



Paweł Rotter

Centro Común de Investigación de la Comisión Europea
Instituto de Prospectiva Tecnológica, Sevilla
AGH-Universidad de Ciencias y Tecnología, Kraków
Departamento de Automática

Sección coordinada y editada por Claudio Feijoo, IPTS-JRC-EC, con la colaboración de COITAOC/ASITANO

Las tecnologías de identificación personal: la biometría

Las huellas dactilares ya se conocían y utilizaban en Persia para autenticar algunos documentos en el siglo XIV y desde hace más de cien años se las utiliza regularmente para la identificación de criminales. Sin embargo se ha producido un cambio radical en los últimos años: las tecnologías de identificación biométrica *automática* se han desarrollado lo suficiente como para ponerlas en práctica de forma masiva.

La capacidad de identificar a las personas depende del tipo de parámetro biométrico que se utilice, pero esta no es la única condición que debe cumplir una tecnología biométrica para tener éxito en aplicaciones reales.

Una biometría debería ser:

- universal – todas las personas la poseen
- única – personas distintas han de tener medidas biométricas diferentes
- permanente – no se modifican con el tiempo
- fácil de obtener
- aceptable en términos sociales y personales
- difícil de falsificar

El cumplimiento simultáneo de estos requisitos hace que no exista una única solución biométrica óptima en todos los casos de interés.

La primera aplicación masiva de la identificación biométrica ha

sido el control de acceso a los dispositivos electrónicos para proteger los datos confidenciales de sus usuarios. Muchos modelos de ordenadores incorporan un lector de huellas dactilares. Un procedimiento similar se aplica en algunos coches para evitar su uso inautorizado y especialmente contra el

robo. Aunque este modo de protección tiene fallos, funciona bien como medida de seguridad adicional y además, los usuarios son quienes deciden si lo utilizan o no.

Pero surgen cambios mucho más significativos para la sociedad con la utilización de sistemas bio-

	Fortalezas	Debilidades
Huellas dactilares	Facilidad para tomar la muestra; pocos errores de identificación; procedimiento barato	Baja aceptación social
Imagen de la cara	Alta aceptación social	Actualmente existen aún muchos errores de identificación
Iris	Muy pocos errores de identificación	Captura onerosa de la muestra
Geometría de la mano	Comodidad; posibilidad de operar en condiciones difíciles (como alta humedad, grasa sobre las manos, u otras)	Exactitud limitada, precio relativamente alto del sensor
Voz	Facilidad de usar en identificación a distancia (por teléfono).	Problemas con el ruido de fondo durante la captura de la muestra

Tabla 1. Principales fortalezas y debilidades de las tecnologías biométricas más utilizadas



Figura 1. Los lectores de huellas dactilares pueden proteger el acceso a un área restringida, a un ordenador portátil, a una memoria USB o el uso de una puerta. Fuentes: a) www.securityinfowatch.com b) www.trustedreviews.com c) www.zive.cz d) www.adelshop.com

tría de la mano o las características del iris. En estos casos la biometría, si se aplica de manera adecuada (a menudo como una medida adicional), puede incrementar la seguridad y la comodidad.

En el año 2007 aparecieron las aplicaciones más destacadas de la tecnología biométrica, relacionadas con los **documentos personales de identidad**, especialmente con los **pasaportes electrónicos** (e-pasaportes). Éstos, obligatorios en muchos países, incluidos todos los estados de la Unión Europea, contienen únicamente por ahora fotos digitales de la cara para la verificación automática de la identidad, pero a partir del año 2009 incorporarán también las huellas dactilares. El argumento para incluir la tecnología biométrica en los pasaportes es el de incrementar la seguridad (los nuevos pasaportes son mucho más difíciles de falsificar), y obtener a la vez un control rápido, pero hay también mucha polémica sobre si las medidas de seguridad y protección de la privacidad son suficientes. Como se ha demostrado, es posible romper la codificación de los datos biométricos intercambiados entre el pasaporte y un lector. El uso de la tecnología inalámbrica RFID es cómodo pero no ayuda para proteger los datos, y existe incluso la posibilidad potencial de leer los datos biométricos de un pasaporte mientras está en una bolsa de viaje. A pesar de estas amenazas, el uso de la tecnología biométrica en los pasaportes hace la falsificación más difícil y, siendo conscientes de los riesgos potenciales, desde luego ayuda a mejorar la seguridad en las fronteras.

Desarrollos recientes de la tecnología de identificación automática de las personas por medio de

métricos a gran escala. Algunos de ellos son obligatorios o cuasi-obligatorios, como los pasaportes electrónicos, y otros incluso pueden encontrar e identificar las personas en lugares públicos por medio de imágenes de sus caras, sin su conocimiento.

► Sistemas biométricos a gran escala

La primera aplicación de los sistemas biométricos a gran escala ha sido los **sistemas forenses** de identificación personal por medio de huellas dactilares. Aunque la comparación de las huellas dactilares por personas es más fidedigna e incluso necesaria en la parte final de la investigación, gracias a los

métodos automáticos se puede encontrar al sospechoso entre un gran número de personas registradas en el sistema (el sistema IAFIS, utilizado por el FBI, incorpora huellas dactilares de 47 millones de personas). En general, la sociedad acepta el uso de la biometría en los sistemas forenses, pero precisamente a causa de este área de aplicación mucha gente considera que las huellas dactilares tienen una connotación criminal y se resiste a aceptarlas, por ejemplo, en los documentos personales.

El acceso a áreas restringidas, privilegios o dispositivos se protege cada vez con mayor frecuencia por medio de características biométricas, especialmente por medio de las huellas dactilares, la geome-

la imagen de la cara han permitido establecer los primeros sistemas capaces de reconocer individuos de una cierta lista (por ejemplo sospechosos) en una muchedumbre, sin su cooperación o incluso sin ser conscientes de ello. El primer caso bien conocido de uso de este tipo de sistema fue durante el Super Bowl en Estados Unidos en 2001. Las caras del público se comparaban automáticamente con una "lista negra". Según la policía este sistema identificó correctamente 19 criminales, pero debido al gran número de falsas alarmas y a la crítica de la Unión Americana por las Libertades Civiles, no se volvió a utilizar.

Algoritmos de comparación de las muestras. Aunque la comparación de las huellas dactilares o de los iris es rápida y fiable, la identificación automática por la imagen

ciones de captura de la muestra. Por ejemplo las características del iris dependen de la luz, y la identificación por voz puede ser difícil por el ruido de fondo. Una gran

.....

“El acceso a áreas restringidas, privilegios o dispositivos se protege cada vez con mayor frecuencia por medio de características biométricas, especialmente por medio de las huellas dactilares, la geometría de la mano o las características del iris. En estos casos la biometría, si se aplica de manera adecuada (a menudo como una medida adicional), puede incrementar la seguridad y la comodidad”

.....

► Mirando al futuro. Los retos de los sistemas biométricos

Los sistemas de identificación biométrica están aún en desarrollo. Algunos ejemplos interesantes de áreas de investigación abiertas son las siguientes:

de la cara, el método preferido por su alta aceptación social y por la facilidad de tomar la muestra, tiene todavía una alta tasa de errores y por tanto su aplicación es limitada. Otras muchas limitaciones para el uso de la identificación biométrica en aplicaciones cotidianas se deben a las malas condi-

parte de estos problemas se puede resolver mejorando los algoritmos de comparación.

Sistemas multimodales, que identifican a las personas a través de más de una medida biométrica. En este tipo de sistemas se puede prácticamente eliminar la posibilidad de equivocación y además se puede incluir a aquellas personas para las que no funciona algún tipo de biometría (por ejemplo por no tener huellas dactilares significativas, lo que sucede con casi el 2% de la población).

Sensores biométricos, especialmente aquellos con la capacidad de detección de muestras artificiales (*liveness detection*). Algunos sistemas biométricos pueden ser engañados por ejemplo con huellas dactilares de gelatina o con la foto del iris de otra persona. Otros retos relacionados son el desarrollo de lectores de huellas dactilares sin contacto y de lectores a distancia del iris.

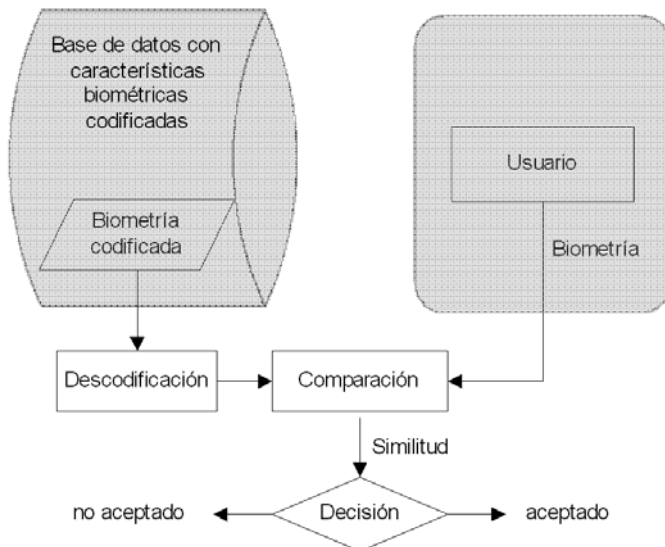


Figura 2. En los sistemas biométricos actuales el cifrado puede proteger los datos biométricos sólo durante su envío por la red o cuando permanecen en la base de datos, pero es necesario descifrarlos antes de la comparación.

Tecnologías de comparación de características biométricas en forma cifrada. Aunque la seguridad de los sistemas no se puede basar en mantener de manera secreta las características biométricas (los atacantes pueden tener muchas oportunidades para tomarlas directamente de la persona), la protección de los datos biométricos es muy importante tanto para la seguridad del sistema, como para mantener unos ciertos requisitos de privacidad. En los sistemas biométricos de hoy, aunque las características biométricas pueden permanecer codificadas en la base de datos y durante su envío por la red, hay que descifrarlas antes de la comparación (Figura 2).

Las investigaciones continúan con el objetivo de elaborar métodos de comparación de características biométricas en forma codificada, lo que permitiría usar un esquema de comparación análogo al que se utiliza para las contraseñas en los sistemas informáticos: las contraseñas se codifican con un algoritmo de cifrado asimétrico

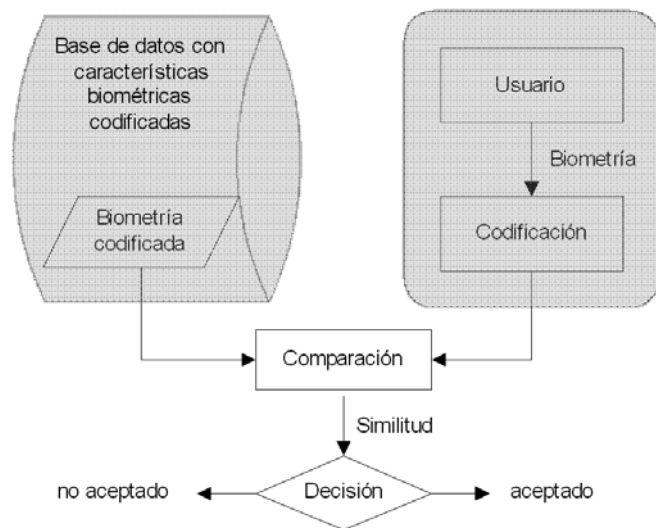


Figura 3. Esquema de comparación de biometrías similar al que se utiliza para las contraseñas en los sistemas informáticos. Sería mucho más seguro, pero todavía no están disponibles métodos de codificación que ofrezcan formas codificadas similares para medidas biométricas similares.

“El uso de la tecnología biométrica en los pasaportes hace la falsificación más difícil y, siendo conscientes de los riesgos potenciales, desde luego ayuda a mejorar la seguridad en las fronteras”

que no conserva la clave para el descifrado. Entonces se pueden comprar las muestras en la forma cifrada, pero no se puede extraer la contraseña original. Para aplicar este esquema a las características biométricas, como se presenta en la Figura 3, hay que elaborar métodos particulares de codificación, donde el grado de similitud de dos muestras codificadas dependería del grado de similitud de las muestras biométricas originales.

Aparte de los retos técnicos descritos anteriormente, para un adecuado desarrollo de los sistemas biométricos, especialmente a gran escala, es necesario darlos a conocer más ampliamente a los usuarios y operadores potenciales. En cualquier caso existe la posibili-

dad de fraudes y no se puede considerar la biometría como el medio único y universal contra el robo de identidad. También hay que tener en cuenta, que la introducción de los sistemas biométricos no siempre se desea. Las mayores causas de resistencia de los usuarios son: procedimientos complicados de alta, posibles incomodidades durante la captura de la muestra, e incluso una cierta impresión de amenaza a la privacidad (en muchos casos justificada).

De otro lado los sistemas de gestión de la identidad exigen cada vez más eficacia y seguridad, lo que no se puede garantizar simplemente con métodos tradicionales. Sin duda, los sistemas biométricos tendrán aquí un papel muy importante.

Este trabajo forma parte de investigaciones del Instituto de Prospectiva Tecnológica del Centro Común de Investigación de la Comisión Europea (IPTS-JRC-EC) sobre los sistemas biométricos y sus perspectivas futuras en la Unión Europea. Para más información consultar <http://ipts.jrc.ec.europa.eu>. ◆

Las opiniones expresadas en este artículo corresponden únicamente a los autores del mismo y, en ningún caso, deben considerarse opiniones oficiales de la Comisión Europea.