

SUMARIO

Identificación Biométrica y su unión con las Tarjetas Inteligentes

Raúl Sánchez Reillo

Grupo Universitario de Tarjeta Inteligente

Dpto. de Tecnología Fotónica

E.T.S.I. Telecomunicación

UNIVERSIDAD POLITÉCNICA DE MADRID

La Identificación Biométrica, es decir, el reconocer a una persona por alguna característica biofísica o de comportamiento, está tomando cada vez más importancia. Esta importancia nace de las limitaciones existentes en los sistemas actuales de identificación de una persona (por contraseñas y/o tarjetas). En este artículo se presenta una introducción a la Biometría, comentando las diversas etapas de que se compone un Sistema de Identificación Biométrica, así como las distintas técnicas existentes en la actualidad. Por último se mencionan las posibles vías para la integración de la Biometría con otra tecnología de seguridad e identificación: las Tarjetas Inteligentes.

Identificación Biométrica y su unión con las Tarjetas Inteligentes

De una forma constante y casi sin darse cuenta, una persona realiza durante todo el día múltiples identificaciones: reconoce a los componentes de su familia y a sus compañeros de trabajo, simplemente viéndolos en persona o en fotografías; a clientes y amigos según se habla con ellos por teléfono, o incluso reconociendo quién ha podido escribir un determinado texto por la caligrafía utilizada. De una forma menos habitual, se puede llegar a identificar a una persona mediante el olor, el tacto o el comportamiento. Y todo esto, y mucho más, lo realiza el cerebro con tal sencillez y velocidad, que lo hace pasar inapreciable.

Sin embargo, la expansión de las redes telemáticas y la proliferación de distintas soluciones en las que nunca se encuentran cara a cara dos personas, para que una de ellas identifique a la otra, complican de gran manera el proceso de identificación. Imaginemos el caso de un Cajero automático. En este caso, el cliente del sistema quiere obtener una cantidad de dinero, pero el propietario del Cajero, el Banco, tiene que estar seguro de que dicho dinero lo saca de la cuenta del cliente preciso y se lo entrega realmente al mismo cliente. Por tanto el Cajero tiene que realizar un proceso de identificación del usuario, en el que se asegure:

- un correcto funcionamiento del proceso;
- un cierto grado de seguridad frente al fraude.

Estas necesidades se plantean cada vez más en los nuevos sistemas que aparecen. Los sectores en los que se requiere una identificación electrónica (es decir, una identificación que debe ser realizada por una máquina), son muy variados. Desde sistemas de mínima seguridad, como puede ser la identificación del socio de un club de campo para reservar una pista de tenis, hasta la consulta de información sanitaria de un paciente. Sin embargo es el movimiento de dinero, y por tanto las aplicaciones bancarias y comerciales, las que suelen tomar mucho más protagonismo a la hora de plantear los esquemas de identificación a utilizar.

A lo largo de las últimas décadas, diversos sistemas se han propuesto para solucionar la identificación de forma electrónica, siendo los más representativos:

- Contraseñas: es el sistema típico de identificación en una red de ordenadores. El usuario introduce su «nombre» (identificador de usuario) y su contraseña. Una variación de este método es la utilización de teclados en un sistema de acceso, donde el usuario debe teclear su Número de Identificación Personal (Personal Identification Number - PIN). La gran ventaja de este método es la no necesidad de una inversión grande en infraestructura, de forma que se tenga que distribuir a los usuarios elementos de identificación. El inconveniente principal es la facilidad con la que las contraseñas pueden ser copiadas y, sobre todo, la imposibilidad de plantear un control del conocimiento de las mismas, sin perjudicar a los usuarios del sistema.

- Elementos de identificación: desde el Pasaporte o el DNI, hasta el uso de Tarjetas Inteligentes, pasando por cualquier otro tipo de elemento identificativo, las soluciones basadas en este tipo de elementos han sido ampliamente utilizadas. La evolución de esta solución ha ido, casi siempre, de mano de la evolución tecnológica conseguida. El inconveniente de esta técnica es la necesidad de distribuir a cada usuario un elemento de identificación y renovárselo con el tiempo, así como la posibilidad de robo y, en algunos casos, la falsificación. La ventaja es que, con la tecnología actual, se pueden plantear sistemas anti-fraude bastante robustos.

- Características biológicas o de comportamiento: es decir, emular al comportamiento humano. Como se verá más adelante, esta solución es la única que permite una verdadera identificación de la persona, sobre todo si se complementa con sistemas anti-fraude, tales como detección de elemento vivo. Los grandes inconvenientes de esta solución son: que la verificación se da en términos de probabilidad; que los algoritmos no se encuentran todavía maduros; y, que los sistemas resultantes suelen ser excesivamente caros.

Para complementar cada una de estas soluciones, se han desarrollado varias propuestas basadas en híbridos de ellas. El ejemplo típico es la tarjeta bancaria en la que hay que usar un PIN para poder acceder a las funciones del cajero. Otra de estas soluciones es la que se propone al final de este artículo, en la que se usan simultáneamente dos tecnologías actuales relacionadas con la seguridad: la Biometría y las Tarjetas Inteligentes.

IDENTIFICACIÓN BIOMÉTRICA

Según el Diccionario de la Real Academia Española, se define BIOMETRÍA como «Estudio mensurativo o estadístico de los fenómenos o procesos biológicos». Esta definición se hace más específica cuando se utiliza el término de Biometría dentro del campo de la Identificación de Personas. Se podría decir en este caso, que Biometría es la ciencia por la que se puede identificar a una persona basándose en sus características biofísicas o de comportamiento. Expuesto en forma de ejemplos, es la ciencia que consigue reconocer a una persona mediante una imagen de su rostro o mediante la impresión de su huella dactilar.

Como es lógico, la capacidad de identificación biométrica es algo innato en los seres vivos, ya que poseen la característica de reconocer a sus semejantes. Pero la Biometría como ciencia de estudio de la individualidad de las personas, nace seriamente a finales del siglo XIX. Es entonces cuando en Europa se extendió con gran éxito el sistema francés de Identificación Antropométrica de Bertillon, en el que se realizaban numerosas medidas del cuerpo de una persona. Fue precisamente un experto en este sistema, Sir Francis Galton, quien realizó a finales del siglo XIX estudios muy

detallados sobre la huella dactilar, estudiando su estabilidad, unicidad y morfología. Sus trabajos, complementados por los de Vucetich, Henry, Hershel y Faulds (cada uno de forma independiente), consiguieron que la identificación por huella fuera aceptada y se convirtiera en el método de identificación biométrica más utilizado por la policía mundial.

La evolución de la tecnología, así como la dificultad, en muchas ocasiones, de captar la huella de una persona y, por supuesto, el progreso por parte de los supuestos criminales de evitar su posible identificación mediante esos métodos, han empujado a pensar en nuevas vías de realizar la identificación biométrica, desarrollándose diversas soluciones alternativas, como las basadas en voz, rostro, etc.

ETAPAS EN UN SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA

Las técnicas de identificación biométrica son muy diversas, ya que cualquier elemento significativo de una persona es potencialmente utilizable como elemento de identificación biométrica. Las distintas técnicas que existen serán tratadas en el próximo apartado. Sin embargo, incluso con la diversidad de técnicas existentes, a la hora de desarrollar un sistema de identificación biométrica, se mantiene un esquema totalmente independiente de la técnica empleada. Los sistemas, tal y como se puede ver en la Figura 1, se basan en dos fases totalmente diferenciadas:

1. **Reclutamiento:** en esta fase, se toma una serie de muestras del usuario, y se procesan, para posteriormente extraer un patrón, el cual se almacenará y será el conjunto de datos que caracterizará a ese usuario. Si se captura más de una muestra, el patrón suele ser el resultado de una media de las características obtenidas. Este proceso se hace de forma supervisada, es decir, existe una persona encargada de controlar cómo se produce la captura de los datos, así como de asegurar la identidad de la persona que se está reclutando en el sistema. Además, se aprovecha esta fase para enseñar al usuario cómo funciona el sistema y aclararle todas las dudas que pudiera tener.

2. **Utilización:** una vez que se tiene almacenado el patrón del usuario, éste puede utilizar el sistema con normalidad, y sus características son comparadas con el patrón almacenado, determinando el éxito o fracaso de esa comparación.

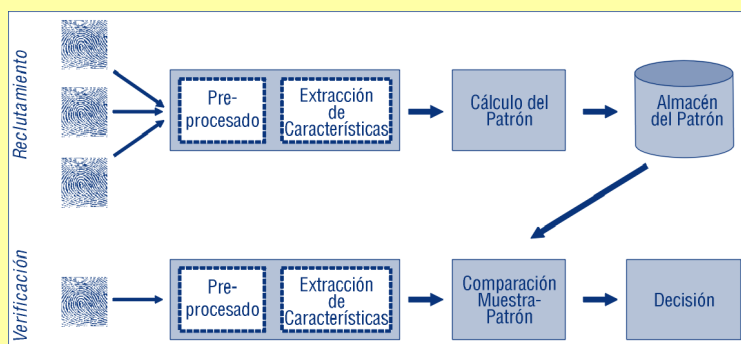


Figura 1: Etapas en un Sistema de Identificación Biométrica

Pero como se observa en la Figura 1, cada una de las fases mencionadas, está basada en una serie de bloques que hacen que las características biológicas o de comportamiento del individuo acaben siendo un elemento que lo identifique. Estas fases son:

- **Captura:** se toman los datos biofísicos o de comportamiento del sujeto. La toma de los datos depende, evidentemente, de la técnica biométrica empleada, pero también se pueden encontrar muchas variaciones para la misma técnica biométrica. Por ejemplo, la huella dactilar puede ser obtenida por cámara de video, ultrasonidos, efecto capacitivo sobre un semiconductor o exploración por láser.

- **Pre-procesado:** en este bloque se adecuan los datos capturados para facilitar el tratamiento que tiene que realizar el siguiente bloque. Este bloque se encarga, dependiendo de la técnica, de tareas como: reconocer el inicio de una frase y medir el ruido de fondo, hacer una extracción de bordes de la imagen capturada, localizar la muestra, rotarla y ampliarla (o reducirla) [Jai89], para que se encuentre entre los márgenes que reconoce el algoritmo siguiente, etc.

- **Extracción de Características:** se puede considerar el bloque

más significativo de la técnica a utilizar. Es el bloque en el que se fundamenta la capacidad del sistema de distinguir entre sujetos. Sin embargo, debido a distintas aproximaciones al problema, este bloque puede seguir orientaciones muy diversas, e incluso contradictorias, para la misma técnica, creándose distintos métodos dentro de una misma técnica. Por otro lado, en algunas ocasiones, el desconocimiento sobre las características que se deben extraer, lleva a utilizar técnicas basadas en Redes Neuronales, que mediante entrenamiento de las mismas, se intentan adecuar a los resultados esperados.

- **Comparación:** una vez extraídas las características de la muestra capturada, se han de comparar éstas con las previamente almacenadas, es decir, el patrón. Lo más importante que hay que dejar claro cuando se habla de este bloque, es que no se trata de una comparación binaria (o de igualdad), sino que la variación de las muestras, por variaciones en la captura o leve variación de las características de sujeto, hacen que la comparación dé como resultado una probabilidad de semejanza. Por tanto, para determinar el éxito o fracaso de la comparación, habrá que determinar un umbral en esa probabilidad. La comparación puede estar basada en cada una de las distintas posibilidades que ofrece la Teoría de Reconocimiento de Patrones [Dud73]: Métricas (como la Distancia Euclídea, Distancia de Mahalanobis o Distancia de Hamming), Estadísticas (utilizando funciones de distribución), o técnicas basadas en modelo de problemas (como Redes Neuronales, Modelos de Mezclas de Gaussianas, etc.)

Sobre los conceptos expuestos cabe hacer un par de puntualizaciones. La primera de ellas tiene que ver con la elección del umbral, ya que si éste se incrementa, hará que el sistema se relaje y permita una mayor probabilidad de accesos por parte de personas no autorizadas (Tasa de Falsa Aceptación, o FAR), mientras que si se disminuye, el sistema se volverá muy restrictivo, aumentando la probabilidad de rechazo de personas autorizadas (Tasa de Falso Rechazo, o FRR). Por lo tanto, la elección del umbral dependerá del grado de seguridad, y amigabilidad hacia el usuario, que se le quiera dar al sistema.

Por otro lado, el modo en el que se hace el reclutamiento no es tampoco trivial. En algunas técnicas basta una única toma de los datos, mientras que en otras puede ser necesario tomar varias muestras y en distintas sesiones (días o semanas), tal y como ocurre, por ejemplo, en los sistemas basados en voz. A todo esto habrá que añadir que si el reclutamiento resulta muy pesado, los usuarios del sistema tenderán a rechazar el sistema de identificación, por lo que habrá que buscar una solución de compromiso entre la comodidad del usuario, y la obtención de un patrón óptimo.

Hasta ahora se ha estado hablando siempre de Identificación Biométrica; sin embargo, la Identificación se puede realizar basándose en dos esquemas de funcionamiento del Sistema de Identificación Biométrica:

- **Reconocimiento:** también llamado, en algunos textos, simplemente Identificación (lo cual llega a causar cierta confusión). Se basa en identificar a un usuario dentro de todos los usuarios que ya se encuentran en el sistema. Por lo tanto, se comparan las características extraídas con los patrones de todos los usuarios reclutados por el sistema. Este esquema de funcionamiento, necesario para muchas aplicaciones, tiene como inconvenientes la necesidad de una Base de Datos de patrones (con los requisitos oportunos de capacidad de almacenamiento y seguridad de los datos) y la existencia de una red de comunicaciones, siempre on-line, que comunique los puestos de identificación con la Base de Datos. El resultado de la comparación puede ser: siempre positivo (es decir, se identifica siempre con el usuario que ha dado una probabilidad más alta), o puede indicar rechazos (si el usuario con la mayor probabilidad no supera un determinado umbral).

- **Autenticación:** también llamado sencillamente Verificación. Trata de responder a la pregunta: ¿es este sujeto la persona que dice ser? En este esquema de funcionamiento, el usuario, al que se le toman sus características biométricas, también comunica su identidad. El sistema se encarga, entonces, de comparar las características extraídas, con el patrón del usuario indicado. Si la comparación supera un determinado umbral de parecido, se considera que el usuario es el indicado, rechazando la comparación en caso contrario. El patrón del usuario puede estar almacenado en una Base de Datos, tal y como se hace en los sistemas de Reconocimiento, o, si el patrón es suficientemente pequeño, en un sistema portátil de información como puede ser una tarjeta. En este último caso no son necesarias ni la Base de Datos ni la red de comunicaciones de los sistemas de Reconocimiento.

TÉCNICAS BIOMÉTRICAS

Aunque las características de la huella dactilar son, sin lugar a duda, las más ampliamente utilizadas para realizar una identificación biométrica, cualquier otra característica biológica o del comportamiento de una persona puede ser usada para realizar la identificación, siempre que dichas características se demuestren propias y únicas de la persona a identificar. Las distintas técnicas que se están estudiando actualmente se pueden ver descritas en [Jai99], siendo:

- **Voz:** es una técnica con uno de los mayores potenciales comerciales: los servicios de atención telefónica personal, como la Banca Telefónica. Es una técnica que se lleva estudiando durante varias décadas, existiendo innumerables métodos para realizar, tanto la extracción de características, como la comparación [Dod85]. Algunos métodos son dependientes del texto pronunciado (es decir, todo o parte del texto que se recita debe ser idéntico en todas las ocasiones), mientras otros son independientes del mismo (pudiéndose recitar cualquier locución para realizar la identificación). Desgraciadamente no están todavía determinados todos los factores que influyen en las locuciones, tales como la edad, las enfermedades, el comportamiento, el estado de ánimo, el canal, etc. Diversos estudios están logrando minimizar los efectos de algunos de esos factores, pero todavía queda mucho camino por andar.

- **Huella Dactilar:** tal y como ya se ha comentado, es, sin lugar a duda, la más estudiada y probada. Existen numerosos estudios científicos que avalan la unicidad de la huella de una persona y, lo que es más importante, la estabilidad con el tiempo, la edad, etc. En estos aspectos es una técnica que le lleva mucha ventaja a las demás, debido a su siglo de existencia. Su captura recibe diversas formas, sobre todo últimamente, debido a la innovación tecnológica. En cuanto a la extracción de características, existen principalmente tres filosofías [Jan99]: la correlación de imágenes, la extracción y comparación de minucias (uniones y terminaciones de los surcos de la huella), y la extracción y comparación de los poros del dedo.

- **Rostro:** el método de identificación que nuestro cerebro usa más a menudo y de una forma más sencilla. En la actualidad existen muchos grupos de investigación trabajando en esta técnica con diversos métodos (estudios morfológicos, transformadas multiresolución, etc.). Los resultados que se están consiguiendo son bastante prometedores, aunque le falta todavía bastante hasta llegar al nivel de otras técnicas [Jan99]. El gran inconveniente encontrado es la variabilidad del rostro del sujeto a lo largo del tiempo: gafas, barba, longitud del pelo, peinado, expresiones, etc.

- **Iris:** esta técnica fue impulsada por John G. Daugman en 1993, tal y como se muestra en [Dau93]. Los resultados obtenidos son, sin lugar a dudas, unos de los mejores de la actualidad [San99b, San99c], teniendo en cuenta que las características en las que está basada, el patrón de la textura del iris ocular, permanece inalterable durante la vida del sujeto debido a la protección que le proporciona la córnea. Por otro lado, los estudios sobre la unicidad de sus características, la han colocado muy por encima de la huella dactilar. Su gran inconveniente es el coste de los equipos, aunque teniendo en cuenta el grado de fiabilidad alcanzado, existen numerosas aplicaciones de alta seguridad que podrían usar esta técnica.

- **Oreja:** desde un punto de vista forense, se ha demostrado que la oreja de un individuo posee muchas características propias del mismo. Es una técnica de estudio muy reciente y su gran inconveniente es la necesidad de que el usuario descubra su oreja frente a una cámara, lo cual puede ser incómodo en el caso de personas con el pelo largo, o de determinados condicionantes sociales, de educación, religiosos, etc.

- **Andadura:** o modo particular en el que una persona camina. Es una técnica basada en características del comportamiento, por lo que es muy susceptible de ser falseada por imitaciones. Su estudio se encuentra en la actualidad en pleno desarrollo.

- **Dinámica de Teclado:** se basa en reconocer a una persona por la forma en que escribe a máquina. Se mantiene la hipótesis de que el ritmo de teclado es característico de una persona, y prototipos existentes parecen reafirmar esa hipótesis. Sin embargo, además de ser una técnica basada en el comportamiento, y por tanto potencialmente emulable, tiene la limitación de no poder ser utilizada con usuarios que no tienen facilidad a la hora de escribir a máquina.

- **DNA:** sin lugar a dudas, la única técnica capaz de identificar unívocamente a una persona. Su potencia en el campo de la identificación choca con la dificultad en el desarrollo de sistemas automáticos de identificación en tiempo real y cómodos para el usuario. Los últimos intentos tratan de tomar la muestra mediante captación del sudor del sujeto. Sin embargo habría que estudiar la reacción de los usuarios frente a ese modo de captar la muestra.

- **Firma:** utilizada desde más antiguo que la huella dactilar, esta técnica siempre se ha visto entredicha por la posibilidad de falsificaciones, debido a que se está basada en características del comportamiento. Las nuevas tecnologías facilitan realizar, no sólo el estudio de la firma ya realizada, sino también el estudio del acto de firmar, captando mediante un bolígrafo especial o una tableta gráfica, parámetros como velocidad, paradas, posición del bolígrafo, fuerzas, etc. en el mismo acto de firmar. Existen diversos prototipos y algunos productos comerciales, pero






Técnica	Ventajas	Inconvenientes
Voz	 <ul style="list-style-type: none"> - Muy bajo coste - En algunas aplicaciones puede resultar inapreciable al usuario (p.e., servicios telefónicos) 	<ul style="list-style-type: none"> - Rendimiento bajo - Se está estudiando el aumentar la unicidad y estabilidad
Huella	 <ul style="list-style-type: none"> - Muy estudiado/desarrollado - Unicidad, estabilidad y rendimiento altos - Reconocimiento legal - Medio coste 	<ul style="list-style-type: none"> - Connotaciones «policiales» para el usuario - Detección de dedo vivo depende de pruebas colaterales a la captura
Iris	 <ul style="list-style-type: none"> - Unicidad mayor que huella - Gran estabilidad por protección de la córnea - FAR prácticamente nula - Fácil detección de ojo vivo 	<ul style="list-style-type: none"> - Alto coste - Inicialmente incómodo para el usuario
Mano	 <ul style="list-style-type: none"> - Fácil uso y gran aceptación por el usuario - Medio coste - Bajo coste computacional - Sin connotación «policial» 	<ul style="list-style-type: none"> - Unicidad y estabilidad no probadas en grandes poblaciones - Detección de mano viva depende de pruebas colaterales
Rostro	 <ul style="list-style-type: none"> - Cómodo, e incluso inapreciable, para el usuario - Medio coste 	<ul style="list-style-type: none"> - Sensible a cambios del sujeto (barba, gafas, pelo, ...) - Todavía en investigación y desarrollo

Tabla 1: Comparativa entre las técnicas más importantes

su éxito comercial ha resultado relativamente decepcionante.

- **Olor:** técnica muy reciente, se basa en reconocer a una persona a través de su olor corporal. Las grandes incógnitas se encuentran en ver el rendimiento de este tipo de técnica frente a perfumes, colonias, olores ambientales, contactos con otras personas, etc.

- **Exploración de la Retina:** se ha demostrado que el patrón de los vasos sanguíneos de la retina presenta una mayor unicidad que el patrón del iris. Además, la casi imposible modificación de ese patrón, así como la facilidad para la detección de sujeto vivo, la hacen ser considerada la técnica más segura. Sin embargo, la forma de hacer la exploración, mediante láser, provoca un rechazo casi total por parte de los usuarios, estando sólo indicada para entornos de extrema seguridad, donde los usuarios son pocos y conscientes del grado de seguridad necesario.

- **Geometría del Contorno de la Mano y/o del Dedo:** se trata de una técnica en la que se estudian diversos parámetros morfológicos de la mano (o el dedo) del usuario, tales como anchuras, alturas, etc [San99a, San99c]. La técnica basada en geometría del dedo se puede considerar como una simplificación de la basada en contorno de la Mano. El gran atractivo de esta técnica, debido a su simplicidad, bajo coste y mínimo tamaño del patrón, la han convertido en la técnica con mayor éxito comercial en el último par de años.

Todas y cada una de estas técnicas tienen sus partidarios y sus detractores. Sin embargo, lejos de lo que piensan unos y otros, se puede afirmar que no existe la técnica única, perfecta e ideal que se pueda utilizar siempre. Cada técnica tiene sus ventajas y

sus inconvenientes que hace que técnicas que ofrecen unos resultados excelentes, no puedan ser usadas en muchos entornos debido al rechazo de los usuarios o, simplemente, al coste. Por otro lado, técnicas que ofrecen un nivel de seguridad inferior, por otras razones pueden ser más fácilmente empleadas en determinados entornos, al ser más importantes las ventajas que proporcionan.

A la hora de juzgar una técnica biométrica, son muchos los parámetros que hay que considerar, de los que se pueden destacar los siguientes:

- Universalidad: si las características se pueden extraer de cualquier usuario o no.
- Unicidad: la probabilidad de que no existan dos sujetos con las mismas características.
- Estabilidad: si las características que se extraen permanecen inalterables en relación con diversos parámetros (tiempo, edad, enfermedades, etc.).
- Facilidad de captura: si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto.
- Rendimiento: o tasas de acierto y error.
- Aceptación por los usuarios
- Robustez frente a la burla del sistema: si la técnica puede reconocer el falseamiento de los datos capturados (uso de fotos, dedos de latex, etc.).
- Coste

Por tanto, para cada situación y entorno, con un determinado requisito de seguridad, habría que seleccionar la técnica óptima para unos buenos resultados en el funcionamiento del sistema de identificación. Una comparativa sobre los sistemas más aceptados actualmente se puede encontrar en la Tabla I.

LA BIOMETRÍA Y LAS TARJETAS INTELIGENTES

IV

En los sistemas de Autenticación Biométrica, es decir, aquellos en los que las características biométricas extraídas han de verificarse sólo frente al patrón del usuario, es necesario habilitar un sistema para comunicar la identidad del usuario. Ese sistema ha sido, tradicionalmente, el uso de una tarjeta de identificación como, por ejemplo, una tarjeta de banda magnética.

Por otra parte, para evitar la necesidad de utilizar una red de comunicaciones entre una base de datos central (donde se encuentran los patrones de todos los usuarios) y los terminales donde se va a producir la verificación, se ha buscado la forma en la que el patrón pudiera ser transportado por el propio usuario. Debido a la limitada capacidad de almacenamiento de las tarjetas de banda magnética (unos 250 caracteres), se han tenido que buscar nuevas soluciones. Dentro de las soluciones posibles, se encuentran las Tarjetas Láser (también denominadas Ópticas) o las Tarjetas Inteligentes.

Ambas soluciones poseen capacidad suficiente como para almacenar el patrón del usuario para casi cualquier técnica biométrica existente (2-32 KB para las Tarjetas Inteligentes; 2-4 MB para las Tarjetas Láser). Sin embargo, mientras que las Tarjetas Láser son unos dispositivos pasivos de almacenamiento de la información (la información va grabada en la superficie de la tarjeta, sin ninguna protección salvo el cifrado de dicha información, por lo que son susceptibles de copia), las Tarjetas Inteligentes son dispositivos activos de almacenamiento de información, incorporando mecanismos para proteger el acceso a la información mediante claves, algoritmos de cifrado, etc [Zor94, IS7816] .

Pero, además, como las Tarjetas Inteligentes están basadas en un microprocesador y un Sistema Operativo que controla todo el flujo de información, cabría la posibilidad de incorporar a este tipo de tarjetas nuevas funcionalidades. De esta forma, para un sistema de Autenticación Biométrica, una Tarjeta Inteligente se podría utilizar como:

- Dispositivo seguro que almacena la identidad del usuario, así como su patrón, sólo dejando leer el patrón por parte del terminal que tiene permiso para ello. Además, la tarjeta, para garantizar la confidencialidad del patrón, puede transmitir el patrón cifrado mediante una clave de sesión, incrementando, por tanto, la seguridad del sistema.

- Además de lo anterior, cabría la posibilidad de pensar en utilizar la Verificación Biométrica como otro sistema más de seguridad dentro de la Tarjeta Inteligente (tal y como se usa, por ejemplo, el PIN). De esta forma, se podría proteger de forma biométrica, no sólo la información almacenada dentro de la tarjeta, sino también determinadas operaciones como, por ejemplo, el débito de un monedero electrónico.

Esta última posibilidad implicaría la fabricación de una nueva máscara de Sistema Operativo para Tarjeta Inteligente, lo que supone una inversión muy elevada y cuya amortización tiene que ser muy cuidadosamente estudiada. Para llevar a cabo la viabilidad de esta última propuesta habría que considerar los siguientes factores:

1. Escoger una técnica biométrica que hubiese demostrado exitosamente su rendimiento y aceptación por los usuarios.
2. Escoger un método de verificación válido para dicha técnica y cuyos tiempos de ejecución en un microprocesador típico para una Tarjeta Inteligente fuesen suficientemente bajos.
3. Promover la normalización de dicha técnica biométrica, del método escogido y, como más importante, la estructura del patrón y de los vectores de características.

Teniendo en cuenta la dificultad de los dos primeros puntos, sobre todo el primero, y la lentitud en los procesos de normalización, se hace muy difícil que las grandes empresas del sector se decidan a abordar este tipo de innovación tecnológica. Sin embargo, la innovación en otros campos, como puede ser el desarrollo de Sistemas Operativos Abiertos para Tarjetas Inteligentes, abren una puerta a la esperanza, ya que pueden facilitar el desarrollo de nuevos proyectos, sin suponer el excesivo gasto derivado de un proceso de creación de una nueva máscara de Sistema Operativo. Tendremos que esperar un tiempo para descubrir si la posibilidad de realizar la Autenticación Biométrica dentro de una Tarjeta Inteligente se vuelve una realidad.

Agradecimientos

El autor quiere agradecer a D. José Antonio Martín Pereda, D^a. Carmen Sánchez Ávila y D^a. Ana Pilar González Marcos, su inestimable ayuda a la hora de realizar los trabajos que se recogen en este artículo.

Estos trabajos han sido posibles gracias a la financiación del Plan Nacional de I+D, bajo el proyecto titulado «Transacciones Seguras a través de Internet: Autenticación Biométrica de Usuarios», y cuyo código es TIC98-1195.

✍ Raúl Sánchez Reillo
 Grupo Universitario de Tarjeta Inteligente
 Dpto. Tecnología Fotónica
 E.T.S.I. Telecomunicación (U.P.M.)
 reillo@tfo.upm.es

REFERENCIAS

- [Dau93] J. G. Daugman. «High Confidence Visual Recognition of Persons by a Test of Statistical Independence». IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, nº 11. Noviembre 1993. pp. 1148-1161.
- [Dod85] G. R. Doddington. «Speaker Recognition - Identifying People by their Voices» Proceedings of the IEEE, vol. 73, nº 11, pp. 1651-1664, Nov. 1985.
- [Dud73] R. O. Duda, P. E. Hart. *Pattern Classification and Scene Analysis*. John Wiley & Sons. 1973
- [IS7816] Normativa internacional ISO/IEC 7816. *Identification Cards - Integrated circuit(s) cards with contacts*. Partes 1-10. Desde 1987 hasta 1999.
- [Jai89] A. K. Jain. *Fundamentals of Digital Image Processing*. Prentice Hall, 1989.
- [Jai99] A. K. Jain, R. Bolle, S. Pankanti, et al. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers. EE.UU. 1999.
- [Jan99] L.C. Jain, U. Halici, I. Hayashi, S. B. Lee, S. Tsutsui, et al. *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. CRC Press LLC. 1999.
- [San99a] R. Sanchez-Reillo, A. Gonzalez-Marcos. «Access Control System with Hand Geometry Verification and Smart Cards». Proc. 33rd Annual 1999 International Carnahan Conference on Security Technology. Madrid, 5-7 Octubre, 1999. pp. 485-487.
- [San99b] R. Sanchez-Reillo, C. Sanchez-Avila, J.A. Martin-Pereda. «Minimal Template Size for Iris-Recognition». Proc. of the First Joint BMES/EMBS Conference. Atlanta (EE.UU.), 13-16 Octubre, 1999. p. 972
- [San99c] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos. «Multiresolution Analysis and Geometric Measure for Biometric Identification». *Secure Networking - CORE [Secure]'99*. Noviembre/Diciembre, 1999. Lecture Notes in Computer Science 1740, pp. 251-258. Springer-Verlag.
- [Zor94] J. L. Zoreda, J. M. Otón. *Smart Cards*. Artech House. 1994.