Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación

Por Javier y TeresaAreitio

Prof. Dr. Javier Areitio Bertolín
jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE.
Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.

Prof. Dra. Teresa Areitio Bertolín
teresa.areitio@ehu.es
Universidad del País Vasco (UPV / EHU)

En el presente artículo se analiza la biometría una tecnología de costo decreciente e importancia creciente, que constituye una alternativa válida a tener en cuenta para complementar las técnicas tradicionales de control de acceso, basadas en contraseñas, tarjetas inteligentes, llaves criptográficas USB, etiquetas RFID, etc. La tecnología biométrica no sólo sirve para la identificación-reconocimiento, es decir para saber si existe una determinada persona en un recinto o empresa sino también para la verificación-autenticación, es decir para saber si esa persona que se presenta es quién dice ser, para ello se compara con su identidad inscrita previamente almacenada. La verificación es más rápida y presenta un rendimiento mejor que la identificación cuando el número de características-rasgos de referencia guardadas de los usuarios es muy elevado.

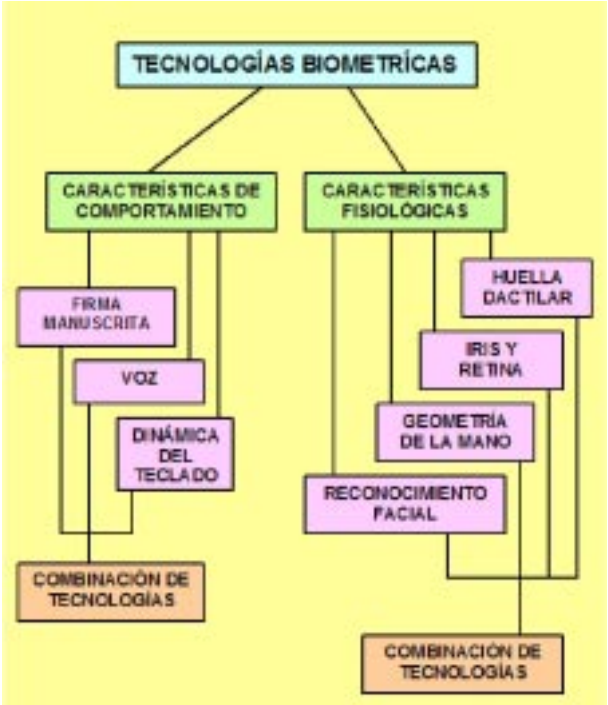

Fig. 1.- Una clasificación sencilla de las tecnologías biométricas.

La biometría permite la autenticación de usuarios en base a sus características físicas como su huella dactilar, patrón del iris, estructura de su voz o forma y aspecto de su escritura manuscrita. El costo de los sistemas biométricos va reduciéndose progresivamente mientras que su fiabilidad y precisión cada vez va en aumento. Existen diversos tipos de enfoques de autenticación como por ejemplo *lo que uno sabe* (una contraseña o *password*, responder a preguntas, *passphrases*, etc.), *lo que uno lleva* (una tarjeta inteligente con PIN), *lo que uno es* (biometría), *donde se encuentra* geográficamente (en base a localización GPS o etiquetas RFID ocultas dentro del cuerpo humano), etc. Para que la autenticación sea usable se requiere que cumpla propiedades como que sea memorizable, entendible, no vulnerable al *phishing,* aceptable psicológicamente, que haga uso de las capacidades cognoscitivas de las personas, por ejemplo que se base en el reconocimiento en vez de tener que recordar. Según el informe sobre el mercado de la industria de la biometría del *Internacional Biometric Group* los ingresos anuales de la industria biométrica han pasado de ser 1,5 billones de dólares en el 2005 a 2,1 billones de dólares en el 2006, para el 2007 se esperan unos 3,01 billones de dólares, para el 2008 se estiman unos 3,8 billones de dólares, para el 2009 se esperan unos 4,7 billones de dólares, para el 2010 se estiman unos 5,6 billones, para el 2011 unos 6,5 billones y para el 2012 unos 7,4 billones de dólares.

La biometría es la ciencia que se encarga de medir las propiedades físicas de los seres vivos. El término biometría proviene del griego donde *bios* significa vida y *metron* medida, puede definirse como el estudio de métodos ideados para el reconocimiento de forma única de personas en base a uno o más rasgos físicos intrínsecos o de comportamiento. La autenticación biométrica permite el reconocimiento automático de una persona utilizando características adecuadas de su cuerpo.

AFIS (Automated Fingerprint Identification System) hace referencia a un sistema biométrico especializado que compara una única imagen dactilar con una base de datos de imágenes de huellas. Lo utiliza normalmente la policía para descubrir criminales a partir de las evidencias recogidas en la escena del crimen, pero también se utiliza en aplicaciones civiles donde las imágenes se capturan colocando el dedo en un escáner o explorando la impresión de la huella sobre papel.

Tecnologias y Tipos de plantillas biometricas. Categorias de aplicaciones y Clases de sistemas.

Las tecnologías biométricas pueden clasificarse atendiendo a muy diversos criterios, así por ejemplo:
(1) Las más actuales: iris, voz, geometría de la mano, rostro, huella dactilar.
(2) No muy utilizadas: medidas del cráneo, termografía facial, patrón de venas de las manos, lóbulos de la oreja, exploración de la retina, huella de la mano, firma manuscrita, dinámica de introducción de teclas sobre un teclado, pigmentación y desarrollo de las uñas, forma de andar o de gesticular, reflectividad óptica de la piel.
(3) Casos especiales: ácidos de la vida (DNA o ácido desoxirribonucleico y RNA o ácido ribonucleico).
(4) Prometido: olor corporal, multiatributos.

Los principales ***tipos de plantillas*** son:
(1) Imagen o impresión bitmap, el filtrado y la compresión *bitmap* permiten seleccionar las características útiles y desechar las inútiles.
(2) Hash tanto unidireccional como reversible.
(3) Cifradas.

Las principales ***categorías de aplicaciones biométricas*** son:
(1) Autenticación uno a uno. (2) Identificación uno a muchos. (3) Investigar contra una lista negra uno a muchos.
(4) Detección de duplicados uno a muchos.
(5) Uno a pocos. Es un híbrido entre identificación uno a muchos y verificación uno a uno. Normalmente el proceso uno a pocos supone comparar una muestra biométrica presentada contra un pequeño número de plantillas de referencia biométricas en un fichero.

Fig. 2.- Ubicación de ataques a un sistema biométrico.

Pueden identificarse las siguientes ***categorías de sistemas biométricos***:
(1) Un ***sistema uni-biométrico*** es aquel que sólo utiliza un único identificador biométrico.
(2) Un ***sistema biométrico unimodal*** es un sub-conjunto de un sistema uni-biométrico que utiliza una única instancia o *snapshot*, una única representación y un único comparador para tomar una decisión de reconocimiento.
(3) Un ***sistema multi-biométrico*** es un sistema biométrico que utiliza más de un identificador biométrico independiente o correlacionado débilmente de un individuo, por ejemplo, la huella dactilar y el rostro de la misma persona o las huellas de dos dedos diferentes de una persona.
(4) Un ***sistema biométrico multi-modal*** es un super-conjunto de un sistema multi-biométrico que puede utilizar más de una medida biométrica correlacionada, por ejemplo varias impresiones de un dedo, varias imágenes de un rostro en un video, varias representaciones de una única entrada, múltiples comparadores de una única representación o una combinación de ellos. La definición de un sistema biométrico uni-modal es la más restrictiva, en cambio, la definición de un sistema biométrico multi-modal es la más general.

Beneficios de la biometría

Algunos de los beneficios que ofrece la tecnología biométrica son: (1) La biometría vincula un evento a un individuo concreto no a una contraseña o dispositivo que lleve como tarjeta inteligente o llave criptográfica USB. (2) Puede considerarse una tecnología conveniente ya que no se tiene que recordar. (3) Es el mismo independiente donde se encuentre el individuo. (4) No puede averiguarse, robarse, transferirse, compartirse, delegarse, perderse, olvidarse o copiarse fácilmente. (5) Previene la suplantación (protege contra robo de identidad y posee un alto grado de no repudio). (6) Mejora la privacidad (protege contra acceso no autorizado a información personal). (7) Es complementario con otros mecanismos de autenticación (como tarjetas inteligentes con PIN y PKI).

La biometría posibilita métodos automatizados para reconocer una persona en base a características fisiológicas, psicológicas o de comportamiento. Algunos ejemplos de tipos biométricos son: huella dactilar (se analizan minucias), rostro de una persona, el patrón del iris o retina, la forma de la mano, la forma de firmar de forma manuscrita (no sólo grafología 2D sino presión en la tableta digitalizadora, rapidez, aceleración, etc.), reconocimiento de voz, forma de teclear sobre un teclado, patrón de surcos de la palma de la mano, patrón de venas del torno de la mano, ácidos de la vida ADN/ARN, olor corporal, estructura de la piel, etc.

Componentes de un sistema biométrico

Los principales componentes que se pueden identificar en un sistema biométrico son:
(1) Sensor. Es el dispositivo de captura los rasgos o características biométricas. Para registrar y convertir los rasgos biométricos en datos de computador se necesitan sensores adecuados. Para la huella dactilar (biometría estática) con vistas a obtener las minucias se utilizan sensores capacitivos, ópticos, térmicos, acústicos y de presión. Para reconocer la firma manuscrita (bimetría dinámica) una tableta sobre la que escribir que detecte presión, aceleración del lápiz, etc.. Para la estructura facial, patrón del iris/retina, geometría de la mano, forma de los

dedos, estructura de las venas de la mano y forma de las orejas una cámara de vídeo, TV o cámara Web. Para la voz, detectando el timbre un micrófono. Para el DNA ácido desoxirribonucleico un laboratorio químico o una unidad electrónica de análisis automatizada. Para el olor corporal sensores químicos. Para reconocer como se pulsan las teclas un teclado.

(2) Repositorio. Es la base de datos donde se almacenan las plantillas biométricas inscritas para su comparación. Debería protegerse en un área física segura, cifradas y firmadas digitalmente.

(3) Algoritmos para extracción de características (procesamiento) y comparación.

Fig. 3.- Tipos de procesos biométricos: de qué formas se trabajar en biometría.

Las tres funciones básicas asociadas a todo sistema biométrico son:

(a) ***Inscripción***. Añade información biométrica a un fichero de datos. Puede incluir protección contra duplicados en la base de datos.

(b) ***Verificación*** (***uno a no***). Se compara contra un único registro. La respuesta es esta persona es quien dice ser.

(c) ***Identificación*** (***uno a muchos***). Se compara todos los registros de la base de datos. La respuesta es se tiene un registro de esta persona.

Las principales sub-funciones comunes a la mayor parte de las técnicas biometricas son:

(1) Captura. Mide la característica biométrica utilizando un dispositivo sensor. Los datos pueden ser una imagen *bitmapped*, un flujo de audio, etc. Pueden capturarse series de muestras. A veces incluye un valor de calidad.

(2) Proceso. Convierte los datos en un identificador numérico o plantilla. Generalmente implica una extracción de características, pero puede también incluir otras manipulaciones.

(3) Comparación. Se compara una plantilla biométrica procesada con una plantilla biométrica inscrita para determinar el nivel de similitud. Existen muchos métodos o tipos de algoritmos a utilizar. La salida del proceso de comparación es el resultado. La probabilidad de coincidencia, es decir que pertenece al mismo sujeto. (4) Decisión. Se determina los resultados de la comparación. Estos resultados se comparan con un resultado umbral, si se encuentra por encima hay coincidencia pero si se encuentra por debajo no la hay. El tiempo de respuesta es el período de tiempo que un sistema biométrico necesita para devolver una decisión sobre identificación o verificación de una muestra biométrica presentada.

Estándares biométricos

Los estándares de interoperabilidad en biometría aunque existen se encuentran en evolución, se pueden distinguir entre otros los relacionados con: la interfaz de aplicación, los de formatos de intercambio de datos biométricos, los de perfiles de aplicación. Son esenciales para el crecimiento de la industria y su adopción generalizada. Algunos de los estándares en biometría son: (1) ISO/IEC 11694-6:2006, utilización de biometría en tarjetas de memoria óptica para identificación. (2) ISO/IEC 19784-2:2007, BioAPI (Biometric Application Programming Interface), (3) ISO/IEC 19795-2:2006, comprobación de rendimiento biométrico. (4) ISO/IEC 24709-2:2007, test de conformidad para BioAPI (Biometric Application Programming Interface). (5) La serie de estándares ISO/IEC 19794 hace referencia a la utilización de las propiedades biológicas para identificar los individuos como por ejemplo huellas dactilares, exploración del iris y reconocimiento del rostro. El ISO/IEC 19794-9:2007, formatos de intercambio de datos biométricos. (6) ISO/IEC 24722:2007, biometría multi-modal y otras multi-biometrías. (7) ISO/IEC 19785-3:2007, formatos de intercambio biométrico comunes. (8) ISO/IEC 19794, formatos de intercambio de datos biométricos. (9) ANSI / NIST-ITL 1-2000, formato común para el intercambio de datos de identificación de huella dactilar, rostro, etc. (10) ANSI X9.84 – 2000, recoge los requisitos de seguridad mínimos para la gestión efectiva de los datos biométricos para la industria de servicios financieros así como la seguridad para la recogida, distribución y procesamiento de datos biométricos. (11) Estándares alemanes DIN NI – AHGB&NI – 37.

La biometría comienza registrando algo de una persona (inscripción) y almacenando los resultados como una referencia biométrica en una base de datos central, en una tarjeta o en un pasaporte que lleva la persona. Siempre que exista la necesidad de identificar una persona existe una posible aplicación biométrica, por ejemplo control de entrada a un edificio o determinadas áreas seguras, a países en controles de frontera, así como acceso a recursos como cuentas bancarias, retirada de dinero y el derecho a servicios. Actualmente estas aplicaciones se realizan por medio de reconocimiento por parte de personas, tarjetas magnéticas e inteligentes con contraseñas o PIN.

Criterios para evaluar técnicas biometricas. vulnerabilidades en un sistema biométrico

A la hora de poder comparar y evaluar un conjunto de técnicas biométricas se pueden identificar diferentes criterios como por ejemplo: (1) ***Universalidad.*** Hace referencia a lo común de encontrar esa biometría o rasgo en cada individuo. Debería darse en el mayor número de personas. Todo el mundo debería tener ese rasgo.
(2) ***Unicidad***. Mide lo bien que la biometría separa un individuo de otro. Cada persona debería tener un valor diferente.
(3) ***Permanencia***. Mide lo bien que una biometría resiste el envejecimiento. No debería cambiar con el tiempo. Debería ser invariante con el tiempo.
(4) ***Medibilidad o coleccionabilidad***. Indica la facilidad para adquirir una biometría para la medida, es decir, facilidad para medir con instrumentos simples. Debería poderse medir cuantitativamente. (5) ***Rendimiento***. Indica la precisión, velocidad y robustez del sistema que captura la biometría.
(6) ***Aceptabilidad***. Indica el grado de aprobación de una tecnología por el público en la vida diaria, que sea fácil y cómodo de medir. La percepción del público debe ser positiva. Debe proporcionar el mayor grado de confort.
(7) ***Burlabilidad***. Mide la facilidad para engañar al sistema biométrico, es decir el grado en que es circunvalable. (8) ***Costo*** debido a los sensores.
(9) ***Dificultad de mantenimiento***.

Los posibles ***puntos de vulnerabilidad*** de un sistema biométrico son:
(1) Dispositivo de captura biométrica o sensor. Actuar sobre el entorno cambiando el grado de luz o generando interferencias electromagnéticas. Simular, sustituir o robar el elemento a medir.
(2) Dispositivo de almacenamiento biométrico. Sustituir o falsificar las referencias biométricas.
(3) Conexiones con los sistemas locales. Interceptar, modificar e insertar mensajes falsos.
(4) Infraestructura local, intermedia y remota. Cortes de alimentación eléctrica.
(5) Redes a los servidores remotos.
(6) Procesadores back-end. Introducción de troyanos.
(7) Bases de datos back-end. Cambiar datos almacenados.

Para valorar lo robusto de un sistema biométrico se pueden seguir dos enfoques:
(1) En caso de no existir adversarios se deben estudiar los parámetros como FAR y FRR.
(2) En caso de haber adversarios. Se debe analizar donde pueden interceptar información y de que modo pueden falsificar algún elemento de la arquitectura desde el ente a verificar, el proceso de decisión sin virus, la base de datos de comparación sin código malicioso, etc. Tener en cuenta que los elementos biométricos que se exploran son privados pero no secretos con lo cual un atacante puede capturar las huellas dactilares de la victima de la copa que previamente haya podido tocar.

Medidas en un sistema biométrico. Efectividad-precisión

Se ha definido numerosos parámetros para medir el rendimiento de un sistema biométrico como por ejemplo:
(1) FAR (False Accept Rate). Es la probabilidad de que una persona no autorizada sea identifica-

Tecnología Biométrica

Criterios de Comparación	Iris	Retina	Huella dactilar	Voz	Venas de la mano	Dinámica del teclado	Rostro
Unicidad	Alto	Alto	Alto	Bajo	Medio	Bajo	Bajo
Rendimiento	Alto	Alto	Alto	Bajo	Medio	Bajo	Bajo
Universalidad	Alto	Alto	Medio	Medio	Medio	Bajo	Alto
Permanencia	Alto	Medio	Alto	Bajo	Medio	Bajo	Medio
Aceptabilidad	Bajo	Bajo	Medio	Alto	Medio	Medio	Alto
Burlabilidad	Alto	Alto	Alto	Bajo	Alto	Medio	Bajo
Coleccionabilidad	Medio	Bajo	Medio	Medio	Medio	Medio	Alto

Tecnología Biométrica

Criterios de Comparación	Termografía Facial	Firma Manuscrita	DNA	Geometría de la mano
Unicidad	Alto	Bajo	Alto	Medio
Rendimiento	Medio	Bajo	Alto	Medio
Universalidad	Alto	Bajo	Alto	Medio
Permanencia	Bajo	Bajo	Alto	Medio
Aceptabilidad	Alto	Bajo	Alto	Medio
Burlabilidad	Alto	Bajo	Bajo	Medio
Coleccionabilidad	Alto	Alto	Bajo	Alto

Fig. 4.- Comparativa entre diversas tecnologías biométricas.

da es decir aceptada como autorizada. Mide la frecuencia con que un usuario no autorizado que no debería concederse acceso se reconoce por equivocación como legítimo. Es la proporción de falsa aceptación de entre un número total de intentos de reconocimiento de impostores. A veces se confunden los conceptos FAR y FMR, no obstante una diferencia de FMR respecto a FAR es que no se contabilizan los intentos previamente rechazados debido a una calidad deficiente de la imagen o FTA. Si el FAR vale 0,01% significa una probabilidad de uno entre 10.000 de averiguar, por su parte un PIN de cuatro dígitos decimales presenta una probabilidad de uno entre (10.10.10.10 = 10.000) de averiguarlo, no obstante si comparamos un PIN y un FAR vemos el secreto del FAR es más difícil de averiguar que el de un PIN de un sistema biométrico ya que los PIN son valores únicos mientras que el FAR no es un valor estático e incluye todas las muestras. A veces el FAR se utiliza como medida de la seguridad de un sistema de verificación biométrica, de modo que *seguridad* = (1 – FAR).

(2) **FRR** (False Reject Rate). Es la probabilidad de que una persona autorizada no se le identifique, es decir se le deniegue el acceso. Es el porcentaje de falsos rechazos de entre el número total de intentos de reconocimiento válidos. Mide la frecuencia con que un usuario autorizado que debería concederse acceso no se le reconoce. A veces la conveniencia de un sistema biométrico se mide a partir del FRR, de modo que *conveniencia* = (1 – FRR). A mayor FRR menos conveniente es el sistema debido a que más sujetos son reconocidos incorrectamente y por tanto están sujetos a denegación de servicio o al proceso de gestión de excepciones.

(3) **FTE** o **FER** (Failure To Enroll Rate). Es la proporción de personas que fallan ser inscritas con éxito. Para una persona el FER se obtiene dividiendo el número de intentos de inscripción sin éxito dividido entre el número total de intentos de inscripción. El FER global para N participantes se define como el producto de la inversa de N multiplicada por el sumatorio de los FER de cada persona. A veces también se utiliza la terminología **FTER** (Failure to Enroll Rate) para designar el porcentaje de fallos para inscribirse del número total de intentos de inscripción. Es decir mide la frecuencia con que los usuarios no pueden inscribir una característica biométrica. La característica física de un usuario impide la creación de la plantilla debido a que la característica no exista (le falte el dedo pulgar) o se encuentre obscura (dedo pulgar quemado). El usuario no es capaz o no esta dispuesto a presentar su rasgo biométrico adecuadamente.

(4) **FTA** (Failure To Acquire). Mide la cuenta de intentos de verificación/identificación sin éxito por error de personas inscritas legítimamente. El FTA puede originarse debido a características temporalmente no medibles por calidad de imagen del sensor no suficiente o un vendaje en el dedo donde se toma la huella. El FTA se suele considerar dentro del FRR y no necesita calcularse por separado.

(5) **FIR** (False Identification Rate). Es la probabilidad de que una persona autorizada sea identificada pero se le asigne un identificador falso. Es la probabilidad en una identificación de que la característica biométrica sea asignada falsamente a una referencia. Después de una comparación de características más de una referencia excederá el umbral de decisión.

(6) **FMR** (False Match Rate). Es la tasa a la que las personas no autorizadas sean falsamente reconocidas durante una comparación de características.

(7) **FNMR** (False Non-Match Rate). Es la tasa de que las personas autorizadas sean falsamente no reconocidas durante una comparación de características. A veces se confunden los conceptos FRR y FNMR, no obstante una diferencia de FNMR con respecto a FRR es que no se contabilizan los intentos previamente rechazados debido a una calidad deficiente de la imagen o FTA. (8)

TECNICAS BIOMETRICAS MÁS UTILIZADAS	PORCENTAJES DE UTILIZACIÓN EN EL MERCADO
AFIS / Live-Scan	33,6 %
Huella dactilar	25,3 %
Reconocimiento del rostro	12,9 %
Reconocimiento del iris	5,1 %
Geometría de la mano	4,7 %
Reconocimiento de voz	3,2 %
Reconocimiento de venas	3,0 %
Biometría múltiple	2,9 %

Fig. 5.- Principales tecnologías biométricas utilizadas en el mercado según el *Internacional Biometric Group*.

EER (Equeal Error Rate). Es el punto común de intersección entre las curvas FAR y FRR.
(9) ROC (Receiver Operating Curve). Es un gráfico que muestra como varía la FRR en función de la FAR de acuerdo a un umbral de decisión. Es decir ROC es una función dibujada sobre unos ejes de coordenadas cartesianas cuyo eje de ordenadas es FRR o FNMR y cuyo el eje de abscisas es FAR o FMR.
(10) DET (Detection Error Tradeoff). Es una curva dibujada sobre unos ejes de coordenadas cartesianas cuyo eje de ordenadas es FRR y cuyo eje de abscisas es FAR. Es similar al ROC y permite comparar sistemas de verificación biométricos.

Técnicas para probar que se es humano

La biometría sirve para identificar y autenticar personas y seres vivos en base a tres factores fundamentales:
(1) De tipo genético (rasgos de genotipo). Los gemelos monocigóticos poseen los mismos rasgos de genotipo.
(2) Debidas a variaciones aleatorias en las fases tempranas del desarrollo embrionario (rasgos de fenotipo o randotipo).
(3) A través del aprendizaje (con rasgos de comportamiento).

Las características biométricas varían con el tiempo debido a factores como el crecimiento, edad, desgaste por el uso, suciedad y mugre, heridas y regeneración subsiguiente, etc. Las HIPs (*Human Interactive Proofs*) permiten a una persona autenticarse como miembro de un grupo dado (como humano frente a máquinas, como ella frente a otras, como adulto frente a niños, etc.), se utilizan para detener spam y mensajería automatizada. Consiste en lo siguiente: el computador presenta un desafío que debe ser fácil para que lo supere la clase de humanos, en cambio debe ser difícil de superarlo por parte de los que no sean miembros.

La mayor parte de los HIPs son de tipo gráfico o CAPTCHAs (*Completely Automated Public Turing test to tell Computers and Humans Aparts*). Un tipo común de CAPTCHA requiere que el usuario teclee las letras de una imagen distorsionada que se le presenta, a veces con la adición de un fondo obscurecido con una secuencia de letras y números que aparecen superpuestos para dificultar las técnicas de visión por computador. Otros tipos de HIPs con desafío no gráfico requieren reconocer voz, resolver puzzles, etc.

Consideraciones finales

La tecnología biométrica proporciona un método robusto de vincular personas a registros de identidad. Los rasgos biométricos no pueden compartirse, ni las personas pueden equivocarse al introducirlos, ni olvidarse lo cual significa una mayor contabilidad y seguridad. Los principales retos con los que se enfrenta la tecnología biométrica son: que las representaciones sean invariantes, la segmentación de una imagen con muchas personas para seleccionar una en concreto, la no universalidad y los datos con ruido, la comparación robusta, las bases de datos de gran tamaño, la seguridad del propio sistema biométrico y la protección de la privacidad del usuario.

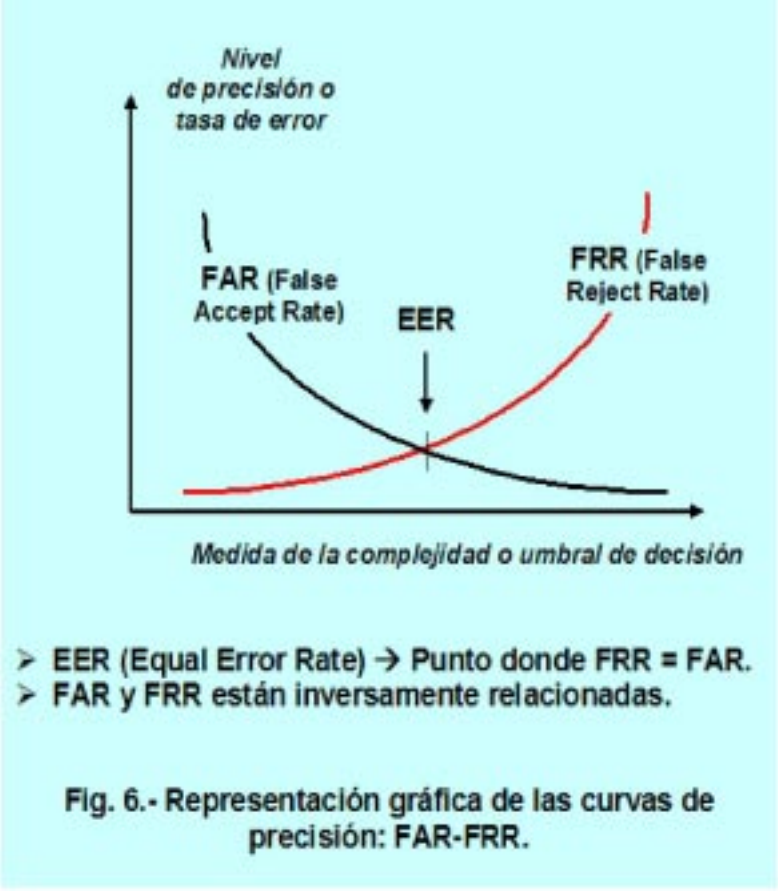

Fig. 6.- Representación gráfica de las curvas de precisión: FAR-FRR.

El futuro de la biometría tenderá a desarrollar dispositivos más pequeños, baratos, rápidos y más precisos. Se observa una fusión de diversas técnicas biométricas como reconocimiento de rostro y reflectancia de la piel. Así mismo los fabricantes combinan la biometría con otros mecanismos de autenticación como tarjetas inteligentes y PKI (Public Key Infrastructure).

Se observa un crecimiento en la concienciación pública y su aceptación. La industria se esta enfocando en la privacidad y securización de los datos biométricos desarrollando dispositivos electrónicos anti-falsificación. Ejemplos de utilización de la tecnología biometría son:

(a) Entorno comercial: acceso a instalaciones y sistemas de información. Control y cronometraje de empleados. Transacciones de punto de venta al por menor.
(b) Entorno de la ejecución de leyes: investigaciones de delitos y análisis forense.

IMAGEN DE UNA HUELLA DACTILAR

Imagen formada por cuatro regiones:

REGIÓN - 1 p(1) = 0,00	REGIÓN - 3 p(3) = 0,25
REGIÓN - 2 p(2) = 0,50	REGIÓN - 4 p(4) = 0,25

n → Número total de posibles regiones o localizaciones para las *minucias* en la imagen. En este caso n = 4.

p(x) → Probabilidad de que las minucias ocurran en cada región concreta.

Entropía en bits aplicando Shannon →

$$H(x) = \sum_{x=1}^{x=n} p(x).\log_2\left(\frac{1}{p(x)}\right) =$$

$$= 0{,}50.\log_2(2) + 2.[(0{,}25).\log_2(4)] = 0{,}5 + 1.0 = 1{,}5$$

Fig. 7.- Cálculo de la entropía de la información del secreto que oculta la imagen de una huella dactilar biométrica.

(c) Entorno de los sistemas civiles: control de fronteras e inmigración, verificación y protección. (d) Entornos militares: acceso a salas de disparo de misiles intercontinentales.
(e) Entorno industrial: acceso a centrales nucleares. Los principales aspectos que consiguen una buena biometría son: que sea única, permanente, fácil de utilizar, rápida, precisa, de bajo costo y de percepción positiva por parte del público.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto *LEFIS-APTICE: Legal Framework for the Information Society II* (financiado por Socrates 2005. *European Commission*).

Bibliografia

- Areitio, J. "Análisis en torno a la auditoria de seguridad en tecnologías de la información y las comunicaciones". Revista Española de Electrónica. Nº 625. Diciembre 2006.

- Areitio, J. "Determinación del ROI/ROSI: Elemento clave del análisis de riesgos de seguridad de la información". Revista Española de Electrónica. Nº 589. Diciembre 2003.

- Areitio, J. "Identificación y análisis en torno a la PKI y su relación con los certificados digitales y la firma electrónica avanzada". Revista Española de Electrónica. Nº 596. Julio 2004.

- Forouzan, B.A. "Network Security". McGraw-Hill. NY. 2007.
- Ashbourn, J.D.M. "Biometrics: Advanced Identity Verification. The Complete Guide". Springer Verlag. 2000.

- Reese, R. "Network Security". John Wiley & Sons. Inc. 2007.