

La identificación de personas mediante la huella dactilar es una técnica que cuenta ya con casi un siglo de antigüedad. Su amplio reconocimiento, como técnica válida, por los sistemas legales de la mayoría de los países del mundo, y su amplia experiencia, impulsaron hace muchos años a que se desarrollaran sistemas que permitiesen la identificación de las personas de forma automática. En el pasado, tanto el volumen como el coste de los sistemas de captura de las huellas, así como el coste computacional involucrado, ha llevado a que su implantación masiva no pudiera ser efectiva. Sin embargo, la evolución tecnológica puede permitir que esa implantación llegue a ser una realidad.

Verificación automática de personas mediante huella dactilar

INTRODUCCIÓN

De entre todas las técnicas de identificación biométrica existentes en la actualidad [1], la más ampliamente utilizada es la basada en la huella dactilar del usuario. Esta técnica se remonta a finales del siglo XVII, aunque hay estudios que exponen la posibilidad de que el ser humano conociera la capacidad de identificación de las huellas incluso en la época de los Egipcios [2].

Pero aunque a finales del siglo XVII estudiosos como Nehemiah Grew o William de Orange, estudiaron la estructura de la huella dactilar, los fundamentos de lo que hoy es considerado como métodos de identificación por huella no se establecerían hasta finales del siglo XIX. Fue en esa época cuando Sir Edward Henry y Sir Francis Galton, de forma separada, trabajaron en la aplicabilidad de la huella dactilar para realizar identificación de personas mediante clasificación.

En estos estudios se formalizó la descripción de la huella dactilar, como una sucesión de crestas, separadas entre sí por valles. El flujo de las crestas sufre una serie de puntos singulares, tales como terminaciones y/o bifurcaciones. A estos puntos singulares se les denominó minucias, y mediante su tipo, localización y orientación, se puede llegar a identificar a una persona. Cabe comentar que diversos autores clasifican las minucias en un número elevado de tipos (normalmente 8), pero todos estos tipos pueden ser considerados como combinaciones de terminaciones y bifurcaciones.

Estudios realizados por el Dr. Henry Faulds a finales del s. XIX, pusieron de manifiesto que la estructura de la huella no es propia de la capa más externa de la piel, sino que es intrínseca a la dermis. Esto provoca que si una persona pierde la piel de un dedo, al volver a crecer la piel se vuelve a reconstituir la huella. Además, posteriormente se comprobó que el grado de unicidad de la huella era muy alto, ya que no

se encontraban dos personas con las mismas huellas. De hecho, cada uno de los dedos de un mismo sujeto presentan huellas totalmente distintas.

Además de las minucias, existen otros puntos singulares que pueden servir para la identificación de personas. En concreto, el núcleo, o core, y el/los deltas de una huella son muy utilizados para realizar clasificación de huellas, y poder facilitar la búsqueda en grandes bases de datos. El núcleo se podría definir como el punto donde la orientación de las crestas tiende a converger, mientras que los deltas son los puntos donde el flujo de las crestas presenta una divergencia.

Todos los estudios realizados empujaron a considerar esta técnica como evidencia desde el punto de vista legal y, especialmente a ser utilizada, a principios del siglo XX, por la policía de diversos países para identificar a criminales.

Anteriormente a la huella se utilizaba el sistema de Bertillon, que no era otra cosa que realizar a los criminales una sucesión de medidas de todo su cuerpo (cara, brazos, pecho, etc.). El sistema basado en huella dactilar tomó tal importancia, que muy poco tiempo después fue aceptado por la gran mayoría de sistemas policiales en el mundo, creándose grandes bases de datos de fichas de huellas dactilares.

El tamaño de esas bases de datos llevó a que no sólo se impulsara el conocimiento sobre las minucias sino que también se pusiese muchos recursos en desarrollar sistemas que pudieran clasificar las huellas de forma eficiente, para que su búsqueda dentro de una base de datos fuese lo más rápida y exacta posible. Por lo tanto, si se revisa la literatura existente sobre huellas (que en la actualidad es muy amplia), aparecen, casi totalmente diferenciados, los siguientes campos de aplicación:

- Clasificación de huellas
- Identificación de un sujeto mediante su huella

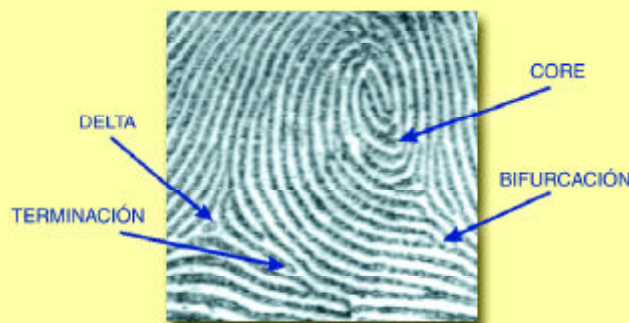


Figura 1: Estructura de la huella y tipos de minucias

- Obtención de huellas dactilares latentes, es decir, obtener las huellas en la escena del crimen

En este artículo, el estudio va a estar basado en los Sistemas Automáticos de Identificación de un sujeto mediante su huella dactilar. Para ello se estudiarán las distintas fases de que se puede componer cualquier sistema de identificación biométrica [3]. Primero se tratará la captura de la huella, es decir, el método de poder tomar una imagen electrónica de la huella de un usuario. Una vez obtenida esa imagen, habrá que procesarla para extraer sus características, formando lo que se denomina vector de características, que se utilizará para compararlo con un patrón del usuario previamente grabado, es decir, realizar la verificación de la huella. Como en todo sistema biométrico, esa comparación dará un porcentaje de éxito, que, dependiendo del umbral especificado para la aplicación particular, provocará la aceptación o el rechazo del usuario.

MÉTODOS DE CAPTURA

Cuando se quiere desarrollar un sistema automático de identificación de personas mediante huella dactilar, es preciso disponer de algún mecanismo para capturar una imagen de la huella del usuario de forma automática, fiable y sencilla. Este ha sido uno de los puntos donde esta técnica ha planteado, durante años, muchos inconvenientes. Éstos han venido tanto por el coste, como por el tamaño de los métodos ópticos de captura de la imagen, los cuales, además, requerían un excesivo mantenimiento.

Debido a que el resto de las partes del sistema de identificación por huella (extracción de características y verificación), estaban ofreciendo resultados más que satisfactorios, la industria del sector impulsó investigaciones que conllevaran a nuevos métodos de captura. Todo esto ha

llevado a que en los últimos años esta técnica haya vivido una auténtica revolución, consiguiendo llegar a mercados donde antes no encontraba cabida, ya que los sensores que se han obtenido son mucho más económicos y drásticamente inferiores en tamaño. Las estrategias seguidas para los nuevos sensores han sido de lo más variado: diferencia de temperatura cuando la piel toca el sensor, efecto capacitivo de la piel, efecto Doppler en el eco de señales de ultrasonidos, etc.

Además, para reducir el tamaño y coste de los sensores, se han desarrollado sistemas en los que no hay que posar todo el dedo, sino deslizarlo longitudinalmente por el sensor, capturando, en cada instante, una línea de la imagen y haciendo la unión de todas esas líneas para formar la imagen.

Con todo esto, se han conseguido sensores que pueden ser fácilmente integrados en todo tipo de dispositivos, desde teclados o ratones en PCs, hasta teléfonos móviles, y con costes muy inferiores a sus antecesores. Además, la imagen obtenida es de una alta calidad, siendo típicas las resoluciones de 500ppp. La diferencia entre cada una de las tecnologías puede llegar a la hora de ver su comportamiento frente a situaciones adversas (dedos muy secos, dedos muy húme-

dos, huellas desgastadas, detección de dedo vivo, etc.). En este punto sería aconsejable realizar un análisis serio, por una entidad independiente, ya que hasta la fecha lo único que se tiene es la descripción de las bondades de cada uno de los fabricantes de una tecnología, comentando las deficiencias de las demás.

EXTRACCIÓN DE CARACTERÍSTICAS

Tal y como ocurre con casi todas las técnicas biométricas, y especialmente en aquellas que llevan mucho tiempo en investigación, el número y variedad de algoritmos matemáticos para realizar cualquiera de los procesos involucrados en el sistema, es enorme [4]. En este caso se van a comentar los dos que más éxito tienen dentro del mundo científico y de investigación.

Por un lado se va a hablar de cómo se extraen características siguiendo la metodología expuesta por Anil K. Jain (sin duda uno de los mayores investigadores en el campo de la huella dactilar, y una obligada referencia). En este caso, la extracción de características va a consistir en una serie de procesamiento sucesivos de la imagen completa de la huella, a la que se le aplican numerosas operaciones.

Por otro lado vamos a exponer el algoritmo diseñado por Dario Maio y Davide Maltoni, de la Universidad de Bolonia.

En este caso se trata de un algoritmo que realiza un seguimiento de cada una de las crestas a lo largo de la imagen, por lo que el procesamiento de la imagen sólo se hace un par de veces, reduciendo su coste computacional.

Pero ambos procesos requieren de un preprocesado previo de la imagen de la huella dactilar. Este preprocesado, común para los dos algoritmos, depende en gran medida del resultado de la huella capturada por el dispositivo concreto, y del grado de tolerancia al movimiento que se le quiera dar

al usuario final. En concreto, este pre-procesado está compuesto de los siguientes pasos [2][5][6] :

1. Localización y segmentación de la huella : en la imagen capturada, no sólo habrá huella, sino que también pueden haber partes de la imagen que no contengan información sobre la misma (ya sea porque el área designada por el dispositivo sea mayor que el tamaño del dedo, o por la incorrecta colocación del dedo en el sensor. Se analizará dónde se encuentra la huella (localización), y se tomará de ella aquella área que sea fuente de estudio, eliminándose todo lo demás (segmentación). Si la zona segmentada no cumple unas determinadas características (como por ejemplo, tamaño inferior a uno dedo), el sistema puede rechazar dicha huella, indicándose al usuario, y evitando de esta forma realizar todo el cálculo restante.

2. Enfatización de la huella : se hace una ecualización de los niveles de grises de la huella, de forma que se pueda aprovechar mucho mejor, la diferencia de tonalidades entre unos puntos y otros, y además, poder equiparar las zonas donde se ha realizado menor presión del dedo (más claras en la imagen), con las zonas de más presión (más oscuras).

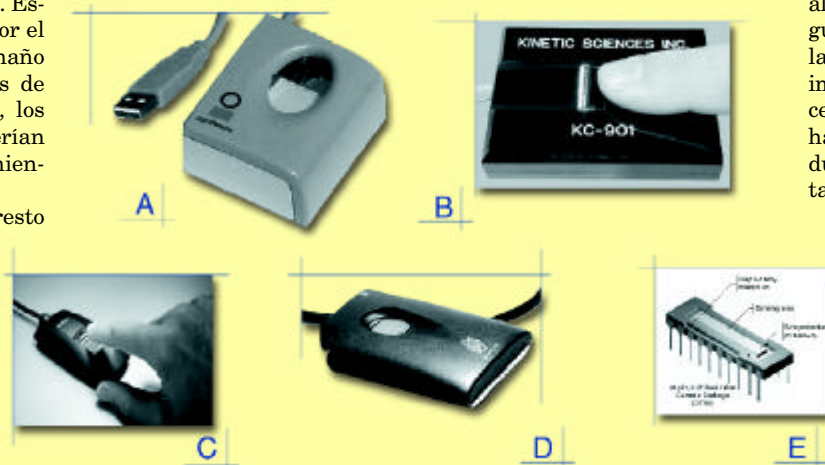


Figura 2: Distintos sistemas de captura de huellas. A) Sistema óptico de UareU; B) Sistema óptico por deslizamiento de dedo de Kinetic Sci. Inc.; C) Sensor de estado sólido de Veridicom; D) Lector de tarjetas inteligentes con Sensor capacitivo de huella (GemPCTouch 440) de Gemplus; E) Chip sensor térmico de huella de Atmel.

3. Cálculo del mapa de orientación : con la imagen resultante de los dos pasos anteriores, se hace un estudio de gradiente a baja escala, para poder obtener, de una forma aproximada, la orientación que tienen las crestas, en cada zona de la imagen. Para ello se hace el estudio en sub-ímagenes, tomando porciones disjuntas de la imagen anteriormente obtenida. Esta información servirá de ayuda para los algoritmos de extracción de características. En algunos sistemas, este paso se hace al principio, para ser utilizado en la segmentación, y luego se vuelve a calcular con imagen obtenida tras la ecualización.

Multiprocesado de la Imagen (Anil K. Jain)

Como se ha comentado, con este algoritmo, detallado en multitud de artículos publicados por Jain [2][5][7], se obtienen las minucias después de todo un procesado sucesivo de la imagen resultante del pre-procesado. Este proceso se divide en los siguientes pasos:

1. Detección de las crestas : una vez que se ha localizado y enfatizado la huella, se intentan localizar las crestas, para separarlas de los valles. En concreto se trata de un proceso de binarización, es decir, de reducir la imagen de 256 niveles de grises, a una imagen de sólo blanco y negro. Los métodos para poder conseguir esta binarización son muchos, desde el uso de umbrales globales o adaptativos (que ofrece resultados pobres si se tienen que procesar imágenes con una densidad de ruido alta), hasta la utilización de la propiedad de que una cresta es aquel punto que obtiene un mínimo local en la dirección perpendicular a su campo de orientación (que como veremos, es parte de la técnica utilizada por Maio).

2. Esqueletización: dependiendo del método de detección de crestas utilizado, será necesario realizar un “adelgazamiento” de los tramos que representan las crestas, es decir, hacer que estas crestas estén representadas por líneas de un único píxel de grosor. A este proceso se le denomina esqueletización, y se suele realizar fijándose en cada uno de los píxeles de la imagen, y dependiendo del número de píxeles puestos a 0 (si el 0 representa cresta) que le rodean (es decir, sus vecinos), eliminar parte de ellos. Este estudio se hace una y otra vez, hasta alcanzar el esqueleto de la huella.

3. Detección de minucias : con la imagen esqueletizada, se realiza un proceso de búsqueda de las “potenciales” minucias dentro de la imagen. Dicho proceso está basado en localizar aquellos píxeles puestos a 0 en la imagen, que tienen un solo vecino, o más de dos, siendo el primer caso el de una terminación, y el segundo, el de una bifurcación.

4. Eliminación de artefactos : en el paso anterior, se ha conseguido un conjunto de puntos que pueden ser minucias, pero muchos de ellos no lo serán, ya que estarán formados por artefactos de la imagen. Por lo tanto, se vuelve a procesar la imagen (post-procesado), para determinar si cada uno de los puntos anteriormente detectados, puede ser considerado realmente una minucia o no.

Como se puede ver, este algoritmo realiza una serie grande de procesados de la misma huella, por lo que su coste computacional es muy elevado.

Seguimiento de Crestas (Dario Maio y Davide Maltoni)

Para intentar evitar ese excesivo coste computacional, los profesores de la Universidad de Bolonia, Maio y Maltoni, analizaron la posibilidad de realizar todas las tareas anteriormente descritas, con un único procesado de la imagen (o como mucho dos), intentado equiparar el algoritmo a lo que la mente humana hace. La filosofía de este método es muy sencilla, y en lenguaje coloquial, el algoritmo se puede describir de la siguiente forma [4][8]:

1. Determinación de puntos de inicio : la imagen de la huella se cuadrícula, estableciendo una serie de puntos, a

partir de los cuales se iniciará el proceso. Simplemente es decidir cada cuántos píxeles se va a considerar que puede haber una cresta nueva. Es un parámetro del algoritmo y, por tanto, una decisión del diseñador del mismo.

2. Búsqueda de una cresta : tomando un punto de inicio, se busca, en la normal al campo de orientación un mínimo local, que determine dónde se encuentra una cresta (como ya se ha comentado antes, esta es la técnica que muy recientemente ha decidido recomendar Jain, para la detección de crestas).

3. Seguimiento de la cresta hacia la derecha : partiendo de la cresta, se va siguiendo la trayectoria de la cresta. Esto se realiza dando pequeños saltos, en la dirección dada por el campo de orientación para ese punto, y posteriormente, volver a buscar el mínimo local en el nuevo punto, para volver a reubicar la cresta. Si en el punto al que se ha saltado no se localiza una huella, se ha detectado una minucia (terminación). Si, en lugar de eso, chocamos con una cresta que ya hemos estudiado anteriormente, tenemos otra minucia (bifurcación). Si no se produce ninguno de esos casos, seguimos dando saltos, hasta que ocurra uno de estos casos o se acabe la imagen.

4. Seguimiento de la cresta hacia la izquierda : desde el punto de inicio (mejor dicho, la cresta detectada cerca de éste), se realiza el mismo proceso que en el paso anterior, pero en lugar de ir hacia la derecha, siguiendo la cresta, se hace en sentido contrario.

5. Determinación del siguiente punto de inicio : una vez terminada de procesar la cresta, tanto para la derecha como para la izquierda, se escoge un nuevo punto de inicio en la imagen, para seguir nuevas crestas. Evidentemente, este punto se escogerá como el siguiente, que no se encuentre dentro de una zona ya estudiada. Y una vez teniendo el nuevo punto, se vuelve al paso 2. Y así hasta que se acaben los puntos de inicio.

6. Eliminación de redundancias: una vez procesada toda la imagen, se obtendrá un conjunto de minucias, dentro de las cuales se pueden encontrar muchas idénticas (por repetición de situaciones en el algoritmo). Por lo tanto se hace una depuración de las minucias extraídas, para eliminar las no interesantes.

Como se puede apreciar, este algoritmo es muy parecido a la forma que puede trabajar nuestro cerebro, si nosotros queremos hacer una búsqueda sistemática de las minucias en la imagen.

VERIFICACIÓN DE LAS HUELLAS

Una vez que se han obtenido las minucias, se crea con ellas (con su localización, tipo, orientación, etc.), un vector, que servirá para identificar al usuario. De la extracción previa de las huellas del usuario, se creará un vector de características que será utilizado como patrón del usuario, y será la referencia para su comparación con las muestras que se obtengan cada vez que el usuario quiera identificarse.

La comparación de dicho patrón con la muestra, es una de las tareas más críticas de todo el proceso de identificación. La problemática viene dada por:

- En las huellas no se dispone de ningún punto de referencia válido universalmente, es decir, un punto a partir del cual se pueda llegar a tomar medidas, y que dicho punto sea válido para todas las huellas. En otras técnicas se tiene un punto claro (el centro de la pupila en el caso de la técnica de reconocimiento por iris [9]). Esta falta de referencia, hace que muchos métodos de comparación propuestos, no sean factibles. Algunos autores intentan utilizar como punto de referencia el core, pero su localización exacta no es sencilla, y además, en algunas huellas no se obtiene ese punto singular.

- La elasticidad del dedo hace que, dependiendo de la

postura del dedo y de la presión realizada, se tenga una variabilidad en las medidas de un mismo usuario, que haga bastante difícil la comparación de las huellas obtenidas. De hecho, el problema puede llegar a ser más grave, ya que, dependiendo del grado de rotación que se haya dado al dedo, pueden llegar a capturarse un elevado número de minucias en la muestra, que no se encuentran consideradas en el patrón.

De todos los algoritmos que se han llegado a proponer existe una tendencia generalizada a utilizar el algoritmo de comparación elástica de A. K. Jain [2][7]. Este algoritmo comienza con la búsqueda de una minucia de referencia. Esto se realiza analizando tanto el vector resultante de la muestra, como el del patrón, de forma que se pueda obtener una minucia cuya semejanza entre los dos vectores sea tan alta, que pueda ser considerada como idéntica.

Posteriormente se hace un cambio de coordenadas de los dos vectores, para pasarlo a polares (radio y ángulo), con el centro en esa minucia de referencia. Una vez realizado esto, se comparan, uno a uno, todos los pares de minucias susceptibles de estar en el mismo sitio. Para considerar que están en el mismo sitio, se crea un área de influencia de cada minucia del patrón, que permita la tolerancia dada por la elasticidad del dedo. Si la minucia de la muestra está en la zona de influencia de la minucia del patrón, y su tipo y orientación son compatibles, entonces se podrá determinar que la minucia es la misma.

Realizando esto para todos los pares de minucias, y aplicando unas fórmulas de medida de proximidad, con factores de penalización para los casos en los que la comparativa haya sido infructuosa, se consigue un resultado numérico que dará la probabilidad de que las huellas sean idénticas.

Como en todo sistema biométrico, dependiendo del umbral que ponga el diseñador del sistema, la probabilidad hará que la huella sí que se considere idéntica (aceptando al usuario), o falsa (rechazándolo). Se estudiarán entonces las posibles tasas de error: Falsa Aceptación (FAR) o Falso Rechazo (FRR), para indicar la calidad del sistema de identificación en la aplicación dada.

ÚLTIMAS TENDENCIAS

La gran madurez de esta técnica biométrica, con casi un siglo de experiencia, y, sobre todo, la drástica mejora de los sistemas de captura, han llevado a que en la actualidad se proponga esta técnica biométrica para multitud de aplicaciones. La idea fundamental es intentar evitar que una persona tenga que recordar varios números de identificación (PIN), a la hora de utilizar un Sistema de Información. Por tanto, toda aplicación con sistema de verificación, está siendo susceptible de aceptar la huella dactilar como método de autenticación de los usuarios.

En esta línea, la telefonía móvil está interesada en poder sustituir el PIN del teléfono, y los códigos de validación de operaciones (por ejemplo, una compra), por la verificación de la huella dactilar. De la misma forma, el acceso a redes de datos o a terminales, está cada vez más sujeto a la identificación segura del usuario del sistema, y el uso de contraseñas, aparte de ser continuamente violado, conlleva molestia y dejadez del usuario, que, o bien se tiene que acordar de numerosas contraseñas –y muchas veces las apunta cerca del terminal–, o utiliza la misma para todos los sistemas.

Sin embargo, aunque la biometría puede ser una solución muy efectiva, su coste (aunque ahora mucho más reducido) y la mentalidad del usuario, que muchas veces ve, sin ningún motivo, en la utilización de la huella, un problema policial o judicial, llevan a que no se termine de implantar dicha técnica.

Además, al utilizar cualquier parámetro biométrico, hay que prestar especial atención para que no sufra ataques ni

robos, por lo que la transmisión de la huella (de sus parámetros, y mucho menos de la imagen en sí) no debe realizarse de forma libre. Esto lleva a plantear dispositivos de identificación, que puedan llevar a cabo la verificación interna de la huella. En esta línea, el Grupo Universitario de Tarjeta Inteligente (GUTI), ubicado en la Universidad Carlos III de Madrid, está trabajando para poder realizar la verificación del patrón de la huella dentro de una Tarjeta Inteligente, y así facilitar su uso en sistemas distribuidos y multi-aplicación. Estos trabajos continúan los ya realizados con otras técnicas biométricas, y expuestos en [10][11][12]. Se espera encontrar soluciones en un futuro muy cercano.

CONCLUSIONES

En este artículo se ha analizado la técnica de autenticación biométrica mediante huella dactilar. Esta técnica lleva mucho tiempo en estudio, por lo que puede considerarse una técnica madura. Los sistemas de identificación automáticos, presentan peculiaridades que se van solucionando gracias a los trabajos de distintos investigadores a nivel mundial, tales como Jain o Maio. Se han descrito los algoritmos fundamentales para estos sistemas de identificación biométrica. La gran mejora y abaratamiento de los sistemas de captura, pueden hacer que en un futuro muy cercano, nos encontremos utilizando esta técnica para multitud de aplicaciones. n



2 Raúl Sánchez Reillo
Grupo Universitario de Tarjeta Inteligente
Departamento de Tecnología
Electrónica – Grupo de Microelectrónica
UNIVERSIDAD CARLOS III DE MADRID
rsreillo@ing.uc3m.es

REFERENCIAS

- [1] A. K. Jain, R. Bolle, S. Pankanti. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers. 1999.
- [2] H. C. Lee, R. E. Gaensslen. *Advances in Fingerprint Technology*. CRC Press LLC. 1994.
- [3] R. Sánchez Reillo. "Identificación biométrica y su unión con las tarjetas inteligentes". *Revista SIC, Seguridad, Informática y Comunicaciones*, nº 39, abril 2000, págs I-IV.
- [4] L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, S. Tsutsui. *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. CRC Press LLC. 1999.
- [5] A. K. Jain, L. Hong, S. Pankanti, R. Bolle. "An Identity-Authentication System Using Fingerprints". *Proceedings of the IEEE*, vol. 85, no. 9, September 1997.
- [6] A. K. Jain. *Fundamentals of Digital Image Processing*. Prentice Hall, 1989.
- [7] A. K. Jain, L. Hong, R. Bolle. "On-Line Fingerprint Verification". *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, April 1997.
- [8] D. Maio, D. Maltoni. "Direct Gray-Scale Minutiae Detection in Fingerprints". *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 19, no. 1, January 1997.
- [9] R. Sánchez Reillo. "El Iris Ocular como parámetro para la Identificación Biométrica". *Revista SIC, Seguridad, Informática y Comunicaciones*, nº 41, septiembre 2000, págs I-IV.
- [10] R. Sánchez-Reillo, A. Gonzalez-Marcos. «Access Control System with Hand Geometry Verification and Smart Cards». *IEEE Aerospace and Electronic Systems Magazine*, vol. 15, nº 2, febrero 2000. pp. 45-48.
- [11] R. Sanchez-Reillo. "Securing Information and Operations in a Smart Card through Biometrics". *IEEE Aerospace and Electronic Systems Magazine*, vol. 16, nº 4, April 2001, pp. 3 - 6
- [12] R. Sánchez Reillo. "Mecanismos de Autenticación Biométrica mediante Tarjeta Inteligente". Tesis Doctoral de la E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid. 2000.