UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

TESIS DOCTORAL

MECANISMOS DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TARJETA INTELIGENTE

RAÚL SÁNCHEZ REÍLLO

MADRID, 2000

UNIVERSIDAD POLITÉCNICA DE MADRID
E.T.S.I. TELECOMUNICACIÓN
DEPARTAMENTO DE TECNOLOGÍA FOTÓNICA

Tesis Doctoral:

MECANISMOS DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TARJETA INTELIGENTE

Autor:

Raúl Sánchez Reíllo

Ingeniero de Telecomunicación

Directores:

José Antonio Martín Pereda
Catedrático de Universidad
Dpt. Tecnología Fotónica - E.T.S.I.
Telecomunicación - U.P.M.

Carmen Sánchez Ávila
Profesora Titular de Universidad
Dpt. Matemática Aplicada - E.T.S.I.
Telecomunicación - U.P.M.

El Tribunal nombrado para juzgar la tesis citada:

Presidente:

Vocales:

Secretario:

acuerda otorgarle la calificación de

Madrid,

A José Luis,
profesor, ingeniero, innovador,
tutor, jefe, director, consejero
y, sobre todo, amigo.

AGRADECIMIENTOS

RESUMEN

El objetivo fundamental de esta Tesis es la creación de nuevos Mecanismos de Autenticación del titular de una Tarjeta Inteligente. La motivación de dicho trabajo ha sido la continua proliferación de nuevas aplicaciones donde es necesaria una autenticación del usuario que las utiliza y, por otro lado, las nuevas posibilidades que se abren dentro de la tecnología de dicho tipo de tarjetas de identificación.

El nuevo Sistema de Autenticación, está basado en la Identificación Biométrica, realizando la comprobación de la identidad del titular dentro de la propia tarjeta. Para ello se han estudiado distintas técnicas biométricas de forma que se puedan extraer conclusiones que lleven a la definición de un modelo para el nuevo Sistema de Autenticación. Las técnicas escogidas para ser analizadas fueron: la de *Reconocimiento de Locutores*, es decir, basada en la voz; la *Geometría del Contorno de la Mano*; y el análisis del *Patrón del Iris Ocular*.

Para cada una de las mencionadas técnicas, se han desarrollado al menos un prototipo, a partir de los cuales se han extraído los datos necesarios para analizar la viabilidad de ser incorporadas dentro de una Tarjeta Inteligente. Del mismo modo, se ha definido un modelo para el nuevo Sistema de Autenticación, desarrollándose prototipos basados en tarjetas con Sistema Operativo Abierto (en concreto, *JavaCard*), que han avalado el modelo definido.

ABSTRACT

This Thesis main target has been the creation of new Authentication Mechanisms for the cardholder who belongs a Smart Card. The motivation for such a work comes from the continuous appearances of new applications where an authentication of the user is needed and, also, from the new possibilities that are being opened in the technology involved with the above mentioned kind of identification cards.

The new Authentication System is based on Biometric Identification, performing the verification of the cardholder's identity inside the card. In order to achieve this result, different biometric techniques have been studied, so conclusions can be extracted for the definition of the new Authentication System Model. The biometric techniques chosen to be analysed has been: *Speaker Recognition*, i.e., based on the human voice; *Hand Outline Geometry*; and the analysis of the *Human Iris Pattern*.

For each of the mentioned techniques, at least one prototype has been developed. With these prototypes, several data has been extracted, in order to analyse the viability of being incorporated inside a Smart Card. Also, a model for the new Authentication System has been defined, and several prototypes have been developed based on Open Operating System Smart Cards (in this case *JavaCard*). The prototypes have endorsed the model defined.

ÍNDICE

ACRÓNIMOS

CA ..... Condición de Acceso
CLA ..... Clase (o tipo) de instrucción
DES ..... Es un algoritmo criptográfico de clave simétrica
EER ..... Tasa de Igual Error (*Equal Error Rate*)
FAR ..... Tasa de Falsa Aceptación (*False Aceptance Rate*)
FD ..... Fichero Dedicado
FE ..... Fichero Elemental
FEC ..... Fichero Elemental Cíclico
FER ..... Fichero Elemental de Registros
FET ..... Fichero Elemental Transparente
FI ..... Fichero Interno
FRR ..... Tasa de Falso Rechazo (*False Rejection Rate*)
GMM ..... Modelado por Mezclas de Gausianas (*Gaussian Mixture Modelling*)
INS ..... Código de instrucción
L_c ..... Longitud de los datos a enviar a la tarjeta
L_e ..... Longitud de los datos a recibir de la tarjeta
LEN ..... Longitud de los datos a intercambiar con la tarjeta
LPCC ..... Coeficientes cepstrum de predicción lineal
P1 ..... Parámetro 1 de la instrucción
P2 ..... Parámetro 2 de la instrucción
P3 ..... Longitud de los datos a intercambiar con la tarjeta
PB ..... Byte de Procedimiento (*Procedure Byte*)
PIN ..... Número de Identificación Personal (*Personal Identification Number*)
RFU ..... Reservado para Futuros Usos
SM ..... Mensajería Segura (*Secure Messaging*)
SOTI ..... Sistema Operativo de Tarjeta Inteligente
SW ..... Palabra de Estado (*Status Word*)
SW1 ..... Primer byte de la SW
SW2 ..... Segundo byte de la SW
TI ..... Tarjeta Inteligente
ULE ..... Unidad de Lectura/Escritura de TI

INTRODUCCIÓN

Cada vez es más frecuente la necesidad de que automáticamente se identifique a una persona para que ésta pueda acceder a un determinado lugar o servicio. Por otro lado, las nuevas aplicaciones que están surgiendo sobre Tarjetas Inteligentes, en las que cada vez se gestiona información más confidencial y personal, hace necesario una mejora en la forma que éstas identifican al titular de la tarjeta. Un ejemplo de este tipo de aplicaciones puede ser las relacionadas con la Banca, en la cual la tarjeta autoriza una determinada operación financiera basándose en la autenticación del titular de la tarjeta.

El método utilizado actualmente para realizar la autenticación del titular, es la verificación de un número de identificación personal, llamado normalmente PIN, el cual puede ser copiado fácilmente para utilizar la tarjeta de forma fraudulenta. En este trabajo, la alternativa que se propone es la utilización de características biológicas, o de comportamiento, del titular; es decir, utilizando Biometría.

Para afrontar la exposición de los trabajos propuestos, en el Capítulo I se reflejará la panorámica actual sobre la autenticación de usuarios, indicando los distintos modos de afrontar la problemática de la identificación. También se introducirá la tecnología de tarjetas, especialmente la de las Tarjetas Inteligentes (TI). Posteriormente se hablará de la Identificación Biométrica, mencionando las principales técnicas utilizadas, los parámetros empleados para su evaluación y los distintos esquemas de funcionamiento. Para facilitar la comprensión de los posteriores capítulos dedicados a las distintas técnicas biométricas, se va a incluir en este primer capítulo una introducción al Reconocimiento de Patrones, detallando los métodos que serán utilizados posteriormente. Por último, en dicho capítulo, se enmarcará la Tesis dentro del Estado del Arte a la hora de iniciar los trabajos de investigación.

Una vez realizada toda la introducción, se iniciará una serie de capítulos dedicados a tratar las distintas técnicas biométricas estudiadas. Se comenzará en el Capítulo II con el sistema basado en la voz, normalmente conocido como *Reconocimiento de Locutores*. Seguirá el sistema basado en la *Geometría del Contorno de la Mano*, en el Capítulo III, para finalizar en el Capítulo IV con el de *Patrón del Iris Ocular*. Estos tres capítulos presentarán una estructura análoga, donde se iniciará dando una introducción a la técnica, incluyendo una breve reseña sobre la anatomía involucrada. Posteriormente se tratarán los distintos bloques del sistema: Captura, Pre-procesado, Extracción de Características y Verificación. Una vez descrito el sistema correspondiente a cada capítulo, se pasará a detallar los resultados conseguidos, no sólo en autenticación, sino también

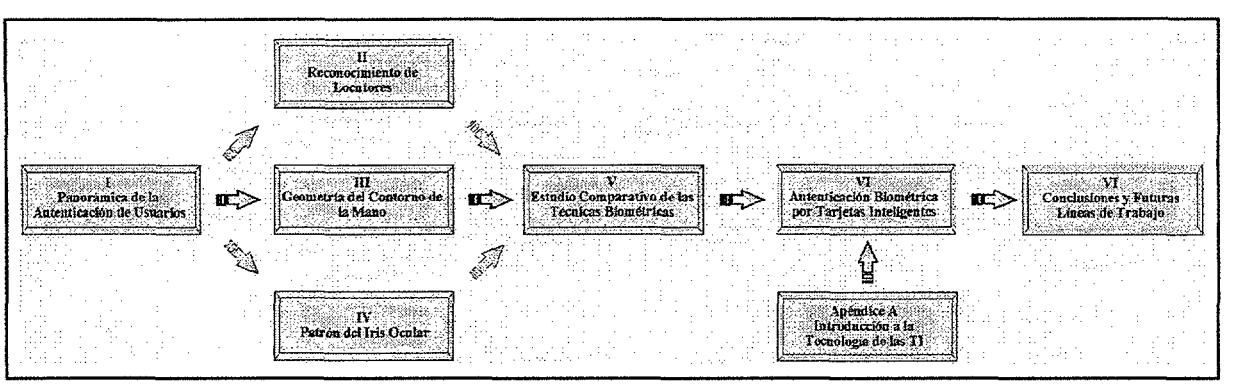
en reconocimiento. Se finalizará cada uno de estos capítulos con las conclusiones obtenidas.

Tras describir cada una de las técnicas y detallar los resultados, se dedicará el siguiente capítulo (el V) para hacer una comparativa entre las técnicas, sobre todo desde el punto de vista de la viabilidad para su incorporación a ser utilizadas dentro de una Tarjeta Inteligente. De esta forma se tratará: la aceptación por parte de los usuarios, el tamaño de los datos, los tiempos de ejecución y el rendimiento obtenido. Las conclusiones de este capítulo indicarán cuáles de estas técnicas son factibles de ser utilizadas para los propósitos de esta Tesis.

Se llega, pues, al momento de tratar el tema fundamental de esta Tesis, el cual quedará recogido en el Capítulo VI: la *Autenticación Biométrica mediante Tarjetas Inteligentes*. En dicho capítulo se dará una panorámica de los mecanismos actuales, que completará la descrita en el Capítulo I, para posteriormente empezar a definir el modelo del nuevo Sistema de Autenticación, lo cual se realizará en dos partes: una primera en la que se establecerán las condiciones de contorno, y una segunda donde se describirá la nueva Arquitectura de Autenticación. Se seguirá con la descripción de los prototipos realizados, relatando los resultados obtenidos, para finalizar con las conclusiones obtenidas.

Las conclusiones parciales obtenidas en cada uno de los capítulos, así como las diversas líneas de trabajo abiertas para futuros investigadores, se recogerán en el capítulo final (Capítulo VII). Aquí también tendrán cabida aquellas conclusiones de índole global que no han podido ser ilustradas en ningún capítulo particular.

Por último, para aclarar conceptos relativos a la tecnología de las Tarjetas Inteligentes, se ha considerado necesaria la incorporación del Apéndice A. Dicho apéndice puede resultar de gran ayuda para el lector, a la hora de seguir el Capítulo VI. En la figura adjunta se puede apreciar la relación entre cada uno de los capítulos.



CAPÍTULO I:

PANORÁMICA DE LA AUTENTICACIÓN DE USUARIOS

Antes de comenzar la exposición de las distintas técnicas biométricas utilizadas a lo largo de este trabajo, se va a dar en este capítulo una visión general sobre las técnicas que permiten la identificación de una persona frente a un sistema automático. La idea que subyace bajo este capítulo es la de establecer la base conceptual que sustentarán los desarrollos expuestos en capítulos posteriores.

Se iniciará, por tanto, planteando la problemática de la identificación electrónica, revisando algunas de las situaciones más típicas que se pueden dar. Esto conducirá a exponer las soluciones dadas en los últimos 75 años, basándose, principalmente en el uso de tarjetas de identificación. Las limitaciones que plantea, desde el punto de vista conceptual (y en cierto modo legal) la identificación mediante tarjetas, lleva a plantearse nuevas soluciones más cercanas a las que realiza el cerebro de una persona: identificar a una persona mediante parámetros biológicos. Como se verá, el conseguir realizar la identificación de esta manera, supone la utilización de técnicas de reconocimiento de patrones. Estas técnicas, algunas comunes para las distintas formas de realizar la identificación biométrica, serán introducidas también en este capítulo. Por último, y antes de acabar con las conclusiones derivadas de este capítulo, se dará una visión del estado del arte en el momento de iniciar los trabajos que han dado lugar a esta Tesis Doctoral.

I.1. LA IDENTIFICACIÓN ELECTRÓNICA

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 quien 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.

Pero todas estas formas de identificación suponen un previo conocimiento de la persona. Sin embargo, si dos personas que no se han encontrado nunca se encuentran en una situación en la que, al menos una de ellas, necesita constatar su identidad, se tiene que recurrir a medios alternativos. Imaginemos dos situaciones:

- Dos comerciantes se encuentran en una reunión del sector. Ambos se presentan mutuamente, y para constatar su identidad, aparte de transmitir otra información más, como la empresa para la que trabajan, se intercambian unas tarjetas de papel, que comúnmente se denominan tarjetas de visita o tarjetas de empresa.
- Un turista quiere coger un avión para irse de vacaciones. Ha comprado un billete con su nombre y para ir a recoger su tarjeta de embarque ha de pasar por un mostrador, donde un empleado de la compañía necesita comprobar la identidad de dicho turista, de forma que esté seguro de que le está entregando la tarjeta de embarque al cliente que realmente corresponde. Una vez pasado este trámite, el turista debe pasar por un control de accesos, de forma que un policía atestigüe que la persona que va a entrar en un avión no es, por ejemplo, un terrorista. Para ambos casos, el turista mostrará un documento acreditativo de su identidad, emitido por una entidad de solvencia reconocida (normalmente un Estado), y que suele ser denominado Pasaporte, o en otros casos, por ejemplo, Documento Nacional de Identidad (DNI).

En estos dos ejemplos queda palpable una de las características más importantes al tratar la identificación de una persona: los requisitos de exactitud de la identificación dependen de la seguridad que se le quiera dar al sistema. Es decir, en el primer caso quedaría demasiado riguroso el que los dos comerciantes se enseñaran el DNI, puesto que sólo quieren identificarse para conocerse, compartir un café y, con un poco de suerte, plantear futuras relaciones entre las

empresas. En el segundo caso no se admitiría nunca la utilización de una tarjeta de visita, ya que ésta puede ser fácilmente falsificable, y se tiene que asegurar el importe pagado por el cliente, por un lado, y la seguridad del resto de los pasajeros, por otro.

En todos los casos comentados hasta ahora, están siempre presentes los dos actores en el proceso de identificación: el que requiere la identificación y el que se identifica. Sin embargo, con la expansión de las redes telemáticas y la proliferación de distintas soluciones en las que nunca se encuentran cara a cara los dos actores, complican de gran manera el proceso de identificación. Imaginemos el caso de un Cajero Automático. En este caso, el cliente del sistema quiere obtener un dinero, pero el propietario del Cajero, el Banco, tiene que estar seguro de que el dinero lo saca de la cuenta del cliente apropiado y se lo entrega realmente a dicho 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.

Por otro lado, alejándose de las aplicaciones telemáticas, una aplicación en la que es más evidente la necesidad de identificación de un individuo, y donde se refleja las diferencias de criterio para definir los requisitos del sistema, es el control de accesos a edificios o estancias. Dependiendo de las restricciones de acceso a una determinada estancia, así se define el nivel de seguridad que tiene que proporcionar el sistema de acceso. Un ejemplo muy significativo es la diferencia de criterio al definir un sistema de acceso a una sala de lanzamiento de misiles en un edificio militar, o el de entrada a una simple sala de reuniones.

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 Identificacion*

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 el 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, las soluciones basadas en este tipo de elementos han sido ampliamente utilizadas. La evolución será comentada en el próximo apartado, focalizándose principalmente en el uso de las tarjetas. 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 puede plantear sistemas anti-fraude bastante robustos.
- **Características biológicas o de comportamiento:** Serán la base de la Biometría y a ello le dedicaremos todo un apartado posteriormente. Es la única solución 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 soluciones basadas en híbridos de ellas. El ejemplo típico es la tarjeta bancaria en la que hay que utilizar un PIN para poder acceder a las funciones del cajero. Otra de estas soluciones es la que se proopone en este trabajo, en el que se mezclan la Biometría y las Tarjetas Inteligentes.

I.2. LA TARJETA COMO TÍTULO DE IDENTIFICACIÓN

Los orígenes de las tarjetas como elemento de identificación se podría fijar con la aparición de las ya mencionadas Tarjetas de Visita. Estas tarjetas, hechas de papel o cartón, reflejan en su superficie el nombre del titular de la tarjeta, así como diversos datos relativos a su domicilio personal o a su situación en una empresa. Sin embargo, dejando a un lado este tipo de tarjetas, las cuales continúan teniendo una gran importancia en nuestros días, podemos establecer el orígen de la utilización de las tarjetas como sistema de identificación en el año 1950. Fue

entonces cuando Diners Club estableció, en Estados Unidos, una tarjeta de plástico que identificaba a su titular como persona con crédito cuando éste lo presentaba en alguno de los hoteles y restaurantes adheridos al programa. Su expansión a partir de entonces, tal y como se describe en [Bri88], vino marcada por el éxito de dicho programa, creándose a finales de los años 50 otros tipos de tarjetas de crédito que dieron lugar a la creación de empresas como la American Express Company, también en EE.UU., o la Carte Blanche en Francia.

Sin embargo, ya a finales de los años 40 algunos bancos estatales de EE.UU. habían emitido tarjetas de crédito. Pero estas iniciativas no tuvieron mucho éxito al no poder ser utilizadas fuera del Estado en el que habían sido emitido. Esto llevó a que, para satisfacer las necesidades de movilidad de sus clientes, se crearan empresas como VISA o Interbank (la cual actualmente se conoce como Mastercard). En Europa se mantenía una posición de cautela, observando las evoluciones de los programas americanos, hasta que en el 1966 el banco Barclays emitió su primera tarjeta de crédito, la cual, tras un empiece lento, alcanzó gran éxito y empujó a la creación de diversos programas de crédito por parte del resto de los bancos europeos en los primeros años 70.

La gran expansión de las tarjetas de crédito provocó nuevas necesidades, tales como la creación de los primeros Cajeros Automáticos a finales de los años 70, o la mejora en la seguridad de las tarjetas. Esto empujó a que de los formatos de las primeras tarjetas, las cuales sólo tenían caracteres empotrados para ser impresos en las populares *"bacaladeras"*, se llegara a la necesidad de introducir una banda magnética que contuviese información que se pudiera leer de forma electrónica. Posteriores medidas de seguridad empujaron a introducir hologramas, marcas de agua, codificación de la información, etc.

La tecnología empezó a ser aceptada y a bajar sustancialmente su coste. Esto facilitó que las tarjetas no sólo se utilizasen en programas de crédito, sino también en muchos otros sectores: fidelización de clientes, seguros sanitarios, identificación de socios de clubs, etc. Todo esto llevó a nuevas necesidades en materia de capacidad de almacenamiento de información, así como de seguridad de la misma. El progreso tecnológico de los últimos 25 años ha facilitado afrontar estos nuevos retos mediante distintas tecnologías, creándose distintos tipos de tarjetas, siendo las más representativas:

- **De Banda Magnética:** son aquellas que en su parte posterior tienen una banda de material ferromagnético donde se puede grabar información. Son las más difundidas actualmente.
- **Ópticas:** poseen una zona de material grabable y leíble de forma óptica, análogo al utilizado en los Discos Compactos (CDs). Permiten una alta capacidad de memoria.
- **De Circuito Integrado de Memoria:** tienen un chip empotrado en su interior. Dicho

chip no es más que una memoria de silicio que, opcionalmente, puede tener algún mecanismo de seguridad realizado con lógica cableada. Las más conocidas son las tarjetas utilizadas para el prepago telefónico.

- **De Microprocesador:** más comúnmente llamadas ***Tarjetas Inteligentes***, tienen al igual que el tipo anterior, un chip, pero que en este caso se trata de un microprocesador con una memoria y unos periféricos asociados. Permite una gran capacidad de almacenamiento (sin llegar a la conseguida mediante las tarjetas ópticas) con una elevadas prestaciones de seguridad.

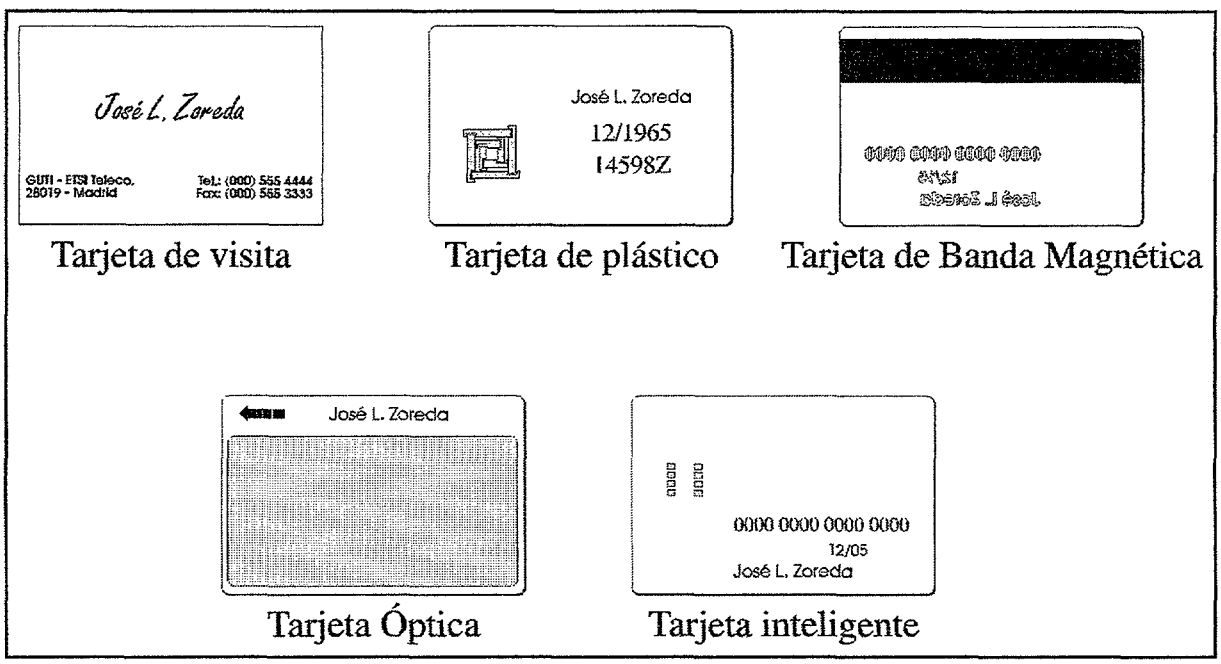


Fig. I.1: Distintos tipos de tarjetas de identificación

Sin embargo, para los temas relativos a esta Tesis, es más interesante hacer una clasificación por las características de seguridad aportadas. De esta forma podemos dividir entre:

- **Pasivas:** son aquellas en las que la información se encuentra sin ninguna protección por parte de la tarjeta, y la única forma existente para garantizar una cierta privacidad de los datos, es el cifrado de los mismos antes de grabarlos. En esta clasificación se encuentran las Tarjetas de Banda Magnética, las Ópticas y algunos modelos de Tarjetas de Circuito Integrado de Memoria.
- **Con protección mediante lógica:** tipo en el que se engloban, exclusivamente, aquellos modelos de Tarjetas de Memoria que no son Pasivos. En estos modelos se puede proteger el acceso a la información mediante alguna secuencia de datos (por ejemplo, un PIN), estando desarrollada esta protección mediante lógica cableada o programada.
- **Activas:** la información incluida en la tarjeta se puede proteger frente a diversas

operaciones mediante una serie de reglas de acceso definidas dentro de la tarjeta. El único tipo de tarjeta que incluye este tipo de protección son las Tarjetas Inteligentes, donde la existencia de un Sistema Operativo gestiona una Arquitectura de Seguridad que rige el acceso a las distintas partes de la tarjeta.

La aparición de las Tarjetas Inteligentes ha hecho posibles numerosas aplicaciones hasta hace poco sólo soñadas. En la actualidad se pueden ver en multitud de entornos, siendo los más activos:

- Telefonía Móvil Digital (GSM): donde la tarjeta sirve como identificación del titular del número de teléfono, herramienta de cifrado y base de datos del titular (donde se guardan sus opciones, sus números de teléfono, sus mensajes cortos, etc.)

- Banca: su gran potencial se ha intentado desarrollar mediante el denominado Monedero Electrónico, en el cual la tarjeta sirve como sustituto de la "calderilla", pudiendo cargarla con un determinado importe y hacer compras frente al saldo existente en la tarjeta. Sin embargo, esta aplicación todavía no ha terminado de ser aceptada pero se espera una evolución positiva a corto y medio plazo, sobre todo por la inclusión de nuevas aplicaciones dentro de la misma tarjeta (como el de un abono transporte o la misma tarjeta de crédito o débito).

Este tipo de tarjetas, la Tarjeta Inteligente, será el utilizado durante el desarrollo de la Tesis, por lo que antes de terminar esta introducción al mundo de las tarjetas, se va a hacer una breve descripción de las mismas que sirva de base para una posterior consulta en textos más detallados como [Bri88, Zor94, Zor96 y San99a].

I.2.1. TARJETAS INTELIGENTES

Tal y como se ha esbozado ya, una Tarjeta Inteligente (TI) no es más que una Tarjeta de Plástico, de dimensiones normalizadas (las mismas que una tarjeta de crédito), que tiene empotrado en su interior un chip compuesto por los siguientes bloques (tal y como se puede ver en la figura I.2):

- Unidad Central de Proceso
- Memorias

- Bloque de entrada/salida
- Sistema de control de la alimentación
- Circuitería de arranque
- Sistema de supervisión del reloj

La Unidad Central de Proceso se encargará de ejecutar las instrucciones de un programa almacenado en la memoria. Dicho programa se encargará de gestionar todo el funcionamiento de la TI, y se le denominará Sistema Operativo de Tarjeta Inteligente (SOTI). En la mayoría de los casos, el SOTI se encuentra almacenado en memoria ROM, dejando libre aquella memoria de tipo RAM y EEPROM para que en éstas se almacenen los datos temporales y los datos del usuario, respectivamente.

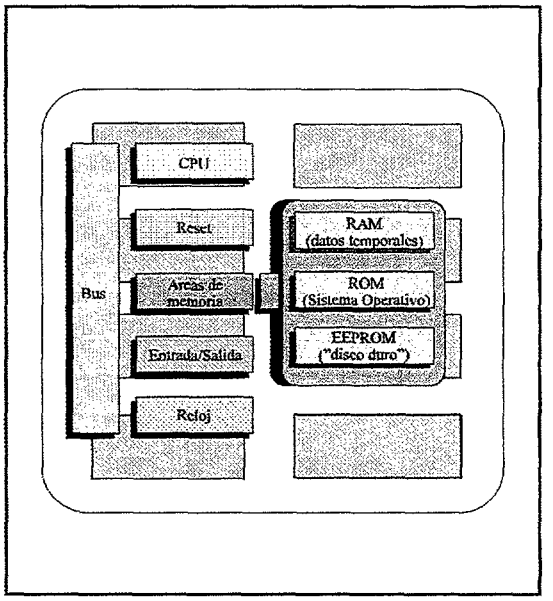


Fig. I.2: Bloques de una Tarjeta Inteligente

El SOTI se encarga de gestionar todos los recursos de la TI, de forma que para cualquier usuario o programador de aplicaciones sobre TI, sólo quede visible al exterior:

- **Una Estructura de Datos:** es decir, la forma en la que se van a poder almacenar los datos correspondientes al usuario y a la aplicación (el nombre, el saldo del monedero, los datos sanitarios de urgencia, etc.). Esta Estructura de Datos es, a grandes rasgos, una estructura jerárquica análoga a la de una partición en el disco duro de un ordenador.

- **La capacidad de memoria disponible en la EEPROM:** o dicho de otra forma, la que se conocerá como capacidad de la Tarjeta.

- **Una Arquitectura de Seguridad:** que va a regir la forma de acceso a las distintas informaciones que contiene la tarjeta. De una forma general, esta Arquitectura de Seguridad estará formada de unos algoritmos de seguridad, unas claves y unas reglas de acceso para cada archivo de información.

- **Un Juego de Comandos:** con el que se va a poder realizar la Entrada y Salida de datos de la Tarjeta.

Para producir ese intercambio de información, la Tarjeta Inteligente se servirá de un canal físico de comunicación. Dicho canal ha sido tradicionalmente los contactos metálicos existentes en la superficie de la tarjeta. Sin embargo, y no entrando en detalles, también existen TI en las que la comunicación se realiza por radiofrecuencia.

Por tanto la Tarjeta Inteligente es un sistema portátil y seguro de almacenamiento de la información. Su característica de poseer una jerarquía en el almacenamiento de la información, permite que la TI pueda ser multiaplicación, es decir, que la misma tarjeta física tenga información de, por ejemplo, una aplicación de monedero electrónico y una aplicación de datos sanitarios del titular. Además, la jerarquía se extiende a la arquitectura de seguridad, por lo que permite que la información de las dos aplicaciones se proteja independientemente, siendo imposible para el banco observar los datos sanitarios, y para la empresa de salud los datos bancarios.

La protección de los datos se realiza, en la actualidad, mediante claves binarias de diversas longitudes (siendo típicas las de 8 y 16 bytes). Una de las claves que puede tener la TI, es la denominada PIN, es decir, Número de Identificación Personal. Esta clave sirve para impedir el uso de la tarjeta, o el acceso a determinadas operaciones o datos de ella, sin el permiso del titular de la misma. De esta forma, se puede realizar la identificación del titular de la tarjeta en un sistema mecánico como, por ejemplo, un Cajero Automático.

Sin embargo la potencia de las TI desde el punto de vista de seguridad va mucho más lejos que el simple uso de claves para proteger los datos. El SOTI permite definir el número de veces que se puede introducir la clave erróneamente. Una vez sobrepasado ese límite, la tarjeta bloquea esa clave y, por lo tanto, toda la información que está protegida mediante ella. Si no se tiene establecido un procedimiento de desbloqueo (decisión que depende de la seguridad y versatilidad que se le quiera dar a la tarjeta), la información contenida dentro de la tarjeta quedará definitivamente inservible, ya que no será posible volver a acceder a ella.

Como se planteará en esta Tesis, estas protecciones, aunque mucho mejores que las existentes mediante otras técnicas, pueden seguir sin ser suficientes, ya que la tarjeta puede ser robada y el PIN escuchado o visto, pudiendo suplantarse la identidad del usuario. Para ello se requeriría una verificación de parámetros biológicos del usuario, tal y como se muestra en los siguientes apartados.

I.3. 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. Sin embargo, descubrir cuando el hombre ha sido consciente de esta capacidad como para poderla utilizar en su propio beneficio, es algo que ha dado lugar a varios estudios. Uno de esos estudios, principalmente interesado en la utilización de las huellas dactilares, se puede seguir en el primer capítulo de [Lee91]. En este texto se induce que hace ya unos 5000 años, los chinos eran conscientes de la individualidad de las huellas, y la colocación de éstas de forma muy cuidadosa en los objetos manufacturados plantean la posibilidad de que lo utilizasen como forma de firmar sus creaciones.

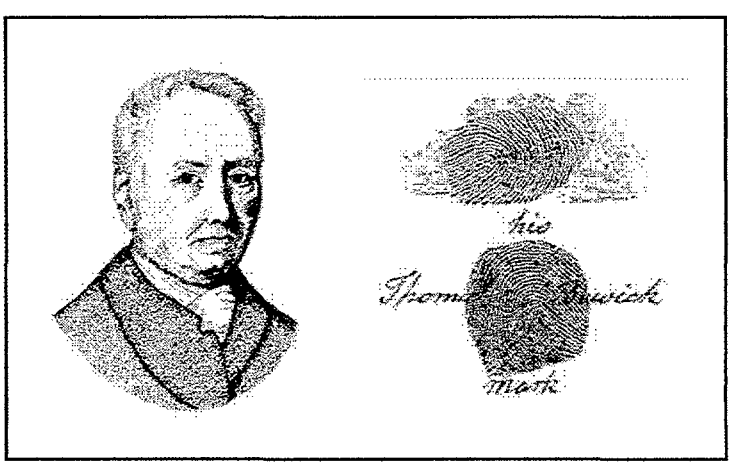


Fig. I.3: Thomas Bewick y sus marcas ([Lee91])

Pero fue en el año 1684 de nuestra era donde se puede encontrar el primer estudio de las huellas dactilares sobre sus características de identidad de la persona. Dicho estudio fue llevado a cabo por el inglés Nehemiah Grew. Algunos contemporáneos de Grew realizaron estudios análogos, pero sin llegar a profundizar mucho más. A finales del siglo XVIII y principios del XIX, nos encontramos con el inglés Thomas Bewick, que es considerado el primer caso oficial de firma mediante la huella dactilar, al utilizar esa técnica para firmar sus libros.

El siglo XIX fue realmente la fecha en la que se produjeron los mayores avances en

técnicas de identificación biométrica. Fue en estos momentos 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. Su utilización por parte de la policía de los distintos países, hizo que el sistema se fuera perfeccionando. Pero fue precisamente un experto en este sistema, Sir Francis Galton, quien a finales del siglo XIX realizó 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 circunstancias, 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.

I.3.1. LAS 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 utilizada para realizar la identificación, siempre que dichas características se demuestren propias de la persona a identificar. Las distintas técnicas que se están estudiando actualmente se pueden ver descritas en [Jai99a], siendo:

- **Voz:** Técnica que será tratada en el próximo capítulo. Como se verá, existen innumerables métodos para realizar esta identificación, siendo algunos dependientes del texto que se pronuncia, mientras otros son independientes del mismo.

- **Huella Dactilar:** Tal y como se ha comentado ya, 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.

- **Rostro:** El método de identificación que nuestro cerebro usa más a menudo y de una forma más sencilla. En la actualidad existen muchos grupos trabajando en esta técnica

con diversos métodos. Los resultados que se están consiguiendo son bastante prometedores, aunque le falta todavía un poco hasta llegar al nivel de otras técnicas.

- **Iris:** Técnica que se verá en un capítulo posterior, fue impulsada por 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, teniendo en cuenta que las características en las que está basada, el patrón de iris, permanece inalterable durante la vida del sujeto debido a la protección que le proporciona la cornea. Por otro lado, los estudios sobre la unicidad de las características, la han colocado muy por encima de la huella dactilar.

- **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.

- **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 saben 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 usuario. 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 trata de una técnica 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.

- **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, provocan 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 de la Mano y/o del Dedo:** La técnica basada en Geometría de la Mano será estudiada con detalle en un capítulo posterior. La basada en geometría del dedo es una simplificación del anterior, en el que solo se considera uno o dos dedos, en lugar de todo el perfil de la mano.

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 utilizadas 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 utilizadas 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. Por ejemplo, la universalidad de Rostro es muy alta, mientras que la de Dinámica de Teclado es muy baja.

- **Unicidad:** La probabilidad de que no existan dos sujetos con las mismas características. Por ejemplo, la unicidad de Mano y Rostro son medias, mientras que las de Iris o Retina son muy altas.

- **Estabilidad:** Si las características que se extraen permanecen inalterables con relación a diversos parámetros (tiempo, edad, ritmo de trabajo, enfermedades, etc.). Por ejemplo, la Voz tiene una estabilidad relativamente baja, mientras que el Iris y la Retina presentan una estabilidad muy alta.

- **Facilidad de captura:** Si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto. Por ejemplo, tanto Voz como Mano presentan una gran facilidad de captura pues usan un simple micrófono o una cámara de fotos. Por otro lado, las técnicas basadas en Retina o en DNA, utilizan sistemas muy complejos.

- **Rendimiento:** Denominado también tasas de acierto y error. Iris, DNA, Retina y algunos métodos de Huella presentan unas tasas realmente buenas, mientras que técnicas como Oreja o Voz presentan tasas bastante bajas.

- **Aceptación por los usuarios:** Se trata de un parámetro habitualmente olvidado y sin embargo es el que puede considerarse más importante para un verdadero éxito del sistema. Si los usuarios no aceptan con agrado el sistema, se pueden llegar a negar a usarlo o, lo que puede llegar a ser peor, a usarlo con desidia, falseándose los resultados. Ejemplos característicos de problemas ocurridos por mala aceptación, son Retina, por el método de captura de los datos biológicos, y en algunos entornos Huella, por su connotación policial o judicial.

- **Robustez frente a la burla del sistema:** Si la técnica puede reconocer el falseamiento de los datos capturados (por ejemplo, uso de fotos, dedos de latex, etc.). Esta característica normalmente viene mejorada por técnicas colaterales para detectar sujeto vivo. En el caso de Huella, se puede detectar el flujo sanguíneo, o en el caso de Voz, cambiando el mensaje a pronunciar por parte del sujeto a reconocer.

- **Coste:** Por supuesto, a la hora de implantar cualquier tipo de sistema, hay que tener en cuenta el coste del mismo, ya que un excesivo coste puede no estar justificado para el nivel de seguridad que se pretende conseguir. Las técnicas basadas en Iris o Retina tienen un coste muy elevado, mientras que las basadas en Voz presentan uno muy bajo.

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.

I.3.2. ETAPAS EN UN SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA

Como se ha mostrado, las técnicas de identificación biométrica son muy diversas. Sin embargo, a la hora de desarrollar un sistema de identificación basado en alguna de esas técnicas, se mantiene un esquema totalmente independiente de la técnica utilizada. Los sistemas, tal y como se puede ver en la figura adjunta, se componen de las siguientes etapas:

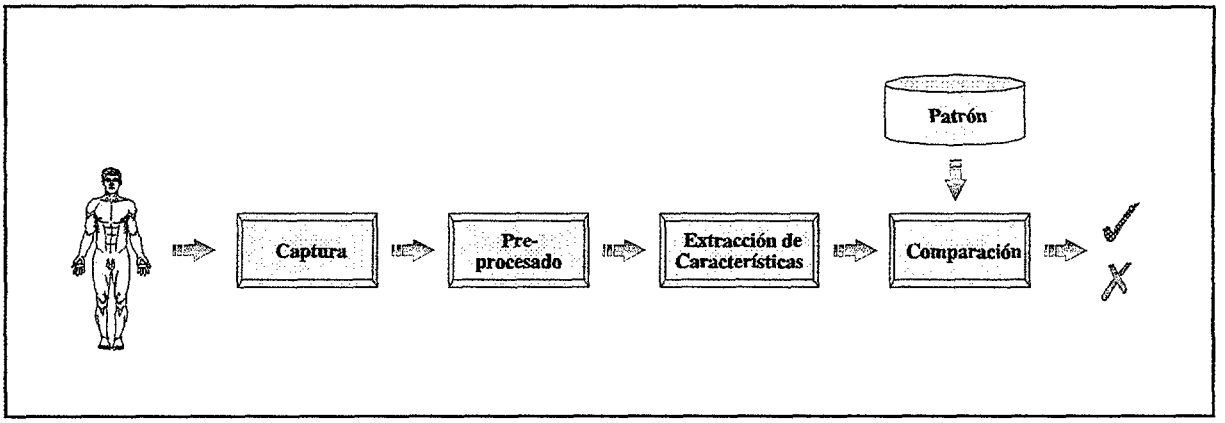


Fig. I.4: Diagrama de bloques de un sistema de identificación biométrica

- **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) para que se encuentre entre los márgenes que reconoce el algoritmo siguiente, etc.

- **Extracción de Características:** Se puede considerar el bloque más característico 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 ser muy distinto, e incluso contradictorio, 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, que se denominan ***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 se va a realizar siguiendo los métodos utilizados en Reconocimiento de Patrones, tal y como se verá en el siguiente apartado.

En la descripción de los distintos bloques de un sistema de identificación biométrica, se han introducido dos elementos de gran importancia: el patrón y el umbral. Sobre este segundo se hablará en la siguiente sección, mientras que sobre el patrón cabe hablar de la forma de obtenerlo. Para obtener el patrón se habilita una fase previa a la de utilización del sistema. De esta forma, todo sistema de identificación biométrica tiene dos fases de uso:

1. **Reclutamiento:** En esta fase, se capturan distintas muestras del usuario, se pre-procesan, se extraen las características y, a partir de las características extraídas, se forma el patrón. Si se capturan 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, se encarga una persona de controlar como 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 enseñarle al usuario el sistema y aclararle todas las dudas que pudiera tener.

2. **Utilización:** Una vez que se tiene almacenado el patrón del usuario, éste utiliza el sistema con normalidad, y sus características son comparadas con el patrón extraído (tal y como ya se ha comentado).

El modo en el que se hace el reclutamiento no es ni mucho menos 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 en los sistemas basados en voz. Por otro lado, la forma de almacenar el patrón dependerá del esquema de funcionamiento del sistema de identificación biométrica, tal y como se va a ver en la próxima sección.

I.3.3. ESQUEMAS DE FUNCIONAMIENTO

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 de capacidad de almacenamiento y seguridad de los datos oportunos) y la existencia de una red de comunicaciones, siempre en linea, 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. Entonces, el sistema se encarga 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. Este último caso no son necesarias ni la Base de Datos ni la red de comunicaciones de los sistemas de Reconocimiento.

A lo largo de esta Tesis, se va a hablar, casi exclusivamente, de Autenticación Biométrica, y se va a obviar la solución que incluye una Base de Datos, ya que el propósito de los prototipos desarrollados será la inclusión y verificación del patrón dentro de una Tarjeta Inteligente. Sin embargo, en cada una de las técnicas se va a hacer referencia a esquemas de Reconocimiento, ya que va a ser la forma de verificar el grado de unicidad de las características obtenidas.

Por último, y antes de acabar con este apartado de introducción a la Biometría, hay que

indicar la forma en la que se dan los resultados en cada uno de los dos esquemas de funcionamiento comentados anteriormente, para así poder entender más fácilmente las gráficas y tablas de los capítulos posteriores.

El caso más sencillo es el del Reconocimiento. En este caso, los resultados se suelen dar en porcentaje de acierto, y en el caso de que se utilice un umbral de rechazo del resultado, el porcentaje de ese rechazo. Sin embargo, en el esquema de Autenticación, los resultados se dan en función de dos tasas de error:

- **Tasa de Falso Rechazo (FRR[1]):** Es el porcentaje de casos en los que a un usuario se le ha rechazado, es decir, cuando las características del usuario correcto no superan el umbral de aceptación al compararlas con el patrón de él mismo.

- **Tasa de Falsa Aceptación (FAR[2]):** Es el porcentaje de casos en los que un intruso ha podido ser reconocido como un usuario. En esos casos, las características extraídas del intruso han superado el umbral de aceptación con respecto al patrón de un usuario del sistema.

Estas dos tasas obtienen sus números en función del umbral que se tome. Además guardan una relación de variación inversa, es decir, si se cambia el umbral de forma que se baje el falso rechazo, la falsa aceptación subirá, y viceversa. La elección del umbral y, por lo tanto, de la FAR y la FRR, dependerá exclusivamente de los requisitos de seguridad y funcionamiento que se quieran obtener para un entorno específico. Por ejemplo, para una sala de alta seguridad, habrá que bajar al mínimo la FAR aun a costa de incrementar enormemente el rechazo de los usuarios. Sin embargo, en un sistema a ser utilizado por muchas personas, puede ser más interesante que el rechazo sea mínimo, para no crear malestar entre los usuarios, lo cual supondrá subir, hasta un límite razonable la FAR.

Debido a esta variación de las tasas de error, para comparar diversas técnicas hay muchos investigadores y comerciales que utilizan la denominada **Tasa de Igual Error (EER[3])**, que es el punto donde la FAR y la FRR tienen el mismo valor. Sin embargo, al realizar la comparación

[1] Las siglas utilizadas corresponden al término inglés *False Rejection Rate*. El equivalente en castellano sería TFR, sin embargo, se ha adoptado el uso del acrónimo anglosajón por homogeneidad con la literatura existente.

[2] El acrónimo corresponde al término inglés *False Aceptance Rate*. El equivalente en castellano sería TFA, pero, por el mismo motivo que en la nota anterior, se ha optado por el uso de las siglas inglesas.

[3] Corresponde al término inglés *Equal Error Rate*. En castellano sería TIE, pero al igual que anteriormente, se ha optado por el término inglés.

mediante este valor, se está perdiendo información sobre la técnica, ya que puede no ser tan importante esa tasa, sino la forma en que evolucionan la FAR y la FRR respecto a las variaciones de un umbral. Además, desde el punto de vista práctico, casi nunca se va a utilizar ese punto como valor del umbral, ya que normalmente se tomará un valor mayor o menor.

I.4. MÉTODOS DE RECONOCIMIENTO DE PATRONES

Como se ha comentado, la comparación entre las características extraídas y el patrón almacenado, se realiza mediante métodos de clasificación y discriminación, los cuales se encuentran recogidos en la literatura que trata la temática de Reconocimiento de Patrones. En este apartado se pretende dar una modesta introducción a dicha temática, que sirva de base para la comprensión de las técnicas empleadas en capítulos posteriores. Se le sugiere al lector interesado en profundizar en estos temas, que consulte bibliografía especializada como [Dud73], [Esc77], [Han81], [Sch96] y [The89]. Tras la breve introducción a la teoría, se abrirán unas secciones para explicar detalladamente algunos de los algoritmos que van a ser utilizados por más de una técnica biométrica, de forma que se simplifique la redacción de los correspondientes capítulos.

I.4.1. TEORÍA BÁSICA

Todo estudio sobre Clasificación y Reconocimiento de Patrones, empieza con una introducción a la Teoría de Bayes, en la que se establecen las reglas de la probabilidad condicionada de pertenencia a una determinada clase, de todas las clases que contiene el espacio de muestras. Pero la exposición que se va a hacer en esta sección va a estar más orientada al esquema final que se va a utilizar.

Si suponemos que el espacio de características es bidimensional, el objetivo es partir ese espacio en el determinado número de clases que identifican a cada uno de los grupos disjuntos. La situación ideal sería que todas esas clases fueran disjuntas y, por tanto, se pudieran establecer fronteras bien definidas entre ellas, tal y como se puede observar en la figura I.5.a. Sin embargo, en la casi totalidad de las ocasiones dadas en Biometría, esas clases no son disjuntas (fig. I.5.b), y por lo tanto hay un cierto solape entre ellas. Eso es lo que provoca que, dependiendo de como se coloquen las fronteras, existan más o menos equivocaciones a la hora de realizar la

clasificación de las diversas muestras.

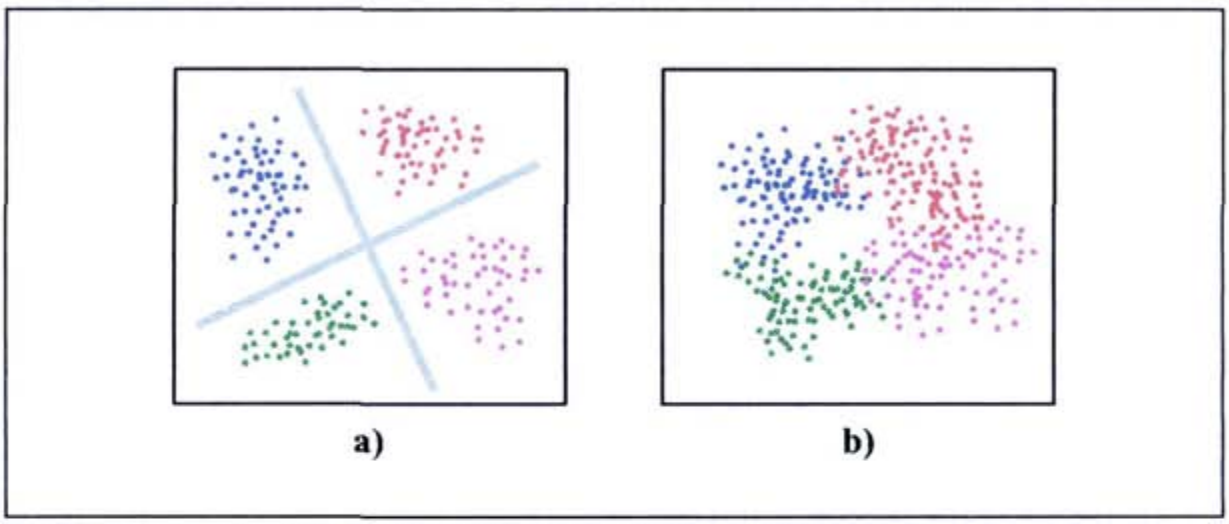


Fig. I.5: División del espacio de características en clases (caso bidimensional)

Por lo tanto, al hacer esa partición del espacio de características en clases, lo que realmente se está haciendo es una clasificación. El problema que hay que resolver, por tanto, es el de cómo describir esas clases. Evidentemente, puesto que no puede conocerse, en la mayoría de los casos, *a priori* cómo va a ser la distribución de las características de cada clase, y como además no se va a tratar normalmente del caso bidimensional, sino multidimensional, el problema no es ni mucho menos trivial.

Existen numerosas formas de abordar este problema. Las más sencillas se basan en encontrar un *centroide* de la clase (un patrón) y delimitar su área de influencia mediante una medida de **distancia**. La forma de obtener el centroide (el patrón) suele ser como media de un determinado número de muestras iniciales. Como ejemplos de esta forma de definir el área de influencia de las distintas clases, están la *Distancia Euclídea* o la *Distancia de Hamming*. En la primera, las clases se modelan como los puntos internos a una esfera ubicada en el centroide, y de radio el valor especificado de la distancia. Mediante la Distancia de Mahalanobis, las clases son los puntos ubicados en los ejes de un elipsoide. Sin embargo, el caso de la Distancia de Hamming conlleva una orientación binaria del problema y se detallará más adelante.

Otra forma de abordar el problema de delimitar las clases, cuando éstas presentan formas más complejas, es modelarlas mediante funciones estadísticas. Existen diversas funciones que están siendo utilizadas para realizar esos modelados, aunque la más usada es la función densidad de probabilidad gausiana (como se verá con el Modelado basado en Mezclas de Gausianas).

Todas estas aproximaciones al problema, al igual que muchas otras, requieren un cierto

conocimiento *a priori* de la forma que van a tener las clases. Cuando no se tiene ese conocimiento, se pueden utilizar soluciones basadas en Redes Neuronales[4], en las que es el propio algoritmo de entrenamiento de la red, el que se va adaptando a la forma que debería tener la clase, en función de los datos que se le facilitan.

En el caso de que estemos tratando de realizar autenticación en lugar de clasificación, habrá que delimitar únicamente el espacio del usuario en cuestión, teniendo en cuenta que el resto del espacio puede corresponder a otros usuarios. Esta nueva característica, no supone una limitación para los métodos basados en conocimiento *a priori*.

Sin embargo, para los métodos basados en Redes Neuronales, implica la imposibilidad de su uso bajo determinadas condiciones. El problema que se presenta es que las Redes Neuronales no poseen un sesgo negativo implícito, es decir, si se entrena una red dándole únicamente muestras del usuario a identificar, y no se le da ninguna muestra de usuarios distintos a él, la red entenderá que todo el espacio de características es válido y por tanto el espacio designado para la clase de ese usuario no tendrá fronteras. Para evitar esto, habría que introducir un determinado número de muestras distintas de las del usuario a verificar. Esto implicaría entrenar la red con muestras de otros usuarios, lo cual implica, a su vez, la existencia de una Base de Datos de muestras de usuarios con la única finalidad de realizar el entrenamiento. La existencia de esa Base de Datos va en contra de la filosofía que subyace en esta Tesis, ya que la idea es que el patrón de cada usuario sólo lo posea el titular de la tarjeta donde está almacenado, y no se encuentren réplicas de él en ningún sistema informático. Es esta la razón por la que no se van a considerar el uso de Redes Neuronales para Autenticación Biométrica mediante Tarjeta Inteligente. Sin embargo, se quiere hacer notar, que el autor de esta Tesis ha probado su viabilidad en sistemas de Reconocimiento, habiendo obtenido unos resultados muy satisfactorios, especialmente con Redes basadas en Funciones de Base Radial.

A continuación se van a exponer los distintos métodos utilizados en más de una técnica, de forma que sirva de referencia para aquellos capítulos donde se haga referencia a ellas. Dos de las técnicas están basadas en distancias, mientras que la tercera está basada en modelado mediante funciones de densidad de probabilidad.

[4] Por motivos que se expondrán posteriormente, no se va a tratar el tema de Redes Neuronales. Sin embargo, para el lector interesado en conocer las distintas técnicas existentes se le recomienda que se refiera (por este orden) a [Lip87], [Hus93] y [Hay94], y como consulta a aplicaciones y nuevos algoritmos a *IEEE Transactions on Neural Networks*.

I.4.2. DISTANCIA EUCLÍDEA

Como ya se ha comentado, el método basado en la Distancia Euclídea, centra la clase en un patrón de características resultado de la media del número de muestras inicialmente tomadas ([Dud73], [Esc77], [Han81]). La distancia desde cualquier muestra nueva a ese centro se mide mediante la siguiente fórmula:

$$d = \sqrt{\sum_{i=1}^{L} \left(x_i - t_i\right)^2} \qquad (I.1)$$

donde L es la dimensión del vector de características, x_i es la i-ésima componente del vector de características y t_i es la i-ésima componente del patrón.

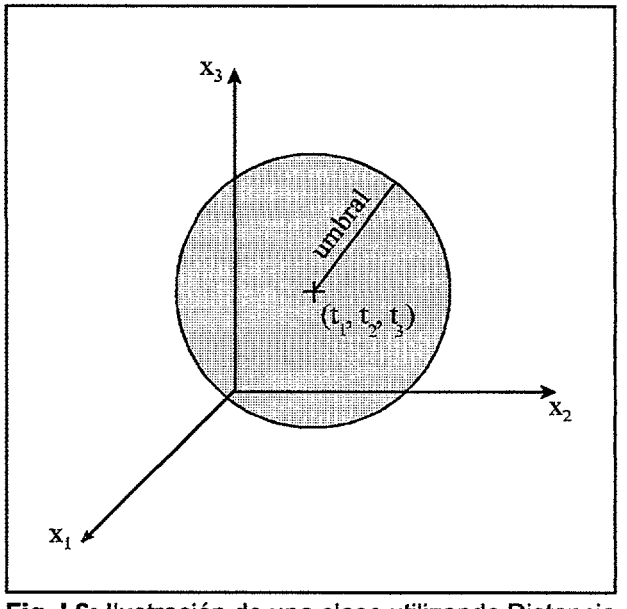


Fig. I.6: Ilustración de una clase utilizando Distancia Euclídea (caso tridimensional).

El umbral para la pertenencia, o no, de la muestra a la clase del usuario se define como el valor de la distancia que marca el límite de la clase.

I.4.3. DISTANCIA DE HAMMING

En este caso ([Ulg99], [Dau93]), la distancia no se mide como la diferencia entre las componentes de los vectores de características (la muestra y el patrón), sino como el número de componentes que son distintas (sin importar el valor de la diferencia). Bajo esta definición se pueden englobar dos casos claramente identificados:

- Si las componentes del vector de características son valores binarios: En ese caso, la distancia de Hamming se establece tal y como se ha indicado en la definición anterior,

es decir:

$$d = \frac{1}{L}\sum_{i=1}^{L} x_i \oplus t_i \qquad (I.2)$$

donde L es la longitud del vector de características, x_i es la componente i-ésima de la muestra y t_i es la componente i-ésima del patrón. Como patrón se toma la primera muestra, tratando que sea tomada con la mejor calidad, y el umbral, es decir, el número máximo de características que deben diferenciar, se toma de forma heurística.

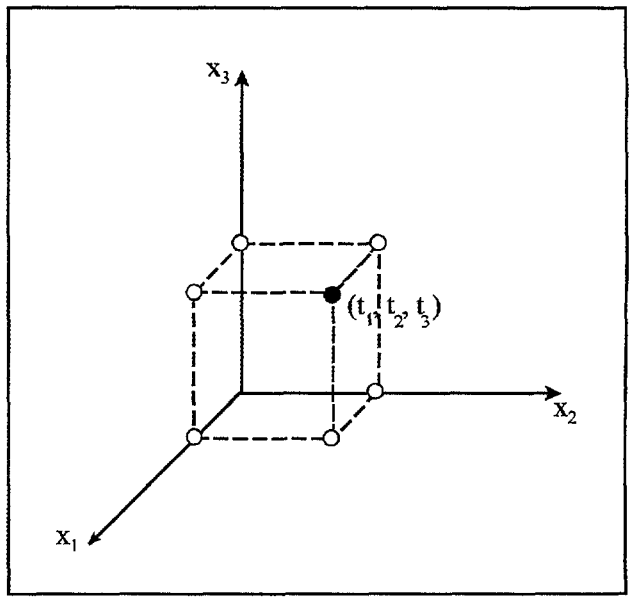


Fig. I.7: Ilustración de una clase utilizando la Distancia de Hamming (caso tridimensional).

- Si las componentes del vector de características no son valores binarios: En ese caso, para cada componente se establece un umbral, de forma que aquellas componentes que exceden ese umbral se cuentan como componentes distantes del patrón. El número de estas componentes es el que establece la distancia. Pueden existir muchos criterios a la hora de establecer esos umbrales, siendo uno de ellos, la desviación típica de la componente dentro de los vectores de características obtenidos en el reclutamiento. En este caso, el patrón se forma como el conjunto de una media de las distintas muestras, más las desviaciones típicas de cada una de las componentes, siendo entonces la distancia:

$$d(x_i, t_i^m) = \#\left\{ i \in \{1,\ldots,L\} / \left| x_i - t_i^m \right| < t_i^\sigma \right\} \qquad (I.3)$$

donde L es la longitud del vector de características, # es la función número de casos que se dan, x_i es la componente i-ésima de la muestra y t_i^m y t_i^σ son, respectivamente, la media y la desviación típica de la componente i-ésima del patrón. Tras este cálculo se verifica el umbral global de la distancia de Hamming, para saber si la muestra pertenece a la clase.

I.4.4. MODELADO POR MEZCLAS DE GAUSIANAS (GMM)

El método basado en Modelos de Mezclas de Gausianas (GMM[5]) aunque se basa en una teoría de hace unas décadas, ha recibido una gran expansión debido a su utilización en procesos de tratamiento de voz, tales como reconocimiento de locutores y análisis del habla. Su funcionamiento radica en modelar mediante funciones normales, cualquier función o distribución, a partir de unos datos de entrada (característica que la hacen familiar a las Redes Neuronales).

Desde el punto de vista matemático, los GMMs se explican como la función representada en la Figura I.8, en la que se puede ver que la densidad de una mezcla gausiana es una suma de M componentes sopesados por unas constantes c_i. Cada una de esas componentes es el resultado de aplicarle al vector $\vec{x}$, una determinada función b_i, la cual es, a su vez, función de unas medias (μ_i) y una matriz de covarianza (Σ_i).

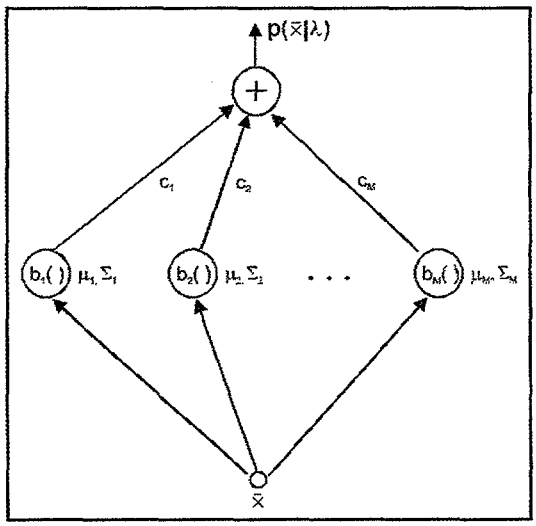


Fig. I.8: Arquitectura de un sistema GMM

Por lo tanto, un modelo de mezclas de gausianas λ se definirá unívocamente por su conjunto de c_i, de vectores μ_i y de matrices Σ_i.

La expresión matemática de b_i es:

$$b_i(\vec{x}) = \frac{1}{(2\pi)^{L/2}\left|\Sigma_i\right|^{1/2}} \exp\left\{-\frac{1}{2}(\vec{x}-\vec{\mu}_i)'\Sigma_i^{-1}(\vec{x}-\vec{\mu}_i)\right\} \qquad (I.4)$$

y por tanto, la densidad de probabilidad es:

[5] Al igual que con las tasas de error, se va a utilizar el acrónimo inglés por homogeneidad con la bibliografía existente, procedente de *Gaussian Mixture Models*. Las siglas en castellano serían MMG.

$$p(\vec{x}|\lambda) = \sum_{i=1}^{M} c_i b_i(\vec{x}) \qquad (I.5)$$

donde:

M es el número de mezclas que existen;

L es la dimensión del vector de entrada, que será igual a la dimensión del vector μ_i.

Sobre esta arquitectura inicial, se puede llegar a hacer determinadas simplificaciones, sobre todo referente a la matriz de covarianzas que, como se verá, tiene mucha importancia en el cálculo de este sistema. Dicha matriz se puede considerar tanto completa como diagonal. Estudios realizados por [Rey95] y [Ort96] en su aplicación a sistemas de voz, indican que utilizar matrices diagonales consigue resultados similares, si no mejores, que con matrices completas, reduciendo considerablemente el coste computacional. Por otro lado, se puede considerar la matriz como única para cada nodo, denominándose al sistema de *covarianza nodal*; única para cada usuario, denominándose de *covarianza total*; y por último, una única matriz para todos los usuarios, denominándose de *covarianza global*. Diversos autores utilizan diversas configuraciones, aunque parece casi descartada la covarianza global al suponer que la covarianza es característica de cada usuario. A partir de aquí, y por ser el criterio más aceptado ([Rey95], [Ort96], [Kam96]), se va a considerar el caso de covarianza diagonal y nodal.

Una vez analizada la estructura de un sistema GMM, se va a describir su funcionamiento. Los GMMs presentan muchas analogías con las redes neuronales (especialmente las de Función de Base Radial). Su funcionamiento radica en tres fases: ***inicialización***, ***entrenamiento*** y ***ejecución***.

I.4.4.a. Inicialización

La inicialización de estos sistemas es un punto, a priori, problemático. Principalmente radica en definir los siguientes valores:

- ***Número de mezclas M:*** Desgraciadamente no existe un método empírico para decidir el valor de M. Su valor se toma de forma heurística, teniendo en cuenta que, como regla general, con un valor de M superior se consiguen mejores resultados a costa de un mayor cálculo. Sin embargo esta tendencia puede verse enturbiada por factores externos como ruido en las muestras, etc.

- ***Valor de los pesos c_i:*** La práctica habitual es iniciarlos a $1/M$, debido a que la única

restricción que se pone a los pesos es que, en todo momento su suma debe ser igual a 1.

- ***Valor de las matrices de covarianza*** Σ_i**:** En el caso de covarianza diagonal y nodal, la inicialización normalmente aceptada es la de utilizar la matriz unidad.

- ***Valor de las medias*** μ_i**:** Este es el valor que más variaciones sufre en su inicialización por diversos autores. Sin embargo, los mismos autores confirman que el valor tomado en la inicialización no varía de forma considerable el resultado final obtenido, por lo que cualquiera de las soluciones propuestas se considera como aceptable. Estas propuestas son: tomar los M primeros vectores de entrada del entrenamiento; tomar M vectores de entrada elegidos aleatoriamente; realizar una inicialización de un Modelo Oculto de Markov y tomar dichos valores como entrada en la inicialización; entre otras. Por simplicidad se escogerá la opción de tomar M muestras de forma aleatoria. De aquí surge una de las primeras condiciones a nuestro sistema: para la inicialización el número de vectores de entrenamiento (T) debe ser mucho mayor que el número de mezclas (M).

I.4.4.b. Entrenamiento

La técnica de los GMMs es conocida desde hace varias décadas. Ya se encuentra referenciada en libros clásicos del reconocimiento de patrones como [Dud73]. El objetivo del entrenamiento radica en maximizar la función de máxima verosimilitud, la cual se expresa como:

$$p(X|\lambda) = \prod_{t=1}^{T} p(\vec{x}|\lambda) \qquad \textit{(I.6)}$$

Sin embargo, con la teoría de los GMMs no se habían conseguido unos resultados muy satisfactorios, ni se había extendido a otras ramas del conocimiento, por falta de un algoritmo de entrenamiento que diese unos resultados eficaces. Años después, se desarrolló el algoritmo EM (*Expectation and Maximization*) [McL97], que consiguió los resultados tan ansiados en la técnica de los GMMs. El funcionamiento de este algoritmo radica en maximizar la función de máxima verosimilitud en base a realizar dos pasos iterativamente, hasta conseguir el resultado deseado. Estos dos pasos son:

- **Paso E (*Expectation*):** Su misión es calcular la probabilidad *a posteriori* de cada una de las mezclas y para cada uno de los vectores de entrada del entrenamiento, mediante la ecuación:

$$p(i|\vec{x}_t,\lambda)=\frac{c_i b_i(\vec{x}_t)}{\sum_{k=1}^{M} c_k b_k(\vec{x}_t)}, \quad \begin{matrix}1\le i\le M\\ 1\le t\le T\end{matrix} \tag{I.7}$$

- **Paso M (Maximization):** Donde se actualizan cada uno de los parámetros del modelo, para maximizar la función de máxima verosimilitud. Los valores de los pesos, medias y varianzas, pasan a ser (los valores con circunflejo, ^, representan los valores nuevos):

$$\hat{c}_i=\frac{1}{T}\sum_{t=1}^{T} p(i|\vec{x}_t,\lambda) \tag{I.8}$$

$$\hat{\vec{\mu}}_i=\frac{\sum_{t=1}^{T} p(i|\vec{x}_t,\lambda)\cdot\vec{x}_t}{\sum_{t=1}^{T} p(i|\vec{x}_t,\lambda)} \tag{I.9}$$

$$\hat{\sigma}_i^2=\frac{\sum_{t=1}^{T} p(i|\vec{x}_t,\lambda)\cdot(\vec{x}_t-\hat{\vec{\mu}}_i)(\vec{x}_t-\hat{\vec{\mu}}_i)'}{\sum_{t=1}^{T} p(i|\vec{x}_t,\lambda)} \tag{I.10}$$

Con respecto a la estimación de la varianza, hay que tener en cuenta que suele darse un problema de singularidades en la matriz de covarianza, por lo que normalmente el valor de las varianzas se limita por debajo, es decir, se establece un σ^2_{min} por debajo del cual no se permite el valor de las varianzas. Por otro lado, diferencias entre los vectores x y μ grandes, pueden dar lugar a valores del argumento de la exponencial de b_i muy grandes, y por lo tanto, valores de b_i prácticamente nulos, por lo que resulta recomendable hacer una normalización de los vectores de entrada.

Estos dos pasos se ejecutan iterativamente hasta que se logre un umbral de finalización, como puede ser que la diferencia entre las medias anteriores y las estimadas esté por debajo de un determinado valor.

I.4.4.c. Ejecución

Una vez entrenado el modelo perteneciente al usuario, se puede entrar en fase de ejecución. En esta fase, se toma una muestra del mismo y se introduce en el modelo calculándose la función de máxima verosimilitud, comparando el valor resultante con un umbral.

I.5. ESTADO DEL ARTE AL INICIO DE LOS TRABAJOS

A la hora de iniciar los trabajos que han conducido a la realización de esta Tesis, es decir 1996, existían diversos trabajos realizados sobre Tarjetas Inteligentes y sobre Biometría. Sin embargo, pocos de ellos unían las dos técnicas, y los que habían surgido intentando incorporar la tecnología de las tarjetas con biometría, se basaban en utilizar aquellas como elemento identificativo de su titular o, como mucho, utilizarlas como simple soporte de almacenamiento del patrón. Por tanto, para poder realizar una mejor explicación del estado del arte en aquel momento, se van a plasmar los distintos logros separando en distintos apartados la situación relativa a biometría y la relacionada con tarjetas.

I.5.1. SITUACIÓN DE LA BIOMETRÍA

A la fecha de inicio de los trabajos, existía mucha documentación de índole científico sobre diversas técnicas biométricas. En particular, era muy intensa la investigación sobre sistemas basados en voz, huella y rostro. También fueron apareciendo en el mercado múltiples sistemas de autenticación o reconocimiento biométrico, donde destacan fundamentalmente los sistemas basados en huella dactilar.

Haciendo una exposición por técnicas, el estado en el que se encontraban, en 1996, las técnicas biométricas más relevantes era:

- **Huella:** Debido a su gran utilización por parte de la policía internacional desde comienzos de siglo, los distintos parámetros que caracterizan la identidad de una persona se encontraban muy estudiados, de forma que incluso existían amplios tratados sobre clasificación de las mismas para su localización en los archivos policiales. Desde el punto de vista de los sistemas automáticos, en 1996 existían varios sistemas de captura de huella, fundamentalmente basados en cámara de vídeo (aunque empezaban a emplearse algunos basados en otras técnicas más avanzadas, y que proporcionaban fácil detección de dedo vivo). También, numerosos documentos científicos habían aparecido, donde hay que destacar, por su continuidad en los últimos años, los del grupo de trabajo de A. K. Jain ([Kar96], [Jai97a], [Jai97b], etc.). En cuanto a sistemas implantados de forma comercial, eran numerosos los implantados en Estados Unidos para su utilización gubernamental, así como el control de identidad de los inmigrantes en Alemania y el inicio del proyecto de Tarjeta de Afiliado a la Seguridad Social, en España.

- **Voz:** En la década de los 70 se inició una proliferación de artículos científicos sobre sistemas de reconocimiento por voz, al mismo tiempo que se investigaba en temas relativos a reconocimiento del habla y a síntesis de voz. Sin embargo, muy alejado de los éxitos conseguidos por estas dos últimas técnicas, a fecha de hoy no se ha llegado a unas conclusiones definitivas sobre qué parámetros de la voz son los que realmente identifican a la persona de una forma única y estable, eliminando factores debidos al canal, a enfermedades, a la edad, etc. Independientemente de esta falta de conocimiento, se han ido desarrollando sistemas que proporcionan un relativamente alto nivel de éxito en laboratorio. Varios de esos sistemas se han ido comercializando, siendo su aplicación más importante, la verificación secundaria en sistemas de Banca Telefónica.

- **Iris:** Se puede plantear el origen de esta técnica con la publicación, en 1993, del artículo de Daugman [Dau93] (tal y como se verá en el capítulo correspondiente). Ese trabajo condujo a que su autor patentara el sistema y crease una empresa con el objetivo de desarrollar y licenciar esa patente. Pero no será hasta principios de 1998, que consiga sacar sus productos al mercado vinculándolos con sistemas de alta seguridad y autenticación de usuarios en Cajeros Automáticos Bancarios. Con respecto a trabajos de otros autores, se ha detectado alguna orientación nueva, pero ninguna con la calidad y el éxito de Daugman.

- **Firma:** Al ser una de las técnicas, al igual que huella, con gran tradición e incluso validez legal, han existido numerosos intentos de plasmar esta solución desde el punto de vista de un sistema automático de identificación. Sin embargo, su limitada

aplicabilidad, y la desconfianza frente a falsificaciones, ha hecho que este sistema no se implante como método de autenticación de usuarios frente a un sistema. En contra, como sistema de reconocimiento, ha sido mundialmente extendido entre bancos y centros de seguros, donde se verifica la firma de un usuario con todas las almacenadas en la base de datos de la compañía.

- **Mano:** Aunque ha aparecido publicado en [Jai99a] un capítulo divulgativo sobre el sistema de la empresa *Recognition Systems*, no se ha encontrado publicación científica alguna sobre esta técnica. Por lo aparecido en dicho capítulo, el sistema se encuentra patentado desde principio de los años 70, pero no ha sido hasta mediado de los 90 que su implantación comercial haya tenido éxito. Pero el éxito comercial conseguido por dicha empresa, ha sido muy superior al de cualquier otra técnica biométrica.

En España, olvidando la compra de sistemas extranjeros, los trabajos han estado especialmente centrados en sistema basados en voz, algún trabajo aislado sobre huella dactilar, y la investigación sobre reconocimiento facial. Desde el punto de vista comercial, y tal como se ha comentado anteriormente, el hecho más significativo fue la decisión de utilizar un sistema de autenticación por huella dactilar para la Seguridad Social en Andalucía.

Dentro del Grupo Universitario de Tarjeta Inteligente, perteneciente al Departamento de Tecnología Fotónica de la E.T.S.I. de Telecomunicación de Madrid, los trabajos relativos a Biometría hasta 1996 se restringieron a mantener un contacto continuo con los resultados obtenidos internacionalmente, y a la asesoría dentro del proyecto anteriormente mencionado de la Seguridad Social en temas de verificación de huella y firma.

I.5.2. SITUACIÓN EN LA INDUSTRIA DE TARJETA INTELIGENTE

Desde que a principios de los años 70 se produjera en Francia y Japón la aparición de la Tarjeta de Circuito Integrado, su evolución tecnológica ha seguido, durante su primera década, a la evolución de la microelectrónica. Sin embargo, a partir de los inicios de la década de los 90, el coste de las tarjetas (teniendo en cuenta que su principal competidor era la tarjeta de banda magnética, con un coste más de 10 veces inferior), frenó su evolución, quedándose estancadas con las siguientes características fundamentales:

- Estructura de Datos Jerárquica.

- Protección de datos mediante jerarquía de claves.
- Mecanismos de Autobloqueo y Autodestrucción.
- Algoritmos de cifrado simétrico (DES).
- 2 Kbytes de memoria EEPROM.

No será hasta prácticamente los inicios de esa Tesis (finales de 1995), que se empezó a ver la necesidad de crear tarjetas con nuevas características. Especialmente el empuje vino dado por las aplicaciones de criptografía pública (creación de tarjetas criptográficas con RSA), tanto para procesado de los algoritmos, como para el almacenamiento de las claves de dichas tarjetas, siendo esta última necesidad la que sirvió de catalizador para que se expandiera el incremento de memoria al resto de los modelos de tarjetas (se empezaban a ver tarjetas de 4KB y a plantear la necesidad futura de llegar a los 8KB).

Toda esta evolución se dio en Europa, siendo bastante paradójico el poco interés de la industria y comunidad científica de EE. UU. por esta tecnología. En esa evolución tuvo un papel principal países como Francia y Alemania, siendo la contribución española muy alta, especialmente a partir de 1987. Fue precisamente en esa fecha cuando, basándose en un proyecto de investigación con el Instituto Tecnológico Bull, el profesor D. José Luis Zoreda creó el Grupo Universitario de Tarjeta Inteligente, convirtiéndose desde entonces este Grupo en un punto de referencia indispensable dentro de la industria de la Tarjeta Inteligente en España.

Las aplicaciones desarrolladas a nivel mundial sobre Tarjetas Inteligentes han sido muy variadas. Desde bancarias hasta telecomunicaciones, pasando por sanitarias y de fidelización. Sin lugar a duda, la aplicación que más ventas está proporcionando es la de telefonía móvil digital GSM, seguida por las bancarias (en forma de Monedero Electrónico).

I.6. CONCLUSIONES

A lo largo de este capítulo se ha intentado dar una visión general de la problemática de la Biometría, así como de la de las Tarjetas Inteligentes. También se ha intentado plasmar los métodos y esquemas que se van a utilizar en capítulos posteriores, y mostrar la situación en la que se encontraba la técnica en los inicios de los trabajos expuestos aquí.

Todo esto se ha intentado hacer con el objeto de facilitar al lector la comprensión de los posteriores capítulos, creándole un conocimiento base que le permita entenderlos de una forma

más completa. Sin lugar a dudas hay que ser conscientes que en estas pocas páginas no se puede resumir todo el trabajo reflejado en multitud de libros, por lo que se le sugiere al lector interesado en alguno de los temas expuestos, que se refiera a las obras de referencia indicadas.

CAPÍTULO II:

RECONOCIMIENTO DE LOCUTORES

En el presente capítulo se va iniciar la exposición de las distintas técnicas biométricas que se han estudiado en el transcurso de esta Tesis, cada una de las cuales ocuparán su capítulo correspondiente. Por tanto, se va a comenzar con la técnica de verificación biométrica mediante voz, conocida normalmente como Reconocimiento de Locutores. La característica fundamental de esta técnica, desde el punto de vista de iniciar un desarrollo, es la gran cantidad de documentación existente. Desde hace varias décadas, se ha tratado de abordar este problema, al mismo tiempo que se estudiaban otras técnicas basadas en la voz, como el Reconocimiento del Habla o la Síntesis de Voz. Como se verá, la cantidad de alternativas tomadas para intentar abordar el problema del Reconocimiento de Locutores es muy amplia. Desgraciadamente, a fecha de hoy, los resultados no son tan satisfactorios como los que la comunidad científica demandaba, quedando, pues, mucho camino por recorrer.

La estructura de este capítulo va a iniciarse con un primer apartado introductor donde se establecerán las bases de conocimiento necesarias para una posterior comprensión del resto de apartados. Seguirá un apartado dedicado a la Captura y el Pre-procesado de la señal de voz, para continuar con un apartado dedicado a los métodos de extracción de características empleados. Posteriormente, un apartado revelará el método de verificación utilizado, detallando los resultados obtenidos y se finalizará el capítulo con las conclusiones obtenidas.

II.1. LA VOZ COMO HERRAMIENTA PARA RECONOCER

Antes de comenzar con la exposición de los métodos empleados y los resultados obtenidos, es necesario ahondar un poco en la naturaleza de las características biométricas que se van a utilizar, así como de los trabajos anteriormente realizados dentro de la comunidad científica. De esta forma se podrá comprender más fácilmente los desarrollos realizados, así como los diversos métodos que se pueden utilizar para afrontar esta tarea.

Se comenzará, por tanto, con una breve explicación a la fisiología involucrada en la producción de voz, comentando los distintos tipos de sonidos que pueden obtenerse. Posteriormente se hablará de los sistemas de Reconocimiento de Locutores, comentando sus propiedades fundamentales y las aplicaciones más aceptadas.

II.1.1. EL ORIGEN DE LA VOZ

La voz se genera en el *aparato vocal*, el cual consta principalmente de *pulmones*, *traquea*, *laringe* y los *conductos nasales* y *vocales* (figura II.1). En la laringe se encuentran las ***cuerdas vocales*** que, mediante su movimiento de separación y acercamiento permiten que el aire salga por el espacio dejado entre ellas, denominado *glotis*. De las cuerdas vocales, parte el ***conducto vocal***, que se puede considerar como un tubo acústico no-uniforme de aproximadamente 17 cm de longitud para un hombre adulto, el cual termina en los labios. El área de su sección transversal puede ser variada de 0 a unos 20 cm^2 mediante el control muscular de los articuladores del habla (*labios*, *lengua*, *mandíbula* y *velo*). El ***conducto nasal*** también es un conducto acústico no-uniforme de área y longitud fija, y se encuentra delimitado en un extremo por los *orificios nasales* y en otro por el

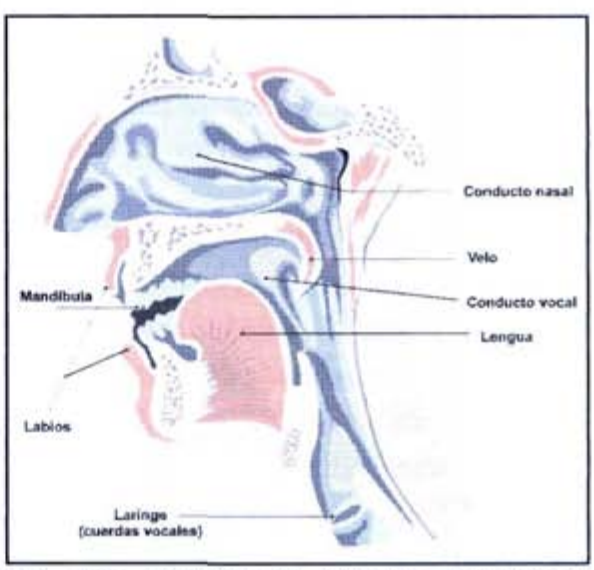


Fig. II.1: Sección del Sistema Respiratorio encargada de la producción de voz.

velo, el cual controla el acoplamiento entre el conducto nasal y el oral, de forma que si el sonido es no-nasal, sólo deja pasar el aire a través de los labios, mientras que si es nasal, deja pasar el aire a través de ambos conductos.

Una vez comprendido someramente el aparato vocal, se puede entender el principio de producción de voz. Éste empieza llenando los pulmones de aire, el cual se expulsa a lo largo de la tráquea, a través de la glotis. Este flujo de aire es la fuente de energía de la producción de voz, la cual puede ser controlada de distintas maneras para producir distintos modos de excitación. Según el modo de excitación, la señal de voz puede ser clasificada en las siguientes categorías:

a. Sonidos sonoros: Si durante la expulsión de aire, se tensan las cuerdas vocales de forma que se cierre la glotis, se obliga al aire a abrir la glotis, provocando una excitación periódica (o casi-periódica) de las cuerdas vocales, lo cual produce una modulación de la energía expulsada. La señal de salida tiene un espectro rico en armónicos de la denominada **frecuencia fundamental** (también conocida como ***pitch***). Esta frecuencia tiene un valor de 50-250 Hz para los hombres, mientras que para las mujeres el límite superior es aproximadamente de 500 Hz. Tras las cuerdas vocales, el tracto vocal actúa como una cavidad resonante que atenúa o amplifica los sonidos producidos.
b. Sonidos sordos: En estos sonidos las cuerdas vocales no vibran. Las variaciones en los sonidos se producen por variaciones de tamaño de la sección transversal del conducto oral, ya sea por cierre leve de la glotis, aproximación de lengua y mandíbula, etc. Desde el punto de vista del espectro, este tipo de sonidos se puede considerar como ruido aleatorio.
c. Sonidos explosivos: Pudiendo ser tanto sordos como sonoros, este tipo de sonidos se diferencia principalmente por el cierre, en algún punto, del conducto vocal, produciéndose repentinamente la apertura del mismo.

El hecho de que tanto la frecuencia fundamental de las cuerdas vocales, como las dimensiones del tracto vocal modifiquen significativamente el sonido, induce a pensar que la voz contiene información propia de la persona que habla, y por tanto, que puede ser utilizada como fuente de un sistema de verificación biométrica. De hecho, el oído y el cerebro tienen entrenado un sistema de estas características, de forma que es posible la identificación de una persona mediante la simple escucha de su voz, incluso a través de canales de limitado ancho de banda, como, por ejemplo, el teléfono.

Sin embargo, aunque existe una determinada información biológica, en el reconocimiento de locutores entran a formar parte también variables del comportamiento y la educación de la persona, lo que hace que a esta técnica biométrica se la considere como un híbrido entre las

basadas en parámetros biológicos y las basadas en el comportamiento. Por otro lado, esta técnica sufre de multitud de variaciones en sus características, debidas a actores externos como pueden ser, el clima, las enfermedades, la edad, etc. He aquí donde radican la mayor parte de los problemas que encuentra esta técnica, ya que tras muchos años de estudio, todavía no se ha llegado a aislar todos estos factores.

II.1.2. SISTEMAS DE RECONOCIMIENTO DE LOCUTORES

A la hora de definir un sistema de verificación biométrica a través de Reconocimiento de Locutores, se ha de elegir entre dos configuraciones:

a. Texto dependiente: En un sistema de estas características, tanto el texto del cual se ha extraído el patrón, como los textos usados para verificación han de ser el mismo. En un sistema de este tipo se toman tanto las características de la persona que habla, como las del texto pronunciado.

b. Texto independiente: En esta configuración, los textos pronunciados para extraer el patrón y para realizar la verificación no tienen por qué ser los mismos. De hecho, en fase de extracción del patrón, el texto utilizado ha de ser habla continua y en varias sesiones, para captar el mayor número de características propias de la persona, eliminando aquellas dependientes del texto.

Cada una de las dos configuraciones presenta unas ventajas y unos inconvenientes. Básicamente, las técnicas basadas en texto dependiente son de menor computación y con unos resultados mejores que las basadas en texto independiente. Sin embargo, las técnicas basadas en texto dependiente son más susceptibles de fraude, puesto que se puede grabar la voz de la persona al recitar el texto fijo, mientras que en las de texto independiente, al ser el texto variable, no existe limitación a la hora de que el sistema le solicite al usuario el texto a recitar. Para subsanar la deficiencia que presentan los sistemas basados en texto dependiente, se hace que el texto con el que se obtiene el patrón y se hace la verificación sea una única palabra, la cual se inserta en un texto más amplio que es el que se le solicita pronunciar al usuario. Evidentemente, y aunque no es un tema que se vaya a tratar aquí, siempre será necesario un sistema de Reconocimiento de Habla, para verificar que el texto relatado es el que el sistema ha solicitado.

Una vez introducida esta técnica biométrica y antes de pasar al estudio de cada una de las fases, se van a analizar sus propiedades principales, así como las aplicaciones donde esta técnica

es susceptible de ser incorporada.

II.1.2.a. Propiedades

Las principales propiedades de esta técnica se van a dividir en aquellas que suponen una ventaja frente a otras técnicas y aquellas que suponen un inconveniente. Desde el punto de vista de las ventajas, éstas son:

- No tiene excesivas connotaciones legales, por lo que la reticencia a su uso por estos motivos no es apreciable.
- Su gran ventaja reside en que es una técnica muy barata, puesto que sólo necesita de periféricos exteriores un micrófono y una tarjeta de sonido.
- Al tratarse de señales unidimensionales, sus tiempos de cálculo, son inferiores a otras técnicas (para una complejidad de algoritmos análoga).
- Es una técnica bastante fácil de usar, relativamente conocida y en la que no hay interacción entre usuarios, con lo que es susceptible de aportar una gran aceptación por parte de los usuarios.

Por otro lado, sus inconvenientes principales son:

- Se trata de una técnica biométrica dependiente no sólo de parámetros físicos, sino también de parámetros basados en el comportamiento. Esto, a priori, puede resultar una desventaja, ya que, el patrón cambiará fácilmente con el tiempo (debido a cambios en el comportamiento del usuario), y los parámetros de comportamiento podrían llegar a ser simulados.
- Determinadas enfermedades pueden afectar seriamente a la producción de voz, por lo que pueden introducir artefactos en las muestras que provoquen aumentos en la FRR[6].
- Se han realizado numerosos intentos, muchos de ellos con éxito, de implementar esta técnica basándose en métodos muy distintos. Esto hace que la información existente sea muy numerosa, y en ocasiones contradictoria. Cada uno de los métodos ofrece unas características particulares que hacen que el tamaño del patrón, así como el coste computacional sea muy variable de uno a otro.
- El usuario puede sufrir de una falta de confianza frente a esta técnica debido a susceptibilidades de grabación o mímica de su propia voz.
- En muchos entornos (refiérase al siguiente subapartado) los usuarios, y sobre todo en

[6] El concepto de Tasa de Falso Rechazo (FRR) ya ha sido introducido en el Capítulo I.

diversos sectores de la población, puede ocurrir que no se tome este tipo de sistemas con naturalidad, y por consiguiente que se forme una especie de *"efecto Karaoke"*, en el que se junte el texto con risas, timideces, dudas, etc.

II.1.2.b. Aplicaciones

A priori, esta técnica es susceptible de ser incorporada en cualquier aplicación de control de accesos y seguridad. Sin embargo, el rechazo a su uso puede ser muy alto en entornos donde no se produce el acto de hablar de una forma natural, tal y como se ha indicado en el último punto de las propiedades. Poniendo un ejemplo, si se utiliza este sistema en el control de acceso a una habitación, el usuario tiene que acostumbrarse a pararse enfrente de la puerta, mirar el texto a recitar, recitarlo y después entrar. Esta aplicación le resulta incómoda al usuario, y aunque esa incomodidad puede ocurrir en otras técnicas, en esta se hace especialmente preocupante, ya que el usuario tenderá a recitar el texto con aburrimiento y dejadez, con lo que la señal recogida puede hacer que se eleve la FRR. Por otro lado, como ya se verá en posteriores apartados, durante la fase de entrenamiento de algunos de los métodos, el usuario debe hablar durante, al menos, un minuto, de habla contínua, lo que realmente resulta difícil en un entorno artificial (es decir, cuando no es una conversación natural).

Sin embargo, si este sistema se integra en una aplicación en la que normalmente se habla, la aceptación del usuario puede ser total. Tómese por ejemplo el caso de una aplicación de banca telefónica. La toma de la señal de voz del usuario se hace mediante una conversación natural entre dicho usuario y la operadora. Por tanto, el usuario nunca es realmente consciente de que se está produciendo esa verificación, y sobre todo, nunca tiene la sensación de pérdida de tiempo para acceder a sus cuentas, por lo que el habla de dicho usuario es siempre natural y puede además ser suficientemente larga la conversación para producir, incluso, el entrenamiento.

Por lo tanto, las aplicaciones para las que se considera adecuada esta técnica son:

- Sistemas de identificación por teléfono, como por ejemplo Banca Telefónica.
- Sistemas informáticos con introducción de datos por voz, como un PC con conversor texto-voz para introducir texto de documentos. De esta forma se asegura que el que introduce los datos es la persona que realmente puede hacerlo.
- Escuchas judiciales e identificaciones forenses.
- Sistemas de presencia mediante identificación de habla.
- y todas aquellas aplicaciones en donde el usuario no sea consciente de estar hablando exclusivamente para su identificación.

II.2. CAPTURA Y PREPROCESADO

Como ya se ha dicho, una de las mayores ventajas de este sistema es lo barato que resulta debido al bajo coste de los dispositivos de captura. A grandes rasgos, lo único que se necesita es un micrófono, un preamplificador, un filtro de entrada, un conversor analógico-digital y un oscilador que le de la frecuencia de muestreo al conversor. Si se tiene en cuenta que en algunos sistemas, como por ejemplo la Banca Telefónica, algunos de esos sistemas ya se encuentran implícitos instalados (micrófono, preamplificador y filtro), el coste disminuye aún más.

Entrando más en profundidad, hay que tener en cuenta que el ancho de banda de la señal de voz se estima en unos 10 kHz [Owe93]. Sin embargo, la mayoría de la información se encuentra por debajo de los 5 kHz, y de hecho, en aplicaciones telefónicas, el ancho de banda se limita a 3,3 kHz. Esto implica que, manteniendo las restricciones del teorema de Nyquist, la frecuencia de muestreo debe ser superior a 6,6 kHz. En realizaciones prácticas de estos sistemas, la frecuencia de muestreo se suele tomar de 8 kHz, y si es necesario, posteriormente se hace un filtrado y un re-muestreo, para reducir el número de datos a incorporar al sistema.

En el proceso de digitalización de la frase, se produce una cuantificación de la señal proveniente del micrófono. Esa cuantificación se puede realizar respecto a distintos formatos normalmente aceptados (PCM, ADPCM, ley-A, ley-μ, etc.). Según diversos autores ([Cam97], [Dod85], [Fur91]), la cuantificación elegida no afecta en gran medida al sistema de reconocimiento de locutores, siendo la más utilizada la ADPCM.

Una vez digitalizada la señal acústica, hay que detectar el inicio de la frase. Para ello se hacen tomas periódicas del nivel de ruido existente, y mediante medida de la energía de la señal, se detecta el inicio de la señal de voz mediante un umbral que depende del valor de ruido existente. Para evitar ruidos espúreos de alta intensidad que puedan confundir al sistema, se utilizan ventanas de una longitud de, por ejemplo, 50-100 ms, para medir la energía.

Tras haber detectado el inicio de la frase, el nivel de ruido se puede utilizar para eliminar aquellos fragmentos acústicos en los que no haya voz (separación entre palabras), o para detectar el final de la frase pronunciada. De esta forma, se reduce tanto el coste computacional del sistema, como la probabilidad de fallo por procesamiento de señal sin información del locutor.

El último paso del preprocesado, es la aplicación de un filtro de pre-énfasis. Este filtro se utiliza para compensar la atenuación de 6 dB/octava producida por la combinación de la atenuación de 12 dB/octava producida en la excitación de voz, y la amplificación de 6 dB/octava dada por la radiación de la boca. La función de transferencia de este filtro, así como el valor utilizado, siguiendo los trabajos de [Fur81] es:

$$H(z) = 1 - az^{-1} = 1 - 0.95z^{-1} \qquad \textit{(II.1)}$$

Por último, para ayudar en las etapas posteriores, se puede hacer un proceso de amplificación de la señal para aprovechar todo el margen dinámico que ofrece nuestro sistema.

II.3. EXTRACCIÓN DE CARACTERÍSTICAS

Las características de la voz que mejores resultados están dando en sistemas de reconocimiento de locutores, son los coeficientes cepstrum, además de su variación (expansión polinomial, o coeficientes polinomiales) y los coeficientes mel. Cada modelo de sistema de reconocimiento de locutores, en sus algoritmos, utiliza alguna o varias de estas características, por lo que se va a hacer un estudio de dichas características independiente del método de verificación.

La extracción de características se realiza por fragmentos de voz, de tal forma, que la frase entera se divide en diversos fragmentos, denominados ventanas, y solapando ventanas entre sí, de forma que lo que se obtiene al final es un conjunto de vectores de características, que nos da la variabilidad temporal de cada una de las características durante el transcurso de la frase. La ventana utilizada normalmente es una **ventana de Hamming**, de duración entre 20 y 30 ms, y solapándolas cada 10 ms. La función de la ventana de Hamming es:

$$w[k+1] = 0{,}54 - 0{,}46\cos\left(2\pi\frac{k}{n-1}\right), \quad k = 0,\ldots,n-1 \qquad \textit{(II.2)}$$

Por tanto, la señal de voz pre-procesada, se toma en fragmentos de duración igual al tamaño de la ventana, cada 10 ms, multiplicando cada uno de éstos por la ventana *w*. Posteriormente se pasa cada uno de estos fragmentos por cada uno de los algoritmos de extracción

de características.

II.3.1. COEFICIENTES CEPSTRUM

La formulación original de los coeficientes cepstrum de una señal x, son los coeficientes resultantes de aplicar:

$$c = FFT^{-1}(\log|FFT(x)|) \tag{II.3}$$

Sin embargo, suele ser muy habitual utilizar los denominados ***coeficientes cepstrum de predicción lineal (LPCC)***, que son el resultado de extraer de la señal x un determinado número de coeficientes de predicción lineal (LPCs), y a partir de esos coeficientes extraer los cepstrum mediante el siguiente algoritmo recursivo ([Fur81]):

$$\begin{aligned} c_1 &= a_1 \\ c_n &= \sum_{k=1}^{n-1}\left(1-\frac{k}{n}\right)a_k c_{n-k} + a_n, \quad 1 < n \leq p \end{aligned} \tag{II.4}$$

donde c_i es el coeficiente cepstrum de orden i; a_i es el coeficiente de predicción lineal de orden i; y p es el número de coeficientes de predicción lineal extraidos.

II.3.2. COEFICIENTES POLINOMIALES

Los coeficientes polinomiales ([Fur81]) surgen como una necesidad de utilizar, no sólo los coeficientes cepstrum, sino también su media y su variación de primer y segundo orden. Para utilizarlos se vuelve a definir otra ventana de tiempo, por ejemplo 90 ms, y se toma por separado cada coeficiente cepstrum, y sus valores durante esa ventana. Es decir, para un coeficiente cepstrum extraído c_i, se toma ese coeficiente y los 8 siguientes (para que sean 90 ms), y se le

aplica las siguientes ecuaciones:

$$\alpha = \left(\sum_{j=1}^{9} c_{i_j} \right) \Big/ 9$$

$$\beta = \left(\sum_{j=1}^{9} c_{i_j} P_{1j} \right) \Big/ \sum_{j=1}^{9} P_{1j}^2 \qquad \gamma = \left(\sum_{j=1}^{9} c_{i_j} P_{2j} \right) \Big/ \sum_{j=1}^{9} P_{2j}^2$$

$$\textit{donde:} \quad P_{0j} = 1 \qquad P_{1j} = j - 5 \qquad P_{2j} = j^2 - 10j + \frac{55}{3} \tag{II.5}$$

El coeficiente α representa la media, el coeficiente β la pendiente, y el γ la curvatura de los coeficientes cepstrum. Normalmente el coeficiente α no se suele considerar, debido a que se obtiene mayor información con los propios coeficientes cepstrum.

II.3.3. COEFICIENTES MEL

Recientemente se ha descubierto que los coeficientes cepstrum se ven muy afectados por el ruido. Es por esto que han aparecido nuevas tendencias en extracción de características. Una de esas tendencias que está dando muy buenos resultados es extraer los coeficientes ceptrales derivados de un banco de filtros frecuencia-mel. Su funcionamiento radica en realizar un cambio de frecuencia de los datos resultantes del log|FFT(x)|, mediante la fórmula:

$$mel(f) = 2595 \log_{10}\left(1 + \frac{f}{700}\right) \tag{II.6}$$

Una vez realizada la transformación, se enventana mediante funciones triangulares uniformes y solapadas en la mitad, con un determinado número de ventanas, por ejemplo 20. Se suma todos los valores correspondientes de una ventana, y con ello se obtiene, mediante la siguiente transformación de coseno, los coeficientes cepstrum.

$$c_i = \sum_{j=1}^{v} m_j \cos\left(\frac{\pi i}{v}(j-0.5)\right), \quad 1 \le i \le p \qquad \textit{(II.7)}$$

donde c_i es el coeficiente cepstral de orden i; m_j es la suma de todas las componentes de la ventana j; v es el número de ventanas triangulares; y p es el número de coeficientes cepstrales a extraer.

II.4. MÉTODOS DE VERIFICACIÓN

Son muy variados los métodos de verificación de locutores que existen en la actualidad. Cada uno de esos métodos utiliza procedimientos matemáticos muy distintos de los demás. Basándose en trabajos realizados por otros autores como [Dod85], [Fur91], [Ros92], [Gis94] y [Cam97], se puede establecer una relación de los métodos más utilizados:

- ***Dynamic Time Warping (DTW):*** Es una técnica considerada bastante antigua ([Fur81]), especialmente diseñada para texto-dependiente, donde la frase pronunciada, tras su extracción de características, se compara con el patrón almacenado, después de haber realizado un ajuste temporal dinámico entre ambos vectores. Sus requisitos en cuanto a coste computacional no son excesivos. Sin embargo, sus requisitos en cuanto almacenamiento, aunque mucho menos exigentes que los de otras técnicas, implican que el patrón del usuario sea el conjunto de características de cada sección de la muestra a ser verificada. Esto implica que la memoria a ser reservada dentro de la tarjeta, para el almacenamiento del patrón, exceda la capacidad de la misma. Por esta razón esta técnica ha sido descartada.

- ***Cuantificación de Vectores (VQ):*** Es una técnica utilizada principalmente en texto-independiente. Sus resultados son muy satisfactorios aunque los requisitos de almacenamiento que presenta han hecho que se rechace para una posible integración con Tarjetas Inteligentes. Su funcionamiento ([Ort96]), a grandes rasgos, radica en proyectar un vector sobre un conjunto finito de representaciones vectoriales. Los vectores representantes de cada clase se les denomina centroides o *codewords*, y al conjunto de centroides se le denomina *codebook*. Para paliar distintos problemas de

esta técnica, como la falta de memoria de eventos anteriores, se han desarrollado otras técnicas como *Cuantificación de Matrices* (*MQ*, [Jua90]), *Filler Template* ([Hig86]) o *Acoustic Segment Quantization* ([Sve87]).

- ***Modelos Ocultos de Markov (HMM):*** Se trata de un modelo que trata las señales de voz como señales estocásticas. Se establecen un determinado número de estados, donde cada estado corresponde a un evento observable de forma determinista. Este modelo puede funcionar tanto en un sistema de texto-dependiente ([Ros90]), como de texto independiente ([Mat91]). Los resultados obtenidos hasta la fecha han sido realmente buenos, pero este modelo sufre de un gran coste computacional, sobre todo en la fase de entrenamiento. Este gran problema, y la aparición de otros métodos alternativos, como los GMMs (véase siguiente punto), han hecho que este modelo se empiece a abandonar por otros, al obtenerse resultados similares con menor coste computacional.

- ***Modelos de Mezclas de Gausianas (GMM):*** Aunque se trata de una teoría de reconocimiento de patrones conocida desde hace tiempo, la falta de un algoritmo óptimo de entrenamiento no ha posibilitado su expansión hasta hace poco. En 1995 ([Rey95]) se empezó a utilizar en el Reconocimiento de Locutores. Su filosofía es análoga a la de los HMMs, pero consiguiendo unos resultados similares con un cálculo más sencillo. Este factor y los requisitos de memoria, potencialmente admisibles, han hecho que este método sea estudiado con más detalle, con intención de ser utilizado en texto-independiente con una Tarjeta Inteligente.

- ***Redes Neuronales:*** Dada la popularidad que están obteniendo la teoría de Redes Neuronales, han empezado a aparecer numerosos intentos de realizar sistemas de reconocimiento de locutores en base al Perceptrón Multicapa (MLP, [Ogl90]), o a Funciones de Base Radial (RBF, [Ogl91]). Sin embargo, tal y como se ha introducido en el Capítulo I, los sistemas de reconocimiento de patrones basados en Redes Neuronales, tienen la limitación de que en su entrenamiento no sólo hay que indicar los vectores que dan una respuesta afirmativa, sino que también hay que indicar vectores que deben dar respuesta negativa, lo cual implica la existencia, *a priori*, de una base de datos de usuarios a "no-verificar". Por otro lado, aunque no es una limitación muy grande en el caso de RBF, con el MLP, cuando se introduzca un nuevo usuario en el sistema, habría que re-entrenar cada una de las redes de cada usuario, lo cual no resulta viable en un sistema de Verificación Biométrica mediante Tarjeta Inteligente.

Una vez vistos los métodos más utilizados en la actualidad, se va a analizar en detalle el

método escogido para su potencial implantación en Tarjetas Inteligentes.

II.4.1. MODELOS DE MEZCLAS DE GAUSIANAS (GMM)

Basándose en la teoría general dada en el Capítulo I, al aplicar este método al Reconocimiento de Locutores hay que tener en cuenta los siguientes puntos:

- Es un método utilizado principalmente en reconocimiento de locutores para texto independiente.
- Cada verificación va a consistir en introducir en el sistema, en lugar de un único vector de características, un conjunto de T vectores, que corresponderán con los T*10 ms de muestra de voz.
- En la fase de entrenamiento se toma, normalmente, $T = 6000$, para realizar dicho proceso con una muestra, o concatenación de muestras de 60 segundos.
- En la fase de ejecución, se toma una muestra del locutor de un tiempo muy inferior a la muestra utilizada en el entrenamiento (1 - 6 segundos), y se introduce en el modelo el conjunto de T vectores (T = 100 - 600), calculándose la función de máxima verosimilitud y comparando el valor acumulado con un umbral. Normalmente, para evitar la multiplicación, se simplifica el cálculo mediante logaritmos, utilizando la siguiente versión de la función de máxima verosimilitud (para el usuario k):

$$V_k = \sum_{t=1}^{T} \log(p(\vec{x}_t|\lambda_k)) \qquad \textit{(II.8)}$$

II.5. RESULTADOS

Tras la exposición de los bloques de pre-procesado, de extracción de características y de verificación, es preciso detallar los resultados obtenidos. Para hacer esto, se va a iniciar este apartado con una descripción de las muestras tomadas, es decir, de la Base de Datos utilizada.

Posteriormente se pasará a detallar los resultados en clasificación, en función de los distintos parámetros del algoritmo de verificación, para terminar detallando los resultados en autenticación, conseguidos con la mejor configuración obtenida en el caso de clasificación.

II.5.1. BASE DE DATOS

Sin lugar a duda, la construcción de la Base de Datos ha sido la tarea más laboriosa, y en algún sentido frustrante de todo el desarrollo llevado a cabo con esta técnica biométrica. Los intentos de creación de dicha Base de Datos empezaron con la grabación directa de voz mediante micrófono. Aquí se empezaron a mostrar los primeros problemas principalmente de dos tipos: negativa a grabarse su propia voz, supuestamente por timidez; intentos infructuosos de grabar voz debido a risas, provocado, como ya se comentó en la introducción de este capítulo, por la falta de naturalidad a la hora de hablar frente a un micrófono.

Debido a los fracasos cosechados, se analizó en profundidad los métodos de grabación de voz utilizados por otros grupos de investigación a nivel internacional. El resultado fue que en prácticamente todos los casos, se planteaban dos soluciones a la creación de dicha Base de Datos:

- La grabación de llamadas telefónicas. Esta solución está siendo principalmente utilizada por aquellos equipos de investigación que tratan de aplicar sistemas de Reconocimiento de Locutores o de Reconocimiento de Habla a aplicaciones telefónicas.
- La grabación en estudios de grabación.

En ambos casos, los usuarios utilizados para la grabación de la voz, suelen recibir una compensación por el servicio prestado.

Con estos datos, el autor de esta Tesis se planteó nuevamente la grabación de voces para crear la Base de Datos. Esto conllevó la toma de las siguientes decisiones:

- El pago a los sujetos que graben su voz, aparte de ser imposible económicamente inviable dentro del marco de esta investigación, va en contra del estudio de la naturalidad de la técnica biométrica (los sujetos, al ser pagados, muestran una mayor predisposición a realizar sus locuciones de la forma mas ortodoxa posible).

- Por otra parte, la utilización de un estudio de grabación va en contra de una potencial

utilización real del sistema, ya que en ningún momento se está contemplando un ruido de fondo real (si se plantea este sistema colocado en un cajero automático, el usuario no se va a poder encontrar dentro de una cámara anecoica, sino que existirá ruido debido a coches, gritos, voces, pasos, etc.).

- Por último, la grabación de voz a través de la línea telefónica, se planteó como la solución óptima, al tratarse de una situación real con un alto grado de aplicabilidad real. Sin embargo, el hecho de grabar voz telefónica en llamadas aleatorias conllevó a cuestionarse la ética de la solución tomada, debido al desconocimiento de los interlocutores de la posible grabación de su conversación. Por tanto, se desechó también esta solución.

Ante estas decisiones hubo que buscar una fuente de voz, en la que se hablase de forma natural, que no supusiese una voz grabada sin ningún ruido, que fuera relativamente fácil de segmentar (para poder diferenciar el usuario que habla en cada momento) y que a cada usuario se le pudiera grabar varias veces a lo largo de prolongados periodos de tiempo. La fuente encontrada que se aproximaba bastante a las características comentadas fue la emisión de noticias en televisión, donde la voz de los locutores es natural, existe un ruido de fondo dado por diversos factores (principalmente los videos que acompañan al relato de la noticia), era fácil de segmentar ya que durante toda la noticia habla principalmente una sola persona y al ser locutores contratados por la cadena de televisión, se les puede grabar durante tantas veces como se quiera durante largos periodos de tiempo.

Con esto, para las pruebas efectuadas, se creó una Base de Datos de 7 locutores de noticias, tomando en total 73 muestras, cada una de duración distinta (en total se tienen 615 fragmentos de 3 segundos).

II.5.2. RESULTADOS EN CLASIFICACIÓN

Configurando el sistema desarrollado para que actúe como un clasificador, se han probado los diversos parámetros que potencialmente pueden influir en el rendimiento del sistema:

- Los coeficientes empleados. Se han empleado los Coeficientes Cepstrum de Predicción Lineal (LPCC) y los Coeficientes Mel (MEL)
- El número de mezclas. Se utilizaron 1, 2, 3, 4, 5, 6, 7, 8 y 16.
- La varianza mínima. Se utilizaron 0.01 (denotada como v2) y 0.001 (v3).

- El tiempo de la muestra de verificación. Se utilizaron muestras de 1, 3 y 6 segundos.

Los resultados obtenidos se pueden observar en la figura II.2:

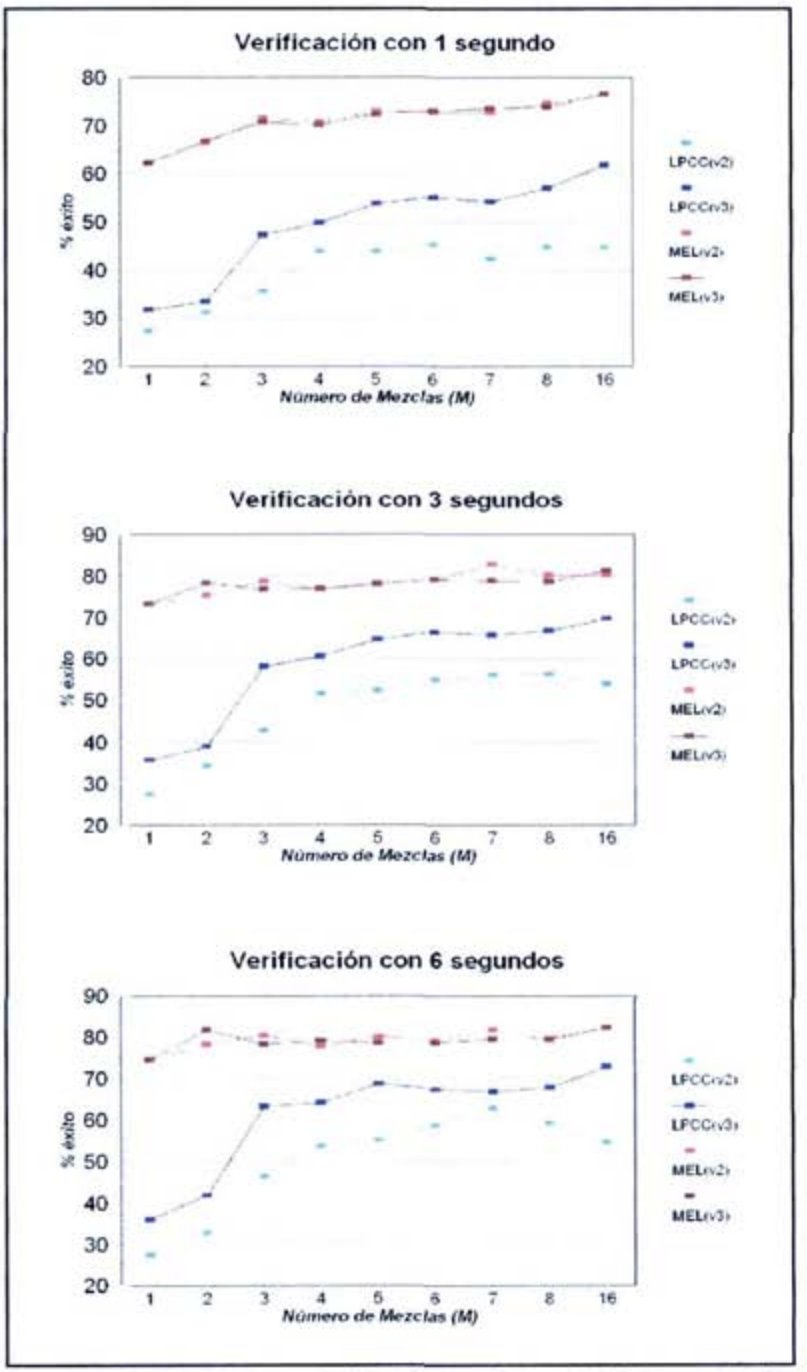


Fig. II.2: Resultados en clasificación mediante GMMs, en relación con el número de mezclas (M), las características extraídas (MEL o LPCC) y el límite de la varianza (v2=0.01 o v3=0.001).

En esta gráfica se puede observar que los coeficientes Mel presentan siempre mejores resultados que los LPCC, para cualquier valor de *M* y limitación de la varianza. Por otro lado, los coeficientes Mel no se ven muy afectados por la varianza mínima, mientras que los LPCC presentan mejores resultados con varianza mínima 0.001.

Respecto al número de mezclas utilizadas, se ve una tendencia creciente con el número de éstas, aunque al llegar a 5 mezclas la pendiente de crecimiento se atenúa. Con relación a la duración de la muestra a verificar, se nota una importante mejoría al pasar de 1 a 3 segundos, no suponiendo prácticamente mejora su evolución a 6 segundos.

Con todo esto, el mejor resultado obtenido es del 82,8%, para los coeficientes Mel, con limitación 0,01, número de mezclas igual a 7 y 3 segundos de duración de la muestra. Dicho resultado, como se verá en posteriores capítulos, es peor que los obtenidos con otras técnicas biométricas.

II.5.3. RESULTADOS EN AUTENTICACIÓN

Tomando las condiciones para las que se ha obtenido el mejor resultado en clasificación, se configuró el sistema para que funcionara como un verificador, obteniendo las tasas de error (FAR,

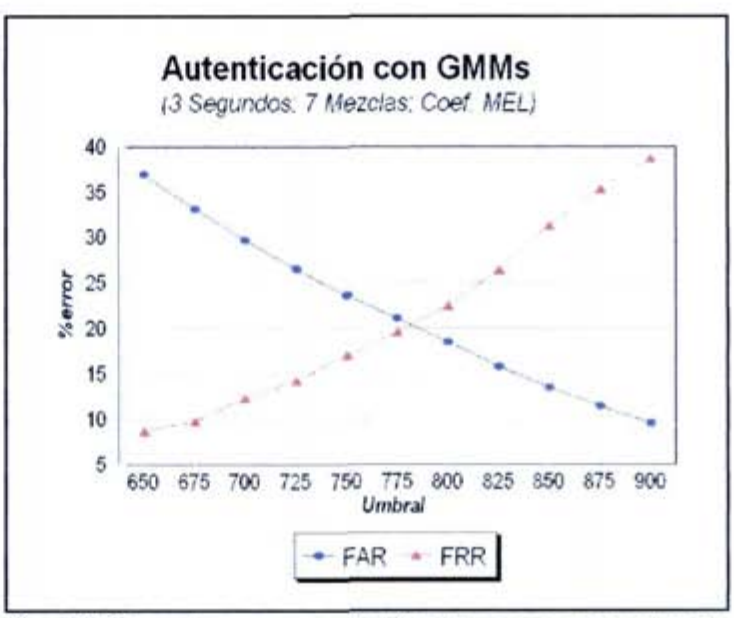


Fig. II.3: Tasas de error en autenticación por voz para el mejor caso encontrado en clasificación

FRR y EER)[7] que se pueden ver en la figura II.3. Queda claro que la EER está algo por encima del 20%, lo que denota que el error que posee el sistema es bastante alto. Además, la apertura de las gráficas del FAR y FRR hace que para obtener un porcentaje aceptable de error en una de esas tasas (supongamos inferior al 10%), la tasa complementaria toma valores superiores al 33%.

II.6. CONCLUSIONES

En el presenta capítulo se ha abordado la técnica de identificación biométrica basada en voz, y conocida normalmente como Reconocimiento de Locutores. Esta técnica, sobre la que proliferan múltiples tratados científicos no ha encontrado todavía el grado de satisfacción que demanda la industria. Sin embargo debido a su popularidad, ha sido estudiada para posteriormente analizar su potencial aplicación dentro de la tecnología de las Tarjetas Inteligentes.

Los resultados obtenidos siguiendo las líneas marcadas en la bibliografía relativa a esta técnica y simulando un entorno real, han sido bastante pobres, habiendo llegado a obtener un éxito de clasificación algo superior al 82% y un EER en autenticación del 20% aproximadamente. Debido a estos resultados, es preciso indicar la necesidad de seguir abordando investigaciones sobre este tema, especialmente en lo relativo a caracterizar mejor aquellos parámetros de la voz que identifican al sujeto, aislándolos de factores como el texto recitado, la evolución con la edad, las enfermedades, el ruido de fondo, etc.

En un capítulo posterior, después de haber tratado el resto de técnicas biométricas, se plantearán los condicionantes específicos de la tecnología de la Tarjeta Inteligente, para poder comprobar más fielmente la viabilidad de su incorporación a dicha tecnología.

[7] Los conceptos de FAR, FRR y EER se han visto en el Capítulo I.

CAPÍTULO III:

GEOMETRÍA DEL CONTORNO DE LA MANO

En este capítulo se va a justificar el diseño realizado para realizar la autenticación de usuarios mediante Marcas Geométricas de la Mano, en concreto de su contorno. Como se verá, a diferencia de cómo se han afrontado las demás técnicas, se ha tenido que realizar el desarrollo desde el inicio, sin contar con apenas ninguna referencia previa. Sólo la publicidad de una empresa estadounidense, que en la actualidad comercializa un sistema basado en esta técnica, ha servido como pauta para avalar la validez del camino tomado.

La estructura de este capítulo va a ser análoga a la usada en el resto de los capítulos sobre técnicas biométricas. Se empezará con una introducción, comentando el estado del arte al inicio de los trabajos y en la actualidad, las aplicaciones existentes y el esquema general usado. Posteriormente se pasará a describir el sistema de captura. En los dos siguientes apartados, se tratará el pre-procesado y la extracción de características. A continuación se expondrán los métodos de verificación empleados con los resultados obtenidos. Se finalizará el capítulo con las conclusiones.

III.1. LA GEOMETRÍA DE LA MANO COMO TÉCNICA BIOMÉTRICA

El uso de la geometría de diversas partes del cuerpo para identificar a las personas, incluyendo la mano, se inició, según algunos estudios ([Lee91]), en la época de los antiguos egipcios, aunque más cercano a nuestros tiempos se encuentra el ya comentado sistema de Bertillon de finales del siglo XIX. Desde el abandono de dicho sistema, no se ha avanzado mucho en esta técnica biométrica, aunque diversos expertos sostienen la capacidad de la mano para identificar a una persona.

Para poder sentar las bases de esta técnica biométrica, en este primer apartado se van a dar unos ligeros conceptos de anatomía de la mano, así como de única clasificación de manos por la forma de su contorno que se ha encontrado. Posteriormente se hará una mención a los pocos trabajos previos existentes sobre esta materia, comentando aplicaciones potenciales donde puede ser aplicada esta técnica.

III.1.1. ESTRUCTURA DE LA MANO

Tomando una definición de enciclopedia ([Lar69]), *"mano es un órgano del cuerpo humano, unido a la extremidad del brazo, que comprende desde la muñeca hasta la punta de los dedos"*. Entrando en el apartado referente a la anatomía de la misma referencia, la mano es la parte más diferenciada de las extremidades y la que permite una mayor matización de la fina actividad mecánica del hombre y, en menor grado, de los simios. Consta, en esencia de un *esqueleto óseo*, provisto de veintisiete huesos articulados entre sí, en los que se insertan un crecido número de *tendones*, provenientes de los músculos del antebrazo, y dotados de un amplio juego de movimientos (fig. III.1).

En la mano existen fundamentalmente tres grupos de huesos: los del ***carpo***, ***metacarpo*** y ***dedos***. El *carpo* es la parte más próxima de la mano, cercana a la muñeca, y consta de ocho huesos dispuestos en dos filas, cuatro en cada una. El segundo grupo está formado por los cinco *metacarpianos*, y forman la parte más distal del esqueleto de la palma. El tercer grupo está

constituido por los huesos de los dedos, las *falanges*, pequeñas y cortas, de las que hay tres en cada dedo, exceptuando el pulgar, en que hay dos.

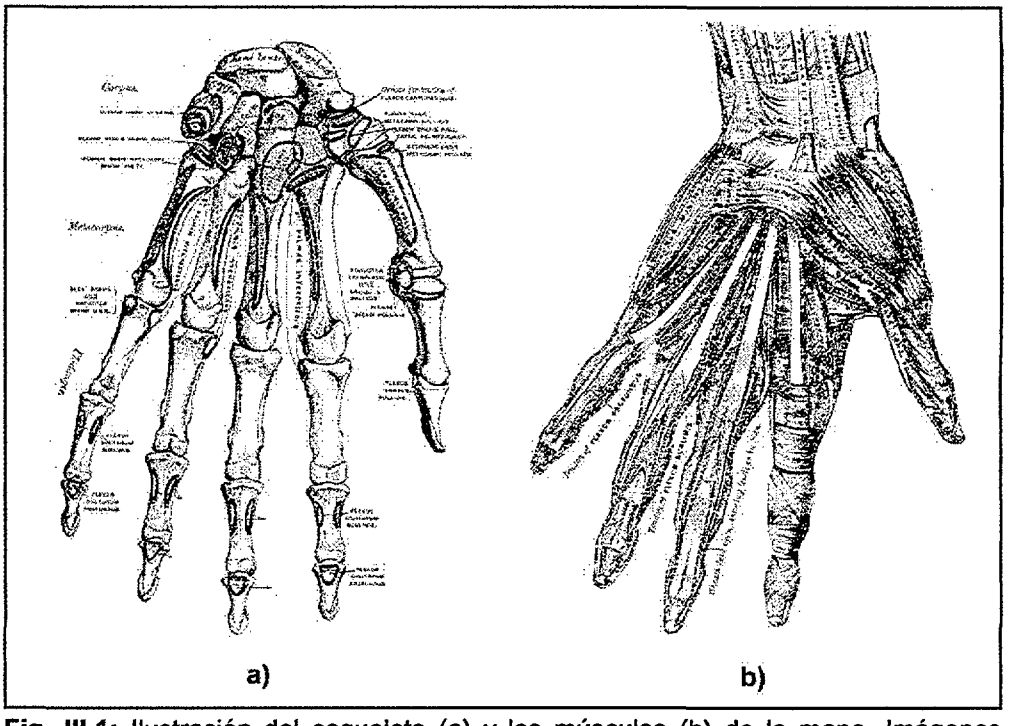


Fig. III.1: Ilustración del esqueleto (a) y los músculos (b) de la mano. Imágenes tomadas de [Gra77].

Los *músculos*, representados a menudo sólo por la terminación tendinosa de una masa muscular del antebrazo, se dividen fundamentalmente en dos grupos: *flexores*, los de la *cara palmar*, y *extensores*, los de la *dorsal*. Existen también los músculos propios de la mano, dispuestos en tres regiones: *eminencia tenar*, o del pulgar; *eminencia hipotenar*, o del borde cubital, y *región palmar*, o media, de la mano, con los interóseos y lumbricales. En conjunto, los músculos de la mano son: cuatro de la *eminencia tenar*, cuatro de la *eminencia hipotenar* y once de la *palma*, cuatro *lumbricales*, cuatro *interóseos dorsales* y tres *interóseos ventrales*. En total, diecinueve músculos propios, más otros quince músculos del antebrazo, cuyos tendones, a veces múltiples, acaban en la mano.

Fisiológicamente, la mano está dotada de la posibilidad de realizar una gran cantidad de movimientos, gracias a la riquísima disposición muscular y del esqueleto óseo. La posibilidad de oposición del pulgar es una de las principales características diferenciales de la mano del hombre.

En una descripción más profana de la forma de la mano, se puede apreciar diversos detalles, a ser considerados para la utilización de la mano como técnica biométrica:

- En la unión de cada una de las falanges, se encuentra una articulación, que hace que la zona donde se encuentra sea más prominente que las áreas que la rodean.
- Las articulaciones de las falanges no se encuentran, en la práctica, siempre alineadas, sino que por diversos motivos, se producen desviaciones (una de las mayores causas de desviación suele ser la forma de escribir durante la infancia).
- Dependiendo de la constitución muscular de la persona, los puntos de unión entre dos dedos y la palma pueden encontrarse más cerca o más lejos de la muñeca, y la relación de la distancia de uno de esos puntos al resto de ellos también variará de una persona a otra. En el transcurso de este capítulo, a esos puntos se les denominará ***puntos inter-dedo***.
- El grosor de cada falange, así como la masa muscular de ella, varía de una persona a otra, e incluso entre las falanges de la misma mano.

En la figura III.2, se puede observar las imágenes correspondientes a la única clasificación de las manos por su forma que se ha podido encontrar. Se trata de un tratado de Quiromancia, en el que se dividen las manos en 7 tipos fundamentales ([Omi95]):

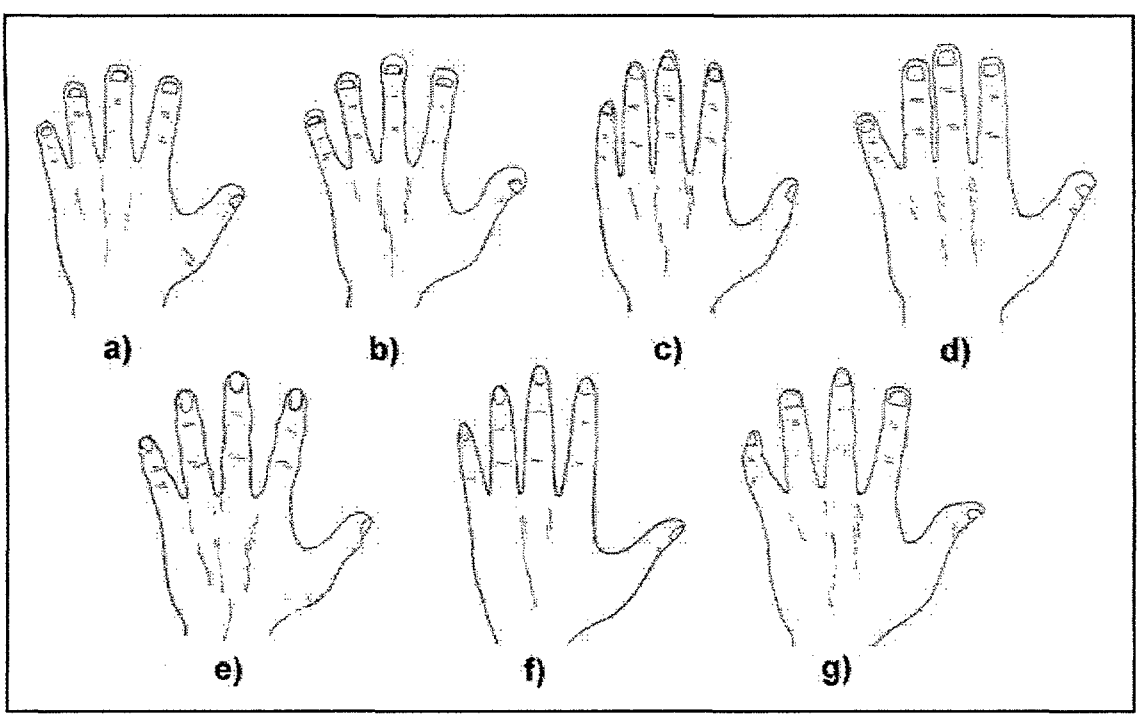


Fig. III.2: Clasificación quiromántica de las manos. Imágenes tomadas de [Omi95].

a. **Mano de gran palma**. También se la denomina *mano elemental*. Sus características esenciales son el grosor y el tamaño reducido de sus dedos. Su pulgar es corto, bastante ancho, y muestra tendencia a curvarse hacia atrás.
b. **Mano espatulada.** Sus dedos suelen ser planos y las articulaciones poco o nada

apreciables. Puede ser considerada como el polo opuesto a la *mano elemental.*

c. **Mano cónica.** También se las conoce como *mano artística.* Este tipo de mano suele parecer larga, a veces también huesuda y, debido a confusiones, se la suele dividir en tres grupos: la de palma ancha y gruesa y dedos en armonía; la de palma de dimensiones medias, pulgar muy fino y, en general, gran flexibilidad; y la de palma estrecha, dedos proporcionados y mínimo grosor.
d. **Mano cuadrada.** Es la que se suele tomar como *"mano normal".* Sus proporciones son medias.
e. **Mano nudosa.** Se la denomina también como *mano filosófica.* Su distintivo es el pulgar ancho. Las articulaciones de los dedos son notorias, nudosas y la palma es amplia.
f. **Mano puntiaguda.** Los dedos carecen de protuberancias en las articulaciones, y cada uno parece dotado de una particular función para dar lugar al encanto del conjunto (se la suele tomar como el tipo de mano más bello). La palma es de dimensiones medias.
g. **Mano mixta.** Es la mano que normalmente se encuentra, ya que se trata de una mezcla de varios de los otros 6 tipos de manos.

III.1.2. TRABAJOS PREVIOS

Tal y como se comenta en el capítulo 4 de [Jai99a], a finales de la década de los 60 y principios de los 70, Robert P. Miller solicitó una serie de patentes sobre un sistema que medía las características de la mano y grababa unas características únicas para realizar reconocimiento y autenticación de la identidad de un usuario. Las máquinas que fabricó eran prácticamente mecánicas en su totalidad. A finales de los 70 y principios de los 80 otras compañías lanzaron desarrollos de nuevos sistemas. Finalmente, a mediados de los 80, David Sidlauskas desarrolló y patentó un equipo electrónico creando al mismo tiempo la empresa *Recognition Systems, Inc.*

Sin embargo, la información sobre estos dispositivos se ha mantenido, hasta la actualidad, bajo las restricciones típicas derivadas del interés comercial. Esto ha empujado a que no se haya publicado, hasta la fecha, ningún artículo técnico en relación con esta técnica. De hecho, hasta 1997 el autor de esta Tesis no tuvo ninguna información, ni siquiera comercial, del producto desarrollado por *Recognition Systems* [RecCOM]. La obtención de dicha información comercial reafirmó la investigación iniciada hacía meses.

Antes de empezar la descripción del sistema desarrollado en el marco de esta Tesis, es necesario hacer una mención al desarrollo comercial de la empresa ya citada. Siendo una técnica

que cuenta con muchos detractores (debido a su aclamada menor unicidad comparada con otras técnicas, como huella o iris), el éxito comercial ha llevado a muchos a considerarse si es lógica la búsqueda de la mejor técnica biométrica para todas las aplicaciones. Este sistema ha demostrado que dependiendo del entorno, una técnica *a priori* peor puede tener una mejor aplicación.

Las propiedades que comúnmente se le asignan a la técnica biométrica de mano, y que como se verá en el transcurso de este capítulo son totalmente reales ([Roj98], [San99b], [San99d]), si no mejores, son:

h. Su unicidad es media. Desgraciadamente no existen estudios detallados que demuestren o contradigan esta afirmación, pero en el sector se la considera correcta.
i. Su estabilidad también es media, ya que ganancias o pérdidas de peso modifican las medidas de la mano. Sin embargo, si en lugar de tomar medidas absolutas se consideran medidas relativas, esta limitación desaparece.
j. Su coste es bajo. Solo se necesita una cámara de media/baja calidad, y una plataforma diseñada al efecto.
k. El tamaño del patrón es muy pequeño (decenas de bytes).
l. La aceptabilidad es muy alta. La no vinculación legal de esta técnica en nuestros días, así como la facilidad de su uso, ha ayudado al gran éxito comercial.

Todas estas características hacen que esta técnica sea ideal para control de accesos físicos en entornos cerrados de media-alta seguridad. Por el contrario, el tamaño del equipo necesario, bastante grande, la desaconseja para otras aplicaciones que no sean de control de acceso físico. A pesar de ello, y debido a dicho tamaño, así como a su coste, es un sistema al que se le pueden acoplar, según el grado de seguridad que se desee, cualquier método alternativo de sujeto vivo, tales como sensores de ultrasonidos para medir la velocidad de circulación sanguínea, exploración térmica de la mano, etc.

III.2. MÉTODO DE CAPTURA

El modo escogido para realizar la captura de los datos biológicos del sujeto ha sido la fotografía digital de baja resolución. Debido al estado actual de la tecnología y los precios de las cámaras (cada vez más bajos para unas mejores características técnicas), las fotografías obtenidas finalmente son de una resolución de 640x480 puntos y 256 colores. Las fotos han sido tomadas

desde un punto superior a la mano, la cual está colocada sobre una plataforma diseñada al efecto. Al tratarse de un prototipo basado en una cámara comercial y haber sido diseñado para el estudio de la técnica, las fotos sacadas son almacenadas en archivo, en formato JPEG. En una realización comercial, la foto extraída pasaría directamente a la etapa de pre-procesado, sin almacenamiento intermedio. El prototipo utilizado se puede observar en la figura III.3.a.

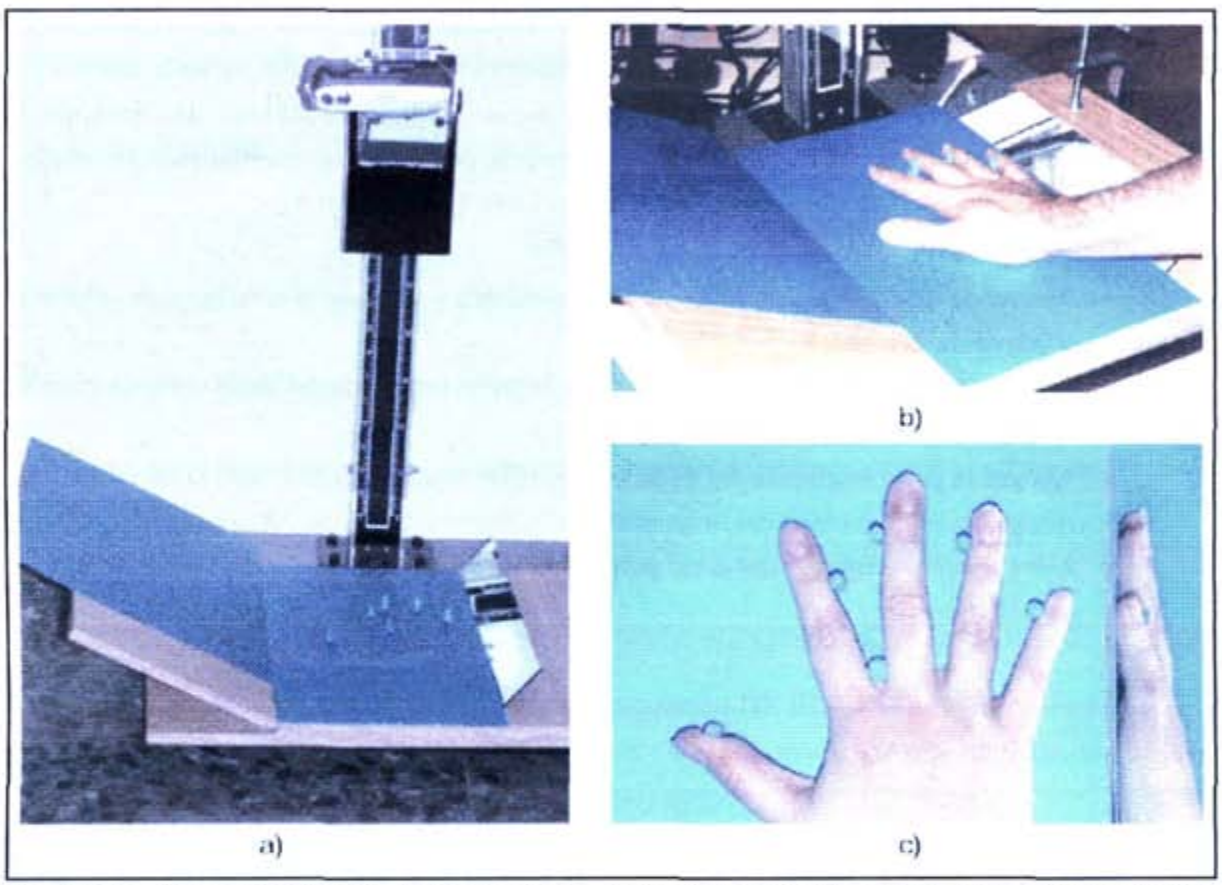


Fig. III.3: Prototipo utilizado (a), colocación de la mano sobre la plataforma (b) y fotografía tomada (c).

La cámara se encuentra situada a 42cm de la palma de la mano y, como se verá al comentar el diseño de la plataforma, capturará, además de la imagen del dorso de la mano, la vista lateral de la misma.

Por último, es importante la colocación del sistema en relación con la altura del usuario. Si la plataforma se encuentra colocada demasiado baja, el usuario tenderá a no posar completamente la mano y, por tanto, a que las medidas resultantes sean inconscientemente falseadas. La altura recomendada para un sistema a ser usado por adultos es la de 1,40 metros o superior.

III.2.1. PLATAFORMA

La plataforma, tal y como se puede ver en la figura adjunta, consta de una superficie en la que se encuentran situados 6 topes que facilitan el guiado y colocación de la mano en una posición determinada y fija. Hay que hacer notar que toda la plataforma está diseñada para la colocación de la mano derecha. Mediante este mismo sistema y debido a la simetría especular de las manos, un usuario que careciera de dicha mano, siempre podría colocar la mano izquierda con la palma hacia arriba, con el inconveniente de tener que estirar siempre la mano (sin embargo, al no tener una plataforma de sujeción, el usuario podría doblar involuntariamente los dedos, falseando las medidas). Volviendo a los topes, éstos están pensados para:

- Apoyar la unión entre el dedo índice y corazón, y de paso ubicar la mano frente al objetivo de la cámara.
- Apoyar la parte interna del dedo índice y la parte izquierda del dedo corazón (fijar la apertura entre ambos dedos).
- Apoyar la parte izquierda del dedo anular (fijar la separación con el dedo corazón).
- Apoyar la parte interna del dedo meñique (fijar la separación con el anular).
- Apoyar la parte interna del dedo pulgar (de forma que se evite su colocación junto al dedo índice).

En una versión comercial del prototipo desarrollado se podría dotar a cada uno de los topes de un sensor de presión, para que una vez pulsados todos, se extrajese automáticamente la foto.

En la parte derecha de la plataforma se encuentra colocado un espejo, formando un ángulo de 60 grados con la superficie de la misma. Este espejo refleja hacia el objetivo de la cámara el perfil lateral de la mano, de forma que se puedan extraer medidas de esa orientación. Para que el fondo de la vista lateral no varíe dependiendo de la colocación del sistema, se ha completado la plataforma con una pared lateral en el extremo contrario al espejo. Esta pared se ha realizado inclinada en el prototipo para evitar sombras (al ser un sistema abierto por arriba). Se entiende que en un producto comercial final, todo formará una caja cuadrada, más pequeña, y con la cámara más próxima debido al uso de óptica no convencional.

Toda la plataforma ha sido decorada en azul para facilitar un alto contraste con la piel humana (ya que la piel de todas las razas tiene una componente azul muy reducida). Al haberse escogido una tonalidad de azul, intermedia entre el claro y el oscuro, el contraste es perfecto tanto para pieles de raza blanca, como para pieles de razas oscuras.

III.3. PRE-PROCESADO DE LA IMAGEN

Una vez capturada una foto de la mano, conteniendo el dorso y la vista lateral, se inicia el bloque de pre-procesado, en el que se van a extraer los bordes de la imagen para su posterior entrada en el bloque de extracción de características, el cual se tratará en el siguiente apartado.

El pre-procesado empieza traduciendo la imagen de color, a una imagen en blanco y negro con alto contraste entre la mano y el fondo. Para conseguir este resultado se va a operar con las distintas componentes de color de la imagen, aprovechando la propiedad de que la piel posee una débil componente de azul. La operación realizada es:

$$I_{ByN} = h\left(h\left(I_R + I_V\right) - I_A\right) \qquad \textit{(III.1)}$$

donde I_{ByN}, I_R , I_V y I_A son, respectivamente, la imagen en blanco y negro resultante y las componentes roja, verde y azul de la imagen original. La función h representa la función de estiramiento del histograma (en la que el rango dinámico de la imagen se pasa de forma lineal a los valores de 0 a 1 aprovechando todo el nuevo rango, [Sca89], [Kle96], [Jäh97], [Jai89]). Como se puede observar, la operación intenta eliminar aquellas zonas de la imagen con mayor componente azul que roja y verde, ya que la diferencia dará negativa (hay que tener en cuenta que en la operación de estiramiento se realiza una eliminación de los valores negativos, pasándolos a 0). Con esta operación todo el fondo pasará a ser negro (valor 0) mientras que la mano, al tener una componente azul muy inferior a las otras dos componentes, pasará a tener valores cercanos al 1 (cercano al blanco).

Tras realizar el paso a blanco y negro, la imagen se pasa a valores binarios utilizando un umbral. El umbral ha sido escogido heurísticamente para que se eliminen todos los valores espúreos dados por brillos o ruidos en la imagen. A la imagen resultante se le puede aplicar fácilmente un algoritmo de extracción de bordes basado en la función de Sobel ([Kle96]). Con esta última operación, se ha obtenido una imagen binaria que representa el borde de la imagen y, por tanto, el contorno del dorso de la mano y el de su perfil. En la figura siguiente se pueden observar las imágenes resultantes de las distintas fases del proceso. Cabe decir que en la figura c), se ha coloreado artificialmente el interior de la mano con el único propósito de facilitar su reproducción en papel a la escala utilizada (al ser el borde extraído de anchura 1 pixel, las operaciones de agrandado y compresión del procesador de textos produce una pérdida de partes de las líneas).

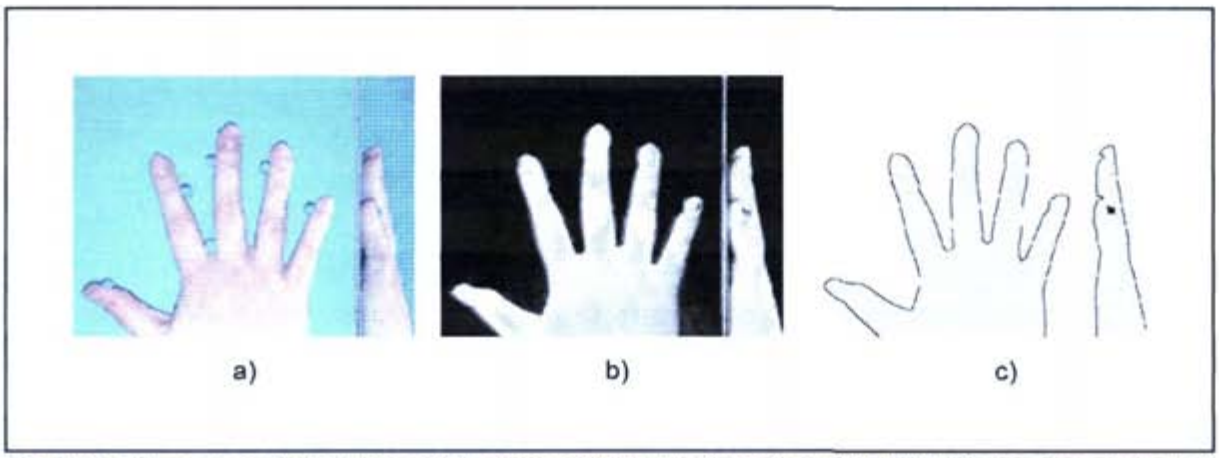


Fig. III.4: Pre-procesado de la imagen: Imagen original (a), Imagen en ByN (b) y Bordes detectados (c).

III.4. EXTRACCIÓN DE CARACTERÍSTICAS

Una vez obtenidos los contornos del dorso y del perfil de la mano, manteniendo fija la ubicación de los topes, se realizan una serie de medidas que darán como resultado el vector de características correspondiente. Las principales medidas tomadas se pueden ver en la figura III.5. Estas medidas se pueden dividir en cuatro tipos principales:

- **Anchuras:** de cada uno de los dedos salvo el pulgar (w_{11}, w_{12}, w_{13} y w_{14}, para el dedo índice; w_{21}, w_{22}, w_{23}, w_{24} y w_{25}, para el dedo corazón; w_{31}, w_{32}, w_{33} y w_{34} para el dedo anular; w_{41}, w_{42}, w_{43} y w_{44} para el dedo meñique), en posiciones fijas evitando los puntos de los topes, debido a la presión ejercida por los dedos en dichos puntos. También se mide la anchura de la palma de la mano (w_0) y las distancias entre los tres puntos inter-dedo

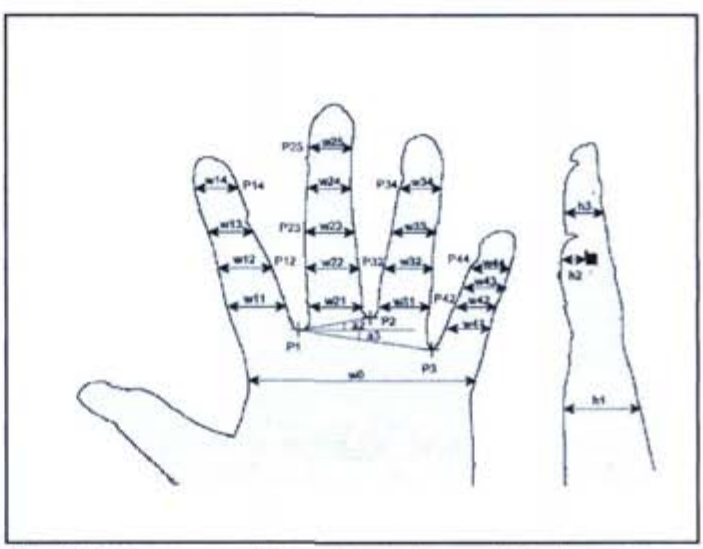


Fig. III.5: Esquema de las principales medidas tomadas

en coordenadas tanto horizontales como verticales (P_1^x-P_2^x ; P_1^x-P_3^x ; P_1^y-P_2^y ; P_1^y-P_3^y ; donde los superíndices indican la coordenada tomada).

- **Alturas:** del dedo corazón (h_3), del dedo meñique (h_2) y de la palma de la mano (h_1).

- **Desviaciones:** de los dedos con respecto a la línea recta ideal que debería formar las falanges. Estas distancias se miden como la distancia entre el punto medio del contorno del dedo (por ejemplo P_{12} para el caso del dedo índice) y el punto medio de la recta definida entre el punto inter-dedo correspondiente (P_1 en el mismo caso) y el punto más alto del contorno de ese dedo, en el que se hacen medidas (P_{14}). De forma matemática, para el dedo índice sería:

$$desv_1 = P_{12}^X - \left(\frac{P_{14}^X - P_1^X}{P_{14}^Y - P_1^Y} \right) \left(P_{12}^Y - P_1^Y \right) \qquad \textit{(III.2)}$$

donde los subíndices indican el punto medido y los superíndices la coordenada utilizada. De esta forma se obtiene $desv_1$, $desv_2$, $desv_3$ y $desv_4$ para los dedos índice, corazón, anular y meñique respectivamente.

- **Ángulos:** entre la línea de unión de los puntos inter-dedo y la horizontal: a_2, para el ángulo entre P_1-P_2 y la horizontal; a_3, para el ángulo entre P_1-P_3 y la horizontal.

Para minimizar la variación de las características con la edad y la pérdida o ganancia de peso, se han tomado medidas relativas, en lugar de medidas absolutas. Es decir, todas las medidas de anchos y alturas han sido divididas por w_{21} (el ancho más cercano a los puntos inter-dedo del dedo corazón).

III.4.1. DISCRIMINABILIDAD DE LAS CARACTERÍSTICAS

Tal y como se ha indicado, de cada foto se han extraído 31 medidas (22 anchos, 3 alturas, 4 desviaciones y 2 ángulos). Una vez extraídas las características de toda la base de datos de manos existente, se ha realizado un estudio de discriminalidad de dichas características, para poder estudiar la viabilidad de reducir el número de medidas a realizar en el sistema final. Para realizar este estudio se ha utilizado el factor F_j, con j variando de 1 a 31 (cada una de las

características obtenidas inicialmente), y cuya función es:

$$F_j = \frac{\text{varianza interclase}}{\text{varianza intraclase}} = \frac{V\left(\frac{\sum_{i=1}^{N} \overline{f_j^i}}{N}\right)}{\frac{\sum_{i=1}^{N} V\left(f_j^i\right)}{N}} \qquad \textit{(III.3)}$$

donde F_j es el valor del factor F para la característica j-ésima, V es la función que extrae la desviación estándar, N es el número de clases (usuarios), f_j^i es la característica j-ésima de la clase i-ésima y $\overline{f_j^i}$ es la media de las características j-ésimas de la clase i-ésima. Tras este estudio se obtuvieron como conclusión, que 25 de las 31 características inicialmente tomadas tienen capacidad discriminante, por lo que se eliminaron directamente las 6 características que no poseían esa capacidad (una explicación más detallada del proceso puede verse en [Roj98], sobre trabajos previos a los resultados mostrados aquí).

Las características eliminadas fueron:

- Ancho del punto más distante del dedo corazón (w_{25}).
- Las diferencias en coordenada x entre los puntos interdedo: (P_1^x-P_2^x) y (P_1^x-P_3^x).
- Las tres alturas medidas: h_1, h_2 y h_3.

Los valores del factor F, de todas las características eliminadas se encontraban por debajo de 1. Por otra parte para todas las características tomadas, los valores del factor F se encontraban por encima de 3,5.

III.5. VERIFICACIÓN Y RESULTADOS OBTENIDOS

En el sistema desarrollado, los métodos que se han utilizado para realizar la verificación han sido:

- Distancia Euclídea
- Distancia de Hamming (con características no binarias)
- Modelado por Mezcla de Gausianas (GMM)

En el capítulo I ya se dio una introducción a dichos métodos, por lo que en este apartado no se van a volver a detallar. Se va a pasar, por ello, directamente al apartado de análisis de los resultados obtenidos. Para realizar esto, se va a hacer una primera presentación de la Base de Datos utilizada. Posteriormente se van a analizar los resultados atendiendo a los métodos de verificación empleados, comentando en cada uno de ellos, no sólo los datos relativos a autenticación de usuarios, sino también los correspondientes al sistema de clasificación.

Se van a realizar dos tipos de estudios para cada método atendiendo a: a) la variación del número de vectores usados en el reclutamiento; y b) la variación del número de características. El número de vectores de entrenamiento utilizados va a ser 3, 4 y 5, debido a que un número mayor implicaría una mayor molestia al usuario y un menor número sería insuficiente para poder crear un patrón con garantías. Con el número de vectores de entrenamiento fijo, se ha ido disminuyendo el tamaño del vector de características estudiando los siguientes casos:

- Todas las características (25)
- Sin las desviaciones (21)
- Con las desviaciones pero sin la mitad de los anchos de los dedos y los ángulos de los puntos inter-dedo (15)
- Sin desviaciones, sin la mitad de los anchos de los dedos, sin los ángulos y sin las medidas de los puntos inter-dedo (9)

III.5.1. BASE DE DATOS

Una vez creada la plataforma y adquirida la máquina fotográfica, el proceso de investigación empezó con la creación de una Base de Datos de fotografías de manos, debido a la falta de existencia de una de dominio público (que hubiese influido muy positivamete en la investigación, tanto en tiempo, como en tamaño de la misma).

La base de datos final está compuesta por 20 personas de distintas edades, sexo y profesión. El más joven tenía sólo 12 años, mientras que el de más edad superaba los 50. Su distribución por sexos era del 50%, y por profesiones había 8 estudiantes universitarios, 5 escolares, 2 amas de casa, 4 ingenieros y 1 mecánico de coches. Una representación de una

muestra de cada usuario se puede ver en la siguiente figura:

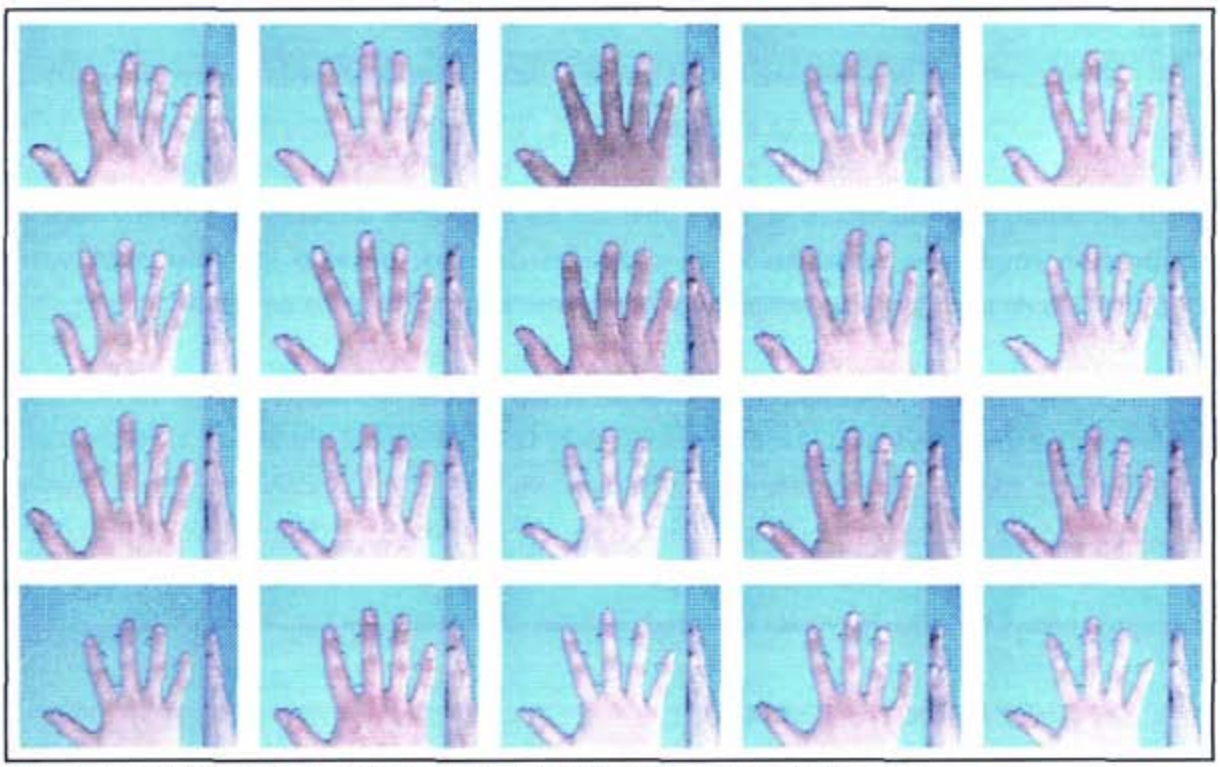


Fig. III.6: Muestras de cada una de las personas incluidas en la Base de Datos

En la creación de la Base de Datos se llegó a una conclusión principal: aunque el 80% de los usuarios no estaban vinculados con el desarrollo, mostraron una muy alta aceptación del sistema. Esa gran aceptación se notó en dos factores fundamentales:

- los sujetos aprendieron a utilizar el sistema de forma casi inmediata, necesitando únicamente un par de consejos durante la primera foto;
- ningún usuario se sintió acosado por el sistema, al no ver en él ninguna vinculación negativa.

III.5.2. DISTANCIA EUCLÍDEA

Haciendo un primer estudio de los resultados obtenidos en clasificación, tal y como se

puede ver en las tablas III.1 y III.2, el número de vectores de reclutamiento no introduce modificación alguna de los resultados obtenidos, estando siempre entre el 85 y 86%. Estos resultados, utilizando todas las características, muestran un error en clasificación superior al 10% y por tanto, se puede derivar que los resultados obtenidos son bastante pobres.

Tabla III.1: Resultados de Clasificación dependiendo del Nº de Vectores de Entrenamiento

Nº Vectores	D. Euclídea	D. Hamming	GMMs
3	86 %	75 %	88 %
4	85 %	82 %	93 %
5	86 %	87 %	96 %

Tabla III.2: Resultados de Clasificación dependiendo de las Características utilizadas

Nº Características	D. Euclídea	D. Hamming	GMMs
25	86 %	87 %	96 %
21	84 %	86 %	97 %
15	86 %	88 %	96 %
9	77 %	75 %	91 %

Si se examinan los resultados en clasificación para distintas longitudes del vector de características (Tabla III.2), se puede apreciar que únicamente cuando el número de características utilizadas es 9, existe un incremento importante del error producido, volviendo a tener un éxito alrededor del 85% para el resto de los casos.

Centrando ahora el estudio sobre el esquema de autenticación de usuarios desarrollado, se pueden apreciar en la figura III.7 los resultados obtenidos para ambas pruebas realizadas. Manteniendo fija la longitud del vector de características y variando el número de vectores de reclutamiento utilizados, se puede observar que la FAR[8] permanece prácticamente constante, siendo la variación de la FRR[9] muy leve. Observando la variación de esta última tasa, se percibe

[8] El concepto de Tasa de Falsa Aceptación (FAR) fue introducido en el Capítulo I.

[9] Al igual que la FAR, la Tasa de Falso Rechazo (FRR) se introdujo en el Capítulo I.

que, para umbrales pequeños, se obtienen resultados sensiblemente mejores utilizando 5 vectores, mientras que para valores del umbral superiores a 350, las tres alternativas presentan valores muy similares, siendo peores los resultados para 4 vectores de características.

En cuanto a la variación del número de características utilizadas para la verificación, manteniendo constante el número de vectores de entrenamiento (5), se puede observar que la EER[10] siempre se encuentra por encima del 10%, y que los resultados obtenidos (tanto la FAR como la FRR) para 25 y 21 muestras son prácticamente iguales. Para los casos de 9 y 15 muestras, se aprecia una EER algo inferior pero, sin embargo, una apertura mayor entre las gráficas de la FAR y la FRR, lo cual indica una mayor inestabilidad a la hora de elegir el umbral, ya que un desplazamiento mínimo en dicho valor, supondría un cambio muy brusco en el rendimiento esperado del sistema.

[10] La Tasa de Error Igual (EER) también se definió en el Capítulo I.

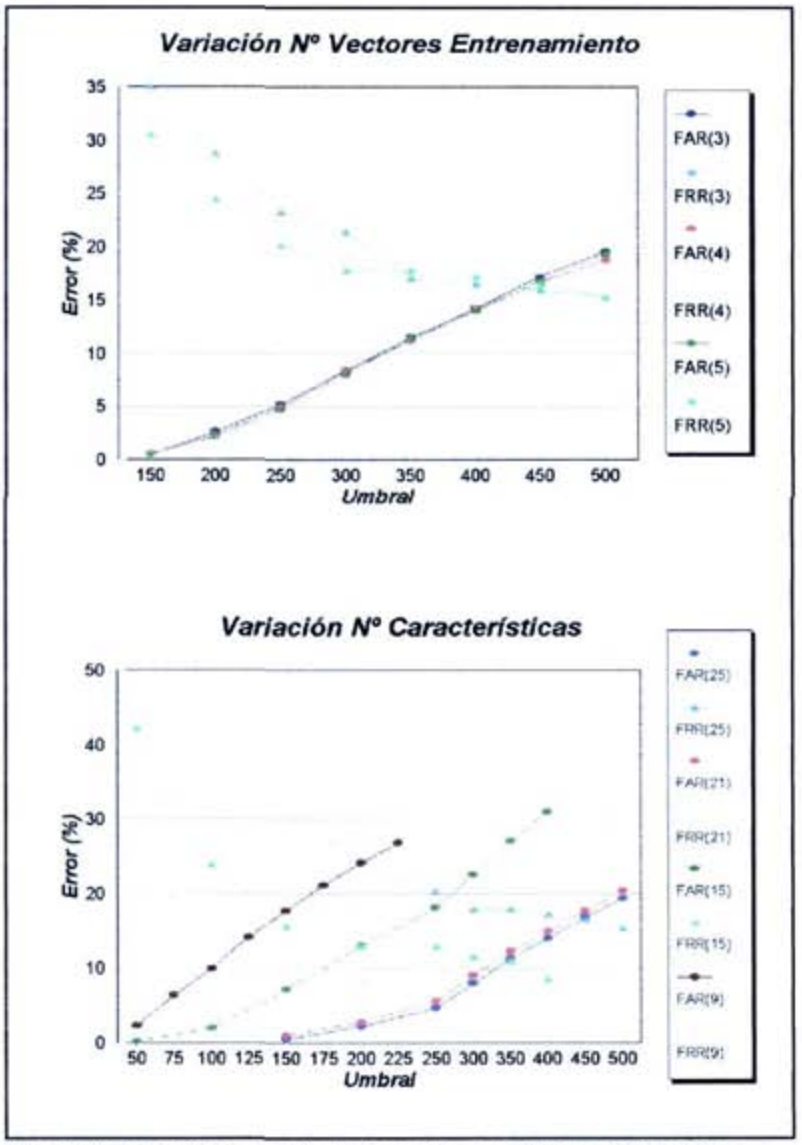


Fig. III.7: Resultados en Autenticación para Distancia Euclídea

Como conclusión, cabe comentar que este método de verificación, aunque prueba que esta técnica es factible de ser utilizada para discriminar entre personas, no consigue unos resultados aceptables para su puesta en funcionamiento.

III.5.3. DISTANCIA DE HAMMING

El segundo método adoptado para realizar la verificación ha sido la Distancia de Hamming, bajo el caso de componentes del vector de características no binarias, utilizando la fórmula expuesta en el apartado correspondiente del capítulo I.

Haciendo un estudio sobre los resultados obtenidos al utilizar el sistema como clasificador, tal y como se puede ver en las tablas anteriormente mencionadas, al contrario de lo que ocurría con la Distancia Euclídea, aquí si se aprecian diferencias con la variación del número de vectores utilizados en el reclutamiento, pasando de un pobre resultado para 3 vectores (75%), a unos resultados ligeramente mejores que los obtenidos en la Distancia Euclídea para 5 vectores (87%).

Con respecto a la variación del número de componentes del vector de características, se aprecia un comportamiento análogo al descrito en la sección anterior: el error permanece casi constante (alrededor del 87%), salvo para 9 características, donde el error se incrementa enormemente (25%).

En cuanto a autenticación (figura III.6), se vuelve a notar el impacto del número de vectores utilizados en el entrenamiento, bajando la EER según aumenta el número de vectores. Pero lo que resulta realmente importante es que con un número de vectores de reclutamiento igual a 5, se baja la EER por debajo del 10%, pudiendo obtener, incluso, una FRR inferior al 10% para una FAR del 5%.

Variando el número de características, se puede observar una EER casi constante para los casos de 25, 21 y 15 componentes, siendo el caso de 9 componentes prácticamente desechable debido, además de su pobre EER, a sus altos valores de error cuando una de las tasas trata de aproximarse al 5%. El caso de 25 características se puede tomar como el mejor, debido a la menor separación de las gráficas de la FAR y la FRR correspondientes.

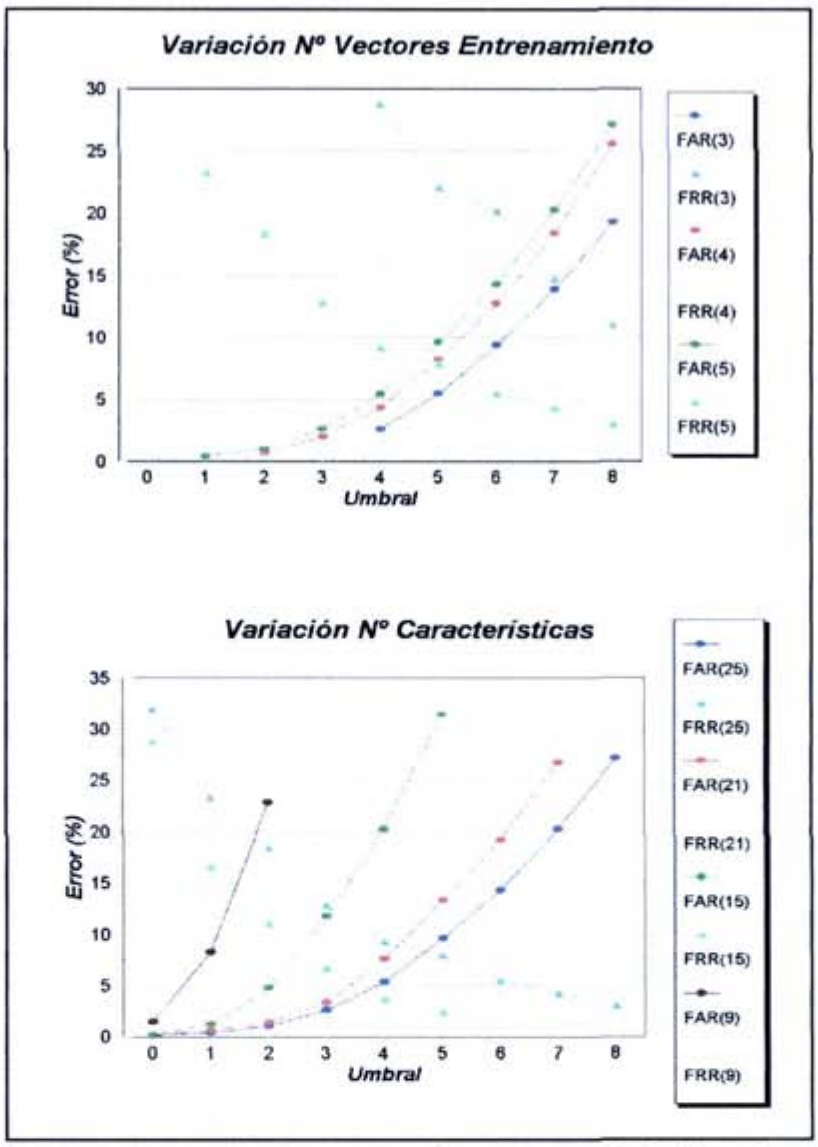


Fig. III.8: Resultados en Autenticación para Distancia de Hamming

Por tanto, aunque en clasificación no se han encontrado unos resultados muy prometedores, en autenticación este método ha plasmado la posibilidad de utilizar esta técnica con un coste computacional ciertamente bajo.

III.5.4. VERIFICACIÓN POR GMMS

Como último método de verificación escogido, se ha utilizado una modelización por mezcla de 10 gausianas, método que conlleva un coste computacional bastante superior a los anteriormente utilizados en este capítulo. Observando de nuevo las tablas de resultados en clasificación, se reflejan unos valores muy superiores para esta técnica, que alcanza para sólo 3 vectores de entrenamiento, un éxito de clasificación ligeramente superior al mejor de los resultados comentados hasta este momento. Los buenos resultados, se reflejan mucho mejor en el caso de la utilización de 5 vectores, donde se reduce el error a un simple 4%.

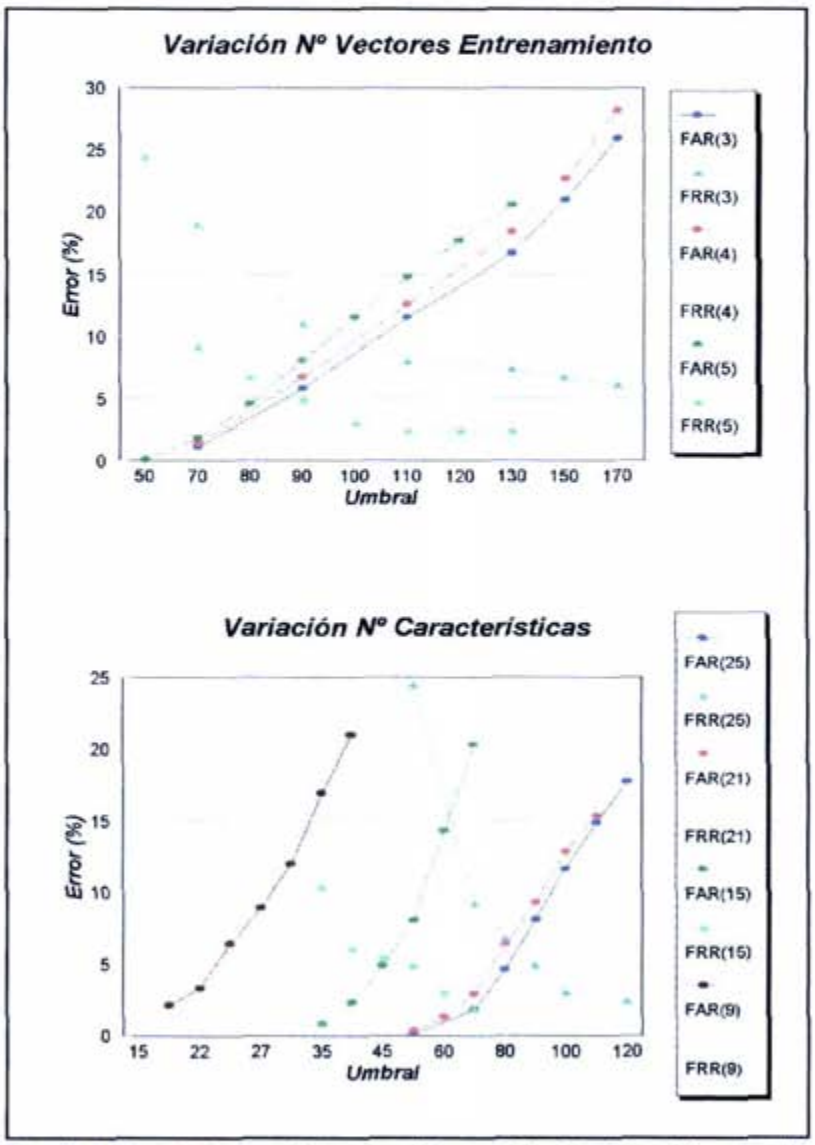


Fig. III.9: Resultados en Autenticación para Modelado por Mezclas de Gausianas

En el caso de modificar el número de características a utilizar para realizar la clasificación, se muestra una evolución análoga a la de los métodos anteriores, con unos resultados entre el 96 y 97% para 25, 21 y 15 características, obteniendo incluso un 91% para 9 características.

En autenticación los resultados son tan prometedores como los vistos en clasificación (figura III.7), con una EER siempre inferiores al 10% y muy cercano al 5% para el caso de 5 vectores de reclutamiento.

Variando el número de características, se observa un comportamiento muy bueno para los 4 casos, haciendo incluso viable la posibilidad de utilizar únicamente 9 características.

Como conclusión a este método, y antes de pasar a las conclusiones relativas a esta técnica biométrica, es de destacar los buenos resultados obtenidos, poniendo a esta técnica a la altura de las comúnmente consideradas de media-alta seguridad.

III.6. CONCLUSIONES

En este capítulo se ha detallado el desarrollo llevado a cabo para la creación de un sistema de autenticación de usuarios basado en la geometría de la mano. Este desarrollo se ha llevado a cabo sin poder partir de ningún trabajo previo, debido a la falta de documentación científica sobre esta técnica. El desarrollo ha sido completo hasta obtener un prototipo susceptible de ser convertido en un producto comercial.

El análisis de los métodos de verificación utilizado, así como el trabajo previo de búsqueda de discriminabilidad en las características, ha llevado a la conclusión de utilizar patrones de un tamaño entre 9 y 25 componentes, siendo recomendable el de 15 características por la relación discriminabilidad/tamaño obtenida. En cuanto al método de verificación a emplear, los resultados obtenidos con GMMs posicionan a esta técnica dentro de las comúnmente reconocidas como de media-alta seguridad. Teniendo en cuenta el coste computacional del método anteriormente mencionado, se puede plantear la utilización de la Distancia de Hamming cuando dicho coste suponga una seria limitación, teniendo en cuenta que esa decisión provoca un descenso en el rendimiento del sistema.

CAPÍTULO IV:

PATRÓN DEL IRIS OCULAR

En los últimos cuatro años, la Identificación Biométrica basada en el Patrón del Iris Ocular, ha experimentado un gran auge debido a los excelentes resultados obtenidos y al gran interés que está mostrando la Banca para incorporar dicha técnica a sus cajeros automáticos. El desarrollo realizado basándose en esta técnica, y que es el motivo del presente capítulo, parte de los trabajos llevados a cabo por John G. Daugman, actualmente profesor de la Universidad de Cambridge. Estos trabajos se encuentran parcialmente expuestos en su artículo [Dau93], y gran parte del desarrollo que aquí se presenta está inspirado en él. Como anticipo a lo que se verá en el primer apartado, se puede decir que Daugman es considerado como el inventor de esta técnica, afirmación que, aunque cierta, será matizada en dicho apartado.

Por tanto, en el primer apartado de este capítulo se hará, como ha sido habitual en los capítulos anteriores, una breve introducción a la técnica, así como a su evolución histórica. Posteriormente se comenzará con la exposición del desarrollo realizado, detallando cada uno de los bloques principales del sistema biométrico: captura, pre-procesado y extracción de características. El apartado correspondiente al bloque de verificación servirá para exponer los resultados obtenidos. Por último se mostrarán las conclusiones obtenidas con este trabajo.

IV.1. INTRODUCCIÓN AL IRIS COMO TÉCNICA BIOMÉTRICA

En este primer apartado del capítulo, se va a presentar las nociones básicas para posteriormente comprender el desarrollo realizado. Se iniciará la exposición con una introducción a la anatomía del ojo, para posteriormente comentar las características que convierten al iris humano en un potencial elemento de diferenciación biométrica. Vistas estas dos primeras secciones, y para concluir esta introdución, se reflejará el nacimiento de esta técnica, así como su evolución comercial.

IV.1.1. ANATOMÍA DEL OJO

Los ojos, son los órganos humanos que facilitan el sentido de la visión. El cuerpo humano consta de dos ojos, lo cual facilita una visión estereoscópica. Se comienzan a formar en el 25º día de la fase embrionaria y hacia la octava semana termina la génesis del esbozo ocular, que seguirá madurando hasta el noveno mes. La estructura de un ojo, una vez maduro, se puede ver en la figura IV.1. De una forma muy simplificada, puede considerarse como una cavidad esférica recubierta por tres capas (externa, media e interna). La cavidad esférica, a su vez, puede considerarse dividida en tres cámaras (anterior, posterior y vítrea).

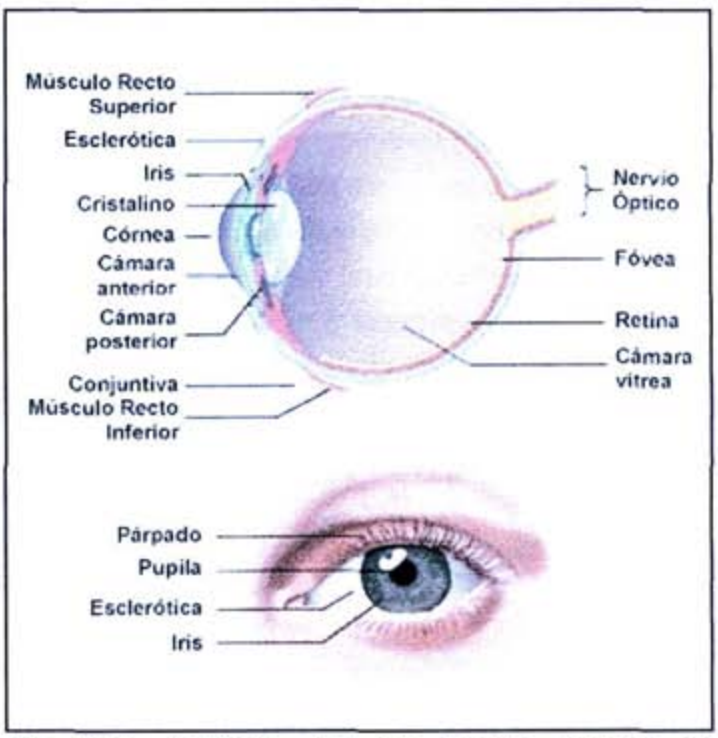


Fig. IV.1: Anatomía del ojo (imagen tomada de http://adam.com)

La capa externa está compuesta por la ***esclerótica*** y la ***córnea***. La esclerótica es una membrana opaca, densa y fibrosa de color blanco, que está formada por fuera por una capa muy vascularizada (es decir, con muchos vasos sanguíneos) contribuyendo a la nutrición del globo ocular. La esclerótica presenta dos orificios principales, uno posterior por donde salen las fibras del nervio óptico, y otro anterior donde se localiza la córnea. La córnea es una capa que comunica ópticamente al exterior con el interior del globo ocular, proporcionando una protección frente a elementos externos. Se encuentra unida a la esclerótica por medio del *limbo* y se puede considerar como una lente externa que posee el mayor poder refractivo dentro del ojo. El limbo es la zona de transición entre la córnea y la esclerótica que contiene las estructuras responsables del drenaje del humor acuoso.

La capa media, también denominada *úvea*, se considera dividida en dos partes, la úvea posterior o *coroides*, y la úvea anterior, formada por el *cuerpo ciliar* y el ***iris***. La úvea posterior es un manto vascular situado entre la esclerótica y la retina (que se verá posteriormente). El cuerpo ciliar está situado entre el coroides y el iris y presenta dos porciones, el *músculo ciliar*, formado por fibras musculares lisas circunferenciales que hacen posible la acomodación del *cristalino* y la *porción epitelial*, que se encarga de realizar la unión con la retina y la producción del humor acuoso.

El **Iris** es uno de los componentes de la capa media, y consta de un *estroma* con células pigmentadas y de un *epitelio* que, además de células pigmentadas, contiene los ***músculos esfínter y dilatador del iris***, que actúan como diafragma ocular. El Iris presenta una apertura en su parte central, que se denomina ***pupila***. El Iris forma la barrera entre la cámara anterior y posterior del glóbulo ocular, y por tanto se encuentra situado entre la córnea y el cristalino.

La capa interna del globo ocular se denomina *retina*, y es la capa sensorial del ojo, cuya función es transformar la luz en un impulso nervioso que será dirigido al cerebro. Está compuesta por diez capas, pero topográfica e histológicamente, la retina puede dividirse en tres tramos: la *ora serrata*, que es la terminación anterior de la retina sensorial situada a unos 7mm del limbo; la *retina periférica*, con un predominio de *bastones*; y la *retina central*, de unos 6mm de diámetro, situada en el polo posterior, en cuyo centro está la *mácula*. En el centro de la mácula, se encuentra la *fóvea*, que es un área deprimida, avascular, donde sólo existen conos, por lo que constituye la zona de máxima visión.

En el interior del globo ocular, se encuentra el *cristalino*, que es una lente biconvexa transparente, avascular y carente de nervios. El cristalino sirve de frontera entre la cámara vítrea (rellena del humor vítreo) y las cámaras anterior y posterior (rellenas de humor acuoso).

La parte del globo ocular que se encuentra en contacto con el exterior, córnea y parte de

la esclerótica, se encuentran a su vez protegidos por los párpados y por segregaciones de las glándulas lagrimales. Tanto la superficie interior de los párpados, como la cara anterior de la esclerótica, están tapizados por la *conjuntiva*, que es una mucosa delgada y trasparente. Por último, el movimiento del globo ocular está controlado por una serie de músculos que lo rodean: cuatro *músculos rectos* y dos *músculos oblicuos*.

IV.1.2. POTENCIALIDAD DEL IRIS PARA IDENTIFICACIÓN

Vista la anatomía del ojo y centrando el análisis en la localización del iris dentro de dicho órgano, se concluye que el iris es un tejido pigmentado de alta movilidad y que se encuentra visible desde el exterior, debido a la trasparencia de la córnea, y gracias a ésta, perfectamente protegido de agentes externos. Todo esto confiere al iris las siguientes características, desde el punto de vista de su potencial aplicación a identificación biométrica:

- Estabilidad frente a cambios originados por accidentes, debido a la protección que le confiere la córnea.
- Fácil mecanismo de detección de *"sujeto vivo"*. Pequeñas variaciones en la iluminación, producen alteraciones en la apertura de la pupila. Incluso, con iluminación fija, el iris no se encuentra estático, sino que presenta pequeñas variaciones en su apertura.
- Los datos (en este caso, la imagen), se puede capturar de forma no invasiva, al ser visible desde el exterior por la transparencia de la córnea.
- El intento de emular el falsificar el iris de una persona, conllevaría operaciones quirúrgicas que podrían dañar muy seriamente la visión.

Todas estas características son, sin duda, muy importantes a la hora de estudiar la viabilidad de esta técnica. Sin embargo falta la característica fundamental: la **unicidad**. Según varios estudios, los cuales quedan reflejados en [Dau93], en el patrón visual del iris hay más información que identifica unívocamente a una persona, que en una huella dactilar. De hecho, los dos ojos de una persona poseen patrones distintos, siendo ésta una característica muy importante que tiene que ser considerada en el sistema al no ser la imagen de los dos ojos intercambiables. Estudios más detallados, han llevado a la conclusión de que incluso los hermanos gemelos poseen patrones de iris bien diferenciados. Esto conlleva a que esta técnica presenta una unicidad extremadamente alta, lo que llevaría a unas tasas de falsa aceptación nulas, garantizando, por tanto, la viabilidad de esta técnica biométrica.

IV.1.3. NACIMIENTO Y EVOLUCIÓN DE LA TÉCNICA

La idea de utilizar el patrón del iris para identificar a las personas fue propuesto inicialmente en 1936 por el oftalmólogo Frank Burch. En la década de los 80 la idea apareció en diversas películas de ficción (James Bond, Misión Imposible, etc.), pero no sería hasta 1987, cuando otros dos oftalmólogos americanos, ***Leonard Flom*** y ***Aran Safir***, patentaron el concepto de Burch. Su incapacidad para poder desarrollar el sistema, les empujó a contactar con ***John G. Daugman***, profesor por entonces de la Universidad de Harvard, para que éste desarrollase los algoritmos necesarios para realizar el reconocimiento biométrico a través del patrón del iris.

Estos algoritmos, patentados por Daugman en 1994, y publicados en parte en [Dau93], son la base de todos los sistemas de reconocimiento por iris existentes. Flom, Safir y Daugman fundaron ***IriScan Corp.*** (http://www.iriscan.com), empresa que tendría en su poder la patente y que se encargaría de licenciarlo a otras compañías, tales como integradores de sistemas y desarrolladores que quieran explotar productos de reconocimiento basados en iris. Una de esas compañías es ***Sensar Corp.*** (http://www.sensar.com), que lanzó al mercado una cámara especial para adquirir las imágenes de iris en los cajeros automáticos. El sistema de Sensar lo adquirió NCR para integrarlo en su línea comercial de cajeros automáticos bancarios. Actualmente, el producto de NCR está siendo experimentado por distintas entidades financieras. En España, ***Argentaria*** (http://www.argentaria.es) adquirió dos unidades que pondrá en pruebas en breve.

IV.2. CAPTURA DE LA IMAGEN

A la hora de empezar el desarrollo del prototipo, se realizó un estudio sobre el método a utilizar para capturar las imágenes de iris. Dentro de las posibilidades se consideraba el uso de cámara fotográfica convencional, cámara fotográfica digital y cámara de video. También se planteó la posibilidad de trabajar en el rango infrarrojo. La decisión final sobre el método de captura elegido se realizó teniendo en cuenta tres factores fundamentales. Por un lado, la facilidad de compra (en precio y plazos), así como la idea de aprovechar el equipo adquirido para futuros desarrollos de otras técnicas, impulsó la utilización del rango visible en lugar del infrarrojo. Por otro lado, la inferior calidad de una imagen capturada con una cámara de vídeo, respecto a una imagen fotográfica, impulsó al uso de cámara fotográfica. Por último, la incomodidad de usar una

película fotográfica convencional, que debería ser revelada y posteriormente digitalizada por un escáner, frente a la facilidad de obtención de la imagen por una cámara digital, eliminó el uso de una cámara fotográfica convencional.

Una vez determinado que el método de captura a utilizar sería una cámara fotográfica digital, se tuvo que plantear cual, de todas las disponibles en el mercado, había que adquirir. El desconocimiento de la resolución mínima con la que había que captar del patrón de iris, implicó las siguientes decisiones:

- utilizar una cámara que pudiera obtener una muy alta resolución;
- aprovechar la resolución que podía obtenerse con la cámara, enteramente para la captura del iris, es decir, a que en la foto apareciese únicamente el ojo del sujeto;
- el sujeto no se debería ver amenazado por la cámara, es decir, no se debería colocar ésta muy cerca de su ojo; y
- la captación a la distancia elegida no supusiera una deformación de la imagen capturada.

Con todas estas consideraciones, se optó por la compra de una cámara digital profesional (Kodak Professional DCS 315). Esta cámara, al no ser compacta, permitía utilizar cualquier objetivo comercial compatible Nikon. Por otro lado, realizaba el almacenamiento de las fotografías en tarjetas flash PCMCIA, permitiendo la descarga de las mismas en cualquier ordenador portátil, o de sobremesa con un lector de tarjetas PCMCIA. La resolución que permite la cámara es de 1,5 millones de puntos, y cada imagen capturada ocupaba 4.490 kilobytes. Tenía flash incorporado, así como multitud de opciones para la captura de la imagen (velocidad, compensación, apertura, etc.).

Fig. IV.2: Cámara y objetivo utilizados

Para conseguir el acercamiento necesario, se utilizó un objetivo Micro-Nikkor 105mm f/2.8D. Este objetivo está recomendado por el fabricante para micro-fotografía, permitiendo un acercamiento de hasta 31cm y proporcionando un alto rendimiento a diversas distancias de enfoque, tanto cercanas como lejanas.

Superada la fase de elección del dispositivo de captura, hubo que diseñar el entorno de captura. Esta segunda fase radicó en tratar el tema de la iluminación que debería recibir el ojo

para obtener una fotografía de calidad. En el tratamiento de este punto, apareció el primer gran problema: la alta capacidad de reflexión de la córnea. La córnea, al ser una superficie lisa y bien lubricada, refleja todo rayo de luz que le llega. Para evitar este problema, se siguió una mezcla de las sugerencias planteadas en [Dau93] y [Wil97], utilizando un foco de iluminación localizado y polarizado. Dicho foco se colocó en la parte inferior de la cámara, de forma que iluminara de abajo hacia arriba, provocando un reflejo de luz localizado en el cono inferior del iris. Para evitar dicho reflejo, se polarizó la luz del foco mediante láminas polarizadoras. Un polarizador, colocado en cuadratura con el del emisor de la luz, situado en el objetivo de la cámara, eliminó, en la foto obtenida, el reflejo anteriormente mencionado.

Sin embargo, el uso de dicho filtro polarizador en el objetivo, resta luminosidad que entra en el objetivo, provocando una pérdida de sensibilidad de la cámara. Teniendo en cuenta la velocidad con que se mueve el iris, la apertura y velocidad de la cámara no podían ser escogidos al azar (una velocidad demasiado lenta, provocaría una imagen borrosa del iris). Por tanto, hubo que aumentar la luz incidente. Este aumento se intentó de dos formas. La primera fue aumentando la intensidad del foco, lo cual provocó un alto rechazo por los usuarios debido al calor y luminosidad recibida. La segunda fue utilizando un segundo punto de luz de corta duración y también localizado. Este segundo punto fue el flash incorporado en la cámara, el cual provoca un reflejo localizado en las inmediaciones del centro de la pupila, y por tanto, fácilmente eliminable.

La imagen obtenida se puede ver en la figura IV.3, a la cual se le ha disminuido el tamaño para facilitar la edición de este capítulo.

Fig. IV.3: Foto tomada de un usuario

Sin embargo, aunque las decisiones tomadas han servido para realizar una captura de fotos de iris de alta calidad, no se considera que el prototipo sea adecuado para su uso final. Habría que estudiar, y de hecho se proponen como lineas futuras de trabajo:

- La utilización de cámara de video, en lugar de cámara fotográfica. Las cámaras de video tienen mayor sensibilidad a costa de una menor resolución. Esa mayor sensibilidad evitaría el uso de focos de alta intensidad. Además, utilizando cámaras de vídeo, se pueden incorporar algoritmos de detección de sujeto vivo, tal y como ya se

ha comentado.

- El posible uso de luz infrarroja, en lugar de luz visible, tanto en la iluminación como en la captura. De esa forma se aumenta la comodidad del usuario, al no percibir el foco de iluminación. Se podría llegar a pensar que el uso de este tipo de luz, implica una pérdida de información, al no apreciar el color del iris. Sin embargo, cabe recalcar de nuevo que lo que se va a analizar no va a ser el color, sino la textura del iris, por lo que, como se verá en el próximo apartado, lo primero que se realizará será pasar la imagen de color a blanco y negro.

IV.3. PRE-PROCESADO DEL IRIS

La etapa de pre-procesado toma una gran importancia en esta técnica, ya que la labor de adaptar la señal a los requisitos del bloque de extracción de características va a conllevar:

- La localización del iris dentro de la imagen.
- La detección de los bordes del iris. En este caso hay que tratar con dos bordes: el exterior (frontera con la esclerótica) y el interior (límite de la pupila).
- Eliminación de las partes de la imagen no deseadas.
- Compensación del tamaño del iris, debido a la distancia del sujeto respecto al objetivo, y de la dilatación o contracción de la pupila.

Todos estos puntos se van a desarrollar en dos secciones, una primera dedicada a la localización, detección y aislamiento del iris respecto a la imagen completa del ojo, y una segunda encargada de las transformaciones necesarias para la eliminación de aquellas zonas que no importan a la imagen y la compensación entre distintas tomas de la imagen.

Sin embargo, antes de entrar en los detalles del trabajo realizado, es preciso hacer una aclaración sobre las partes del iris que van a ser de interés para esta técnica. Tal y como se puede ver en la figura IV.4, las fotos que normalmente se captan del ojo de un sujeto son ligeramente distintas de la mostrada en IV.3. La diferencia radica en que en estado normal, la parte superior o inferior (o ambas) del iris puede estar tapada por el párpado correspondiente impidiendo, por tanto, la extracción de características correspondientes a dichas zonas.

Basándose en las ideas sugeridas por Daugman, se ha decidido dividir el iris en 4 conos (superior, inferior, izquierdo y derecho), eliminando los dos primeros del proceso de localización del iris, del de extracción del borde externo y de la transformación, considerando únicamente los conos laterales en estos casos.

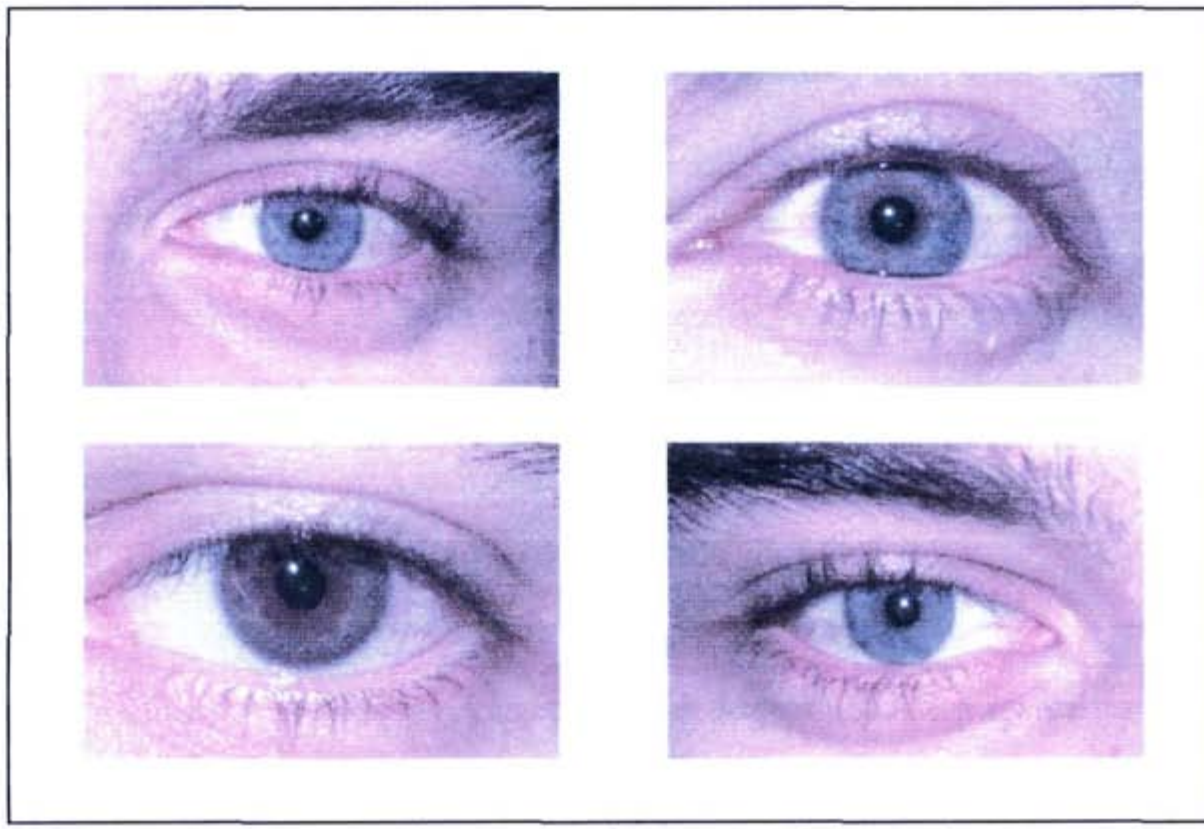


Fig. IV.4: Muestras de usuarios. Nótese la ocultación de parte del iris por los párpados

IV.3.1. DETECCIÓN Y AISLAMIENTO

El primer paso en el pre-procesado, teniendo en cuenta las características de las imágenes capturadas, es una conversión a blanco y negro, seguido de un estiramiento del histograma. Una vez realizado esto, se va a proceder a la detección del borde externo del iris, mediante los siguientes pasos:

1. Se obtiene una copia de la imagen 4 veces más pequeña (para aligerar el coste computacional).

2. Se elimina, mediante un umbral, las partes de la imagen sobre-expuestas, debido a la utilización del flash. Una vez realizado esto, se vuelve a estirar el histograma.

3. Se establece una cuadrícula, en cuyos puntos se situarán los centros del algoritmo de detección de bordes. El punto que determine el mejor borde, será tomado como el centro del iris, realizándose así, al mismo tiempo la localización del iris y la detección del borde externo.

4. Partiendo de un punto elegido (x_0,y_0), se toma éste como centro y a partir de él se muestrea la imagen, tomando puntos a partir de un incremento de radio (Δ_r) y un incremento de ángulo (Δ_θ), buscando el múltiplo n de Δ_r que maximiza el parámetro D:

$$D = \sum_m \sum_{k=1}^{5} \left(I_{n,m} - I_{n-k,m} \right) \qquad \textit{(IV.1)}$$

$$I_{i,j} = I(x_0 + i\Delta_r \cos(j\Delta_\theta), y_0 + i\Delta_r \operatorname{sen}(j\Delta_\theta))$$

donde m son aquellos múltiplos de Δ_θ que caen en los conos laterales del iris e $I(x,y)$ son los valores de intensidad de la imagen.

5. Una vez encontrado el punto de la cuadrícula que proporciona el máximo para D, se crea una nueva cuadrícula, con mayor resolución, y que sólo abarca el cuadrado formado por los puntos comprendidos entre el anterior y el posterior del escogido, tanto en el eje horizontal como en el vertical.

6. Se vuelve a realizar el mismo proceso que en el punto 4, obteniendo un centro más más refinado (al ser la cuadrícula de mayor resolución).

7. Una vez localizado el centro, se disminuye el factor Δ_r para obtener una mayor precisión en la posición del borde, determinando la distancia del centro al borde mediante el $n\Delta_r$, siendo n el valor que maximiza D.

Una vez detectado el borde externo, se aplican las trasformaciones necesarias al centro y el valor del borde para obtener los correspondientes en la imagen original. Se recorta la imagen original formando un cuadrado que englobe al iris detectado, y se eliminan aquellos puntos que quedan fuera de la circunferencia que enmarca al iris. Una vez realizado esto, se vuelve a hacer una copia de dicha imagen, se eliminan mediante umbral los puntos de sobre-exposición y se

estira el histograma. Esta última operación va a permitir aprovechar todo el rango dinámico de intensidad en el iris, de forma que, aunque éste sea oscuro, se va a poder distinguir de la pupila a la hora de detectar el borde interno.

Para detectar el borde interno, se podía pensar en utilizar el mismo centro y buscar un nuevo máximo de D, al considerar que la pupila y el iris son concéntricos. Sin embargo, según lo comentado en [Dau93], y demostrado con la experiencia, la pupila no es concéntrica con el iris, sino que suele estar algo inferior y hacia la nariz, llegando esta desviación, en algunos casos, a ser del 15%. Por tanto, partiendo de dicho centro, se va a crear una cuadrícula que abarque el ±20% del tamaño del iris (es decir, de la imagen obtenida del paso anterior), y se le va a volver a aplicar el mismo proceso que para el borde externo.

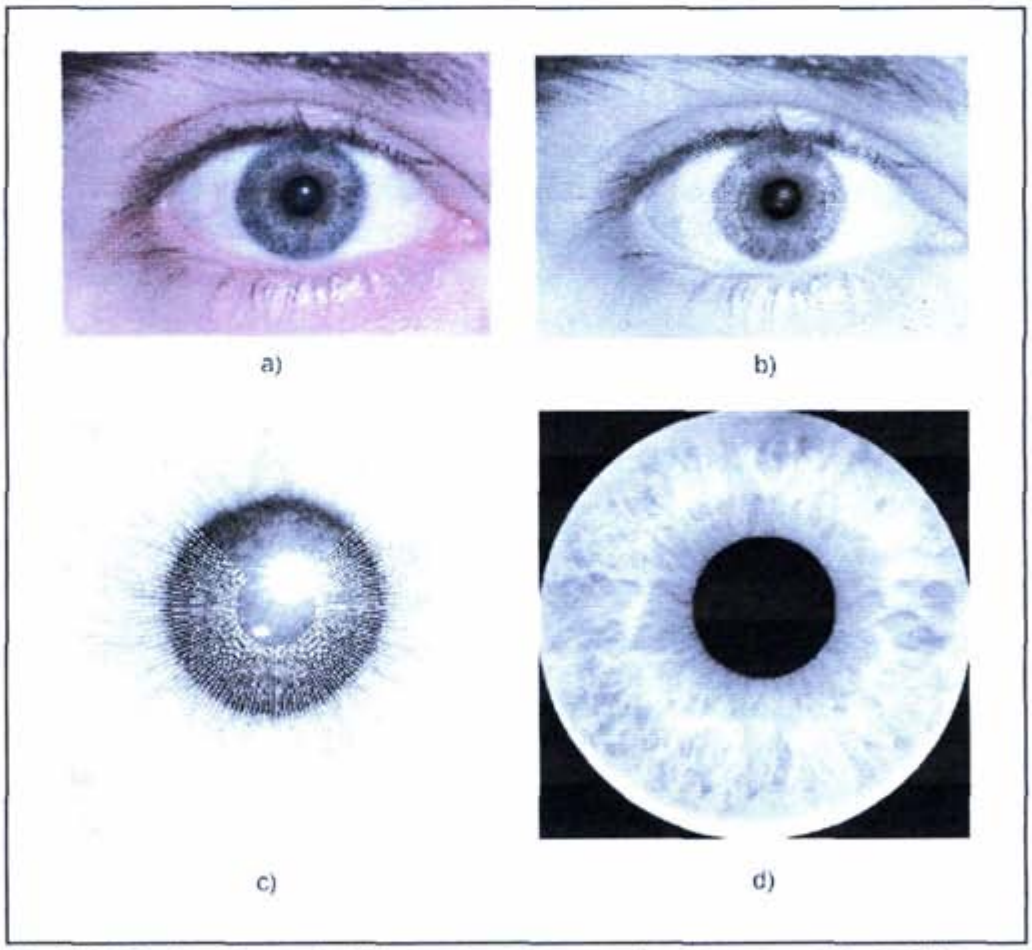


Fig. IV.5: Distintas fases del bloque de pre-procesado: a) imagen original; b) imagen pasada a blanco y negro, con los puntos muestreados para la detección del borde externo; c) puntos muestreados para la detección del borde interno; d) iris resultante de la detección de bordes.

El resultado, vuelve a ser un punto central (x_p, y_p), y una distancia desde ese punto a la

frontera entre pupila e iris. Los puntos comprendidos dentro de la circunferencia definida, se anulan en la imagen resultante de la detección del borde externo, y se vuelve a realizar un estiramiento del histograma, obteniendo el iris aislado del resto de la imagen. En la figura IV.5 se pueden observar las distintas operaciones realizadas con la imagen del ojo, para la obtención del iris aislado (parte d) de la figura). Nótese los puntos de muestreo de la imagen para las detección de los bordes externo e interno, donde se evita, para el caso del borde externo, los conos superior e inferior por posible superposición de los párpados.

Analizando con un poco más de detalle la figura IV.5, se puede observar que b) es la imagen en blanco y negro de a), en la que se han atenuado las zonas sobreexpuestas de esta última (paso 2 del algoritmo dado). Hay que hacer constar, que la imagen de b) en realidad es realidad 4 veces más pequeña que a), aunque en la figura las representa al mismo tamaño por razones puramente de facilitar la visualización. Los puntos que aparecen en los conos laterales del ojo en b), y que en dicha figura aparecen centrados en la pupila, es la posición final alcanzada por el algoritmo, ya que durante el transcurso del algoritmo, dichos puntos serán trasladados a uno y otro lado para encontrar el máximo que localice el borde y, al mismo tiempo, el centro del iris.

En la imagen c) se puede observar que, una vez detectado el borde externo, se ha tomado una sección de la imagen dentro de dicho borde, centrada en el punto detectado anteriormente, y se ha procesado, esta vez a tamaño natural, para encontrar el borde interno. Debido a que en este caso la superposición de los párpados no afectaría (ya que de hacerlo, no quedaría visible parte de iris para poder hacer la identificación), se han tomado puntos, no solamente en los conos laterales, sino también en el inferior (el superior no se ha tomado por interferencia del flash de la cámara, el cual al estar colocado en una posición superior, recae siempre en dicho cono).

Como se ha comentado ya, se repite el mismo proceso que se ha efectuado para el borde externo, para el caso del borde interno, tomando estos nuevos puntos y, por tanto, localizando el centro de la pupila y dicho borde, quedando el iris totalmente localizado y aislado del resto de la imagen, tal y como se ve en d).

IV.3.2. TRANSFORMACIÓN

Una vez aislado el iris de toda la imagen, hay que considerar las variaciones debidas al tamaño del mismo y a la dilatación de la pupila. Para simplificar el algoritmo de extracción de características, se va a realizar una transformación, de forma que en los datos que se le van a pasar a dicho bloque:

- estén suprimidos los conos superior e inferior;
- el tamaño de los datos sea el mismo independientemente del tamaño del iris y de la pupila.

Para realizar esto, se ha hecho un muestreo, tanto en radio como en ángulo, de la imagen del iris obtenida anteriormente, según el sistema de ecuaciones (IV.2), donde: $J(x,y)$ es la nueva imagen; $IE(a,b)$ es la imagen resultante de los pasos anteriores, encontrándose el centro de la pupila en (x_p,y_p); r_i, r_e y Δ_r son respectivamente el radio interno, el radio externo y el incremento del radio; Δ_θ es el incremento de ángulo; y $\mathcal{N}$ es el conjunto de los números naturales.

$$J(x,y) = IE(x_p + r\cos\theta\,,\, y_p + r\,\mathrm{sen}\theta)$$

$$r = r_i + (x-1)\Delta_r \quad , \quad \forall x \in \mathcal{N} : x \le \frac{r_e - r_i}{\Delta_r}$$

$$\theta = \begin{cases} \dfrac{-\pi}{4} + (y-1)\Delta_\theta & , si \quad y \le \dfrac{\pi}{2\Delta_\theta} \\ \dfrac{3\pi}{4} + (y-1)\Delta_\theta & , si \quad y > \dfrac{\pi}{2\Delta_\theta} \end{cases} \quad , \quad \forall y \in \mathcal{N} : y \le \frac{\pi}{\Delta_\theta} \qquad \textbf{(IV.2)}$$

De una forma visual, la transformación realizada se ilustra en la figura IV.6, donde se puede observar como cada uno de los conos laterales, mediante muestreo de radio y ángulo, se convierte en una imagen cuadrada, que tomada como matriz rectangular, sus columnas indicarán fracciones del radio, mientras que las filas serán incrementos de ángulo. Concatenando ambas imágenes, se obtiene la matriz rectangular que se utilizará en el bloque de extracción de características.

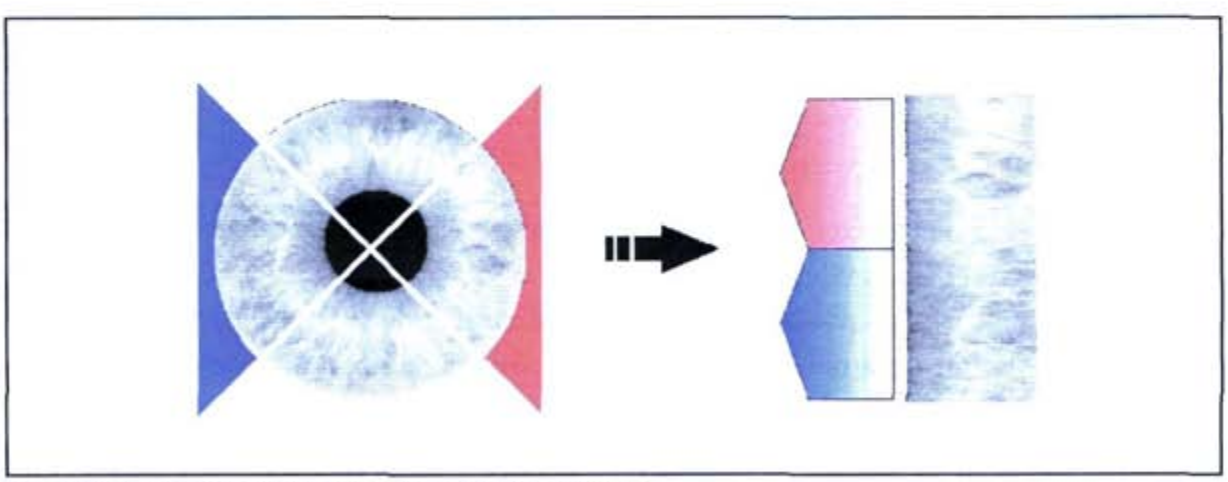


Fig. IV.6: Ilustración sobre la transformación realizada

Debido a que el muestreo se realiza en función de la separación entre el borde externo y el borde interno, siempre se coge el mismo número de puntos y, por tanto, la matriz resultante será siempre del mismo tamaño, lo cual facilitará el tratamiento del siguiente bloque.

IV.4. EXTRACCIÓN DE CARACTERÍSTICAS

Una vez realizado el pre-procesado de la imagen, obteniendo una matriz rectangular de datos que reflejan un muestreo de la intensidad de los conos laterales del iris, se entra en el bloque de extracción de características. A la hora de decidir el método a extraer, se analizaron las distintas posibilidades que se habían presentado en la escasa bibliografía dedicada a este tipo de técnica. De todas las alternativas, la escogida fue el análisis multi-resolución mediante filtros de Gabor, los cuales vienen dados por la siguiente expresión:

$$g(x,y,\varphi_k,\lambda) = \exp\left\{-\frac{1}{2}\left[\frac{(x\cos\varphi_k + y\,\mathrm{sen}\varphi_k)^2}{\sigma_x^2} + \frac{(-x\,\mathrm{sen}\varphi_k + y\cos\varphi_k)^2}{\sigma_y^2}\right]\right\} \cdot \exp\left\{\frac{2\pi(x\cos\varphi_k + y\,\mathrm{sen}\varphi_k)^2}{\lambda} i\right\} \qquad \textit{(IV.3)}$$

donde φ_k es la orientación, λ es la escala y σ_x y σ_y son los parámetros de dispersión de la envolvente del filtro para las coordenadas x e y, respectivamente. Por tanto, los coeficientes de Gabor de la imagen $J(x,y)$ resultante del pre-procesado, serán, para cada escala y orientación:

$$c(x,y) = J(x,y) * g(x,y,\varphi_k,\lambda) \qquad \textit{(IV.4)}$$

Múltiples pruebas con distintas orientaciones, escalas y coeficientes de dispersión, llevaron a unos resultados muy pobres en relación al esquema de clasificación, siendo el mejor un 76,4% de éxito. Estos resultados, muy alejados de los inicialmente esperados y de los detallados en [Dau93], llevaron a replantearse el método de extracción de características a utilizar.

Por otro lado, el coste computacional derivado de la convolución de la imagen con el filtro (operación IV.4), era muy elevado. Para tener una idea, en un ordenador Pentium II 300 Mhz, realizado el programa en Matlab, traduciendo la extracción de forma automática a C, el tiempo

que se tardaba en extraer los coeficientes para 4 orientaciones y 4 escalas era superior a 20 minutos (cabe notar que, si bien Matlab tiene muchas ventajas para la investigación, los tiempos de ejecución alcanzados son muy malos, esperándose un cambio drástico con la traducción completa de todos los algoritmos a C).

Teniendo en cuenta unas ideas débilmente esbozadas en [Dau93], basadas en el estudio de la media de las componentes de los filtros de Gabor, se planteó la posibilidad de, en lugar de utilizar filtrado, ponderar segmentos de la imagen por los valores de un filtro de Gabor. En concreto, teniendo en cuenta que la parte imaginaria de un filtro de Gabor tiene media nula, se puede estudiar la variabilidad de la intensidad de zonas localizadas de una imagen, extrayendo características de dicha variabilidad. Por tanto, los coeficientes obtenidos serían:

$$c(i,j) = \sum_{x=1}^{N}\sum_{y=1}^{M} J\left(i + x - \frac{N}{2}, j + y - \frac{M}{2}\right) \cdot \mathrm{Im}\left[g(x,y,\varphi_k,\lambda)\right] \qquad \textit{(IV.5)}$$

donde *(i,j)* son puntos en la imagen *J* elegidos para obtener los coeficientes, y *N* x *M* es el tamaño del filtro *g* elegido.

Por tanto, la imagen *J* se divide en un determinado número de secciones, solapadas o no (dependiendo de lo próximo que se encuentren los puntos de la cuadrícula). Cada una de esas secciones se multiplica por el filtro *g*, obteniéndose un coeficiente (o característica). Esta misma operación se repite para todas las escalas y orientaciones deseadas.

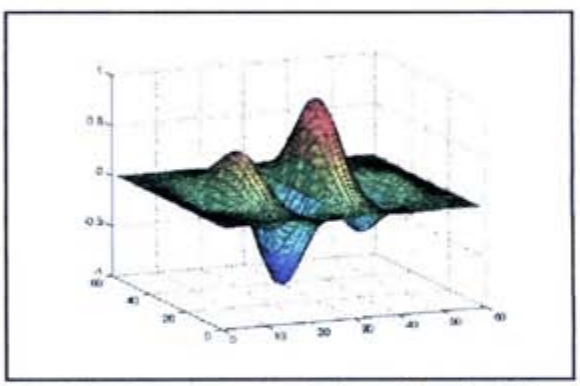


Fig. IV.7: Parte Imaginaria de un filtro de Gabor

Con este sistema se consiguieron excelentes resultados, como se verá en la próxima sección, pero cabe decir que, para unos valores de *N* y *M* de 20, sin solapar las secciones, una escala de 10, cuatro orientaciones (0, $\pi/4$, $\pi/2$ y $3\pi/4$) y desviaciones idénticas, e igual a 3, para cada eje, el tiempo de cálculo, para las mismas condiciones mencionadas anteriormente, bajó de los 15 segundos.

En la actualidad se está trabajando en encontrar una explicación, así como una solución, al hecho de que el resultado utilizando filtrado multi-resolución sea bastante peor que el obtenido mediante ponderación. Aún ya iniciados estos estudios, la complejidad de los mismos los hacen aptos para ser propuestos como línea futura de trabajo, tal y como se indicará en el capítulo correspondiente.

IV.5. VERIFICACIÓN: MÉTODO Y RESULTADOS

Con las características extraídas se planteo la utilización de distintos métodos de verificación. Con los buenos resultados obtenidos previamente por otras técnicas, así como por ser el método utilizado por Daugman, se decidió comenzar el estudio por la Distancia de Hamming (ya descrita en el capítulo I). Siguiendo las pautas de Daugman, se decidió aplicar la distancia de Hamming en su versión para componentes binarias. Por tanto se realizó una transformación de las características extraídas para pasarlas a binarias. Dicha transformación fue asignar un 1 a aquellas características cuyo valor fuera positivo o nulo, y un 0 a aquellas que tuvieran valor negativo.

Los resultados obtenidos fueron tan satisfactorios, que eliminó la idea de plantear otros métodos de verificación, debido al mínimo coste computacional de la Distancia de Hamming en sentido estricto.

Por otro lado se simplificó el sistema, ya que el reclutamiento sólo necesita de una única fotografía, lo que redundará en una mayor aceptabilidad por parte del usuario final.

IV.5.1. BASE DE DATOS

La no disponibilidad de una base de datos de irises para identificación (es decir, con varias tomas de cada sujeto) de dominio público, forzó a realizar todo el trabajo de investigación sobre la captura de la imagen (que ya se ha comentado en el apartado correspondiente) y a iniciar el desarrollo con la creación de una base de datos propia.

Los requisitos de memoria (ya que por cada toma se ocupan 4,5 MB), así como la incomodidad del sistema utilizado, no permitieron que el tamaño de la base de datos creada fuera tan grande como le hubiese gustado al autor de esta Tesis. Sin embargo, se intentó que en la base de datos pudiera estar recogido el mayor número de factores que pudiesen afectar al rendimiento del sistema desarrollado. De esta forma, se capturaron irises de distintas tonalidades (desde el azul claro al marrón oscuro), de cada usuario se tomaron muestras de los dos ojos y al menos 8 muestras de cada uno. Así se pudo demostrar el rendimiento de la etapa de pre-procesado (al

probar distintas tonalidades), y la afirmación de que los patrones de los iris de los dos ojos de una persona no eran iguales. En la figura IV.8 se puede observar una muestra de cada uno de los ojos tomados.

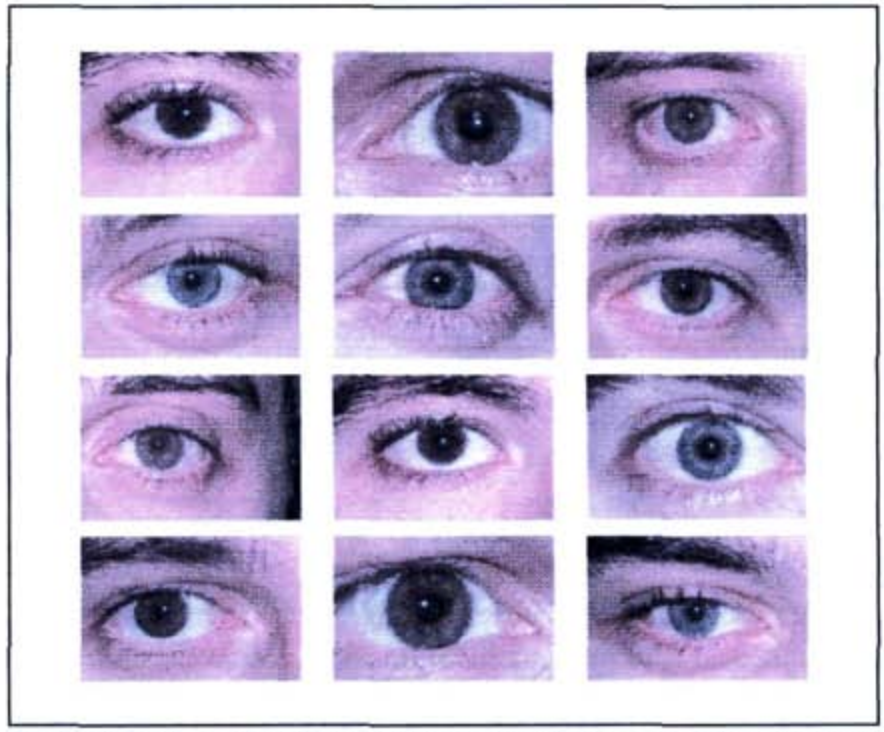


Fig. IV.8: Muestras de cada uno de los ojos incluidos en la Base de Datos

IV.5.2. RESULTADOS

Para analizar el rendimiento del sistema, se procedió a realizar un estudio respecto a la dimensión del vector de características, es decir, del número de secciones que se van a extraer de la imagen que se introduce en el algoritmo de extracción de características. Como se verá, y tal y como ya se ha comentado, los resultados mediante la Distancia de Hamming van a ser tan positivos, que no se ha considerado útil el estudio de otros métodos de verificación, que implicarían un coste computacional superior. Por otro lado, como la Distancia de Hamming en sentido estricto (es decir, con componentes binarias), sólo requiere un único vector de reclutamiento, tampoco ha sido necesario realizar el estudio de la variación del número de estos.

Se van a mostrar los cuatro casos más significativos de variación de la dimensión del vector de características, los cuales se pueden ver detallados en la tabla IV.1. Uno de los casos,

el de 512 bits, hace un estudio de la variación del rendimiento con el cambio de incremento de ángulo en la etapa de pre-procesado. Los otros tres, analizan el rendimiento con respecto al solapamiento de las secciones, desde no tener solapamiento (256 bits), solapamiento sólo en el eje de las y de la imagen J (992 bits) y solapamiento en los dos ejes de J (1860 bits).

Tabla IV.1: Variación del tamaño del vector de características

Dimensión	Δ_θ	Solapamiento en J_x	Solapamiento en J_y
256	1	0	0
512	0,5	0	0
992	1	0	50%
1860	1	50%	50%

Observando la primera de las gráficas de la figura IV.9, podemos observar que el error en clasificación decrece según aumenta el tamaño. El aumento de la resolución angular en el pre-procesado, que implica una mayor cantidad de datos a ser tratada por el algoritmo de extracción de características, no compensa, ya que introduciendo solapamiento con una resolución inferior, se consiguen mejores resultados. El resultado en clasificación ya denota el éxito de esta técnica, consiguiendo, en su peor condición un porcentaje de error inferior al 7%, y obteniendo cuando se utiliza solapamiento, un éxito del 98,3%.

En cuanto a autenticación, lo primero que se observa es que la EER[11] siempre se encuentra por debajo del 10% y en el caso de solapamiento, por debajo del 5%. Sin embargo, el mejor resultado que se puede mostrar, es la viabilidad de crear sistemas de muy alta seguridad, en los que la FAR sea nula, con unos valores de FRR aceptables. Esto se puede observar en los dos casos de solapamiento, donde para obtener una FAR nula, la FRR puede estar por debajo del 15%.

En particular, el caso de 1860 bits, presenta unas gráficas de error muy próximas, con un FRR prácticamente constante y por debajo del 5%. Su EER es del 3,6%, y para una FAR nula, el valor de su FRR es solamente de 3,51%.

[11] Las definiciones de las tasas de error EER, FAR y FRR se encuentran en I.3.3.

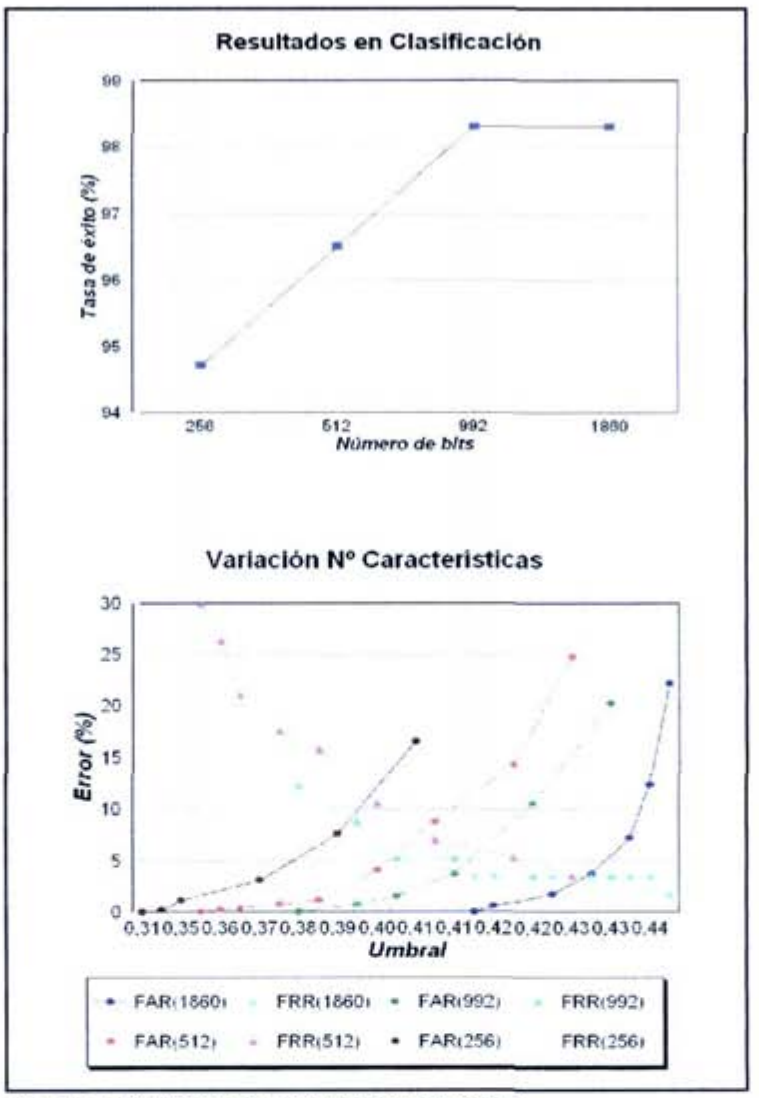


Fig. IV.9: Gráficas de Resultados obtenidos

IV.6. CONCLUSIONES

En este capítulo se ha analizado la técnica de Autenticación Biométrica mediante el Patrón del Iris, además de explicar el desarrollo realizado. Los resultados obtenidos han sido más que satisfactorios, consiguiendo un sistema potencialmente utilizable en entornos de muy alta seguridad, tal y como se ha visto en el apartado anterior.

Sin embargo, durante el desarrollo del sistema, se han ido planteando nuevas posibilidades y caminos alternativos, que habría que considerar para intentar mejorar, aún más, los resultados obtenidos. Entre estas líneas futuras que se plantean están, no sólo las ya comentadas sobre la captura de la imagen (uso de cámara de vídeo y de infrarrojos), sino también nuevas técnicas de extracción de características, como las basadas en análisis multi-resolución (tanto con filtros de Gabor como con Wavelets), ya sea mediante los coeficientes obtenidos, o por el estudio de los cruces por cero de dichas transformadas.

CAPÍTULO V:

ESTUDIO COMPARATIVO DE LAS TÉCNICAS BIOMÉTRICAS TRATADAS

Una vez descritos los desarrollos llevados con las distintas técnicas biométricas que se han tratado en esta Tesis, es momento de hacer un estudio comparativo de los resultados obtenidos. Por tanto, se dedicará este breve capítulo a realizar dicho estudio, contemplando aquellos factores que se estiman de una mayor importancia para la potencial incorporación de estas técnicas dentro de las Tarjetas Inteligentes.

Este capítulo va a estar estructurado en cuatro apartados, atendiendo cada uno a un parámetro comparativo entre las técnicas, más un último de conclusiones globales. El primero de ellos, será el que atañe a la aceptación de las técnicas biométricas por parte del usuario. El segundo versará sobre los tamaños, tanto de los patrones como de las muestras a ser verificadas. Seguirá un apartado sobre los tiempos de realización del reclutamiento y de la verificación, éstos últimos divididos en dos bloques: en primer lugar los de pre-procesado y extracción de características; y en segundo lugar el del algoritmo de verificación. Posteriormente, se establecerá la comparativa respecto al rendimiento del sistema, de acuerdo a las tasas de error en autenticación. Las conclusiones se irán estableciendo según se vayan desarrollando cada uno de los apartados, dándose una valoración global en el último apartado.

V.1. ACEPTACIÓN POR LOS USUARIOS

En los capítulos anteriores ya se ha comentado bastantes anécdotas sobre la aceptación que los distintos sujetos utilizados para crear la Base de Datos han mostrado sobre el sistema. Por tanto, sintetizando:

- En los sistemas basados por **voz** existe, si no un rechazo, sí un mal uso del sistema en aquellas situaciones en las que la locución de una frase no surge de forma natural. Por tanto, se recomienda este tipo de sistemas para aplicaciones basadas, por ejemplo, en telefonía, donde utilizando técnicas de texto independiente (o incluso dependiente si siempre se le fuerza al sujeto a decir, por ejemplo, su D.N.I.), se puede producir tanto el reclutamiento como la verificación sin ningún tipo de problemas (salvo los derivados de la algoritmia).

- En los sistemas basados en geometría del **contorno de la mano**, la aceptación por parte de los usuarios ha sido total, resultando un sistema amigable, fácil de usar e, incluso según dicho por algunos usuarios, simpático.

- En los sistemas basados en el **patrón del iris ocular**, ha existido un leve rechazo, principalmente por el flash utilizado en la captura. Se intentó quitar el flash para evitar ese rechazo, pero la iluminación excesiva necesaria para capturar la imagen, provocaba un rechazo aún mayor. Es, por tanto, necesario abrir una nueva línea de investigación sobre sistemas basados en otro tipo de sensores de luz, de mayor sensibilidad, y con otro tipo de iluminación (por ejemplo, la infrarroja), tal y como se comentó en el capítulo correspondiente.

Atendiendo, pues, a la aceptación del usuario, la mejor técnica ha resultado la de **contorno de mano**, al no presentar ningún tipo de rechazo ni connotación negativa. Posteriormente se situaría la de **patrón del iris ocular**, técnica en la que hay que trabajar para eliminar el flash, provocando un rechazo prácticamente nulo. Por último se colocaría la basada en **voz**, al necesitar que su campo de aplicación sea muy específico para ser aceptado con naturalidad.

V.2. TAMAÑO DE LOS DATOS

Tal y como se puede observar en la figura V.1, se va a realizar la comparativa atendiendo al tamaño del patrón necesario, y al tamaño de las muestras a ser verificadas. La comparativa se ha efectuado entre:

- **Voz**, utilizando GMMs, con 7 mezclas, coeficientes Mel, varianza mínima de 0.01, 60 segundos de vector de reclutamiento y 3 segundos de muestra para la verificación.

- **Mano**, con 5 vectores de reclutamiento y 25 características, utilizando:
  - Distancia Euclídea
  - Distancia de Hamming
  - GMMs

- **Iris Ocular**, utilizando Distancia de Hamming, con 1860 bits (233 bytes).

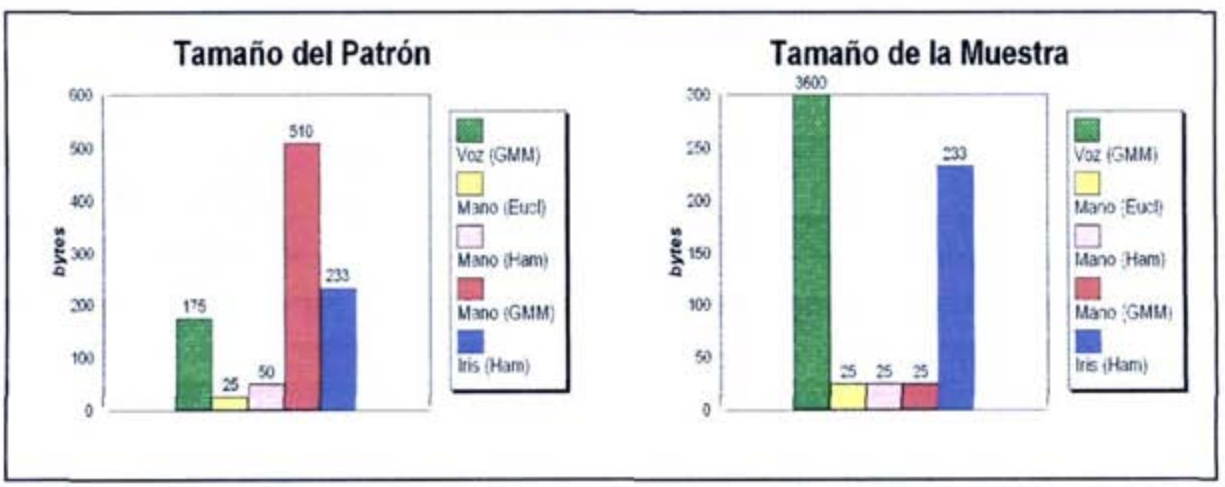


Fig. V.1: Gráficas comparativas del tamaño de los datos utilizados para cada una de las técnicas

Las gráficas muestran que para todos los casos, el tamaño del patrón es admisible para su almacenamiento en una Tarjeta Inteligente, puesto que siempre se encuentra ampliamente por debajo de la capacidad típica de las Tarjetas (entre 2 y 4 kilobytes). Destaca la técnica basada en mano, ya que los métodos de verificación utilizados dan el máximo y el mínimo tamaño del patrón. Atendiendo al tamaño más alto del patrón (510 bytes), hay que tener en cuenta que se ha utilizado un byte para cada característica y, además, se ha utilizado el mayor número de éstas. Este tamaño podría ser drásticamente reducido bajando el número de características y cambiando la codificación de éstas.

En cuanto al tamaño de las muestras a ser verificadas, observamos que tanto la técnica de mano, como la de iris, manejan un tamaño de la muestra que es aceptable para su transmisión en una única orden hacia la tarjeta (el tamaño máximo del buffer de transmisión, admitido por el protocolo, es de 255 bytes). Sin embargo, se observa que en el caso de verificación por voz, el tamaño de la muestra supera, con mucho, al resto de las técnicas (3.600 bytes), necesitando al menos 15 instrucciones para transmitir dicha muestra a la tarjeta. Este hecho, tal y como se verá en el capítulo siguiente, será determinante para la viabilidad de su implantación.

A la vista de los datos obtenidos, se puede concluir que, atendiendo al tamaño de los datos utilizados, la técnica basada en el **contorno de la mano**, utilizando los métodos de verificación de distancias (tanto Euclídea, como de Hamming), presenta unos valores excelentes. La misma técnica, utilizando GMMs, así como la basada en el **iris**, muestran su compatibilidad con la tecnología de las Tarjeta Inteligentes, mientras que se pone en entredicho la potencial integración de la técnica de **voz** dentro de las Tarjetas.

V.3. TIEMPOS DE EJECUCIÓN

Utilizando las técnicas tal y como se han utilizado en el apartado anterior, se ha efectuado la medida de los tiempos necesarios para el Reclutamiento y la Autenticación. El tiempo de Reclutamiento se ha medido globalmente (incluyendo pre-procesado, extracción de características y cálculo del patrón), mientras que el de la Autenticación se ha dividido en dos: el necesario para realizar el pre-procesado y la extracción de características; y el ocupado en el algoritmo de verificación. La razón de esta división radica en que en el sistema final que se quiere crear, la verificación la haría la tarjeta, mientras que el resto lo realizaría el terminal asociado.

Hay que hacer una salvedad sobre los valores de los tiempos que se observan en la figura V.2. Estos tiempos han sido calculados con Matlab, al estar desarrollados los prototipos de cada una de las técnicas en dicho sistema de programación matemática. Como es bien sabido, este sistema, si bien presenta muchas otras ventajas, tiene el inconveniente del tiempo de ejecución obtenido en los programas realizados. Es por eso que los tiempos son muy superiores a los que, a priori, cabría esperar en un sistema comercial. Estos tiempos se podrían bajar drásticamente traduciendo los algoritmos a lenguaje de alto/medio nivel como, por ejemplo, C++, y ejecutando

los programas resultantes en máquinas de dedicación exclusiva. Sin embargo, los valores obtenidos son totalmente válidos dentro del ámbito de este capítulo, en el que lo único que se pretende es la comparación entre técnicas.

Por tanto, atendiendo a los resultados obtenidos para el Reclutamiento, se observa que la técnica de voz necesita un tiempo muy superior al necesario por cualquier de las otras dos técnicas (casi 30 veces superior a la de mano y cerca de 8 veces superior a la de iris). Por su parte, tal y como se puede ver en el tiempo necesario para el pre-procesado y la extracción (en la gráfica contigua), la técnica de iris se encuentra limitada por los mencionados dos bloques, siendo el tiempo de cálculo del patrón despreciable frente a aquel. Por su parte, la técnica basada en geometría de la mano sigue presentando los mejores valores.

Fig. V.2: Gráficas obtenidas de la medición de Tiempos de Ejecución

Por otro lado, el tiempo necesario para realizar el pre-procesado y la extracción es bastante bajo tanto en técnicas de voz, como de mano, manteniéndose bastante alto, tal y como ya se ha dicho, el de técnicas de iris. Esto induce a que resulta necesario un profundo trabajo de optimización de estos dos bloques para el caso de reconocimiento por iris.

Por último se ha estudiado el tiempo necesario para realizar la verificación, uno de los datos más importante para la integración dentro de las Tarjetas Inteligentes. Se observa que todos los valores se encuentran por debajo de los 30 milisegundos, tiempo totalmente compatible con lo requerido para una función de autenticación dentro de las Tarjetas. Sin embargo, la técnica de voz vuelve a mostrar unos valores excesivos, necesitando 16 segundos (debidos a tener que ejecutar el GMM entrenado, tantas veces como vectores de características posee la muestra, que en el caso estudiado son 300).

Se puede concluir que, a la vista de los tiempos conseguidos, la técnica basada en **mano**

sigue mostrando las mejores propiedades, mientras que la basada en **voz** vuelve a plantear serios problemas para los propósitos de esta Tesis. La técnica basada en **iris**, si bien no muestra problemas frente a su integración dentro de la Tarjeta Inteligente, sí que necesita una optimización de los programas que irán dentro del terminal.

V.4. RENDIMIENTO OBTENIDO

Volviendo a utilizar las mismas técnicas, con las mismas configuraciones que se han detallado en el segundo apartado, se han sacado tres valores de las tasas de error, para realizar la comparativa entre las técnicas. De esta forma se ha medido la EER[12], la FAR (cuando la FRR alcanza el 10%) y la FRR (cuando la FAR se igual al 10%). De esta forma se obtiene las gráficas de la figura V.3.

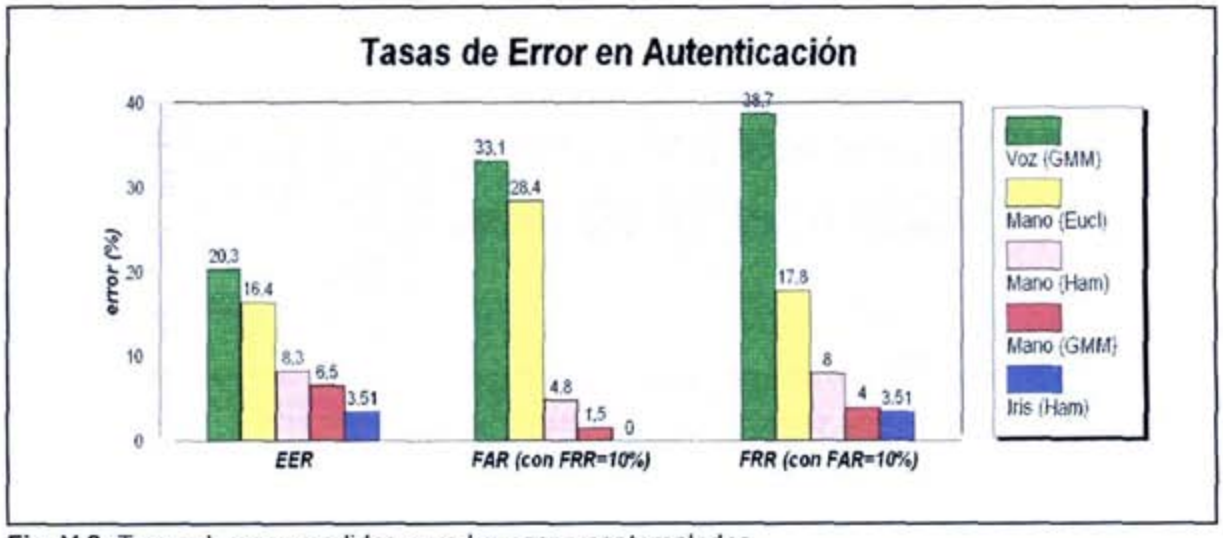


Fig. V.3: Tasas de error medidas para los casos contemplados

La primera conclusión que se obtiene, observando los tres tipos de valores obtenidos, es la inconveniencia de utilizar tanto la técnica de voz, como la de mano con Distancia Euclídea, al estar todos sus valores por encima del 10%, lo cual supone un rendimiento excesivamente bajo del sistema.

[12] Los conceptos de Tasa de Igual Error (EER), de Tasa de Falso Rechazo (FRR) y de Tasa de Falsa Aceptación (FAR), fueron introducidos en el Capítulo I.

En línea opuesta, destaca la técnica de iris, ya que sus tasas de error son las más bajas, llegando a obtener un 0% de FAR (incluso con valores de FRR por debajo del 10%, tal y como se comentó en el capítulo anterior). Los valores obtenidos facultan a esta técnica para intentar abordar su implantación en entornos de alta/muy alta seguridad. Por su parte, la técnica de contorno de mano, obtiene unos resultados bastante aceptables para facilitar su implantación, tanto con Distancia de Hamming, como utilizando GMMs.

V.5. CONCLUSIONES

Sintetizando las conclusiones obtenidas en cada uno de los apartados anteriores, se obtiene, como primera observación, la inconveniencia del uso de la técnica basada en **voz**, al obtener tasas de error muy altas, tamaños de muestra excesivamente elevados y tiempos de reclutamiento y verificación muy por encima del resto de las técnicas. Además, su limitada aplicabilidad debido a la dificultad de obtener un buen uso por parte de los usuarios en la mayor parte de potenciales aplicaciones, y que los valores obtenidos sean incompatibles con la tecnología de las Tarjetas Inteligentes, obliga a tomar la decisión de no utilizar esta técnica (decisión que se verá en el próximo capítulo).

La técnica basada en **iris**, aún teniendo que mejorar en muchos aspectos, presenta unas tasa de error muy prometedoras y que empujan, aún más, a continuar el trabajo en sus distintos bloques, especialmente para reducir el tiempo de pre-procesado y extracción de características.

Por último, la técnica basada en **contorno de mano**, además de haber presentado muy buenos resultados tanto en la aceptación por parte de los usuarios, como en el tamaño de los datos necesarios y en los tiempos de ejecución, llega a obtener unas tasas de error muy aceptables, que avalan su utilización en gran número de entornos y aplicaciones.

Se ha querido mostrar de una forma gráfica las conclusiones globales, atendiendo a los parámetros numéricos obtenidos en los apartados anteriores. De esta forma, por cada apartado, se han sumado los valores numéricos obtenidos para cada técnica, se ha invertido el valor (para eliminar el efecto de los malos resultados) y se han establecido tres diagramas de sectores, tal y como se puede observar en la figura V.4.

En esta figura queda patente los buenos resultados obtenidos con la técnica de **contorno de mano**, sobre todo utilizando métricas, así como la importancia que toma la técnica basada en el **iris** a la hora de analizar el rendimiento del sistema, en relación a las tasas de error obtenidas.

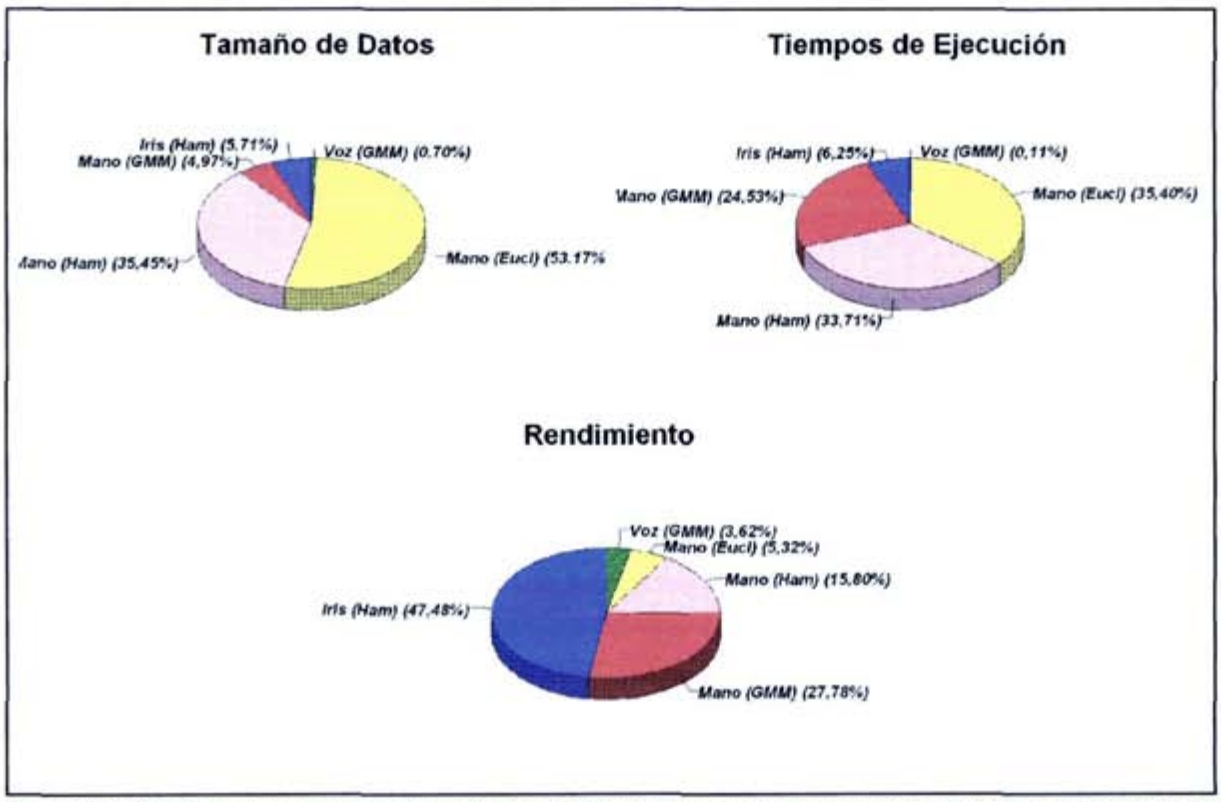


Fig. V.4: Diagramas de sectores que reflejan la importancia de cada una de las técnicas respecto a los parámetros medidos.

CAPÍTULO VI:

AUTENTICACIÓN BIOMÉTRICA

MEDIANTE TARJETAS INTELIGENTES

Con todo lo expuesto en los capítulos precedentes, es momento de plantear la solución a la problemática inicialmente planteada en esta Tesis: la Autenticación Biométrica dentro de la Tarjeta Inteligente. Por tanto, en este capítulo se desarrollará la solución propuesta y se comentarán los resultados obtenidos en la maqueta experimental. Es preciso hacer una recomendación al lector no familiarizado con la tecnología de las Tarjetas Inteligentes: para un mejor seguimiento de este tema puede ser recomendable consultar el Apéndice A.

El presente capítulo se iniciará con un nuevo acercamiento a las soluciones integradas actualmente en Tarjetas Inteligentes. Seguirá con la relación de condicionantes para permitir la viabilidad de la autenticación biométrica según los requisitos planteados. Dichos condicionantes justificarán las decisiones tomadas a la hora de definir los mecanismos necesarios para la nueva Arquitectura de Autenticación (estructuras de datos, arquitectura de seguridad e instrucciones). Posteriormente se detallará el prototipo desarrollado y los resultados obtenidos para, finalmente, acabar el capítulo con las conclusiones obtenidas.

VI.1. PANORÁMICA ACTUAL

En un sistema basado en Tarjetas Inteligentes, la autenticación del titular de la tarjeta es necesaria por dos motivos fundamentalmente. El primero es, al igual que en los sistemas basados en banda magnética, facilitar un mecanismo al sistema para comprobar que la persona que quiere utilizar la tarjeta es el titular de la misma. La segunda, propia sólo de las Tarjetas Inteligentes, es poder proteger el acceso a determinada información o a determinas operaciones que existan dentro de la tarjeta (por ejemplo, se podría proteger el débito del monedero de la tarjeta por medio de la autenticación de su titular).

El único mecanismo que actualmente poseen las Tarjetas Inteligentes para facilitar este servicio es la utilización de una clave personal, conocida comúnmente como PIN[13], siglas anglosajonas de Número de Identificación Personal [Bri88][San99a][Zor94]. Esta clave consta simplemente de un determinado número de dígitos que debe recordar el titular de la tarjeta. Para facilitar el recuerdo al titular, el PIN suele ser sólo de 4 o 5 dígitos, y éstos son dígitos decimales. Aquí radica variación entre lo que la tarjeta entiende como clave personal y lo que normalmente se conoce como PIN. Las claves que suele manejar una Tarjeta Inteligente suele ser una sucesión de 8, 16 o más bytes, tamaño muy superior al necesario para almacenar un PIN[14].

Por tanto, para discernir entre los dos conceptos, la clave de la tarjeta que se encarga de almacenar el PIN, se denomina habitualmente CHV-Key[15], acrónimo de *Card Holder Verification Key*. Esta clave, cuya longitud depende de la máscara de tarjeta utilizada, puede contener el PIN, rellenando, de alguna forma, con bytes constantes (como podrían ser caracteres nulos) o valores dependientes de la aplicación o del titular (nombre de la empresa que emite la tarjeta, fecha de nacimento del titular, etc.). Las soluciones son todo lo diversas que permita la imaginación, por

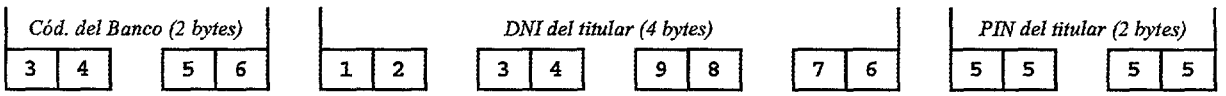
[13] Se va a utilizar el acrónimo anglosajón por homogeneidad, no sólo con la literatura existente, sino también con el argot aceptado en el sector.

[14] Sin realizar ningún tipo de codificación, para almacenar 4 dígitos decimales, se necesitaría un máximo de 4 bytes. Si además se utilizase una codificación BCD, por ejemplo, el número de bytes necesario sería de 2. Por ejemplo, el PIN 1234, se puede almacenar con el byte 12 (hexadecimal) y el byte 34 (hexadecimal).

[15] De nuevo, por homogeneidad con la literatura existente, se toma el término anglosajón. El acrónimo en castellano sería Clave-VTT, procedente de Clave de Verificación del Titular de la Tarjeta.

lo que no existe ninguna regla general para el almacenamiento del PIN. Esta falta de generalidad se utiliza a veces como mecanismo extra de seguridad frente al fraude.

Un ejemplo de cómo se puede generar la CHV-Key a partir de un PIN, puede ser el concatenar bytes correspondientes a la empresa emisora de la tarjeta, datos propios del titular de la tarjeta (que se encuentran grabados en la misma) y el propio PIN. Imagínese el siguiente caso: la empresa emisora es un Banco, cuyo número identificativo es 3456; el dato que se escoge del usuario es el DNI en 8 cifras, que en el caso del usuario del ejemplo será 12.349.876; y el PIN del usuario es 5555. Utilizando codificación BCD, el CHV-Key quedaría:



La CHV-Key se crea en la tarjeta en el proceso de personalización de la misma, es decir, cuando se emite la tarjeta y se graban los datos del titular de la misma. Para grabar dicha clave se escoge un PIN, se codifica según las reglas expuestas en el sistema, y se transmiten a la tarjeta mediante un comando. Si previamente se han satisfecho aquellas condiciones de seguridad definidas como necesarias para la creación de dicha clave, se produce la grabación de la misma.

Para realizar la autenticación del usuario, el titular de la tarjeta teclea su PIN en el terminal. Éste codifica el PIN para formar la CHV-Key y transmite ésta a la tarjeta mediante el comando habilitado en la misma para efectuar dicha operación. Si la verificación es correcta, se habilita el acceso a aquellas informaciones o aquellas operaciones de la tarjeta que estaban protegidas por el PIN. Si la verificación es incorrecta, se decrementa un contador de presentaciones[16] erróneas del PIN, de forma que si dicho contador llega a valor nulo, se bloquea la presentación del PIN en la tarjeta, quedando por tanto bloqueada la información y operaciones involucradas. Dependiendo de la tarjeta, puede existir un mecanismo de desbloqueo del PIN mediante la presentación de una clave administrativa.

El titular de la tarjeta puede cambiar el PIN de la misma de forma que se resulte más familiar. Esto se podrá realizar tantas veces como requiera el usuario, siempre que antes se hayan satisfecho las condiciones de seguridad establecidas (presentación del PIN anterior, presentación de una clave administrativa, etc.).

El último punto que falta por tratar en la panorámica actual es la forma en la que se transmite la CHV-Key a la tarjeta. Esto siempre se realiza mediante un comando, ya sea el de

[16] En el argot del sector "presentar" una clave indica transmitir una clave a la tarjeta para que ésta la verifique.

grabación, el de actualización o el de presentación. Sin embargo, los bytes correspondientes a la CHV-Key pueden ir en claro[17] (tal y como es la propia clave) o cifrado mediante alguna clave. En caso de optarse por esta última solución, se puede utilizar una clave fija, o una clave que cambie con la sesión de utilización de la tarjeta. Esta solución proporciona un nivel mayor de seguridad, con el coste de incrementar la complejidad del sistema y de los terminales donde se vaya a realizar la autenticación del titular. La elección de utilizar cualquiera de las soluciones propuestas depende de como se haya configurado la tarjeta, y por tanto, de los requisitos de seguridad definidos en el sistema.

Es necesario mencionar los proyectos nacionales e internacionales que se han llevado a cabo en línea con la incorporación de la Biometría dentro de las Tarjetas Inteligentes. Si bien es verdad que todas las empresas del sector, tanto a nivel nacional, como internacional, tratan de seguir las evoluciones de la Biometría, sólo se conocen dos proyectos que hayan intentado integrar ambas tecnologías, uno nacional y otro europeo.

Por mencionarlos desde el punto de vista cronológico, el europeo es un proyecto subvencionado por la Unión Europea, conocido por el acrónimo CASCADE, en el que participaron varias empresas entre las que destaca Gemplus (multinacional francesa líder mundial en ventas de tarjetas con circuito integrado), como socio principal. Dicho proyecto tuvo un problema principal, el exceso de ambición. Se trataba de crear una nueva dimensión dentro del sector de las Tarjetas Inteligentes, creando una tarjeta con un micro-procesador de arquitectura RISC de 32 bits, con unas mayores capacidades de memoria, mayor potencia de cálculo y que incorporara algoritmos de Redes Neuronales. Una de las aplicaciones de dicha tarjeta sería la telefonía móvil, actuando como tarjeta SIM en el sistema GSM (para lo cual estaba la empres Nokia en el proyecto), facilitando la autenticación biométrica del usuario mediante voz. El proyecto fracasó parcialmente, no conociéndose resultados sobre la aplicación de autenticación biométrica. Sin embargo, sirvió para crear una nueva arquitectura de Tarjeta Inteligente que se aprovechó para lanzar al mercado una tarjeta JavaCard muy por encima en prestaciones que el resto de sus competidores. Dicho proyecto tuvo su origen en los meses finales de 1996.

El segundo proyecto, éste de índole nacional, se denomina *Transacciones Seguras a través de Internet: Autenticación Biométrica de Usuarios*, y es conocido por el acrónimo *TABU* (Tarjeta de Autenticación Biométrica de Usuarios). Está subvencionado por el Plan Nacional de I+D, fue concedido en diciembre de 1998 y en el participan el GUTI (Grupo Universitario de Tarjeta Inteligente) del Departamento de Tecnología Fotónica de la E.T.S.I. de Telecomunicación de Madrid y el Departamento de Matemática Aplicada de la citada Escuela. Dicho proyecto partió de los mismos trabajos de investigación que han llevado a la realización de esta Tesis, siendo ésta

[17] Es decir, no cifrado.

uno de los principales resultados de dicho proyecto. Resumiendo las características del mismo, también peca de un exceso de ambición, aunque en este caso no tecnológica, sino de variedad de técnicas biométricas. Sin embargo, el estudiar distintas técnicas biométricas ha llevado a sacar conclusiones muy positivas y a encontrar técnicas biométricas susceptibles de ser incorporadas a una Tarjeta Inteligente, tal y como se ve a lo largo de esta Tesis, y fundamentalmente en los resultados de este capítulo.

VI.2. CONDICIONANTES DE LA AUTENTICACIÓN BIOMÉTRICA

Vista la forma en la que actualmente se realiza la autenticación del titular de la tarjeta, se ha obtenido la base sobre la que se va a desarrollar el nuevo esquema de autenticación de usuarios, basado en Biometría. Sin embargo, para poder llevar a cabo un desarrollo coherente, es preciso detectar los condicionantes que van limitar la viabilidad del nuevo esquema. Por tanto, en este apartado se van a tratar dichos condicionantes, realizándose el estudio en dos secciones, que corresponden a las dos fases del utilización de un sistema biométrico: Reclutamiento y Verificación.

Pero antes de entrar en materia, se ha visto conveniente refrescar el esquema de sistema de autenticación, mediante un ejemplo ilustrativo (este esquema ya se introdujo en el Capítulo I). Obsérvese los distintos pasos que aparecen en la figura VI.1.

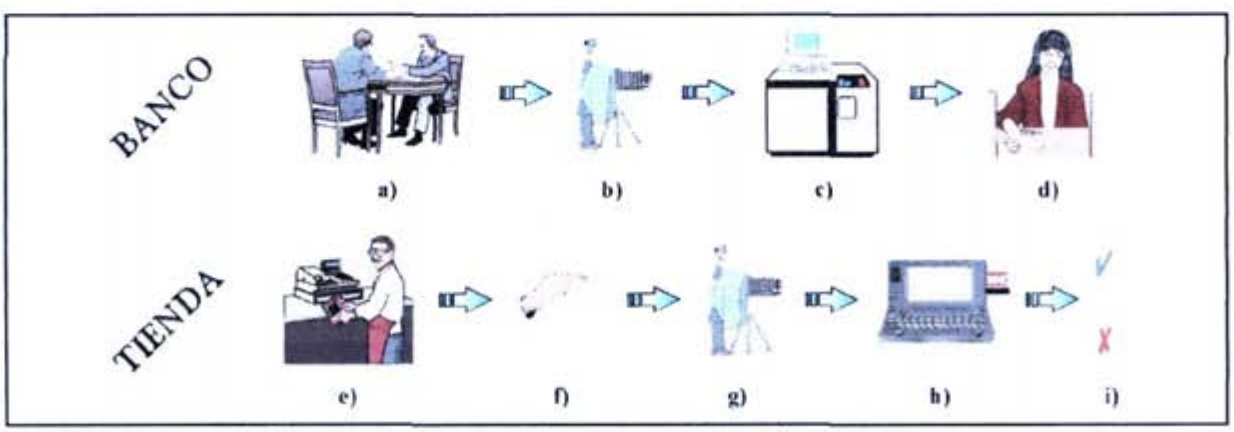


Fig. VI.1: Ejemplo de Sistema de Autenticación mediante Biometría y Tarjetas

Un usuario se acerca a una oficina bancaria, solicitando un servicio (a), para el cual va a

ser necesaria la utilización de una Tarjeta con Autenticación Biométrica. Una vez aceptado el nuevo servicio, se le toma una serie de muestras (b), para posteriormente realizar el cálculo de su patrón y la personalización de su tarjeta (c), es decir, grabarle en la tarjeta sus datos personales, financieros y su patrón biométrico. Una vez obtenida la tarjeta, ésta se entrega al usuario (d). A toda esta fase se la denomina Reclutamiento y típicamente sólo se efectuará una vez en la vida de la tarjeta.

El usuario, una vez que tiene la tarjeta y habiendo sido informado de su uso, ve conveniente acercarse a una tienda a comprar (e). Allí, le entrega la tarjeta al comerciante (f), para que éste proceda al cobro de la mercancía retirada. Para poder hacer el pago, ve necesario utilizar el sistema biométrico y tomará una nueva muestra del usuario (g). Esta muestra es procesada en el terminal del dependiente, obteniendo el vector de características, el cual será presentado a la tarjeta para su comprobación (h). La tarjeta, basándose en el algoritmo, el patrón y el umbral que tiene almacenados, calcula la probabilidad de que el vector de características pertenezca al titular de la tarjeta, aceptando o no la operación (i) si esa probabilidad recae dentro de los márgenes establecidos por el umbral. A toda esta fase, es a la que se le va a denominar como Verificación, pudiéndose realizar tantas veces como permita la tarjeta o el propio sistema.

VI.2.1. RECLUTAMIENTO

Como ya se ha visto, en un sistema de autenticación biométrica, el primer paso es el Reclutamiento. Para realizar este paso, hay que tomar una serie de muestras del sujeto, pre-procesarlas, extraer sus características y, una vez extraídas éstas, obtener el patrón. Dicho patrón ha de ser almacenado para su posterior comparación en la fase de Verificación.

Se podría pensar en realizar todos los pasos dentro de la tarjeta, es decir, facilitar la generación del patrón dentro de la tarjeta. Sin embargo, como se verá, los procesadores incluidos en una Tarjeta Inteligente tienen una baja potencia de cálculo, además de estar muy limitados en memoria y en tiempos de comunicación, por lo que con la tecnología actual no resulta viable el transmitir a la tarjeta la muestra obtenida para que posteriormente ésta obtenga el patrón. Esta solución se deja para futuros trabajos en los que la tecnología a utilizar sea muy superior a la actualmente disponible. La ventaja de esta futura solución radicaría en la homogeneidad a la hora de obtener el patrón, así como en la mayor simplificación de los terminales donde se produzca la autenticación.

En lugar de utilizar esta solución, se va a plantear que el patrón se obtenga en un ordenador asociado y que sea éste el que transmita a la tarjeta el patrón obtenido. En este sistema se plantean una serie de condicionantes. El primero, que no está involucrado con la Tarjeta Inteligente, es la necesidad de que el ordenador mencionado se encuentre securizado, de forma que no se pueda extraer el patrón de ninguno de los usuarios del sistema. Por lo tanto, **un requisito fundamental es que, una vez obtenido el patrón y almacenado en la tarjeta, se borre automáticamente.**

En cuanto a las limitaciones que están relacionadas con la tarjeta, hay que mencionar las siguientes:

- **TAMAÑO DEL PATRÓN.** Este tamaño es fundamental por dos razones:

    - **Capacidad de almacenamiento del mismo:** ya que la memoria disponible en una tarjeta inteligente es muy escasa, aunque ésta se va incrementando año tras año. Con la tecnología actual, y las aplicaciones a incorporar en una misma tarjeta, se podría suponer que un tamaño de patrón superior al kilobyte resultaría inaceptable.

    - **Tiempo de transmisión del patrón:** puesto que al tratarse de una comunicación serie de media-baja velocidad (de 9600 a 115000 baudios) y tamaño de paquete inferior a los 256 bytes, la transmisión de un patrón demasiado grande, puede suponer unos tiempos de latencia muy apreciables. Sin embargo, debido a que el reclutamiento sólo se realiza una vez, esta limitación no resulta tan importante, al contrario de lo que ocurrirá en la fase de Verificación.

- **IMPORTANCIA DE LA INFORMACIÓN TRANSMITIDA.** El patrón es una información altamente confidencial. La difusión del mismo provocaría la ruptura de la seguridad de, no sólo la información de la tarjeta, sino también de todo aquel sistema que para autenticar al usuario utilice la misma técnica biométrica con la misma configuración del patrón. Por tanto, aunque el reclutamiento se realice en un entorno seguro, se antoja necesario el que la transmisión del mismo se realice siempre de forma cifrada y firmada[18]. En el apartado correspondiente al prototipo desarrollado se expondrá una

[18] Este sistema se conoce en el sector como *Secure Messaging*, término anglosajón que significa Mensajería Segura, utilizando datos cifrados. Una breve de explicación del *Secure Messaging* se encuentra en el Apéndice A. Para una información más amplia, se recomienda consultar la normativa en [IS7816] y distintos manuales de Sistemas Operativos de Tarjeta, como por ejemplo [CEC96], [Gem98a], [GyD98] o

forma de realizar este proceso.

VI.2.2. VERIFICACIÓN

Una vez realizado el Reclutamiento, el usuario puede pasar a la fase de Verificación, en donde se le extraerá otra muestra que, tras pre-procesarla y extraer sus características, se calculará el vector de características y se comparará éste con el patrón almacenado. Una propiedad fundamental de esta fase es que, al contrario que el Reclutamiento, ésta se va a ejecutar muchas veces, por lo que cualquier condicionante que se presente en esta fase va a ser determinante para el rendimiento del sistema.

Para el diseño de esta fase, se puede plantear la extracción del vector de características dentro de la tarjeta, de forma análoga a lo comentado en el Reclutamiento. Sin embargo, por las mismas limitaciones tecnológicas esta alternativa va a ser relegada a futuros trabajos. Tomando la misma solución que la utilizada en el Reclutamiento, es decir, obteniendo el vector de características en el terminal y transmitiendo éste a la tarjeta, se plantean varias limitaciones. De nuevo, la primera, la cual queda fuera del entorno de la tarjeta, es que el terminal que capture la muestra y obtenga el vector de características debe ser seguro. El grado de seguridad puede ser algo inferior al ordenador utilizado en el Reclutamiento, ya que aquí lo que se podría llegar a capturar es un único vector de características, el cual no es tan crítico como el patrón, aunque su grado de confidencialidad es muy elevado.

Planteando los condicionantes que se encuentran más relacionados con la tarjeta, se tiene:

- **TAMAÑO DEL VECTOR DE CARACTERÍSTICAS.** Al igual que en Reclutamiento, estas condiciones son de dos tipos:

    - **Capacidad de almacenamiento.** Estas limitaciones no presentan gran importancia, debido fundamentalmente a que dicho vector va a encontrarse en la tarjeta de forma temporal, mientras dure el proceso de verificación. Si el tamaño supusiese una limitación a este respecto, siempre se puede diseñar el algoritmo de verificación para que según le van llegando componentes del vector de características, las vaya procesando y eliminando de la memoria

[Gem99a].

temporal.

- **Tiempo de comunicación.** En este caso, debido a que esta fase se va a ejecutar numerosas veces, cualquier tipo de retraso es fundamental, ya que ralentizará la operativa del sistema, pudiendo producir rechazos por parte del usuario. Hay que tener en cuenta que el usuario actual está acostumbrado a que su autenticación sea prácticamente instantánea.

- **ALGORITMO DE VERIFICACIÓN EMPLEADO.** Las limitaciones vienen impuestas por doble motivo:

  - **Tamaño del código necesario para incorporar el algoritmo a la tarjeta.** Hay que tener en cuenta que el tamaño de ROM de que dispone una Tarjeta Inteligente para almacenar todo el Sistema Operativo se encuentra encuadrado en unas pocas decenas de kilobytes.

  - **Tiempo de ejecución de la verificación.** Por la mismas consecuencias del tiempo de comunicación del vector de características, es imprescindible que la verificación tarde menos de 750 ms. Una verificación de, por ejemplo, 2 segundos, podría suponer un tiempo acumulado en todo el proceso de autenticación demasiado grande para ser aceptable en la mayoría de las aplicaciones.

- **CONSECUENCIAS DE UN FALLO EN LA VERIFICACIÓN.** La gran ventaja de las Tarjetas Inteligentes, frente a otro tipo de tarjeta, es que un determinado número de fallos consecutivos a la hora de presentar una clave puede provocar no sólo el bloqueo de una determinada información, sino incluso la auto-destrucción, por bloqueo total, de toda la tarjeta. Por tanto un sistema nuevo de autenticación, debe proporcionar, al menos, los mismos servicios. Es por tanto imprescindible que si se supera un determinado número de fallos consecutivos en la verificación, se provoque el bloqueo de la autenticación biométrica y, por consiguiente, el bloqueo de la información asociada a dicha verificación. Esto provoca dos decisiones fundamentales:

  - **Número de fallos consecutivos admitidos.** Dependiendo de los requisitos de seguridad de la aplicación a ser instalada, se deberá escoger un número de fallos consecutivos. Habrá que tener en cuenta que la probabilidad de un nuevo rechazo, suponiendo que es el mismo usuario y en las mismas condiciones, será de FRR^n, siendo n el número de intentos consecutivos (es decir, la probabilidad acumulada de falso rechazo decrece con el número de

intentos). Al igual que lo que ocurre con el resto de las claves de una tarjeta, se dejará la posibilidad de que el diseñador de la aplicación seleccione el número máximo de fallos consecutivos admitidos.

- **Posibilidad de desbloqueo de la autenticación biométrica.** Si se ha superado el número de fallos consecutivos admitidos, el proceso de autenticación biométrica quedará bloqueado. Se podría plantear la posibilidad de, utilizando una clave administrativa, se produzca el desbloqueo, de forma que se pueda seguir en la fase de Verificación u obligando a realizar un nuevo proceso de Reclutamiento. La elección de facilitar este servicio y de como configurarlo es un tema para ser tratado muy detenidamente, siendo aconsejable la experimentación mediante proyectos piloto. No obstante, desde un punto de vista riguroso, una vez bloqueada la autenticación biométrica, sería preceptivo no facilitar el desbloqueo, y que el usuario debiera pedir una re-emisión de su tarjeta, pasando nuevamente por un Reclutamiento. Esta decisión está tomada basándose en que parece algo ilógico el que el nuevo sistema de autenticación personal se encuentre finalmente sujeto a la seguridad proporcionada por el sistema ya existente.

- **UMBRAL DE ACEPTACIÓN DEL USUARIO.** La elección de este umbral es, tal y como ya se ha comentado varias veces en anteriores capítulos, el punto más crítico a la hora de diseñar un sistema de autenticación biométrica. Por tanto será necesario que a la hora de crear el patrón dentro de la tarjeta, se incluya también el umbral escogido.

- **SEGURIDAD EN LA COMUNICACIÓN DEL VECTOR DE CARACTERÍSTICAS.** Como ya se ha comentado, el vector de características es una información altamente confidencial, aunque sus requisitos de seguridad no son tan elevados como los del patrón. Por lo tanto, se plantea como necesario el que la comunicación del vector de características que hay que verificar, se haga de forma cifrada y firmada (utilizando *Secure Messaging* cifrado) mediante una Clave de Sesión[19].

[19] Una Clave de Sesión es una clave que se genera al comienzo de una sesión de trabajo y que una vez que se ha terminado dicha sesión, se borra de memoria. Mediante este sistema, cada vez que se produzca una comunicación cifrada del vector de características, estará cifrada con una clave distinta, imposibilitando aún más la obtención de dicho vector por parte de un potencial pirata informático.

VI.3. NUEVA ARQUITECTURA DE AUTENTICACIÓN

Una vez vistos las condiciones de contorno de la nueva solución que se quiere incorporar al problema de la autenticación de usuarios, es hora de plantear dicha solución. Para realizar esto, hay que detallar cada uno de los elementos necesarios a incluir dentro de la Tarjeta Inteligente. Dichos elementos se van a dividir en tres grandes bloques. El primero de ellos tratará de aquellas estructuras de datos que habrá que incorporar para, por ejemplo, almacenar el patrón del usuario. El segundo bloque versará sobre la arquitectura de seguridad a incorporar, es decir, condiciones de acceso, algoritmos de verificación, determinación de umbrales, etc. Por último, habrá que definir aquellos comandos que deben estar incorporados dentro del Sistema Operativo de la Tarjeta Inteligente, para poder realizar todas las operaciones relacionadas con el nuevo sistema de autenticación.

VI.3.1. ESTRUCTURA DE DATOS

A la hora de afrontar un cambio (o ampliación) de la estructura de datos existente en una Tarjeta Inteligente, hay que plantearse dos necesidades principales: el almacenamiento del patrón del usuario y si supone algún cambio este nuevo sistema de autenticación para el resto de las estructuras de datos que contiene la Tarjeta.

En cuanto a la primera necesidad, el patrón puede ser almacenado simplemente en un fichero interno[20] de un tamaño suficiente, siempre que se cumplan una serie de requisitos:

- Su lectura debe estar prohibida (para asegurar la confidencialidad del patrón).
- Su escritura debe hacerse mediante *Secure Messaging* con los datos cifrados mediante una clave de sesión.
- Debe indicarse el tipo de algoritmo que se va a utilizar. Esto producirá un condicionante en la forma que debe tener el patrón, en el caso de que el patrón esté formado por más de un tipo de información (por ejemplo, el patrón de mano utilizando una distancia de Hamming está formado por las medias y por las desviaciones típicas ponderadas). Por tanto, habrá que indicar a qué tipo de algoritmo corresponde ese

[20] Tal y como se puede ver en el Apéndice A, un fichero interno es aquel en el que se guarda una información que va a ser utilizada internamente por la Tarjeta, sin permitir una manipulación directa por parte del usuario. Como ejemplo de este tipo de ficheros, se pueden encontrar todos los ficheros de claves.

patrón, para que de esta forma no se produzcan errores en la ejecución de los algoritmos.

- También debe indicarse el número de fallos consecutivos en la verificación y el número de intentos restantes.
- Y por último, si se habilita el mecanismo de desbloqueo y la forma en la que se produce dicho desbloqueo (si por simple desbloqueo o por nuevo reclutamiento). Para indicar esto último, se habilitará un byte que indique el estado en el que se encuentra la información contenida en el fichero.

Por lo tanto, el patrón va a ser almacenado en un fichero interno, sin estructura y del tamaño necesario como para alojar el patrón y el umbral a utilizar, es decir, se tomarán 2 bytes iniciales para guardar el umbral de verificación, siendo el resto del espacio del fichero para el almacenamiento del patrón. La cabecera del fichero corresponderá a la siguiente:

1 2	3 4	5 6 7 8	9	10	11
ID	TAMAÑO	CA	ALG	NRV	EST

donde:

ID: Es el identificador del fichero.

TAMAÑO: Es el tamaño del cuerpo del fichero, excluyendo la cabecera, es decir, lo que ocupará el patrón.

CA: Condiciones de Acceso. Su codificación se verá al hablar de la arquitectura de seguridad.

ALG: Algoritmo de verificación empleado. La codificación de este byte (en hexadecimal) será:

00 - RFU[21]
01 - Distancia Euclídea
02 - Distancia de Hamming (datos binarios)
03 - Distancia de Hamming (datos continuos)
04 - GMMs
Resto de valores - RFU

NRV: Número de reintentos en verificación. El nibble menos significativo indica el

[21] RFU significa Reservado para Futuros Usos.

número de intentos restantes, mientras que el más significativo indica el número máximo de intentos. Por lo tanto se proporcionarán hasta 15 reintentos. El valor 0 para el nibble más significativo está prohibido.

EST: Estado en el que se encuentra la tarjeta. Su codificación será de acuerdo a la siguiente tabla (siendo el resto de valores RFU):

X	-	-	-	-	-	-	-	**Posibilidad de desbloqueo**
0								Permitido
1								Prohibido
-	X	X	X	X	X	X	X	**Estado del patrón**
	0	0	0	0	0	0	0	A reclutar
	0	0	0	0	0	0	1	Verificación Posible
	0	0	0	0	0	1	0	Bloqueado

Sobre la segunda necesidad planteada, es decir, la necesidad de si la nueva arquitectura plantea variaciones sobre el resto de estructura de datos existente en una Tarjeta Inteligente, cabe decir que la única variación que implicaría, sería la relativa a los cambios en las Condiciones de Acceso. Tal y como se verá en la siguiente sección, no existen tales cambios, ya que si se quiere proteger una información mediante Autenticación Biométrica, se configurará una protección por CHV-Key, indicando que la clave a utilizar será la del patrón biométrico.

VI.3.2. ARQUITECTURA DE SEGURIDAD

Para un Sistema Operativo de Tarjeta Inteligente, el nuevo sistema de autenticación va a suponer cambios bastante importantes en su arquitectura de seguridad. Dichos cambios van a verse en el sistema de condiciones de acceso a la información, en los algoritmos para producir la verificación y, por último, aquellas variables que sean necesarias incluir en la arquitectura de seguridad de la tarjeta para facilitar la autenticación biométrica. Sin embargo, debido a la probada fiabilidad de las soluciones ya existentes, se va a intentar minimizar los cambios en la filosofía de autenticación, de forma que el nuevo sistema, por un lado, se beneficie de la experiencia del antiguo, y por otro, que la integración del nuevo sistema en los Sistemas Operativos de Tarjeta Inteligente existentes en la actualidad sea asequible y, por tanto, viable.

Tomando en primer lugar las condiciones de acceso a la información de la tarjeta (CA), éstas tienen que incorporar la verificación del patrón biométrico como llave para dicho acceso. Esto se podría haber planteado de dos formas diferentes:

- Establecer una nueva condición de acceso basada en la autenticación biométrica. Esta aproximación independiza totalmente la autenticación biométrica del resto de métodos, provocando un cambio en la codificación de dichas CA. Dicho cambio implicaría variar las cabeceras de los ficheros de la tarjeta, llegando incluso a tener que cambiar el tamaño de las mismas.

- Incorporar la autenticación biométrica como si de una CHV-Key fuera, reservando únicamente un número de clave para indicar que la clave es el patrón biométrico. Con esta orientación, el impacto del nuevo sistema en los demás elementos del Sistema Operativo de Tarjeta Inteligente se minimiza, no debiendo realizar cambios en las Estructuras de Datos, sino solamente en el algoritmo general de autenticación.

Esta segunda opción es la que se ha tomado. Para plasmar cómo se codificarían las CA en la Tarjeta, pongamos el caso de un Sistema Operativo con las siguientes limitaciones:

- Para todos los ficheros se asume un máximo de 4 operaciones posibles a realizar con ellos. El numero de operaciones puede ser inferior, pero nunca superior. Por ejemplo, los ficheros elementales tradicionales pueden estar protegidos sólo frente a lectura y escritura, mientras que los de tipo monedero, pueden estar protegidos para lectura, escritura, crédito y débito.

- El número de claves del mismo tipo existentes en un directorio nunca puede ser superior a 16.

- La información se puede proteger mediante claves existentes en el mismo directorio, o en el directorio raiz.

- El cambio de un directorio a otro de su mismo nivel supondrá la eliminación de aquellos indicadores de presentación de claves del directorio de procedencia.

Por lo tanto, la codificación de las CAs en las cabeceras de los ficheros será mediante 4 bytes de la siguiente forma:

1	2	3	4

CA lectura	CA escritura	CA operación1	CA operación2

donde cada uno de los bytes se codifica de la siguiente manera

X	-	-	-	-	-	-	-	**Nivel de protección**
0								Directorio actual
1								Directorio padre
-	X	X	X	-	-	-	-	**Tipo de protección**
	0	0	0					Libre
	0	0	1					Por CHV-Key
	0	1	0					Cifrado por clave (PRO)
	0	1	1					RFU
	1	0	0					Secure Messaging
	1	0	1					RFU
	1	1	0					Secure Messaging cifrado
	1	1	1					RFU
-	-	-	-	X	X	X	X	**Número de clave**

En caso de que la protección sea por CHV-Key, se podrán utilizar como tales sólo 15 claves, en lugar de 16, ya que se reservará el número 0, para indicar al patrón biométrico. En caso de se trate de *Secure Messaging*, ya sea con los datos en claro (es decir, sólo firmado) o con los datos cifrados (es decir, firmado y cifrado), el número de clave indicará la clave a utilizar para generar la Clave de Sesión que facilitará el mecanismo de protección.

La inclusión de nuevos algoritmos de verificación es, sin lugar a duda, el punto más delicado tecnológica y económicamente de la incorporación del nuevo sistema. Mientras que algunos algoritmos de verificación biométrica utilizados no suponen un cambio tecnológico importante frente a los micro-controladores actualmente utilizados (por ejemplo, la distancia de Hamming), otros, como los GMMs, precisan cálculo potente en coma flotante. Técnicamente esto no supondría una limitación excesiva, ya que en la actualidad existen co-procesadores matemáticos que efectúan operaciones de complejidad análoga (por ejemplo criptografía pública). Sin embargo, el interés comercial puede estar muy mermado si la Tarjeta Inteligente resultante tiene un precio alto, al negarse los potenciales clientes a adoptar la solución facilitada (una muestra de este tipo de situaciones se ha dado, y se sigue dando, en relación a las tarjetas

criptográficas, producto que está resultando deficitario tras 3 años de vida).

Por lo tanto, los cambios en la arquitectura de seguridad relacionados con los algoritmos de verificación, radican fundamentalmente en programar dichos algoritmos y crear el acceso pertinente a las rutinas diseñadas. En el apartado dedicado a mostrar el prototipo creado se podrá ver algunos ejemplos del trabajo aquí esbozado.

Los últimos elementos que faltan por tratar de la arquitectura de seguridad son aquellas variables de control que indicarán el estado de la Tarjeta en lo referente a la autenticación. De nuevo se va a plantear una solución compatible con las ya existentes. Esta solución se basará en tener una serie de bits indicadores en memoria RAM de la tarjeta, por cada una de las distintas formas de hacer la autenticación. Esto quiere decir que, teniendo en cuenta el ejemplo que se ha planteado anteriormente, hay hasta un máximo de 16 claves ha ser utilizadas para autenticación (15 CHV-Keys y 1 de Autenticación Biométrica) tanto por parte del directorio actual, como por parte del directorio paterno. Es decir, se necesitarán 4 bytes, utilizando un bit para cada caso.

El incluirlo en memoria RAM facilita, no sólo la velocidad de consulta del bit correspondiente, sino que intrínsecamente permite que al retirarse la alimentación de la tarjeta, se borren esos indicadores, teniéndose que realizar nuevamente la autenticación. Evidentemente, durante la inicialización de la tarjeta (*reset*), esos bits se escribirán a estado desactivado. Cuando se tenga que acceder a una información protegida por autenticación biométrica, se consultará si el bit correspondiente se encuentra activado, lo cual solo se producirá si anteriormente se ha realizado una Autenticación Biométrica, mediante los comandos que se van a ver en la siguiente sección.

VI.3.3. INSTRUCCIONES NECESARIAS

Una vez especificadas las estructuras de datos y la arquitectura de seguridad, el único paso que resta para crear la Nueva Arquitectura de Autenticación es la ampliación del juego de comandos para poder realizar las operaciones de autenticación. Estas operaciones deberán contemplar el reclutamiento, la verificación y el potencial desbloqueo de dicho patrón. Los comandos a tener en cuenta son los que a continuación se detallan. La codificación de los mismos se ha hecho respetando al máximo lo actualmente definido en la norma ISO 7816 [IS7816]. La codificación aparecerá siempre en hexadecimal.

VI.3.3.a. Crear fichero de patrón

La creación de un fichero patrón es una operación, desde el punto de vista del comando, idéntica a la creación de cualquier otro fichero elemental[22], con la salvedad de que hay que indicar que en este caso se trata de un fichero que va a albergar un patrón biométrico. La estructura del comando será:

CLA	INS	P1	P2	Lc	DATOS	Le
84	E0	00	00	19	*datos*	-

donde los *datos* indican:

N° bytes	Contenido	Observaciones
4	83 02 xx xx	Donde xx xx son los dos bytes del identificador del fichero
4	81 02 yy yy	Donde yy yy es el tamaño del fichero: 2 (del umbral) + tamaño patrón
3	82 01 tt	Donde tt es el tipo de fichero (10 para biometría)
6	86 04 ll ss pp qq	Donde ll ss pp qq son las CA de, respectivamente, lectura, escritura, operación 1 y operación 2. En el caso de un fichero de patrón, la operación 1 equivale a desbloqueo. Por tanto, en caso de un fichero patrón ll debe indicar prohibido, ss indicar Secure Messaging cifradocon el número de clave a utilizar y pp prohibido (si no se permite el desbloqueo) o por Secure Messaging con el número de clave a usar (si se permite).
5	85 03 gg vv kk	Donde gg es el código del algoritmo a usar, vv es el número máximo de re-intentos en la verificación y kk es el código de desbloqueo (00 si no hay desbloqueo, 01 si lo hay).
3	ff ff ff	Son los tres bytes menos significativos de la firma (Secure Messaging), obtenida utilizando la Clave de Sesión según las condiciones de seguridad del FD donde se está creando el fichero.

Las posibles respuestas de la tarjeta por orden de comprobación serán:

SW1	SW2	Significado
6E	00	Clase no permitida
6D	00	Instrucción no permitida o incompatible con la clase
6A	86	Parámetros P1 y/o P2 incorrectos

[22] Un fichero elemental (FE) es un fichero que sólo contiene datos, al contrario que un fichero dedicado (FD) que contiene FEs e incluso otros FD.

69	10	Tipo de fichero no existente
6A	85	Longitud de datos de entrada incongruente con tipo de fichero
69	11	Identificador ya utilizado
69	12	Tipo de algoritmo no existente
6A	84	Tamaño insuficiente dentro de la tarjeta
6A	80	Tamaño incongruente con tipo de algoritmo (Si es Hamming con datos continuos el tamaño debe ser par)
69	85	Condiciones de uso no satisfechas (por ejemplo, CA no válida)
69	82	Condiciones de seguridad no satisfechas
65	81	Fallo en la memoria
90	00	Procesamiento correcto

Si la ejecución del comando ha sido correcta (respuesta 90 00), el Sistema Operativo de la Tarjeta Inteligente habrá asignado el espacio necesario en la memoria para alojar en fichero y habrá rellenado la cabecera, indicando que el estado de la clave es *"A reclutar"*.

VI.3.3.b. Escribir fichero patrón

Una vez creado el fichero que va a alojar al patrón, hay que escribir dicho patrón. Esta operación sólo será posible si el estado de dicho fichero es *"A reclutar"*, estando imposibilitada la escritura de dicho fichero en cualquier otro caso. La instrucción será idéntica a la de Actualizar en Binario con Seguridad (conocida por su nombre acrónimo inglés *UpdateBinarySeg*), transmitiendo los datos cifrados. La estructura en el caso particular que se está tratando será:

CLA	INS	P1	P2	Lc	DATOS	Le
04	D6	*P1P2*		*Long*	*datos*	-

donde la codificación de *P1P2* sigue la parte 4 de la norma ISO 7816, donde si el bit más significativo (b_8) de *P1* es 1, entonces b_7 y b_6 de *P1* se colocan a 0 (RFU), y los bits b_5 a b_1 de P1 son el identificador corto del fichero a actualizar, y en *P2* se codifica el desplazamiento del primer byte a ser actualizado desde el principio del fichero. En caso que b_8 de *P1* sea 0, entonces P1P2 es el desplazamiento del primer byte a ser actualizado desde el principio del fichero, el cual ha tenido que ser previamente seleccionado.

Por otro lado *Long* codifica la longitud de los *datos* a transmitir más los 3 de la firma, y los *datos* deben actualizarse en el fichero, de forma que los dos primeros bytes contengan el umbral y los bytes subsiguientes contengan el patrón. Por cada fracción de *datos* a ser enviada,

éstos han de cifrarse y posteriormente firmarse (añadiendo los 3 bytes menos significativos de la firma al final de los *datos*).

Las posibles respuestas de la tarjeta por orden de comprobación serán:

SW1	SW2	Significado
6E	00	Clase no permitida
6D	00	Instrucción no permitida o incompatible con la clase
6B	00	Desplazamiento en P1P2 fuera de rango
6A	86	Parámetro en P1 incorrecto (sólo para selección implícita)
6A	84	No existe suficiente memoria en el fichero
6A	82	Fichero no encontrado
69	82	Condiciones de seguridad no satisfechas
69	81	Comando incompatible con la organización del fichero
67	00	Longitud incorrecta (L_c incompatible con Secure Messaging)
65	81	Fallo en memoria
90	00	Procesado correcto

Si la ejecución del comando ha sido correcta (respuesta 90 00), y ya se han escrito todos los bytes del fichero, el Sistema Operativo de la Tarjeta Inteligente cambiará el estado de la clave a *"Verificación Posible"*.

VI.3.3.c. Autenticación Personal

Para realizar esta operación, se va a utilizar el mismo comando que si se tratase de verificar una CHV-Key utilizando firma y cifrado, ampliando el comando para que se pueda verificar algo de un tamaño diferente a dicho tipo de clave. Por tanto la codificación del comando será:

CLA	INS	P1	P2	Lc	DATOS	Le
04	20	00	*clave*	*Long*	*datos*	-

donde P2, que indica la clave a verificar, se codifica de la siguiente manera:

X	-	-	-	-	-	-	-	Nivel de verificación
0								Directorio padre

1								Directorio actual
-	0	0	-	-	-	-	-	**RFU**
-	-	-	1	-	-	-	-	**Clave de la tarjeta**
-	-	-	-	X	X	X	X	**Número de clave**

Si el número de clave es distinto de 0, *Long* tendrá un valor igual al tamaño de la clave a verificar más 3 (de la firma). En caso de que el número de clave sea 0, se trata del patrón biométrico, por lo que *Long* será igual al tamaño del vector de características ha transmitir a la tarjeta más 3 (de la firma). Por su parte, los *datos* irán cifrados y se le añadirán los 3 bytes menos significativos de la firma obtenida mediante Secure Messaging.

Las posibles respuestas de la tarjeta por orden de comprobación serán:

SW1	SW2	Significado
6E	00	Clase no permitida
6D	00	Instrucción no permitida o incompatible con la clase
6A	86	Parámetros P1 y/o P2 incorrectos
69	83	Método de autenticación bloqueado
69	82	Condiciones de seguridad no satisfechas
67	00	Longitud errónea
65	81	Fallo en memoria
63	Cx	Verificación fallida, x indica el número de intentos restantes.
90	00	Procesado correcto, verificación válida.

Después de realizar todas las comprobaciones correspondientes, si el número de clave es 0, el Sistema Operativo de la Tarjeta Inteligente buscará el fichero de patrón, comprobará que no se encuentra *"Bloqueado"* ni *"A reclutar"* y, en ese caso, leerá el tipo de algoritmo asociado. Con ese dato, ejecutará la rutina correspondiente para realizar la verificación, obteniendo un resultado que comparará con el umbral. Si la comparación es positiva, se responderá 90 00, actualizando el número de reintentos restantes al número máximo. Si la comparación es negativa, se disminuirá el contador de reintentos restantes y se devolverá dicho número en la respuesta (siendo el valor de x) 63 Cx. Si dicho número es 0, el estado del patrón se le pasará a *"Bloqueado"*.

VI.3.3.d. Desbloqueo de Clave

Para realizar esta operación, se va a volver a utilizar el mismo comando que si se tratase de verificar una CHV-Key. La codificación del comando será:

CLA	INS	P1	P2	Lc	DATOS	Le
80	18	00	*clave*	03	*datos*	-

donde P2, que indica la clave a desbloquear, se codifica de la misma manera que en la instrucción anterior, y *datos* contiene únicamente los 3 bytes menos significativos de la firma calculada.

Las posibles respuestas de la tarjeta por orden de comprobación serán:

SW1	SW2	Significado
6E	00	Clase no permitida
6D	00	Instrucción no permitida o incompatible con la clase
6A	86	Parámetros P1 y/o P2 incorrectos
6A	82	Fichero no encontrado
69	82	Condiciones de seguridad no satisfechas
67	00	Longitud errónea
69	85	Condiciones de uso no satisfechas (por ejemplo, no se puede desbloquear la clave)
65	81	Fallo en memoria
90	00	Procesado correcto, desbloqueo efectuado.

Si la respuesta es 90 00, y el número de clave era 0 (es decir, el patrón biométrico) el Sistema Operativo de Tarjeta Inteligente borrará todo el contenido de dicho fichero, y colocará el estado de la tarjeta en *"A reclutar"*.

VI.4. PROTOTIPO DESARROLLADO

Una vez detallado el nuevo sistema de autenticación, era necesario evaluarlo en base a un prototipo. A la hora de plantear el cómo desarrollar dicho prototipo, se plantearon dos posibilidades:

- Diseñar, desarrollar y fabricar una nueva máscara de Tarjeta Inteligente. Esta solución se tuvo que rechazar por motivos puramente económicos, ya que la realización de una máscara supone el contratar un nuevo proceso de fabricación microelectrónica, lo cual supone unos costes iniciales de muchas decenas de millones de pesetas.

- Encontrar otras vías para poder incorporar el nuevo sistema a una máscara ya existente. Al comienzo de esta tesis (1996), esta solución se planteaba como muy difícil, previendo que se tendría que desarrollar todo un Sistema Operativo de Tarjeta Inteligente en base a un micro-controlador comercial incluido en una placa de circuito impreso de dimensiones muy lejanas a las tarjetas inteligentes; es decir, realizar en base a electrónica convencional una emulación de una Tarjeta Inteligente.

Por las razones comentadas anteriormente, se tomó la decisión de utilizar la segunda solución. Afortunadamente, la evolución tecnológica dentro del sector de las Tarjetas Inteligentes, ha jugado en favor de esta Tesis. En 1997 se empezaron a plantar las bases de las Tarjetas Inteligentes con Sistema Operativo Abierto, en las que se podrían incluir rutinas a medida del cliente final, sin necesidad de tener que fabricar una nueva máscara. Los primeros prototipos, aunque defraudaron bastante, supusieron un empuje tecnológico y una guerra comercial entre las grandes empresas del sector. Durante 1998 ya empezaron a verse productos con unas posibilidades muy atractivas, mejorando a lo largo de 1999 donde además, empezaron a aparecer alternativas a las soluciones por entonces tomadas.

En la actualidad se habla de 3 plataformas de Sistemas Operativos Abiertos para Tarjeta Inteligente, siendo éstas:

- **JavaCard:** Sin lugar a duda la más popular de todas debido, fundamentalmente a la gran aceptación del lenguaje Java, diseñado por Sun Microsystems. Se trata de una Tarjeta Inteligente a las que se le pueden añadir rutinas y comandos programados en lenguaje Java. Casi todas las empresas multinacionales han sacado su versión de este tipo de tarjetas, siendo muy distintas las funcionalidades de unas y de otras debido a dos razones: la precipitación comercial de sacar el producto y los cambios en las especificaciones. De este tipo de tarjetas, al ser el escogido a la hora de desarrollar el prototipo, se hablará en la siguiente sección. Para información directa, consultar http://java.sun.com/products/javacard/.

- **MultOS:** Sistema Operativo Abierto de Tarjeta Inteligente desarrollado por Maosco Ltd., una empresa inglesa asociada al sistema bancario Mondex. A diferencia de la solución JavaCard, este Sistema Operativo tiene un altísimo nivel de seguridad y de rigurosidad, debido a su vinculación bancaria. Esta misma razón es la que hace bastante difícil la obtención de especificaciones y muestras de tarjetas, lo cual ocurre para incrementar el grado de seguridad. Las rutinas se realizan en un lenguaje propietario, denominado MEL, aunque se proporciona un conversor de lenguaje C a lenguaje MEL. Tecnológicamente se considera muy superior a las tarjetas JavaCard y hubiese sido la plataforma elegida para la realización de esta Tesis; sin embargo, la

falta de tarjetas ha imposibilitado tomar esta decisión. Para más información, consultar http://www.multos.com/.

- **WinCard:** La mención de este tipo de tarjetas es necesaria por la gran publicidad que se le está dando, aunque es necesario decir que a fecha de hoy no existen ni especificaciones cerradas, ni tarjetas en el mercado (ni siquiera en fase beta). La importancia viene dada por que es una solución lanzada por Microsoft Corp., supuestamente como respuesta tecnológica frente a uno de sus grandes competidores Sun Microsystems. De las pocas cosas que se conocen de esta solución, hay que comentar que la idea es que sean programables en Visual Basic. Para más información, http://www.microsoft.com/windowsce/smartcard/.

Teniendo en cuenta todo lo comentado sobre las tres tecnologías, el prototipo se ha desarrollado utilizando tres tarjetas JavaCard de dos fabricantes distintos. Por eso, este apartado se va a dividir en dos secciones: una primera en la que se comentarán los aspectos más relevantes de las tarjetas JavaCard, y una segunda en el que se expondrán los resultados obtenidos.

VI.4.1. TARJETAS JAVACARD

Como ya se ha comentado, las tarjetas JavaCard son tarjetas que poseen un Sistema Operativo Abierto, de forma que se puedan programar rutinas y comandos mediante lenguaje Java, para satisfacer las necesidades particulares de un cliente sin tener que desarrollar una nueva máscara de tarjetas. Las especificaciones de este tipo de tarjetas se encuentran en su versión 2.1 ([Sun99]), que aunque parece bastante más completa que la anterior ([Sun97]), apunta a una nueva revisión para solucionar problemas como, por ejemplo, los relativos a compatibilidad entre fabricantes.

Cualquier fabricante de tarjetas puede crear una tarjeta JavaCard, siempre que pague los correspondientes derechos y siga las especificaciones existentes. Dicha tarjeta tendrá una máquina virtual Java que traducirá las instrucciones del *Cardlet* (versión de *Applet* para tarjetas), a comandos del procesador que contiene la tarjeta. El *Cardlet* se comunicará con el exterior en base a pares comando/respuesta con la misma estructura que la marcada en la norma ISO 7816 ([IS7816]).

Sin embargo, debido a que no se trata de ejecutar una aplicación en un ordenador, sino que hay que ejecutarla en un micro-controlador de reducida potencia de cálculo y procesamiento, el

lenguaje Java en el que se escriben los *Cardlets* es, en realidad, un sublenguaje en el que se han eliminado elementos basándose en un doble propósito: limitar el uso de la memoria y evitar al procesador cálculos excesivos. En referencia al prototipo a ser desarrollado, estas limitaciones afectaron fundamentalmente a la posibilidad de hacer algunos algoritmos de verificación, debido a que en las JavaCard están eliminados todo tipo de cálculo de punto fijo y de coma flotante, y aquellos tipos de datos asociados (en realidad, en una JavaCard sólo existen cuatro tipos de datos primitivos: *boolean*, *byte*, *short* y, en algunos ocasiones ya que no es obligatorio, *int*).

El autor de esta Tesis es plenamente consciente que la información dada aquí sobre este tipo de tarjetas es excesivamente limitada, por lo que se sugiere al lector interesado en conocer esta tecnología, la consulta de la documentación de Sun Microsystems, que se puede encontrar libremente en la página anteriormente mencionada.

VI.4.2. RESULTADOS OBTENIDOS

De todas las tarjetas JavaCard a las que se ha tenido acceso, se escogieron 3 de ellas para desarrollar el prototipo basandose en el grado de compatibilidad con las especificaciones existentes. Estas tres tarjetas fueron:

- **GemXpresso 2.0:** Tarjeta JavaCard de la empresa multinacional francesa Gemplus. Es 100% compatible con la versión 2.0 de las especificaciones JavaCard, añadiendo funcionalidades muy interesantes en su sistema de desarrollo. La tarjeta se aprovechó de los pocos resultados positivos que arrojó el proyecto CASCADE (mencionado en el primer apartado de este capítulo), en concreto de la integración de un micro-controlador RISC de 32 bits. Esto permite que esta tarjeta sea la única que contempla dentro de su sublenguaje, la utilización del tipo *int* (entero de 32 bits). [Gem98b].

- **GemXpresso 2.11:** Evolución de la anteriormente mencionada para seguir las especificaciones JavaCard 2.1, añadiendo comandos de interoperabilidad entre diversos fabricantes, los cuales no se encuentran todavía recogidos en las especificaciones de Sun. Debido al coste del chip integrado en la anterior tarjeta, se ha vuelto al uso de un chip de 16 bits, no siendo posible el uso del tipo *int*. A la hora de finalización del prototipo, esta tarjeta se encontraba en fase beta totalmente operativa para las necesidades de esta Tesis. [Gem99b].

- **Sm@rtCafe:** Tarjeta JavaCard de la multinacional alemana G+D. Esta tarjeta es compatible 100% con las especificaciones 2.0, añadiendo funcionalidades de las especificaciones 2.1 debido a su momento de salida al mercado. También se encuentra basada en un chip de 16 bits. [GyD99].

Fig. VI.2: Tarjetas JavaCard utilizadas

Se desarrolló la Nueva Arquitectura de Autenticación tal y como se ha detallado en el apartado anterior, teniendo en cuenta las siguientes restricciones:

- Al no poseer operaciones en coma flotante, el desarrollo del algoritmo basado en GMMs se ha tenido que dejar fuera del marco de esta Tesis. Se espera que en el futuro, ya sean en forma de linea abierta para el desarrollo de un algoritmo de GMM que se pueda integrar en una JavaCard, o en forma de evolución tecnológica, se pueda incorporar este algoritmo de verificación que tan buenos resultados ha arrojado.

- Al no poseer la función de raíz cuadrada, se ha aproximado la distancia Euclidea eliminando el uso de dicha función, aprovechando el carácter monótona creciente que posee. Los resultados obtenidos han sido análogos a los obtenidos en los temas anteriores, habiendo tenido únicamente que cambiar el valor de los umbrales.

- Debido a la longitud de los datos que se han de transmitir en el caso de verificación por voz (no sólo en reclutamiento, sino también en verificación), la viabilidad de la inclusión de esta técnica de autenticación biométrica dentro de una Tarjeta Inteligente es muy baja, si no nula. Como línea futura, tal y como se comentó en el tema correspondiente, se deja el estudio de nuevos métodos de autenticación basándose en la voz de forma que sean más estables, con menor carga computacional y/o con menor longitud de los datos a utilizar.

Con todo esto, se probó el funcionamiento de la Autenticación Biométrica Mediante

Tarjeta Inteligente para el resto de los casos (mano con Distancia Euclídea, y mano e iris con Distancia de Hamming), obteniendo tasas de error idénticas a las vistas en los capítulos correspondientes. En cuanto al tiempo de ejecución del algoritmo de verificación, se han conseguido tiempos despreciables (comparados con los dedicados a la transmisión de comando y respuesta), lo cual es lógico teniendo en cuenta el bajo costo computacional de los algoritmos utilizados.

Dadas las tasas de falso rechazo existentes en mano, se recomienda que el número de intentos antes del bloqueo de la clave sea superior o igual a 5, mientras que en iris un valor igual a 3 arroja unos resultados más que aceptables.

VI.5. CONCLUSIONES

En este capítulo se ha expuesto todo el trabajo realizado para llevar a cabo la Autenticación Biométrica dentro de una Tarjeta Inteligente, lo cual suponía el objetivo final de la Tesis. Se ha comentado la panorámica actual, haciendo mención al único proyecto conocido que se encuentra en línea con esta Tesis. Posteriormente se han detallado las condiciones de contorno a la inclusión de la Biometría dentro de la Tarjeta Inteligente y las especificaciones para la creación del Nuevo Sistema de Autenticación en base a Biometría. Por último se ha expuesto las decisiones tomadas para el desarrollo del prototipo y se han comentado los resultados obtenidos.

Sobre los resultados es preciso intentar sacar al menos un par de conclusiones. La primera, la positiva, es que se ha demostrado que es posible llevar a cabo los objetivos propuestos inicialmente, aunque por problemas principalmente económicos no se han podido demostrar algunas de las técnicas de verificación.

La segunda conclusión, que no es que se deba tomar como negativa, pero sí como una llamada de atención, es sobre la parcialidad de los resultados obtenidos. Hay que tener en cuenta que los resultados obtenidos han sido basados en un número pequeño de sujetos que han participado en las distintas bases de datos, los cuales, aunque no todos estaban familiarizados con la tecnología, no veían ningún riesgo en los experimentos. Habría que realizar un proyecto piloto, relativamente ambicioso en el cual se tratase con personas sin ninguna relación con la tecnología, utilizando ésta en unas situaciones que les pueda resultar importantes. Por ejemplo, si se

estableciese un proyecto piloto en el cual una entidad financiera protegiera la utilización de las tarjetas de crédito mediante el sistema propuesto, habría que examinar el verdadero porcentaje de rechazo que se produciría y, por tanto, el número de bloqueos de la tarjeta. Tampoco habría que dejar olvidado el estudio de la aceptación de la nueva tecnología por parte de los usuarios, así como la evolución temporal del sistema (lo cual es de vital importancia, siendo un tema que muy pocas veces se ha estudiado). Esta conclusión, como se verá en el último capítulo de esta Tesis, es común a todo sistema nuevo que se intenta desarrollar y muy especialmente aquellos que tienen que ver con la Biometría.

CAPÍTULO VII:

CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO

Tras todo el trabajo expuesto en los capítulos anteriores, es hora de realizar un último capítulo en el que se recojan todas las conclusiones obtenidas, algunas de las cuales ya se han mencionado en cada capítulo correspondiente, mientras que otras, por ser de tipo general, no se han reflejado todavía.

Por otro lado, todo trabajo de investigación, aunque intente ser lo más completo posible, siempre deja flecos que deberán ser tratados como futuras líneas de investigación. De hecho, en la mayoría de las ocasiones ocurre que, cuanto más se intenta profundizar en un tema, más líneas nuevas surgen. Como no podía ser de otra forma, en el desarrollo de esta Tesis han ido surgiendo multitud de lineas abiertas a la investigación o, por lo menos, al desarrollo. Por tanto, como segundo apartado de este capítulo se resumirán las principales futuras líneas, de forma que pueda servir de referencia para presentes y futuros investigadores.

VII.1. CONCLUSIONES OBTENIDAS

En esta Tesis se han obtenido los mecanismos necesarios para poder realizar una Autenticación Biométrica dentro de una Tarjeta Inteligente. Para llegar a dicho resultado, se han analizado distintas técnicas biométricas, desarrollando una serie de prototipos que sirvieran para obtener conclusiones que condujeran a la definición de dichos mecanismos. Al analizar técnicas biométricas muy dispares, se ha logrado que los resultados fueran compatibles con más de una técnica biométrica, promoviendo la generalidad del nuevo Sistema de Autenticación de Usuarios.

Desgraciadamente, problemas principalmente de tipo económico, no han permitido que se pudiese llegar al desarrollo de alguno de los prototipos finales: en concreto, la autenticación utilizando GMMs. Y, aunque los resultados son muy prometedores, tampoco se ha podido demostrar la viabilidad del nuevo sistema mediante un proyecto piloto que analizara el rendimiento del sistema y la verdadera aceptación por parte de los usuarios. Sin lugar a dudas en esta imposibilidad radica la principal limitación de los trabajos de esta Tesis: todos los resultados, tanto a nivel de Tarjetas, como a nivel de Biometría, se han obtenido mediante Bases de Datos muy reducidas. Por consiguiente, es preciso realizar futuros trabajos para incrementar dichas Bases de Datos, obteniendo resultados reales que avalen los logros de esta Tesis.

Particularizando para cada una de las técnicas biométricas, se pueden establecer diversas conclusiones. Respecto a ***Reconocimiento de Locutores***, cabe decir que se ha desarrollado un prototipo basado en reconocimiento a través de GMMs, dejando de lado otros métodos utilizados tradicionalmente en esta técnica biométrica, por limitaciones de memoria y capacidad de cálculo de las Tarjetas Inteligentes. Uno de los principales objetivos que se han buscado, ha sido la aplicabilidad de la técnica a entornos reales, olvidando estudios de grabación u otras situaciones ideales. De las conclusiones obtenidas, una ha sido el limitado número de casos donde se puede utilizar esta técnica con una aceptación buena de los usuarios. Estos casos son aquellos en los que los usuarios tienen que hablar de forma natural, sin sentirse cohibidos por el hecho de tener que utilizar un sistema de identificación. Por tanto, se recomienda que esta técnica se utilice, principalmente, para aplicaciones telefónicas, como puede ser la de Banca Telefónica. Sin embargo, en lo relativo a la creación de la Base de Datos, se han tenido que buscar una situación de compromiso para lograr locuciones no forzadas, sin tropezar en problemas éticos derivados de la grabación de conversaciones privadas.

Entrando a los resultados plenamente numéricos, el rendimiento obtenido con el prototipo

de Reconocimiento de Locutores se puede considerar como excesivamente bajo, ya que las tasas de error obtenidas superaban con mucho el 10% (la Tasa de Error Igual *EER*, en el mejor caso, ha sido superior al 20%). Es por tanto necesaria la continuación del trabajo que se está realizando por parte de numerosos equipos de investigación (a nivel mundial), para mejorar los resultados. Sin embargo, incluso con tasas de error mucho más bajas, la integración de esta técnica biométrica dentro de las tarjetas, se ha demostrado difícil, debido a la longitud de los vectores de características de las muestras a verificar.

Posteriormente al trabajo realizado en Reconocimiento de Locutores, se ha trabajado en técnicas biométricas basadas en imagen. En concreto en dos técnicas: la primera realizando análisis morfológico del contorno de la mano, mientras que en la segunda, se ha realizado estudio multi-resolución del iris ocular.

La ***Geometría del Contorno de la Mano*** ha sido una de las mayores contribuciones de esta Tesis. Habiendo iniciado el desarrollo desde cero, se ha desarrollado un sistema de identificación biométrica. Se creó una plataforma para capturar la foto de la mano, se pre-procesó dicha foto, se extrajeron un gran número de características morfológicas de la geometría obtenida, se analizó la discriminalidad de dichas características y se evaluó el rendimiento basándose en 3 métodos de reconocimiento de patrones diferentes: Distancia Euclídea, Distancia de Hamming con valores no binarios y GMMs. El resultado final ha sido un sistema de identificación biométrica muy sencillo, de gran aceptación por parte de los usuarios y que, además, ha obtenido unos rendimientos muy positivos, especialmente con GMMs (*EER* algo superior al 5%). Sin embargo la falta de una Base de Datos suficientemente grande, deja sin resolver la incógnita sobre la viabilidad de esta técnica biométrica en su aplicación a entornos con un gran número de personas.

Por último, se ha trabajado con el ***Patrón del Iris Ocular***. El trabajo se inició siguiendo los artículos de J. G. Daugman, referidos en el capítulo correspondiente, explorando aquí nuevas posibilidades. El resultado ha sido un sistema con un alto rendimiento, llegando incluso a obtener una Tasa nula de Falsa Aceptación (FAR=0), con una Tasa de Falso Rechazo (FRR) del 3,51%. El algoritmo utilizado para la verificación ha estado basado en la Distancia de Hamming, con lo que su tiempo de computación es muy bajo. No se puede decir lo mismo del algoritmo de pre-procesado de la imagen, cuestión en la que hay que seguir trabajando, ya que el coste computacional y, por tanto, el tiempo consumido, es excesivamente elevado. Los usuarios presentaron una gran aceptación al sistema, sólo entorpecida por los temas relativos a iluminación del ojo para la extracción de la foto

Como resumen, y completando lo mencionado al principio del presente apartado, en esta Tesis se han creado cinco prototipos de sistemas de autenticación biométrica, de los cuales los tres basados en el contorno de la mano son de realización totalmente nueva. Salvo el prototipo

basado en voz, todos los demás han sido susceptibles de ser incorporados dentro de una Tarjeta Inteligente. Se ha creado un modelo de Autenticación Biométrica mediante Tarjeta Inteligente, desarrollándose varios prototipos utilizando tarjetas JavaCard, los cuales han avalado el modelo diseñado. Es por tanto, hora de continuar los trabajos aquí reflejados, siguiendo las líneas abiertas que se detallan en el siguiente apartado.

VII.2. LÍNEAS ABIERTAS A LA INVESTIGACIÓN

Sin lugar a dudas, los dos puntos principales en los que habría que trabajar para completar esta Tesis, tal y como se ha mencionado anteriormente, son:

- Incrementar el tamaño de todas las Bases de Datos utilizadas, tomando muestras de personas escogidas al azar, de forma que se comprueben los resultados obtenidos con cada uno de los prototipos de sistemas de identificación biométrica desarrollados.
- Plantear un proyecto piloto en el que se pruebe en un entorno real la Tarjeta Inteligente con Autenticación Biométrica de su titular.

Pero centrándose en los trabajos más puramente relacionados con la Investigación, habrá que tener en cuenta los siguientes puntos, los cuales se han ordenado por técnicas biométricas empleada:

- *Reconocimiento de Locutores:*
  - Estudiar nuevos coeficientes que modelen mejor las características de la voz que son propias de la persona, intentando eliminar factores como la edad, las enfermedades, el estado de ánimo, el ruido, etc.
  - Reducir el tamaño de las muestras a verificar, de forma que se obtengan mejores tasas de error con un coste computacional y de memoria inferior.

- *Geometría del Contorno de la Mano:*
  - Estudiar con detalle la unicidad de las características extraídas del contorno de la mano.
  - Expandir los trabajos realizados, incorporando información sobre las líneas características de la palma de la mano.
  - Extrapolar el trabajo aquí expuesto a otras técnicas biométricas, o a otras partes del cuerpo todavía no consideradas como elementos identificativos de

la persona.
- Analizar nuevos sistemas de captura más baratos y con mejores prestaciones.

- *Patrón del Iris Ocular:*
  - Utilizar para la captura cámara de vídeo, de forma que se habiliten mecanismos de detección de *"ojo vivo"*.
  - Sustituir la iluminación utilizada por iluminación infrarroja, de forma que se elimine el leve rechazo que posee ahora el sistema.
  - Analizar nuevas técnicas de extracción de características. En concreto, intentar mejorar el rendimiento conseguido con filtrado de Gabor. O intentar aplicar transformada ondicular (*wavelets*), analizando sus coeficientes o los cruces por cero de dichos coeficientes.

- *Integración en Tarjetas Inteligentes:*
  - Desarrollar, con las restricciones planteadas en Tarjetas Inteligentes, algoritmos de verificación con procesado en coma flotante, como es el caso de los GMMs.

El autor de esta Tesis espera que, en un futuro, haya investigadores que se motiven por alguna de las líneas aquí expuestas, de forma que se puede mejorar el Estado del Arte de la ***Autenticación Biométrica mediante Tarjeta Inteligente.***

APÉNDICE A:

INTRODUCCIÓN A LA TECNOLOGÍA DE LAS TARJETAS INTELIGENTES

Para aquellos lectores no familiarizados con la tecnología de las Tarjetas Inteligentes, se ha considerado necesario la introducción de un apéndice que aclare diversos conceptos sobre dicha tecnología, de forma que sirva de ayuda al seguimiento del texto de la presente Tesis. Se abre, por tanto, este apéndice como continuación a los conceptos ya mostrados en el Capítulo I (sección I.2.1). Se es consciente que la introducción que aquí se va a dar, va a ser precisamente una introducción, quedando como decisión para el lector, el profundizar en esta tecnología, en base a las referencias bibliográficas comentadas en los diversos capítulos, recomendando inicialmente [Bri88], [Zor94] y [San99a].

Teniendo en cuenta que en el Capítulo I se ha visto un poco de la historia de las Tarjetas de Identificación, de la Arquitectura Funcional y del Sistema Operativo de Tarjeta Inteligente (SOTI), este apéndice va a hacer hincapié principalmente en tres aspectos: la estructura de datos, el protocolo de comunicación y los mecanismos de seguridad. A cada uno de estos aspectos se le va a dedicar un apartado.

A.1. ESTRUCTURA DE DATOS

La Estructura de los Datos dentro de una Tarjeta Inteligente (TI), se asemeja a la organización jerárquica que tiene el sistema de ficheros de un ordenador personal, existiendo un directorio raíz y unos archivos, los cuales se pueden organizar en directorios. Un esquema de ejemplo se puede ver en la figura A.1.

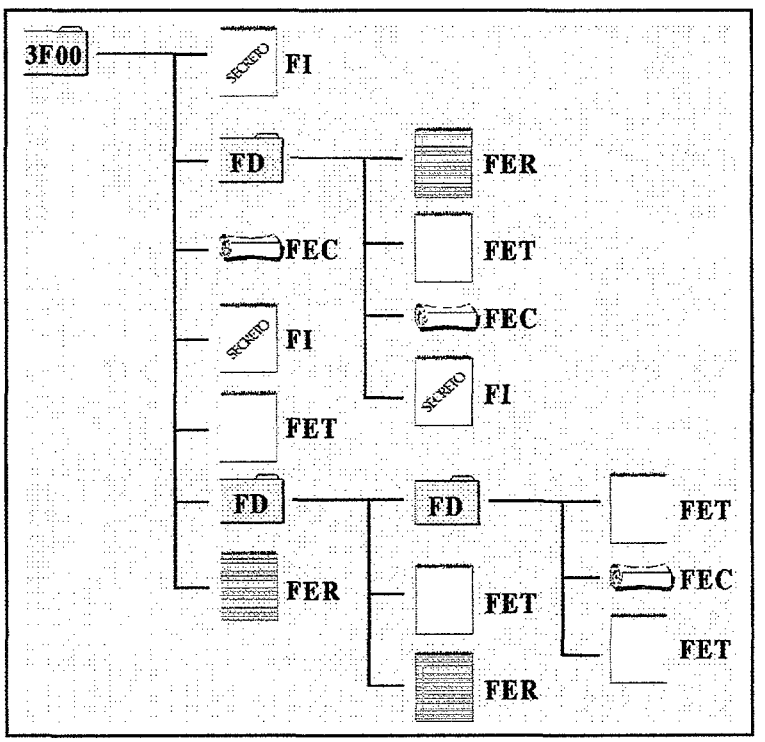


Fig. A.1: Ejemplo de estructura jerárquica en una TI.

En dicha figura se pueden observar los distintos tipos de ficheros que se pueden encontrar en una TI, los cuales se clasifican de la siguiente manera:

- **Ficheros Dedicados (FD):** Son lo que se puede denominar directorios. En su interior no contienen información propiamente dicha, sino otros archivos, e incluso otros directorios (esto último depende del SOTI de la tarjeta particular).

- **Ficheros Elementales (FE):** Son los ficheros propiamente dichos, es decir, los que

contiene información. Estos ficheros pueden ser de dos tipos:

- **Ficheros Elementales Internos (FI):** Contienen información que va a utilizar directamente el SOTI. Ejemplo de este tipo de ficheros son los ficheros de claves, los contadores de transacciones, el fichero de respuesta al *reset*, etc.
- **Ficheros Elementales de Trabajo (FEW):** Estos ficheros contienen la información de la aplicación, como datos del usuario, perfil bancario, datos sanitarios, etc. (dependiendo de la aplicación que se le vaya a dar a la tarjeta). Este tipo de fichero, atendiendo a su estructura interna, se clasifican en:
  a. **Ficheros Elementales Transparentes (FET):** No tienen estructura interna, es decir, almacenan los bytes según le indica la instrucción.
  b. **Ficheros Elementales de Registros (FER):** Estos ficheros almacenan la información estructurada en registros, los cuales pueden ser de longitud fija (igual para todos) o de longitud variable (distinta para cada registro).
  c. **Ficheros Elementales Cíclicos (FEC):** Son ficheros de registros, pero en los que éstos se encuentran ordenados de una manera cíclica. Es decir, no existe primer ni último registro, sino que existe el registro actualmente seleccionado y el resto en relación a él.

Por tanto, dependiendo del tipo de fichero, así como de la capacidad que se le asigne a cada uno de ellos, se puede almacenar un tipo de información u otro. Esa decisión depende del que defina la *aplicación*[23] de la tarjeta.

A.2. PROTOCOLO DE COMUNICACIÓN

La comunicación entre un terminal de TIs y la TI se realiza por medio de una comunicación serie a través del contacto I/O de ésta. Esta comunicación puede ser de varios tipos, estando contemplados en la parte 3 de la norma ISO7816 ([IS7816]), dos de ellos, conocidos como ***T=0*** y como ***T=1***. Los dos son protocolos serie semi-dúplex, donde la principal diferencia radica en que el *T=0* está orientado a carácter, mientras que el otro está orientado a bloques de

[23] El concepto de *aplicación* en Tarjetas Inteligentes no indica un programa que se vaya a ejecutar, sino la distribución de ficheros y directorios a definir dentro de la TI, en proceso de personalización, para satisfacer las necesidades del sistema donde va a ser aplicada esa TI.

caracteres. Por simplicidad, así como por ser el mayoritariamente utilizado por las tarjetas del mercado, se va a comentar brevemente el primer protocolo.

Antes de establecer el protocolo de comunicación y, por tanto, intercambiar instrucciones con la TI, ésta ha de ser inicializada mediante un pulso en el contacto *RESET* que posee. A dicha inicialización (también conocida directamente como *reset*), la tarjeta contesta con un ***ATR***[24], en el cual le transmite al terminal su identificación y sus parámetros de comunicación (así como los protocolos que soporta). Una vez finalizada la recepción del ATR, se comienza con el protocolo de comunicación el cual consta de un intercambio de instrucciones. Atendiendo al protocolo *T=0*, este intercambio siempre es iniciado por el terminal, el cual es el único que puede enviar instrucciones, limitándose la TI a dar respuestas. En la figura A.2, se pueden observar los tres casos distintos que soporta este protocolo.

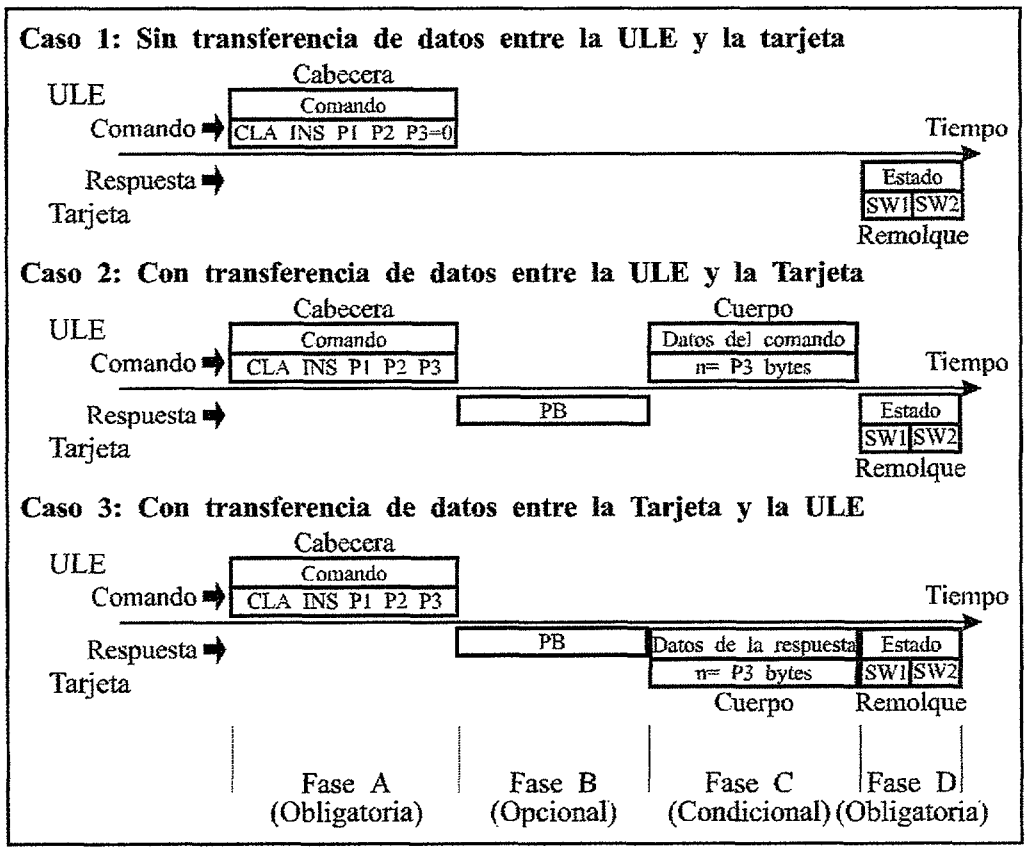


Fig. A.2: Posibles casos de transmisión en el protocolo *T=0*.

[24] Acrónimo anglosajón procedente de la frase *Answer To Reset*, o Respuesta al Reset. Se ha decidido utilizar la versión inglesa por homogeneidad con el argot del sector, ya que el acrónimo castellano (RAR), resulta totalmente desconocido.

Como se puede observar, el protocolo está compuesto por un *Comando* y una *Respuesta*. Por su parte, el *Comando* está compuesto de una *cabecera* (que es obligatoria siempre) y un *cuerpo* (que sólo se enviará cuando se quieran mandar datos a la TI), mientras que la *Respuesta* está formada por un *cuerpo* (que sólo envía la tarjeta cuando tiene que devolverle datos al terminal) y un *remolque* (obligatorio siempre y que devuelve el estado en el que se encuentra la TI). En control del flujo está gobernado por un *byte de procedimiento* (PB) que transmite la tarjeta tras haber recibido la *cabecera* del *Comando*.

Como se puede observar, no se contempla el caso en el que se tengan que enviar y recibir datos en una única instrucción. Por tanto, si es necesario este tipo de operaciones, hay que habilitar en la tarjeta una instrucción que entregue la respuesta cuando se la pida el terminal (instrucción normalmente conocida como *GetResponse*).

Es importante prestar especial atención a la estructura de la *cabecera* del *Comando*, así como a la del *remolque*. La *cabecera* está formada siempre por 5 bytes que representan (por orden de envío):

- Clase de Instrucción (CLA).
- Código de Instrucción (INS).
- Parámetro 1 de la instrucción (P1).
- Parámetro 2 de la instrucción (P2).
- Longitud de los datos a intercambiar entre la Unidad de Lectura/Escritura (ULE) y la tarjeta (P3, o también conocido como LEN).

Por su parte, el *remolque* está formado por dos bytes, y se suele denominar normalmente **palabra de estado**, representándose por **SW**, acrónimo de *Status Word*. Al ser 2 bytes, éstos se suelen representar, por orden de recepción, con SW1 y SW2. La codificación de SW se encuentra normalizada en gran parte de sus valores, mediante la parte 4 de la norma ISO7816.

A.3. MECANISMOS DE SEGURIDAD

Los mecanismos de seguridad que incorporan las TI son muy diversos y dependen del SOTI definido en cada TI en particular. Los mecanismos van desde los de protección física (evitar la revelación de información grabada dentro de la tarjeta mediante el ataque físico a la tarjeta), a los basados en asegurar la comunicación entre la tarjeta y el terminal, pasando por el control de

acceso a la información de la tarjeta basándose en la presentación de claves.

Para el interés de esta Tesis, la protección física no resulta de especial interés, siendo mucho más importantes los otros dos tipos de mecanismos mencionados. En el capítulo titulado *Autenticación Biométrica mediante Tarjetas Inteligentes*, se ha hecho una introducción al control de acceso a la información mediante claves. Por tanto, en este apéndice se va a hablar de los mecanismos orientados a asegurar la comunicación de la información entre la ULE y la tarjeta.

Asegurar una comunicación contempla comprobar la integridad de los datos transmitidos y/o cifrar dichos datos para garantizar la confidencialidad de los mismos. Para comprobar la integridad de los datos se utilizan técnicas de **firma**, mientras que para tratar la confidencialidad se utilizan técnicas de **cifrado**. Debido a que la gran mayoría de las tarjetas del mercado utilizan criptografía de clave simétrica (también conocidos como de clave secreta) y, en particular, suelen utilizar el algoritmo DES, se va a basar la explicación en este tipo de técnica criptográfica.

Dentro del sector de las TI, al mecanismo encargado de facilitar estos servicios se le denomina ***Secure Messaging***[25] (que traducido al castellano significa Mensajería Securizada, referenciado normalmente por su acrónimo inglés *SM*). Este mecanismo se basa en una clave (almacenada o calculada) en la tarjeta, la cual se utiliza como clave de cifrado. Antes de entrar en detalle en los servicios que proporciona, es preciso hacer una advertencia al lector: existen multitud de formas de realizar el *SM* y, por desgracia, cada SOTI desarrolla una variante diferente. Aquí se va a comentar una de esas variantes para que sirva de ejemplo ilustrativo.

Si lo que se quiere es únicamente garantizar la integridad de los datos, es decir, que no han sufrido ninguna manipulación y que el que los envía tiene permiso para hacerlo, lo que se realiza es una función *f*, por la que pasan los datos a transmitir, incluyendo la cabecera del comando, de tal forma que el resultado sea un determinado número de bytes (por ejemplo, 3), que correspondan unívocamente con los datos a enviar. Una vez calculados esos bytes, para lo cual se ha utilizado la clave correspondiente, se añaden a los datos a transmitir, incrementando el parámetro P3 en ese número de bytes, para posteriormente transmitir todo el comando nuevo.

CLA	INS	P1	P2	P3	DATOS	
CLA	INS	P1	P2	L+3	*datos* (en claro) (L bytes)	f(cabecera,*datos*) (3bytes)

Si por el contrario, lo que se quiere hacer es únicamente garantizar la confidencialidad de

[25] Se utiliza el nombre en inglés por homogeneidad con el argot del sector.

los datos a transmitir (o a recibir), estos datos se transmitirán cifrados por la clave correspondiente, transmitiéndose la instrucción de forma idéntica a si los datos viajasen en claro.

Si lo que se quiere es hacer las dos cosas al mismo tiempo, lo único que hay que hacer es juntar los dos procedimientos anteriormente mencionados. Aquí es donde surgen el mayor número de disparidades de criterio entre SOTIs: los hay que firman antes de cifrar, mientras que otros lo hacen después; los hay que en este caso incluyen la cabecera del comando, mientras que otros sólo toman los datos; etc. El resultado final, sería la transmisión de una instrucción del siguiente tipo (tomando la cabecera y firmando con los datos en claro):

CLA	INS	P1	P2	P3	DATOS	
CLA	INS	P1	P2	L+3	*datos* (cifrados) (L bytes)	*f*(cabecera,*datos*) (3bytes)

El último tema que falta por tratar en cuanto al *SM*, es la procedencia de la clave. Ésta puede ser una previamente almacenada en la tarjeta, la cual está encargada de proteger el acceso al fichero que se intenta escribir o leer. Sin embargo, si se utiliza dicha clave tal cual, se facilitaría un ataque a la tarjeta mediante inspección de varios mensajes transmitidos, de forma que se podría llegar a obtener la clave secreta en la tarjeta (aún así, esta posibilidad es bastante remota). Para asegurar la confidencialidad de la clave, lo que se puede hacer es calcular en cada sesión (es decir, cada vez que se inicializa la tarjeta), una clave distinta, función de un número aleatorio y la clave real almacenada en la tarjeta. El procedimiento por el cual se obtiene esta ***Clave de Sesión***, se puede ver en la figura A.3.

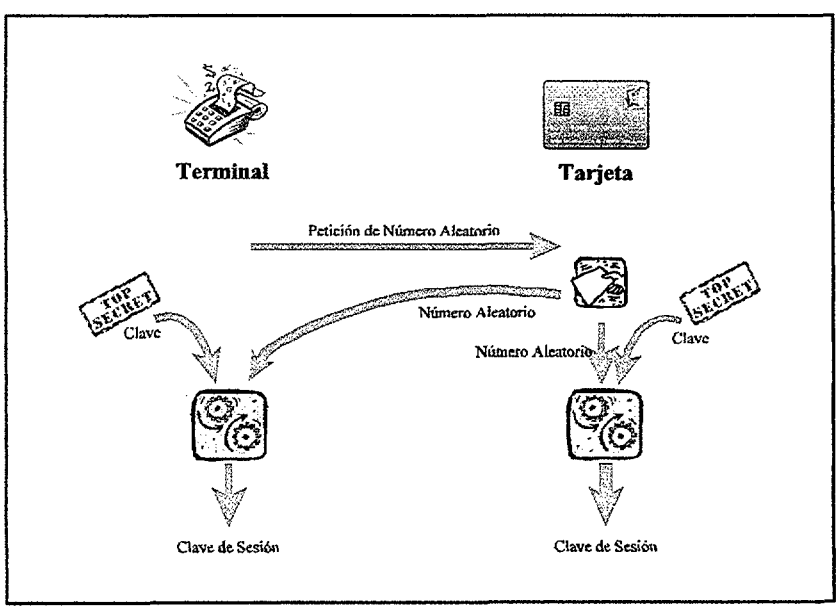


Fig. A.3: Mecanismo de cálculo de una Clave de Sesión

El procedimiento es sencillo. El terminal le pide a la tarjeta un número aleatorio, ésta se lo entrega y en ese momento, tanto el terminal, como la tarjeta, basándose en la clave secreta que ambos conocen y al algoritmo escogido para obtener la *Clave de Sesión*, calculan ésta, la cual será utilizada para aquellas funciones de seguridad que sean necesarias.

Como ya se ha comentado, basándose en los conceptos vertidos en este apéndice, existen multitud de realizaciones prácticas, cada una de las cuales debe ser estudiada particularmente. El autor espera que, con estos conceptos, el lector pueda haber obtenido el conocimiento necesario para hacer frente a los temas relativos a TI de esta Tesis.

BIBLIOGRAFÍA

[Bri88] R. Bright
Smart Cards: Principles, Practice, Applications
John Wiley & Sons, Inc. Chinchester (Inglaterra), 1988.

[Cam97] J. P. Campbell, Jr.
"Speaker Recognition: A Tutorial"
Proceedings of the IEEE, vol. 85, nº 9, pp. 1437-1462, Sep. 1997.

[CEC96] Confederación Española de Cajas de Ahorros (CECA)
Detailed Functional Specification of "Euro6000" Card
Versión 2.0. Diciembre 1996.

[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. EE.UU. 1973

[Esc77] L. F. Escudero
Reconocimiento de Patrones
Paraninfo. Madrid. 1977

[Fur81] S. Furui
"Cepstral Analysis Technique for Automatic Speaker Verification"
IEEE Trans. on ASSP, vol. 29, nº 2, pp. 254-272, Abr. 1981

[Fur91] S. Furui
"Speaker-dependent-feature extraction, recognition and processing techniques"
Speech Communication, vol. 10, pp. 505-520, 1991

[Gem98a] Gemplus
MPCOS-EMV - Reference Manual
Versión 1.5. Octubre 1998.

[Gem98b] Gemplus
GemXpresso Tutorial
Versión 1.0. 1998.

[Gem99a] Gemplus
GPK - Reference Manual
Versión 2.2. Octubre 1999.

[Gem99b] Gemplus
GemXpresso RAD 211 - Reference Manual
Versión 1.0. Octubre 1999.

[Gra77] H. Gray
Anatomy, descriptive and surgical
Gramercy Books, Nueva York (EE.UU.), 1977.

[Gis94] H. Gish, M. Schmidt
"Text-Independent Speaker Identification"
IEEE Signal Processing Magazine, vol. 11, pp. 18-32, Oct. 1994.

[GyD98] Giesecke und Devrient (G+D)
STARCOS S 2.1 - Reference Manual
Munich (Alemania). Septiembre 1998.

[GyD99] Giesecke und Devrient (G+D)
Sm@rtCafe 1.1 Card - Reference Manual
Munich (Alemania). Mayo 1999.

[Han81] D. J. Hand
Discrimination and Classification
John Wiley & Sons. EE.UU. 1981

[Hay94] S. Haykin
Neural Networks: A Comprehensive Foundation
Prentice Hall. New Jersey (EE.UU.) 1994.

[Hig86] A. L. Higgins, R. E. Wohlford
"A new method of text-independent speaker recognition"
Proc. IEEE International Conference ASSP, vol. 2, pp. 869-872, 1986.

[Hus93] D. R. Hush, B. G. Horne
"Progress in Supervised Neural Networks. What's New Since Lippmann?"
IEEE Signal Processing Magazine, January 1993, pp. 8-39.

[IS7816] Normativa internacional ISO/IEC 7816
Identification Cards - Integrated circuit(s) cards with contacts
Partes 1-10. Desde 1987 hasta 1999.

[Jäh97] B. Jähne
Digital Image Processing
Springer-Verlag. 1997.

[Jai89] A. K. Jain
Fundamentals of Digital Image Processing
Prentice Hall, 1989.

[Jai97a] 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, pp. 302-313.

[Jai97b] 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, pp. 1365-1388.

[Jai99a] A. K. Jain, R. Bolle, S. Pankanti, et al.
Biometrics: Personal Identificacion 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. EE.UU., 1999.

[Jua90] B. H. Juang, F. K. Soong
"Speaker recognition based on source coding approaches"
Proc. IEEE Inernational Conference ASSP, Alburquerque, S5.4, 1990.

[Kam96] N. Kambhatla
Local Models and Gaussian Mixture Models for Statistical Data Processing
Tesis Doctoral, Oregon Graduate Institute of Science & Technology, 1996.

[Kar 96] K. Karu, A.K. Jain
"Fingerprint Classification"
Pattern Recognition, vol. 29, nº 3, pp. 389-404, 1996.

[Kle96] R. Klette, P. Zamperoni
Handbook of Image Processing Operators
John Wiley and Sons, Inc. 1996.

[Lar69] *Gran Enciclopedia Larousse*
Editorial Planeta, S.A. Barcelona, 1969.

[Lee91] H. C. Lee, R. E. Gaensslen, et al.
Advances in Fingerprint Technology
Elsevier. Nueva York (EE.UU.). 1991
CRC Press LLC. EE.UU. 1994

[Lip87] R. P. Lippmann,
"An Introduction to Computing with Neural Nets"
IEEE ASSP Magazine, April 1987, pp. 4-22.

[Mat91] T. Matsui, S. Furui
"A text-independent sepaker recognition method robust against utterance variations"
Proc. IEEE International Conference ASSP, Toronto, 1991.

[McL97] G. J. McLachlan, T. Krishnan
The EM Algorithm and Extensions
John Wiley and Sons, Inc. 1997.

[Ogl90] J. Oglesby, J. S. Mason
"Optimization of neural models for speaker identification"
Proc. IEEE International Conference ASSP, Albuquerque, S5.1, 1990.

[Ogl91] J. Oglesby, J. S. Mason
"Radial Basis Function Networks for Speaker Recognition"
Proc. IEEE International Conference ASSP, S6.7, pp. 393-396, 1991.

[Omi95] Equipo Ómicron
Quiromancia
Editorial de Vecchi, Barcelona, 1995.

[Ort96] J. Ortega-García
Técnicas de Mejora de Voz Aplicadas a Sistemas de Reconocimiento de Locutores
Tesis Doctoral, E.T.S.I. Telecomunicación - U.P.M., 1996.

[Owe93] F. J. Owens,
Signal Processing of Speech
The Macmillan Pres Ltd., 1993.

[RecCOM] Recognition System Inc.
http://www.recogsys.com

[Rey95] D. A. Reynolds, R. C. Rose
"Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models"
IEEE Trans. on Speech and Audio Processing, vol. 3, num. 1, pp. 72-83, Ene. 1995.

[Roj98] M. P. Rojo Bautista
Sistema de Identificación Biométrica por Características de la Mano
Proyecto Fin de Carrera de la E.T.S.I. de Telecomunicación de la U.P.M.. Tutelado por D. Raúl Sánchez Reíllo. Madrid, 1998.

[Ros90] A. E. Rosenberg, C. H. Lee, F. K. Soong
"Sub-word unit talker verification using hidden Markov models"
Proc. IEEE International Conference ASSP, Alburquerque, S5.3, 1990.

[Ros92] A. E. Rosenberg, F. K. Soong
"Recent Research in Automatic Speaker Recognition"
Advances in Speech Signal Processing, cap. 22, pp. 701-738, Marcel Dekker, 1992.

[San99a] R. Sánchez Reíllo, et al.
La Tecnología de las Tarjetas Inteligentes
Servicio de Publicaciones de la E.T.S.I. Telecomunicación. Madrid, 1999.

[San99b] 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.

[San99c] 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

[San99d] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos
"Multiresolution Analysis and Geometric Measure for Biometric Identification"
Secure Networking - CQRE [Secure]'99. Noviembre/Diciembre, 1999.
Lecture Notes in Computer Science 1740, pp. 251-258.

[Sca89] R. J. Schalkoff
Digital Image Processing and Computer Vision
John Wiley & Sons, 1989.

[Sch96] J. Schürmann
Pattern Classification: A Unified View of Statistical and Neural Approaches
John Wiley & Sons, Inc. Nueva York (EE.UU.). 1996

[Sun97] Sun Microsystems, Inc.
Java Card 2.0 Application Programming Interfaces
Revisión Final 1.0. 1997.

[Sun99] Sun Microsystems, Inc.
Java Card™ Virtual Machine Specification
Revisión Final 1.0. Marzo, 1999.

[Sve87] T. Svendsen, F. K. Soong
"On the automatic segmentation of speech signals"
Proc. IEEE International Conference ASSP, vol. 1, pp. 77-80, 1987

[The89] C. W. Therrien
Decision, Estimation and Classification
John Wiley & Sons, Inc. Nueva York (EE.UU.). 1989

[Ulg99] F. Ulgen, N. Akamatsu, M. Fukumi
"On-line Shape Recognition with Incremental Training using a Neural Network with Binary Synaptic Weights"
Industrial Applications of Neural Networks, cap. 1, pp. 1-32.. CRC Press LCC. EE.UU. 1999.

[Wil97] R. P. Wildes
"Iris Recognition: An Emerging Biometric Technology"
Proceedings of the IEEE, vol. 85, nº 9. Septiembre 1997. pp. 1348 - 1363.

[Zor94] J. L. Zoreda, J. M. Otón
Smart Cards
Artech House. Norwood (EE.UU.), 1994.

[Zor96] J. L. Zoreda Bartolomé, et al.
Tarjeta Inteligente: Génesis, Arquitectura, Funcionalidad, Aplicaciones. (I y II)
Servicio de Publicaciones de la E.T.S.I. Telecomunicación. Madrid, 1996.