

Sistemas de seguridad basados en características biométricas

Autores: Juan Carlos Pérez Cortés - Roberto Paredes Palacios

Los métodos biométricos de identificación son aquellos que permiten reconocer una persona basándose en características fisiológicas o de comportamiento. Se caracterizan por la necesidad de que la persona esté físicamente presente en el lugar de la identificación, pueden o no requerir la colaboración del usuario e incluso pueden obviar la necesidad de que éste conozca la existencia del sistema que lo está identificando.

Los métodos de tipo fisiológico incluyen los siguientes: Reconocimiento de huellas dactilares, Exploración del iris, Exploración de la retina, Geometría de la mano, Reconocimiento facial en luz visible (2D ó 3D), Reconocimiento de la imagen termográfica facial, Análisis de ADN, Reconocimiento auricular, Exploración del patrón venoso en la muñeca, etc.

Entre los métodos basados en comportamientos tenemos: Identificación por la voz, Identificación por la escritura, Dinámica de pulsación en teclado, Análisis del patrón de marcha, etc.

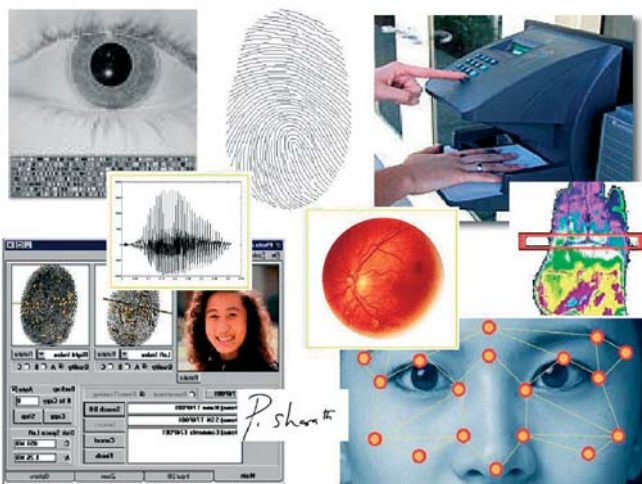
Existen dos modos fundamentales de funcionamiento para un sistema de reconocimiento basado en parámetros biométricos: verificación e identificación. En el primer caso, el usuario se identifica mediante un método típicamente no biométrico, como un código (PIN) o una tarjeta, y el sistema ha de comprobar (verificar) que la identidad proporcionada se corresponde con la realidad. En el segundo caso, se trata de averiguar la identidad del sujeto buscando en una base de datos una representación de parámetros biométricos suficientemente aproximada.

Son aplicaciones típicas de verificación las siguientes: Control de acceso a un recinto, Control de acceso a un sistema informático, Control de identidad por las autoridades, Identificación en votaciones, Utilización de servicios (cajeros automáticos, transporte público, etc.), Cobro de servicios (comercio electrónico, pago a distancia, etc.), Utilización de dispositivos (teléfonos móviles, automóviles, etc.), Confirmación forense de la identidad (identificación de cadáveres, paternidad, etc.).

Entre las aplicaciones de identificación se incluyen: Identificación forense de huellas dactilares latentes, Detección de sujetos en "listas negras" (terrorismo, delincuencia, etc.) en espacios públicos, Control de fronteras, Cobro automático sin interacción del usuario (pequeñas cantidades). La seguridad de un sistema de acceso basado en palabra de paso o número de identificación personal se basa en la confidencialidad de esa palabra o número y, en el caso de una llave o tarjeta de identificación, en evitar su pérdida o su duplicación clandestina. Pero en todos estos casos, la introducción del código o el dispositivo físico siempre sin excepción (salvo fallo del sistema) resulta en un acceso franco al servicio requerido.

Sin embargo, en los sistemas biométricos, debido a la variabilidad de la información procesada (imagen de una huella, de una cara, medidas de longitud de los dedos, etc) se pueden dar casos de falso rechazo del usuario legítimo o, lo que es peor, falsa aceptación de un sujeto no autorizado.

En la práctica, se plantea un compromiso entre la comodidad del usuario (cada falso rechazo implica un nuevo intento por parte del sujeto que intenta acceder o una alarma innecesaria) y la seguridad del sistema. Cuanta más similitud se exige entre los parámetros leídos y los almacenados, más seguridad se obtendrá (menos falsas aceptaciones), pero también más frecuentes serán los falsos rechazos. Así pues, siempre dispondremos de un umbral, normalmente ajustable, que nos permita aumentar la seguridad a costa de disminuir la comodidad del usuario.





La probabilidad de falsa aceptación (False Accept Rate, FAR) representa, pues, la probabilidad de que acceda un individuo no autorizado y la probabilidad de falso rechazo (False Reject Rate, FRR) incide en la frecuencia en que los usuarios legales son rechazados y, por tanto, han de repetir el intento de identificación. La FAR debe ser suficientemente baja, en un rango que suele establecerse entre el 0.0001% y el 0.1%. Por ejemplo, en el 60% de las centrales nucleares de EE.UU. se emplean lectores de geometría de la mano con una FAR de 0.1%. Hay que tener en cuenta que la tasa real de entradas no autorizadas resulta del producto de la FAR por la probabilidad de que un sujeto no autorizado alcance el dispositivo de control e intente el acceso. Si el sistema está complementado con un elemento físico como una tarjeta magnética o un código numérico, por ejemplo, el intruso debe además poseer la tarjeta correspondiente o una copia de la misma, o bien conocer el código de acceso.

La FRR debe también mantenerse baja para evitar el descontento de los usuarios y la ineficiencia del sistema. Por ejemplo, en un recurso con 1000 accesos diarios y una FRR del 1% se producirán 10 incidencias diarias.

La validación de las tasas proporcionadas por los fabricantes no es fácil a causa de los porcentajes tan bajos que se manejan, exigiendo el examen supervisado de miles de accesos para obtener resultados significativos estadísticamente.

Describiremos en detalle los parámetros biométricos más utilizados y sus ventajas e inconvenientes.

Huellas dactilares

La identificación por huellas dactilares es la más antigua de las técnicas biométricas útiles y empleadas ampliamente. La huella dactilar resulta de la impresión dejada por los dedos en el papel mediante tinta, o en otro material por los propios fluidos exudados por la piel (huella latente), o bien de la exploración por parte de un dispositivo electrónico de las crestas papilares presentes en las yemas de los dedos.

Estas crestas configuran un patrón complejo que se considera único para cada individuo (En gemelos idénticos o univitelinos los patrones son similares, pero distinguibles). Existe evidencia

científica de la extrema improbabilidad de que dos huellas dactilares procedentes de dos dedos distintos (del mismo o diferentes individuos) coincidan por azar.

Tradicionalmente, las características extraídas de las huellas han sido, por un lado su tipo (clasificándose en varios tipos y subtipos de acuerdo a diversos esquemas y taxonomías, para facilitar su búsqueda, y por otro las minucias, que son bifurcaciones y finales abruptos de las crestas cuyas posiciones relativas identifican unívocamente la huella junto con la posición del centro y de unas estructuras denominadas deltas. En una huella típica encontramos entre 50 y 100 minucias.

Para obtener estas minucias se realiza un preproceso de la huella que filtra la imagen original y binariza y adelgaza las crestas evitando en lo posible la influencia de manchas, pequeñas cicatrices y residuos presentes en el momento de la impresión digital.

**Se plantea un compromiso
entre la comodidad del usuario
y la seguridad del sistema**

Además de comparar las minucias, existen otros procedimientos de comparación automática entre huellas basados en la correlación de las imágenes de las crestas ya preprocesadas o de las direcciones de las mismas detectadas mediante filtros. Pese a que estos procedimientos poseen la potencialidad de conseguir excelentes resultados, presentan importantes dificultades debido a las deformaciones elásticas que sufren diferentes impresiones de un mismo dedo. Esto los hace en general poco eficientes para búsquedas en grandes conjuntos de huellas.

Ventajas:

- **Alta Universalidad.** La ausencia de algún dedo o de una o ambas manos es relativamente poco frecuente.

- **Alta Permanencia.** Se ha demostrado la invarianza esencial de las huellas dactilares a lo largo de toda la vida de un individuo.
- **Alta Unicidad.** Existe abundante evidencia que demuestra la extrema improbabilidad de que huellas de dedos distintos sean idénticas.
- **Buenas prestaciones.** Existen algoritmos eficientes de comparación entre huellas. La información básica de las minucias puede almacenarse en poco espacio.
- **Alta aceptabilidad.** La larga tradición de uso de huellas dactilares genera una sensación de normalidad en la mayor parte de la población, aunque en casos esporádicos puede asociarse a criminalidad o invasión de la intimidad.

Desventajas:

- **Media Facilidad de medida:** Los lectores electrónicos han llegado a tener costes muy bajos y son fáciles de instalar y mantener, aunque la adquisición de una buena impresión dactilar siempre se halla sujeta a la presencia de suciedad, cicatrices, heridas, etc. Así como muchos de los usuarios no saben colocar correctamente la huella en el lector.

Aunque la aceptabilidad por parte de los usuarios es alta muchos de ellos se resisten a tocar físicamente un sensor que ha sido utilizado previamente por mucha gente.

Identificación por la voz

La voz es uno de los rasgos que identificamos como particulares de las personas y, en la vida diaria, nos permiten reconocerlas con facilidad. Es un medio natural de interacción con el entorno y por tanto resulta muy aceptable para los usuarios pronunciar una palabra o frase ante un micrófono para identificarse.

Las características específicas de la voz de cada persona se deben a diferencias en aspectos fisiológicos y de comportamiento del aparato fonador. La forma del tracto vocal (laringe, faringe, cavidad oral, cavidad nasal, etc.) goza del papel más importante porque modifica fuertemente el contenido espectral de la onda sonora generada. Son precisamente las características del espectrograma de la voz las que configuran los parámetros biométricos usados habitualmente para distinguir un locutor de otro.

Las gran variabilidad de la voz de un mismo individuo a lo largo de periodos relativamente cortos de tiempo, y la moderada especificidad de los parámetros que se extraen de ella hacen que el reconocimiento del locutor sea una técnica de verificación que se usa únicamente en combinación con identificación por tarjeta inteligente, por código de acceso, etc.

Resumimos como en los casos anteriores las características básicas de esta técnica.

Ventajas:

- **Alta Facilidad de medida.** El coste del "hardware" necesario es mínimo y la adquisición muy sencilla y cómoda para el usuario.

- **Alta Universalidad.** El sector de la población con dificultades en el habla es relativamente reducido.
- **Buenas prestaciones.** Actualmente, la verificación es posible con recursos de cómputo muy bajos y el volumen de información almacenado es perfectamente aceptable con los medios de almacenamiento actuales.
- **Alta Aceptabilidad.** Alta. Casi ningún usuario muestra reticencia a pronunciar una palabra o frase para acceder a un recinto o servicio.

Desventajas:

- **Baja Permanencia.** Los parámetros básicos de la voz pueden alterarse fácilmente debido a muchos factores en periodos de tiempo muy cortos.
- **Baja Unicidad.** La capacidad de distinguir un usuario de otro es sólo moderada, ya que un importante parecido de los parámetros vocales no es raro.
- **Baja Resistencia al engaño.** Una simple grabación de calidad permitiría el acceso a no ser que la frase a pronunciar sea, por ejemplo, variable, o haya de ser la respuesta a una pregunta realizada por el sistema de forma aleatoria, etc.

Identificación facial

El reconocimiento facial, es decir, a través de la imagen del rostro, es uno de los que mayor crecimiento, al menos en cuanto a inversión y expectativas, está experimentando actualmente. Se trata de un problema complejo, pero de gran interés, ya que el ámbito de aplicación es muy amplio. Por otro lado, también despierta importantes suspicacias en la población, fundamentalmente en los sectores especialmente preocupados por los posibles perjuicios causados por las nuevas tecnologías en contra de la intimidad y las libertades individuales.

El reconocimiento facial es uno de los que mayor crecimiento en cuanto a inversión y expectativas está experimentando.

Se trata de una área de investigación activa actualmente y por tanto no existe consenso amplio todavía respecto al mejor tipo de características y los procedimientos de comparación más adecuados. En cualquier caso, se trata de almacenar información local (ojos, nariz, boca, etc.) y global (posición de cada rasgo en la cara) e integrarla en un modelo que facilite la identificación y, en su caso, la búsqueda eficiente.

Un sistema típico consta de dos fases. En la primera se trata de localizar la cara en la imagen, distinguiéndola del fondo. En la segunda se caracteriza la misma y se comparan sus parámetros con los almacenados. De la flexibilidad de la

primera fase depende el rango de aplicaciones del sistema y de la precisión de la segunda, las prestaciones del mismo.

Como en el caso de la geometría de la mano o de la identificación por la voz, la aplicabilidad del reconocimiento facial en este momento no alcanza a aplicaciones de búsqueda en grandes conjuntos de "sospechosos" o accesos de alta seguridad si no va acompañada de sistemas clásicos como tarjetas o códigos personales. Los últimos intentos de aplicación a la localización de terroristas, de los cuales el más conocido es el de la policía de Florida en el aeropuerto de Tampa, han supuesto notorios fracasos.

En los sistemas biométricos se pueden dar casos de falso rechazo del usuario legítimo o, lo que es peor, falsa aceptación de un sujeto no autorizado.

Ventajas:

- **Alta Facilidad de medida.** El coste del "hardware" (cámaras) es bajo y la adquisición puede incluso pasar inadvertida al usuario.
- **Alta Universalidad.** Cualquier rostro no oculto por vestimenta es susceptible de verificación.
- **Buenas prestaciones.** La verificación es posible con recursos de cómputo razonables y la búsqueda lo es para conjuntos almacenados de tamaño pequeño o mediano (en el rango de pocos miles de caras) y el volumen de información almacenado es fácil de acomodar con los medios actuales.
- **Alta Aceptabilidad.** Los usuarios no ven interrumpido su flujo de acceso, trabajo, etc.

Desventajas:

- **Baja Permanencia.** El aspecto facial puede cambiar muy rápidamente debido a la aparición de barba, corte de pelo, uso de gafas, etc.
- **Baja Unicidad.** La capacidad de distinguir un usuario de otro es actualmente moderada.
- **Baja Resistencia al engaño.** El uso de disfraces y accesorios como gafas, sombreros, pañuelos, maquillaje, tintes, e incluso cortes de pelo o peinados concretos pueden confundir al sistema. Otras formas de fraude como máscaras o fotografías son posibles, pero su uso se dificulta gracias a las capacidades 3D o termográficas añadidas a algunos sistemas recientes.

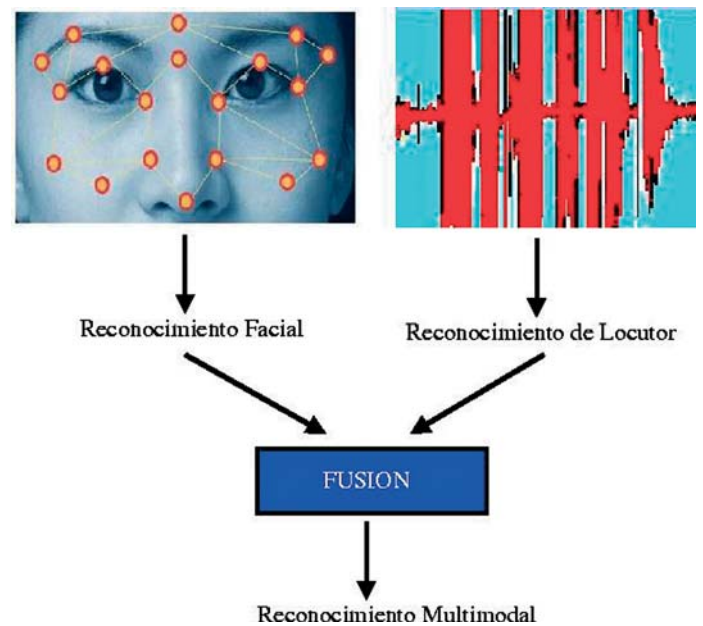
El Instituto Tecnológico de Informática tiene larga experiencia en el desarrollo sistemas de seguridad biométrica. El primer

sistema desarrollado fue un sistema AFIS (sistema de identificación automática de huellas dactilares).

Existen numerosos tipos de sistemas biométricos, cada uno con su rango de aplicación, sus ventajas e inconvenientes. Pero la tendencia actual en sistemas de alta seguridad es utilizar más de una aproximación al mismo tiempo. Esta aproximación Multimodal reduce las tasas de falsa aceptación y falso rechazo, y mejora muy significativamente las prestaciones.

En la actualidad el ITI centra sus esfuerzos en el Reconocimiento Facial y Reconocimiento de Locutor. Ambos sistemas tienen una alta aceptabilidad y universalidad así como un bajo coste de los sensores. En ambos sistema el usuario no tiene que tocar ni interactuar "directamente" con el sensor simplemente ponerse delante de la cámara y hablar. Como desventaja de ambos a resaltar en la baja resistencia al engaño.

Ante esta desventaja el ITI actualmente está trabajando en la combinación de ambos sistemas de reconocimiento biométrico. La combinación del resultado de dichos sistemas resulta en una confianza mucho más alta que la de los sistemas aislados. El resultado del reconocimiento facial junto con el resultado del reconocimiento de locutor se fusiona en un único valor que el sistema evalúa para decidir el reconocimiento final.



En la actualidad el ITI tiene desarrollados varios prototipos y demostradores de dichas tecnologías de seguridad biométrica. Por una parte se ha desarrollado un portero automático para control de acceso a recintos que utiliza el reconocimiento facial junto con el reconocimiento de locutor para permitir o denegar el acceso a un recinto. Asimismo se dispone de un demostrador de detección y reconocimiento facial en tiempo real. Por otra parte también se ha desarrollado toda una serie de librerías y herramientas de desarrollo (SDK) para poder incorporar esta tecnología a cualquier tipo de herramienta que lo requiera. ■