método original de la transformada de Hough se utiliza para localizar las líneas rectas predominantes de una imagen. En el caso del iris se usa una variación de este método para localizar las circunferencias más notorias de la imagen. También se puede usar para detectar los párpados, considerando radios mayores.

- **Los métodos de contornos activos.** A pesar de que los contornos del iris son prácticamente circulares, no tienen por qué ser círculos perfectos, especialmente si el ojo no se observa de forma completamente frontal. Los métodos basados en contornos activos o *snakes* sitúan inicialmente una curva paramétrica en la imagen (en este caso, un círculo) y la van adaptando continuamente a los contornos de la imagen, en este caso el iris en cuestión. El problema principal de esta técnica es que depende en gran medida de una buena posición inicial de la curva, pues de lo contrario puede dar lugar a resultados erróneos. También es aplicable para detectar los párpados.

Partiendo del resultado de cualquiera de estas técnicas, los contornos interior y exterior del iris y los párpados superior e inferior se pueden localizar de forma muy precisa. La segmentación se puede mejorar todavía más buscando las partes de la región anular que se encuentran invadidas por elementos tales como los reflejos luminosos y las pestañas. Estas partes que esconden la región anular del iris se descartan, durante la extracción de características, para tomar solo la parte de imagen que nos interesa.

Una vez se ha logrado la segmentación del iris, el resto de pasos hasta llegar a la identificación suele ser muy convencional y de uso generalizado. En primer lugar, se suele hacer **una transformación de los ejes de coordenadas** de la imagen, de cartesianas a polares, de forma que la región anular se acaba desplegando en un zona rectangular, donde el eje horizontal está formado por ángulos y el vertical por radios.

Transformación de la imagen de iris de coordenadas cartesianas (izquierda) a polares (derecha).



El eje vertical del nuevo espacio representa el radio (incremental de arriba abajo) y el eje horizontal, los ángulos. La región de iris es la banda central de contraste medio. Se puede observar la invasión del párpado superior a $\pi/2$, que hay que enmascarar.

Para la extracción de características se suele utilizar todavía hoy la **técnica de IrisCode** propuesta por Daugman, con la que se caracteriza al individuo a partir de la información de fase encontrada en la banda del iris, que es mucho más discriminante e invariante que la información de amplitud.

Para obtener la fase se utilizan las llamadas *wavelets* de Gabor, que localizan información tanto en el dominio frecuencial como en el espacial con resolución óptima entre los dos dominios.

Las plantillas biométricas obtenidas son fáciles de almacenar, debido a su reducido volumen de información, y también se comparan entre sí de forma fácil y rápida. La clasificación se puede llevar a cabo con una simple instrucción XOR (OR exclusivo) sobre los dos códigos binarios a comparar, con la cual se obtiene el número de bits diferentes (distancia de Hamming). La cantidad de bits diferentes entre ambos códigos dan una medida de la similitud entre códigos.

Transformada *wavelet* e *IrisCode*

Podemos pensar en una transformada *wavelet* como una transformada de Fourier en la que la señal a transformar se multiplica por una función armónica y una función gaussiana. La información de fase se guarda de forma binaria (00, 01, 10, 11) de acuerdo con los signos de las partes real e imaginaria de la transformada *wavelet*, creando así un mapa binario que se conoce como IrisCode y se estandariza a 256 bytes (2.048 bits de información de fase, partiendo de 1.024 píxeles de región de iris). Estos códigos constituyen en sí mismos una plantilla biométrica de iris (PI).

Hasta la actualidad, el reconocimiento de iris se ha utilizado principalmente para aplicaciones de control fronterizo, en sustitución de los pasaportes, y aplicaciones de alta seguridad, a pesar de que su uso se está viendo progresivamente incrementado y normalizado por parte de gobiernos, aeropuertos y empresas privadas. En la actualidad se están poniendo en marcha varios proyectos de seguridad nacional a gran escala, como por ejemplo el proyecto Aadhaar en la India, que planea recoger cerca de 600 millones de plantillas faciales, dactilares y de iris hasta el 2014 para documentos nacionales de identidad.

3.3. Reconocimiento dactilar

El reconocimiento dactilar consiste en identificar o verificar la identidad de una persona a partir del análisis de las crestas dérmicas encontradas en la punta de uno o más de sus dedos.

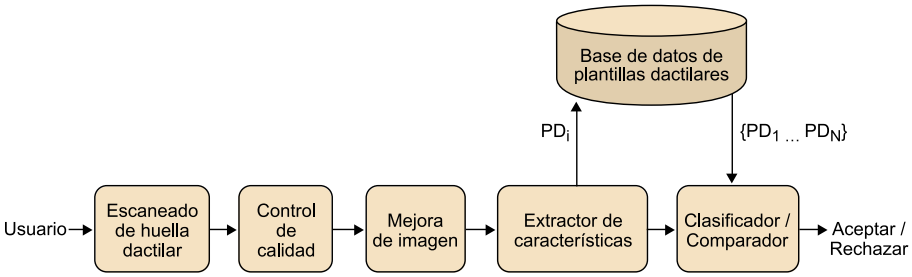
Estas crestas se encuentran representadas por medio de **huellas dactilares**. Además de ser uno de los procedimientos biométricos más antiguos para la identificación personal, el reconocimiento dactilar es también el **método biométrico más implementado en todo el mundo** en la actualidad.

La formación de las crestas y valles en la epidermis de las puntas de los dedos depende de factores tanto genéticos como ambientales y tiene lugar durante el desarrollo embrionario hasta el séptimo mes de gestación de cualquier persona, cumpliendo así el atributo de universalidad. Es igualmente aceptada la unicidad de esta biometría: circunstancias como, entre otras, la posición del feto durante estos meses condicionan estas características biométricas, por lo que incluso las huellas dactilares de dos gemelos iguales son diferentes. Su perdurabilidad es mucho más discutible: a pesar de que en principio las configuraciones de estas crestas se mantienen invariantes durante la vida de la persona, los dedos son mucho más sensibles a las alteraciones físicas que otras partes del cuerpo (iris, retina) por estar más expuestos a quedar marcados, entre otras causas, por cicatrices o quemaduras a consecuencia de posibles accidentes.

En cuanto a atributos deseables, ha habido muchas discusiones en torno a las posibilidades de elusión de los métodos de reconocimiento dactilar. Existen varios métodos para confeccionar falsos modelos de crestas dactilares en diversos materiales (gelatina, plástico, silicona) a partir de moldes, e incluso se

han dado casos mucho más violentos, en los que bandas de ladrones han llegado a seccionar un dedo a personas autorizadas para acceder a automóviles de gama alta o a zonas de alta seguridad. Por otro lado, la aceptación de la tecnología es limitada por el hecho de ser una biometría de contacto, con las consecuentes reticencias higiénicas.

Arquitectura modular de un sistema de identificación personal a partir de la huella dactilar.



La arquitectura de un sistema de reconocimiento de huellas dactilares contiene los módulos propios de cualquier sistema biométrico, con algunas variaciones particulares.

En primer lugar, el dedo del individuo a identificar es escaneado mediante un sensor que **captura** una imagen digital de la huella dactilar. Esta imagen se codifica típicamente en mapas de grises a 8 bits de resolución, suficiente para poder contrastar adecuadamente los detalles de las crestas y valles de la epidermis que servirán para caracterizar al individuo.

Adquisición de huella dactilar de tipo espiral.

Fuente: NIST (CC).

Es muy habitual que los dispositivos utilizados para la captura inicial incorporen mecanismos para detectar intentos de fraude mediante el empleo de técnicas como la de **detección de dedo vivo**, entre otras. Estos métodos no solo son capaces de rechazar imágenes impresas de huellas y moldes sintéticos de varios materiales, sino que, además, pueden llegar a detectar con un alto grado de certeza que el dedo presentado haya sido cortado, pertenezca a una persona difunta o, incluso, que el individuo que intenta acceder se encuentre bajo una importante presión emocional. Para hacerlo, se pueden me-

Métodos más utilizados para detectar intentos de fraude

Los métodos posiblemente más utilizados son la medida de conductividad e impedancia eléctricas de la piel y la estimación de la oxigenación sanguínea a partir de transmisiones luminosas (oximetría de pulso).

dir diversas variables, como el calor superficial, el movimiento, la circulación sanguínea o la cantidad de proteínas o de moléculas odoríferas presentes en la muestra analizada.

La imagen de la huella dactilar adquirida por el sensor puede verse fácilmente degradada por varios motivos.

> La mala colocación del dedo en el sensor, un contraste de imagen insuficiente, la presencia de suciedad, una excesiva humedad ambiental o la aparición de distorsiones de diversos tipos pueden comprometer enormemente la calidad de la imagen obtenida y, consecuentemente, deteriorar el reconocimiento.

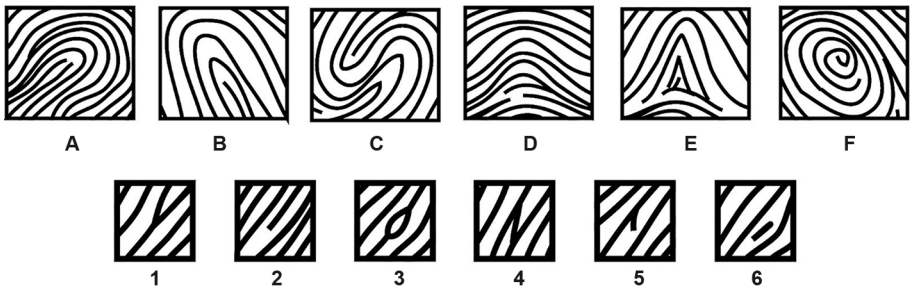
En estas circunstancias, resulta indispensable incorporar un módulo de **control de calidad** para garantizar que las imágenes analizadas están en condiciones de ser procesadas. La medida de calidad de la imagen se obtiene a partir de la estimación automática de diversos parámetros, tales como la continuidad y uniformidad de la estructura de crestas y valles o el contraste de la imagen. Si la imagen analizada no tiene suficiente calidad, se descarta y se insta al usuario a repetir la captura. Por otro lado, las imágenes que pasan el control se envían a un módulo de **mejora de imagen** que filtra el ruido local de las regiones que lo necesiten e incrementa la claridad de la estructura global.

En segundo lugar, el módulo de **extracción de características** analiza la imagen mejorada resultante, en la que la estructura de crestas y valles ya es visiblemente clara, y extrae las características biométricas que se utilizarán para caracterizar al individuo. Generalmente, las características que se pueden extraer de una huella dactilar se sitúan en tres posibles niveles:

- Los patrones de flujo macroscópicos formados por la estructura de crestas.
- Las minucias, puntos singulares en los que la estructura de crestas y valles pierde localmente su regularidad. Los dos tipos básicos de patrones minuciales son la bifurcación y la terminación de crestas.
- Los poros de las glándulas sudoríparas y atributos de contorno de las crestas.

Los **patrones de flujo** vienen dados por la forma en que las crestas de un dedo se agrupan unas con otras, formando determinadas estructuras. La siguiente figura muestra las categorías de patrones de flujo más habituales (A-F): bucles, que pueden estar orientados hacia la derecha (A), hacia la izquierda (B), o ser dobles (C); arco normal (D) y arco en tienda (E); y espirales (F).

Categorías principales de patrones de flujo.



(A) bucle derecho, (B) bucle izquierdo, (C) doble bucle, (D) arco, (E) arco en tienda y (F) espiral. Las minucias o irregularidades de cresta más habituales son: (1) bifurcación, (2) terminación, y otros tipos derivados de uso común: (3) laguna u ojal, (4) cruce, (5) aguijón, (6) isla.

Por otro lado, las **minucias** son las características más utilizadas en biometría dactilar y forman el 80% de los puntos singulares de una huella. Las dos categorías básicas de minucias son las bifurcaciones y las terminaciones de cresta, a pesar de que las aplicaciones biométricas suelen utilizar más categorías según su diseño específico. Se han llegado a definir 52 tipos de minucias diferentes, de los que los 6 presentados en la figura anterior suelen ser los más utilizados por los expertos en comprobaciones manuales (1-6). Para cada minucia localizada, el extractor de características guarda el tipo y la posición y orientación relativas respecto de las otras minucias de la misma huella; por lo tanto, las plantillas biométricas de minucias tienen medida variable. La relación geométrica entre todas las minucias de dos muestras a comparar permite validar la identidad de un individuo, en caso de coincidencia. Aparte de estas minucias, también se suelen guardar el número de crestas cortadas por la recta que conecta dos minucias, así como los puntos *core* y *delta*, puntos de referencia centrales y separadores, respectivamente, definidos según los patrones de flujo anteriormente mencionados.

Por último, en un plano todavía más detallado, encontramos los **poros** y otros **atributos de contorno**. Los poros tienen una medida considerablemente más reducida que las minucias y no son apreciables en huellas dactilares en tinta, por lo que se requiere el uso de escáneres ópticos para detectarlos. Entre los atributos de contorno se suele incluir información relativa al grosor o la forma de determinadas crestas, la orientación o frecuencia local de crestas en cada región de la imagen y la localización de crestas incipientes (las muy delgadas y discontinuas en algunos tramos).

En tercer lugar, una vez extraídas, las características dactilares escogidas se incorporan a una plantilla dactilar (PD_i) que caracteriza al individuo a partir de estos patrones. Tal como sucedía con el resto de biometrías analizadas hasta ahora, esta plantilla únicamente se almacena en la base de datos en el caso de registrar al individuo en el sistema de reconocimiento. En los demás casos, dicha plantilla obtenida se envía al **clasificador**. Allí se compara, ya sea directamente con la plantilla de la identidad propuesta para confirmar esta identidad (verificación), ya con cada una de las plantillas de la base de datos para averiguar la identidad del individuo en cuestión (identificación).

Por el hecho de ser la tecnología biométrica más implementada en todo el mundo, existen muchísimas aplicaciones que utilizan reconocimiento dactilar, desde las de análisis forense a las de control de acceso para trabajadores, aeropuertos o agencias gubernamentales. También se pueden destacar los lectores de huella dactilar para hacer *login* en sesiones de ordenador, control de acceso de estudiantes a escuelas de primaria en el Reino Unido, préstamo de bibliotecas y, virtualmente, cualquier situación de verificación de identidad.

3.4. Reconocimiento de hablante

Las tecnologías de reconocimiento de hablante se ocupan de reconocer a las personas a partir de su habla[7].

(7)No se debe confundir con el reconocimiento de habla, que no reconoce al hablante sino lo que se ha dicho, independientemente de quien lo haya dicho, y por lo tanto no participa de la definición de esta biometría.

El reconocimiento de hablante extrae y modela características acústicas del habla para diferenciar individuos.

Observación

Por lo tanto, es una de las pocas biometrías que no se basa en el procesamiento de imagen.

Las características del habla de un individuo vienen condicionadas por aspectos intrínsecos a su fisiología, como por ejemplo, la forma del tracto vocal, las cavidades nasales, la boca o los labios, y por la forma en que el individuo los utiliza todos juntos para generar un sonido (es decir, el estilo de habla y otros rasgos de comportamiento). Los condicionantes fisiológicos son invariantes para cada persona, a diferencia de lo que sucede con la vertiente de comportamiento, que puede variar con la edad, el estado de salud e, incluso, el estado emocional de la persona en el momento del análisis. Por este motivo, se suele situar la biometría de voz **a medio camino** entre las biometrías físicas y las de comportamiento.

La precisión del reconocimiento de hablante se considera mediana, generalmente no tan buena como la de las otras biometrías. Ello se debe a tres razones fundamentales:

- La habitual presencia de ruido ambiental durante el análisis de la señal sonora.
- La alta variabilidad intraclase: un mismo hablante cambia su voz por razones de edad, enfermedad o emoción.
- La baja variabilidad interclase: dos personas diferentes pueden tener una voz muy parecida, especialmente dentro de una misma familia.

Así pues, a pesar de que el atributo de universalidad está claro, los de mensurabilidad, perdurabilidad y unicidad son más débiles que el primero.

No obstante, esta tecnología tiene otros **puntos fuertes** que la hacen muy interesante para determinadas aplicaciones biométricas. El habla es una acción muy natural y sencilla, de alta aceptación entre toda la población. Además, no es nada invasiva, dado que no requiere contacto físico; de hecho, se permite la identificación a distancia de los usuarios por vía telefónica. Finalmente, el coste de su implantación es mucho más reducido que el de otras biometrías, punto que incrementa sus prestaciones tecnológicas. Se trata de una biometría que ha experimentado constantes avances científicos durante los últimos veinticinco años, por lo que ha adquirido un alto grado de madurez tecnológica. No obstante, se trata de una biometría cooperativa, ya que el individuo a identificar tiene que producir activamente los sonidos que lo identifiquen.

Existen dos **modalidades básicas** de reconocimiento de hablante: con **dependencia** y con **independencia textual**, según si el sistema conoce o desconoce a priori el texto hablado por el individuo. A pesar de que el contenido textual también se puede recibir mediante sistemas de reconocimiento automático de habla, este proceso es muy susceptible a errores, por lo que se suele evitar cuando se requieren niveles de seguridad más altos. Por otro lado, se puede añadir un extra de seguridad a la modalidad dependiente, haciendo que el texto hablado por el individuo varíe para cada usuario del sistema (por ejemplo, usando como texto el número del carné de identidad, el código de usuario o una contraseña).

El **habla** se produce a partir del aire expulsado por los pulmones, que provoca la vibración de las cuerdas vocales cuando estas se tensan, y posteriormente se modela por la acción del tracto vocal (formado por las cavidades faríngea y bucal) y el tracto nasal (cavidad nasal). Particularmente, el tracto vocal modela el habla a partir de la posición de la lengua, los labios, el paladar y la mandíbula. La vibración de las cuerdas vocales, localizadas en la laringe, produce los llamados sonidos vocálicos, formados por combinaciones de señales periódicas a determinadas frecuencias, que después resuenan en los espacios creados por las diferentes cavidades. Cuando las cuerdas vocales no se encuentran tensas al expirar el aire, se crean los sonidos consonánticos, tanto los fricativos como los oclusivos. La concatenación progresiva de sonidos producidos por las diferentes configuraciones vocales a lo largo del tiempo es lo que genera la señal de habla.

Así pues, las **características propias del hablante** quedan reflejadas en esta señal de dos maneras diferentes.

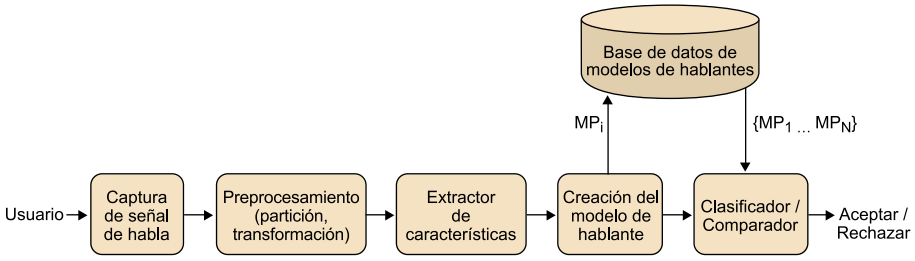
- En primer lugar, a partir de los rasgos anatómicos, es decir, la geometría y dimensiones de las cavidades y elementos implicados en los tres tractos vocales, que determinan pasivamente los sonidos que se generan.

- Por otro lado, los rasgos de comportamiento, tales como la velocidad y el ritmo de habla, la prosodia (variación de la entonación), la dicción,

las expresiones utilizadas y el empleo de muletillas, entre otros muchos factores, determinan de forma activa el habla producida.

En general, una característica fuerte tendría que ser común y fácil de encontrar en la señal de habla, invariante durante el habla y difícil de falsificar. Pero no se conoce ninguna característica que cumpla perfectamente estas propiedades, de forma que la información que habitualmente se utiliza es la anatómica, que suele ser más fácil de extraer y de modelar. Concretamente, se suelen estimar parámetros a partir del **espectro de voz**.

Arquitectura modular de un sistema de reconocimiento de hablante.



La captura de una señal de habla es fácil de realizar utilizando un micrófono convencional o convirtiendo en audio digital la señal recibida por vía telefónica. Como es habitual en cualquier tecnología biométrica, previamente a la extracción de características hay que realizar un preprocesamiento de la señal capturada. En el caso del reconocimiento de hablante, se corta la señal de habla y se enventana en ventanas de unos 20 milisegundos, y se transforma cada uno de los fragmentos a dominio frecuencial. También se suele filtrar cada fragmento[8] usando un banco de filtros para ponderar los componentes frecuenciales de forma que se ajusten a la escala de percepción humana (escala de Mel).

[8]Este paso es similar al que realiza el algoritmo de compresión JPEG sobre imágenes para conservar la información que se percibe mejor y descartar el resto.

Finalmente, puede ser necesario llevar a cabo algún procesamiento adicional de acuerdo con las imposiciones del canal.

Por ejemplo, el habla recibida por vía telefónica supone alta variabilidad, debido al canal y un ancho de banda limitado.

La fase de **extracción de características** suele emplear técnicas de análisis cepstral, que también son muy utilizadas por los sistemas de reconocimiento automático de habla.

A grandes rasgos, cada fragmento de señal de voz enventanado se transforma en dominio frecuencial, y la envolvente del espectro se aproxima por medio de los llamados coeficientes cepstrales[9].

[9]Es habitual obtener coeficientes cepstrales mediante técnicas como MFCC (*mel frequency cepstrum coefficients*) o LPC (*linear predictive coding*).

Estos coeficientes se pueden considerar similares a los coeficientes de las series de Fourier, que permiten aproximar funciones cualesquiera, y donde la aproximación será tanto más precisa cuantos más coeficientes se usen. La principal diferencia es el uso de la escala logarítmica para tener en cuenta el factor de percepción humana, descrito anteriormente.

A resultas de la extracción, a partir de una señal de habla se obtiene una secuencia temporal de vectores de coeficientes, donde cada fragmento enventanado origina un vector de coeficientes cepstrales de medida fija. Estos conjuntos de coeficientes son las características biométricas que servirán para comparar y clasificar a los hablantes.

Posteriormente a la extracción, las características extraídas se procesan para generar un **modelo de hablante** propio de cada usuario que participa en el sistema.

Estas técnicas, entre las que se incluyen las de cuantización vectorial o las estadísticas de segundo orden, pueden ser muy simples, pero es normal utilizar métodos de aprendizaje automático más sofisticados y robustos, como modelos de mezclas de gaussianas (GMM), redes neuronales, modelos ocultos de Markov (HMM) o máquinas de vectores de soporte (SVM).

La técnica más utilizada para este problema es sin duda la de los **modelos de mezclas de gaussianas**, que permiten aproximar cualquier función de densidad de probabilidad mediante un número predefinido de gaussianas, cada una definida únicamente por su vector de medias y su matriz de covarianzas. Ello hace que el modelo resultante sea sencillo y fácil de almacenar.

La **clasificación** final del hablante se realiza comparando la función de probabilidad del modelo obtenido con la de cada uno de los modelos ya registrados en la base de datos. Se usa un criterio de máxima verosimilitud, es decir, se busca cuál de los modelos de probabilidad guardados explica mejor las observaciones de entrada. Los modelos de hablante guardados se pueden actualizar fácilmente a partir de nuevas muestras biométricas de habla, cosa que es muy conveniente si tenemos en cuenta la variabilidad temporal de la voz.

Las aplicaciones del reconocimiento automático de hablante son principalmente cuatro:

- identificación,
- verificación,
- seguimiento de hablante, y
- diarización.

Las dos primeras son las propias de cualquier tecnología biométrica, pero cuentan con la ventaja de poder garantizar la verificación de identidades prácticamente desde cualquier lugar, con ayuda de un teléfono móvil o de Internet. Son aplicaciones comunes el acceso a cuentas bancarias y sistemas financieros, la compra telefónica o el reinicio periódico de contraseñas para trabajadores. Por otro lado, las dos últimas aplicaciones tienen sentido en el caso de múltiples hablantes en una misma grabación. El seguimiento de hablante consiste en identificar los momentos en que una determinada persona está hablando dentro del grupo. De forma más general, la diarización de hablantes identifica y segmenta los momentos de una grabación en la que hablan todos y cada uno de los integrantes de una conversación de grupo.

3.5. Otras biometrías

Existe un amplio conjunto de técnicas biométricas diferentes de las ya descritas. Estas, ya sea por el hecho de estar todavía en fase experimental, ya por resultar mucho más inaccesibles que las anteriores, todavía están lejos de la comercialización, y los expertos del sector no las consideran como estándares. Destacamos las siguientes:

1) Huella genética (ADN)

Cada célula del cuerpo humano contiene una copia de la cadena de ADN que codifica la información de una persona. A pesar de que la mayor parte de este ADN es idéntico en dos personas cualesquiera, un 10% de la cadena es único para cada individuo (excepto en el caso de los gemelos idénticos) y altamente variable, lo que se conoce como secuencias minisatélites. La técnica de análisis de ADN, también llamada huella genética, consiste en comparar directamente dos muestras de ADN de un mismo individuo, de forma que para esta biometría no se extraen plantillas biométricas. Debido a que no todas las etapas del proceso están automatizadas y algunos de los pasos necesarios requieren procesos químicos complejos, el análisis genético se restringe en la actualidad a las aplicaciones forenses. A pesar de que es posiblemente la biometría más robusta en la actualidad, también cuenta con los graves inconvenientes de ser altamente intrusiva, no operar en tiempo real y ser muy susceptible en cuestiones de privacidad, dado que revela condiciones genéticas de los usuarios. Además, es relativamente fácil conseguir muestras genéticas de otros usuarios con finalidades fraudulentas. Para ello basta por ejemplo con obtener un cabello de la persona, siempre que incorpore el folículo capilar de la raíz.

2) Retina

La retina es un tejido fotosensible situado en la superficie interna del ojo, donde se proyecta la luz proveniente del exterior. Después de una serie de procesos electroquímicos, la retina transmite información al nervio óptico para recrear la imagen que le ha sido proyectada. La retina humana está cubierta por una gran cantidad de vasos sanguíneos que están dispuestos de forma diferente en cada persona, lo que la convierte en la clave de esta biometría. Los escáneres de retina aplican una fuente de luz coherente de baja intensidad para iluminar estos vasos sanguíneos y obtener una fotografía de su distribución, que posteriormente se compara con otras plantillas de imágenes almacenadas en

la base de datos. Los sistemas de reconocimiento de retina se utilizan desde la década de los setenta, especialmente para aplicaciones de alta seguridad como por ejemplo las de carácter militar, debido a la alta precisión que proporcionan en las tareas de verificación de identidades. Como contrapartida, el análisis de retina es extremadamente invasivo y más lento que otras tecnologías, como las de iris o huella dactilar.

3) Termografía facial

Se emplean cámaras infrarrojas para detectar los patrones de calor creados por las ramificaciones de las venas sanguíneas propias de cada persona, denominados termogramas. Esta biometría no invasiva tiene muchos paralelismos con el reconocimiento facial, pese a que, al contrario que este, la termografía facial es independiente de las a menudo difíciles condiciones de iluminación ambiental. A pesar de ello, su comercialización inicial no ha sido posible debido al coste tan elevado de su implementación, principalmente por el alto precio de las cámaras térmicas o termográficas que se emplean.

4) Geometría de la mano

La base de esta biometría es la comparación de un conjunto de distancias y dimensiones medidas a partir de una imagen de la mano, que incluyen por ejemplo su tamaño global, la longitud de cada dedo, la posición de las uniones o su forma. Su simplicidad la convierte en una tecnología barata y fácil de aplicar y, a diferencia de la huella dactilar, no se ve perjudicada por los cambios de temperatura o humedad de la piel. No obstante, las características biométricas empleadas no son muy distintivas, la geometría es variable durante la etapa de crecimiento y, por otra parte, las imágenes pueden contener elementos de distorsión, como anillos o pulseras. En consecuencia, se pueden producir altos niveles de error en conjuntos grandes de usuarios.

5) Firma

Está generalmente aceptado que la forma en que una persona firma su nombre es una característica propia de esta persona. Se trata de una biometría de comportamiento por condicionantes externos del individuo, tanto físicos como emocionales. Además, se requiere la cooperación del usuario, a diferencia de lo que ocurre en otras biometrías, como por ejemplo la de reconocimiento facial. Otro de sus puntos débiles es la posible variabilidad de la firma a lo largo de la vida de una persona. Un sistema de reconocimiento de firma es capaz de analizar, además del nombre firmado y la rúbrica, otros parámetros como la presión ejercida y la velocidad instantánea con que el usuario ejecuta la firma, si se cuenta con un sensor adecuado.

6) Patrones cutáneos

La piel de una persona se caracteriza y distingue por el grueso de sus diferentes capas, pigmentación, densidad de colágeno y otras proteínas, estructura subyacente de los capilares, etc. El reconocimiento de patrones cutáneos analiza el espectro característico de la piel de un individuo por medio de técnicas espectroscópicas, trabajando con luz visible e infrarroja reflejada por la piel. Se trata de una biometría emergente.

7) Análisis de la marcha

El estudio espaciotemporal de la forma en que una persona anda es complejo, la marcha puede modificarse a lo largo del tiempo debido a lesiones, cambios de peso o alteraciones temporales de la conducta, y no es excesivamente diferenciadora entre individuos. No obstante, esta biometría de comportamiento es aceptable para verificación en condiciones de baja seguridad, principalmente debido a que puede operar a distancia y a que las muestras de vídeo son fáciles y baratas de obtener. Para realizar la verificación se llegan a tener en cuenta varios factores, como por ejemplo velocidad, cadencia, longitud y anchura del paso, o las medias de los ángulos en las diferentes articulaciones. Su uso también llega a aplicaciones no biométricas, como las de diagnóstico médico o modelado virtual de movimiento humano.

8) Olor corporal

Esta biometría se basa en capturar sustancias químicas volátiles emitidas por los poros cutáneos. Todavía se encuentra en fase experimental a causa de la gran cantidad de dificultades asociadas, como la presencia de contaminantes externos (por ejemplo, olores intensos a perfume o a tabaco), el hecho de que el olor de una persona puede ser mucho menos distintivo que el de otra y la posibilidad de que dicho olor varíe significativamente a lo largo del tiempo, debido a factores dietéticos o fisiológicos.

9) Lecho ungueal

El lecho ungueal es una estructura longitudinal formada por hileras de piel prácticamente paralelas y ricas en patrones vasculares, unidas a estructuras dérmicas por medio de canales muy estrechos. La biometría de lecho ungueal escanea estas estructuras presentadas por la piel bajo las uñas de los dedos y, posteriormente, se tratan estos datos de forma similar a como lo hacen el resto de biometrías basadas en patrones vasculares.

4. Aplicaciones principales

Las aplicaciones industriales, comerciales y cotidianas de la biometría continúan extendiéndose día tras día en todo el mundo. Actualmente, podemos clasificar las aplicaciones principales de la biometría en la serie de bloques temáticos que encontramos a continuación.

1) Control de acceso físico

Engloba todos los mecanismos destinados a autenticar la identidad de una persona en una localización de control mediante el análisis de sus características biométricas. Para estas aplicaciones, la falsa aceptación y el falso rechazo se ajustan a niveles especialmente bajos, y para conseguirlo se trabaja en entornos controlados de iluminación y distancia. Entre las biometrías más utilizadas para control de acceso se pueden destacar las de huella dactilar, cara y venas de la palma de la mano; sus aplicaciones típicas incluyen zonas seguras de bancos, hospitales, edificios policiales o militares y cajeros automáticos. No obstante, la rápida adopción de las tecnologías biométricas permite pensar a corto y medio plazo en nuevos escenarios de control de acceso, como los relativos a la identificación de alumnos en la entrada de las escuelas o la puesta en marcha personalizada de un automóvil.

2) Control fronterizo y aeropuertos

En esta aplicación se utilizan tecnologías biométricas de autenticación para regular o monitorizar el tránsito masivo de personas que entren o salgan por las fronteras de un país. Generalmente, estos sistemas de base biométrica van ligados a sistemas de reconocimiento de documentos (por ejemplo, pasaportes y carnés de identidad). También se suele trabajar con sistemas globales distribuidos, capaces de identificar a individuos inscritos en bases de datos internacionales. Las tecnologías más utilizadas suelen ser las de iris, huella dactilar y verificación vascular.

3) Videovigilancia

El reconocimiento facial puede realizarse a distancia, sobre múltiples usuarios y sin intervención ni conocimiento de estos, circunstancias que lo convierten en una tecnología idónea para la identificación de individuos en espacios multitudinarios. A pesar de que se suele conectar la videovigilancia con la identificación por listas negras (individuos sospechosos o con otras connotaciones negativas), también es habitual utilizar estos sistemas para identificación de listas blancas, como en el caso del reconocimiento instantáneo de clientes importantes o personalidades de interés. Por lo demás, son importantes las aplicaciones de análisis forense, que permiten rastrear fuera de línea horas de con-

tenido audiovisual y metraje capturado con cámaras de vigilancia, por ejemplo para la identificación de individuos relacionados con actos vandálicos o la busca masiva de personas.

4) Control de acceso lógico

Se busca restringir electrónicamente el acceso a archivos de datos y la ejecución de determinadas aplicaciones a los usuarios que tengan autoridad para acceder a tales servicios. De este modo se elimina la tradicional dependencia de contraseñas o *pins*, posibilitando además la grabación de los intentos de acceso y la información biométrica de quien haya intentado acceder. Tiene especial aplicación en el campo de seguridad en la Red, tanto para compras en línea como para transacciones bancarias.

5) Justicia y orden público

La biometría tiene claras aplicaciones legales y policiales, entre las que podemos destacar las relativas a los programas nacionales de gestión de la identidad (es el caso de pasaportes y documentos de identidad biométricos), la investigación de escenas de crimen, el acceso a documentos oficiales y la administración de prisiones. Las tecnologías biométricas más comunes para estas aplicaciones son las de huella dactilar, cara y voz.

6) Registro de entrada

El uso de la biometría es también común en empresas de envergadura, especialmente para el control de asistencia en el puesto de trabajo, de cara a agilizar el proceso de registro y evitar el préstamo, robo o uso fraudulento de tarjetas de identificación. Se trata de un tipo de control de acceso físico, que suele incluir restricciones horarias (por ejemplo, dejando entrar al personal solo en horario de oficina), y suele proporcionar información estadística sobre diferentes cuestiones, como el número de horas de trabajo semanales que lleva cada trabajador, cuáles son las horas de tráfico más alto, o bien cuánta gente permanece todavía en el interior del edificio en caso de una evacuación de emergencia. El método más utilizado es el de la huella, a pesar de que también se emplean el reconocimiento facial, el de iris, el de voz y el de patrones vasculares de la mano.

7) Sanidad/Asistencia sanitaria

Las aplicaciones sanitarias de la biometría incluyen el acceso a historiales y diagnósticos médicos personales (un tipo de control de acceso lógico), así como la asociación de bebés con sus madres para evitar intercambios accidentales de niños.

8) Seguridad en finanzas y transacciones (telecompra)

Las transacciones financieras y la compra de artículos por vía telefónica o a través de Internet (mediante voz sobre IP) también se pueden beneficiar de capas adicionales de seguridad durante el proceso de verificación de este tipo de operaciones. La biometría más adecuada en este caso es la de voz, que resulta muy barata, dado que todos los teléfonos y la mayoría de los ordenadores incorporan micrófonos. Esta tecnología suele complementarse con otros tipos de protección, entre los que figuran las contraseñas o los códigos de identificación.

9) Biometría móvil

De la misma forma que algunas biometrías (cara, huella dactilar) se han introducido con facilidad en el mercado de los ordenadores portátiles para proveer servicios de control de acceso lógico, también se está observando esta tendencia en el caso de los *smartphones* y otros dispositivos móviles. Igualmente existen importantes aplicaciones para la identificación a distancia mediante biometría de voz. Por tanto, este conjunto de aplicaciones es un tipo de control de acceso lógico que suele estar preparado para transacciones comerciales seguras.

10) Marketing y análisis de mercado

Las tecnologías de análisis facial se pueden utilizar no solo para identificación personal, sino también como medio para seleccionar automáticamente los anuncios en función del tipo de audiencia observada (basándose en parámetros como el sexo o la edad), identificar el posible interés de los clientes por ciertos productos y proveer estadísticas de los diferentes segmentos de población observados en los comercios o en zonas concretas de una tienda.

Además de estas aplicaciones genéricas, existe un elevado número de grandes proyectos biométricos en diferentes países de todo el mundo, especialmente en lo referente a programas nacionales de gestión identitaria (en Alemania, Australia, Brasil, Canadá, Estados Unidos, India, Iraq, Israel, Holanda, Nueva Zelanda, Noruega y Reino Unido, por ejemplo). La mayor iniciativa biométrica en la actualidad es la del proyecto Aadhaar, o *India's Unique Identification project*, que pretende recoger 600 millones de registros de huellas dactilares, caras e iris de la mayoría de los 1.200 millones de habitantes de la India hasta finales del 2014.

5. Conclusiones y retos futuros

El hecho de poder reconocer la identidad de una persona de forma confiable constituye un problema de suma importancia para multitud de escenarios de la sociedad actual: finanzas, asistencia sanitaria, redes de transporte, espectáculos, seguridad y orden público, control de acceso, control fronterizo, órganos de gobierno o comunicación.

En este sentido, la biometría, que permite establecer de forma automática la identidad de una persona a partir de sus rasgos personales distintivos, tiene potencial para convertirse en una parte esencial e irremplazable de nuestras vidas.

Las características biométricas, que no pueden compartirse ni traspapelarse, representan de forma íntegra la identidad del individuo a partir de su fisiología o su comportamiento. La conexión de estos rasgos a identidades establecidas de forma externa comporta indudablemente enormes consecuencias, tanto positivas como negativas. Pero utilizadas de forma prudente y racional, estas tecnologías pueden conducir a la sociedad a aumentar la seguridad, reducir el fraude y mejorar la experiencia de usuario.

Las tecnologías biométricas tienen que cumplir una serie de **condiciones necesarias** para poder ser implementadas con garantías:

- universalidad,
- unicidad,
- permanencia,
- mensurabilidad, y
- dificultad de elusión.

No obstante, existen otros **atributos deseables** que refuerzan la utilidad de unas biometrías frente a otras, como por ejemplo su bajo coste, usabilidad o intrusismo, rapidez y sencillez, facilidad para localizar y consultar los datos almacenados, así como el hecho de disfrutar de aceptación, no tener connotaciones negativas y estar en manos de organizaciones confiables, dado que los datos son susceptibles de ser utilizados para finalidades dudosas. La comparación de características entre posibles biometrías nos facilita la tarea de escoger las que mejor se adapten a determinadas aplicaciones o necesidades específicas.

Finalmente, a pesar de que desde la entrada en la era del procesamiento digital se han efectuado enormes progresos en el campo de la biometría, todavía existen a día de hoy un número de **retos importantes** que innegablemente condicionan su futura evolución e implantación, tales como el de lograr la invariancia de las características biométricas en las condiciones del entorno o conseguir sistemas más robustos de detección de vida en las muestras biométricas para evitar casos de fraude identitario (conocido como *spoofing*).

Respecto a los retos de carácter más sociológico, los principales problemas de las instituciones relacionadas con la biometría son garantizar la privacidad personal de los individuos y sensibilizar a la sociedad sobre el verdadero conocimiento de las tecnologías biométricas, para facilitar así su implantación.

Bibliografía

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

Beardsley, C. T. (1972). "Is yourk computer insecure?". *IEEE Spectrum* (vol. 9, nº. 1, págs. 67-78).

Daugman, J. (2004). "How iris recognition works". *IEEE Trans. on Circuits and Systems for Video Technology* (vol. 14, n.º 1, págs. 21-30).

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

Jain, A.; Pankanti, S.; Prabhakar, S.; Hong, L.; Ross, A; Wayman, J. (2004). "Biometrics: A Grand Challenge". *Proceedings of the 17th ICPR.* (vol. 2, n.º 1, págs. 935-942). Piscataway (Nueva Jersey): IEEE publishing.

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

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

Proença, H.; Alexandre, L. A. (2006). "Iris segmentation methodology for non-cooperative recognition". *IEEE Proc. Vis. Image Signal Process* (vol. 153, n.º 2, págs. 199-205).

Ross, A.; Jain, A. (2003). "Information fusion in biometrics". *Pattern Recognition Letters* (vol. 24, n.º 13, págs. 2115-2125). Nueva York: Elsevier.

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

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

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

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

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