UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

DESARROLLO DE UN SISTEMA DE RECONOCIMIENTO DE HUELLA DACTILAR PARA APLICACIONES MATCH-ON-CARD

Ingeniería de telecomunicación

Gustavo Francisco Sanz

JULIO 2009

DESARROLLO DE UN SISTEMA DE RECONOCIMIENTO DE HUELLA DACTILAR PARA APLICACIONES MATCH-ON-CARD

AUTOR: Gustavo Francisco Sanz

PONENTE: Javier Ortega García

TUTOR: Manuel R. Freire Santos

Área de Tratamiento de Voz y Señales - ATVS

Dpto. de Ingeniería Informática

Escuela Politécnica Superior

Universidad Autónoma de Madrid

Julio de 2009

Resumen

En este Proyecto se estudia, implementa y evalúa un sistema de reconocimiento de huella dactilar para aplicaciones Match-on-Card. Como base de datos para la experimentación se emplea Biosecure multimodal Database, en la que el Grupo ATVS de la Universidad Autónoma participó en su adquisición.

Tras una introducción a la biometría y un estudio del estado del arte en reconocimiento de huella dactilar, se realiza una selección e implementación de los mecanismos más representativos con el fin de estudiar los resultados obtenidos y proponer mejoras.

El sistema de reconocimiento de huella dactilar propuesto se basa en minucias. Para la parte experimental se han realizado pruebas con el fin optimizar el rendimiento y simular las condiciones de trabajo de una tarjeta inteligente. Estas pruebas se han centrado en mejorar la parte de alineación y cálculo de similitud entre plantillas de huellas, realizando todas ellas para conjuntos de datos capturados con dos sensores diferentes, uno basado en tecnología térmica y otro en tecnología óptica.

Por último se evalúa el rendimiento global del sistema desarrollado analizando los resultados obtenidos por tipo de sensor. Finalmente, se presentan las conclusiones y se proponen líneas de trabajo futuras.

Palabras Clave

Biometría, procesamiento de imágenes, reconocimiento de patrones, reconocimiento de huella dactilar, minucias, Match-on-Card.

Abstract

In this M.Sc. Thesis, we study, implement and test automatic fingerprint recognition system for Match-on-Card applications. For our experiments, we use the Biosecure Multimodal Database, in which the ATVS Group from the Universidad Autónoma has participated in its acquisition.

At first, we start by describing the existing methods for fingerprint recognition. After a review of the state of the art in biometrics, and more specifically of fingerprint systems, we implement and test a selection of mechanisms, in order to study and improve the final results.

The proposed fingerprint recognition system is based on minutiae. In the experimental section, we evaluate the performance of the implemented system at different stages, in order to optimize it and simulate a smart card working conditions. We evaluate the system for two types of fingerprint images, ones captured with a thermal sensor and the others captured with an optical sensor. Subsequently, we make a comparison between them, in order to determine which one achieves better results.

After the optimization, we evaluate the overall system's performance, analyzing the global error rates and comparing them with those in the reference system. Lastly, we present the conclusions and based on them, we give some future directions to improve the implemented system.

Key words

Biometrics, image processing, pattern recognition, fingerprint recognition, minutiae, Match-on-Card.

Agradecimientos

Si hoy este Proyecto está acabado, ha sido gracias al apoyo, ayuda y buenos consejos de muchísimas personas... En primer lugar quiero agradecer a mi ponente, Javier Ortega, la oportunidad de formar parte del Grupo ATVS, por su motivación en la búsqueda de la excelencia y el apoyo recibido.

Agradezco a todo el profesorado de la Universidad Autónoma de Madrid, en especial a Guillermo González de Ribera, el esfuerzo que realizan por hacer de la misma, no sólo un lugar donde aprender, sino un punto de referencia capaz de inculcar inquietudes, motivación y capacidad para seguir formándonos a lo largo de nuestra vida.

También quería agradecer a los miembros del ATVS, tanto la ayuda recibida como ese sentimiento de Grupo que inunda los laboratorios, lugares en los que era imposible permanecer sin dibujar una sonrisa. Especialmente me gustaría agradecer a mi tutor, Manuel Freire, toda la ayuda y dedicación aportada a este Proyecto, junto con la experiencia y consejos transmitidos, a Julián, Fernando, Galbally y Pedro, por ser modelos de referencia, siempre con un hueco para solucionar problemas y a "las Babies", Virginia, Alicia y Almudena por su simpatía y apoyo.

Quiero agradecer, su ayuda, y toda la valiosa información que me ha facilitado a Juan Llorente, quien se ha preocupado e interesado por el desarrollo de este PFC.

Como muy bien decía Vero en su PFC, "no agradezco a mis compañeros de promoción, sino a mis amigos" y es la pura verdad. Vine a estudiar a Madrid y conseguisteis que me sintiera como en casa. Pablo, Chus y Kiko, en una palabra "Superpepos", no sólo presentes en los buenos momentos, siempre aportándome valores positivos y por supuesto, magníficos compañeros de prácticas, gracias a los cuales merecía la pena estar allí. A Ele, Vero, Moni, Sonso y Esther por su facilidad para hacerme reír y por saber que siempre podía contar con vosotras. A Peter, por toda la ayuda recibida y por ser uno de esos amigos con mayúsculas. Y por supuesto a Castro, Fonts, Tato... A todos ellos, por haber formado y estoy seguro, seguiréis formando parte de mi vida.

Tampoco puedo olvidarme de mis amigos del colegio, con los que comencé a aprender, desde los tres años y nunca han dejado de estar presentes.

Durante la última etapa del Proyecto, quiero agradecer a mis amigos del trabajo, especialmente a María, Joel y Roció la ayuda prestada, y en general, a todos ellos lo agradable que es ir a trabajar sabiendo que tienes al lado gente que merece la pena, que van a dejar lo que están haciendo por ayudarte y que no veras más que sonrisas en sus caras.

Quiero hacer una especial mención a María Amparo Aznar, quien confió en mí, me apoyo y defendió en los momentos de universidad más duros que he vivido.

Por último y más importante, quiero agradecer y dedicar este Proyecto a mis padres, Félix y Angelines, quienes me han dado TODO, y siempre he podido contar con ellos

para afrontar cualquier problema. Quiero agradecerles su confianza, su apoyo y sobre todo la educación y valores que me han transmitido y me han permitido afrontar y superar los retos y objetivos, que hasta la fecha, me han surgido. A mi hermana Susana gracias por la paciencia y psicología que ha tenido que emplear conmigo.

A todos, GRACIAS.

El trabajo de investigación que ha dado lugar a este Proyecto Fin de Carrera fue desarrollado en el Área de Tratamiento de Voz y Señales, Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid. El Proyecto ha sido financiado parcialmente por el Ministerio de Defensa y el Ministerio de Educación y Ciencia a través del Proyecto TEC2006-13141-C03-03.

Índice de contenidos:

Índice de Figuras:

Índice de Tablas:

1. Introducción

1.1 Motivación al Proyecto

Hoy en día la necesidad de poder identificar a cada persona de una forma rápida y fiable ha propiciado un rápido desarrollo de técnicas biométricas que permiten implementar sistemas de reconocimiento automáticos [1]. Tradicionalmente se identifica a la persona por algo que posee, como puede ser una llave o una tarjeta, pero surge el problema de que lo que se posee puede ser perdido o robado, y de esta manera, cuando el objeto pasa a manos de otra persona, ésta adquiere los privilegios del legítimo dueño. Por otro lado, se puede autentificar por algo que la persona sabe, como puede ser un PIN, una contraseña... pero ésto tiene el problema de que puede ser olvidado o ser fácilmente averiguable, ya que por ejemplo, la mayoría de las personas guardan sus claves (PIN tarjetas) en lugares tales como agendas, archivos en el ordenador, o usan contraseñas basadas en datos personales, como fechas de nacimiento y aniversarios.

La identificación basada en información de rasgos biométricos intrínsecos a lo que una persona es, cuenta con la ventaja de que el elemento de identificación no puede ser perdido, robado u olvidado. Los rasgos biométricos pueden clasificarse en dos grandes grupos: [1] rasgos anatómicos, que se encuentran presentes constantemente en el individuo, como por ejemplo las huellas dactilares, iris, geometría de la mano etc. y los rasgos de comportamiento, los cuales tienen una mayor variabilidad ya que para obtenerlos necesitamos una realización, por ejemplo decir un PIN (voz), firmar, la manera de andar, teclear etc.

Para que un sistema biométrico tenga éxito debe basarse en la medición de un rasgo biométrico que cumpla una serie de requisitos y características [1], es decir, un rasgo biométrico tiene que ser **universal**, toda persona debe poseerlo además debe tener **unicidad**, personas distintas deben poseer rasgos diferenciados. Dicho rasgo debe de ser invariable en el tiempo a corto plazo (**permanente**) y a largo plazo (**perenne**). Por último para facilitar la tarea de reconocimiento debe de ser fácilmente caracterizable cuantitativamente (**mensurabilidad**) de la forma menos molesta e invasiva posible para el usuario.

La huella dactilar es uno de los rasgos biométricos que mejor cumple estos requisitos, y por ello se ha venido utilizando en multitud de tareas de identificación. El objetivo de este Proyecto Fin de Carrera es el desarrollo de un sistema biométrico basado en huellas dactilares, que trabaje en un entorno simulado de verificación dentro de una tarjeta inteligente, Match-on-Card, (MoC) [2]. El entorno Match-on-Card tiene una gran importancia debido a que la seguridad se incrementa, ya que la propia tarjeta contiene la realización de la huella y el proceso de reconocimiento se realiza en un entorno cerrado.

Esta solución surge como respuesta a una mejora de los actuales sistemas de reconocimiento biométrico, que se basan en el uso de bases de datos centralizadas

en servidores, a las que se accede a través de redes potencialmente vulnerables a ataques informáticos. Por esta razón surge Match-on-Card, ya que esta tecnología elimina la necesidad de usar una base de datos centralizada, permitiendo guardar en su interior una realización del rasgo biométrico, aumentando así la seguridad y privacidad del sistema y facilitando las posibilidades de escalabilidad del mismo [2].

1.1.1 Historia de la huella dactilar

El reconocimiento de huella, a pesar de haber recibido un importantísimo impulso en las últimas décadas gracias al empleo de nuevas tecnologías, escáneres, procesado digital de imágenes, algoritmos de reconocimiento..., se ha venido usando desde la antigüedad. Una de las primeras muestras la encontramos en el siglo XIV, en China, donde, según textos de João de Barros [3], los mercaderes estampaban las huellas de la palma de la mano y los pies de los niños en un papel con tinta, para distinguirles unos de otros.

En 1823 Jan Purkine, médico y científico natural checo, identificó la naturaleza única de las huellas digitales de los individuos, él identificó las espirales, elipses y triángulos en las huellas digitales.

En 1858 Sir William Herschel, trabajador del servicio civil de la India, imprimió la huella de la mano al reverso del contrato de cada trabajador, para distinguir los empleados de otros que intentaran suplantar a los trabajadores el día de pago.

Henry Faulds publicó el 28 de octubre de 1880 en Nature, un artículo sobre cómo identificar criminales a partir de sus huella digitales llamado “On the Skin-Furrows of the Hand” (ver Figura 1.1 izquierda).

Figura 1.1: (Izquierda) Artículo de Henry Faulds publicado en Nature en 1880. (Centro) Portada libro “Finger Prints” publicado por Macmillan and Co. (Derecha) Primera patente que registra el uso de huellas dactilares.

Sir Francis Galton publicó en 1892 un libro llamado “Finger Prints”, ver Figura 1.1 centro, detallado estudio de huellas digitales en donde presentó un nuevo sistema de clasificación usando las huellas de los 10 dedos de las manos. El método lo llamo Galtoneano o Icnofalangometría.

En 1918 Edmond Locard escribió que si 12 puntos o detalles Galton coinciden en una comparación de dos huellas digitales, es suficiente para una identificación positiva, sin embargo, no hay un estándar mundial sobre el uso mínimo de puntos para identificación positiva, así pues algunos países tienen sus propios estándares al respecto. En concreto en España el sistema judicial ha fijado dicho umbral entre 8 y 10 minucias coincidentes, dependiendo de la probabilidad de aparición de las mismas (ver tabla A.1, en anexo puntos característicos).

La primera patente que registra el uso de huellas digitales es la No.2530758 del 21 de Noviembre de 1950 en Estados Unidos, ver Figura 1.1 derecha, y se trataba de una cámara de identificación y huellas digitales, desarrollada por William T. Cirone,

El FBI consolidó en 1975 el uso de escáneres y tecnología para la extracción de minucias, que llevó al desarrollo de un prototipo lector. Sólo se almacenaban las minucias de la huella digital y los lectores usaban técnicas capacitivas para recolectar las características de las huellas digitales.

Hoy en día, el uso de huella dactilar no sólo se restringe al ámbito policial, o de seguridad, sino que se ha extendido y forma parte de nuestra vida cotidiana hasta el punto de que la mayoría de los portátiles, PDAs, y algunas memorias USB llevan lectores y algoritmos de verificación de huella dactilar integrados. En España, el nuevo Documento de Identidad Nacional (DNI) lleva almacenada una huella dactilar del propietario (ver Figura 1.2).

Figura 1.2: (Izquierda) Documento Nacional de Identidad español, (derecha) memoria USB con lector de huellas dactilares.

1.2 Objetivos y enfoque

El presente Proyecto se centrará en el estudio de una serie de características que permitan identificar a las personas en base a la estructura de valles y crestas que componen sus huellas dactilares. Además el sistema aquí descrito tendrá en cuenta las restricciones de capacidad de cálculo y espacio de almacenamiento impuestos por la plataforma que contendrá y ejecutará el algoritmo, una tarjeta inteligente.

La característica fundamental de este Proyecto es que el propio usuario es el portador del sistema que realizará la comparación (portador de la tarjeta), por consiguiente nos aseguramos de que sea un entorno controlado, el cual posee una o varias realizaciones de su propia huella dactilar, almacenado todo ello en la tarjeta inteligente y protegido de cualquier acceso. Por otro lado puede existir el riesgo de pérdida o robo de la tarjeta, pero dicha tarjeta es del todo inútil si no se activa con la huella del legítimo dueño. De esta manera ya no es necesario conectarse con bases de datos centralizadas para obtener la huella legítima con la que comparar, y por tanto se evita el riesgo en materia de seguridad que esto entraña, permitiendo además conseguir un sistema dinámico, flexible y fácilmente escalable.

Las fases en las que se divide este sistema biométrico son cuatro: Comienza por el procesado de la imagen digital de la huella dactilar; después se eligen dos minucias de referencia en la huella almacenada en la tarjeta, en la fase de alineación se intenta encontrar dichos puntos característicos en la huella recibida a través del escáner para intentar alinear las huellas a comparar; a continuación, se determina el número de minucias coincidentes en posición y orientación entre ambas huellas y, por último, se calcula la similitud entre dichas huellas basándose en el número de minucias coincidentes.

Para la evaluación del sistema se han realizado pruebas, con la base de datos Biosecure Multimodal [4] cuya adquisición fue llevada a cabo, entre noviembre de 2006 y junio de 2007, conjuntamente por 11 instituciones europeas participantes en la Red de Excelencia Biosecure. Los resultados del trabajo que serán estudiados y discutidos en el capítulo 6, extrayendo conclusiones y planteando las posibles líneas de trabajo futuro.

1.3 Metodología y plan de trabajo

Para poder alcanzar los objetivos de este Proyecto Fin de Carrera, los cuales se acaban de definir, se ha seguido una metodología basada en cuatro pilares fundamentales:

- **Formación**: Adquirida a lo largo del periodo universitario, donde se ha aprendido a comprender los problemas, estudiar las diferentes situaciones y alternativas para aplicar la mejor solución posible. Especialmente en el último año se ha recibido una formación especializada en reconocimiento de patrones y tratamiento digital de imágenes.

- **Investigación**: uno de los puntos fundamentales en cualquier PFC. Se ha buscado información para caracterizar el estado del arte, a partir del cual se ha desarrollado y mejorado un algoritmo de la literatura.
- **Desarrollo**: se ha implementado un simulador de reconocimiento de huella dactilar, imponiéndole las restricciones propias del entorno, en este caso una tarjeta inteligente. Para ello se han desarrollado las fases que lo componen: extracción de minucias, alineación, cálculo de similitud y toma de decisión.
- **Memoria**: es la última fase del Proyecto, en la cual se ha descrito el sistema, junto con los problemas encontrados durante la fase de investigación y desarrollo. Además se han recogido los resultados obtenidos con el simulador implementado y se han propuesto mejoras para el sistema.

2. Introducción a la biometría

El término biometría viene del griego “bio” que significa vida y “metría” que significa medida o medición. De acuerdo al diccionario de la Real Academia de la Lengua Española, biometría es el estudio mensurativo o estadístico de los fenómenos o procesos biológicos; sin embargo, nos centraremos para el tema que nos concierne en el concepto de sistema biométrico, que es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas [1].

Desde la antigüedad se han utilizado diferentes partes del cuerpo para identificar a las personas. Prueba de ello son las evidencias arqueológicas que relacionan huellas con identidad (dibujos rupestres junto con impresión de huellas), y más formalmente en los primeros trabajos científicos del siglo XVI donde aparecen estudios de formación anatómica, caracterización del cuerpo... y concretamente en el ámbito de identificación en los siglos XVIII-XIX. Más adelante, durante el siglo XX, algunos rasgos biométricos como las huellas son aceptados como método de identificación y pruebas en procesos judiciales [5].

2.1 Características de los rasgos biométricos

La biometría aprovecha que hay ciertas características biológicas o conductuales singulares e inalterables, por lo que pueden ser analizadas y medidas para crear una realización biométrica. Estas características son difíciles de perder, transferir u olvidar y son perdurables en el tiempo.

La biometría se soporta en cinco pilares o conceptos básicos que son [5]:

- **Universalidad**: todo individuo debe poseerlo.
- **Unicidad**: personas distintas deben poseer rasgos diferenciados.
- **Permanencia**: el rasgo debe ser invariable en el tiempo a corto plazo.
- **Perennidad**: el rasgo debe ser permanente a largo plazo.
- **Mensurabilidad**: el rasgo debe de poder ser caracterizado cuantitativamente.

En la biometría se distinguen dos grupos de rasgos biométricos los fisiológicos o morfológicos y los conductuales.

Los rasgos biométricos morfológicos o fisiológicos son aquellos que se componen de características físicas inalterables y presentes en la mayoría de los seres humanos tales como: huella dactilar, geometría de la mano, características del iris, patrones vasculares de la retina, mano, etc.

Los rasgos biométricos conductuales son aquellos que se basan en parámetros de la conducta del ser humano tales como: pulsaciones del teclado, discurso, dinámica de la firma, etc.

2.2 Rasgos biométricos

A pesar de la multitud de modalidades biométricas que se han documentado en la literatura, no todas cumplen o son viables para ciertas aplicaciones, esto implica que a la hora de realizar un sistema de reconocimiento automático se debe realizar un estudio del entorno en el que va a trabajar para poder elegir el rasgo biométrico más adecuado. A continuación se presenta una descripción de los principales rasgos biométricos.

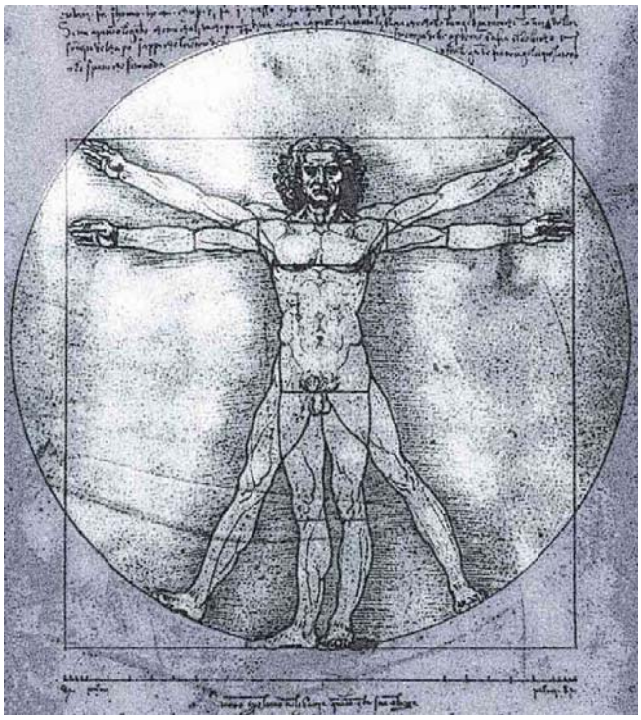


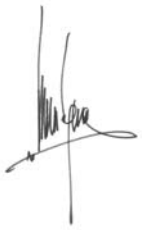
Figura 2.1: **El Hombre de Vitruvio, famoso dibujo con notas anatómicas de Leonardo da Vinci, forma parte de un estudio sobre las proporciones del cuerpo humano 1492.**

- **Huella dactilar**

La huella dactilar se lleva usando como método de identificación de individuos desde hace ya varios siglos en entornos policiales y forenses. Una huella consiste en un conjunto de valles y crestas que son capturados al presionar el dedo contra un sensor. Es única para cada persona y cada dedo. Actualmente la exactitud de los sistemas de reconocimiento de huella disponibles es muy elevada. Los sensores son baratos y una gran cantidad de dispositivos portátiles comienzan a incluirlos (PDAs, móviles, portátiles, etc.)

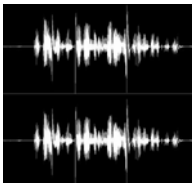
- **Iris**

El iris es altamente distintivo para cada uno de los dos ojos de cada individuo. Su captura requiere participación por parte del usuario, ya que debe situarse a una distancia predeterminada del sensor, y la tecnología es cara. Han aparecido nuevos sistemas menos intrusivos y con mejor relación precio-efectividad.



- **Firma**

La forma de firmar de cada persona es característica de ella misma. Aunque requiere contacto con una superficie y la cooperación del usuario. Es un rasgo muy aceptado como método de autenticación ya que se usa ampliamente en cantidad de transacciones. La firma varía a lo largo del tiempo para un mismo individuo y está influenciado por su estado físico y emocional. Además existen sujetos cuya firma varía muy significativamente en cada realización, por lo que su identificación es compleja.

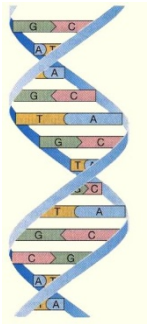


- **Voz**

La voz es una combinación de características físicas y de conducta. Las características físicas del habla de cada individuo permanecen invariables, pero las características de conducta cambian a lo largo del tiempo y se ven influenciadas por la edad, las afecciones médicas o el estado de ánimo de la persona. Las principales desventajas de este rasgo son su baja distintividad y la facilidad con la que puede ser imitado. Por el contrario, la voz es un rasgo biométrico muy aceptado y fácil de obtener.

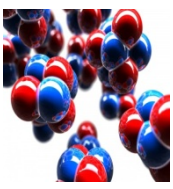
- **Escritura**

La escritura está dentro de los rasgos biométricos de comportamiento, por lo que es variable a lo largo del tiempo. Su captura es poco invasiva pero no constituye un rasgo tan discriminatorio como el ADN, por ejemplo.



- **ADN**

El ADN es un código único para cada individuo, excepto en el caso de los gemelos idénticos (monocigóticos). Actualmente es el método más común en aplicaciones forenses para reconocimiento de personas, pero presenta ciertas limitaciones en aplicaciones de reconocimiento automático. Los factores que limitan su uso en este tipo de aplicaciones son la facilidad para robar este rasgo biométrico, la lentitud del proceso de reconocimiento y la necesidad de que sea asistido por una persona. Además, la información que se puede extraer a partir del ADN de una persona puede revelar discapacidades u otras características que el individuo no desee hacer públicas.



- **Olor**

Cada objeto produce un olor que es característico de su composición química, lo distingue del resto de objetos y que puede ser capturado por sensores químicos, cada uno sensible a una sustancia química. Una parte del olor emitido por los seres humanos es distintiva para cada uno de ellos, pero resulta complicado descartarla de sustancias artificiales como perfumes y desodorantes.

- **Huella de la palma de la mano**

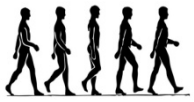
La palma de la mano, al igual que la huella dactilar, consiste en una estructura de valles y crestas. Al tener un área mayor que la de un dedo, este rasgo es más distintivo que la huella dactilar y proporciona información adicional que permite una mayor exactitud.

- **Escáner de retina**

La estructura vascular de la retina se supone diferente para cada individuo y cada ojo. Es el rasgo biométrico más seguro por su dificultad para duplicarlo. Pero su captura requiere la cooperación del usuario y contacto con el sensor, por lo que su aceptabilidad por parte del usuario se ve seriamente afectada. Además, puede revelar ciertas afecciones médicas.

- **Dinámica de tecleo**

Hipotéticamente cada persona tiene una dinámica de tecleo característica. Este rasgo es de conducta por lo que varía a lo largo del tiempo y es poco distintivo, pero proporciona información suficientemente discriminatoria para identificación en casos sencillos. Para su captura basta con emplear secuencias de tecleo del usuario, por lo que no es intrusivo.

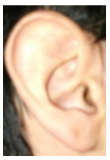


- **Forma de caminar**

La forma de caminar de cada individuo es un rasgo biométrico complejo a nivel espacio-temporal. No es un rasgo muy distintivo, pero puede ser suficientemente discriminatorio en aplicaciones que requieran un bajo nivel de seguridad. Forma parte de los rasgos biométricos de comportamiento y varía a lo largo de tiempo, pero su adquisición es no invasiva y para su captura es suficiente una cámara de vídeo.

- **Geometría de la mano**

Los sistemas de reconocimiento para este rasgo se basan en un conjunto de medidas físicas como la forma de la mano, el tamaño de la palma y la longitud y el ancho de los dedos. Los factores ambientales no suponen un problema pero la geometría de la mano es un rasgo de baja distintividad de cada individuo y está sujeto a cambios a lo largo de la vida de una persona.



- **Oreja**

La forma del borde de la oreja y la estructura gelatinosa es una característica única en cada persona. Los sistemas propuestos en la actualidad suelen emplear la distancia de los salientes del borde de la oreja con respecto a una referencia común del interior de la oreja.

- **Cara**

El rostro es probablemente el rasgo biométrico más usado en el reconocimiento humano entre individuos y supone un método de reconocimiento no invasivo. Las aproximaciones para el reconocimiento facial se basan bien en la localización y forma de los atributos faciales como ojos, nariz, labios y barbilla junto con su relación espacial (análisis local), o bien en un análisis global de la imagen de la

cara. Las mayores limitaciones consisten en la forma de adquisición de las imágenes, requiriendo a veces un fondo fijo y simple o una iluminación especial, y en los problemas de reconocimiento de imágenes capturadas desde diferentes ángulos y bajo diferentes condiciones de iluminación.

- **Termogramas**

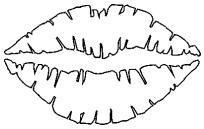
El patrón de calor radiado por el cuerpo humano es característico de cada individuo. Puede ser capturado por una cámara de infrarrojos de forma no intrusiva o incluso oculta. La mayor desventaja de esta clase de sistemas es el coste de los sensores y su vulnerabilidad ante otras fuentes de calor no controlables. Los termogramas también se emplean para captar la estructura de las venas de la mano.

- **Venas de la mano**

La identificación biométrica por las venas de la mano es un medio seguro difícilmente falsificable. Las venas tienen múltiples e innumerables características que las diferencian, por lo que asumir una falsa identidad falsificándolas es extraordinariamente difícil.

- **Espectroscopia de la piel**

La calidad óptica de la piel humana está determinada por sus propiedades químicas y estructurales, que varían de una persona a otra. Estas propiedades pueden ser medidas usando espectroscopia óptica de reflexión difusa. Esta tecnología biométrica usa un sensor biométrico basado en un diodo emisor de luz (LED) y foto detectores de silicio que fueron desarrollados para mejorar las medidas biométricas basadas en las propiedades ópticas de la piel en los dedos, manos u otros sitos de la piel.



- **Reconocimiento de labios**

Esta tecnología biométrica se divide en tres subcategorías que son: huella de los labios, movimiento de los labios y forma de los labios. La huella de los labios es conocida en la ciencia forense por ser diferente para cada individuo, así como las huellas digitales. El movimiento de los labios ayuda a la identificación asociada con el reconocimiento de la voz. La forma de los labios puede ser usada como una característica o rasgo individual para lograr la autenticación.

- **Más tecnologías**

Actualmente se encuentran en desarrollo muchas otras tecnologías, algunas de ellas son:

- **Reconocimiento de uña**, tecnología emergente que no ha sido muy estudiada. Existe una patente del 17 de febrero de 1998 en Estados Unidos asignada a Minnesota Mining and Manufacturing Company.
- **Dinámica del ratón**, desarrollado en Queen Mary, Universidad de Londres.
- **Pulso de la sangre**, pulso cardíaco, investigado en La escuela Klipsh de ingeniería eléctrica y computadores, New Mexico State University.

- **Radiografías Dentales**, La universidad de West Virginia está desarrollando un sistema automático de identificación dental (ADIS – Automated Dental Identification System)
- **Marcas de mordida**, patentado como aparato y método de identificación en 1986 por Sheryl L. Ames en Estados Unidos.
- **Reflexión de ondas acústicas en el cabeza, desarrollado** por el doctor James Wayman del Departamento de defensa de Estados Unidos.
- **Impedancia de la piel**.
- **Crestas de las articulaciones de los nudillos**, patentado en Estados Unidos por Charles Colbert en 1997 y asignada a Personnel Identification & Entry Access Control Inc.
- **Arrugas del dedo**, Toshiba + TEC presentaron un sistema para medir las arrugas del dedo en 1998.
- **Perfil de presión de la mano**, patentado en 2003 ante la Organización Mundial de propiedad intelectual, Estados Unidos, Canadá y Australia por parte de Robert D. Inkster, David M. Lokhorst y Ernest M. Reimer.
- **Transmisión de sonido de los huesos**, patentado en 2003 en Estados Unidos por parte de Yumi Kato, Tadashi Ezaki y Hideo Sato y asignado a Sony Corporation.
- **Campo Bioeléctrico**, se encuentra disponible en el mercado biofinder II y III que detecta los campos bioeléctricos de una persona a una distancia máxima de 20 pies, registrado con la Agencia Logística de defensa (DLA) código 0KYJ6, Departamento de justicia y Departamento de Agricultura de Estados Unidos.
- **Firma bio-dinámica**, patentada por Daniel H. Lange, asignada a IDesia Ltd., la patente más antigua es de 2004, se ha patentado en la Organización Mundial de propiedad intelectual, Oficina Europea de patentes, Canadá, China, Australia, Estados Unidos y Corea del sur. Todas las patentes tienen como título "Método y aparato para el reconocimiento de la identidad electro-biométrica".
- **Seguimiento del movimiento del ojo**, propuesto por el Instituto de Ciencias Computacionales de la Universidad de Tecnología de Silesian en Polonia.
- **Topografía de la superficie de la córnea**, patentado por Franciscus Hermanus Maria Jongsma y Johny de Brabander en 2004 ante la Organización Mundial de Propiedad Intelectual.
- **Superficie tridimensional del dedo**, investigación desarrollada por Damon L. Woodard en el laboratorio de investigación de visión de computadores del Departamento de Ciencias de la Computación e Ingeniería de la Universidad de Notre Dame.

Tecnología	Firma	Voz	Geometría facial	Iris	Retina	Geometría de la mano	Huella digital
Como Trabaja	Captura y compara ritmo, aceleración, y presión de la firma	Captura y compara cadencia, pitch, y tono de la voz	Captura y compara patrones faciales	Captura y compara los patrones del iris	Captura y compara los patrones de la retina	Mide y compara dimensiones de la mano y dedos	**Captura y compara patrones de la huella digital**
Tamaño plantilla (bytes)	1000 – 3000	10000-20000	84 o 1300	512	96	9	**250- 1000**
Fiabilidad	Alta	Alta	Baja	Baja	Baja	Baja	**Muy alta**
Facilidad De Uso	Media	Media	Baja	Baja	Baja	Alta	**Alta**
Posibles Incidencias	Edad, cambios, analfabetismo	Ruido, temperatura y meteorología	Edad, Cabello, luz	Luz	Gafas	Edad, Ausencia de miembro	**Ausencia de miembro**
Costo	Alto	Alto	Medio	Muy alto	Alto	Bajo	**Bajo**
Aceptación Usuario	Media	Media	Baja	Baja	Baja	Alta	**Alta**

Tabla 2.1: Comparativa de las tecnologías biométricas más comunes [1].

Para mejorar la fiabilidad del sistema y hacerlo más robusto en cada una de las áreas que se han expuesto en la tabla anterior, se ha propuesto la combinación de distintos rasgos en un mismo sistema biométrico en lo que se conoce como sistemas biométricos multimodales [6].

2.3 Sistemas biométricos

Un sistema biométrico está constituido por un reconocedor de patrones cuyo modo de operación es el siguiente: captura un rasgo biométrico, extrae un conjunto de características y las compara con varios patrones almacenados para decidir acerca de la identidad del individuo.

2.3.1 Aplicaciones de los sistemas biométricos

A lo largo de la historia, se ha tratado de identificar a las personas de una forma fácil y rápida. Esta necesidad ha ido aumentando con el tiempo: compras a través de Internet, venta telefónica... y esto ha llevado a un aumento de los intentos de suplantación de identidad y los riesgos de seguridad que entraña el no poder tener un control de identidad, tanto a nivel de ciudadanos de un país como de sus fronteras. Como solución a estos problemas aparece la biometría, capaz de identificar a un individuo no por lo que posee o sabe, sino por lo que es. Los campos de operación de los sistemas biométricos se dividen en tres grandes grupos [1]:

- Aplicaciones comerciales: protección de datos electrónicos, protección en red, e-comercio, cajeros automáticos, control de acceso físico, etc.
- Aplicaciones gubernamentales: DNI, carné de conducir, pasaporte, control en fronteras, etc.
- Aplicaciones forenses: identificación de cadáveres, investigación criminal, identificación de terroristas, determinación de parentesco, etc.

Hoy en día, los sistemas biométricos se encuentran cada vez más presentes en nuestra vida cotidiana. Un ejemplo de ello es el ValleyCare Hospital [7] en la Costa Oeste de Estados Unidos, que se ha convertido en el tercer hospital del país que instala un sistema biométrico, por el cual un profesional de la salud puede acceder instantáneamente a la historia clínica del paciente cuando escanea el patrón de venas de la palma de su mano. De esta manera, pretenden eliminar los registros de pacientes duplicados y aumentar la seguridad de los mismos. Adicionalmente, va a ayudar a identificar a aquellos pacientes que están inconscientes y no pueden responder.

Como hemos dicho antes, "la biometría toca a la puerta" no es sólo una forma de hablar, ya que las cerraduras biométricas se han hecho asequibles a nivel de consumidor. Los propietarios de casas pueden dejar de preocuparse si pierden u olvidan las llaves, a la vez que mantienen un alto nivel de seguridad en el hogar, según un artículo del Chicago Tribune [8].

El ejemplo específico es el cerrojo SmartScan (imagen de la derecha), el cual opera con la tecnología de escaneo subcutáneo, mucho más difícil de falsificar que los escáneres que leen la superficie de la piel, y requiere que el dedo a escanear forme parte de un ser humano viviente, a la vez que no exige manos limpias o secas.

Por otro lado, el desarrollo de grandes sistemas biométricos conlleva un aumento de costes, tal es el caso de los nuevos pasaportes biométricos, que comenzaran a implantarse en el Reino Unido, según un artículo de Tech Radar [9]. Para las nuevas implementaciones, se añaden las huellas digitales y reconocimiento facial a los chips de las tarjetas sin contacto instalados en dichos pasaportes, lo cual representará un incremento de 28 libras para la renovación de un pasaporte británico.

Paralelamente a estos avances, y muy relacionado con el objetivo de este PFC, el Instituto Nacional de Estándares y Tecnología (NIST) [10] continúa su marcha hacia la aprobación de una tarjeta de identificación que almacena una huella digital y puede ser rápidamente autenticada sin que los datos abandonen la misma. Las pruebas Match-On-Card [2] (coincidencia en la tarjeta) muestran que la tecnología existente funcionará, aunque la precisión de la coincidencia no está a la altura de los estándares de NIST.

Por último, otro gran mercado para los sistemas biométricos es el de la seguridad en los aeropuertos. El Aeropuerto Internacional de Bahréin [11] instalará puertas de seguridad biométricas, según un artículo de Gulf Daily News. Los nuevos sistemas, llamados ImmSec, fueron desarrollados por la empresa sueca de tecnología de seguridad Gunnebo Security Group.

Los sistemas ImmSec utilizarán un escáner de huellas digitales y tarjetas inteligentes, y contienen además pantallas LCD para escanear a los pasajeros y al equipaje. Estas pantallas serán ubicadas en cuatro puntos del aeropuerto.

Las puertas detienen a cada individuo con unos paneles giratorios que requieren que la información de la tarjeta y las huellas coincidan para entonces dejarlos pasar. El sistema está conectado al servidor de la Central Informatics Organization para poder acceder a la información de identidad.

Figura 2.2: Sistemas ImmSec de identificación biométrica para aeropuertos.

Cada puerta está equipada además con sensores en la parte superior, diseñados para captar cualquier brecha de inmigración, por ejemplo, tratar de pasar niños u objetos a escondidas. Bahréin será el tercer país en implementar dicha tecnología en sus aeropuertos internacionales, después del Reino Unido y Japón.

2.3.2 Problemas y limitaciones de los sistemas biométricos

El sistema de identificación perfecto no existe, y los sistemas biométricos, por tanto, presentan deficiencias, debidas en un alto grado a que los rasgos biométricos de una persona y su representación varían considerablemente según el método de adquisición, el entorno en el que se realiza la captura y la interacción del usuario con el sistema de adquisición (ver Figura 2.3). Las razones más comunes por las que se producen variaciones son [1]:

- **Presentación inconsistente**: la señal capturada por el sensor depende tanto de las características intrínsecas del rasgo biométrico como de la forma en la que se presenta dicho rasgo, pudiendo llegar a presentarse fuera de la zona de captura del sensor. Por ejemplo, la forma tridimensional de un dedo se mapea en una superficie bidimensional del sensor, por lo que se pueden tener diferentes impresiones de un mismo dedo.

Figura 2.3: Variación de una señal biometría en diferentes capturas del la huella del mismo dedo.

- **Presentación irreproducible**: los rasgos biométricos representan medidas de una característica biológica o de comportamiento y están expuestos a accidentes y heridas que pueden cambiar su estructura de forma permanente, a cambios en su aspecto externo debido a adornos como joyas o al maquillaje, etc. Todos estos fenómenos contribuyen a la variación de la señal capturada en diferentes adquisiciones. Casos extremos pueden ser amputaciones de falanges, quemaduras, desfiguraciones...
- **Captura imperfecta**: las condiciones de captura de una señal en situaciones prácticas no son perfectas y causan variaciones en la señal capturada. Estas condiciones pueden ser la iluminación para la captura de imágenes faciales, las características del canal para señales de voz, un contacto no uniforme en la toma de huellas dactilares, etc.

Asimismo, los sistemas biométricos tienen otras limitaciones:

- **Ruido en los datos adquiridos**: los datos adquiridos pueden tener un componente ruidoso o estar distorsionados. El ruido puede estar producido por un sensor sucio o en mal estado o por condiciones ambientales desfavorables. Los datos adquiridos con ruido pueden dar lugar a que un usuario sea rechazado erróneamente.
- **Variaciones intra-clase**: los datos biométricos adquiridos durante un proceso de autenticación suelen ser diferentes de los datos que fueron usados para generar el patrón durante el proceso de registro, afectando por tanto al proceso de verificación. Estas variaciones pueden producirse porque el usuario interactúa de forma diferente con el sensor (ejemplo: cambia la forma de poner el dedo) o porque hay cambios en el rasgo (ejemplo: el usuario lleva distinta indumentaria en una foto o vídeo)

- **Unicidad**: aunque se espera que un rasgo biométrico varíe entre individuos, pueden existir similitudes entre diferentes usuarios en el conjunto de características usadas para representar ese rasgo. Esta limitación restringe la capacidad de discriminar usando ese rasgo biométrico.

- **No universalidad**: aunque se espera que todos los individuos posean un cierto rasgo biométrico, es posible que exista un subconjunto de individuos que carecen de él, por ejemplo: sufrir daños irreparables en un dedo, no saber escribir, etc.

- **Ataques**: un impostor puede intentar imitar el rasgo biométrico de un usuario legítimo para sortear el sistema. Los rasgos biométricos de comportamiento son más susceptibles a este tipo de ataques que los fisiológicos (imitadores de firma o voz, etc.)

2.4 Aceptación en la sociedad

La sociedad es la que determina el éxito de los sistemas de identificación basados en rasgos biométricos. La facilidad y comodidad en la interacción con el sistema contribuye a su aceptación [1]. Si un sistema biométrico permite medir una característica de un individuo sin necesidad de contacto directo, se percibe como mejor. Además, las tecnologías que requieren muy poca cooperación o participación de los usuarios suelen ser percibidas como más convenientes. Por otro lado, los rasgos biométricos que no requieren la participación del usuario en su adquisición pueden ser capturados sin que el individuo se dé cuenta y esto es percibido como una amenaza a la privacidad por parte de muchos usuarios. El tema de la privacidad adquiere gran relevancia con los sistemas de reconocimiento biométrico porque los rasgos biométricos pueden proporcionar información muy personal de un individuo, como afecciones médicas, y esta información puede ser utilizada de forma poco ética.

Por otro lado, los sistemas biométricos pueden ser empleados como uno de los medios más efectivos para la protección de la privacidad individual. Si un individuo extravía su tarjeta de crédito y otra persona la encuentra, podría hacer un uso fraudulento de ella. Pero si la tarjeta de crédito únicamente pudiese ser utilizada si el impostor suplantase los rasgos biométricos del usuario, éste estaría muchísimo más protegido. Otra ventaja del uso de los rasgos biométricos consiste en limitar el acceso a información personal.

La mayoría de los sistemas biométricos comerciales disponibles hoy en día no almacenan las características físicas capturadas en su forma original, sino que almacenan una representación digital en un formato encriptado. Esto tiene dos propósitos: el primero consiste en que la característica física real no pueda ser recuperada a partir de su representación digital, lo que asegura privacidad, y el segundo se basa en que el encriptado asegura que sólo la aplicación designada puede usar dicha representación digital.

Para una visión global de la evolución de los sistemas biométricos a lo largo de la historia, consultar anexo: Línea del tiempo de la biometría.

3. Sistemas automáticos de reconocimiento

3.1 Estructura general

Todos los sistemas de reconocimiento automático de patrones poseen una estructura funcional común, formada por varias fases, cuya forma de proceder depende de la naturaleza del rasgo o señal a reconocer. Además hay que diferenciar entre dos tipos de sistema, los que necesitan una base de datos centralizada para identificar o verificar al usuario, ver Figura 3.1, y los sistemas con base de datos distribuida, como es el caso de sistemas formador por tarjetas inteligentes, ver Figura 3.2, objeto de estudio de este Proyecto, en los que además del algoritmo de verificación, también llevan guardado una o varias realizaciones de los patrones con los que se comparará la identidad solicitante.

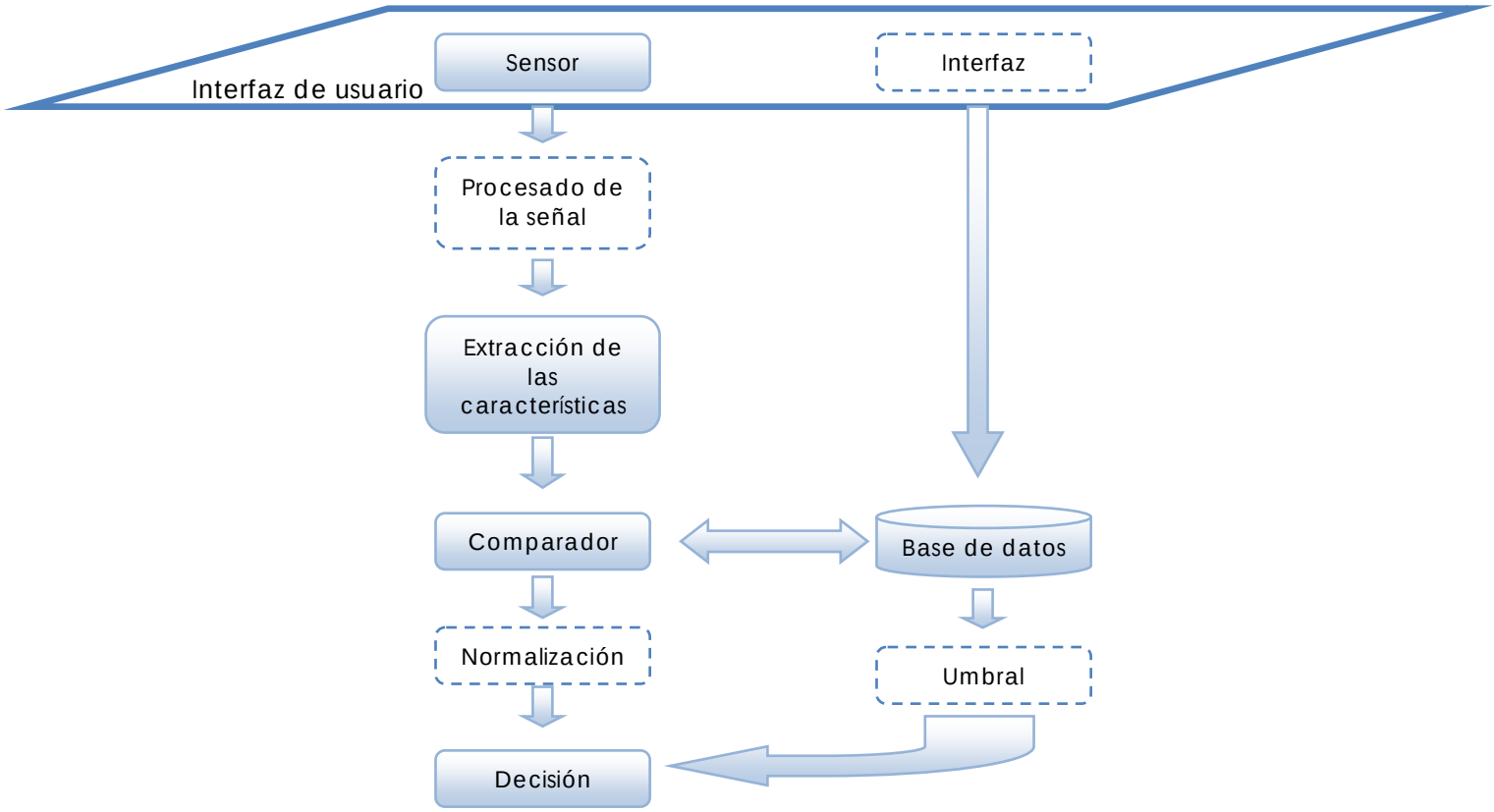


Figura 3.1: Esquema de funcionamiento de un sistema de reconocimiento biométrico con base de datos centralizada.

En general el usuario únicamente tiene acceso al sensor, el cual captura el rasgo biométrico. Los módulos marcados con línea continua son las entidades hardware o software básicas del sistema, y las etapas de procesado opcionales son las marcadas con línea discontinua.

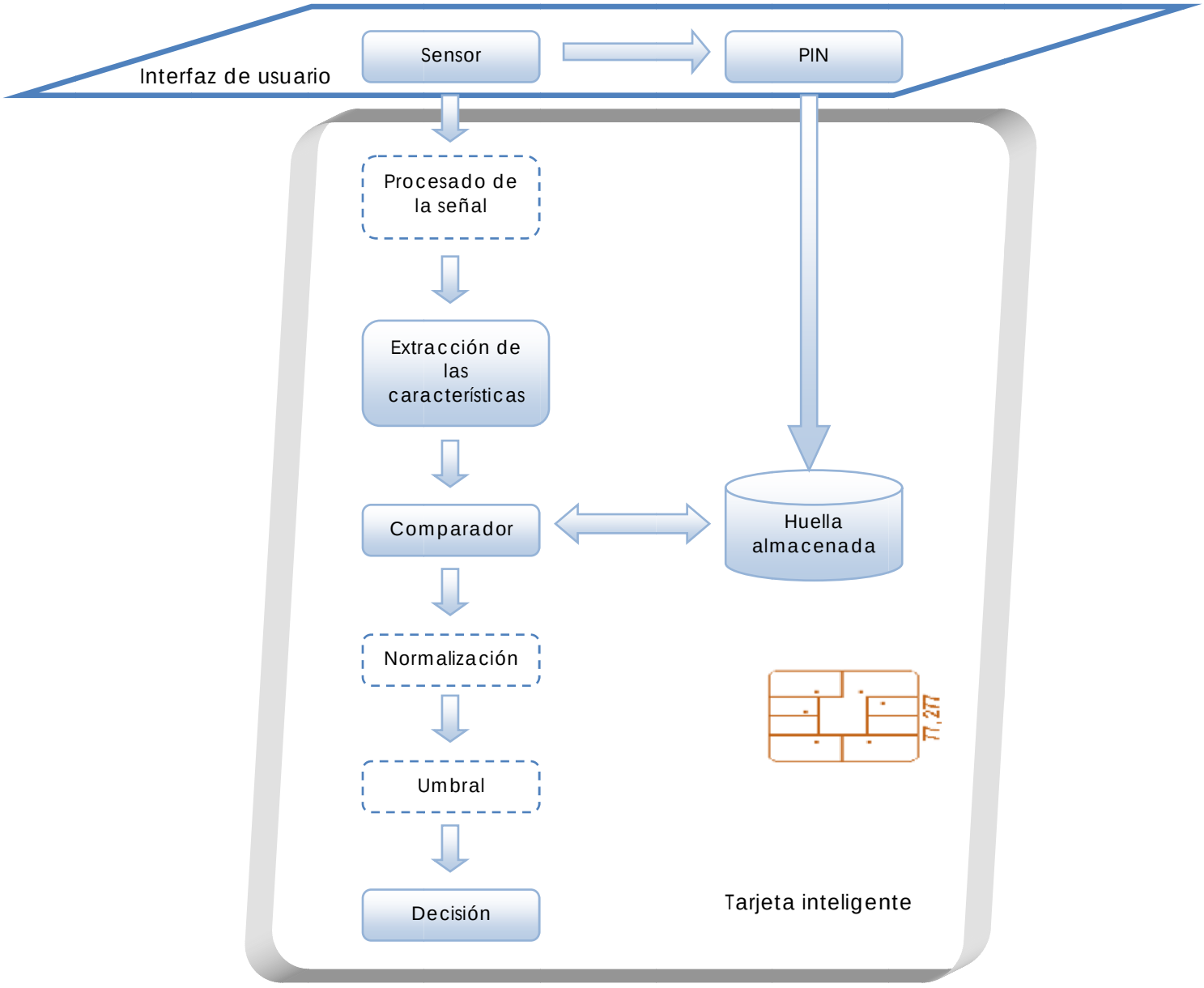


Figura 3.2: Esquema de funcionamiento de un sistema de reconocimiento biométrico con base de datos distribuida.

Para explicar los diagramas anteriores, podemos dividirlos, de forma general, en cuatro fases de funcionamiento, formadas por la adquisición de datos, seguida de el pre-procesado, extracción de características y terminando con la comparación de patrones.

- **Adquisición de datos:** En esta fase se recogen los datos analógicos de partida a través de un transductor o sensor y se convierten en un formato digital. Este proceso es determinante ya que de él depende la cantidad y la calidad de la información adquirida, la implementación de las siguientes fases, y, por tanto, el resultado final que se obtiene.
- **Preprocesado**: En algunos casos es necesario acondicionar la información capturada para eliminar posibles ruidos o distorsiones producidas en la etapa de adquisición, o para normalizar la información a unos rasgos específicos para tener una mayor efectividad en el reconocimiento posterior.
- **Extracción de características:** En esta etapa se elimina la información que no resulte útil en el proceso de reconocimiento, ya sea por no ser específica de cada individuo o por ser redundante. De este modo, se extraen únicamente aquellas características que sean discriminantes entre distintos individuos y que al mismo tiempo permanezcan invariables para un mismo usuario, reduciéndose así mismo la duración de todo el proceso de reconocimiento, su coste computacional y el espacio a utilizar para almacenar la plantilla.
- **Comparación de patrones:** Una vez extraídas las características más significativas, es necesario elaborar un modelo que represente a cada individuo y que permita la evaluación de la correspondencia entre los patrones de entrada y el modelo de un individuo en particular.

En función del tipo de aplicación, los sistemas biométricos pueden trabajar con bases de datos centralizadas o distribuidas. Si necesitamos identificar a una persona, el sistema debe de contener alguno de sus rasgos biométrico en la base de datos, junto en el resto de información biométrica del resto de individuos asociados a esa base de datos, por ejemplo, el sistema AFIS de la Guardia Civil devuelve una lista ordenada de mayor a menor similitud en función del rasgo biométrico comparado en el sistema, y para ello es imprescindible un sistema centralizado con toda la información junta. Por otro lado están los sistemas distribuidos, que sólo cuentan con realizaciones del rasgo del "dueño" del dispositivo, (en nuestro caso, la tarjeta inteligente) con los que se realiza una comparación, cuyo resultado es aceptación o rechazo, para verificar al portador como legitimo dueño, o por el contrario, en el caso de que sea un impostor, rechazarlo sin tener la posibilidad de conocer su verdadera identidad. Esto se debe a que a diferencia de las bases de datos centralizadas no se cuenta con la información del resto de individuos.

Dentro del ámbito de sistemas de reconocimiento basados en bases de datos, pueden trabajar de dos formas: modo reconocimiento positivo o modo reconocimiento negativo. El reconocimiento positivo trata de determinar si un usuario es quien afirma ser, mientras que el reconocimiento negativo intentan determinar si un usuario es quien niega ser, un ejemplo de este tipo de sistemas está instalado en los aeropuertos, con las listas negras de terroristas. Cabe destacar que la identificación negativa sólo puede ser realizada mediante rasgos biométricos, y no mediante métodos clásicos como contraseñas o llaves.

3.2 Modos de operación

Un sistema biométrico puede trabajar en modo verificación o identificación, pero para que ambos funcionen necesitan una fase previa, un modo registro, que es común a estos dos modos de funcionamiento [1]. Un esquema de cada uno de estos tres modos se muestra a continuación.

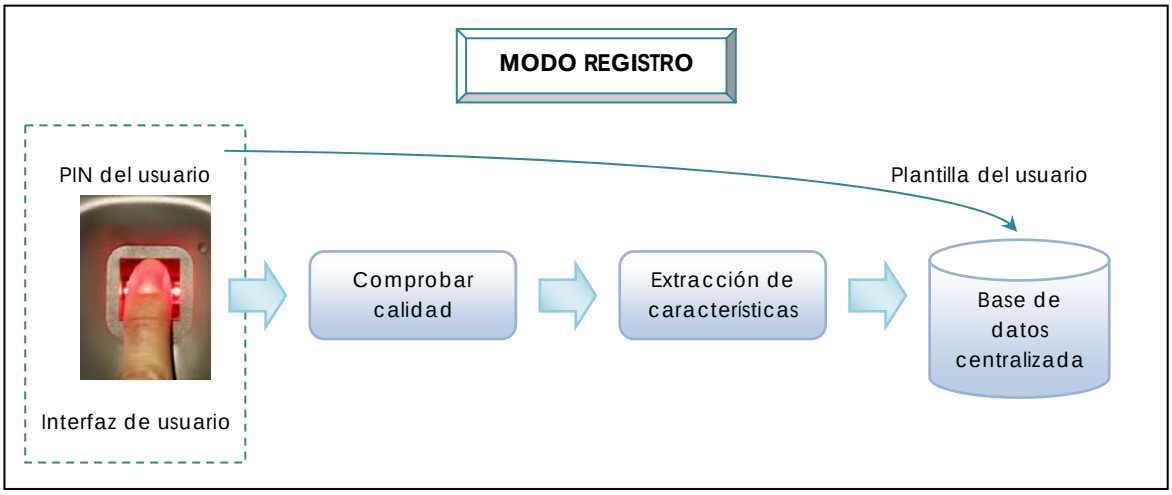


Figura 3.3: Esquema de funcionamiento en modo registro.

En el modo **registro**, el sistema adquiere una plantilla del rasgo biométrico que será utilizada posteriormente para evaluar la validez del usuario (ver Figura 3.3). Durante esta etapa, se produce un preprocesado de la señal biométrica, se extraen las características de interés y se almacenan en el sistema construyendo un modelo del usuario registrado. Dependiendo de la aplicación esta información será guardada en la base de datos del sistema o en otro tipo de dispositivos externos, como por tarjetas inteligentes, PDA's etc.

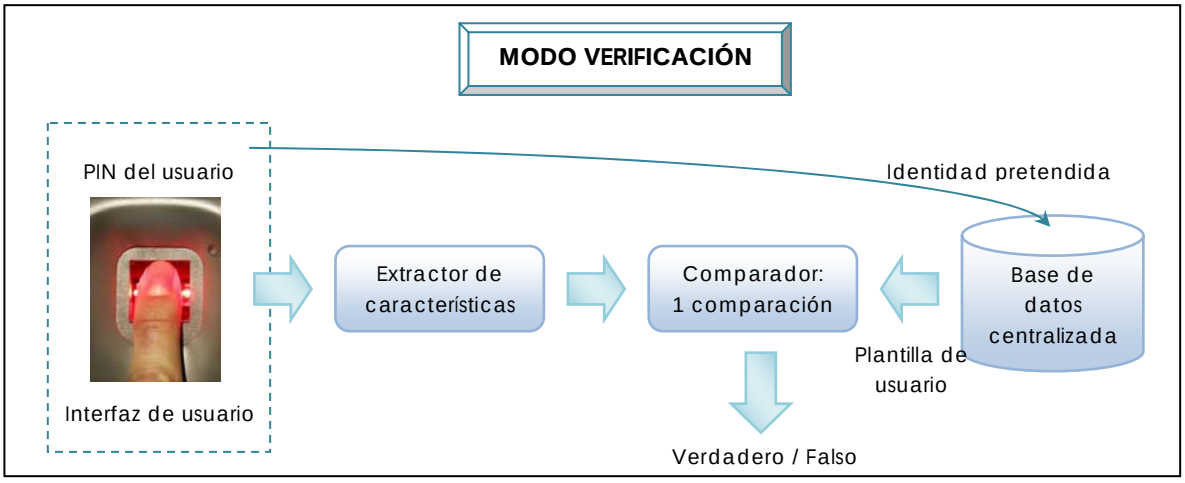


Figura 3.4: Esquema de funcionamiento en modo verificación.

Una vez creada la base de datos el sistema podrá entrar en funcionamiento en modo identificación o en modo verificación, además siempre se puede volver a la fase de registro para añadir o borrar usuarios.

En el modo **verificación o autenticación**, ver Figura 3.4, el sistema valida la identidad de una persona comparando el rasgo biométrico capturado en la entrada con su propia plantilla biométrica previamente almacenada en la base de datos. En general, el usuario indicará su identidad mediante un número de identificación personal, un nombre de usuario, una tarjeta o algún tipo de código. Posteriormente el sistema realizará una comparación uno a uno para determinar si el individuo es quien dice ser.

Las dos posibles salidas en este modo de funcionamiento dan lugar a la aparición de dos errores distintos:

- Falso Rechazo: se produce cuando el sistema indica que la información adquirida del usuario en la entrada no se corresponde con la plantilla almacenada, cuando realmente sí se corresponde.
- Falsa Aceptación: es complementario al falso rechazo y se produce cuando el sistema indica que la información adquirida del usuario en la entrada sí se corresponde con la plantilla almacenada, cuando realmente no se corresponde.

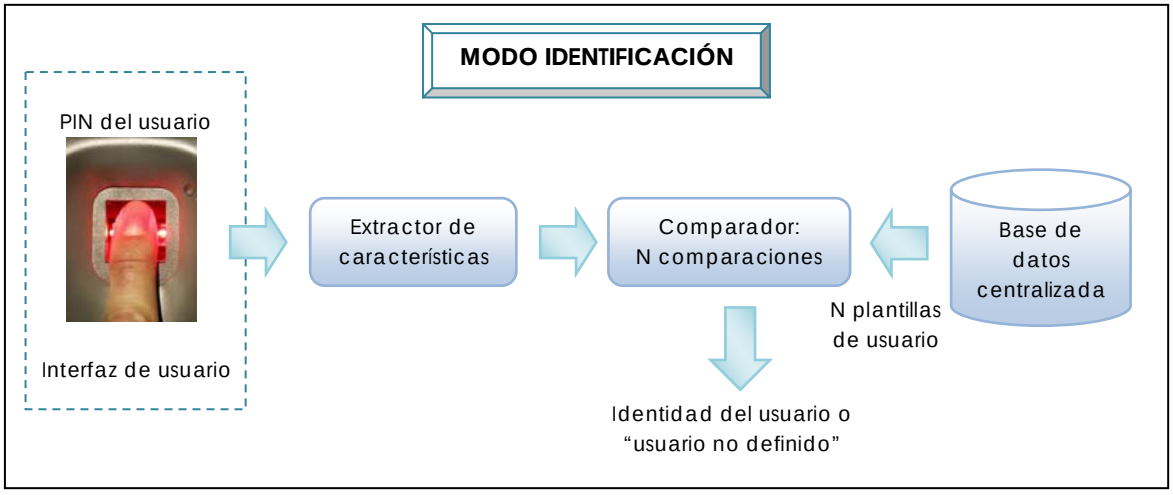


Figura 3.5: Esquema de funcionamiento en modo identificación.

En el modo **identificación**, el objetivo del sistema es el de clasificar una realización determinada de un rasgo biométrico de identidad desconocida como perteneciente a un usuario de entre un conjunto de *N* posibles individuos (ver Figura 3.5). El resultado de este tipo de sistemas suele ser una clasificación de las plantillas biométricas en función a su similitud con la plantilla que queremos identificar.

Dentro de estos sistemas debemos diferenciar dos posibles casos:

- Identificación en conjunto cerrado: en este caso el resultado del proceso es una asignación de identidad a uno de los individuos modelados por el sistema y conocidos como usuarios. Existen, por tanto, *N* posibles decisiones de salida posibles.

- Identificación en conjunto abierto: aquí debemos considerar una posibilidad adicional a las *N* del caso anterior; que el individuo que pretende ser identificado no pertenezca al grupo de usuarios, con lo que el sistema de identificación debería contemplar la posibilidad de no clasificar la realización de entrada como perteneciente a las *N* posibles. En este caso habría *N + 1* posibles decisiones.

Otro caso especial de los sistemas de identificación es el modo de búsqueda **screening o lista negra**, donde tenemos un conjunto reducido de plantillas biométricas de individuos y queremos saber si la persona es uno de ellos. Es una identificación en conjunto abierto, pero con resultado casi siempre negativo. Por ejemplo el caso antes mencionado del aeropuerto y la lista de terroristas más buscados.

3.2.1 Sistemas con bases de datos distribuidas

Una vez estudiado los modos de trabajo de un sistema biométrico, nos centraremos en los sistemas con bases de datos distribuidas. Estos sistemas cuentan con la gran ventaja de permitir un enorme grado de escalabilidad ya que el número de usuarios puede aumentar fácilmente sin tener que redimensionar la base de datos, precisamente porque no existe una gran base de datos como tal, sino que cada usuario es portador de una o varias realizaciones de su propio rasgo biométrico empleado por el sistema de reconocimiento. Una buena forma de implementar estos sistema puede ser usando tarjetas inteligentes ya que no sólo permiten el almacenado seguro de la información biométrica, sino que proporcionan un entorno capaz de ejecutar un algoritmo.

De esta manera un sistema con base de datos distribuida contaría con un **modo de registro**:

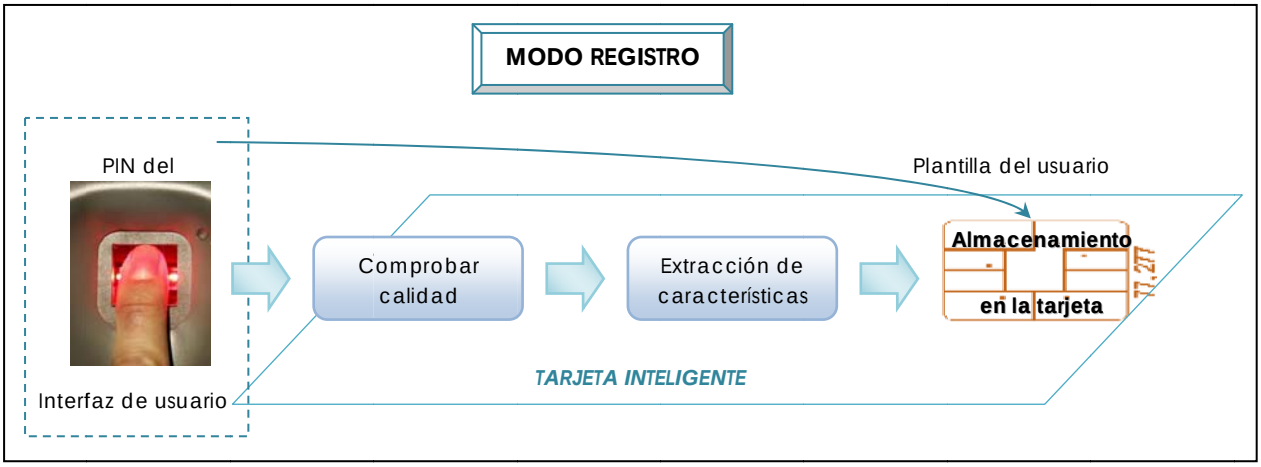


Figura 3.6: Esquema de funcionamiento en modo registro con base de datos distribuida.

El proceso sería el mismo que el descrito anteriormente, con la diferencia de que todo el procesado de la imagen se realizaría en la tarjeta (ver Figura 3.6).

En el **modo de verificación** la tarjeta se conecta con un sensor capaz de capturar el rasgo biométrico y de transferirlo a dicha tarjeta (ver Figura 3.7).

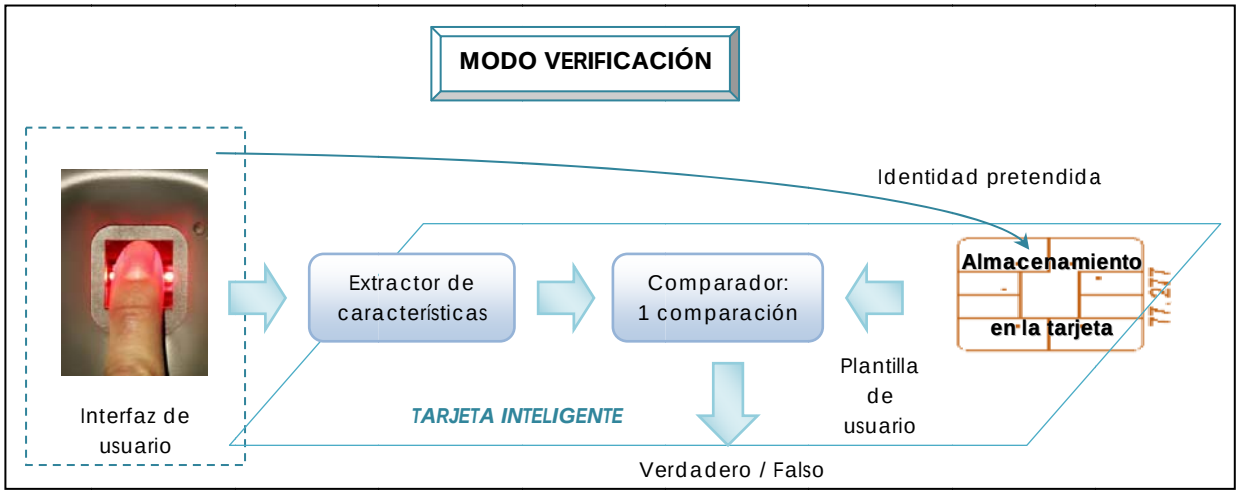


Figura 3.7: Esquema de funcionamiento en modo verificación con base de datos distribuida.

Una vez transferido, se realiza la comparación entre la plantilla enviada por el sensor y las plantillas almacenadas en la propia tarjeta. Si esta comparación resulta positiva se verifica al portador de la tarjeta como su legítimo dueño, en caso contrario se le considera un impostor.

Una característica de los sistemas con base de datos distribuida es que no pueden trabajar en modo identificación ya que sólo cuentan con la información biométrica del legítimo dueño del dispositivo.

3.3 Evaluación del rendimiento

Para determinar la bondad de nuestro sistema de reconocimiento, ya sea de verificación o de identificación, necesitamos una medida objetiva del rendimiento del mismo. Entenderemos rendimiento de un sistema biométrico como la precisión en el proceso reconocimiento. El rendimiento de un sistema lo podemos representar mediante curvas, valores, etc. que permitirán al desarrollador evaluar el sistema y compararlo con otros sistemas de referencia.

A la hora de poner en funcionamiento un sistema biométrico, hay que tener en cuenta que dos muestras de un mismo rasgo biométrico no son exactamente iguales debido a imperfecciones en las condiciones en las que se captura la imagen, cambios en los rasgos fisiológicos o de comportamiento del usuario, factores ambientales y a la interacción del usuario con el sensor entre otros. Por tanto, la respuesta del comparador de un sistema biométrico consiste en una puntuación o score que cuantifica la similitud entre la entrada y el patrón de la base de datos con el que se

está comparando. Cuanto mayor sea el parecido entre las muestras, mayor será la puntuación devuelta por el comparador y más seguro estará el sistema de que las dos medidas biométricas pertenecen a la misma persona.

La decisión del sistema está regulada por un umbral: los pares de muestras que generen puntuaciones mayores o iguales que el umbral se supondrán correspondientes a la misma persona, ordenándolas en una lista, mientras que los pares de muestras cuya puntuación sea menor que el umbral se considerarán de personas diferentes.

3.3.1 Criterios de evaluación de sistemas en modo verificación

En un sistema ideal, los rangos de variación de las puntuaciones obtenidas para usuarios impostores y genuinos están separados, de manera que no hay solapamiento entre sus distribuciones, pudiéndose establecer un umbral de decisión que discrimine perfectamente ambas clases. Sin embargo, en un sistema real existe una región en la que se solapan ambas distribuciones, como se muestra en la Figura 3.8 Si se fija un umbral, todas las puntuaciones, tanto de usuarios como de impostores, cuyo valor sea superior a ese umbral serán interpretadas por el sistema como usuarios registrados. Como consecuencia, el área bajo la curva de impostores que queda por encima del umbral es la probabilidad de que un impostor sea aceptado y se conoce como la tasa de falsa aceptación (FA). De igual modo, el área bajo la curva de usuarios válidos que queda por debajo del umbral es la probabilidad de que un usuario registrado no sea aceptado por el sistema y se denomina tasa de falso rechazo (FR). Según se sitúe el umbral, la FA y la FR varían. Si el umbral es bajo, el sistema será muy permisivo y dará como válidas informaciones impostoras, mientras que si el umbral es alto, se producirá el efecto contrario.

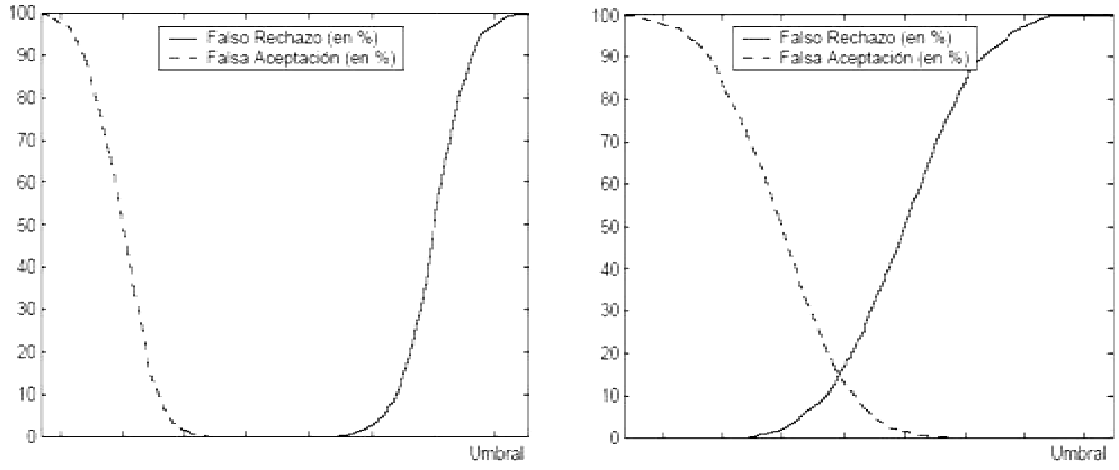


Figura 3.8: Izquierda: sistema ideal; Derecha: sistema real.

Un punto de dichas graficas que nos permite caracterizar de forma directa el funcionamiento del sistema es el punto de error igual (equierror), o EER (Equal Error Rate), ver Fig. 3.9, que es el punto en que las curvas de falsa aceptación (FA) y falso rechazo (FR) en función del umbral se cruzan. Por ello la tasa de igual error (EER) suele usarse para caracterizar con un único número el rendimiento de un sistema biométrico.

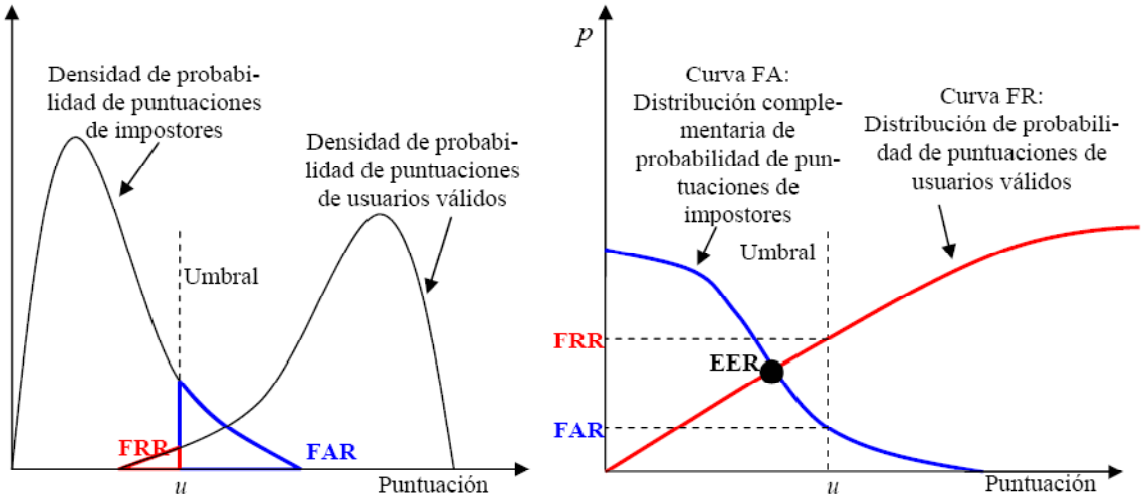


Figura 3.9: Densidades y distribuciones de probabilidad de usuarios e impostores.

A pesar de que el punto de EER corresponde al umbral donde se igualan FA y FR, ésto no implica que el sistema deba trabajar en ese punto. Para establecer el punto de trabajo del sistema se suele emplear la representación en forma de curvas DET (Detection Error Tradeoff), que consiste en la presentación de un error frente al otro en un eje normalizado, obteniéndose así una única curva para ambos tipos de error definida por todos los posibles puntos de trabajo del sistema. En esta curva, ver Figura 3.10, cualquier punto está dado por un valor de FA y otro de FR, de modo que no es necesario estar manejando varias curvas para determinar el punto de trabajo. Por contra, perdemos facilidad para encontrar el EER, que se localiza en la bisectriz del ángulo formado por la parte positiva del eje de FA y FR.

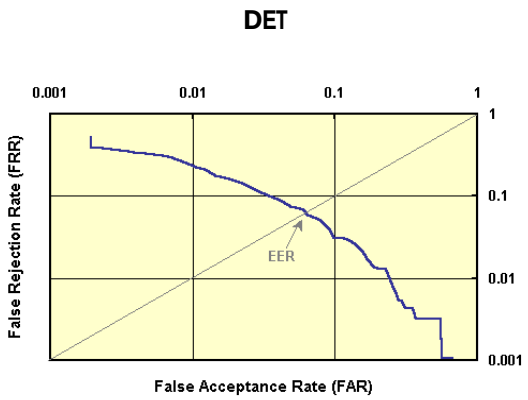


Figura 3.10: Curva DET (Detection Error Tradeoff)

En aplicaciones de alta seguridad (control de accesos), el punto de trabajo suele situarse en valores bajos de FA, para evitar que accedan impostores, a costa de tener alta FR. Por el contrario, en aplicaciones forenses se trabaja en baja FR para no perder individuos buscados, a costa de una alta FA. Las aplicaciones civiles suelen trabajar en un punto intermedio.

3.3.2 Criterios de evaluación de sistemas en modo identificación

En modo identificación, el sistema tiene que comparar los datos de entrada con todos los modelos de identidad almacenados en la base de datos, devolviendo una lista ordenada con los modelos con mayor parecido, en caso de que existan. De esta manera el rendimiento de un sistema de identificación se mide calculando en número relativo de veces que el sistema falla en identificar correctamente al usuario de entrada, o lo que es lo mismo, con qué frecuencia una realización de prueba es asignada a una identidad errónea.

3.4 Sistemas multibiométricos

Los sistemas multibiométricos son aquellos que combinan varias fuentes de información biométrica para mejorar el rendimiento de un determinado sistema, aumentando la cobertura de la población, ya que se reduce el fallo en el registro y se mejora la seguridad del sistema al aumentar la dificultad de imitar o falsificar varios rasgos simultáneamente [6]. De esta forma se mejora bastante el rendimiento de los sistemas clásicos unimodales.

Un sistema de este tipo puede operar de tres modos diferentes:

- **Modo serie**: las salidas del análisis de un rasgo biométrico se usan como entrada para análisis del siguiente rasgo, reduciendo así en cada paso el número de identidades posibles antes de emplear la siguiente característica. Este modo se usa, por ejemplo, poniendo en primer lugar un sistema poco preciso pero de rápido procesado para después, una vez reducidas rápidamente las posibles identidades, emplear un sistema más exacto.
- **Modo paralelo**: la información de múltiples rasgos biométricos se emplea simultáneamente en el proceso de reconocimiento. En contraposición al caso anterior, siempre se utilizan todos los sistemas fusionados lo cual a su vez requiere capturar todos los rasgos antes de decidir.
- **Modo jerárquico**: los clasificadores individuales se combinan en una estructura de árbol.

A su vez, existen varios niveles donde se puede combinar la información de múltiples sistemas, estos niveles de fusión son (ver Figura 3.15):

- **A nivel de sensor** (Figura 3.11): combinando la información capturada procedente de los diferentes sensores, por ejemplo la reconstrucción tridimensional de varias imágenes a partir de varias cámaras.

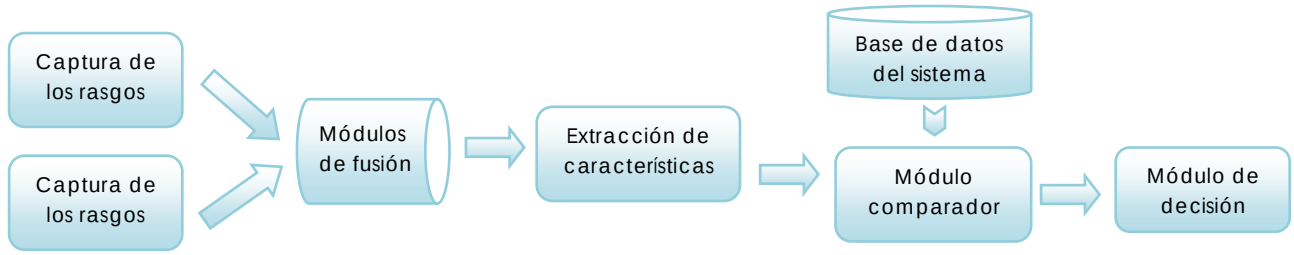


Figura 3.11: Fusión a nivel de captura del rasgo biométrico.

- **A nivel de extracción de características** (Figura 3.12): combinando las diferentes características extraídas.

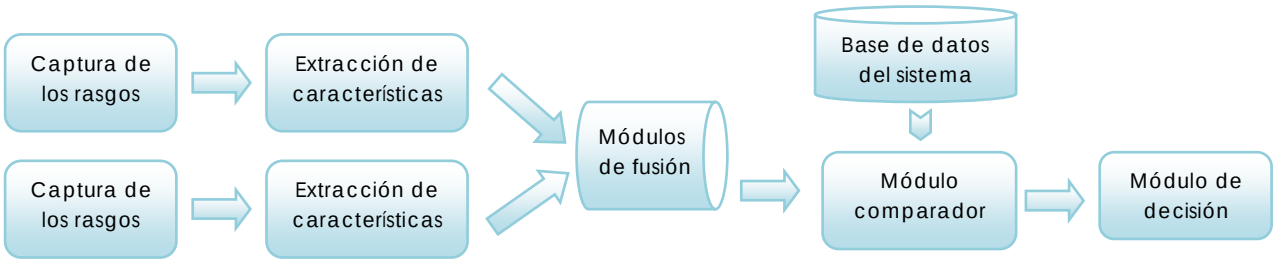


Figura 3.12: Fusión a nivel de extracción de características.

- **A nivel de puntuación (score)** (Figura 3.13): combinando las diferentes puntuaciones de similitud, por ejemplo un promedio.

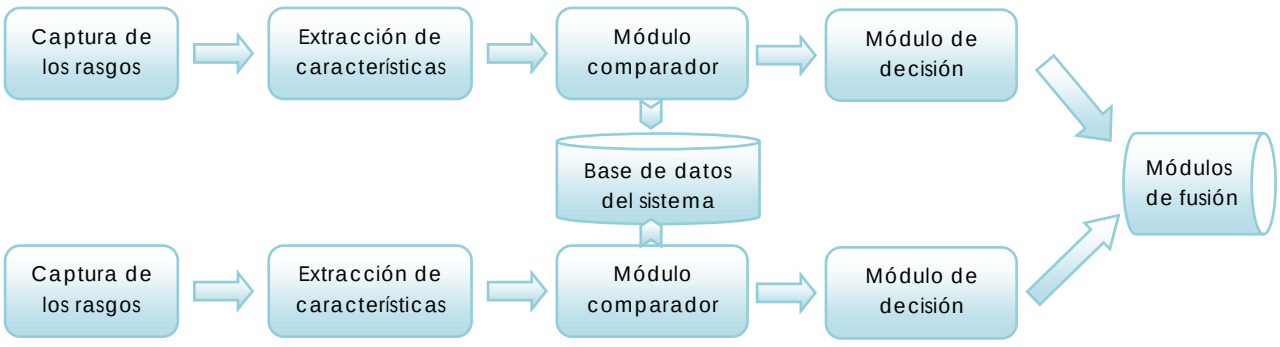


Figura 3.13: Fusión a nivel de puntuación.

- **A nivel de decisión** (Figura 3.14): a partir de las distintas decisiones de aceptado/rechazado, por ejemplo por mayoría.

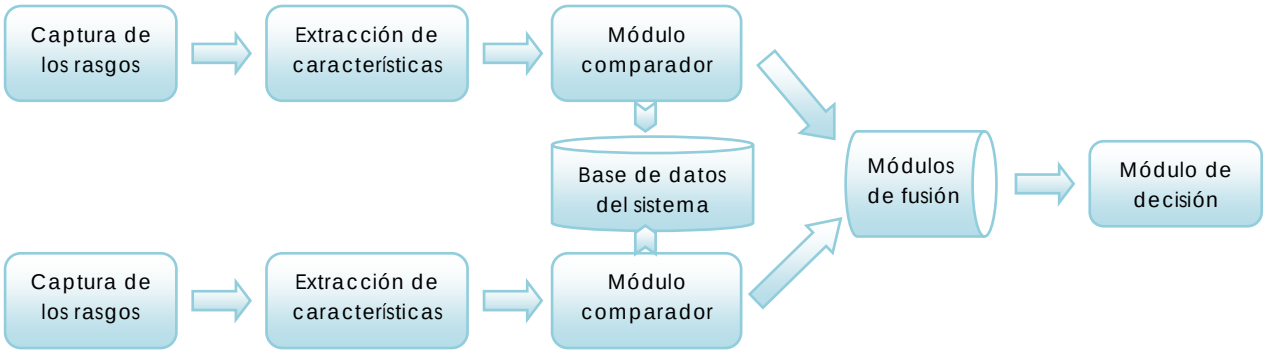


Figura 3.14: Fusión a nivel de decisión.

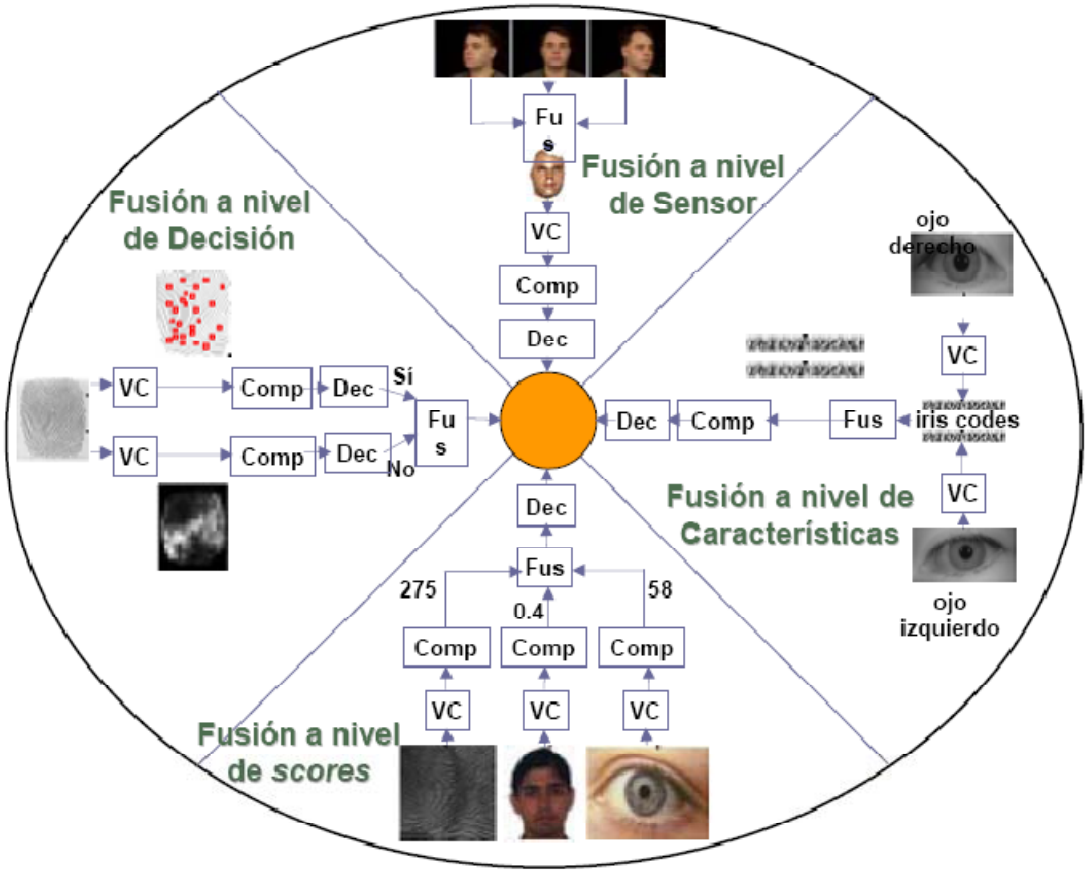


Figura 3.15: Niveles de Fusión

Los sistemas biométricos multimodales pueden trabajar en cinco posibles escenarios (ver Figura 3.16):

- **Múltiples sensores**: se combina la información obtenida de diferentes sensores para el mismo rasgo biométrico. Por ejemplo: para capturar huellas dactilares se pueden emplear sensores ópticos, sensores basados en ultrasonidos y sensores de estado sólido.
- **Múltiples rasgos**: se combinan diferentes rasgos biométricos como pueden ser la cara y la huella dactilar. Estos sistemas contendrán necesariamente más de un sensor, cada uno para un rasgo biométrico distinto. Un escenario de múltiples rasgos se emplea, en un sistema de verificación, para mejorar la exactitud del mismo, mientras que en un sistema de identificación se utiliza para mejorar la velocidad de comparación.
- **Múltiples instancias de un mismo rasgo**: permite combinar las huellas dactilares de dos o más dedos de una persona, o una imagen de cada uno de los dos iris de un sujeto.
- **Múltiples capturas de un mismo rasgo**: se emplea más de una captura del mismo rasgo biométrico. Por ejemplo: se combinan múltiples impresiones del mismo dedo, múltiples muestras de voz o múltiples imágenes de la cara.
- **Múltiples algoritmos**: implica combinar diferentes enfoques para la extracción y comparación de las características biométricas, tratando de aprovechar la mayor información posible del rasgo biométrico.

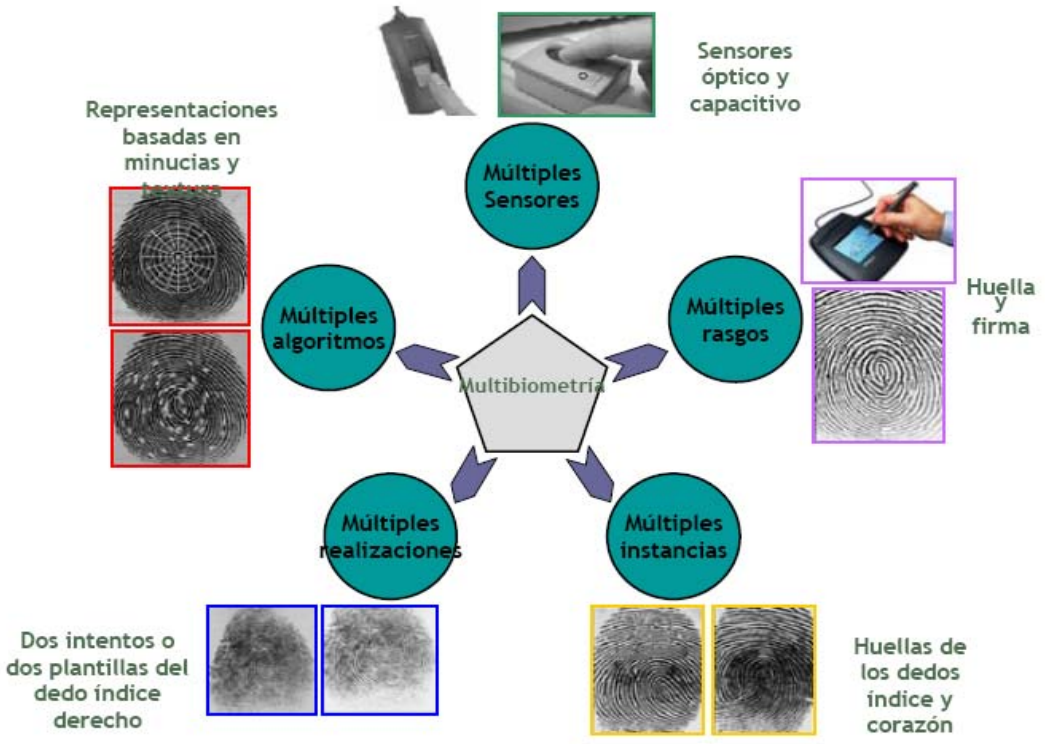


Figura 3.16: Escenarios multibiométricos.

En este Proyecto se hará uso de un sistema unimodal, ya que cuanta más información biométrica se utiliza mayor son los requerimientos de capacidad de cálculo y espacio de almacenamiento, siendo estos dos parámetros unas de las restricciones en este PFC.

4. Reconocimiento de huella dactilar. Estado del arte

Desde la antigüedad se han utilizado diferentes partes del cuerpo para identificar a las personas, prueba de ello son las evidencias arqueológicas que relacionan huellas con identidad (dibujos rupestres junto con impresión de huellas), y más formalmente en los primeros trabajos científicos del siglo XVI donde aparecen estudios de formación anatómica, caracterización del cuerpo... y, concretamente, en el ámbito de identificación en los siglos XVIII-XIX. Más adelante, durante el siglo XX, algunos rasgos biométricos como las huellas son aceptados como método de identificación y pruebas en procesos judiciales [1].

En la actualidad el reconocimiento automático de huella dactilar se ha consolidado como el rasgo biométrico más utilizado en el mercado, tanto es así que acapara casi el 50% del mismo. Esto se debe a la gran riqueza de información que podemos obtener de cada dactilograma, que son las figuras formadas por el relieve de las crestas del dedo, y gracias a los procesos de digitalización de la huella se ha facilitado enormemente el procedimiento de extracción de los puntos característicos llamados minucias. Estos puntos representan las anomalías en el normal fluir de una cresta, como vemos en la Figura 4.1, clasificándolos a grandes rasgos en dos grupos: bifurcaciones e interrupciones de crestas (fin de cresta).

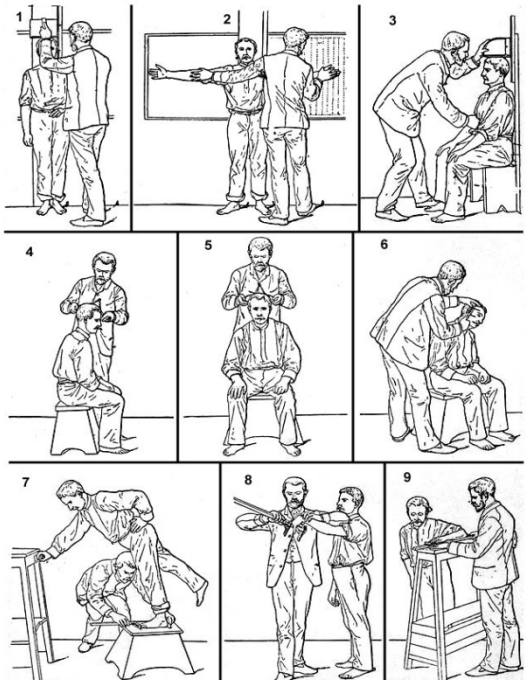
Figura 4.1: huella dactilar.

La huella dactilar pertenece al grupo de rasgos biométricos fisiológicos, y supone un modo robusto de identificación de individuos debido a la reducida variabilidad a lo largo del tiempo. Esta característica se ha venido usando como método principal para la identificación en el ámbito policial; por ejemplo: en el año 2003 el FBI contaba con 200 millones de tarjetas impresas con huellas dactilares y miles de peticiones diarias de identificación.

4.1 Historia, nacimiento y evolución

El ser humano siempre ha sentido la necesidad de "identificar o reconocer" a las personas que lo rodean. Según palabra del Dr. Oloriz, [12] "la identificación personal es el acto más frecuente y elemental de la vida social ya que cada vez que encontramos a individuos de nuestra familia o a conocidos nuestros los identificamos haciendo un cotejo mental e instantáneo entre el hermano o amigo que en carne y hueso se nos presenta y la imagen que de él llevamos estereotipada en la memoria".
De esta forma, todo nuestro sistema social tanto a nivel jurídico como a nivel comercial y personal se basa en que cada individuo tiene una identidad individual, y es capaz de probarla, evitando así que una persona pierda su identidad o que otra se adueñe de ella. Este problema ha existido desde tiempos inmemoriales, y en cada época han tratado de dar una solución al problema de la identidad. Por ejemplo: en la Francia de finales de siglo XVII y principios del XVIII se marcaba a los ladrones con la marca V (voleurs) si no eran reincidentes; si por el contrario lo eran se les enviaba a galeras y se les marcaba con las siglas G.A.L. Esta práctica duró hasta 1823. A mediados del siglo XIX se comienza a emplearse descripciones fisionómicas y demás particularidades del ser humano. Este proceso se hacía sin base científica, y dependía del observador que tomaba las medidas. Esto cambió cuando Alfonso Bertillón, (1.852-1.914), [13] un modesto empleado del Servicio de Identidad de París, presentó en el año 1879, a la Prefactura de Policía el sistema antropométrico que llevaría su nombre. Este sistema, Figura 4.2, que en 1.888 obtiene su consagración en Francia, aplicándose de forma obligatoria en todo el país se basa en 3 supuestos:

1) En la fijeza casi absoluta del sistema óseo a partir de los 20 años de edad del individuo.
2) En la extrema diversidad de la dimensiones que presenta el esqueleto de un individuo comparado con el de otro.
3) En la facilidad y relativa precisión con que se puede medir sobre el cuerpo vivo, ciertas dimensiones del esqueleto.



1) Altura
2) Envergadura
3) Tronco

4) Longitud de la cabeza
5) Anchura de la cabeza
6) Oreja derecha

7) Pie izquierdo
8) Dedo medio de la mano izquierda
9) Antebrazo izquierdo

Figura 4.2: Sistema antropométrico de Alfonso Bertillón

4.1.1 Dactiloscopia, estudio de las huellas dactilares

La dactiloscopia, al igual que la antropometría, ha sido una ciencia cuyo objetivo es el de conseguir la identificación de la persona y, concretamente, en el caso de la dactiloscopia mediante la impresión o reproducción de los dibujos formador por las crestas papilares en las yemas de los dedos de las manos.

El término dactiloscopia proviene del griego daktilos (dedo) y skopein (examinar). Y el origen de esta ciencia se remonta a los más lejanos tiempos, ya que se han encontrado representaciones palmares y dactilares de huellas humanas en pinturas rupestres en las cuevas de Altamira (España), Marsolan (Cargas) y Font-de-Gaune (Francia) entre otras, sin olvidar las impresiones dactilares halladas en vasijas y tablillas babilónicas conservadas en el Museo Británico de Londres que datan de hace más de tres mil años.

A pesar de estas primeras reseñas históricas donde se comienza a asociar la huella dactilar con la identidad del autor, el verdadero padre de la dactiloscopia fue Juan de Vucetich [14], quien partiendo de las ideas de Bertillón, clasificó las huellas dactilares bajo una relación directa entre la presencia y ausencia de deltas en las mismas. Ésto le permitió en 1.892 resolver el primer caso policial utilizando huellas dactilares (ver Figura 4.3). Una mujer de nombre Francisca Rojas asesinó a sus dos hijos. Luego se cortó la garganta, no produciéndose una herida fatal sino leve. Ésta acusó a su vecino como el autor de los hechos, pero Juan Vucetich utilizando la huella latente encontrada en el cuchillo demostró que la señora Rojas fue quien dio muerte a sus dos hijas [15]. A partir de este hecho se dio gran importancia desde el punto de vista identificativo a las huellas dactilares.

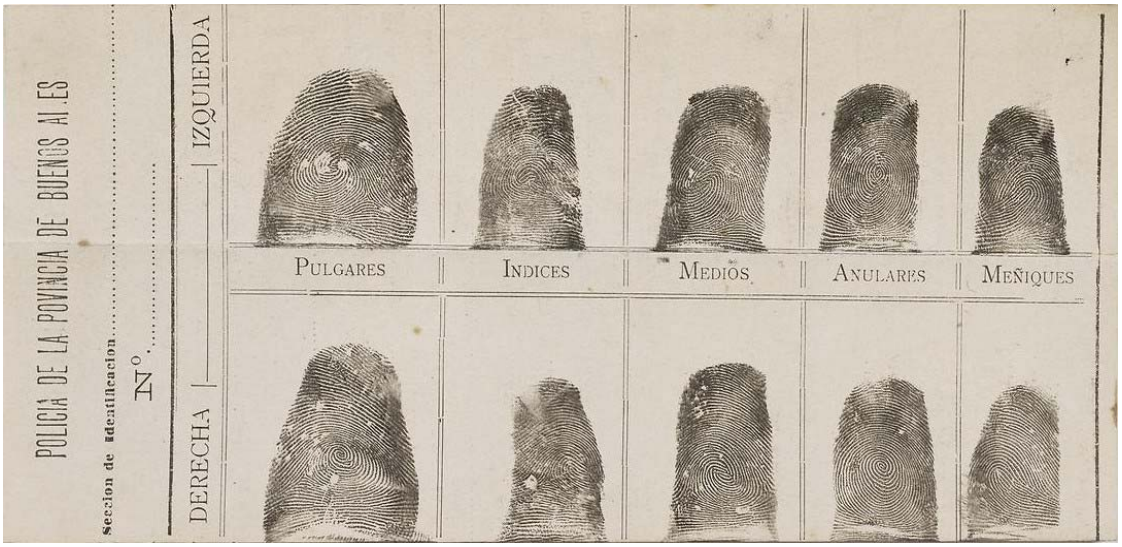


Figura 4.3: Ficha Dactiloscópica de Francisca Rojas. Imagen extraída de [15]

Durante este período, Francis Galton [16], (1.822 – 1.911) estudió los dibujos papilares de los dedos de la mano y estableció una clasificación de las "anomalías" que encontró en las formas de las crestas papilares (ver Figura 4.4). Esta clasificación de los puntos característicos fue publicada en junio de 1.900 y un año más tarde fue introducida en la policía de Scotland Yard como método fundamental en la identificación de criminales y es actualmente la base del reconocimiento basado en huella dactilar.

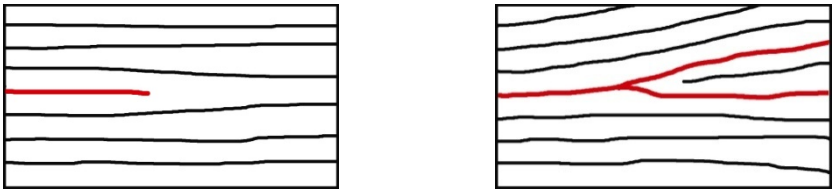


Figura 4.4: Puntos Galton o puntos característicos de las huellas dactilares. Izquierda Fin de cresta, derecha Bifurcación

Más información sobre puntos característicos de las huellas dactilares en el anexo: Puntos característicos.

4.1.2 Formación de las huellas dactilares

La piel es el mayor órgano del cuerpo humano o animal. Ocupa aproximadamente 2 m² y su espesor varía entre los 0,5 mm (en los párpados) a los 4 mm (en el talón). Su peso aproximado es de 5 kg. Actúa como barrera protectora que aísla al organismo del medio que lo rodea, protegiéndolo y contribuyendo a mantener íntegras sus estructuras.

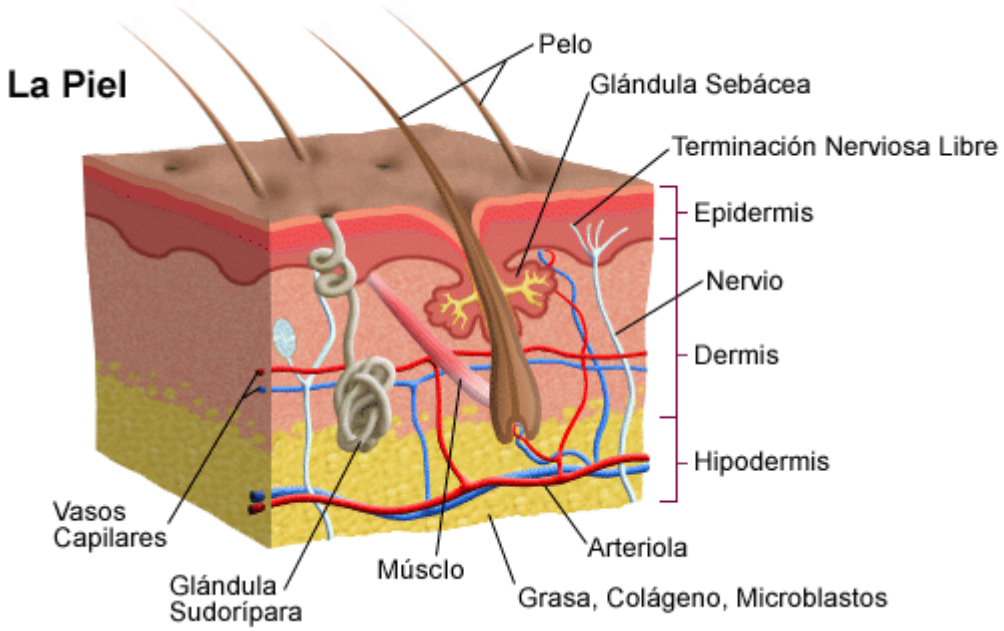


Figura 4.5: Piel humana, corte transversal.

La piel humana tiene tres capas, como podemos ver en la Figura 4.5: la hipodermis, que es más profunda; la epidermis, que es más superficial y la dermis que se encuentra entre ambas. La dermis tiene dos extractos: un extracto más interno o extracto subcutáneo; y un extracto más externo o extracto papilar formado por las papilas dérmicas. Según estén dispuestas estas papilas dérmicas así lo estarán también, pues son su origen, las crestas papilares. Las papilas dérmicas se proyectan hacia la superficie dando lugar a la formación de los relieves llamados crestas papilares. Las crestas papilares, en identificación, son los relieves epidérmicos que formando muchos dibujos aparecen visibles en la cara palmar de las manos y en la cara plantar de los pies [17]. Las crestas están separadas entre sí por unas fisuras o depresiones, llamados surcos papilares o interpapilares (ver Figura 4.6). Podríamos comparar esto con una tierra labrada donde el lomo de la tierra arada sería la cresta papilar, mientras que el surco de la tierra sería el surco papilar o interpapilar. El lomo de las cresta es redondeado y está invadido por una multitud de orificios microscópicos (poros) por donde se excreta el sudor.

El origen de las huellas está en las excreciones cutáneas (sudor y materia sebácea), que nosotros dejamos al tocar objetos, superficies... Son las huellas latentes. Éstas también están compuestas por una serie de elementos: agua en más del 99%, cloruro sódico, aminoácidos (arginina, tiroxina...), ácidos grasos y proteínas.

Características de las crestas [17]:

- Son comunes a todos los seres humanos.
- Son perennes; permanecen a lo largo de toda la vida y se forman en el sexto mes de la vida intrauterina, no desapareciendo hasta que tiene lugar la descomposición del cadáver. Si el cadáver es embalsamado duran eternamente (momias egipcias presentaban crestas papilares después de 25 siglos).
- Son inmutables; no cambian salvo accidentes. El dibujo no se modifica fisiológicamente. El recién nacido lo conserva hasta después de su muerte, creciendo al mismo ritmo que el cuerpo humano. Si sufre modificaciones accidentales que no afecten a la dermis (capa intermedia), se regeneran.
- Son diversiformes; distintas en todas las personas, no hay ninguna igual.
- Son clasificables; permiten su clasificación y formulación. Los dibujos se llaman lofogramas.

Figura 4.6: Detalle de crestas y valles de una huella palmar.

4.2 Adquisición de huellas dactilares

Una vez conocido el gran poder discriminante de las huellas dactilares, el problema que surge es, ¿cómo almacenar toda esta información de una forma eficaz? En los siglos XVIII y XIX con la explosión de la huella como sistema veraz de identificación se capturaba humedeciendo la yema de los dedos en tinta y presionando el dedo contra una tarjeta de papel [17]. Con el desarrollo de la tecnología se pasó al mundo digital y estas tarjetas fueron escaneadas para su mejor almacenamiento y consulta.

En las últimas décadas, gracias a la proliferación de sistemas de adquisición electrónicos, ha dejado de ser necesaria la adquisición con tinta. El mercado, viendo la gran demanda de sistemas de captura digitales que se ha producido, ha respondido ofreciendo un amplio catálogo de sensores capaces de capturar un dactilograma.

4.2.1 Sensores Ópticos

Los sensores ópticos son capaces de capturar imágenes. Para obtener dicha información, estos sensores cuentan con un prisma de vidrio para captar la luz que refleja el objeto, en nuestro caso la superficie del dedo. De esta manera, la parte en contacto con el prisma, las crestas de la huella dactilar, reflejarán la luz y parecerán en tonos claros en la imagen mientras que los valles absorberán la luz y aparecerán en tonos oscuros.

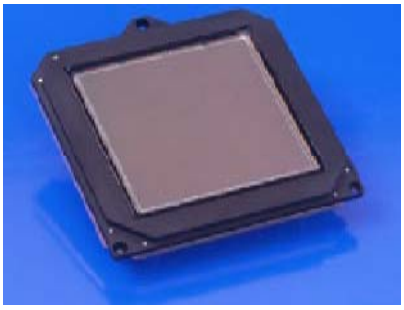


Figura 4.7: Sensor óptico Full Frame CCD

I. **FTIR (Frustrated total Internal Reflection):** Esta es la tecnología más antigua y utilizada. El dedo se coloca sobre un prisma de vidrio y se ilumina mediante una luz difusa. La diferente reflexión entre las crestas y los valles de la huella es reconocida mediante un sensor CCD, ver Figura 4.7, o CMOS que registrará la huella. Estos sensores proporcionan imágenes de buena calidad pero no pueden miniaturizarse, ya que el tamaño del prisma es crítico si no se desean grandes distorsiones en la imagen obtenida.

II. **FTIR con prisma laminar**: Este sensor busca una reducción en el tamaño del sensor FTIR clásico. Para ello se talla la superficie interna del sensor en forma de micro prismas que simulará el prisma de mayor tamaño. La calidad de las imágenes obtenidas es en general menor que en el caso no laminar.
III. **Fibra óptica**: Consiste en crear una matriz de fibras ópticas verticales con las que el dedo entrará en contacto. La luz residual emitida por el dedo es recogida por un sensor CCD/CMOS que registra la imagen. La imagen tendrá tanta resolución como número de fibras haya.
IV. **Lectura directa**: Esta técnica es la única que no requiere contacto directo con el sensor y consiste en tomar una fotografía de muy alta calidad de la huella y post-procesarla para corregir posibles distorsiones. Es la técnica menos invasiva pero resulta complicado obtener imágenes con la resolución y el contraste necesarios.

4.2.2 Sensores de estado sólido

Los sensores de estado sólido son circuitos integrados capaces de medir magnitudes físicas del entorno. Los más importantes de detallan a continuación:

I. **Capacitivos:** Este método es muy común en la actualidad. Consiste en una superficie compuesta por una matriz bidimensional de placas unidas a pequeños condensadores. La piel del dedo actúa como la segunda placa de los condensadores y dependiendo de la distancia, la capacidad variará; por lo tanto se pueden distinguir fácilmente las crestas de los valles. El principal problema de estos sensores es su mantenimiento ya que el recubrimiento del sensor ha de ser lo suficientemente fino para que sea preciso, sin ser tan delgado como para que pueda resultar fácilmente dañado. Adicionalmente, descargas electroestáticas pueden causar daños irreversibles al sensor.
II. **Térmicos**: Los sensores términos están fabricados con un material piroeléctrico. La diferencia de temperatura entre las crestas y los valles puede ser capturada fácilmente. Estos sensores son mantenidos a una temperatura relativamente alta para que esta diferencia sea aún mayor. Un factor importante a tener en cuenta es que en cuanto el equilibrio térmico se alcanza, la imagen desaparece, ya que este tipo de sensores miden variaciones de temperatura, no temperaturas absolutas. La solución más común es que la huella se adquiera mediante barrido deslizando el dedo en una dirección por la superficie del sensor, manteniendo así la variación de temperatura. Estos sensores permiten reducir el área de adquisición pudiéndose integrar en sistemas portátiles y son más resistentes a daños externos que los capacitivos.
III. **Campo eléctrico**: Esta clase de sensores tiene incorporada un anillo que genera una señal modulada por la superficie del dedo. El dedo debe estar en contacto con el anillo y el sensor para su correcto funcionamiento. La señal recibida es amplificada, integrada y digitalizada para formar la imagen.
IV. **Piezoeléctrico**: Son sensores sensibles a la presión, produciendo un campo eléctrico cuando son sometidos a fuerzas mecánicas. Las diferencias entre las presiones que ejercen las crestas y los valles puede ser aprovechada para formar la imagen. De todos modos, no se ha conseguido implementar sensores con precisión suficiente con esta tecnología.

4.2.3 Sensores de ultrasonidos

Los sensores de ultrasonidos son comparables a una ecografía. Envían señales acústicas a la superficie del dedo y captan la señal de eco recibida. Esta señal de eco permite reconstruir la forma de la huella y la estructura de crestas y valles. Una gran ventaja de este método es que es inmune a la suciedad o incluso a materiales que se interpongan entre el dedo y el sensor como por ejemplo guantes finos. Existen desventajas que hacen que este sensor no haya proliferado. La principal es su complejidad, que hace difícil integrarlo en dispositivos pequeños y su elevado precio. La adquisición de las imágenes es, además, relativamente lenta.

4.3 La huella dactilar: tipos y características

Las huellas dactilares, como ya hemos explicado anteriormente, son una parte más del desarrollo del ser humano, se consideran bien formadas y con capacidad discriminatoria a partir del sexto mes fetal. Este patrón de valles y crestas que se ha formado permanece invariable hasta la descomposición post-mortem, excepto accidentes, como cortes, quemaduras... y sin olvidar que la piel tiene una capacidad regenerativa. Estas figuras formadas por las crestas y valles, ver Figura 4.8, tienen tal variedad que resultan características de cada individuo, y por tanto las huellas dactilares resultan muy interesantes para la identificación personal.

La estructura de crestas y valles, que es capturada con cualquiera de los sensores que se acaban de explicar, generalmente se representa en las imágenes siguiendo la nomenclatura de representar las crestas con tonos más oscuros, mientras que a los valles se les asigna tonos claros. Esta forma de representar la imagen de una huella viene influenciada por los primeros sensores ópticos.

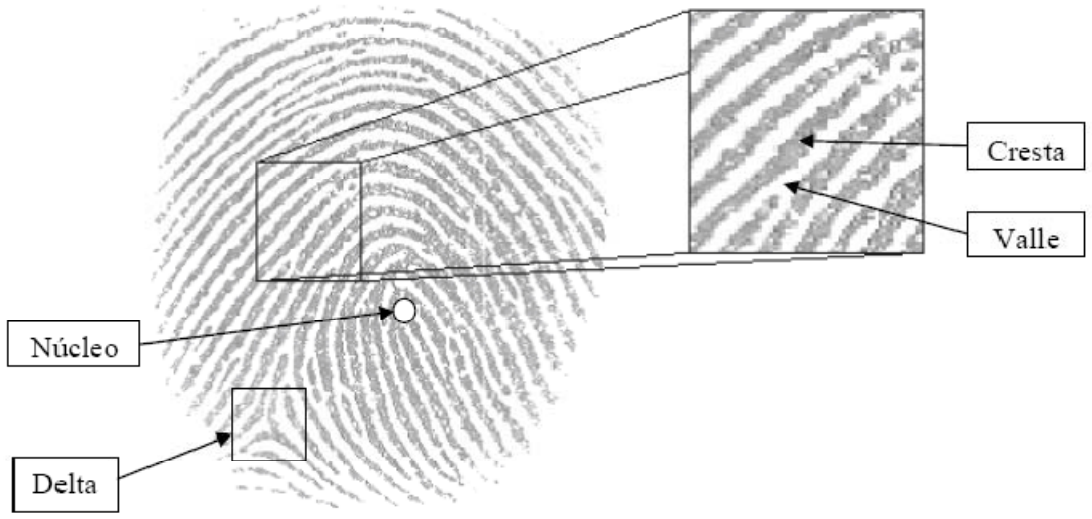


Figura 4.8: Detalle de huella dactilar: núcleo, delta, cestas y valles.

4.3.1 Clasificación de las huellas dactilares

Una primera forma de clasificar una huella dactilar puede ser fijándonos en el patrón que dibujan sus crestas y valles (ver Figura 4.9). Estas estructuras son conocidas como lazo, delta y espiral. En total, según la distribución de dichas estructuras se definen cinco clases de huellas [5]: lazo izquierdo, lazo derecho, espiral, arco y arco tensado.

Figura 4.9: Tipos de huellas en función de su patrón de crestas y valles.

Otra parte importante en el reconocimiento de huellas suele ser la localización del **núcleo** y la **delta (**ver Figura 4.10). El núcleo es [18] "el punto que se encuentra más al norte de la cresta mas interna de la huella". En la práctica puede ser interpretado como el punto central de la singularidad de lazo situada más al norte. En el caso de que no existan singularidades de lazo, como en las huellas de tipo arco, el núcleo será el punto de mayor curvatura de las crestas. La delta se corresponde con una estructura de tipo triangular, formada por tres orientaciones de crestas que divergen en un punto. Se produce por la intersección de las tres zonas de la huella dactilar (ver Figura 4.8): la zona basilar, la zona nuclear y la zona marginal.

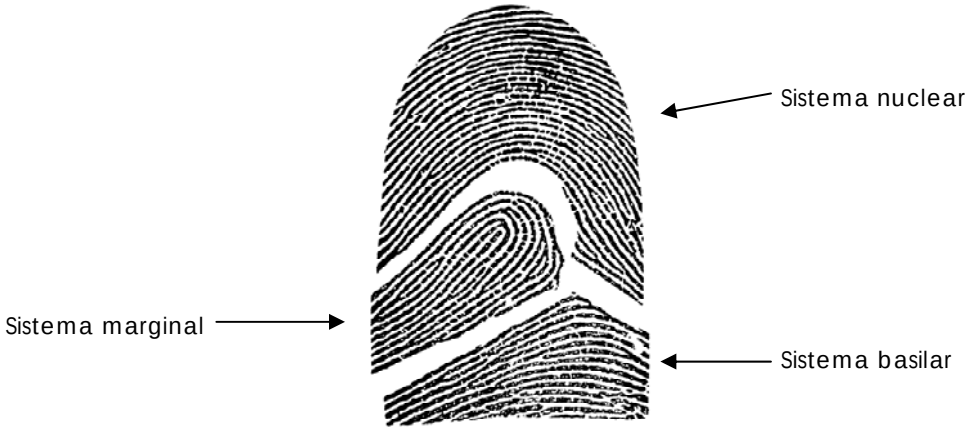


Figura 4.10: Los sistemas papilares

Pero no todas las huellas tienen una estructura bien definida y se pueden clasificar por tanto dentro de alguna de las clases expuestas. Esto se debe a que existen huellas con un aspecto intermedio entre dos o más tipos. En consecuencia, se podrán clasificar las huellas de un modo aproximado y nunca sistemático.

Por último, existe un tipo de singularidades locales en las huellas denominadas minucias (minutiae, en inglés). Una minucia, como ya se ha dicho anteriormente, es una anomalía en el normal fluir de una cresta. Estas irregularidades presentan una gran variedad entre distintos usuarios, siendo tal que el sistema judicial español fija en doce el número de minucias que deben coincidir en tipo, posición y ángulo para asegurar que dos huellas pertenezcan inequívocamente a la misma persona. Existen cientos de tipos de minucias (ver anexo Puntos característicos), aunque todos ellos se pueden resumir en dos: **bifurcaciones** y **terminaciones**. Cada minucia se caracteriza por su coordenadas x e y, su ángulo θ que forma la recta tangente a la cresta con el eje horizontal y en ocasiones, un parámetro Q que indica la calidad de la minucia.

4.4 Extracción de características

Uno de los puntos claves en cualquier proceso de reconocimiento es el correcto tratamiento de la información biométrica, para poder extraer las características que nos permitirán modelar y comparar con el resto de plantillas biométricas con el fin de reconocer al individuo.

4.4.1 Obtención de la orientación local y frecuencia de las crestas

La orientación local de las crestas es el ángulo que forman con el eje horizontal (ver Figura 4.11 izquierda). El método aparentemente más sencillo de calcular su orientación es mediante el gradiente. Para ello se debe realizar una convolución de la imagen con la máscara de operador gradiente para hallar ∇_x y ∇_y y calcular posteriormente el arco tangente ∇_x/∇_y. El mayor inconveniente de esta técnica es la discontinuidad del arco tangente y su sensibilidad frente al ruido.

Se han propuesto técnicas más robustas empleando medias locales de gradientes y estimaciones del gradiente. La imagen de orientación local se obtiene representando la orientación dominante de las crestas en una matriz de bloques cuyo tamaño se corresponde al de la máscara utilizada para determinar el gradiente o su equivalente.

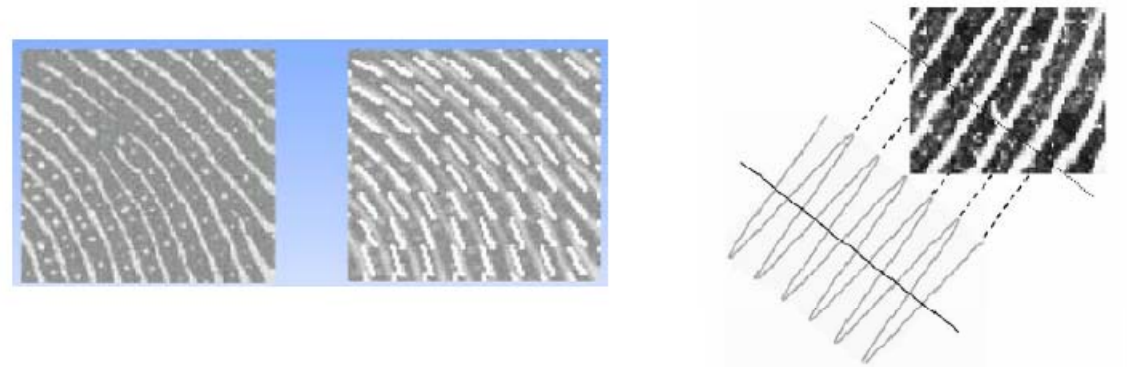


Figura 4.11: Izquierda: orientación de las crestas; derecha: frecuencia espacial de las cresta

La frecuencia de las crestas es la inversa del número de crestas que cortan un segmento de una unidad de longitud perpendicular a su dirección (ver Figura 4.11 derecha). Para su determinación hay diversos métodos: contar el número de píxeles de cada intensidad de gris entre las crestas; modelado de las crestas como un patrón sinusoidal o empleando la transformada de Fourier por bloques.

4.4.2 Segmentación

La segmentación en una huella dactilar, consiste en separar el área que contiene información de la huella del fondo de la imagen (ver Figura 4.12). No se suelen emplear técnicas que dependan de la intensidad de los píxeles, pues el fondo suele ser ruidoso, sino que se busca separar zonas con regiones estriadas (crestas y valles) de zonas sin variaciones predominantes, isotrópicas.

Figura 4.12: Segmentación de la zona de interés de una huella dactilar.

4.4.3 Detección de singularidades

La mayoría de los métodos para detectar singularidades (núcleos y deltas) emplean la imagen resultante de calcular la orientación local de las crestas. El índice de Poincaré [19] es el método más empleado, definiéndose caminos cerrados por una secuencia de bloques de la imagen de orientación.

El índice de Poincaré $P_{G,C}(i,j)$ se calcula sumando las diferencias de orientación entre elementos adyacentes del camino. Como no se conoce el sentido, sólo la dirección, se asigna uno aleatoriamente al primer bloque y a los siguientes se les asigna aquel que sea más parecido al anterior.

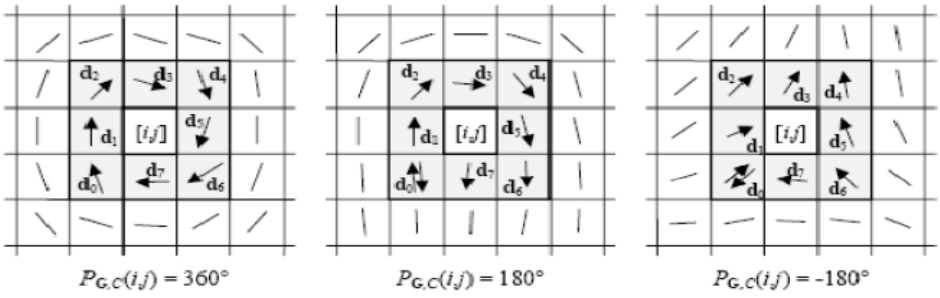


Figura 4.13: Ejemplos de cálculo del índice de Poincaré. Imagen extraída de [20].

En función del valor de índice de Poincaré, se puede determinar la singularidad que encierra el camino elegido (ver Figura 4.13).

- $P_{G,C}(i,j) = 0°$ si no existe ninguna singularidad.
- $P_{G,C}(i,j) = 360°$ si la singularidad es una espiral.
- $P_{G,C}(i,j) = 180°$ si la singularidad es un lazo.
- $P_{G,C}(i,j) = -180°$ si la singularidad es una delta.

4.4.4 Mejora y binarización

La mejora de las imágenes obtenidas mediante los sensores pretende aumentar el contraste entre crestas y valles a fin de facilitar la extracción de minucias y descartar zonas demasiado ruidosas o de baja calidad.

Las técnicas clásicas para esta tarea no son suficientes para lograr resultados satisfactorios con huellas dactilares. Por eso se emplean filtros contextuales, es decir, en vez de emplear un único filtro para toda la imagen se emplea un filtro diferente en función de la zona que se esté filtrando.

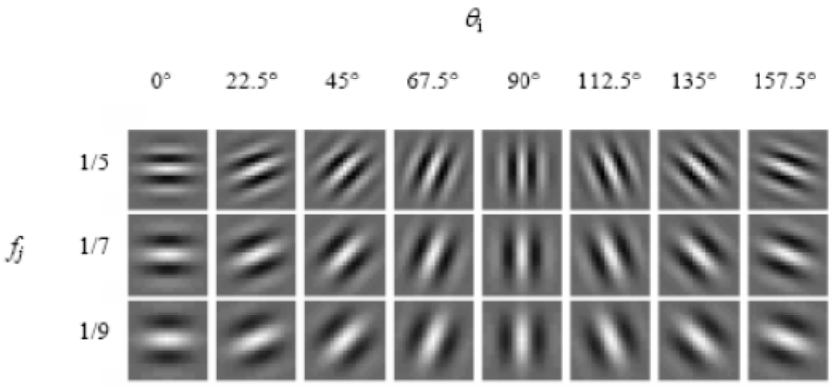


Figura 4.14: Representación gráfica de 24 filtros de Gabor. Imagen extraída de [20].

Estos filtros que se emplean tienen una estructura sinusoidal con diferentes frecuencias y orientaciones. Una clase de filtros muy extendida en el ámbito de la mejora de las huellas dactilares son los filtros de Gabor [20]. En la Figura 4.14 se muestra un conjunto de filtros de Gabor de diferentes frecuencias empleados en la actualidad para la mejora de imágenes de huella dactilar.

Figura 4.15: Binarización de una huella.

Una vez mejorada la imagen, se puede binarizar, es decir, convertir sus píxeles en blanco o negro puro exclusivamente, ver Figura 4.15, estableciendo un umbral de binarización. Muchos de los algoritmos utilizados para la mejora de las imágenes producen la imagen ya binarizada.

4.4.5 Extracción de minucias

Los métodos de extracción de minucias suelen requerir una imagen de la huella dactilar ya binarizada. Es frecuente realizar un proceso de afinado de las crestas para reducir su grosor hasta un píxel de tal modo que se facilite su procesado.

Posteriormente, las minucias se extraen seleccionando todos los puntos en los que se produce una terminación o bifurcación de una cresta (ver Figura 4.16).

Algunos autores han propuesto no utilizar binarización ya que es posible que se pierda una gran cantidad de información en ese proceso. La binarización es además un proceso complejo y lento que puede introducir minucias no existentes. Si la imagen de la huella no es suficiente calidad, la binarización arrojará resultados desastrosos. En [21] se ilustra un método de extracción de minucias sobre la imagen directamente en escala de grises.

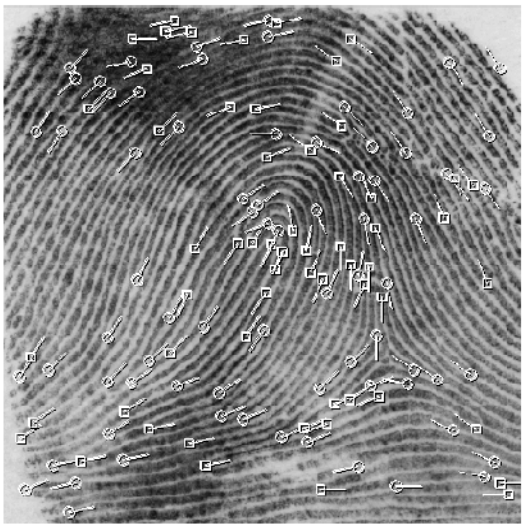


Figura 4.16: Extracción de minucias; bifurcaciones (cuadrados) y fin de crestas (círculos)

En general suele existir una etapa de post-procesado para eliminar minucias espurias, resultado de las fases anteriores de mejora y binarización. En esta etapa de procesado se pueden eliminar minucias que se hayan localizado en zonas de baja calidad o minucias que se encuentren demasiado próximas.

4.5 Comparación de huellas

La comparación o matching de huellas es una de las fases más críticas en un sistema de verificación de huella dactilar. Comparar dos huellas puede ser un proceso muy complejo ya que en general las dos huellas a comparar habrán sufrido desplazamientos, rotaciones, distorsiones o quizá su calidad pueda ser baja. Por lo tanto, un buen algoritmo de comparación deberá ser robusto frente a la variabilidad en las huellas a comparar.

Las principales dificultades ante las que debe actuar un algoritmo de comparación son las siguientes:

- ***Desplazamiento y rotación***: son el resultado de que el usuario sitúe su dedo en un lugar diferente del sensor en cada ocasión. Pueden ocasionar que una parte de la huella se encuentre fuera del área de captura, por lo que las huellas a comparar tendrán un área menor en común a la real. Este problema afecta en gran medida a los sensores con una reducida área de captura.
- ***Distorsión no lineal***: es la consecuencia de plasmar en una imagen de dos dimensiones una huella dactilar de 3 dimensiones, con una elasticidad que provoca deformaciones no lineales en su superficie.
- ***Diferencias de presión y de las condiciones de la piel***: la presión que se ejerza contra el sensor y la humedad o sequedad de la piel hacen que la captura sea diferente en cada situación. También afectan sustancias corporales como el sudor o la grasa.
- ***Errores en la extracción de características***: los algoritmos de extracción de minucias tienden a producir minucias espurias en las huellas de baja calidad que enmascaran a menudo minucias reales.

Figura 4.17: Dos realizaciones de la misma huella en instantes diferentes.

En la Figura 4.17 se observan dos impresiones de la misma huella de un usurario tomadas en condiciones diferentes procedentes de la base de datos [22].

Existen en la literatura un gran número de algoritmos automáticos de comparación o *matching* para huellas dactilares [1]. La mayor parte de ellos presentan un buen rendimiento cuando las huellas dactilares que se les presentan son de buena calidad, sin embargo, conseguir discernir entre huellas de baja calidad o entre huellas dactilares incompletas sigue siendo un foco de interés científico. Una muestra clara de ello son las competiciones internacionales celebradas periódicamente con el fin de evaluar el rendimiento de los sistemas que son propuestos en la actualidad, como las competiciones FVC (*Fingerprint Verification Competition)* [23]. Los algoritmos de reconocimiento desarrollados hasta la fecha pueden clasificarse en tres grandes grupos:

- ***Basados en correlación, normalmente a nivel de bloque***: las imágenes del par de huellas a comparar se superponen y se calcula la correlación entre píxeles equivalentes para diferentes alineaciones (variaciones en la posición y el ángulo).
- ***Basados en minucias***: se trata de la técnica más extendida al sustentar la comparación manual de huellas por parte de los expertos forenses en la materia. Las minucias se extraen de ambas huellas y se almacenan en vectores como conjuntos de puntos en el plano bidimensional de la imagen. Estos algoritmos tratan de hallar la alineación óptima para conseguir el mayor número posible de coincidencias entre pares de minucias de la huella de referencia y la huella a comparar.
- ***Basados en características del patrón de crestas o en texturas:*** en imágenes de baja calidad la extracción de las minucias es bastante complicada y poco fiable mientras que otras características (orientación local, forma de las crestas, información de las texturas), en general menos distintivas, pueden obtenerse de manera más robusta. Los algoritmos pertenecientes a esta familia comparan las huellas en términos de las características antes mencionadas extraídas del patrón de crestas.

Existen además otras aproximaciones al problema basadas en redes neuronales o aquellas que utilizan procesadores en paralelo o algún tipo de arquitectura dedicada.

4.5.1 Técnicas basadas en correlación

Esta clase de métodos se basa en el cálculo de la correlación cruzada entre la imagen de muestra y la de entrada tratando de maximizarla. Si se define $\boldsymbol{T}^{(\Delta x,\Delta y,\theta)}$ como la rotación de la imagen de Test $\boldsymbol{T}$ en un ángulo $\boldsymbol{\theta}$ y desplazada $(\Delta \boldsymbol{x}, \Delta \boldsymbol{y})$ píxeles, la similitud entre la imagen de la huella de la base de datos o *Registrada* $\boldsymbol{R}$ y $\boldsymbol{T}$ se puede medir calculando:

$$S(R,T) = \max_{\Delta x,\Delta y,\theta} \mathrm{R}_{R,T}\,(R, T^{\Delta x,\Delta y,\theta})$$

Donde $\mathbf{R}_{R,T}$ es la correlación cruzada entre las imágenes R e T ya binarizadas de las huellas a comparar. Cuanto mayor sea la correlación mayor será la similitud entre las huellas a comparar y su maximización permitirá calcular el valor del desplazamiento y la rotación que hacen que las dos imágenes sean lo más parecidas posibles.

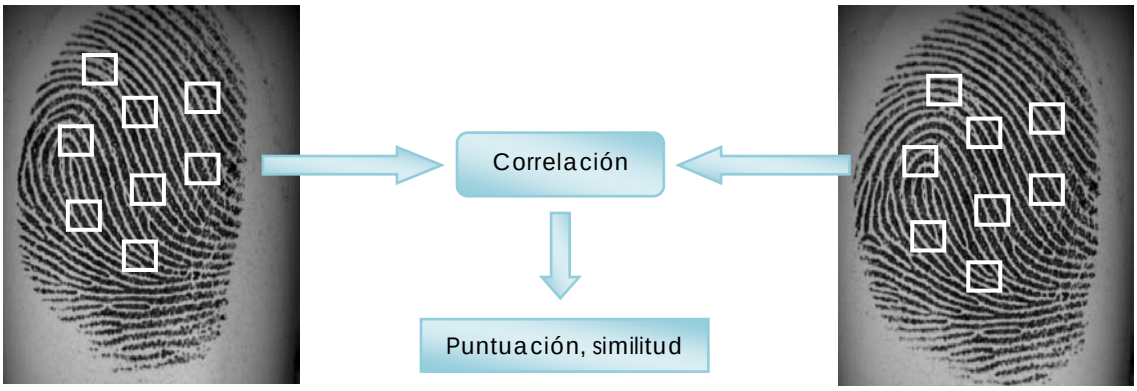


Figura 4.18: Correlación local entre huellas.

A pesar de su aparente simplicidad este algoritmo tiene un coste computacional muy elevado y es vulnerable a distorsiones no lineales en la imagen de la huella, muy frecuentes dada la elasticidad de la piel. Tomemos como ejemplo una imagen de 400 × 400 píxeles. Si se contemplan desplazamientos en el eje vertical y horizontal de ±200 píxeles y se miden rotaciones en un margen de ±30º con paso de 1º, sería necesario realizar 401×401×61 correlaciones cruzadas, dando lugar a aproximadamente 1.569.000.000 operaciones.
Se han desarrollado algoritmos que consiguen disminuir considerablemente el coste computacional mediante el cálculo de la correlación de forma local en lugares estratégicos de la huella (en el núcleo o cerca de minucias de buena calidad), en vez de globalmente (ver Figura 4.18). De todas formas ninguno de estos métodos asegura una mejora drástica de los resultados proporcionados por el método general.

Los algoritmos de correlación por bloques son un foco de interés en la actualidad al reducir el coste computacional necesario con respecto a la correlación global.

4.5.2 Técnicas basadas en minucias

Los métodos basados en minucias son los más conocidos y de uso más extendido en la actualidad. Están basados directamente en la forma en que los expertos forenses realizan la comparación entre huellas.

A diferencia de las técnicas basadas en correlación, donde la representación de la huella coincide con la imagen de la misma, en este caso la representación es un vector de características de longitud variable cuyos elementos son las minucias de la huella. Cada minucia se puede describir a partir de un número de atributos como su posición en la imagen, su orientación, tipo (final de cresta o bifurcación de cresta), un peso basado en la calidad de la imagen en su vecindad, etc. La mayor parte de los algoritmos basados en minucias consideran cada singularidad como una tupla (x, y, θ, Q) indicando las coordenadas espaciales, orientación y calidad de la minucia.

Las minucias de las huellas se almacenan con el siguiente formato:

$$R = \{m_{R1}, m_{R2}, \dots, m_{Rm}\}, \qquad m_{Ri} = \{x_{Ri}, y_{Ri}, \theta_{Ri}, Q_{Ri}\}, \qquad i = 1, \dots, m$$

$$T = \{m_{T1}, m_{T2}, \dots, m_{Tn}\}, \qquad m_{Tj} = \{x_{Tj}, y_{Tj}, \theta_{Tj}\, Q_{Tj}\}, \qquad j = 1, \dots, n$$

donde m y n son el número de minucias dentro de las huellas R (Registrada) e T (huella a verificar) respectivamente.

Dos minucias se consideran correspondientes si la distancia euclidea d_e y la diferencia en sus direcciones d_θ son menores a una cierta tolerancia d_2 y θ_2 respectivamente:

$$d_e(m'_j, m_i) = \sqrt{(x'_j - x_i) + (y'_j - y_i)} \leq d_2$$

$$d_\theta(m'_j, m_i) = \min(|\theta'_j - \theta_i|, 360° - |\theta'_j - \theta_i|) \leq \theta_2$$

Las tolerancias compensan las posibles deformaciones entre las huellas a comparar y los posibles errores a nivel de píxel en los logaritmos de extracción de minucias.

Por consiguiente, la alineación previa de las huellas es absolutamente necesaria para poder realizar las comparaciones hasta ahora presentadas. Será necesario desplazar y rotar una de las dos imágenes e incluso realizar algunas transformaciones no lineales para que las minucias correspondientes se encuentren lo más próximas posible.

Para realizar una alineación correcta se debe efectuar una exploración de posición (desplazar una huella sobre la otra en pasos verticales y horizontales de un determinado tamaño) y de rotación (girar una huella sobre otra hasta maximizar el número de correspondencias), ver Figura 4.19. Pueden considerarse otro tipo de transformaciones geométricas como el escalado o la aceptación de distorsiones no lineales, siempre teniendo en cuenta que cuantas más transformaciones se toleren más grados de libertad se están considerando y por tanto el cálculo de la alineación requerirá un mayor coste computacional.

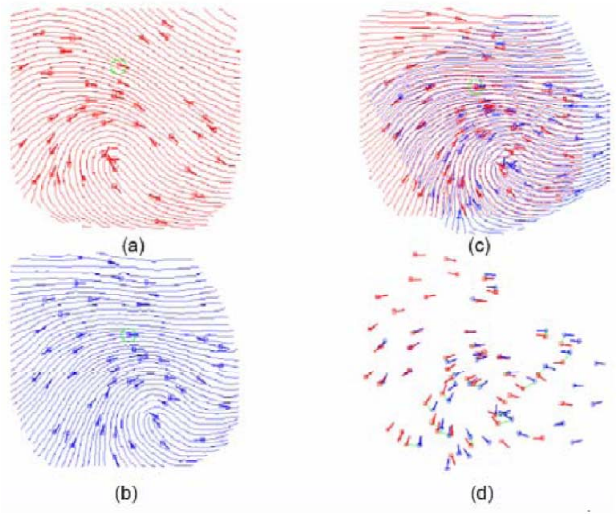


Figura 4.19: Comparación de huellas basada en minucias. (a) y (b) huellas a comparar, (c) alineación entre huellas y (d) detección de minucias coincidentes.

Realizar la alineación de las huellas dentro del propio algoritmo de *matching* da lugar a algoritmos muy robustos pero de mucho gasto computacional y en consecuencia, bastante lentos. Se han documentado técnicas que aceleran el proceso realizando una prealineación y guardando en las bases de datos sólo huellas dactilares ya alineadas, de forma que el algoritmo de *matching* únicamente tiene que calcular el número de minucias coincidentes. Existen dos aproximaciones básicas al problema de prealineación:

- ***Absoluto***: cada huella dactilar es prealineada, de forma independiente al resto, antes de ser almacenada en la base de datos. La técnica de prealineación más extendida es la que reubica la imagen en función del núcleo de la huella, aunque no es del todo fiable puesto que la detección del núcleo de la huella con nivel excesivo de ruido o con patrones tipo arco es complicado y poco preciso. El prealineación en cuanto al ángulo es aún más complejo y aún no se ha logrado una manera fiable de conseguirlo. La huella de entrada sólo será alineada una vez y puede ser comparada con las huellas de la base de datos directamente al encontrarse éstas ya prealineadas.
- ***Relativo***: la huella de entrada se prealinea con respecto a cada una de las huellas de la muestra con las que va a ser comparada. Consigue una mayor velocidad que los algoritmos de *matching* que no realizan ningún tipo de prealineación, (ya que éstos deberán realizar la alineación), aunque su eficiencia es sensiblemente menor que la del prealineación absoluto. En cuanto a su precisión es mayor que la del método absoluto pero inferior a las de las técnicas con la alineación incluida en el algoritmo de *matching*.

La alineación de las huellas conlleva gran consumo de recursos. En consecuencia, varios autores [1, 24] han propuesto métodos locales de *matching* de minucias. Estas técnicas consisten en comparar las huellas dactilares de acuerdo a estructuras locales de minucias; las estructuras locales están caracterizadas por atributos invariables con respecto a transformaciones globales (traslación, rotación…) y por tanto, sirven para realizar la correspondencia entre huellas sin necesidad de prealineación. Los algoritmos locales relajan las dependencias espaciales y por tanto reducen la información disponible para discriminar entre las huellas, lo que resulta de menor precisión que aquellos que operan con características globales.

En general a la hora de diseñar un algoritmo hay que alcanzar un compromiso entre la utilización de características globales (mayor complejidad pero mayor poder discriminativo) y el uso de características locales (mayor simplicidad y velocidad pero menor capacidad de diferenciación entre huellas)

4.5.3 Técnicas basadas en patrones de crestas o texturas

A pesar de que las técnicas basadas en minucias están hoy en día muy extendidas, se han buscado otros métodos eficientes para comparar huellas sin emplear minucias. Los motivos de esta proliferación son:

1. Es complicado extraer de forma fiable las minucias de una huella de baja calidad.

2. El tiempo de extracción de minucias es alto y requiere una capacidad de computación moderadamente elevada.
3. Pueden conseguirse características que utilizadas junto con las minucias mejoren las prestaciones de las técnicas basadas exclusivamente en dichas minucias.

Los rasgos alternativos a las minucias comúnmente utilizados son:

- Tamaño de la huella y forma de la silueta externa de la misma (en general muy inestable)
- Número, tipo y posición de las singularidades (poco fiable)
- Relación espacial y atributos geométricos de las líneas de crestas.
- Características relativas a la forma.
- Poros de la piel. Poseen un alto grado discriminativo pero su detección requiere sensores de alta resolución con elevado coste.
- Información de texturas global y local. Esta es una alternativa importante a los métodos basados en minucias y en estado de investigación. Las texturas se definen por la repetición espacial de elementos básicos, y se caracterizan por propiedades como la escala, orientación, frecuencia, simetría, etc.

Las líneas de crestas quedan caracterizadas por su orientación y frecuencia excepto en las regiones singulares, que son discontinuidades en un patrón regular básico e incluyen bucles y deltas a un nivel de resolución bajo y las minucias en una resolución alta.

En [1] se describe una técnica basada en texturas locales en la que el área de la huella se subdivide en zonas respecto al núcleo de la huella. Se calcula un vector de características basado en la información de cada zona resultante de la subdivisión.

La información local se descompone en canales empleando los filtros de Gabor. En concreto se emplearon 8 canales y un total de 80 zonas dando lugar a un vector de 640 características denominado *FingerCode*. Los elementos de cada vector se calculan hallando la desviación media absoluta (AAD, *Absolute Average Deviation*) con respecto a la media de las respuestas de cada filtro sobre píxeles de la celda. La figura 4.20 muestra gráficamente las fases del procesado de la imagen de huella dactilar que realiza el sistema propuesto en [1].

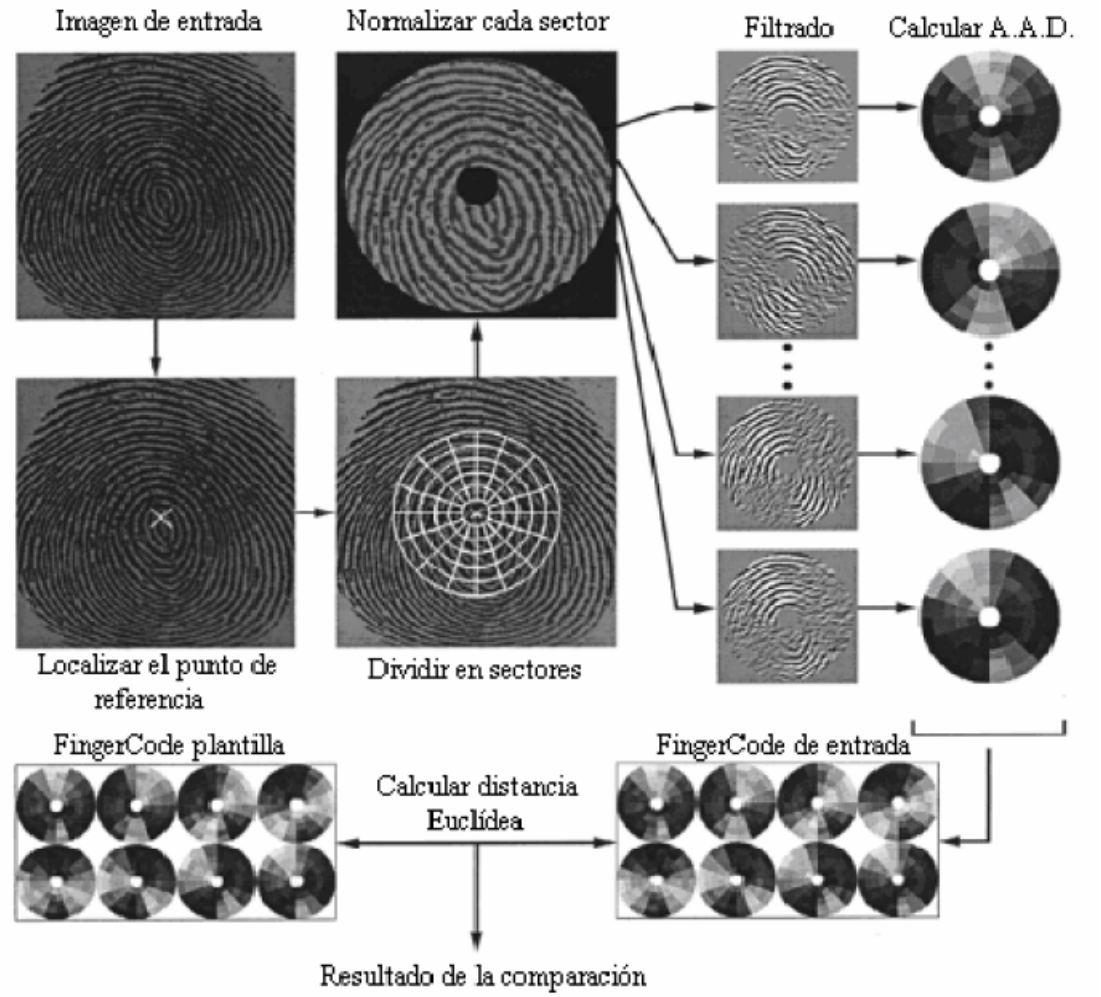


Figura 4.20: Diagrama del sistema propuesto por Jain *et al*.

4.5.4 Influencia de la calidad en el rendimiento de las técnicas de *matching*

Un factor determinante en la comparación de dos o más huellas es la calidad de las imágenes tras su captura. Existen diversos métodos para caracterizar la calidad de una imagen de huella dactilar [25]. Estos métodos adoptan tres enfoques diferentes: unos utilizan características globales de la imagen, otros características locales y por último, los basados en clasificadores, que determinan la calidad de una imagen en función de la separación y las distribuciones de puntuaciones de usuario e impostor para cada huella.

Se ha comprobado que las técnicas de comparación basadas en texturas son en general más robustas [26] en los casos en los que la calidad de la huella de la base de datos o la huella a comparar sean bajas. En cambio, las técnicas basadas en minucias suelen tener un rendimiento mejor en casos de alta calidad. Por lo tanto, una posible solución es la de emplear sistemas de identificación que utilicen diferentes técnicas de comparación y combinar sus puntuaciones de salida de tal manera que se puedan

aprovechar las ventajas que cada técnica ofrece. En [27] se desarrolla este caso y se documenta una notable mejoría en el rendimiento en la verificación de huellas dactilares.

4.6 Match-on-Card

La mayoría de los sistemas biométricos hoy en uso operan en torno a una base de datos. Tanto si se trata de una base de datos a gran escala como US-VISIT o un pequeño banco de información biométrica almacenado en un servidor para un acceso en una oficina, las soluciones se basan en redes que son potencialmente vulnerables a ataques. La tecnología Match-on-Card elimina la necesidad de la base de datos al almacenar y procesar la información biométrica directamente en una tarjeta inteligente (smartcard), ver Figura 4.21, proporcionando un entorno biométrico seguro, aumentando la privacidad, flexibilidad y escalabilidad del sistema [2].

Figura 4.21: Tarjeta inteligente (smartcard)

A lo largo de los años la biometría ha demostrado ser un útil sustituto de PINs y claves con independencia del mercado, la tecnología de la tarjeta o la aplicación.
La ventaja de usar sistemas biométricos incluye la seguridad, velocidad y aceptación por parte del usuario. Sin embargo, los sistemas biométricos han sido largamente cuestionados en lo que concierne a la privacidad y la seguridad.

La tecnología Match-on-Card permite mejorar la privacidad de los sistemas biométricos. Además lleva la seguridad biométrica y la comodidad un paso más lejos al realizar la comparación de huellas dactilares en un entorno controlado como es una tarjeta inteligente. Esto minimiza el riesgo que entraña una comparación de huellas dactilares en un aparato conectado a la red, un servidor externo, o una base de datos, normalmente considerados eslabones débiles de la cadena de seguridad. Ejemplos de aplicaciones típicas de la tecnología Match-on-Card son los documentos de identificación nacional (Figura 4.22) y los documentos de viaje (pasaportes)

Figura 4.22: Documento Nacional de Identidad español.

4.6.1 Ventajas

- **Seguridad**

La plantilla o modelo de huella dactilar biométrica debe guardarse de forma segura en un entorno cerrado. Si el procedimiento de comparación biométrica se realiza fuera de la tarjeta se expone a un entorno abierto, donde cualquiera podría robar la plantilla o modelo de huella dactilar [2]. La única manera de garantizar la seguridad del sistema es guardar el modelo de huella siempre dentro de la tarjeta.

En este caso la comparación biométrica también tiene que tener lugar en un entorno cerrado.

- **Privacidad**

Con Match-on-Card el propietario de la tarjeta inteligente controla la única grabación de su plantilla biométrica. No hay ninguna necesidad de una base de datos externa, lo cual es bueno desde dos perspectivas: los propietarios de la tarjeta inteligente pueden disfrutar la privacidad al no facilitar información biométrica y los emisores no tienen que preocuparse de la actualización y mantenimiento de las bases de datos [2].

Incluso si una tarjeta inteligente es robada o se pierde, el modelo de huella dactilar biométrico no puede ser extraído fácilmente. Está guardado de forma segura en la tarjeta.

- **Coherencia**

Cuando el modelo de huella dactilar biométrico se lleva fuera de la tarjeta el procedimiento de comparación de huellas o el umbral de la comparación puede ser cambiado sin conocimiento o consentimiento del propietario de la tarjeta. Por tanto el uso de la tecnología MoC nos permite certificar que el proceso de reconocimiento se realiza de forma correcta e integra dentro de la tarjeta donde no puede ser manipulado y alterado [2].

- **Graduación**

En contraste con un sistema basado en un servidor, no hay limitación al número de posibles usuarios cuando se utiliza la tecnología Match-on-Card. El proceso de verificación de huellas dactilares se realiza localmente en la tarjeta inteligente sin ninguna necesidad de recursos tales como redes o procesos de servidor [2]. Match-on-Card crea una base de datos altamente escalable y distribuida entre cada usuario, de forma que permite abordar proyectos con grandes bases de datos biométricos en los que el coste y mantenimientos de servidores con semejantes volúmenes de información resultaría poco práctico, caro y vulnerable.

- **Integración**

Como cualquier programa que se ejecuta en un procesador, el algoritmo de reconocimiento que se integra dentro de las tarjeta Match-on-Card requiere un mínimo espacio para el código, a pesar de que éste se diseñe utilizando bibliotecas como Java-card o MULTOS (que optimizan el rendimiento del algoritmo en términos de espacio de almacenamiento y velocidad de ejecución). En cualquier caso, cada modelo de huella dactilar almacenada en la tarjeta, requiere un espacio de memoria adicional. El tamaño del modelo de huella dactilar depende de cómo esté configurado el algoritmo y varía entre 150 y 1000 bytes para cada modelo de huella dactilar. La pequeña memoria requerida para almacenar la huella y el algoritmo hacen posible que la mayoría de las tarjetas inteligentes puedan soportar estos servicios [2].

La implementación de sistemas biométricos sobre tarjeta Match-on-Card no interfiere con otras aplicaciones de la tarjeta tales como aplicaciones de banca (banda magnética) o aplicaciones de identificación (tarjetas acreditativas). De hecho, estas otras aplicaciones tienen la posibilidad de beneficiarse del funcionamiento de las tarjetas biométricas, ya que pueden utilizar los procesos de verificación que ofrece la biometría en combinación con el uso de una tarjeta, y de esta manera dar un valor añadido a cada proceso que realicen, como por ejemplo: una autentificación a la hora de realizar una operación financiera en un cajero automático.

4.6.2 Inconvenientes

Los sistemas biométricos se pueden dividir en un mecanismo de captura, un algoritmo y un procesador que ejecute dicho algoritmo. En un sistema biométrico tradicional, el procesador no tiene límites y el desafío para el algoritmo es el rendimiento, la velocidad y la efectividad cuando tiene que procesar enormes cantidades de datos biométricos. Para una ejecución Match-on-Card los retos son diferentes [2], el procesador es en este caso el diminuto microprocesador de la tarjeta inteligente y el algoritmo tiene que consumir el menor número de recursos posibles y ofrece el nivel de seguridad y velocidad que se necesitan para la aplicación y para un uso práctico. Se debería recalcar, una vez más, que la definición Match-on-Card se aplica cuando la comparación de los datos de referencia frente a los pendientes de verificar se realizan en el interior de la tarjeta inteligente, no cuando la tarjeta es sólo utilizada para almacenar los datos de referencia (la plantilla o el modelo de huella dactilar) y transferirlos al ordenador que ejecute la comparación de los modelos. A este caso lo denominaremos como tarjeta de plantilla (Template-on-Card).

Para entender el reto que supone una tarjeta inteligente, uno necesita examinar brevemente cómo están compuestas dichas tarjetas y cómo afecta esto al rendimiento de un sistema biométrico. El "corazón" de la tarjeta inteligente, Figura 4.23, actualmente lo forma un procesador de 8 bits y las gamas más altas tienen uno de 32 bits. Para almacenar datos en la tarjeta hay diferentes memorias: la ROM (memoria sólo de lectura) contiene el sistema operativo y podría también contener el mecanismo de comparación biométrico, el contenido de la ROM se inserta durante el periodo de fabricación de la tarjeta; La EEPROM (memoria solamente de lectura eléctricamente borrable y programable) es la memoria disponible para poder ejecutar el algoritmo, es también donde el código de comparación de huellas biométrico, así como el modelo de huella dactilar, la plantilla, es almacenado. Los modelos de las memorias EEPROM van desde 8KB a 128KB (y en un futuro cercano alcanzarán los 512KB).

Figura 4.23: Chip de una tarjeta inteligente.

Debido a todas estas restricciones, los algoritmos implementados no son todavía tan exactos, rápidos y fiables como los desarrollados para los sistemas biométricos tradicionales que se ejecutan en grandes servidores.

4.6.3 Estándares

La autentificación biométrica es una práctica muy extendida como componente de seguridad cuya ejecución en un cierto tiempo y lugar debe estar vinculada a la presencia del legítimo usuario. La importancia de la estandarización biométrica comienza cuando los componentes del sistema biométrico de diferentes fabricantes deben interactuar, especialmente si la tarea de autentificación del usuario se subdivide en módulos independientes. En particular, esta situación se produce en las "aplicaciones abiertas" donde tiene que haber una interoperabilidad de los componentes, los cuales son "desconocidos" entre sí antes de ser conectados. También ocurre en aplicaciones cuyos usuarios no pertenecen a un grupo limitado y bien definido:

- Aplicación de tarjeta de identidad con dominio de uso internacional.
- Permiso de conducir.
- Aplicaciones de banca y pago.
- Aplicaciones de firma electrónica.

Por ejemplo: las tarjetas inteligentes se usan a menudo como instrumentos para el almacenamiento y comparación de información biométrica durante el proceso de autentificación. Para ello es necesario que exista una interoperabilidad total entre los diferentes módulos que componen los sistemas biométricos como son las tarjetas, lectores y escáneres, ver Figura 4.24, y para ello es fundamental contar con unos estándares que normalicen y regulen todos los procesos de envío, gestión y tratamiento de datos.

Figura 4.24: Izquierda: escáner de huella dactilar, centro: puerta con control de acceso biométrico, derecha: tarjeta inteligente y lector.

El estándar principal sobre el que se basan las características de las tarjetas inteligentes es el ISO 7816 [28]. Es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial con las tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional De Normalización (ISO) y Comisión Electrotécnica Internacional (IEC) [28].

Este estándar detalla la parte física, eléctrica, mecánica y la interfaz de programación para comunicarse con el microchip. Un breve resumen sobre la descripción de cada una de las partes de la ISO 7816 [28] es:

- ✓ 7816-1: Características físicas.
- ✓ 7816-2: Dimensiones y ubicaciones de los contactos.
- ✓ 7816-3: Señales electrónicas y Protocolo de Transmisión.
- ✓ 7816-4: Comandos de intercambio inter-industriales.
- ✓ 7816-5: Sistema de numeración y procedimiento de registro.
- ✓ 7816-6: Elementos de datos inter-industriales.
- ✓ 7816-7: Comandos inter-industriales y consultas estructuradas para una tarjeta
- ✓ 7816-8: Comandos inter-industriales relacionados con seguridad.
- ✓ 7816-9: Comandos para la gestión de la tarjeta.
- ✓ 7816-10: Señales electrónicas y respuesta al *reset* para una Smart Card Síncrona.
- ✓ 7816-11: Verificación de la identidad personal a través de métodos biométricos.
- ✓ 7816-12: Tarjetas con contactos. Interfaz eléctrica USB y procedimientos operativos.
- ✓ 7816-15: Aplicación de información criptográfica.

Para más información sobre los estándares ISO e IEC, consultar el anexo Estándares ISO.

4.6.4 Proyectos y competiciones

- **MINEX II**

MINEX II [29] es la parte del programa MINEX (Test de cambio de operatividad de minucias) dedicado a la evaluación y el desarrollo de los comparadores de minucias de las huellas dactilares que se ejecutan en las tarjetas inteligentes ISO/ IEC 7816. MINEX junto con NIST coordinan esfuerzos de desarrollo dirigidos a mejorar el resultado y la operatividad de las herramientas de extracción de minucias según el estándar INCITS 378 y ISO/IEC 19794-2 de las huellas dactilares.

- **NPIVP (NIST Programa Personal de Verificación de Identidad)**

La División de Seguridad de Ordenadores NIST inició un nuevo programa para mejorar la identificación y autenticación de los empleados federales y contratados para acceder a las instalaciones federales y sistemas de información. Este programa, conocido como Programa Personal de Identidad y Verificación NIST (NPIVP) [30] se dirige a validar componentes (PIV) de Verificación de Identidad Personal, requeridos para el Proceso de Información Federal Standard (FIPS) 201. Los objetivos del programa NPIVP son:

- Validar la conformidad de dos componentes PIV de las tarjetas PIV con las especificaciones en NIST SP 800-73-1 [10].
- Proporcionar la certeza de que el equipo de PIV middleware y aplicaciones de tarjeta PIV que han sido validadas por NPIVP son factibles entre sí.

- **SBMoC (La Seguridad Biométrica de la tarjeta Match-on-Card)**

Los modelos estándares FIPS 201-2 [31, 32] definen un método para llevar a cabo la autentificación biométrica del portador de la tarjeta PIV (Verificación de Identificación Personal) cuando es insertada dentro de un lector. En algunos casos, sin embargo, se requiere trabajar sin conexión. La transacción de datos puede ser protegida mediante mensajes seguros y datos encriptados, pero estos métodos pueden entorpecer el rendimiento. Para entender los efectos de la seguridad en el rendimiento, NIST dirigirá un estudio de la viabilidad de la transferencia segura de datos sobre el terreno, sin conexión para realizar operaciones biométricas en las tarjetas Match-on-Card.

El estudio usará PKI (Clave de Infraestructura Pública) para crear una sesión autentificada y segura (como una sesión SSL/TLS) que proteja la integridad y la confidencialidad de los mensajes enviados desde la tarjeta inteligente al terminal. El protocolo nunca revela los datos biométricos desde la tarjeta inteligente. En vez de eso, el instrumento recibe una plantilla de la huella dactilar, encriptada, desde un lector biométrico, realiza una comparación sobre un modelo de huella de referencia almacenada en tarjeta y devuelve al lector un *sí* (las plantillas comparadas pertenecen al mismo usuario) o un *no* (caso contrario) como resultado de la comparación.

- **FVC (Competición de Verificación de Huellas Dactilares**

Las series de competiciones internacionales sobre reconocedores de huellas dactilares fueron organizadas en el 2000, 2002, 2004 y 2006 [4] respectivamente. Estos acontecimientos recibieron gran atención por parte de la comunidad académica y la industria biométrica. Establecieron una referencia común, permitiendo a los promotores, sin ambigüedad, comparar sus algoritmos y proporcionando una visión de conjunto sobre el estado del arte en el reconocimiento de huellas dactilares.

En las competiciones de 2004 y 2006 se definió una categoría especial para algoritmos concebidos para dispositivos móviles y además caracterizados por bajas capacidades de cálculo, limitada memoria de uso y pequeño tamaño de la huella almacenada (como en los sistemas Match-on-Card). Esta categoría se denomino light (ligera). El tiempo máximo para la fase de registro fue de 0,3 segundos y el tiempo máximo para la comparación fue de 0,1 segundos. La memoria máxima que podría estar disponible para los procesos fue de 4 MBytes. El tamaño máximo del modelo de huella fue de 2KBytes.

FVC2004 demostró que la imposición de restricciones en los recursos de computarización (tiempo, modelo y tamaño de la memoria) afecta drásticamente a los resultados. Sin embargo, las restricciones en FVC2004 y FVC2006 en la categoría ligera están todavía lejos de la capacidad real de una tarjeta inteligente o de un aparato de bajo coste.

4.6.5 Trabajos previos

Varios trabajos de investigadores independientes han sido propuestos para ver cómo poder adaptar el tradicional algoritmo automático de comparación o *matching* a las limitaciones del hardware de una tarjeta inteligente. Seguidamente se presenta una pequeña visión de conjunto de algunos de estos algoritmos y su eficacia en términos de escala de velocidad y reconocimiento. Todos ellos usan minucias basadas en algoritmos automáticos de comparación.

- **Sung, 2003**

En Sung [33], 2003, un algoritmo automático de comparación de ultra-baja memoria se presenta y se implementa en una tarjeta inteligente de 32 bits. En primer lugar se evalúa tanto el número de instrucciones ejecutadas como la memoria requerida para cada paso de un típico algoritmo de comparación de huella dactilar. Entonces los autores desarrollaron un algoritmo de memoria eficaz para la parte del proceso que consumía una mayor cantidad de memoria (la alineación). Los resultados experimentales muestran que el algoritmo propuesto puede reducir el espacio de memoria requerido por un factor de 62 y que puede ser ejecutado en tiempo real en un procesador (el AR7TDMI) de 32 bits de una tarjeta inteligente. La memoria de la tarjeta inteligentes usada es de 64 Kbytes de ROM (usado por el sistema operativo de la tarjeta), 8Kbytes de RAM (usada como área de almacenamiento temporal), y 32Kbytes de EEPROM (donde se almacena la información)

- **Barral, 2004**

En este trabajo se describe una tarjeta de memoria muy económica capaz de realizar comparaciones de huellas dactilares [34]. En el protocolo propuesto la tarjeta almacena la información de la huella dactilar del usuario a la que se añaden aleatoriamente las minucias (este modelo de huella dactilar viene denominado por $\mathbf{t}$). La tarjeta también almacena una cadena binaria $\mathbf{w}$ codificada con las minucias que pertenecen a $\mathbf{t}$. Cuando comienza una sesión de identificación, el terminal lee $\mathbf{t}$ de la tarjeta y basándose en la entrada de datos del escáner, determina cual de las minucias de $\mathbf{t}$ son auténticas. El terminal crea un candidato $\mathbf{w''}$ y lo envía a la tarjeta. Todo lo que la tarjeta necesita hacer es examinar que el peso Hamming de $\mathbf{w} \oplus \mathbf{w''}$ es más pequeño que una entrada de seguridad $\mathbf{d}$. Para ello, la tarjeta sólo necesita almacenar la información que recibe y utilizar una puerta "xor" junto con un registro de desplazamiento, un contador y un comparador (menos de 40 puertas lógicas).

- **Bistarelli, 2005**

En este trabajo se propone un moderno algoritmo de comparación de huellas dactilares [35]. El algoritmo se basa en las estructuras locales de minucias que son invariables con respecto a las transformaciones globales como traslación y rotación. El algoritmo de comparación fue realizado usando la plataforma de la tarjeta TM JAVA

dentro de una tarjeta inteligente con 32 Kbytes de memoria EEPROM, 1Kbyte de memoria RAM y 8bits CPU trabajando a 7.5MHz. La principal característica del algoritmo es tener un comportamiento asimétrico con respecto al tiempo de ejecución entre comparaciones correctas positivas y negativas. Los resultados en términos de fiabilidad en la autentificación y velocidad fueron comprobados en dos bases de datos (capturados con dos sensores ópticos diferentes) en la competición de verificación de huellas dactilares 2002 (FVC 2002) alcanzando en ambos un 8.5% EER.

- **Mostafa, 2005**

En este trabajo los autores presentan un método para reducir los requerimientos de memoria para su almacenamiento y reducir el tiempo de procesamiento de la imagen [36]. En este trabajo también se señalan las ventajas de usar un esquema de extracción de una línea para reducir el tamaño de la matriz del acumulador y acelerar el proceso de comparación de huellas dactilares. El método propuesto contiene más información por bit que el método tradicional, que puede ser ejecutado en tarjetas inteligentes para su utilización en el sistema Match-on-Card en tiempo real. Se presenta un ejemplo de utilización de identificación de huellas dactilares en una plataforma DSP con acumulación de memoria limitada para evaluar el rendimiento de la prueba. Un FR de 0,77% y 1,05% son respectivamente presentados para un FA de 1% y 0,1%.

- **Fons, 2006**

Este trabajo describe un hardware-software de un sistema de huella dactilar para tarjeta inteligente, responsable de la comparación de dos grupos de minucias de huellas dactilares de una forma fiable y segura [37]. El sistema de arquitectura propuesto comprende un microprocesador de 8 bits y una FPGA (Field Programmable Gate Array) de 40 Kgates, todo ello embebido en un sólo chip. El tiempo medio de ejecución del algoritmo es de unos 0,25 segundos.

- **Mueller, 2006**

En este trabajo [38] los autores describen un algoritmo híbrido de tarjeta inteligente que combina los modelos de huellas dactilares estandarizadas desde dos diferentes modelos (ISO/IEC 19794-2 Y ISO/IEC 19794-8) [28] para crear un sistema que mejora la comparación de huellas. En este caso la información de minucias (ISO/IEC 19794-2) se complementa con la información de la cresta de la huella dactilar almacenada en un formato compacto (esqueleto) siguiendo el modelo ISO/IEC 19794-8.

4.7 Conclusión

En los últimos años la tecnología MoC ha experimentado un importante desarrollo, no sólo a nivel de hardware, aumentando tanto la capacidad de cálculo del microprocesador como el nivel de espacio disponible para el almacenamiento de programas y archivos, sino también a nivel de mercado donde cada vez son más los fabricantes de tarjetas inteligentes y empresas que demandan sus servicios de seguridad. Es en el ámbito de bases de datos distribuidas y los entornos seguros donde esta tecnología demuestra su potencial.

Unos ejemplos de empresas que utilizan tarjetas inteligentes:

Lugar	Tarjeta	Proveedor	Introducción
Malasia	Touch 'n Go	Teras Technologi Sdn Bhd	1997
Washington, D.C.	SmarTrip	Cubic Transportation Systems	1999
Bogotá	Angelcom	Angelcom	2000
Malasia	MyKad	IRIS Corporation Berhad	2001
Chicago	Chicago Card	Chicago Transit Authority	2002
Santiago de Chile	Multivía	Indra Sistemas para Metro de Santiago	2003
São Paulo	Bilhete Unico	Prefeitura de São Paulo	2004
V Región de Chile	Metro Valparaíso	Indra Sistemas para EFE	2005
Donostia	Kutxa-chip sin contacto	Kutxa	2006
Guipúzcoa	Lurraldebus txartela	Lurraldebus	2006
Mendoza	Redbus	Siemens	2006
Santiago de Chile	Tarjeta bip!	Transantiago	2006
Boston	Charlie Card	Massachusetts Bay Transportation Authority	2006
Córdoba	Redbus	Siemens	2007
Medellín	Cívica	UT Equant-Smart N IT para	2007
Toronto	GTA Farecard	GO Transit	2007

Tabla 4.1: Implantación en el mercado de tecnología de tarjetas inteligentes (Smartcard)

5. Sistema de reconocimiento propuesto

En esta sección se detalla el algoritmo de reconocimiento de huella dactilar que se implementará en el simulador (ver anexo Simulador). El objetivo de este Proyecto es desarrollar un sistema de reconocimiento de huella dactilar con comparación basada en minucias, funcional, automático, y que tenga en cuenta las limitaciones de la tecnología Match-on-Card. Para ello se ha tomado como punto de partida el trabajo de Mueller y Martini [38], cuyo algoritmo se ha adaptado y mejorado en base a los objetivos de este documento. El algoritmo se ha implementado en el lenguaje de programación Matlab sobre una plataforma PC.

El algoritmo de reconocimiento propuesto incluye cuatro fases, que se detallan en las siguientes secciones: primero, se realiza una extracción de las minucias de la huella que se caracterizan por sus coordenadas espaciales y su ángulo. A continuación se realiza una alineación en translación entre las dos huellas a comparar. Seguidamente, si la alineación se ha realizado con éxito, se realiza una comparación en la que se establece el número de minucias coincidentes. Por último, el sistema toma la decisión de aceptación o rechazo de la huella de entrada que se está comparando con la huella registrada del usuario reclamado, en función de si el número de minucias ha superado o no el umbral de decisión.

5.1 Introducción

El algoritmo tiene, como entrada, dos conjuntos de minucias F_R y F_T, procedentes de la huella de registro y huella de test respectivamente, y como salida, emite una decisión acerca de si son o no pertenecientes a la misma huella. Los estándares no nos proporcionan una definición sobre la similitud entre dos plantillas, de esta manera queda abierto el criterio a utilizar y el diseñador del sistema debe determinar qué reglas sigue para considerar si dichas plantillas pertenecen o no al mismo usuario. Sin embargo, en el caso concreto de un algoritmo de reconocimiento de huella dactilar basado en minucias, es muy común usar el número de minucias coincidentes entre ambas plantillas como medida de similitud o coincidencia.

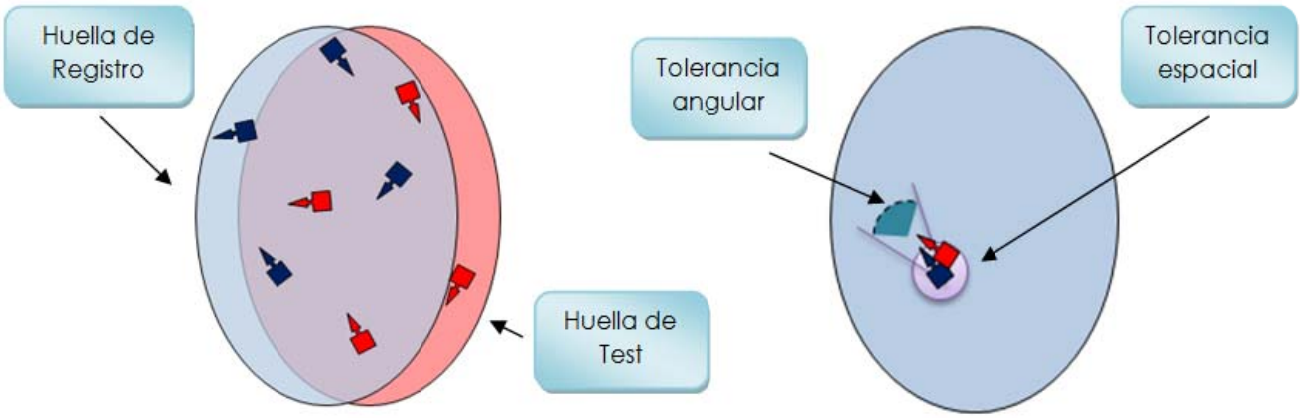


Figura 5.1: Izquierda: representación esquemática de dos huellas dactilares junto con sus minucias, derecha: superposición de minucias y aéreas de tolerancia.

Para considerar que dos minucias son equivalentes, ambas deben coincidir en posición y orientación, siempre teniendo en cuenta una tolerancia (ver Figura 5.1). Sin embargo, la posición y el ángulo de cada minucia vienen dados inicialmente en un sistema de coordenadas fijo respecto al sensor (no al dedo) de manera que no es posible comparar dichas coordenadas directamente (ver Figura 5.2). Los sistemas de reconocimiento superan este problema usando una fase previa a la comparación de minucias, es decir, una fase de alineación donde se intenta solventar los posibles fallos cometidos por el usuario a la hora de colocar su dedo sobre la superficie del sensor, ya que pequeñas variaciones en la posición en que se coloque podrían ocasionar, si no hubiera una etapa de alineación, que la valoración de similitud entre dos huellas de un mismo usuario se viera fuertemente afectada.

Figura 5.2: Izquierda: huella de Test (minucias rojas) y derecha huella de Registro (minucias azules). Pertenecen al mismo usuario, pero no están alineadas.

A la hora de diseñar el sistema hay que tener en cuenta los siguientes puntos:

1. Minimizar el número de falsas aceptaciones.
2. Minimizar el número de falsos rechazos.
3. Minimizar el tiempo de ejecución del sistema de reconocimiento.

Pero esta tarea no es trivial ya que dichos objetivos en parte son excluyentes, de manera que se debe llegar a un compromiso razonable entre ellos para determinar el punto óptimo de funcionamiento. Esto se consigue eligiendo apropiadamente los valores y condiciones que determinaran cuando dos plantillas estén alineadas y cuál será el mejor punto para la elección del umbral, de manera que indique si dos minucias son coincidentes, con una cierta tolerancia.

5.2 Características del sistema

Minucias: Como ya se ha mencionado antes, el sistema de verificación que aquí se presenta está basado en minucias. Una minucia es una alteración en el normal fluir de una cresta (o valle). Existen muchos tipos de minucias, pero se pueden resumir en dos, "fin de cresta" y "bifurcaciones" (ver Figura 5.3). Cada huella está definida como un conjunto de N minucias m_i, con $i = 1...N$. Cada minucia m_i se caracteriza mediante la tupla $m_i = \{x_i, y_i, \theta_i, Q_i\}$, donde (x_i, y_i) son las coordenadas espaciales de la minucia con origen en la esquina superior izquierda de la imagen, θ_i su orientación en grados definidos del eje x al eje y en sentido horario, y Q_i es un factor de la calidad en función del ruido de la imagen en el entorno de la minucia, como ya se definió en la sección 4.5.2.

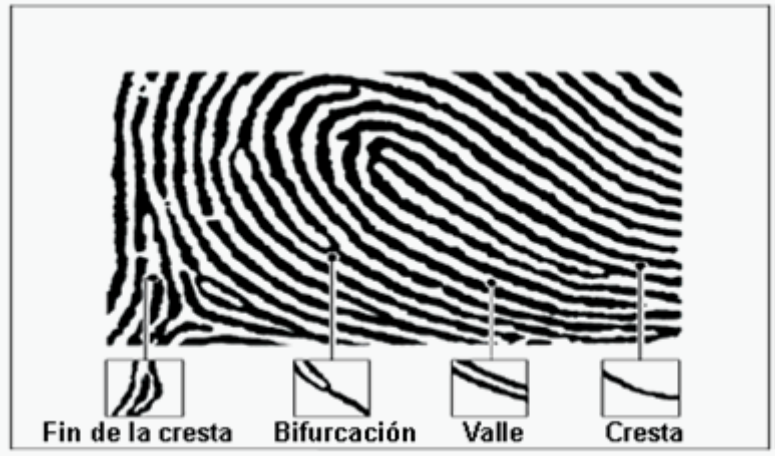


Figura 5.3: Detalle de las crestas, valles, bifurcaciones y finales de cresta de una huella dactilar.

- **Coordenadas:**

El sistema utilizado para almacenar la información de la posición de las minucias es el sistema habitual de coordenadas utilizado en el procesado de imágenes, donde el origen se define en la parte superior izquierda de la imagen (de la huella). De esta manera los ángulos se definen desde el eje X al eje Y en el sentido de giro de la agujas del reloj (ver Figura 5.4).

Figura 5.4: Eje de coordenadas y ángulo de referencia para representar imágenes.

- **Ángulos:**

La orientación de cada minucia se fija contando en sentido horario desde el eje de abscisas (ver Figura 5.4). A la hora de almacenar el ángulo de cada minucia se define el parámetro de cuantificación q como el número de bits que se utilizan para cuantificar el ángulo θ_i. Este parámetro simula las condiciones operacionales de Match-on-Card, donde la plantilla incluye habitualmente valores cuantificados de los ángulos. Los valores habituales de q son 8 y 6 bits (256 y 64 valores posibles, respectivamente).

- **Uso de decimales:**

Para tener en consideración la capacidad aritmética de los distintos dispositivos de Match-on-Card, se define el parámetro *d* como el número de decimales con los que opera el algoritmo, donde *d*=0 representa aritmética de coma fija. Por tanto, todas las operaciones del algoritmo se redondean al número más cercano con *d* decimales.

5.3 Descripción del algoritmo

A continuación se detallan los distintos bloques del algoritmo propuesto: extracción de minucias, alineación, cálculo de similitud y decisión (ver Figura 5.5):

- Extracción de las minucias de cada huella.
- Alineación entre la plantilla de referencia y la de verificación.
- Estimación de la similitud entre dichas plantillas.
- Regla de decisión, aceptación o rechazo de la plantilla a verificar (usuario genuino o impostor).

Figura 5.5: Esquema del algoritmo diseñado para la comparación de huellas dactilares.

5.3.1 Extracción de minucias

En esta fase se obtienen los puntos característicos (minucias) de la huella dactilar. Esta etapa es especialmente sensible ya que pueden aparecer distorsiones en la imagen que den lugar a aparición de minucias falsas o desaparición de minucias genuinas. Este efecto es especialmente grave en caso de que la imagen obtenida sea de mala

calidad, lo cual puede estar causado por cicatrices, sudor, sequedad u otras condiciones que afecten al sensor.

Para la extracción de los puntos característicos de la huellas se ha utilizado el software de dominio público NIST Biometric Image Software (NBIS) del National Institute of Standards and Technology [10]. Este software de referencia es ampliamente utilizado en reconocimiento de huella dactilar. En el algoritmo propuesto solamente se ha utilizado el módulo MINDTCT, encargado de extraer las minucias a partir de la imagen de la huella dactilar. Así, utilizando este módulo se obtiene la información de posición, orientación y calidad descrita en el apartado anterior.

A continuación se describe el funcionamiento del módulo de extracción de puntos característicos de las huellas.

- **MINDTCT** toma una imagen de una huella dactilar y localiza todas las minucias en la imagen asignando a cada minucia sus coordenadas, orientación y calidad. La arquitectura de MINDTCT se puede observar en la Figura 5.6.

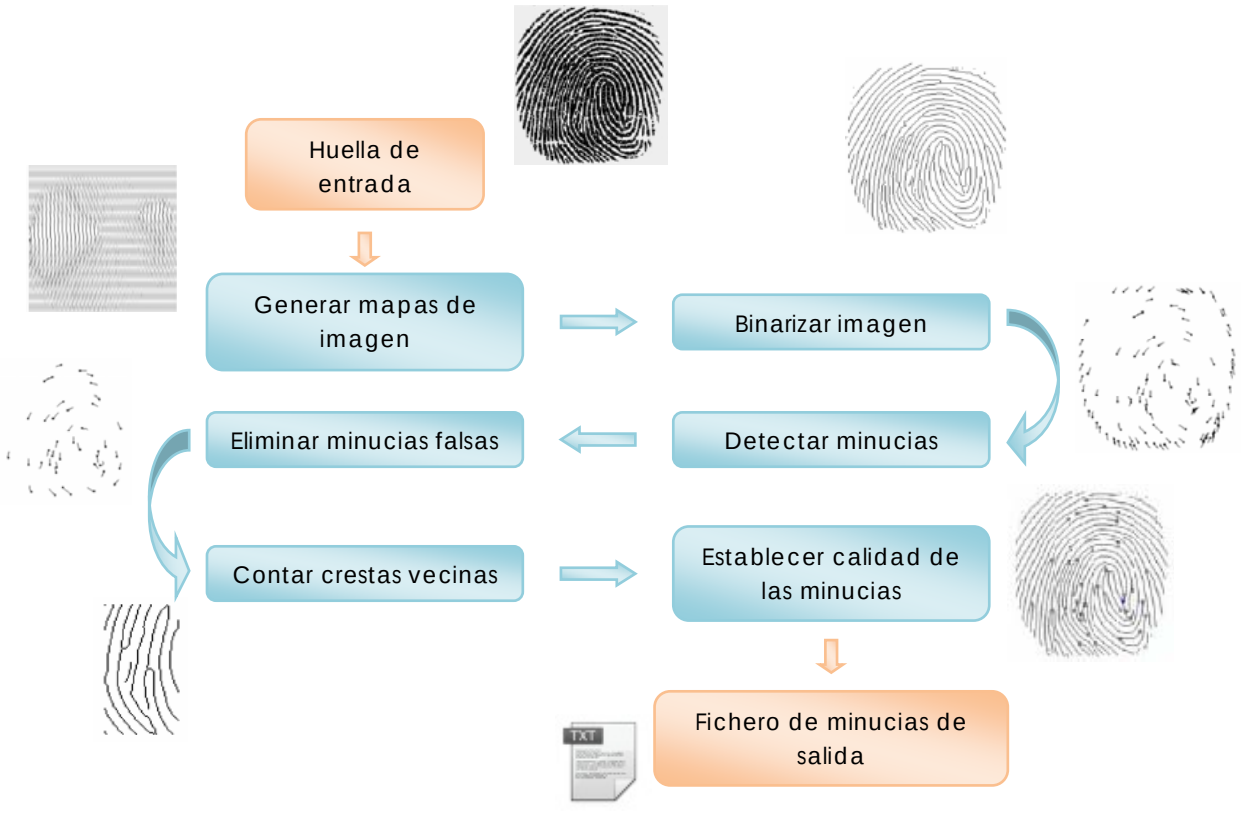


Figura 5.6: Arquitectura del módulo MINDTCT.

Los pasos que MINDTCT sigue son los siguientes:

Generar mapas de calidad de la imagen, entre los cuales cabe destacar: mapas de dirección, para determinar zonas en las que la estructura de crestas está claramente definida; mapas de zonas de bajo contraste o no pertenecientes a la huella, para descartarlas en el proceso de detección de minucias; mapas de alta curvatura, para tener en cuenta las zonas como el núcleo de la huella en las que las minucias se detectan con mayor dificultad.

Binarizar la imagen, para que el resto del proceso opere con imágenes de sólo dos niveles de color.

Detectar minucias, mediante búsqueda de patrones. A partir de unos patrones conocidos, se buscan las minucias en la imagen binarizada de la huella.

Eliminar falsas minucias. Se eliminan todas las minucias de zonas de baja calidad, minucias que forman islas y lagos, minucias excesivamente próximas y otros tipos de minucia que son susceptibles de ser producto de una detección errónea.

Contar crestas vecinas. Se cuentan las crestas existentes entre una minucia y sus minucias vecinas para su utilización en otros módulos del paquete NBIS.

Establecer la calidad de las minucias. Mediante los mapas de calidad previamente calculados y otras medidas de calidad de la imagen inicial, se establece un nivel de calidad con 5 posibles niveles para clasificar las minucias.

Fichero de minucias de salida. Se crean ficheros de salida con los mapas de calidad y con los mapas de minucias. El mapa de minucias es un fichero de texto que contiene un listado de minucias en filas formado por sus coordenadas, su orientación y su nivel de calidad.

Una vez extraída toda esta información sobre las minucias de cada huella podemos comenzar a trabajar con la representación de cada una de ellas a través de sus minucias, es decir, ya no necesitamos seguir utilizando la imagen de la huella, que ocupa unos 40KBytes, sino que ahora, con el fichero de minucias, en el que cada una de ellas está perfectamente definida a través de su posición (coordenadas x,y), su orientación y su calidad podemos definir completamente una huella en una plantilla de unos 1.500Bytes (1,5KBytes) con lo que disminuimos en más de 20 veces el espacio requerido para almacenamiento y los recursos necesario para tratar la información.

5.3.2 Alineación

Se ha partido de la metodología propuesta en Mueller y Martini [38] para determinar la coincidencia entre las plantillas. Con el proceso de alineación se logra solventar los posibles desajustes a la hora colocar el dedo sobre la superficie del sensor entre distintas sesiones de adquisición. Para ello se ha supuesto que las diferentes adquisiciones están tomadas aproximadamente con la misma rotación de la huella, lo que es razonable para la mayoría de los dispositivos de adquisición de huella dactilar electrónicos actuales; ver por ejemplo: Figura 5.7, en donde se muestran varias adquisiciones de huellas capturadas con el sensor óptico Biometrica FX2000 y con el sensor térmico Atmel Yubee. Estas imágenes pertenecen al conjunto de la base de datos Biosecure Multimodal Database, con la que se han realizado las pruebas y experimentos para optimizar y evaluar el sistema desarrollado.

Figura 5.7: Imágenes de ejemplo de la base de datos Biosecure Multimodal Database. Arriba: capturadas con el sensor óptico Biometrica FX2000. Abajo capturadas con el sensor térmico Atmel Yubee.

El tiempo empleado por un sistema de verificación es aproximadamente proporcional al número de translaciones necesarias para determinar la coincidencia de las plantillas. Para intentar reducirlo, lo primero que se ha hecho ha sido ordenar las minucias en función de su orientación. Esta operación puede ser llevada a cabo tanto en el terminal que lee la huella como en el interior de la propia tarjeta ya que los estándares proporcionan librerías con funciones de ordenación que permiten trabajar con los datos directamente en la tarjeta.

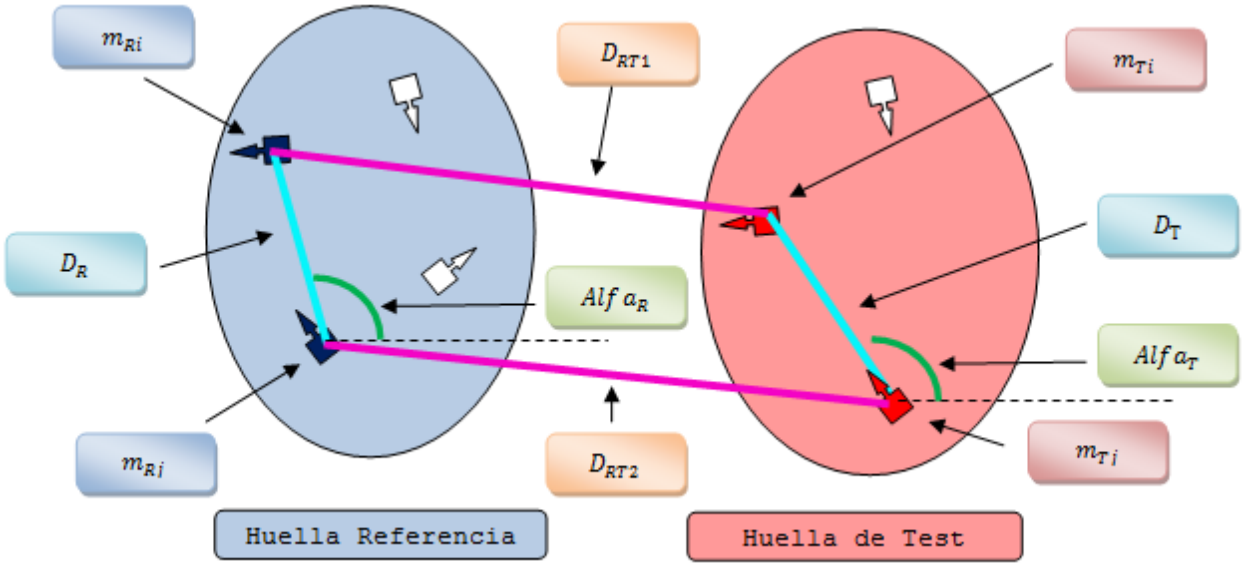


Figura 5.8: Alineación entre huellas de referencia y test (verificación).

Para alinear las dos plantillas, ver Figura 5.8, se eligen aleatoriamente dos minucias distintas $\{m_{Ri}, m_{Rj}\}$ en la huella de referencia F_R. Entre las minucias de F_T con orientación similar a las dos elegidas, se buscan las que tengan una separación entre ellas también similar a la separación entre m_{Ri} y m_{Rj}, obteniendo $\{m_{Ti}, m_{Tj}\}$. Para ello se definen los parámetros d_1 y θ_1, máxima diferencia de separación permitida y máxima diferencia de ángulos permitida entre $\{m_{Ri}, m_{Rj}\}$ y $\{m_{Ti}, m_{Tj}\}$ respectivamente. Esta operación se repite iterativamente hasta encontrar dos pares correspondientes (con diferencia de separación menor que d_1 y diferencia de ángulos menor que θ_1), ver Figura 5.9 o hasta que se supera un número M de intentos. Si se han encontrado dos pares coincidentes antes de agotar las iteraciones, las cuatro minucias obtenidas se utilizarán para definir el desajuste entre las dos plantillas (ver Figura 5.9). Si no, las huellas se consideran como diferentes y termina la ejecución del algoritmo.

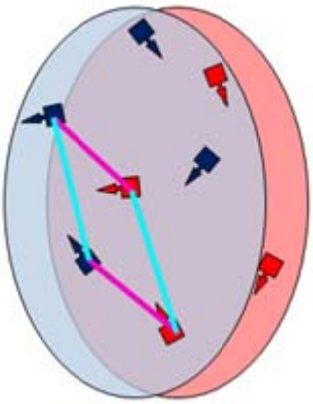


Figura 5.9: Representación de dos pares coincidentes en la alineación. Las elipses azul y roja representan las huellas de registro y test, respectivamente. Los puntos azules representan minucias en la huella de registro y las rojas minucias de la huella de test. Los pares coincidentes se resaltan con las líneas magenta.

De esta manera definimos la distancia que separa las dos minucias elegidas en la huella de referencia y en la huella a verificar (líneas cian) como:

$$D_R = distancia\left\{m_{Ri}, m_{Rj}\right\} = \sqrt{(x_{Ri} - x_{Rj})^2 + (y_{Ri} - y_{Rj})^2}$$

con i,j = 1,2, ...N_R (número de minucias de la huella de referencia)

$$D_T = distancia\left\{m_{Ti}, m_{Tj}\right\} = \sqrt{(x_{Ti} - x_{Tj})^2 + (y_{Ti} - y_{Tj})^2}$$

con i,j = 1,2, ...N_T (número de minucias de la huella a verificar)

y consideraremos que dichas cuatro minucias son válidas para definir el desplazamiento necesario para alinear las plantillas de las huellas si se cumplen estas condiciones:

$$\|\theta_{Ri} - \theta_{Ti}\| \leq \theta_1$$

$$\left\|\theta_{Rj} - \theta_{Tj}\right\| \leq \theta_1$$

$$\|D_R - D_T\| \leq D_1$$

Los valores de d_1 y θ_1 se han obtenido experimentalmente para maximizar el rendimiento del sistema sobre el subconjunto de desarrollo de la base de datos Biosecure Multimodal Database. Los valores resultantes para ambos parámetros han sido: d_1=120 píxeles y θ_1=6º. Un ejemplo de una correcta alineación entre plantillas pertenecientes al mismo usuario lo encontramos en la Figura 5.10:

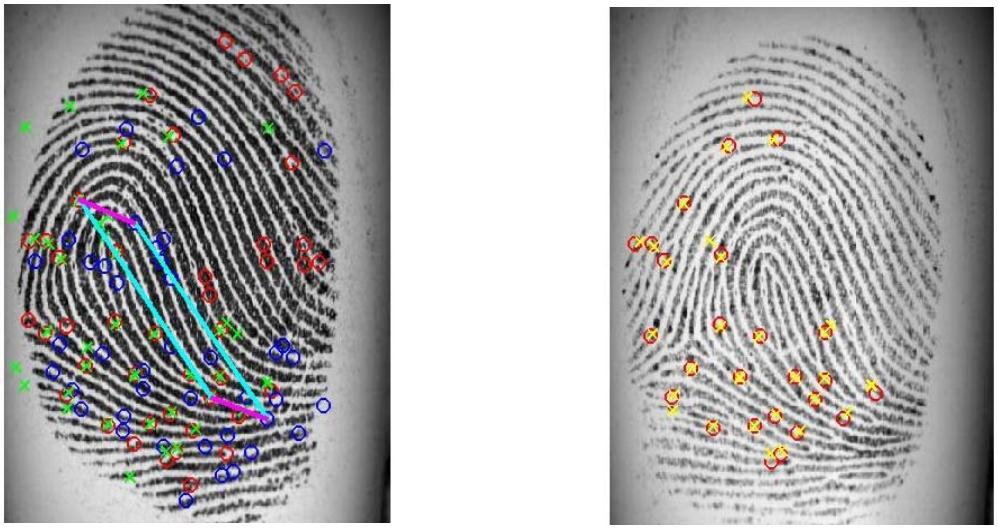


Figura 5.10: Alineación correcta entre las minucias de dos huellas diferentes pertenecientes al mismo usuario, los círculos representan las minucias de cada huella y las equis las minucias de la huella de referencia alineadas sobre las minucias de la huella a verificar (huella de Test).

Este método es muy sencillo de implementar y consume muy pocos recursos, pero también tiene una eficiencia bastante baja ya que en la mayoría de los casos no encuentra las minucias de la huella a verificar que se corresponden con las de la huella de referencia (ambas pertenecientes al mismo usuario), dando lugar a alineaciones erróneas que no permiten una buena estimación de la similitud entre las huellas y por tanto nos impiden determinar correctamente si las huellas pertenecen o no a la misma persona.

El número de posibles combinaciones resultante de este primer paso se ve fuertemente reducido si añadimos las siguientes condiciones:

- Para intentar corregir este tipo de fallos en la alineación (ver Figura 5.11), la primera de estas medidas ha sido imponer que la distancia entre cada una de las dos minucias de la huella de referencia y las minucias de la huella de Test D_{RT1} y D_{RT2} sea prácticamente la misma. Dicha distancia, si nos fijamos en la Figura 5.8, es la correspondiente a la separación entre las minucias marcadas en rojo (huella de referencia) y en azul (huella a verificar) y queda remarcada con una línea morada.

El objetivo es formar un paralelogramo cuyos vértices se correspondan con las minucias de ambas huellas $\{m_{Ri}, m_{Rj}, m_{Ti}, m_{Tj}\}$, ver Figura 5.9, de esta manera podremos asegurar que el proceso de alineación ha funcionado correctamente para un porcentaje muy alto de huellas.

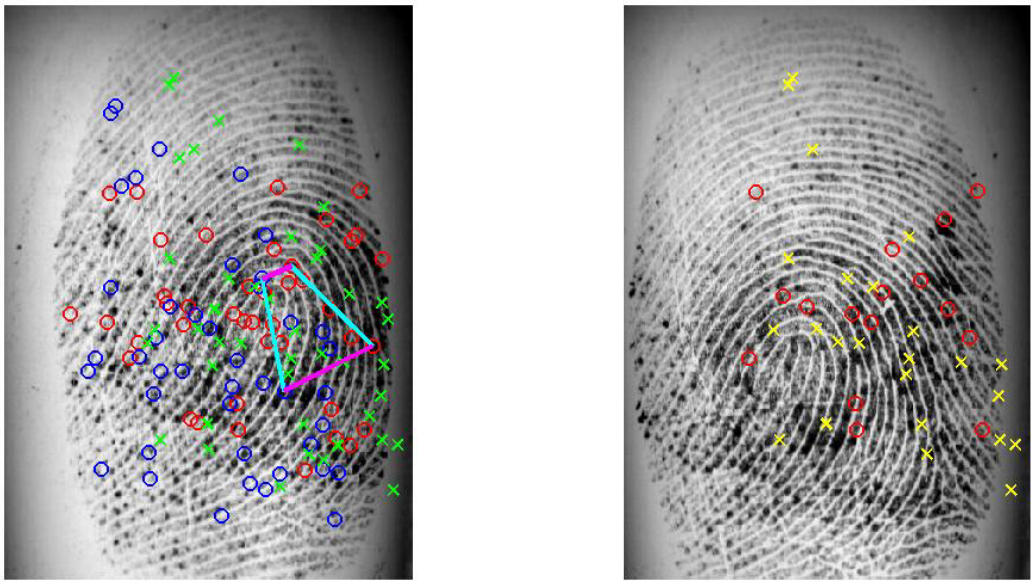


Figura 5.11: Errores en el proceso de alineación, distinta distancia entre pares de minucias (D_{RT1} y D_{RT2}, líneas moradas diferentes).

Debido a errores de detección observados experimentalmente, se añade una comprobación adicional para la detección de los pares coincidentes, consistente en imponer que la diferencia entre las pendientes de las dos rectas que unen los dos pares ($Alfa_R$ y $Alfa_T$, ver Figura 5.12) sea menor que cierto valor (pequeño) p_1.

Figura 5.12: Errores en el proceso de alineación, cruce de aristas.

De esta manera nos aseguramos que las minucias de una y otra huella se corresponden y por tanto podemos determinar de forma precisa cual es el desplazamiento existente entre ellas y corregirlo. Como resultado del éxito de la alineación, el proceso de comparación proporcionará puntuaciones más fiables.

- Para terminar de delimitar la alineación, impondremos una restricción en el desplazamiento máximo que puede sufrir una plantilla sobre otra D_{max}, es decir, en ningún caso una huella puede ser sometida a una translación mayor que su ancho o alto ya que se saldrían de la superficie del sensor y no tendría ninguna zona en común para realizar la comparación (ver Figura 5.13).

$$\frac{D_{RV1} + D_{RV2}}{2} \leq D_{max}$$

A partir de ahora nos referiremos a las líneas que unen las minucias entre la plantilla de referencia y la de verificación D_{RT1} y D_{RT2} (líneas moradas) como "líneas maestras de alineación" (baselines of the match) (ver Figura 5.9). La distancia media entre los dos pares de minucias coincidentes se utiliza para alinear en posición las minucias de F_T respecto a F_R. Dicho desplazamiento D_{DESPL} se determina haciendo la media entre el desplazamiento que tendría que sufrir cada una de las dos minucias elegidas en la huella de verificación para "encajar" sobre las minucias de la huella de referencia, (líneas moradas) (ver Figura 5.14).

$$\boldsymbol{D_{Despl} = \frac{D_{RT1} + D_{RT2}}{2}}$$

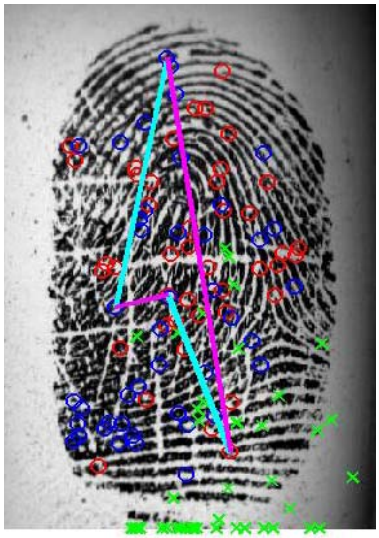


Figura 5.13: Error en la alineación, desplazamiento máximo excedido.

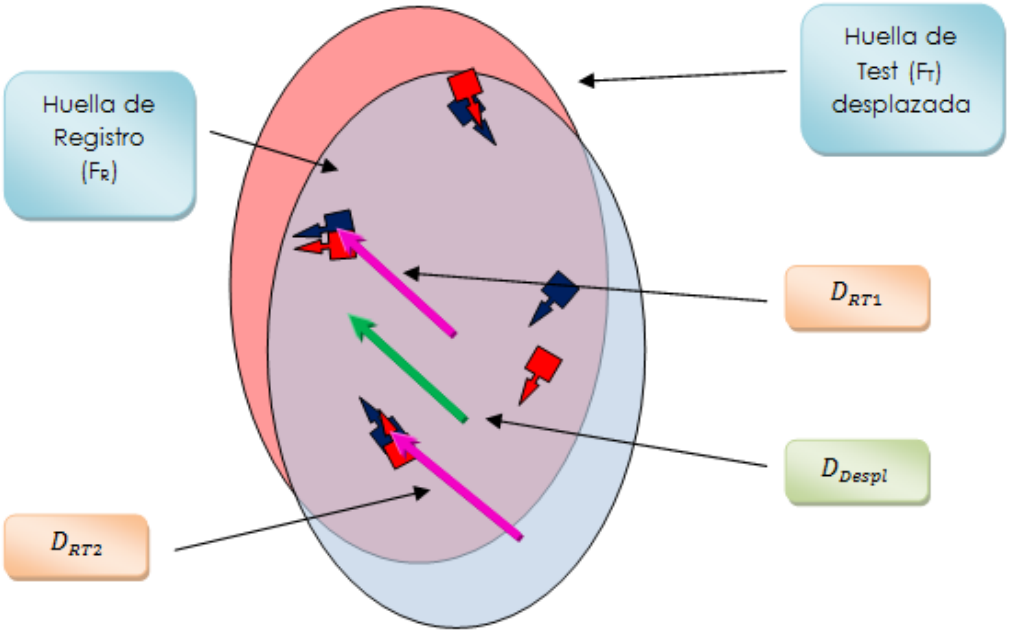


Figura 5.14: Desplazamiento de las minucias de la huella a verificar (huella de Test) como resultado del proceso de alineación. Comparar con Figura 5.1

5.3.3 Determinación de la similitud entre huellas (Match Score)

Las dos líneas maestras, a las que nos acabamos de referir, son las responsables de la alineación ya que la media de ambas representa cual debería ser el desplazamiento que la plantilla de verificación debe sufrir para que sus minucias coincidan con las de la plantilla de referencia. Esta fase del proceso de verificación determina la precisión del método en términos de falsa aceptación o falso rechazo, es decir, si muchas minucias que no se deberían corresponder entre las dos plantillas si lo han hecho, o si por el contrario, muchas minucias coincidentes son rechazadas como diferentes debido a criterios estrictos de tolerancia, provocaría que fuera imposible encontrar una medida de similitud que permitiera discriminar suficientemente entre las plantillas genuinas (pertenecientes al mismo usuario) y las de los impostores.

El objetivo de esta tercera fase es, por tanto, determinar la coincidencia o no entre un par de minucias, pertenecientes a diferentes huellas, de la forma más fiable posible.

Para conseguirlo, el comparador sigue un proceso iterativo en el que se comprueba para cada minucia de F_R todas las minucias de F_T hasta que se encuentra una coincidencia o se agotan las minucias. Los posibles criterios para determinar si un par de minucias son coincidentes son:

- Tipo de minucia.
- Coordenadas de la minucia.
- Orientación de la minucia.
- Ángulo que forma la minucia y la línea maestra.
- Ángulo entre las líneas maestras y la horizontal (de la imagen).

Como se ha explicado al comienzo de este capítulo, existen multitud de tipos de minucias (ver anexo Puntos característicos), aunque todos ellos se pueden catalogar en dos grandes grupos, fin de crestas y bifurcaciones, como hace el programa del NIST. De esta manera la información aportada por este campo es muy pequeña y para reducir costes de almacenamiento y computación no se tiene en cuenta dicho criterio.

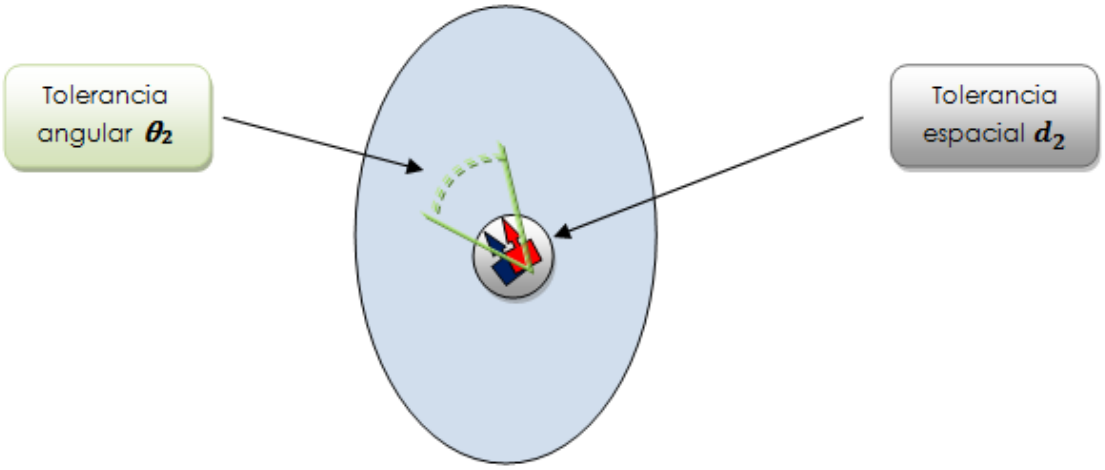


Figura 5.15: Aéreas de tolerancia para determinar la equivalencia entre minucias.

Por otro lado la posición de las minucias tras la alineación, sus **coordenadas**, ha sido junto con la **orientación** de las mismas, los criterios seguidos para determinar si dos minucias son coincidentes. Dos minucias se consideran coincidentes si su distancia euclídea es menor que d_2 y su diferencia de ángulos es menor que θ_2.

$$d(m_{Rk}, m_{Tp}) = min\sqrt{(x_{Rk} - x_{Tp})^2 + (y_{Rk} - y_{Tp})^2} \leq d_2$$

$$\theta(m_{Rk}, m_{Tp}) = min(|\theta_{Rk} - \theta_{Tp}|) \leq \theta_2$$

Si se declara una coincidencia entre la plantilla de referencia y la de verificación, ver Figura 5.14, la puntuación preliminar entre ambas plantillas se incrementa en una unidad, ver Figura 5.15 y las minucias responsables de dicha coincidencia son almacenadas en una lista de minucias equivalentes. De esta manera el sistema continúa buscando coincidencias con una nueva minucia de la plantilla de referencia.

5.3.4 Regla de decisión

Una vez analizadas todas las parejas de minucias, se comprueba si el número de minucias coincidentes supera el umbral de decisión. En caso positivo, se declaran ambas plantillas como pertenecientes a la misma huella; en caso contrario, se decide que la comparación no ha tenido éxito y que por tanto las huellas son distintas.

6. Experimentos realizados y resultados

6.1 Bases de datos

Para las pruebas de este Proyecto hemos elegido la base de datos (BMDB) Biosecure Multimodal Database [4]. La adquisición de la Base de Datos Biosecure Multimodal fue llevada a cabo, entre noviembre de 2006 y junio de 2007, conjuntamente por 11 instituciones europeas participantes en la Red de Excelencia Biosecure. La institución a cargo de la coordinación de la adquisición del proceso fue la Universidad Politécnica de Madrid (UPM), de España, a través del ATVS/Grupo de Reconocimiento Biométrico.

Esta base de datos cuenta con rasgos de más de 600 personas, adquiridos simultáneamente en tres escenarios diferentes. Se compone de tres conjuntos de datos con una institución a cargo de coordinar cada conjunto de datos. Los tres conjuntos de datos son:

- Data set 1 (DS1). Adquiridos a través de Internet bajo condiciones supervisadas (por ejemplo: conectándose a una URL y siguiendo las instrucciones que aparecen en pantalla).
- Data Set 2 (DS2). Adquirido en un entorno de oficina (ordenador personal) usando un ordenador estándar y un número de sensores comerciales bajo la supervisión de un experto.
- Data Set 3 (DS3). Adquirido usando dispositivos móviles, como por ejemplo: portátiles, PDA's, móviles... bajo dos condiciones de adquisición: interior y exterior. Las adquisiciones en interiores fueron hechas en una habitación tranquila (con luz controlada, sin ruidos etc.), mientras que las adquisiciones en exteriores fueron grabadas en ambientes ruidosos (pasillos de oficinas, la calle, etc.) permitiendo al usuario mover y cambiar su posición.

La BMDB ha sido diseñada para ser representativa de la población que haría un posible uso de los sistemas biométricos. Como resultado del proceso de adquisición, un 40% de los sujetos están entre los 18 y 25 años. El 20-25% entre los 25 y 35 años, el 20% de los sujetos están entre los 35 y 50 años, y el restante 15-20% tienen más de 50 años. Además la distribución por géneros fue diseñada para ser tan equilibrada como fuera posible, con una diferencia entre grupos de hombres y mujeres inferior al 10%.

Los tres conjuntos de datos de BMDB incluyen una parte común de datos de audio y video.

En este Proyecto se ha utilizado el subconjunto de BMDB capturado en la Universidad Autónoma de Madrid, que incluye datos biométricos de 145 personas.

6.1.1 Proceso de adquisición y validación de los datos:

Para la adquisición de DS2 y DS3 se contó con la supervisión de un experto. En la validación de las adquisiciones se deben distinguir entre muestras de baja calidad válidas y muestras no válidas. Las muestras de baja calidad son aceptables en tanto que se siga estrictamente el protocolo de adquisición, y los diferentes sensores biométricos sean usados correctamente. Por el contrario, muestras no válidas son aquellas que no cumplen con las especificaciones dadas para la base de datos. En cuyo caso son descaradas por el supervisor.

Características DS2:

Para las pruebas de este Proyecto, hemos elegido el subconjunto DS2 de la base de datos Biosecure Multimodal Database. Dicho conjunto cuenta con las huellas dactilares de 145 personas. En DS2, la adquisición de las mismas se realizó en un ambiente de oficina, el hardware usado para la adquisición incluye un PC con base Windows, puerto USB y los sensores biométricos, que en el caso de huella dactilar son: el sensor Óptico de huella dactilar Biometrica FX2000 (bmp 296x560 pixels, 569dpl) y el sensor de huella dactilar Térmico Atmel Yubee (bmp 400x500pixels, 500dpl) (ver Figura 6.1).

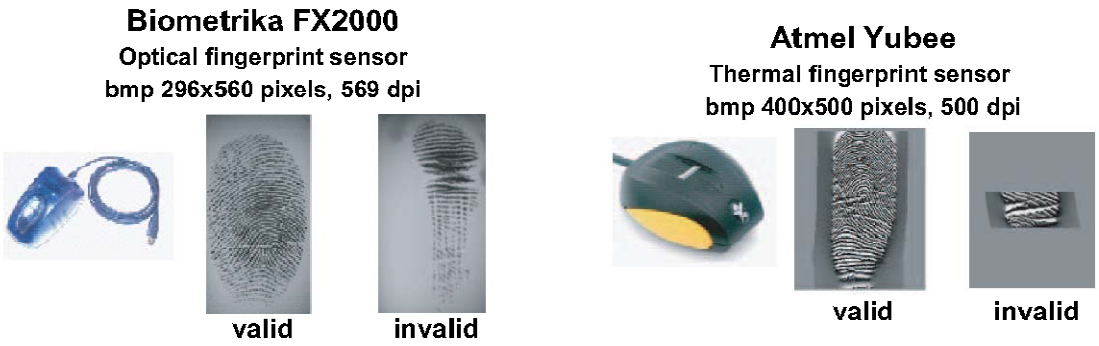


Figura 6.1: Sensores con los que se ha calculado la base de datos.

Este subconjunto de la base de datos (DS2) está formado por 24 muestras de huella dactilar por persona, tomadas con el sensor térmico: de 3 dedos (pulgar, índice y corazón) x 2 manos x 2 repeticiones por dedo x 2 sesiones, lo que hacen 24 muestras; y otras 24 muestras por persona adquiridas con el sensor óptico: 3 dedos x 2 manos x 2 repeticiones por dedo x 2 sesiones. Lo que hacen un total de 48 muestras por persona y para un total de 145 personas x 48 muestras = 6.960 huellas dactilares.
Durante la adquisición de la huella dactilar con el sensor térmico (como el sensor de huella dactilar térmico Yubee es difícil de usar correctamente), al usuario se le permitió realizar múltiples pruebas antes de la primera adquisición. Este sensor también provocaba malestar en algunos usuarios, debido a los fallos. Las huellas dactilares de muy baja calidad o tamaño muy pequeño, debido a un mal uso del sensor, no fueron admitidas.

A continuación se muestra ocho capturas de la misma huella dactilar, primero cuatro en el sensor térmico y a continuación 4 con el sensor óptico:

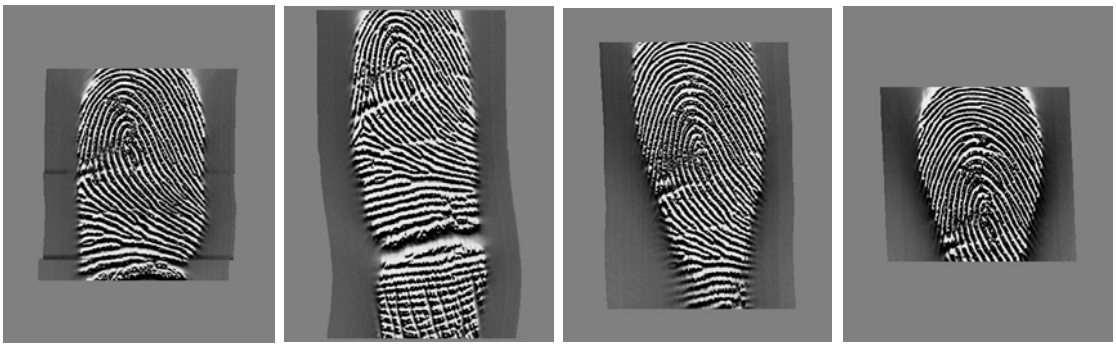


Figura 6.2: Cuatro realizaciones independientes del mismo rasgo biométrico, capturadas con el sensor térmico. Las dos huellas de la izquierda pertenecen a la primera sesión y las de la derecha a la segunda.

Figura 6.3: Cuatro realizaciones independientes del mismo rasgo biométrico, capturadas con el sensor óptico. Las dos huellas de la izquierda pertenecen a la primera sesión y las de la derecha a la segunda.

6.2 Protocolo experimental

Para ajustar y evaluar el sistema de reconocimiento de huella dactilar implementado en este Proyecto, se ha dividido la base de datos DS2 en dos conjuntos independientes, Entrenamiento y Evaluación. A su vez, cada uno de estos grupos se dividen en imágenes de huellas adquiridas con el sensor térmico y con el sensor óptico. Esta división, por tipo de sensor, se debe a que el objetivo de este Proyecto es evaluar el rendimiento de cada sensor por separado, quedando fuera del alcance del mismo las pruebas de interoperabilidad entre sensores.

Para el conjunto de entrenamiento (DS2_Entrenamiento), que se ha utilizado para determinar el punto óptimo de trabajo del sistema, se han seleccionado las 45 primeras personas de la base de datos, aproximadamente un tercio del total, lo que supone 45 personas x 48 muestras = 2.160 huellas dactilares. Mientras que para el conjunto de evaluación (DS2_Evaluación) se han seleccionado las 100 personas restantes (aproximadamente dos tercios del total) lo que supone 100 personas x 48 huellas = 4.800 huellas dactilares. Este conjunto se empleará para obtener las tasas de error del sistema, previamente ajustado con la base de datos de entrenamiento, simulando la diversidad de usuarios que podrían utilizar dicho sistema.

Asimismo el conjunto DS2_Entrenamiento se divide en dos categorías: imágenes capturadas con el sensor térmico e imágenes capturadas con el sensor óptico (DS2_Entrenamiento_Térmico y DS2_Entrenamiento_Óptico respectivamente). De esta manera tendremos 1.080 huellas dactilares térmicas pertenecientes a 45 usuarios y sus equivalentes, 1.080 huellas dactilares capturadas con el sensor óptico. Para el conjunto de evaluación DS2_Evaluación se seguirá el mismo procedimiento, obteniendo finalmente un conjunto de 2.400 huellas dactilares capturadas con el sensor óptico (DS2_Evaluación_Optico) y los mismos dedos capturados con el sensor térmico (DS2_Evaluación_Térmico).

Figura 6.4: Imágenes de la base de datos DS2_Entrenamiento_Óptico pertenecientes a diferentes dedos del mismo usuario.

Para diseñar el protocolo de pruebas, se ha considerado que las huellas pertenecientes a diferentes dedos de un mismo usuario se han tomado como huellas pertenecientes a usuarios distintos (ver Figura 6.4). Esta consideración es válida ya que a pesar de que las huellas de diferentes dedos de un mismo usuario están algo correlacionadas (núcleo y delta) existe una variabilidad entre ellas suficientemente grande para poder identificarlas como diferentes.

En cuanto a las pruebas de verificación, se ha diseñado el mismo procedimiento tanto para las imágenes térmicas como para las ópticas. Realizando, por un lado, las

pruebas con las imágenes térmicas y por otro la pruebas con las imágenes ópticas de los mismos usuarios. Estas pruebas nos proporcionaran dos tipos de puntuaciones:

- *Puntuación de usuarios*: obtenido mediante la comparación de todas las imágenes tomadas con el mismo sensor para cada usuario, sin considerar las comparaciones simétricas (por ejemplo la primera con la segunda y luego la segunda con la primera).
- *Puntuación de impostores*: obtenido mediante la comparación de la primera imagen de un usuario con la primera imagen del resto de usuarios capturadas con el mismo sensor, evitando también comparaciones simétricas.

6.3 Experimentos de entrenamiento

A la hora de diseñar y organizar las pruebas, se ha decidido realizar dos grupos, uno para el sensor óptico y otro para el sensor térmico. De esta manera se intentará optimizar el sistema primero para el sensor óptico, ya que el tener una resolución mayor, a priori tendría que proporcionar mejores resultados, y a continuación ajustarlo para el sensor térmico.

Para la realización de las pruebas de alineación se ha determinado de forma experimental los márgenes de tolerancia para distancias en 8 pixeles y 8 grados para diferencias de orientación. Además, hasta que se indique lo contrario, el sistema trabajará utilizando decimales y considerando las 40 mejores minucias de cada huella.

❖ **Etapa 1: Alineación.**

Descripción: en esta etapa se realiza un desplazamiento de una plantilla sobre la otra con el fin de fin de poder comparar dichas huellas a pesar de no haber sido tomadas colocando el dedo sobre el sensor siempre en la misma posición, como se explicó en la sección 5.3.2. Para realizar la alineación partiremos de nuestra implementación del método propuesto por Mueller y Martini [38] (Sistema de Referencia) y le añadiremos mejoras y aportaciones propias de este Proyecto.

Metodología: para analizar el rendimiento del algoritmo de alineación, basado inicialmente en el método propuesto por Mueller y Martini y a continuación el algoritmo mejorado, se ha hecho uso de los conjuntos de datos DS2_Entrenamiento_Térmico y DS2_Entrenemiento_Óptico. El procedimiento seguido para evaluar la bondad de dichos métodos ha sido calcular cuantas huellas de usuarios legítimos han sido alineadas correctamente y cuantas huellas de impostores han sido descartadas (no alineadas) como no pertenecientes a dicho usuario. Para este propósito los criterios elegidos son:

1. Evaluación del número de usuarios alineados correctamente: se estudia cuantas huellas de usuarios legítimos han sido alineadas, identificadas como pertenecientes a dichos usuarios, según los criterios del método de alineación.
2. Evaluación del número de impostores rechazados (no alineados): se estudia cuantas huellas de impostores han sido descartadas (no alineadas por superar el número máximo de iteraciones).

3. Numero de minucias: para realizar las pruebas de alineación se ha fijado el número de minucias a 40. Más adelante se hará un estudio del impacto de este parámetro en las tasas de acierto del sistema.

Resultados y Conclusiones: en primer lugar estudiaremos los resultados obtenidos con el método de alineación del Sistema de Referencia. En la tabla 6.1 se puede observar como el 100% los usuarios genuinos has sido correctamente alineados con las realizaciones de sus huella, sin embargo, todos los impostores han conseguido hacerse pasar por un usuario genuino según los criterios de alineación. Esto significa que tanto los genuinos como los impostores pasarán a la siguiente fase del proceso de reconocimiento donde se calcularán las minucias coincidentes entre las parejas de plantillas alineadas.

Alineación plantillas	**TÉRMICO** Sistema de Referencia		**ÓPTICO** Sistema de Referencia	
Impostores alineados	1.176	100%	1.176	100%
Impostores rechazados	0	0%	0	0%
Genuinos alineados	870	100%	870	100%
Genuinos rechazados	0	0%	0	0%

Tabla 6.1: Comparación de los resultados obtenidos con el Sistema de Referencia tanto para el sensor óptico como para el térmico.

a **b** **c** **d**

Figura 6.5: Errores en la alineación, entre el impostor a haciéndose pasar por b (imágenes ópticas) y entre el impostor c haciéndose pasar por d (imágenes térmicas).

Para intentar descartar impostores en la etapa de alineación, ver Figura 6.5, se van a añadir condiciones a nuestra implementación del método de Mueller y Martini o Sistema de Referencia con la finalidad de mejorarlo. A continuación se mostraran los resultados del algoritmo mejorado al que llamaremos Sistema de Desarrollo y lo compararemos con el Sistema de Referencia.

- Condición 1: distancia entre las minucias de alineación en cada par de huellas (ver Figura 6.6). Inicialmente el Sistema de Referencia, como se ha explicado en la sección 5.3.2 elige aleatoriamente dos minucias en una de las huellas a

comparar y busca otras dos minucias en la otra huella tomando como criterio que las minucias equivalentes de la otra huella tengan orientaciones similares y una separación entre ellas (las minucias de cada huella entre sí) semejante. A esta condición añadiremos que la distancia entre las minucias de una huella y sus equivalentes en la otra huella se encuentre dentro del margen de tolerancia para distancias. Una vez aplicada esta condición los resultados obtenidos se muestras en la tabla 6.2 donde se aprecia una pequeña mejora de los resultados.

Alineación plantillas	**SENSOR TÉRMICO**				**SENSOR ÓPTICO**			
	Sistema de Referencia		Sistema de Desarrollo		Sistema de Referencia		Sistema de Desarrollo	
Impostores alineados	1.176	100%	1.149	97,70%	1.176	100%	1.119	95,15%
Impostores rechazados	0	0%	27	2,30%	0	0%	57	4,85%
Genuinos alineados	870	0	0%	98,97%	870	100%	863	99,20%
Genuinos rechazados	0	0%	9	1,03%	0	0%	7	0,80%

Tabla 6.2: Tanto para el sensor térmico como para el óptico se muestra la comparativa entre los resultados del Sistema de Referencia y los del Sistema de Desarrollo con la primera mejora.

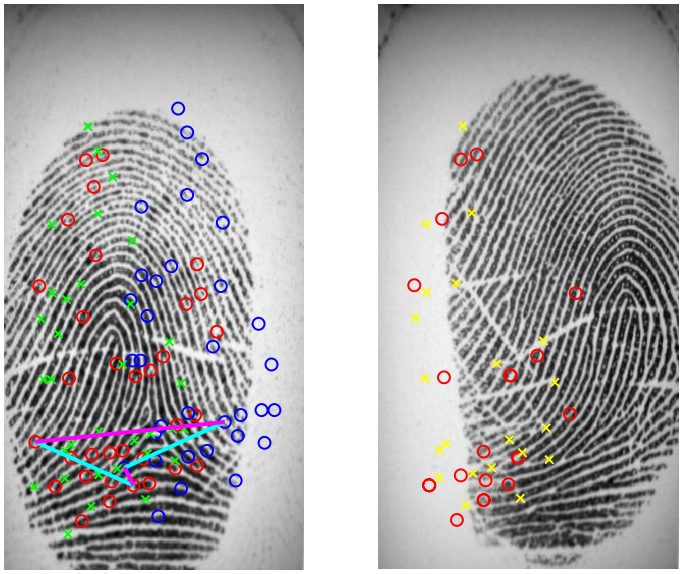


Figura 6.6: Error en la alineación, debido a diferentes distancias entre las minucias de alineación en cada par de huellas (líneas moradas), solucionado añadiendo la condición 1.

- Condición 2: obtención de un paralelogramo: Aun imponiendo la condición 1 siguen ocurriendo errores en la alineación, producidos por cruces en las aristas del paralelogramo formado por las cuatro minucias que determinarán la alineación (ver Figura 6.7). Para corregirlo, se va a añadir una condición que, además de todo lo anterior, sólo considere alineadas las dos huellas si también se cumple que la diferencia en la pendiente de las líneas maestras de

alineación, ver sección 5.3.2, está dentro del margen de tolerancia para ángulos (ver Figura 6.8).

Alineación plantillas	SENSOR TÉRMICO				SENSOR ÓPTICO			
	Sistema de Referencia		Sistema de Desarrollo		Sistema de Referencia		Sistema de Desarrollo	
Impostores alineados	1.176	100%	972	82,65%	1.176	100%	892	75,85%
Impostores rechazados	0	0%	204	17,35%	0	0%	284	24,15%
Genuinos alineados	870	0	837	96,21%	870	100%	841	96,67%
Genuinos rechazados	0	0%	33	3,79%	0	0%	29	3,33%

Tabla 6.3: Comparativa de resultados entre el Sistema de Referencia y nuestro Sistema de Desarrollo aplicando la segunda mejora.

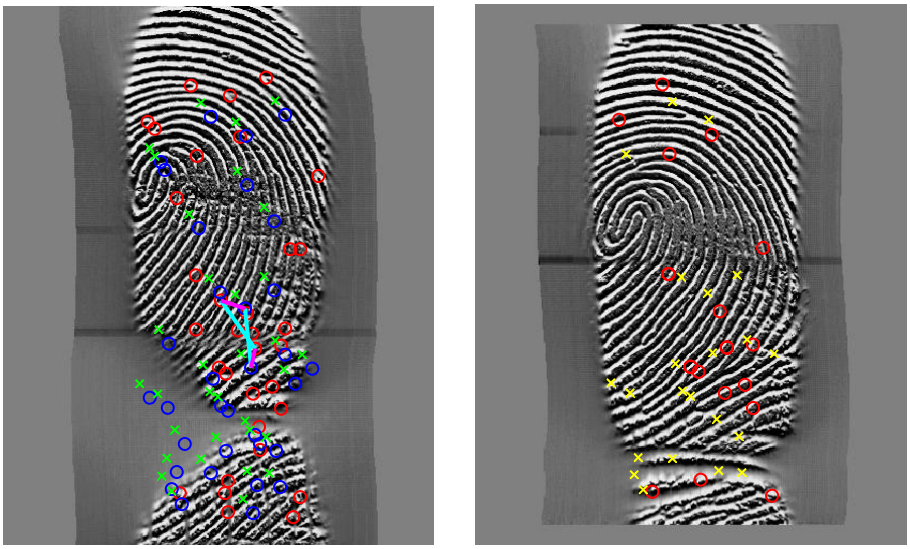


Figura 6.7: Error producido por un cruce entre las aristas del paralelogramo, solucionado cuando se impone la condición 2.

Al imponer esta condición conseguimos aumentar significativamente el número de impostores rechazados, por encima del 15% para el sensor térmico y casi un 25% para el sensor óptico tras añadir la segunda condición. Por otro lado también se observa como el número de usuarios genuinos rechazados incorrectamente también aumenta para ambos sensores, siendo del 3,79% para el sensor térmico y 3,33% para el sensor óptico.

- Condición 3: límite máximo en el desplazamiento entre huellas: por último, deberemos contemplar la posibilidad de que existan huellas de un mismo usuario, pero que debido a errores en la colocación del dedo sobre la superficie del sensor apenas tengan una parte de superficie en común, o que simplemente el programa se confunda y el desplazamiento que determine sea superior a la mitad del tamaña de la imagen, caso en el que no tendríamos ninguna parte en común y por tanto nunca se podría verificar que dos huellas pertenecen a un usuario.

Alineación plantillas	SENSOR TÉRMICO				SENSOR ÓPTICO			
	Sistema de Referencia		Sistema de Desarrollo		Sistema de Referencia		Sistema de Desarrollo	
Impostores alineados	1.176	100%	898	76,36%	1.176	100%	813	69,13%
Impostores rechazados	0	0%	278	23,64%	0	0%	363	30,87%
Genuinos alineados	870	0%	807	92,76%	870	100%	824	94,71%
Genuinos rechazados	0	0%	63	7,24%	0	0%	46	5,29%

Tabla 6.4: Comparativa de resultados entre el Sistema de Referencia y nuestro Sistema de Desarrollo aplicando la segunda mejora.

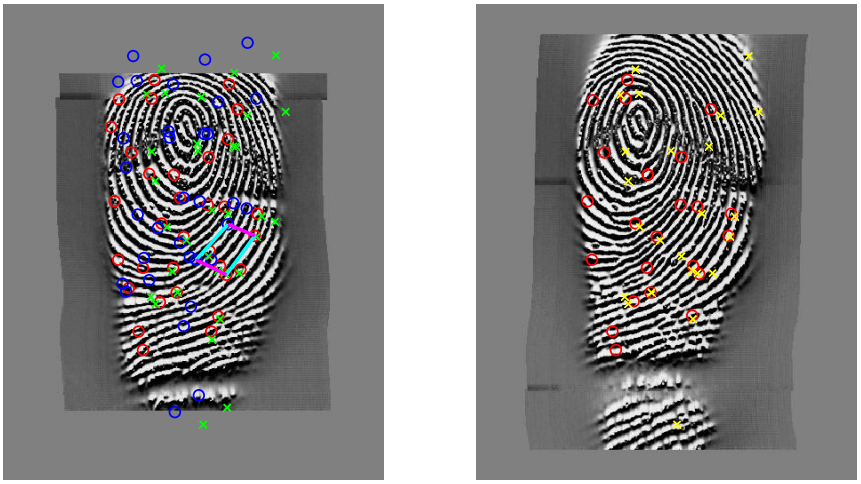


Figura 6.8: Se consigue alinear correctamente las dos plantillas del mismo usuario, formando un paralelogramo cuyas líneas moradas indican el desplazamiento de las minucias azules sobre las rojas.

A la vista de estos resultados, comparándolos con el Sistema de Referencia se aprecia como se ha conseguido mejorar el Sistema de Referencia para alinear dos plantillas. Tas añadir la tercera condición y evaluar los resultados obtenidos en la etapa de alineación, reflejados en tabla 6.4, vemos como ahora el Sistema de Desarrollo es capaz de descartar correctamente a un 23,64% de los impostores en el caso de usar el sensor térmico y un 30,87% de los impostores para el sensor óptico. Por otro lado, al aumentar las restricciones para descartar impostores también se rechaza un pequeño número de usuarios genuinos, que representa el 7,24% de los casos para el sensor térmico y un 5,29% de los intentos para el sensor óptico.

Con estos resultados en la etapa de alineación conseguimos descartar alrededor de uno de cada cuatro impostores, de esta manera no tenemos que calcular la puntuación de similitud para sus plantillas de huellas, mejorando el rendimiento del sistema.

- **Etapa 2: Elección de umbrales:**

Descripción: una vez definido el sistema de alineación, se ha procedido a ajustar los parámetros de tolerancia, que inicialmente se habían establecido empíricamente para la anterior entapa en 8 pixeles y 8 grados para los márgenes de tolerancia en posición y orientación respectivamente. Esta parte es crucial para poder identificar si dos huellas pertenecen al mismo usuario, ya que múltiples realizaciones del mismo dedo van a dar lugar a imágenes diferentes, ligeramente deformadas entre ellas al haber sufrido distintos grados de presión contra el sensor.

Metodología: La estrategia seguida para determinar cuáles son los márgenes, tanto en posición como en orientación, ver Figura 6.9, que ofrecen el mejor rendimiento para el sistema, se basa en utilizar el método de alineación ajustado en la etapa anterior e integrarlo en el sistema de verificación. Una vez alineadas la huellas se calculará el número de minucias coincidentes (ver sección 5.3.3) entre las huellas a verificar y de esta manera tendremos una medida de similitud entre plantillas de huellas que nos permita obtener la tasa de error del sistema (EER, Equal Error Rate) y analizar los resultados.

Para ello se variará el margen de tolerancia en posición desde 5 pixeles hasta un máximo de 25, y para cada uno de ellos se calculará la tasa de error del sistema (EER) variando el margen de tolerancia en orientación desde 5 grados hasta 25. Estas pruebas se realizarán, independientemente para los sensores térmico y óptico, fijando en 40 el número de minucias a tener en cuenta en la alineación y matching y cuantificando los ángulos con 8 bits.

Resultados y conclusiones: si nos fijamos en la tabla Térmico y en la tabla Óptico, del Anexo "Resultados sensor térmico" y "Resultados sensor óptico" respectivamente, podemos ver las tasas de error del sistema en función del margen de tolerancia en posición y ángulo. El código de colores empleado para el relleno de las celdas nos indica los mejores resultados, en verde y las peores tasas obtenidas, en rojo. Además para cada margen de posición, es decir, cada columna, se marca en negrita el mejor resultado. Notar que en ambos sensores, los mejores resultados se obtienen con márgenes de tolerancia inferiores a 12 pixeles, encontrando el punto óptimo de trabajo para el sensor térmico en 6 pixeles de margen de tolerancia en posición y permitiendo una diferencia máxima de 13 grados en la comparación de las orientaciones. Este punto nos ofrece una tasa de error del 24,59%, trabajando con las 40 mejores minucias de cada huella, usando decimales y cuantificando los ángulos con 8 bits. Por otro lado el sensor óptico alcanza su punto óptimo de trabajo cuando fijamos los márgenes de tolerancia en 7 pixeles y 13 grados. Con esta configuración obtenemos una tasa de error de 13,36%, trabajando bajo las mismas condiciones que el sensor térmico, 40 minucias, usando decimales y cuantificando los ángulos con 8 bits.

A la vista de estos resultados observamos como las imágenes obtenidas con el sensor óptico proporcionan mejores resultados que las imágenes capturadas con el sensor térmico para cualquier configuración de parámetros de tolerancia.

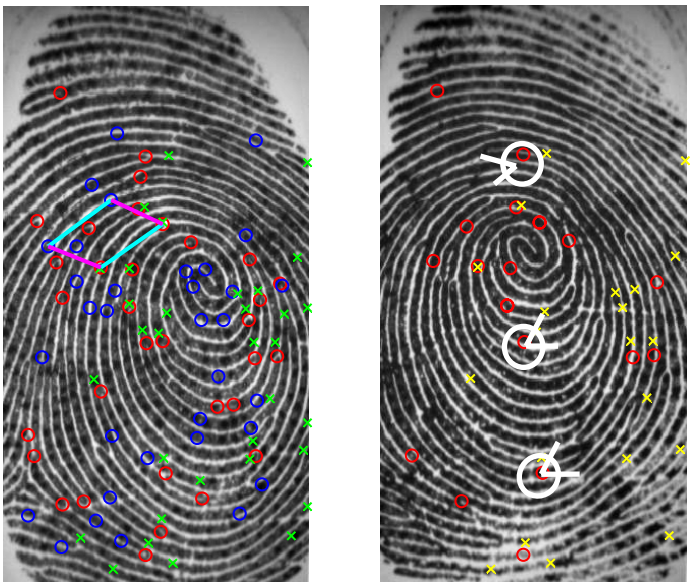


Figura 6.9: Plantillas de un mismo usuario, alineadas correctamente. A la derecha zonas de tolerancia en posición y orientación, para determinar si dos minucias son coincidentes.

- **Etapa 3: cuantificación de los ángulos.**

Descripción: la siguiente etapa de pruebas es la de cuantificación del ángulo con el que definimos la orientación de cada minucia. Para simular las condiciones de trabajo de una tarjeta inteligente se ha limitado el número de bits con los que cuantificar cada ángulo a 6 y 8 bits. De esta manera, para cada uno de los dos conjuntos de datos se ha obtenido como afectaría al rendimiento del sistema si los ángulos que determinan la orientación de cada minucia se cuantificaran con 64 o 256 posiciones para representar los 360 grados. Nótese que la cuantificación a 6 u 8 bits es una restricción muy fuerte que se le impone al sistema, ya que cada uno de los 360 grados de una circunferencia lo podemos descompones en décimas, centésimas... de grado, con lo que con esta condición estamos consiguiendo reducir en gran medida la información necesaria para almacenar los parámetros que representan a una huella, si bien también estamos perdiendo información para discriminar entre ángulos.

Metodología: la metodología aplicada para cuantificar los ángulos se ha basado en diseñar un simulador que permite elegir el número de bits con los que cuantificar dichos ángulos, ver anexo Simulador. Además para estudiar el impacto global sobre el sistema y poder determinar cuál será el punto óptimo de trabajo, las pruebas se realizaran barriendo un margen de 15 a 50 minucias. De esta manera sabremos cual es el número óptimo de minucias para cada cuantificación.

	Sensor Térmico		Sensor Óptico	
Minucias	**6 Bits**	**8 Bits**	**6 Bits**	**8 Bits**
15	46,21	45,92	45,46	44,54
16	44,71	44,48	42,53	41,49
17	43,05	42,53	39,66	38,16
18	42,01	40,57	36,61	34,31
19	39,83	38,20	33,45	30,69
20	37,93	35,73	30,69	28,10
21	36,32	34,25	28,45	24,54
22	34,87	32,50	25,34	21,95
23	33,25	30,41	23,85	20,40
24	31,45	28,79	21,61	17,18
25	30,34	27,91	20,16	16,31
26	29,39	26,56	19,08	15,75
27	28,85	25,77	18,89	15,14
28	28,69	25,09	17,93	14,17
29	28,66	25,18	17,64	13,43
30	28,18	25,02	17,30	12,70
31	26,95	24,55	16,49	12,39
32	26,96	25,07	17,27	13,40
33	27,48	24,72	**14,95**	**10,97**
34	**26,46**	24,01	16,42	11,80
35	27,33	**23,20**	15,67	12,05
36	26,89	25,04	16,30	12,31
37	27,23	24,34	16,08	13,47
38	27,20	24,18	16,09	13,39
39	27,88	24,22	15,81	13,00
40	26,92	24,59	15,65	13,36
41	28,90	26,74	17,71	14,23
42	27,06	25,88	17,24	14,23
43	27,36	25,68	18,08	15,46
44	28,75	25,97	18,34	15,66
45	29,11	26,25	17,80	14,73
46	28,40	26,61	17,78	15,44
47	29,29	27,44	17,81	15,42
48	30,42	28,05	19,54	16,61
49	31,51	27,71	18,94	16,29
50	29,89	26,93	19,81	16,92

Tabla 6.5: Tasas de error variando el número de minucias para cuantificaciones de 6 y 8 bits en los ángulos. Mínimo marcado en negrita.

Resultados y conclusiones: una vez conocidos los resultados para cada una de las dos cuantificaciones, y a su vez para ambos conjuntos de datos podemos estudiar no sólo el efecto que supone limitar el número de posibles valores que pueden tomar los

ángulos, sino cual es el numero óptimo de minucias a tener en cuenta durante la fase de alineación y calculo de similitud (match score).

Si observamos la tabla 6.5, y realizamos un estudio global sobre los datos obtenidos, nos damos cuenta de que no por usar un número mayor de minucias en los cálculos de alineación y similitud se consiguen mejores resultados de rendimiento. Esto se debe a que al aumentar el número de minucias, por encima de un límite, crece la complejidad de los cálculos para alinear dos huellas y por tanto se obtienen peores resultados. El caso contrario lo observamos al intentar realizar la verificación de dos huellas limitando mucho el número de minucias a utilizar. En este caso las tasas de error se disparan, debido a que el sistema tiene problemas para alinear plantillas con menos de 25 minucias. Esto ocurre porque puede que las n mejores minucias de una huella no sean exactamente las m mejores minucias de la huella con la que va a ser comparada, lo que puede implicar que el sistema no tenga suficientes minucias con correspondencia en ambas huellas, a pesar de que pertenezcan al mismo usuario.

Si nos centramos en las columnas que representan las tasas de error del sistema para el sensor térmico, vemos como el punto óptimo de trabajo, es decir, el número de minucias que intervendrán en el proceso, depende d la cuantificación utilizada. De esta manera, con 34 minucias, obtenemos la mínima tasa de error, 26,46%, para una cuantificación de 6 bits, mientras que para 8 bits el mejor rendimiento del sistema lo encontramos en 33 minucias, con una tasa de error del 23,02%. Este hecho permite conseguir mejores resultados para el sistema de verificación que si empleásemos, por ejemplo 40 minucias (como se venía haciendo en las etapas de ajuste del sistema), lo que se traduce en una disminución de operaciones, ya que se reduce el número de posibles combinaciones, minimizando el espacio de almacenamiento y consecuentemente aumentando el rendimiento del sistema.

Para el sensor óptico se obtiene una curva de tendencia similar, localizándose los mejores resultados entre 28 y 40 minucias, fuera de este rango la tasa de error se dispara, sobre todo si disminuimos significativamente el número de minucias que tomaran parte en la verificación. De esta manera el punto óptimo de trabajo lo encontraríamos utilizando 33 minucias, independientemente de la cuantificación utilizada, y nos proporcionará una tasa de error del 14,95% en el caso de emplear 6 bits y 10,95% de error si se cuantifica la información con 8 bits.

Además, como cabria esperar, fijando el tipo de sensor, los resultados son mejores para el uso de 8 bits en la cuantificación de los ángulos que si utilizamos 6 bits. Esto se pone de manifiesto a lo largo de toda la zona de estudio, obteniendo las mejores tasas de error en el intervalo de 28 a 40 minucias.

Comparando ambos sensores se aprecia como el sensor óptico ofrece unos resultados mejores que el sensor térmico, esto se debe a la mayor resolución del sensor óptico y sobre todo a la facilidad con la que se toman las imágenes de las huellas dactilares con este último. Por el contrario, el sensor térmico al necesitar que el propio usuario desplace su dedo sobre su pequeña superficie, es mucho más sensible al ruido y dependiente de la habilidad del usuario para utilizarlo. Todo esto provoca peores resultados en el sistema de verificación.

- **Etapa 4: uso de decimales.**

Descripción: otra posible restricción de los entornos Match-on-Card es su probable limitación para el uso de decimales a la hora de ejecutar operaciones matemáticas. Esto se debe a la limitación de ciertos chips para realizar operaciones en coma flotante, lo que implicará que el algoritmo de verificación tenga que trabajar perdiendo la información de los decimales en cada operación, y así simular este entorno.

Metodología: para estudiar el impacto del uso o no de decimales, se ha adaptado el algoritmo de reconocimiento de huellas para trabajar, por un lado, utilizando hasta cuatro decimales en cada operación y por otro realizando los cálculos necesarios sin la parte decimal.

Además, se ha hecho un estudio del uso de decimales cuantificando los ángulos a 6 y 8 bits, tanto para el conjunto de huellas térmicas como el conjunto de huellas obtenidas con el sensor óptico.

Resultados y conclusiones: a la vista de los resultados obtenidos en la tabla 6.6 para cada uno de los dos sensores y para cada cuantificación de ángulos observamos como la tasa de error empeora ligeramente cuando no se permite el uso de decimales. Con ello confirmamos los datos esperados, en condiciones más limitadas las tasas de error empeoran.

Aunque debemos fijarnos en que dichos valores se mantienen muy próximos a los obtenidos cuando se trabaja con 4 decimales en cada operación. Estas diferencias en las tasas de error, entre uso o no de decimales, se hacen menores cuando el número de minucias utilizado para realizar las comparaciones está fuera del rango óptimo, como hemos definido anteriormente entre 28 y 40 minucias. Esto se debe a que fuera de este rango la ausencia de decimales no es la principal limitación, sino la dificultad que sufre el sistema para realizar el proceso de verificación cuando el volumen de minucias en grande o pequeño.

Notar que la restricción a la hora de cuantificar los ángulos es mucho mayor, en términos de rendimiento del sistema, que la restricción del uso de decimales, ya que como se muestra en la tabla 6.6, para un número fijo de minucias, los resultado para 6 bits de cuantificación y uso de decimales son siempre peores que los obtenidos para 8 bits sin decimales.

A continuación se muestra gráficamente el funcionamiento del sistema de Desarrollo con el conjunto de datos de entrenamiento. En la Figura 6.10 tenemos los resultados obtenidos para ambos sensores, trabajando sin decimales y en la Figura 6.11 las mismas tasas de error (EER) trabajando con decimales.

	Sensor Térmico				Sensor Óptico			
	Cuantificación 6 Bits		Cuantificación 8 Bits		Cuantificación 6 Bits		Cuantificación 8 Bits	
Minucias	*SIN Decimales*	*CON Decimales*	*SIN Decimales*	*CON Decimales*	*SIN Decimales*	*CON Decimales*	*SIN Decimales*	*CON Decimales*
15	46,26	46,21	46,03	45,92	45,96	45,46	44,94	44,54
16	45,00	44,71	44,54	44,48	43,32	42,53	41,78	41,49
17	43,22	43,05	42,87	42,53	40,50	39,66	38,51	38,16
18	41,90	42,01	40,52	40,57	37,40	36,61	34,77	34,31
19	39,54	39,83	38,09	38,20	33,78	33,45	30,86	30,69
20	37,82	37,93	36,02	35,73	31,36	30,69	28,33	28,10
21	36,38	36,32	34,60	34,25	28,83	28,45	24,66	24,54
22	34,87	34,87	32,86	32,50	25,96	25,34	22,13	21,95
23	32,96	33,25	30,99	30,41	24,58	23,85	20,46	20,40
24	31,43	31,45	29,12	28,79	21,99	21,61	17,64	17,18
25	30,46	30,34	28,40	27,91	20,71	20,16	16,71	16,31
26	29,72	29,39	26,86	26,56	19,35	19,08	15,69	15,75
27	28,83	28,85	26,08	25,77	18,93	18,89	15,77	15,14
28	28,63	28,69	25,24	25,09	17,45	17,93	14,67	14,17
29	28,73	28,66	25,29	25,18	17,63	17,64	13,84	13,43
30	27,99	28,18	25,56	25,02	17,01	17,30	12,60	12,70
31	**26,85**	26,95	24,23	24,55	16,42	16,49	12,52	12,39
32	27,09	26,96	25,16	25,07	16,95	17,27	13,41	13,40
33	27,61	27,48	24,97	24,72	**15,70**	**14,95**	**11,54**	**10,97**
34	26,87	**26,46**	24,33	24,01	16,36	16,42	12,00	11,80
35	27,93	27,33	**23,65**	**23,20**	**15,70**	15,67	11,98	12,05
36	27,18	26,89	24,52	25,04	16,50	16,30	12,17	12,31
37	27,03	27,23	23,71	24,34	16,52	16,08	13,55	13,47
38	27,52	27,20	23,94	24,18	16,48	16,09	13,62	13,39
39	27,75	27,88	24,21	24,22	15,84	15,81	13,15	13,00
40	27,15	26,92	24,38	24,59	16,03	15,65	13,02	13,36
41	28,50	28,90	26,61	26,74	17,57	17,71	13,64	14,23
42	26,98	27,06	26,09	25,88	17,86	17,24	13,74	14,23
43	27,69	27,36	26,16	25,68	17,87	18,08	14,98	15,46
44	28,68	28,75	25,73	25,97	18,04	18,34	15,41	15,66
45	29,25	29,11	26,55	26,25	17,45	17,80	14,65	14,73
46	28,95	28,40	26,94	26,61	17,75	17,78	14,67	15,44
47	29,45	29,29	26,85	27,44	18,18	17,81	15,01	15,42
48	30,27	30,42	27,75	28,05	20,10	19,54	16,83	16,61
49	31,13	31,51	27,97	27,71	19,47	18,94	15,69	16,29
50	30,38	29,89	27,25	26,93	19,56	19,81	16,84	16,92

Tabla 6.6: Tasas de error variando el número de minucias para cuantificaciones de 6 y 8 bits en los ángulos trabajando con y sin decimales. Mínimo marcado en negrita.

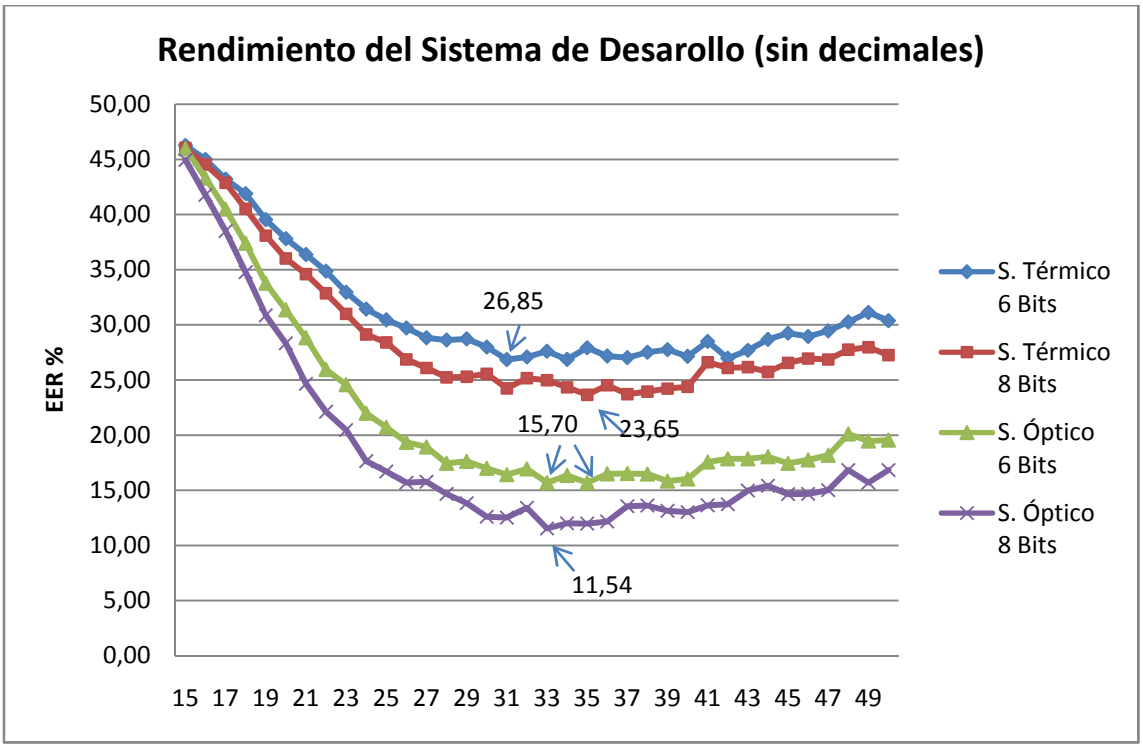


Figura 6.10: Evaluación del rendimiento del Sistema de Desarrollo, tanto para el sensor óptico como el térmico, con cuantificación de 6 y 8 bits trabajando sin decimales.

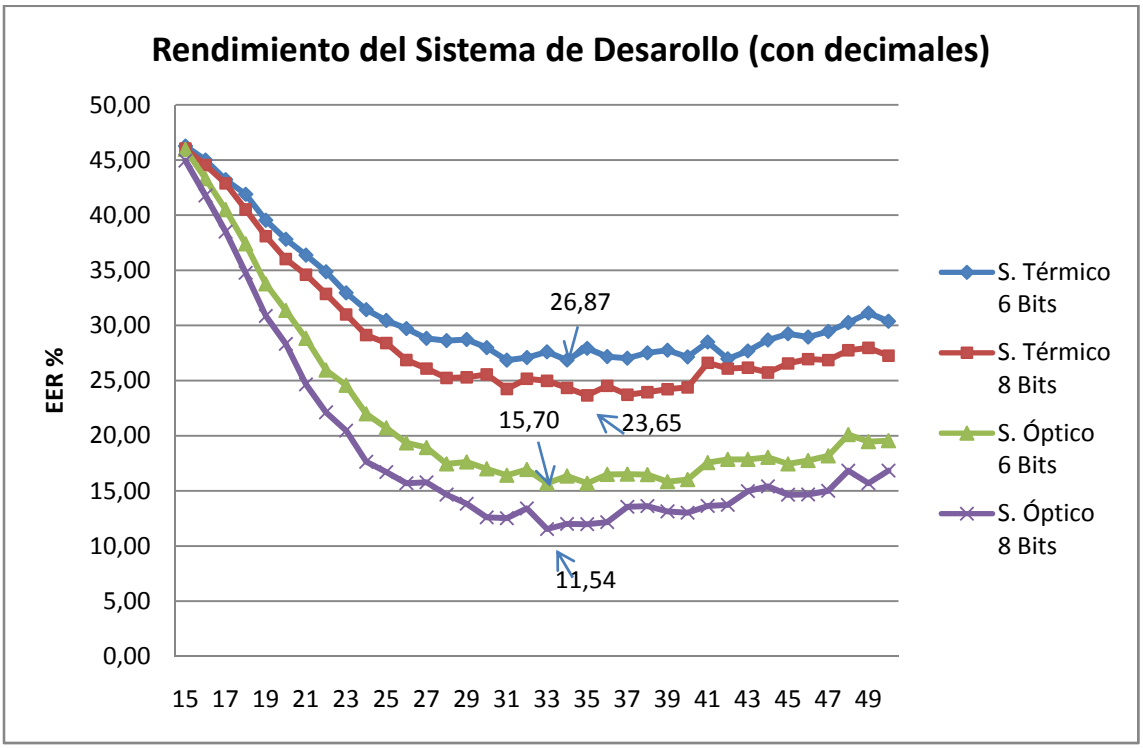


Figura 6.11: Evaluación del rendimiento del Sistema de Desarrollo, tanto para el sensor óptico como el térmico, con cuantificación de 6 y 8 bits utilizando decimales.

6.4 Evaluación del sistema

Para validar el desarrollo y los ajustes realizados a lo largo de este Capítulo, se mostrará el rendimiento del sistema completo sobre los conjuntos de datos de evaluación, DS2_Evaluación, tanto para el sensor térmico como para el sensor óptico. Notar que este conjunto de imágenes no han sido utilizados en los ajustes previos. También mostraremos el rendimiento del sistema original o Sistema de Referencia a modo de comparación.

En primer lugar, en la tabla 6.7 se muestran los resultados del proceso de alineación, sobre los conjuntos de evaluación (térmico y óptico) de acuerdo con los criterios que hemos definido en la Etapa 1 de ajustes de alineación. Si comparamos los resultados con los obtenidos sobre los conjuntos de entrenamiento, tabla 6.4, vemos que el sistema es capaz de rechazar a más del 50% de los impostores, mejorando el rendimiento de la alineación. Por otro lado la tasa de alineación de usuarios genuinos se ve ligeramente reducida, obteniendo peores resultados con el sensor térmico.

Alineación plantillas	**SENSOR TÉRMICO**				**SENSOR ÓPTICO**			
	Sistema de Referencia		Sistema de Desarrollo		Sistema de Referencia		Sistema de Desarrollo	
Impostores alineados	4.656	100%	2222	47,72	4.656	100%	2156	46,31%
Impostores rechazados	0	0%	2.434	52,28	0	0%	2.500	53,69%
Genuinos alineados	1.738	99,89%	1.299	74,66	1.740	100%	1.515	87,07%
Genuinos rechazados	2	0,11%	441	25,34	0	0%	225	12,93%

Tabla 6.7: Comparativa de resultados entre el Sistema de Referencia y nuestro Sistema de Desarrollo aplicando la segunda mejora.

A continuación mostraremos el rendimiento del sistema completo en términos de EER tanto para el sensor térmico como para el óptico, cuantificando los ángulos con 6 y 8 bits para cada caso utilizando o no decimales. Notar que todas las tasas de EER se han calculado utilizando la configuración de los parámetros realizada a lo largo de este capítulo y el número de minucias que ofrecía el mejor rendimiento con los datos de entrenamiento. Los resultados se detallan en la tabla 6.8. Observamos que el rendimiento de ambos sistemas empeora, manteniendo no obstante las mismas diferencias relativas entre los mismos.

TIPO	Cuantificación 6 Bits		Cuantificación 8 Bits	
	SIN Decimales	CON Decimales	SIN Decimales	CON Decimales
Sensor Térmico	31,05 a 31 minucias	30,05 a 34 minucias	29,12 a 35 minucias	28,65 a 35 minucias
Sensor Óptico	19,74 a 33 minucias	20,02 a 33 minucias	15,92 a 33 minucias	15,76 a 33 minucias

Tabla 6.8: Tasas de error del Sistema de Reconocimiento para las configuraciones mostradas.

7. Conclusiones y trabajo futuro

En el presente Proyecto se ha estudiado, desarrollado, implementado y documentado un sistema de reconocimiento de huella dactilar, capaz de simular las condiciones en las que tendría que trabajar un algoritmo de verificación de huella que se ejecutara en un entorno con capacidades limitadas. De esta manera conseguimos realizar el proceso de verificación en un entorno seguro.

Para abordar este Proyecto se ha partido de la metodología propuesta por Mueller y Martini [38], donde se describe un método "ligero" para alinear y comparar huellas. El principal objetivo de dicho método es conseguir alinear dos plantillas de huellas dactilares utilizando el menor número de operaciones y recursos posible. De esta forma se ha implementado el método propuesto por Mueller y Martini en Matlab y se ha tomado como sistema de referencia en el proceso de alineación. Partiendo de este sistema se ha conseguido optimizarlo, tal y como se explica en la etapa de alineación del capítulo 6, consiguiendo por un lado, detectar y rechazar un porcentaje alto de impostores y por otro, mejorando la precisión y fiabilidad de la alineación entre plantillas de un mismo usuario.

Los resultados experimentales de la etapa de alineamiento indican que las modificaciones introducidas al sistema original mejoran el rendimiento del sistema completo. Esto se debe a que las mejoras añadidas, que suponen muy pocas operaciones extra, permiten descartar un gran número de impostores, para los cuales ya no será necesario calcular el número de minucias coincidentes, siendo descartados por el sistema.

Además para mejorar la parte del "Matching" o cálculo de similitud entre plantillas se ha realizado un gran número de pruebas, para determinar los parámetros de tolerancia que permitan identificar dos minucias como correspondientes y al mismo tiempo sea capaz de detectar si dos minucias por próximas que se encuentren, una vez alineadas y desplazadas las plantillas, no son equivalentes.

Los experimentos para evaluar el sistema propuesto se han realizado con la base de datos Biosecure Multimodal Database [4], la cual nos ha permitido evaluar el sistema con imágenes de huellas obtenidas con dos tipos de sensores, térmico y óptico. Todas las pruebas y ajustes se han realizado utilizando cada grupo de imágenes independientemente, para así poder optimizar el rendimiento del sistema adaptándolo al sensor con el que va a trabajar, y proporcionando los resultados del rendimiento alcanzado con cada uno.

Como trabajo futuro se propone estudiar la interoperabilidad entre sensores, simulando escenarios donde la fase de registro se realice con un tipo de sensor y la de verificación utilice huellas capturadas con un tipo distinto de sensor. Esto ofrecería grandes posibilidades, ya que el sistema sería independiente del hardware con el que fue adquirida la imagen, y de esta manera podría operar en diferentes entornos que compartieran la interfaz con la tarjeta.

Por otro lado también se ha estudiado otras posibles restricciones que pudiera sufrir el entorno Match-on-Card. Una de ellas la cuantificación que utiliza cada sistema para almacenar la información de los ángulos. Los resultados obtenidos con diferentes cuantificaciones se analizan en la etapa 3 del capítulo 6, donde se muestra una comparativa del rendimiento del sistema. Además se ha simulado el funcionamiento del sistema en el caso de que el chip obligue a operar sin decimales.

Finalmente, este Proyecto nos ha permitido simular un sistema de reconocimiento de huella dactilar, optimizado para trabajar en entornos con restricciones de capacidad de cálculo y almacenamiento, ofreciendo la posibilidad de limitar el sistema en función de las características del hardware donde va a ser ejecutado. Como consecuencia, este Proyecto ofrece un amplio abanico de posibilidades, al poder seguir mejorando el sistema y adaptándolo a vigentes o futuras plataformas móviles que puedan surgir.

Glosario de acrónimos

ADN Ácido Desoxirribonucleico, molécula que almacena la información genética de cada individuo.

AFIS Automated Fingerprint Identification System, Sistema Automático de Identificación de Huellas Dactilares utilizado por las principales policías del mundo.

BIT Contracción de Binary digIT. Es la parte más pequeña de información que es capaz de procesar un ordenador.

CCD Carged Coupled Device. Dispositivo de carga acoplada. Sensor microeléctrico de estado sólido sensible a la luz.

CMOS Tecnología de semiconductores utilizada como sistema de captación de imágenes. No está tan extendido como el CCD, aunque consume menos potencia.

CPU Central Processing Unit. Es la unidad central de procesamiento.

DET Detection Error Tradeoff.

DNI Documento Nacional de Identidad.

DSP Digital Signal Processor o Procesamiento Digital de Señales .

EEPROM Electrically-Erasable Programmable Read-Only Memory, ROM programable y borrable eléctricamente.

EER Equal Error Rate, tasa de equierror.

FA Falsa Aceptación.

FBI Federal Bureau of Investigation. Es la Oficina Federal de Investigación.

FPGA Field Programmable Gate Array. Es un dispositivo semiconductor que contiene bloques de lógica programables.

FR Falso Rechazo.

FVC Fingerprint Verification Competition. Es la mayor competición mundial para la evaluación de algoritmos de reconocimiento de huella dactilar.

IEC International Electrotechnical Commission. Es la Comisión Electrotécnica Internacional.

ISO International Standard Organization. Es la Organización Internacional para la Estandarización.

LCD Liquid Cristal Display. Es una pantalla de cristal líquido.

LED Light Emission Diode. Es un Diodo emisor de luz.

MoC Match-on-Card, comparación de huellas en una tarjeta inteligente.

NIST National Institute of Standards. Es el Instituto Nacional de Normas y Tecnología .

PDAs Personal Digital Assistant. Asistente Digital Personal. Es un híbrido de reducido tamaño entre los ordenadores portátiles y las agendas electrónicas.

PFC Proyecto Fin de Carrera.

PIN Personal Identification Number o Número de Identificación Personal.

RAM Random Access Memory.

ROM Read-Only Memory, que significa "memoria de sólo lectura".

USB Universal Serial Bus o bus universal en serie. Es una interfaz de tipo serie que permite conectar hasta 127 dispositivos a un ordenador.

Bibliografía

[1] Anil K. Jain, Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition". IEEE Trans. Circuits Syst. Video Techn., 1(2):125_143, 2006.

[2] J. Galbally, J. Fierrez, J. Ortega-García, M. Freire-Santos, M. Martinez-Diaz, J. Gonzalez-Rodriguez and J. A. Sigüenza-Pizarro, "Match-on-Card State of the Art", *Technical report, Biometric Recognition Group – ATVS*, December 2007.

[3] Historia de la biometría, disponible en: http://www.monografias.com/trabajos43/biometria/biometria.shtml/

[4] Javier Ortega-Garcia et al., "The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB)", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2009 (to appear).

[5] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. "Handbook of Fingerprint Recognition". Springer, New York, 2003.

[6] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. "Handbook of Multibiometrics (International Series on Biometrics)". Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[7] Hospital de ValleyCare, disponible en: http://www.valleycare.com/

[8] Artículo del Chicago Tribune, disponible en: http://www.chicagotribune.com/

[9] Artículo de Tech Radar, disponible en: http://www.gulf-daily-news.com/Story.asp?Article=234324&Sn=BNEW&IssueID=31234

[10] National Institute of Standars and Technology, disponible en: http://www.nist.gov/

[11] Seguridad en el Aeropuerto Internacional de Bahréin, disponible en: http://www.gulf-daily-ews.com/Story.asp?Article=234324&Sn=BNEW&IssueID =31234

[12] Biografía Dr. Oloriz, disponible en: http://es.wikipedia.org/wiki/Federico_Ol%C3%B3riz_Aguilera

[13] Biografía de Alfonso Bertillón, disponible en: http://es.wikipedia.org/wiki/Bertill%C3%B3n

[14] Biografía de Juan de Vucetich, disponible en: http://es.wikipedia.org/wiki/Vucetich

[15] Resolución del primer caso policial utilizando huellas dactilares, disponible en: www.nlm.nih.gov/ y http://www.nlm.nih.gov/visibleproofs/galleries/cases/vucetich.html

[16] Biografía de Francisco Galton, disponible en: http://es.wikipedia.org/wiki/Francisco_Galton

[17] Dactiloscopia, estudio sobre la huella dactilar, disponible en: http://es.wikipedia.org/wiki/Dactiloscopia

[18] E. Henry. "Classification an Uses of Finger Prints", *Routledge*, London, 1900.

[19] M. Kawagoe, A. Tojo. "Fingerprint Pattern Classification. Pattern Recognition", 17:295-303, 1984.

[20] D. Maltoni. "A Tutorial on Fingerprint Recognition, Advanced Studies in Biometrics. Summer School on Biometrics", Alghero, Italy, June 2003. M. Tistarelli, J. Bigun, E. Grosso (Eds.), LNCS 3161 Springer, 2005.

[21] D. Maio, D. Maltoni. "Direct Gray-Scale Minutiae Detection in Fingerprints". IEEE Trans. On Pattern Analysis and Machine Intelligence, 19(1), 1997.

[22] J. Ortega, J. Fierrez, D. Simon, J. Gonzalez, et al. "MCYT Baseline Corpus: A Bimodal Biometric Database". IEE Proc. Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet, 150(6):395-401, 2003.

[23] FVC2006: the Fourth International Fingerprint Verification Competition, disponible en http://bias.csr.unibo.it/fvc2006

[24] X. Jian, W.Y. Yau. "Fingerprint Minutiae Matching Based on the Local and Global Structures". Proc. Int. Conf. On Pattern Recognition (15th). 2:1042-1045, 2000.

[25] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. Ortega-Garcia. "A review of schemes for fingerprint image quality computation". Proc. 3rd COST-275 Workshop on Biometric on the Internet, COST275, 3-6, Official Publisher of the European Communities, Hatfield, UK, October 2005

[26] J. Fierrez-Aguilar, L.M. Muñoz-Serrano, F. Alonso-Fernandez and J. Ortega-Garcia, "On the effects of image quality degradation on minutiae and ridge-based automatic fingerprint recognition". Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST, IEEE Press, 79-82, Las Palmas de Gran Canaria, Spain, October 2005

[27] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia and A.K. Jain. "Incorporating image quality in multi-algorithm fingerprint verification". Proc. IAPR Intl. Conf. on Biometrics, ICB, Springer LNCS-3832, 213-220, Hong Kong, January 2006

[28] ISO/IEC: FDIS 19794-2, Biometric data interchange Formats. Part 2: Finger minutiae data, ISO/IEC JTC1 SC37, 2005

[29] Información del sistema MIMEX: http://fingerprint.nist.gov/MINEX/

[30] Información del sistema NPIVP: http://csrc.nist.gov/groups/SNS/piv/npivp/index.html

[31] Información de los modelos y estándares FIPS201: http://www.fips201.com/

[32] Nist MOC, disponible en: http://csrc.nist.gov/groups/SNS/piv/documents/NIST-BMOC-Test-Approach.pdf

[33] Sung B. Pan, D. Moon, and others, “An ultra-low memory fingerprint matching algorithm and its implementation on a 32-bit smart card”, in Trans. On Consumer Electronics, vol. 49, no. 2, pp. 453-459, 2003-

[34] C. Barral, J.-S. Coron, and D. Naccache, “Externalized Fingerprint Matching”, inProc. ICBA, Springer LNCS 3072, pp. 309-315, 2004.

[35] S. Bistarelli, F. Santani, and A. Vaccarelli, “An asymmetric fingerprint matching algorithm for Java Card”, in Proc. AVBPA, Springer LNCS 3546, pp. 279-288, 2005.

[36] M. Mostafa, “A fast and memory efficient approach for fingerprint authentication system”, in Proc. ICAVSS, pp. 259-263, 2005.

[37] M. Fons, F. Fons, and others, “Hardware-Software co-design of a fingerprint Matcher on-Card”, in Proc ICEIT, pp. 113-118, 2006.

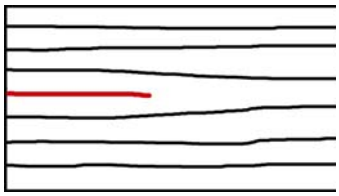
[38] R. Mueller, and U. Martini, “Decision level fusion in standardized fingerprint Match-on-Card,” in Proc. IEEE International Conference on Control, Automation, Robotics and Vision, ICARCV 2006, pp. 185-190, 2006.

Anexos

Puntos característicos

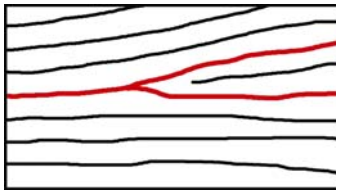
Las crestas papilares [18, 19] no son normalmente unas líneas regulares de trazado continuo que aparezcan en un extremo del lofograma y terminen en el opuesto, por el contrario, lo frecuente es que, en marcha, **sufran irregularidades, accidentes diversos o anomalías conocidas como puntos característicos**, o puntos de Galton.

Abrupta (a). Es la cresta situada entre otras dos paralelas a ella que se interrumpe sin volver a aparecer. El punto característico radica en el extremo de la cresta.

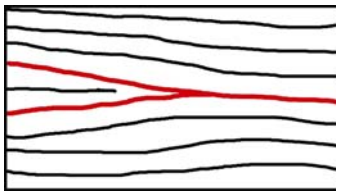


Bifurcación (b). Es el punto en el que **una cresta se transforma en dos paralelas**. La cresta se sigue **en sentido dextrógiro** si es curva y de **izquierda a derecha** si es recta.

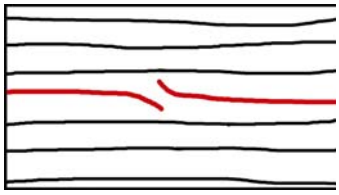
Las crestas que nacen en la bifurcación se denominan ramas, siendo superior o inferior, externa o interna, según la posición que ocupen en el dibujo. Atendiendo a su longitud pueden ser: iguales o desiguales y pequeñas o grandes.



Convergencia (c). Es el **punto de confluencia de dos crestas paralelas que se transforman en una sola**. La forma de seguir la resta y la clasificación de las ramas son idénticas a las señaladas para la bifurcación.

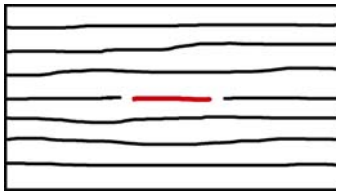


Desviación (d). Forman esta figura dos crestas abruptas, de la misma dirección pero de sentidos opuestos, que se aproximan y, cuando están muy próximas, se desvían en sentido oblicuo de la dirección que traen, para quedar paralelas y separadas por un surco interpapilar.

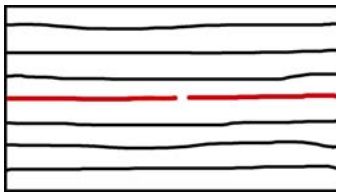


Empalme (e). Existe cuando dos crestas paralelas quedan unidas por un fragmento oblicuo que forma con ellas ángulos muy agudos.

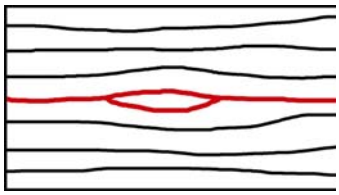
Fragmento (f). **Es la cresta con los dos extremos abruptos**. Si la longitud es inferior a cinco veces su anchura, **es pequeña**, y si está comprendida entre cinco y diez, **grande**. La cresta que excede de esta longitud **pierde su consideración de fragmento para definirse como cresta de extremos abruptos.**



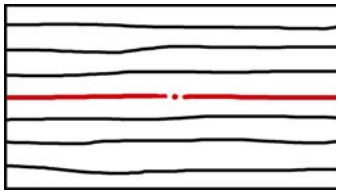
Interrupción (i). Se produce cuando una cresta desaparece en un punto cualquiera, para volver a reaparecer inmediatamente. El espacio en blanco que aparece entre los extremos abruptos ha de tener una longitud aproximada de dos veces la anchura de la cresta. Sólo se consideran como tales las interrupciones naturales.



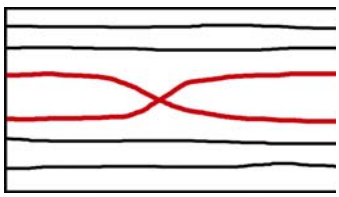
Ojal (o). Figura cerrada y en blanca formada por una bifurcación seguida de una convergencia. Sus dimensiones se miden según las normas dadas para el fragmento.



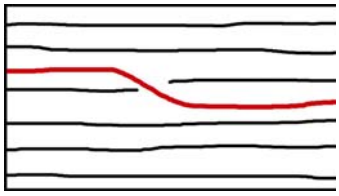
Punto (p). Es el fragmento de igual longitud que anchura.



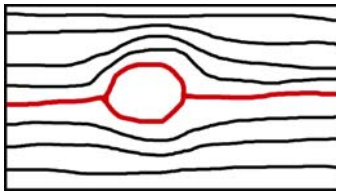
Secante (s). Es el punto formado por dos crestas paralelas que se cortan saliendo del encuentro otra vez paralelas, aunque invertidas.



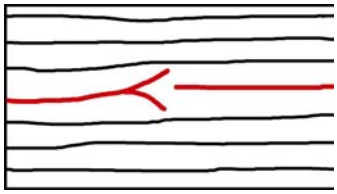
Transversal (t). Se produce este punto cuando **una cresta cambia de dirección bruscamente,** apartándose de la que lleva su sistema, **para seguir la diagonal,** aprovechando la interrupción de su cresta vecina y **retornando de nuevo a la dirección primitiva, al otro lado de la cresta.**



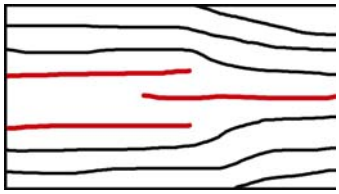
Círculo (ci). Es el ojal circular cuyos diámetros perpendiculares no difieren entre sí más del 10% de su longitud. Puede estar formado por figuras distintas a las que componen el ojal.



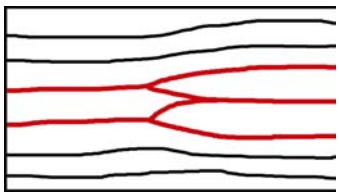
Delta (de). Esta figura puede ser considerada punto característico cuando no esté formada por la aproximación o fusión de las limitantes de los tres sistemas.



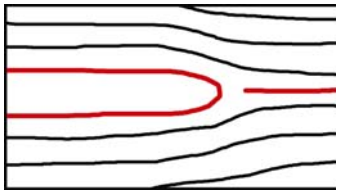
Ensamble (en). Figura formada por tres o más abruptas, dos a dos opuestas e intercaladas que mueren después de rebasar la terminación de las opuestas. El ensamble es simple si tiene tres abruptas, doble si son cuatro y múltiple si son más de cuatro.



M (eme). Esta figura la producen dos bifurcaciones o convergencias que tengan una cresta. Los dos trozos internos de la figura no deben tener una longitud que exceda de cuatro veces su anchura.



Vuelta (v). Es todo asa que no forme el núcleo de un sistema.



Aunque **no hay un acuerdo internacional** sobre el número de puntos característicos exigibles para establecer la identidad entre dos huellas o impresiones, la opinión mayoritaria es que es suficiente con que haya de ocho a doce puntos. **En España la jurisprudencia considera suficientes entre ocho o diez.**

Los servicios de identificación españoles argumentan que **es posible establecer la identidad con un número menos de puntos característicos atendiendo a su valor cualitativo** basándose en la tabla de Florentino Santamaría que realizó un estudio estadístico fijándose en el carácter cualitativo de los mismos, teniendo en cuenta para ello la frecuencia con que aparecen en el dibujo dactiloscópico, con el siguiente resultado:

TABLA DE SANTAMARÍA

Abrupta	53,4%	Ojal	4,2%	Empalme	1,3%
Bifurcación	15,1%	Desviación	2,2%	Transversal	1,3%
Convergencia	13,1%	Punto	2,2%	Secante	0,2%
Fragmento	5,4%	Interrupción	1,6%		

Tabla A.1: Frecuencia de aparición de cada tipo de minucia.

Simulador

DESCRIPCIÓN DEL SIMULADOR

En este anexo se describe el simulador del algoritmo de reconocimiento de huella dactilar para entorno Match-on-Card descrito en el Capítulo 5. Dicho simulador, implementado en Matlab sobre una plataforma PC, permite comprobar los efectos de las limitaciones propias de la tecnología Match-on-Card sobre el rendimiento y la robustez frente ataques, tales como el efecto de la cuantificación de los ángulos, el número de minucias procesadas, o el cómputo en coma fija.

Parámetros

El simulador permite ajustar una serie de parámetros:

- **Número de minucias**: El número de minucias que utiliza el algoritmo de reconocimiento repercute de forma significativa tanto en la tasa de error (efecto positivo) como en el tiempo de ejecución (efecto negativo). Este parámetro permite por tanto estudiar el impacto en estos criterios comunes de evaluación para diferentes restricciones en el número de minucias correspondientes a diferentes sistemas Match-on-Card.

- **Cuantificación de los ángulos**: Las plantillas definidas en el estándar ISO en su versión reducida almacenan la información del ángulo de las minucias cuantificado a 8 ó 6 bits. Para evaluar el efecto de esta pérdida de resolución, el simulador incluye un parámetro que permite modificar la cuantificación.

- **Coma fija / coma flotante**: Debido a las restricciones propias de los procesadores incluidos en las smartcard, en algunos casos los algoritmos deben realizar sus operaciones únicamente con números enteros (coma fija). Para poder estudiar el efecto de la pérdida de resolución en estos casos, se ha incluido un parámetro que permite establecer si se opera en coma fija o flotante, y en el segundo caso el número de decimales de precisión.

Interfaz gráfica

El simulador incluye una interfaz gráfica de usuario que facilita su uso (ver Figuras A.1 y A.2). La interfaz incluye las opciones:

- **Registrar**: Registra una nueva huella en el sistema, que es la que se utilizará en la autenticación.

- **Autenticar**: Realiza la comparación entre la huella registrada y una huella de test. Se permite modificar los parámetros del sistema para estudiar su efecto: número de minucias en la comparación, número de bits de cuantificación de los ángulos y número de decimales en las operaciones.

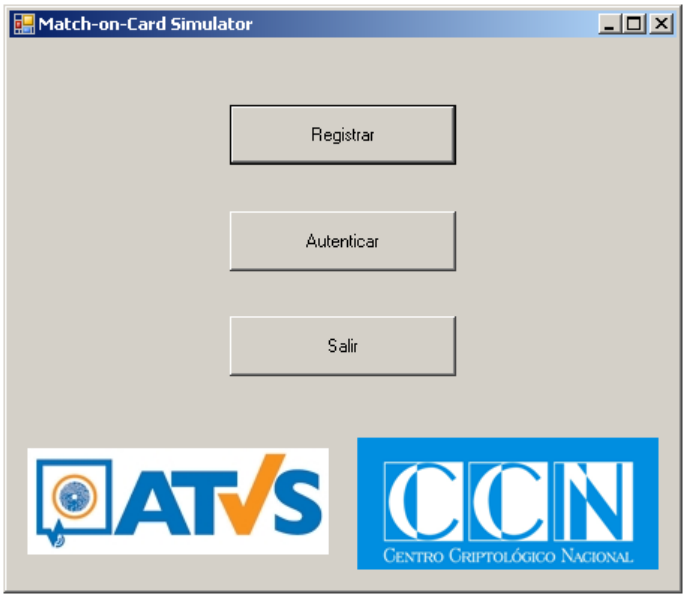


Figura A.1: Menú principal de la interfaz de usuario del simulador, con las opciones de Registrar y Autenticar.

Figura A.2: Interfaz del modo Autenticar.

Línea del tiempo de la biometría

Tecnología	Fecha	Descripción
	6000 A.C.	Almacenamiento de huellas digitales, usado por asirios, babilónicos, japoneses y chinos.
	Siglo XIV	Chinos estampaban las huellas de manos y pies de los niños para identificarlos
	1686	Malpighi identificó diferencias en los patrones de huellas digitales
	1823	Purkine, identificó la naturaleza única de las huellas digitales
	1858	Hershel crea el primer registro de huellas palmares de empleados
	1870	Bertillon desarrolla el sistema de antropometría descriptiva
	28-oct-1880	Faulds publica el artículo “On the Skin-Furrows of the Hand”
	1882 -1890	La policía de Francia utiliza la técnica desarrollada por Bertillon
	1883	Mark Twain publica el libro “life on the Mississippi”
	1-sep-1891	Se empieza a utilizar el método de Juan Vucetich en Argentina
	1892	Francis Galton publica el libro “Finger Prints”
	1892	Se identifica por primera vez por la huella digital a una asesina
	1894	Mark Twain publica el libro “The tragedy of Pudd’nhead Wilson”
	1896	La policía de Bengal implementa el sistema de huella digital
	1900	Scotland Yard adopta el sistema de huellas digitales de Henry
	1902	Denmark Hill en el Reino Unido es conectado con la escena del crimen
	1903	El departamento de policía de New York empieza los archivos de huellas digitales
	1903	Colapsa el sistema Bertillon
	1905-1908	Se implementa el sistema de huellas digitales en las Fuerzas Militares de EEUU
	1918	Locard establece 12 detalles Galton como mínimo para identificación positiva de una persona.
	Sep-1935	Se publica el artículo “A new Scientific Method of Identification”
	1936	Burch propone el concepto de los patrones de iris para reconocimiento
	1955	Se publica el artículo “The fundus Oculi in monozigotic twins: Report of six pairs of identical twins”

Tecnología	Fecha	Descripción
	1960	Publicación modelo de los componentes fisiológicos de la producción del discurso acústico.
	9-mar-1963	Publicación articulo "automatic Comparison of Finger-Ridge Patterns"
	1964-1965	Desarrollo del primer sistema semi-automático de reconocimiento facial.
	1965	Desarrollo del primer sistema de reconocimiento de firma
	1969	El FBI impulsa la automatización del proceso de identificación de huellas digitales.
	1969	Pierce publica un artículo titulado "Whither Speech Recognition?"
	25-nov-1969	Danna patenta un instrumento para identificar la firma
	Década 70s	Goldstein, Harmon y Lesk presentan los primeros resultados en la automatización del reconocimiento Facial
	1970	Perkell modela por primera vez componentes conductuales del discurso
	25-May-1971	Se patenta un sistema de identificación de la palma de la mano
	1974	El primer sistema de reconocimiento de la geometría de la mano estuvo disponible
	1975	FBI desarrollo un prototipo lector de huellas digitales
	1976	Se desarrolla primer prototipo de sistema de reconocimiento del hablante ¿?
	25-may-1976	Patentado un aparato para grabar la firma
	28-jun-1977	Namur patenta un arreglo de reconocimiento de hablante
	12-jul-1977	Se patenta un aparato para identificación personal
	22-ago-1978	Se patenta un aparato y método para identificar individuos a través de sus patrones vasculares de la retina
	Década 80s	NIST crea el grupo de discurso NIST
	1983	James Bond utiliza tecnología de reconocimiento de iris
	1985	Flom y Safir proponen el concepto de que no hay dos iris iguales
	3-feb-1987	Se patenta un sistema de reconocimiento de iris
	31-jul-1987	Se patenta un método para identificar una persona a partir de la geometría de la mano
	1988	El condado de Los Ángeles empieza a usar tecnología de reconocimiento facial
	14-feb-1989	Se patenta un método y aparato para verificar la identidad de un individuo
	Ene-1990	Kirby y Sirovich publican "Application of the Karhunen-loeve procedure for the characterization of human faces"
	1991	Turk y Pentland publican "Eigenfaces for recognition"
	Oct-1992	Primera Reunión de Biometric Consortium

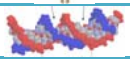
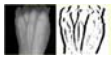
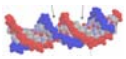
Tecnología	Fecha	Descripción
	1993-1997	Corre el programa FacE REcognition Technology (FERET)
	1993	Se inician trabajos para probar y entregar un prototipo de unidad de reconocimiento de iris.
	31-ago-1993	Patentado método para decodificar símbolos de códigos de barras para escaneos parciales
	7-sep-1993	Patentado sistema para codificar y decodificar datos en una maquina lectora de formas gráficas
	1994	Lockheed Martin es seleccionado para construir el IAFIS del FBI
	1994	Sale al mercado RECOderm™
	1-mar-1994	Daugman patenta un sistema biométrico de identificación personal basado en el análisis del iris
	1995	OKI Electric Industry Ltd. Ofrece cajeros automáticos con reconocimiento de iris en Japón
	1997	Se presenta el proyecto HA-API
	1998	El FBI lanza Combined DNA Index System (CODIS)
	28-jul-1998	Se patenta una identificación biométrica de individuos usando patrones de venas subcutáneas
	1999	La ICAO inicia estudio de la aplicabilidad de los biométricos en MRTD
	Ene-2001	Se usa el sistema de Reconocimiento facial en el Super Bowl en Tampa, Florida
	2000	Se da inicio a la prueba de reconocimiento facial del vendedor (FRVT)
	2001	Se publica un paper sobre el uso de patrones de venas subcutáneas
	2002	Se establece el comité de biométricos en la ISO
	1-feb-2002	Se crea el programa FEARID
	30-may-2002	Patente Colombiana para un “Sistema de Lectura de huellas dactilares”
	2003	Se establece European Biometrics Forum
	30-ene-2004	Se patente en Colombia un “dispositivo portátil que tiene capacidades de autentificación basadas en biometría”
	May-2004	Se da inicio al gran reto del reconocimiento facial (FRGC)
	2005	Expira la patente de Estados Unidos para el concepto de reconocimiento del iris
	2005	Iris on Move™ es anunciado en la Conferencia de Biometrics Consortium por parte de Sarnoff Corporation
	31-may-2005	Termina el programa FEARID
	14-dic-2006	Se patenta un método y aparato para obtener información biométrica del iris de un sujeto en movimiento
	**2007**	Biosecure Multimodal Evaluation Campaign

Tabla A.2: Línea del tiempo.

Leyenda:

 Adn

 Biométricos

 Firma

 Geometría de la mano

 Huella dactilar

 Huella palmar

 Iris

 Pulsaciones de tecla

 Reconocimiento facial

 Retina

 Vascular

 Voz

 Huella de la oreja

ISO 7816

ISO 7816 [28] es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional De Normalización (ISO) y Comisión Electrotécnica Internacional (IEC). Se trata de una extensión de la ISO 7810.

A continuación se describen las diferentes partes de esta norma ISO 7816:

✓ 7816-1: Características físicas

Creado en 1987, actualizado en 1998, modificado en 2003.

En el estándar **ISO/IEC 7816** parte 1 se definen los siguientes tamaños para tarjetas inteligentes, ver Fig. C.1:

- **ID 000**: el de las tarjetas SIM usadas para teléfonos móviles GSM. También acostumbran a tener este formato las tarjetas SAM (*Security Access Module*) utilizadas para la autenticación criptográfica mutua de tarjeta y terminal.
- **ID 00**: un tamaño intermedio poco utilizado comercialmente.
- **ID 1**: el más habitual, tamaño tarjeta de crédito.

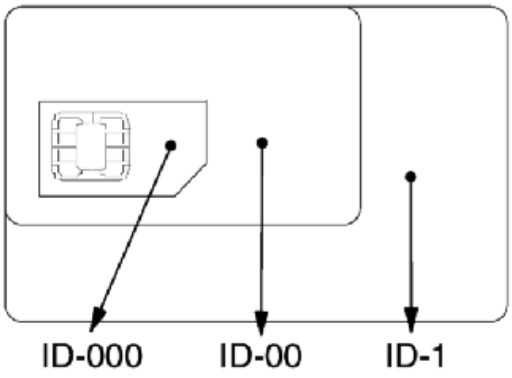


Figura A.3: Tamaño de tarjetas inteligentes.

✓ 7816-2: Tarjetas con contactos - Dimensiones y localización de los contactos

Creado en 1988, actualizado en 1999, modificado en 2004.

Define la posición de los pines en el chip, ver Fig. C.2.

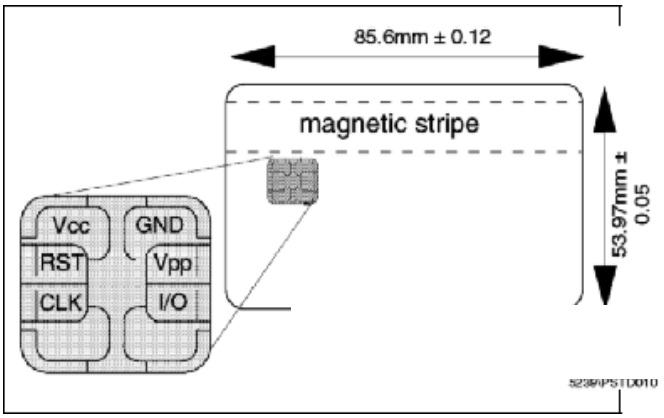


Figura A.4: Contactos del chip de una tarjeta *con contactos*

✓ 7816-4: Organización, la seguridad y los comandos para el intercambio de información

Creado en 1995, actualizado en 2005.

ISO/IEC 7816-4:2005 es independiente de la tecnología de la interfaz física (no sólo se aplica a tarjetas con contactos). Se aplica a las tarjetas de contactos, de proximidad, radiofrecuencia...

El sistema de ficheros descrito en este apartado del estándar es jerárquico como en la mayoría de los sistemas operativos modernos. Los archivos se nombran por un identificador de archivo de dos bytes.

Las tarjetas inteligentes contienen 3 tipos principales de archivos:

- **Archivo Principal (MF)**: es la raíz de la jerarquía. Se identifica por *3F 00* y contiene la información y la lista de los archivos contenidos dentro de ella.
- **Archivo Dedicado (DF)**: son como directorios en las tarjetas inteligentes, subdividen las tarjetas para sostener archivos llamados **Elementary Files (EF)**. Normalmente contienen los datos relativos a una aplicación.
- **Archivo Elemental (EF)**: en los que se almacenan los datos realmente. Pueden ser de cuatro tipos:
- ***Archivo transparente o binario***: sin estructura interna, son sólo almacenes de bytes con un tamaño máximo. Los datos se pueden direccionar con un *offset*.
- ***Archivo lineal de registros de longitud variable***: archivos con una estructura prefijada consistente en una lista de registros individualmente identificables

donde cada uno puede tener una longitud variable (el tamaño se fija en el momento en el que se crea). Los registros son direccionados según el orden de su creación y su número no se puede modificar ya posteriormente.

- ***Archivo lineal de registros de longitud fija***: archivos con una estructura prefijada consistente en una lista de registros individualmente identificables con una longitud fija cada registro. Los registros son direccionados según el orden de su creación y su número no se puede modificar ya posteriormente.
- ***Archivo cíclico de registros***: archivos con una estructura prefijada consistente en un 'anillo' (lista enlazada circular) de registros individualmente identificables cada uno con un ancho fijo. Los registros son direccionados en orden inverso a su creación/modificación.

✓ 7816-5: Registro de la solicitud de los proveedores

Creado en 1995, actualizado en 2004.

ISO/IEC 7816-5 define cómo usar un identificador de aplicación para determinar la presencia y/o realizar la recuperación de una aplicación en una tarjeta.

✓ 7816-6: Interoperabilidad en los elementos de datos para el intercambio

Creado en 1996, actualizado en 2004.

Especifica los elementos de datos utilizados para el intercambio basado en las tarjetas de circuito integrado, con contactos y sin contactos. Se da el identificador, el nombre, la descripción, el formato, la codificación y el diseño de cada elemento de datos y define los medios de recuperación de éstos desde la tarjeta.

✓ 7816-8: Comandos para operaciones de seguridad

Creado en 1995, actualizado en 2004.

Especifica los comandos de las tarjetas (ya sea con o sin contactos) que pueden utilizarse para operaciones criptográficas. Estos comandos son complementarios, y sobre la base de los comandos enumerados en la norma ISO/IEC 7816-4.

La elección y condiciones de utilización de los mecanismos criptográficos pueden afectar a la posibilidad de exportar la tarjeta (debido a las restricciones impuestas en algunos países). La evaluación de la idoneidad de los algoritmos y protocolos está fuera del alcance de la norma ISO/IEC 7816-8.

- ✓ **7816-9: Comandos para la gestión de la tarjeta**

Creado en 1995, actualizado en 2004.

Especifica los comandos de las tarjetas (con contactos y sin contactos) para la gestión de ficheros, por ejemplo la creación y borrado de ficheros. Estos comandos abarcan todo el ciclo de vida de la tarjeta y, por consiguiente, algunos comandos pueden ser usados antes de que la tarjeta ha sido expedida a su titular o después de que ésta haya caducado.

- ✓ **7816-11: Verificación de la identidad personal a través de métodos biométricos**

Creado (o actualizado) en el año 2004.

Especifica el uso de los comandos y de los datos relacionados con la verificación de la identidad de una persona a través de los métodos biométricos en las tarjetas de circuito integrado. Los comandos utilizados se definen en la norma ISO/IEC 7816-4. Los datos se definen parcialmente en esta norma y en parte importados de la norma ISO/IEC 19785-1.

- ✓ **7816-12 Tarjetas con contactos. Interfaz eléctrica USB y procedimientos operativos**

Creado en el año 2005.

Especifica las condiciones de funcionamiento de una tarjeta de circuito integrado a través de una interfaz USB.

ISO/IEC 7816-12:2005 proporciona dos protocolos para controlar las transferencias. Se trata de soportar el protocolo T=0 (versión A) o utilizar la transferencia de APDU (versión B). ISO/IEC 7816-12:2005 proporciona los diagramas de estado para la interfaz USB-ICC para cada una de las transferencias (transferencias a granel, el control de las transferencias versión A y versión B).

- ✓ **7816-15: Aplicación de información criptográfica**

Creado en el año 2004.

Especifica una aplicación que contiene información sobre la funcionalidad criptográfica. Por otra parte, ISO/IEC 7816-15:2004 define una sintaxis común (en ASN.1) y el formato de codificación de la información y los mecanismos para compartir esta información cuando sea apropiado.

ISO/IEC 7816-15:2004 es compatible con las siguientes capacidades:

- Almacenamiento de múltiples claves de información criptográfica en una tarjeta.
- Uso de la información criptográfica.
- Recuperación de la información criptográfica.
- Referencias cruzadas de la información criptográfica con denominaciones definido en la norma ISO/IEC 7816, cuando proceda.
- Diferentes mecanismos de autenticación.
- Múltiples algoritmos criptográficos.

Tolerancia orientación (en grados)	SENSOR TÉRMICO Tolerancia posición (en pixeles)																				
	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
5°	26,40	25,60	25,94	26,38	26,78	27,19	27,29	27,72	28,62	28,50	28,59	28,95	32,34	31,83	31,80	32,05	32,25	32,36	31,73	33,88	33,97
6°	26,11	25,19	25,52	26,03	26,43	26,43	26,94	27,36	28,04	27,84	**28,24**	**28,69**	31,67	31,32	31,20	31,51	31,81	31,88	31,49	33,75	33,80
7°	25,84	24,89	25,38	25,89	26,19	26,43	26,99	27,41	28,20	27,94	28,31	32,64	31,49	31,16	31,02	31,19	31,27	31,15	32,74	32,91	33,14
8°	25,73	25,05	25,86	26,50	26,74	26,74	27,07	27,58	28,32	27,94	32,12	32,07	31,20	30,99	30,72	30,65	30,54	30,53	31,82	31,98	32,20
9°	25,57	24,92	25,58	26,32	26,52	26,49	26,78	27,44	27,99	**27,48**	31,20	31,11	30,36	30,25	30,30	30,27	29,94	29,69	31,20	31,26	31,56
10°	25,48	24,75	25,50	26,11	26,28	26,34	26,57	27,38	27,92	27,71	31,47	31,48	30,78	30,69	30,68	30,64	31,65	31,34	31,00	31,09	31,25
11°	25,46	24,62	25,34	26,06	26,07	26,01	26,34	27,22	27,78	27,80	31,45	31,57	30,89	30,78	30,48	30,50	31,48	31,27	31,03	30,96	31,25
12°	25,49	24,60	25,18	25,79	25,76	25,85	26,22	27,28	27,94	31,48	31,43	31,58	31,01	30,87	30,56	30,73	30,22	31,34	31,13	31,07	31,32
13°	25,50	**24,59**	25,03	25,56	25,44	25,65	**26,18**	**27,02**	**27,74**	31,17	31,16	31,26	30,51	30,41	30,07	30,16	31,57	31,31	31,03	30,96	31,25
14°	25,47	24,60	25,03	**25,38**	**25,28**	**25,60**	26,22	27,06	27,76	30,99	30,91	30,88	29,92	29,98	29,68	29,59	29,22	28,85	30,62	30,51	30,91
15°	25,31	24,71	25,04	25,58	25,86	25,95	26,42	27,30	27,98	31,22	31,14	31,03	30,01	30,01	29,61	29,49	29,14	28,71	30,47	30,24	30,54
16°	25,29	24,67	**24,93**	25,67	26,00	26,09	26,66	27,44	28,08	31,35	31,19	31,14	30,16	30,12	29,75	29,57	29,16	28,81	28,49	28,44	30,68
17°	25,44	24,81	25,04	25,76	26,09	26,16	26,72	27,46	28,06	31,20	31,05	31,06	30,06	30,07	29,62	29,38	28,97	28,42	28,08	27,92	30,32
18°	25,11	24,65	25,00	25,68	26,06	26,09	26,60	27,43	28,02	30,71	30,56	30,57	29,54	29,61	29,22	29,02	28,51	28,12	27,78	27,58	27,97
19°	25,14	24,80	25,13	25,87	26,16	26,05	26,50	27,34	27,92	30,48	30,39	30,50	29,53	29,61	29,31	29,11	28,68	28,24	27,90	27,70	28,05
20°	**25,08**	24,65	25,00	25,97	26,20	26,26	26,68	27,47	28,03	30,38	30,15	30,43	29,34	29,38	29,04	28,68	28,26	27,94	**27,73**	**27,42**	**27,82**
21°	25,26	24,78	25,04	26,07	26,16	26,28	26,65	27,52	30,95	30,36	30,17	30,50	29,30	29,45	29,17	28,93	28,43	28,02	27,93	27,76	28,12
22°	25,31	24,79	25,01	26,10	26,16	26,28	26,58	27,45	30,85	30,16	30,01	30,28	29,10	29,21	**28,82**	**28,64**	28,27	27,92	27,93	27,72	28,02
23°	25,33	24,91	25,18	26,27	26,29	26,52	26,62	27,59	30,92	30,13	30,14	30,41	**29,09**	**29,12**	28,84	28,66	**28,24**	**27,89**	28,06	27,76	28,15
24°	25,38	25,05	25,33	26,28	26,50	26,73	26,79	27,82	31,00	30,24	30,15	30,39	29,16	29,33	29,04	28,86	28,50	28,13	28,26	27,93	28,37
25°	25,38	25,05	25,44	26,50	26,72	26,93	27,11	28,02	31,01	30,26	30,20	30,47	29,33	29,68	29,44	29,26	28,96	28,49	28,48	28,23	28,67

Tabla Térmico: Tasas de EER obtenidas para el sensor térmico, restringiendo el número de minucias a 40 y cuantificando los ángulos con 8 bits.

Tolerancia orientación (en grados)	SENSOR ÓPTICO Tolerancia posición (en pixeles)																				
	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
5°	15,54	14,57	14,54	14,32	14,49	14,57	14,57	14,65	15,11	14,97	14,65	15,02	15,32	15,68	15,96	15,92	16,00	16,18	16,37	16,52	16,67
6°	14,89	14,24	14,11	14,14	14,21	14,25	14,12	14,14	14,70	14,71	14,62	14,90	15,22	15,66	15,96	16,00	16,23	16,38	16,44	16,59	16,90
7°	14,78	14,06	14,02	14,00	13,89	13,73	13,61	13,61	14,32	14,40	14,20	14,37	14,74	15,23	15,53	15,69	15,73	16,02	16,00	16,08	16,52
8°	14,12	13,60	13,42	13,50	**13,37**	13,55	**13,43**	**13,60**	**13,96**	**14,03**	**13,94**	**13,85**	**14,28**	**14,69**	**15,10**	**15,13**	**15,15**	**15,53**	**15,67**	**15,66**	**16,20**
9°	13,96	13,43	13,42	13,54	13,45	**13,51**	13,74	13,71	14,33	14,24	14,04	14,18	14,57	14,87	15,23	15,28	15,27	15,68	15,79	15,72	16,23
10°	13,96	13,44	13,43	13,64	13,47	13,64	14,07	14,14	14,70	14,60	14,35	14,61	15,14	15,37	15,58	15,66	15,58	16,00	15,99	15,83	19,37
11°	13,95	13,48	13,47	13,56	13,53	13,64	14,15	14,12	14,83	14,78	14,75	15,01	15,54	15,81	16,04	16,06	16,10	16,46	16,44	16,40	19,75
12°	13,89	13,52	13,47	13,46	13,43	13,58	14,00	13,98	14,73	14,78	14,80	15,07	15,54	15,71	15,90	15,91	15,96	16,44	16,45	19,32	19,61
13°	13,87	13,61	**13,36**	13,54	13,47	**13,51**	13,92	13,91	14,63	14,73	14,85	15,01	15,38	15,47	15,56	15,73	15,77	16,23	16,28	19,08	19,54
14°	13,72	13,44	13,43	**13,43**	13,50	13,61	14,02	14,11	14,77	14,91	15,04	15,15	15,54	15,67	15,74	15,91	15,93	16,33	19,32	19,07	19,53
15°	13,79	13,48	13,41	13,55	13,61	13,68	14,15	14,11	14,81	14,95	15,02	15,15	15,54	15,67	15,74	15,91	15,99	16,45	19,31	18,94	19,40
16°	13,67	**13,41**	13,46	13,45	13,61	13,58	13,99	13,95	14,64	14,78	14,97	15,11	15,54	15,77	15,93	16,13	16,22	19,44	19,35	19,12	19,58
17°	13,66	13,45	13,37	13,50	13,55	13,59	14,05	14,11	14,81	14,85	15,04	15,23	15,70	15,83	15,93	16,13	16,27	19,28	19,14	18,83	19,23
18°	**13,64**	13,58	13,54	13,62	13,74	13,84	14,29	14,31	14,90	14,88	15,07	15,27	15,86	15,97	15,95	16,16	16,32	18,95	18,81	18,53	18,93
19°	13,69	13,58	13,48	13,57	13,89	14,05	14,57	14,58	14,95	14,94	15,12	15,33	15,97	16,14	16,08	16,29	16,40	18,96	18,89	18,60	18,95
20°	13,74	13,73	13,54	13,68	14,12	14,11	14,62	14,52	14,95	14,92	15,17	15,37	16,01	16,19	16,13	16,27	16,39	19,01	18,99	18,70	18,99
21°	13,74	13,73	13,54	13,68	14,15	13,98	14,45	14,45	14,88	14,85	15,10	15,28	15,93	16,04	15,98	16,13	16,19	18,91	18,94	18,72	18,98
22°	13,76	13,79	13,56	13,54	14,05	13,92	14,45	14,41	14,74	14,75	15,00	15,18	15,77	15,89	15,83	16,03	16,09	19,01	18,94	18,72	19,02
23°	13,82	13,83	13,60	13,58	14,10	13,97	14,44	14,45	14,81	14,83	15,07	15,24	15,77	15,99	15,88	16,14	19,05	19,07	19,00	18,78	19,08
24°	13,76	13,83	13,66	13,58	14,05	13,92	14,31	14,43	14,89	14,84	15,08	15,26	15,79	15,96	15,96	16,27	19,03	18,98	18,91	18,67	18,92
25°	13,70	13,89	13,66	13,52	14,10	14,12	14,57	14,64	15,14	15,04	15,28	15,46	15,93	16,10	16,16	16,53	19,37	19,26	19,18	18,99	19,21

Tabla Óptico: Tasas de EER obtenidas para el sensor óptico, restringiendo el número de minucias a 40 y cuantificando los ángulos con 8 bits.

Presupuesto

1) Ejecución Material

- Compra de ordenador personal (Software incluido)..... ..... 2.200 €
- Alquiler de impresora láser durante 6 meses .....60 €
- Material de oficina .....180 €
- Total de ejecución material..... 2.440 €

2) Gastos generales

- 16 % sobre Ejecución Material..... 390,4 €

3) Beneficio Industrial

- 6 % sobre Ejecución Material..... 146,4 €

4) Honorarios Proyecto

- 1.200 horas a 25 € / hora ..... 30.000 €

5) Material fungible

- Gastos de impresión..... 70 €
- Encuadernación ..... 300 €

6) Subtotal del presupuesto

- Subtotal Presupuesto..... 33.346,8 €

7) I.V.A. aplicable

- 16% Subtotal Presupuesto..... 5335,49 €

8) Total presupuesto

- Total Presupuesto ..... **38.682.29 €**

Madrid, Julio de 2009

El Ingeniero Jefe de Proyecto

Fdo.: Gustavo Francisco Sanz

Ingeniero Superior de Telecomunicación

Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un sistema de reconocimiento de huella dactilar para aplicaciones Match-on-Card. En lo que sigue, se supondrá que el Proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el Proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente Proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el Proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del Proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al Proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a

juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad “Presupuesto de Ejecución de Contrata” y anteriormente llamado ”Presupuesto de Ejecución Material” que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.