AVANCES EN TÉCNICAS BIOMÉTRICAS Y SUS APLICACIONES EN SEGURIDAD

ING. ENRIQUE J. TORREALBA
HARDWELL Caracas-Venezuela
E-mail: etorrealba@hardwell.com

RESUMEN

La biometría se basa en la premisa de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris de los ojos, etc) o de comportamientos (la voz, la manera de firmar, etc), los cuales pueden ser utilizados para identificarla o validarla. La medición biométrica ha venido estudiándose desde tiempo atrás y es considerada en la actualidad el método ideal de identificación humana. Esta ciencia trae consigo implícitamente aplicaciones para sistemas de seguridad como control de acceso, identificación en votaciones, utilización de servicios (cajeros automáticos, transporte publico, etc), cobro de servicios, utilización de dispositivos (teléfonos móviles, automóviles, etc). En este trabajo se describe el funcionamiento básico de los productos biométricos así como la probabilidad de aceptación falsa (FAR) y la probabilidad de rechazo falso (FRR). Los diferentes métodos biométricos son mencionados, analizando los mas recientes y los que desarrollan mas actualmente como son: escáner de iris, reconocimiento facial, etc. Con la idea de unificar y orientar todas las investigaciones en una sola dirección se han desarrollado algunos estándares de Biometría, los cuales se mencionan al final del trabajo.
Palabras claves: Biometría, Autentificación, PIN, FAR (False accept Rate), FFR (False Reject Rate).

ABSTRACT

The biometry is based in the fact that each individual is unique and has distinguishing physical characteristics (face, fingerprints, iris of the eyes, etc) or of behaviors (the voice, the way to sing, etc), which can be used to identify or validate them. Biometric measurement has been studied for many years and it is considered the ideal method for human identification at the present time. This science implicitly has applications for security systems like access control, identifications in elections, use of services (automatic bank machine, public transportations, etc), charge of services, use of devices (mobile phones, cars, etc). In this work is described the basic operations of the biometrics products as well as the false accept rate (FAR) and false reject rate (FRR). Several biometrics methods are examined in this document. While all methods will be identified only the most recent methods, and those presently in development will be analyzed in depth; iris scanners, face recognition, etc. With the idea to unify and to orient all the investigations in a single direction, standards of Biometry have been developed, which are mentioned at the end of the work.
Keyword: Biometry, Authentication, PIN, (False accept Rate), FFR (False Reject Rate).

INTRODUCCIÓN

El concepto tradicional de biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Esta definición comprende una disciplina que se inicio a principios del siglo XX. En el contexto tecnológico esta palabra se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas con el objeto de establecer una identidad.

Los sistemas de seguridad utilizan básicamente tres tipos de autentificación:

- Algo que el individuo sabe: una contraseña, un PIN (Personal Identification Number)
- Algo que el individuo tiene: una llave, una tarjeta de proximidad, una smart card, etc.
- Quien es el individuo: seguridad biométrica.

De los tres métodos, las técnicas biométricas es la más segura y conveniente ya que una contraseña puede ser traspasada, una tarjeta robada, pero la identidad difícilmente puede ser falsificada.

Después de los lamentables atentados del 11 de Septiembre de 2001, se ha creado una enorme demanda de productos de seguridad. Por su alto nivel de seguridad, los productos biométricos han acaparado gran parte de la demanda. Aunque en algunos casos estos productos son considerados innovadores, existen desde hace mas de 15 años y han sido usados principalmente en Europa e Israel, donde se presentaba la mayor cantidad de secuestros y atentados terroristas durante los años 70's y 80's.

FUNCIONAMIENTO DE LOS PRODUCTOS BIOMÉTRICOS

Para realizar la autentificación biométrica, primero se debe registrar a los individuos que van a hacer uso del sistema. Para el registro (en ingles, enrollment) se utiliza un dispositivo biométrico para examinar el atributo físico o de comportamiento elegido. Un software realiza el procesamiento de datos y los convierte en patrones matemáticos, este conjunto de datos matemáticos constituye la plantilla (en ingles, template) y forma parte de la base de datos que identifica al individuo. La plantilla y un dato asociado con al individuo como por ejemplo nombre o PIN, son guardados electrónicamente.

La autentificación posterior se realiza cuando el individuo presenta su rasgo corporal o muestra su comportamiento ante un dispositivo biométrico. Nuevamente los datos del rasgo son cuantificados pero guardados en una plantilla diferente, para posteriormente realizar la comparación con la que esta almacenada en la base de datos. La búsqueda para realizar esta comparación se realiza de dos maneras. La primera es una búsqueda de uno a muchos (1:N), solamente se presenta el rasgo y el sistema se encarga de buscar entre todas las plantillas guardadas, quien es el individuo, esto es conocido como identificación. Este método requiere mayor cantidad de procesamiento que el segundo, es usado en aplicaciones criminalísticas. La segunda manera de llevar a cabo la búsqueda es uno a uno (1:1), en este caso el individuo presenta adicionalmente su nombre o numero de identificación. Es sistema se encarga de buscar la plantilla que este guardada con el nombre presentado, y realiza la comparación. Esta última es conocida como verificación.

Para que se certifique al individuo, la comparación no necesariamente resulta en una igualdad entre ambas plantillas. En realidad pueden pasar años antes de que el individuo presente una plantilla igual a la guardada. Una serie de factores pueden influir en leves variaciones matemáticas asociadas al patrón tomado. Para realizar la certificación, las plantillas deben ser similares entre si en cierto grado. Esto no implica que los sistemas biométricos no sean seguros, sino que son sistemas probabilísticos, no absolutos.

Sin embargo, en los sistemas biométricos, debido a la variabilidad de la información procesada (imagen de una huella, 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 del sujeto no autorizado.

En la práctica, se plantea un compromiso entre la comodidad del usuario y la seguridad del sistema. Cuanta mas similitud se exige entre los parámetros leídos y los almacenados, mas seguridad se obtendrá (menos falsas aceptaciones), pero también mas frecuentes serán los rechazos. Así, pues

siempre dispondremos de un umbral, normalmente ajustable, que nos permita ajustar la seguridad a costa de disminuir la comodidad del usuario.

FAR Y FRR

La probabilidad de falsa aceptación (False Accept Rate, FAR) representa, *la probabilidad de que acceda un individuo no autorizado y la probabilidad de falso rechazo (False Reject Rate, FRR) inciden 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 los EE.UU se emplean lectores con la geometría de 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 esta completamente 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.

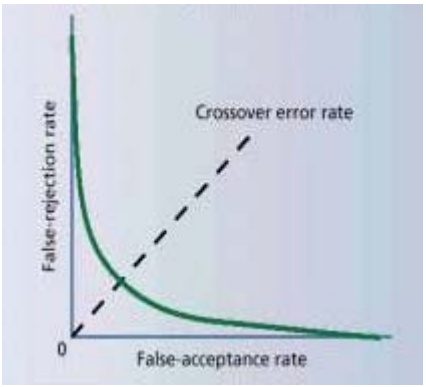

Figura 1. Tasa de error cruzada entre FRR y FAR.

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 y una FRR del 1% se producirán 10 incidencias diarias.

MÉTODOS BIOMÉTRICOS

Los métodos de tipo fisiológico incluyen lo siguiente: reconocimiento de huellas dactilares, exploración del iris, exploración de la retina, geometría de la mano, reconocimiento facial en luz visible (2D y 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 se tiene: Identificación para la voz, identificación por la escritura, dinámica de pulsación de teclado, análisis del patrón de marcha.

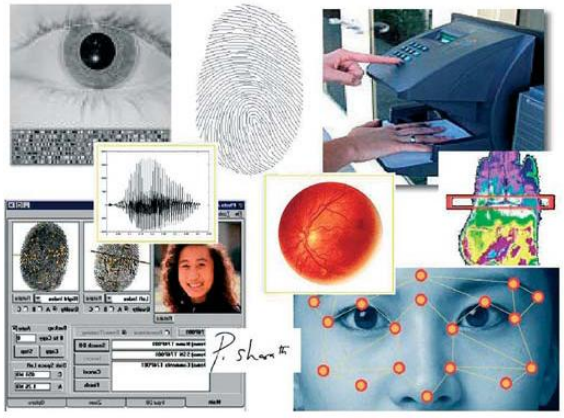

Figura 2. Diferentes técnicas biométricas usadas en aplicaciones de seguridad.

ESCANER DE LA IRIS

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de

hasta 266 grados de libertad - inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado, usando una cámara de alta resolución.

Generalmente esto se hace mirando a través del lente de una cámara fija, la persona simplemente se coloca frente a la cámara y el sistema automáticamente localiza los ojos, los enfoca y captura la imagen del iris, ésta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 KBytes) suficiente para los propósitos de autenticación. Esa muestra, denominada iriscode (en la figura 3 se muestra una imagen de un iris humano con su iriscode asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.

El iris del ojo como un identificador es quizás uno de los métodos más ajenos para las personas, ya que entre nosotros no nos reconocemos por la apariencia del iris.

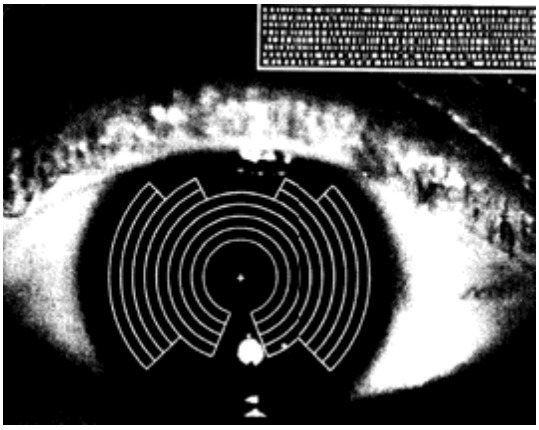

Figura 3. Iris humano y su iriscode.

Este identificador es uno de los más precisos entre los sistemas biométricos. Algunos factores que han afectado su proliferación lo son la poca aceptación entre sus usuarios y el precio muy caro de la tecnología.

IDENTIFICADOR DE PATRONES DE VOZ

La voz es otra característica que las personas utilizan comúnmente para identificar a los demás. Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares. Tan solo basta recordar las veces en que reconocemos a alguien conocido por teléfono para comprender la riqueza de esta característica como método de reconocimiento.

Los sistemas de verificación mediante la voz “escuchan” mucho mas allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que emitimos, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, también crean modelos de la anatomía de la traquea, cuerdas vocales y cavidades. Muchos de estos sistemas operan independientemente del idioma o el acento de la persona.

Esa tecnología ya fue utilizada, pero no fue bien recibida (a pesar de ser relativamente barata) pues es relativamente fácil de romper con grabaciones digitales y por la posibilidad de rechazar una autenticación de alguien que tenga los patrones levemente a alterados por causa de la inestabilidad de la voz.

RECONOCIMIENTO FACIAL

Muy popular hoy en día, relativamente barato y con niveles razonables de acierto, este dispositivo captura patrones geométricos en el rostro a través de una cámara. Los sistemas de reconocimiento de rostro son tal vez los más fáciles de comprender ya que para nosotros la cara es la manera más directa de identificar a los familiares, amigos, conocidos o celebridades.

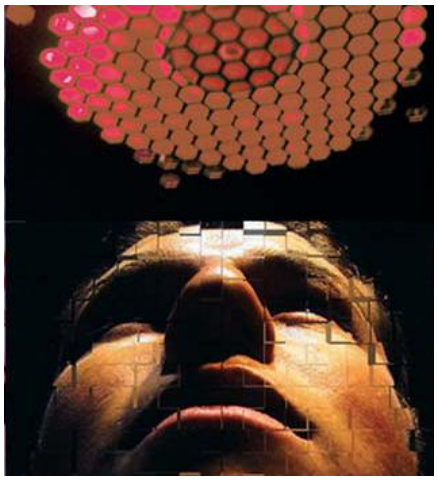

Figura 4. Reconocimiento facial

Los métodos utilizados en el reconocimiento de rostros van desde la correlación Estadística de la geometría y forma de la cara, hasta el uso de tecnología de redes neuronales que buscan imitar la manera en que funciona el cerebro humano. Muchos de estos sistemas pueden reconocer a una persona aun cuando esta se haya dejado crecer la barba o el bigote, se pinte o se cambie el estilo del cabello, tenga maquillaje o use anteojos.

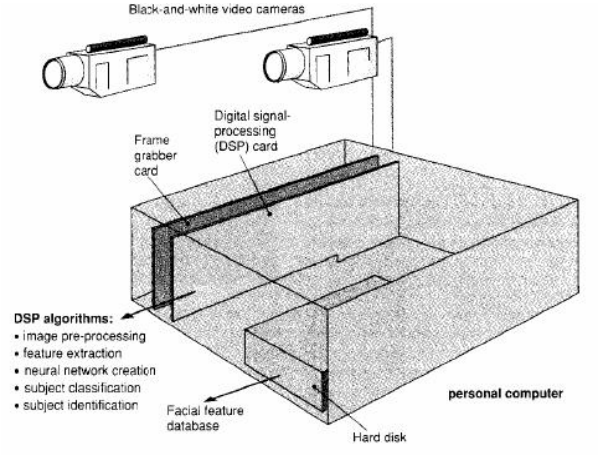

Figura 5. Componentes de lector biométrico facial.

ESTÁNDARES EN BIOMETRÍA

La aparición de este número importante de nuevos estándares es reflejo del creciente interés industrial por este ámbito tecnológico, ya que estos estándares persiguen garantizar el marco imprescindible para el análisis comparativo de los nuevos productos que desarrollen las diferentes empresas. No se considera iniciativas que sólo tengan aplicación a una sola modalidad biométrica, sino que se hace referencia a las que abarcan un ámbito más multi-modal.

A escala internacional el principal organismo que trata de aunar las diferentes actividades de estandarización biométrica es el Sub-Comité 17 SC17 del *Joint Technical Committee on Information Technology* (ISO/IEC JTC1), del *International Organisation for Standardisation* (ISO) y el *International Electrotechnical Commission* (IEC). En Estados Unidos desempeña un papel similar el Comité Técnico *M1* del

INCITS (*InterNational Committee for Information Technology Standards*), que guarda una estrecha relación con el *National Institute of Standards and Technology* (NIST) que desde hace décadas viene desempeñando un papel muy activo en el mismo ámbito.
Ya dentro de los resultados que se van alcanzando por los organismos anteriores en el ámbito de la estandarización, podemos destacar como principales las siguientes iniciativas:

- **BioAPI**. Es sin duda uno de los estándares más conocidos, que define una interfaz de programación API abierta, común para el desarrollo de aplicaciones de un amplio espectro de tecnologías biométricas.

- **CBEFF** (*Common Biometric Exchange Framework Format*). Desarrollado por NIST y *Biometric Consortium* propone un formato estandarizado para el intercambio de información biométrica. No persigue conseguir una compatibilidad entre diferentes tecnologías biométricas, pero permite una fácil identificación de información de utilidad como: tipo de sensor, versión, fabricante, etc.

- **X9.84**. Es un estándar consensuado para la industria de servicios financieros que hace referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

- **HRS/CDSA** (*Human Recognition Service - Common Data Security Architecture*). Contempla una jerarquía de niveles de seguridad y un marco de aplicación de técnicas criptográficas para entornos cliente-servidor multi-plataforma. Este estándar es de nuevo compatible con la especificación **BioAPI** y **CBEFF**.

CONCLUSIONES

La tecnología biométrica representa un área de los sistemas de seguridad que no debe ser ignorada por las compañías. Los biométricos incluyen una gama de características que benefician a dueños, empleados y clientes. Las compañías que adopten los biométricos en forma temprana gozaran de una ventaja competitiva.

La biometría busca la automatización de tareas que involucran el reconocimiento del individuo, el hecho de que las maquinas no evalúen ningún otro factor al tomar una decisión si no que la identidad, esto resta cualquier factor subjetivo que pueda comprometer la seguridad.

Algunos dispositivos biométricos son más fáciles de usar que otros. Por ejemplo, los biométricos de mano utilizan guías para indicar la posición de la mano; en los lectores de cara puede ser difícil registrarse porque algunas personas tienen dificultad para alinear la cara en la posición correcta.

BIBLIOGRAFIA

www.neotec.com.pa/pdf/introduccionalos**biometricos**.pdf

http://www.biometricaccess.com/products/wp_impor.htm

http://bibliotk.gdl.up.mx/ceup/huella.pdf

http://www.bio-tech-inc.com/bio.htm

http://www.iti.upv.es/services/reviewtic/publ ic/2005/06/pdf/2005-06-biometria.pdf/attach/2005-06-biometria.pdf

http://www.jeuazarru.com/docs/biometria.pdf

www.madrimasd.org/informacionidi/entrevistas/quienesquien/pdf/53.pdf