Universidad Autónoma de Madrid

Escuela politécnica superior

ATAQUES TIPO "SIDE-CHANNEL" A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR

-PROYECTO FIN DE CARRERA-

Alicia Hortensia Beisner Muñoz
Abril 2010

ATAQUES TIPO "SIDE-CHANNEL" A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR.

Autor: Alicia Hortensia Beisner Muñoz
Tutor: Javier Galbally Herrero
Ponente: Javier Ortega García

ATVS Grupo de Reconocimiento Biométrico
(http://atvs.ii.uam.es)
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Abril de 2010

Resumen

Este proyecto se centra en el estudio de las vulnerabilidades de los sistemas biométricos por el interés que han generado en la identificación personal automática en los últimos años. Dentro de los diferentes rasgos biométricos que podemos encontrar, la huella dactilar es el que más análisis ha suscitado por las atractivas características que presenta, y como consecuencia, el presente proyecto se centra en este rasgo.

Es importante conocer los tipos de vulnerabilidades que pueden presentar los sistemas de reconocimiento automático para prevenir y evitar riesgos. De hecho, los posibles puntos de ataque, así como los tipos de ataque, han sido clasificados y documentados en diferentes publicaciones científicas. Por otro lado, conocer y modificar diferentes parámetros de cada sistema pueden permitir mejorar la eficiencia y comprobar el comportamiento del mismo.

En la literatura se han propuesto ataques *hill-climbing* basados en la puntuación obtenida en el comparador. Esta clase de ataques consiste en la generación de patrones de características de huellas dactilares aleatorios que son modificados iterativamente hasta alcanzar una similitud deseada con respecto a una huella real para lograr ser aceptado por el sistema de verificación. En base a esto se han implementado este tipo de ataques sobre una gran base de datos adquirida en condiciones reales con diferentes tipos de sensores para poder comparar los resultados obtenidos con las observaciones realizadas en trabajos previos del estado del arte.

El estudio de ataques *hill-climbing* nos permite determinar una serie de parámetros iniciales para el desarrollo de ataques *side-channel* basados en el tiempo del comparador. La realización de estos ataques necesita un estudio previo del sistema para obtener una relación entre la puntuación devuelta por el comparador y el tiempo de cómputo. Una vez establecida la relación, se acometen diferentes ataques para evaluar su eficiencia.

El análisis de ambos tipos de ataques se realiza sobre dos sistemas reales de reconocimiento de huella dactilar: el software de referencia NFIS2 del NIST americano, desarrollado para el procesamiento automático de huellas dactilares y basado en módulos que pueden ser ejecutados en un PC; y un sistema *Match-on-Card*, que permite la ejecución de los algoritmos de reconocimiento en un chip de capacidad limitada integrado en una tarjeta inteligente. Este tipo de tecnología evita tener que utilizar una base de datos centralizada para el almacenamiento de las plantillas de usuario y, por tanto, solventa el problema de las comunicaciones, que pueden ser interceptadas, entre el sistema y dicha base de datos.

Los experimentos implementados en el laboratorio demuestran la existencia de una vulnerabilidad de los sistemas frente a los ataques *hill-climbing* basados en puntuación, así como una relación clara entre la puntuación y el tiempo de comparación que pudiera ser explotada por los ataques *side-channel* basados en tiempo. Además, la utilización de una gran base de datos adquirida bajo condiciones realistas de operación y con la inclusión de distintos sensores, permite alcanzar nuevas y más precisas conclusiones sobre las vulnerabilidades de los

sistemas de reconocimiento frente a este tipo de ataques, al tiempo que nos ayuda a comprender mejor las fortalezas y debilidades de esta tecnología.

Palabras clave

Biometría, reconocimiento biométrico, huella dactilar, seguridad, vulnerabilidades, algoritmos *hill-climbing*, ataques *side-channel*.

Abstract

This project is focused on the vulnerabilities of biometric systems due to the interest that they have generated in automatic personal identification in recent years. Among the different biometric features that can be found, the fingerprints are the most studied because of the different valuable properties they present.

It is important to study the different vulnerabilities that automatic recognition systems may present in order to prevent possible risks. The possible points of attack, as well as the types of attacks have been classified and documented in the literature. On the other hand, this type of vulnerability analysis can help to acquire and modify some parameters of the systems in order to improve their efficiency and verify their performance.

In the literature we can find the so called hill-climbing attacks based on the matching score. In such attacks, random patterns containing fingerprint information are generated and iteratively modified in order to achieve a specific likelihood between them and a given fingerprint. Thus, the verification system determines the synthetically generated pattern as a valid one. Based on these findings we have implemented such attacks on a large database acquired with different types of sensors to compare the results with observations made in previous contributions of the state of the art.

The study of hill-climbing attacks allows us to identify a set of initial parameters for the development of side-channel attacks based on the matching time. The realization of these attacks requires a previous study of the system to obtain a correlation between the matching score and the matching time. Once the relationship has been determinated different attacks are launched to evaluate their efficiency.

The analysis of both types of attacks are performed on two fingerprint recognition systems: NIST's NFIS reference software, developed for fingerprint automatic processing and based on modules that are executed on a PC; and a Match-on-Card system, which runs on a limited capacity chip embedded in a smart-card. This kind of technology avoids using a centralized database for storing the user's templates and thus solves all communication issues between the system and the database.

The experiments implemented in the laboratory have shown the existence of a vulnerability when the systems are attacked using the hill-climbing algorithm based on scores, as well as a clear correlation between the score and the matching time that could be exploited by side-channel attacks based on time. Furthermore, using a large database acquired under realistic conditions of operation and the inclusion of various sensors, enable new and more accurate conclusions about the vulnerability of recognition systems to those attacks. At the same time, this type of study helps to understand the strengths and weaknesses of this technology.

Key words

Biometrics, Biometric recognition, fingerprint, security, vulnerabilities, hill-climbing attacks, side-channel attacks.

Agradecimientos

Quisiera comenzar dando las gracias a mi ponente, Javier Ortega, por haberme dado la oportunidad de colaborar con el grupo ATVS durante estos últimos 2 años y poder haber llevado a cabo aquí este proyecto.

Quiero agradecer, en especial, a mi tutor del proyecto Javier Galbally por su ayuda a la hora de realizar el PFC y por los momentos inolvidables que hemos compartido.

En cuanto al resto de miembros del grupo, les quiero dar las gracias por ayudarme cuando lo he necesitado y por hacer que los días tristes o desesperantes sean más amenos. En especial agradezco su colaboración a Manuel Freire (mi primer tutor dentro de ATVS) que me guió en mis primeros pasos en la investigación, a Julián Fierrez que me ha apoyado en todo momento y a mis amigas y compañeras del grupo María y Almudena.

Me gustaría agradecer al profesorado que trabaja en la Escuela Politécnica Superior el trato que ofrecen al alumnado. Nos hacen pasar buenos y malos momentos, pero ante todo, nos ayudan a madurar y crecer como personas.

Una de las mejores cosas que me llevo de la universidad es la gente y los amigos que he conocido. Sería imposible nombraros a todos o listar la cantidad de cosas que recuerdo que han hecho que sea muy feliz a vuestro lado. Simplemente quiero que sepáis que me alegro de haberos conocido y haber compartido tanto con vosotros. Espero que nuestros viajes y salidas duren mucho tiempo, eso sí, ¡PIDO NO! organizarlas.

También doy las gracias a mis amigas de toda la vida Alex, Carol, Isa, María, Patri y Sil por estar a mi lado cuando las he necesitado, por apoyarme siempre y por todos los momentos que hemos vivido juntas.

Agradezco a toda mi familia (abuelos, tíos y primos), a Agata y a la familia Muñoz García el cariño, apoyo y confianza que me han dado.

Quiero hacer un nombramiento especial a mi hermano Tito (que me ha ayudado en todo lo posible) y a mis padres. Al fin y al cabo, ellos son los que han hecho que sea quien y como soy, los que me han aguantado cuando estaba estresada y los que celebran a mi lado los triunfos y me ayudan a levantarme en las derrotas.

Para terminar, agradezco haber estado en esta universidad porque me dio la posibilidad de conocer a Alberto. Él ha estado a mi lado desde casi el primer día de carrera y ha tenido que aguantarme 'mucho' en los malos momentos. Gracias por estar siempre ahí, por apoyarme, aconsejarme y hacerme feliz. Sin ti, todo sería mucho más complicado.

Índice

Índice de figuras

Índice de tablas

1 Introducción

1.1. Motivación

El estudio de la identificación personal basado en los sistemas de reconocimiento y autenticación biométrica es un tema actual de investigación ya que se propone como una manera segura, automática y fiable de identificar a un usuario. Esto es debido a que los rasgos biométricos no pueden, en general, ser robados, prestados, olvidados, sustraídos o copiados, lo cual presenta una gran ventaja frente a sistemas basados en contraseñas, tarjetas magnéticas y otros elementos que necesitan el conocimiento de una información (PIN, contraseña)o posesión de un elemento(tarjeta, llave).

Existen múltiples rasgos biométricos con diferentes características que se emplean en los sistemas de reconocimiento biométrico para identificar unívocamente a cada individuo, clasificarlo y reconocerlo. De entre los rasgos más utilizados en la actualidad para el reconocimiento personal, la huella dactilar cobra gran importancia (de hecho es el rasgo biométrico con mayor ocupación en el mercado en la actualidad) gracias a su alta eficiencia como método identificativo, su reducido tamaño, bajo coste y su relativo sencillo funcionamiento.

El estudio de las vulnerabilidades frente a ataques externos de los sistemas de reconocimiento personal es importante para poder prevenir y evitar los riesgos derivados de estas vulnerabilidades, por lo que es necesario profundizar en ellas y conocerlas en detalle con el objetivo de proteger los datos y el acceso fraudulento al sistema.

En el presente proyecto se pretende realizar un análisis de la vulnerabilidad de los sistemas de reconocimiento automático de huella dactilar en función de la puntuación devuelta por el comparador y el tiempo relacionado. Los métodos de ataque serán tanto "*hill-climbing*", como "*side-channel*" y aportarán documentación acerca de las amenazas existentes en los sistemas reales.

Hay que tener en cuenta que los sistemas de reconocimiento automático de huella dactilar que se van a emplear poseen ciertas limitaciones causadas, normalmente, por los sensores, el área de captura, la distorsión de la imagen de la huella o la calidad de la imagen capturada.

1.2. Objetivos

Para llevar a cabo las labores antes mencionadas, se plantean como objetivos del presente proyecto:

- Revisión del estado del arte de los sistemas de reconocimiento biométrico.
- Revisión de las vulnerabilidades de los sistemas de reconocimiento biométrico.
- Revisión del estado del arte de ataques que se hayan llevado a cabo en otras tecnologías basados en el tiempo de cómputo del sistema.
- Análisis de la información recopilada.
- Desarrollo de ataques tipo *hill-climbing* basados en puntuación y análisis de resultados.
- Desarrollo de ataques *side-channel* basados en el tiempo del comparador en función de los parámetros definidos en los ataques anteriores y análisis de su efectividad para atacar con éxito sistemas de reconocimiento automático de huella dactilar.

Los experimentos serán desarrollados sobre una gran base de datos adquirida en un entorno real y capturada con dos sensores diferentes: uno óptico de contacto y otro térmico de barrido. Se analizarán las vulnerabilidades de dos sistemas reales de reconocimiento de huella dactilar diferentes: el software de referencia NFIS2 del NIST americano y un sistema basado en tarjeta inteligente Match-on-Card (MoC).

1.3. Metodología

La documentación se ha organizado dividiéndola en los siguientes capítulos:

1. **Introducción:** se presenta la motivación, los objetivos y la metodología expuesta en el proyecto.
2. **Reconocimiento biométrico:** se realiza una exposición del estado del arte de los sistemas biométricos, de su modo de operación y el rendimiento. Además, se clasifican los diferentes tipos de rasgos biométricos existentes y las características que poseen.
3. **Reconocimiento de huella dactilar:** nos centramos en el estado del arte de la huella dactilar desarrollando aspectos como tipología, adquisición, extracción de características y clasificación.
4. **Ataques a sistemas de reconocimiento biométrico:** se presentan las amenazas a las que están expuestos los sistemas de reconocimiento automático centrándonos en el estudio de los tipos de ataques existentes y especialmente en los ataques *hill-climbing* y *side-channel* que se desarrollan a lo largo del proyecto.

5. **Entorno experimental:** se presentan los sistemas analizados (software NFIS2 del NIST y software sobre tarjeta inteligente o *Match-on-Card*), así como el rendimiento que presentan estos sistemas con la base de datos que emplearemos en los siguientes apartados (BiosecurID) y para los dos sensores (óptico y térmico) con los que fue capturada.
6. **Métodos de ataque *hill-climbing*:** este capítulo detalla el algoritmo llevado a cabo con las huellas dactilares de los distintos sensores y para los dos sistemas de estudio. Se analizan los resultados obtenidos y se comparan con otras bases de datos.
7. **Métodos de ataque *side-channel*:** Los ataques *side-channel* implementados están basados en ataques *hill-climbing* utilizando información adicional al sistema como es el tiempo. Por esta razón se realiza un análisis previo de la relación entre la puntuación y el tiempo sobre los ataques *hill-climbing*, se presenta el algoritmo de los ataques *side-channel* y se analizan los resultados obtenidos tras atacar la base de datos.
8. **Conclusiones y trabajo futuro:** se trata del capítulo final de la memoria en el que se detallan conclusiones extraídas y posibles vías de trabajo futuro.

1. Introducción

2

Reconocimiento biométrico

2.1. Introducción

Hoy en día la forma más común para identificar a un individuo de manera automática consiste en la utilización de tarjetas magnéticas, contraseñas, códigos PINs y elementos basados en la posesión o conocimiento de información cuyo principal problema es que pueden ser perdidos, robados u olvidados. De ahí surge la importancia del reconocimiento personal a partir de uno o varios rasgos biométricos.

Figura 1: Aparatos comerciales clásicos de identificación personal.

Los sistemas biométricos utilizan el rasgo biométrico para identificar unívocamente a cada individuo. Esto supone un incremento de seguridad en comparación con los sistemas clásicos al tener una mayor capacidad discriminatoria entre el usuario y el impostor que intenta acceder fraudulentamente al sistema.

Figura 2: Aparatos comerciales que utilizan rasgos biométricos para la identificación personal.

2.2. Propiedades de los rasgos biométricos

Las características que debe cumplir todo rasgo biométrico son [1]:

- **Universalidad**: Toda persona debe poseerlo.
- **Unicidad o distintividad:** Personas distintas deben poseer rasgos diferenciados.
- **Estabilidad o permanencia**: El rasgo biométrico debe ser invariante en el tiempo a corto plazo.
- **Perennidad:** Perpetuo a lo largo de la vida y en condiciones ambientales diversas.
- **Evaluabilidad**: Debe poder caracterizarse de manera cuantitativa.

Es necesario que cumpla dichas características para poder ser utilizado como identificador personal. Además, también es deseable que el rasgo biométrico: tenga una alta aceptación personal y social; no necesite de excesiva cooperación por parte del usuario para su adquisición; posea un rendimiento aceptable; y sea robusto frente a posibles ataques externos.

2.3. Rasgos biométricos

Existen múltiples rasgos biométricos utilizados para distintas aplicaciones en la actualidad. Cada uno de esos rasgos posee diferentes ventajas y desventajas, por lo que la elección estará muy ligada a sus características y a la aplicación que se quiera llevar a cabo (en la Figura 3 se muestran ejemplos de los rasgos biométricos más comunes).

Se pueden clasificar en:

- **Rasgos fisiológicos:** son rasgos que miden características inherentes a la fisiología del ser humano. En este conjunto se encuentra el ADN, la huella dactilar, el iris, etc.
- **Rasgos conductuales:** Aquellos que miden características o comportamientos aprendidos tales como la firma, la voz, el modo de caminar, etc.

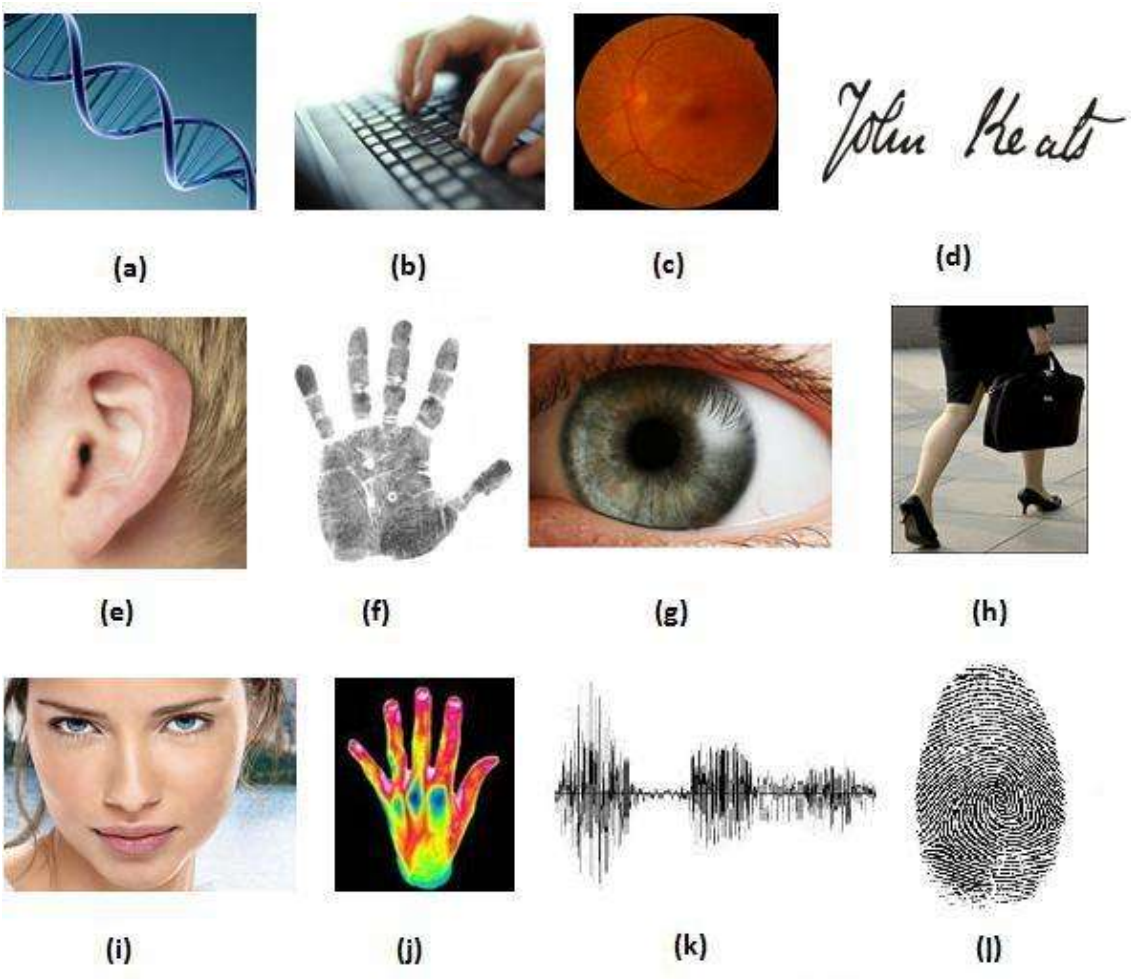


Figura 3: Algunos rasgos biométricos utilizados en la actualidad. a)ADN, b) Dinámica del tecleo, c) Escáner de retina, d) Firma, e) Forma de la oreja, f) Geometría de la mano, g)Iris ,h)Modo de caminar, i) Rostro, j) Termograma de la mano, k) Voz, l) Huella dactilar.

Los principales rasgos biométricos son [1]: el ADN, la cara, la huella dactilar, la voz, la firma, el iris y la mano. También se pueden encontrar estudios, aunque en menor medida, que han utilizado la retina, la oreja, el olor, la forma de caminar, la forma de teclear, la forma de las venas de la mano, el termograma de la cara, etc.

También existen modalidades biométricas emergentes como son las radiografías dentales, el patrón vascular cutáneo, el perfil de presión de la mano o los llamados *soft biometrics,* que son aquellos rasgos que proporcionan información sobre el individuo pero que no son lo suficiente distintivos o permanentes como para identificar a una persona de forma eficaz (altura, peso, sexo, color de ojos, etc).

A continuación se listarán por orden alfabético y con mayor detalle algunos de estos rasgos biométricos.

ADN

El ADN es único para cada individuo excepto para los gemelos monocigóticos. Presenta graves problemas de privacidad ya que se pueden revelar discapacidades o características del individuo con una simple porción de ADN que se considera fácil de robar. Por otro lado, es necesario que un experto lo analice. Se utiliza en gran medida para aplicaciones forenses de reconocimiento.

Dinámica del tecleo

Se trata de un rasgo biométrico que puede obtenerse de manera no invasiva ya que se puede capturar mientras la persona teclea. Es suficientemente discriminatorio en casos sencillos de verificación de identidad pero hay que tener en cuenta que no es único para cada individuo y que varía mucho con el tiempo.

Escáner de retina

La estructura vascular de la retina es diferente en cada persona. Es considerado el rasgo biométrico más seguro ya que es complicado cambiar o duplicar la estructura de la retina. Se considera un rasgo biométrico con problemas para ser aceptado por la sociedad por el hecho de necesitar un usuario cooperativo en la captura. Además, al igual que ocurre con el ADN, la retina vascular tiene problemas de privacidad al poder revelar afecciones como la hipertensión.

Firma

Es un rasgo biométrico muy aceptado por su alta utilización.

La captura requiere contacto con una superficie mediante una necesaria cooperación por parte del usuario. La identificación personal mediante este rasgo resulta compleja por la variabilidad que posee la firma de un individuo a lo largo del tiempo e incluso de cada realización. Existen dos tipos de reconocimiento de firma: firma *On-line* y firma *Off-line*. El primer caso hace uso de la información instantánea ya que tiene acceso al acto de la firma. La firma *off-line*, solo dispone de la forma del rasgo como imagen. Este tipo de sistemas de reconocimiento se encuentran ya implementados en diversas aplicaciones comerciales (tiendas, mensajería express).

Forma de la oreja

El reconocimiento de oreja está basado en la forma del borde de la oreja y la estructura del tejido cartilaginoso. Evita problemas de cambio con la expresión o con el paso del tiempo. Pueden utilizarse sensores infrarrojos para extraer la forma de la oreja incluso en presencia del pelo. Los sistemas implementados hasta el momento suelen utilizar comparación de distancias entre un punto común del interior de la oreja y las zonas salientes.

Geometría de la mano

La geometría de la mano es otro rasgo biométrico poco distintivo entre usuarios lo que implica que sólo se suele usar para verificar a un usuario pero no para identificarlo. El sistema de adquisición necesita que el sujeto sitúe la mano sobre un escáner o dispositivo capturador que normalmente poseen plantillas que permiten un uso limitado de memoria o ancho de banda.

Iris

La estructura del iris de cada ojo muestra alto grado de unicidad y estabilidad con el tiempo. El patrón se mantiene prácticamente invariante desde la infancia del individuo. La pigmentación y el tamaño de la pupila se estabilizan en la adolescencia y en la vejez se observa despigmentación. La herencia genética sólo determina la estructura general. La adquisición de la imagen sigue un procedimiento no invasivo pero necesita que el usuario sea cooperativo situando adecuadamente su iris. La imagen debe: poseer alta calidad, resolución, contraste,

estar centrada y libre de artefactos. Se considera que la tecnología de reconocimiento de iris es sumamente precisa y rápida.

Modo de caminar

La forma de andar y correr es distinta en cada persona. Se puede utilizar para verificación de usuarios en aplicaciones de baja seguridad ya que posee unas tasas de acierto menores que otros rasgos biométricos. La adquisición se realiza con cámaras de video y se utilizan las secuencias grabadas para medir los diferentes movimientos de cada articulación. Al tener tanta información, el coste computacional es muy elevado.

Olor

El olor que desprende un cuerpo es diferente en cada ser humano y por tanto es una característica distintiva de cada individuo. Este rasgo se capta mediante sensores químicos cada uno de ellos sensible a un cierto grupo de sustancias diferentes. Presenta problemas con componentes artificiales como desodorantes o perfumes ya puede afectar a la capacidad distintiva del sistema.

Rostro

La cara es comúnmente utilizada por los hombres para el reconocimiento de individuos y por ello es un rasgo biométrico con una buena aceptación entre los usuarios. El modo de adquisición es sencillo y no invasivo, simplemente se necesita una fotografía. A su vez presenta algunas desventajas que se intentan solucionar con diferentes aplicaciones como son la tolerancia de los sistemas a cambios producidos por el efecto de la edad, expresiones faciales, iluminación y posición relativa de la cara con respecto a la cámara.

Termogramas

Miden los patrones infrarrojos de la emisión de calor de zonas corporales como la mano o la cara, causado por el flujo de sangre bajo la piel. Dichos patrones de calor son característicos de cada individuo e incluso permite distinguir entre gemelos idénticos. La captura se lleva a cabo mediante una cámara infrarroja de forma no invasiva y a cierta distancia. Como desventajas cabría destacar que este tipo de sensores son realmente caros y que es una técnica sensible a entornos no controlados donde el calor desprendido por superficies emisoras cercanas al cuerpo afecta a la adquisición de la imagen.

Voz

La voz es un rasgo biométrico muy aceptado y fácil de obtener. Es el único que se puede utilizar en aplicaciones telefónicas para reconocimiento de personas. Sin embargo no se considera lo suficientemente distintivo para identificar individuos en una amplia base de datos debido a su relativamente baja distintividad y laposibilidad de ser imitada. También hay que considerar que la voz se ve afectada por el estado emocional, la salud de las personas, el estrés, etc. La captura se realiza de forma no invasiva, pero la calidad de la señal se ve degradada por el micrófono, el canal de comunicaciones y la digitalización.

La Tabla 1 muestra las características presentadas en el apartado 2.2 además del rendimiento y la aceptabilidad que poseen los rasgos biométricos descritos anteriormente. Los valores de la tabla no deben tomarse como absolutos sino como una apreciación orientativa.

Identificador biométrico	**Universalidad**	**Distintividad**	**Estabilidad**	**Evaluabilidad**	**Rendimiento**	**Aceptabilidad**
ADN	A	A	A	B	A	B
Dinámica del teclado	B	B	B	M	B	M
Escáner de retina	A	A	M	B	A	B
Firma	B	B	B	A	B	A
Forma de caminar	M	B	B	A	B	A
Geometría de la mano	M	M	M	A	M	M
Huella dactilar	M	A	A	M	A	M
Iris	A	A	A	M	A	B
Olor	A	A	A	B	B	M
Oreja	M	M	A	M	M	A
Rostro	A	B	M	A	B	A
Termograma facial	A	A	B	A	M	A
Venas de la mano	M	M	M	M	M	M
Voz	M	B	B	M	B	A

Tabla 1: Comparación de tecnologías biométricas. A, M y B denotan niveles Alto, Medio y Bajo respectivamente. Tabla extraída de [1].

2.4. Sistemas biométricos

Los sistemas biométricos aparecen por la necesidad de autentificar usuarios a partir de un rasgo biométrico mediante técnicas automáticas, fiables y seguras. Se trata básicamente de un sistema de reconocimiento de patrones que funciona del siguiente modo: el sensor captura un rasgo biométrico; se extraen un conjunto de

características tras procesar la señal (patrón); y se comparan con las características de los usuarios (plantillas o *templates*) que hay almacenadas en la base de datos. En función de los resultados obtenidos por el comparador y el umbral de decisión, el sistema caracteriza el patrón de entrada como válido o no.

En la Figura 4 se muestra la estructura general del funcionamiento de los sistemas de reconocimiento biométrico.

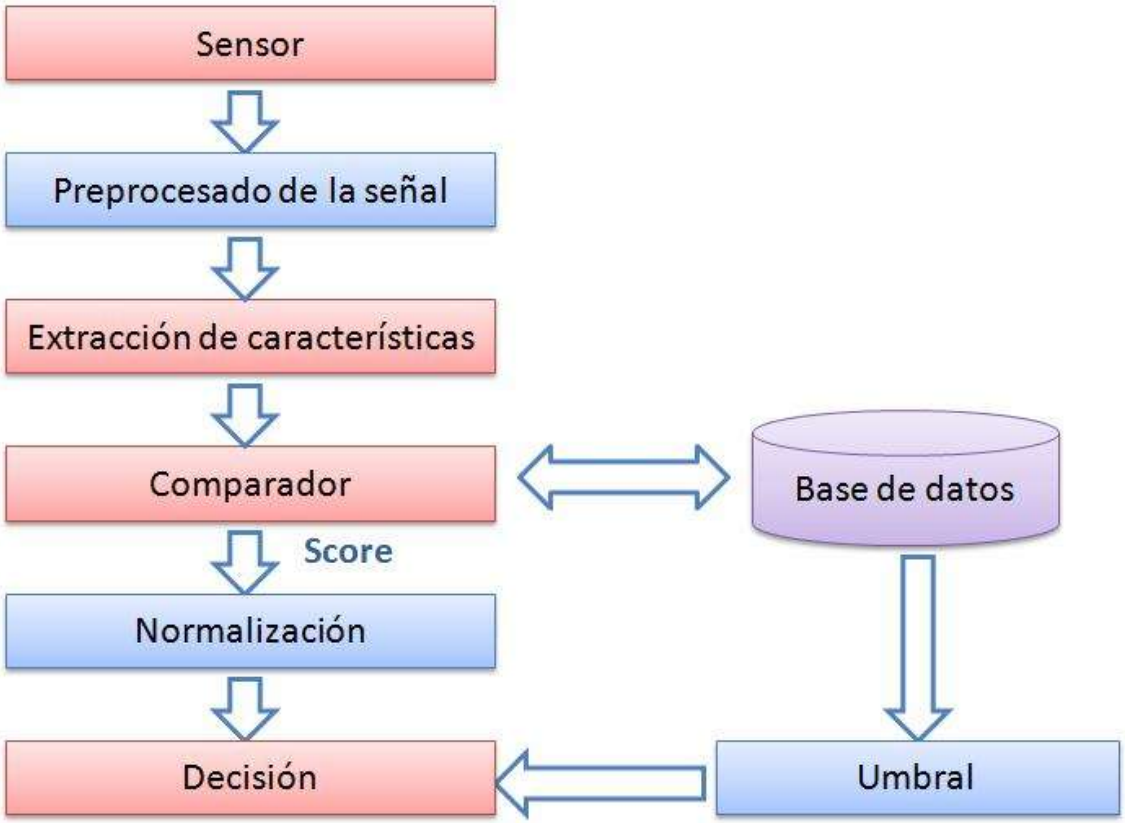


Figura 4: Arquitectura general de un sistema biométrico.

Es deseable que estos sistemas posean un alto rendimiento, precisión y aceptación social y personal. Otra cuestión importante es la seguridad que deben poseer para evitar que se produzcan ataques y sea posible acceder al sistema de manera fraudulenta.

2.5. Modos de operación sistemas biométricos

Modo registro

El modo registro es común a todos los sistemas biométricos ya que en esta etapa son dados de alta los usuarios en la base de datos. Consiste en la introducción de los rasgos biométricos en el sistema utilizando el sensor adecuado. Para almacenar los datos de cada usuario (plantillas de usuario o *templates*) en la base de datos es

necesario procesar la señal capturada y realizar la extracción de características que conforman la plantilla.

Modo verificación

Los sistemas de verificación (también conocidos como autenticación) toman dos entradas:

- Una realización del rasgo biométrico a verificar.
- Una solicitud de identidad: generalmente se indicará por algún tipo de código, identificador, nombre de usuario o tarjeta inteligente.

El rasgo biométrico es comparado con la plantilla almacenada en la base de datos y correspondiente a la identidad del usuario, es decir, el sistema realiza una comparación 1 a 1 generando una puntuación o *score* que servirá para verificar la identidad del usuario.

Las únicas posibles salidas del sistema son la aceptación o el rechazo del individuo dependiendo de si el *score* supera un determinado umbral o no. El solicitante queda catalogado respectivamente como usuario auténtico o como impostor.

En este proyecto se trabajará siempre en modo verificación.

Modo identificación

El objetivo es identificar una realización de un rasgo biométrico de un usuario desconocido como perteneciente a un individuo dentro de un conjunto de N posibles usuarios almacenados en una base de datos. La identificación se puede realizar en dos escenarios diferentes:

- **Identificación en conjunto cerrado:** El rasgo de entrada pertenece a uno de los N posibles individuos modelados por el sistema, por lo que sólo existen N salidas posibles.
- **Identificación en conjunto abierto:** El solicitante que pretende ser identificado puede no pertenecer al grupo de usuario, así pues, existen (N+1) salidas posibles. La identificación en conjunto abierto se considera una mezcla de identificación en conjunto cerrado y verificación.

Utilizaremos a partir de este momento el término *reconocimiento* en aquellas situaciones en las que no se tenga intención de diferenciar entre verificación e identificación. La Figura 5 muestra un esquema de los tres modos de funcionamiento de un sistema de reconocimiento biométrico.

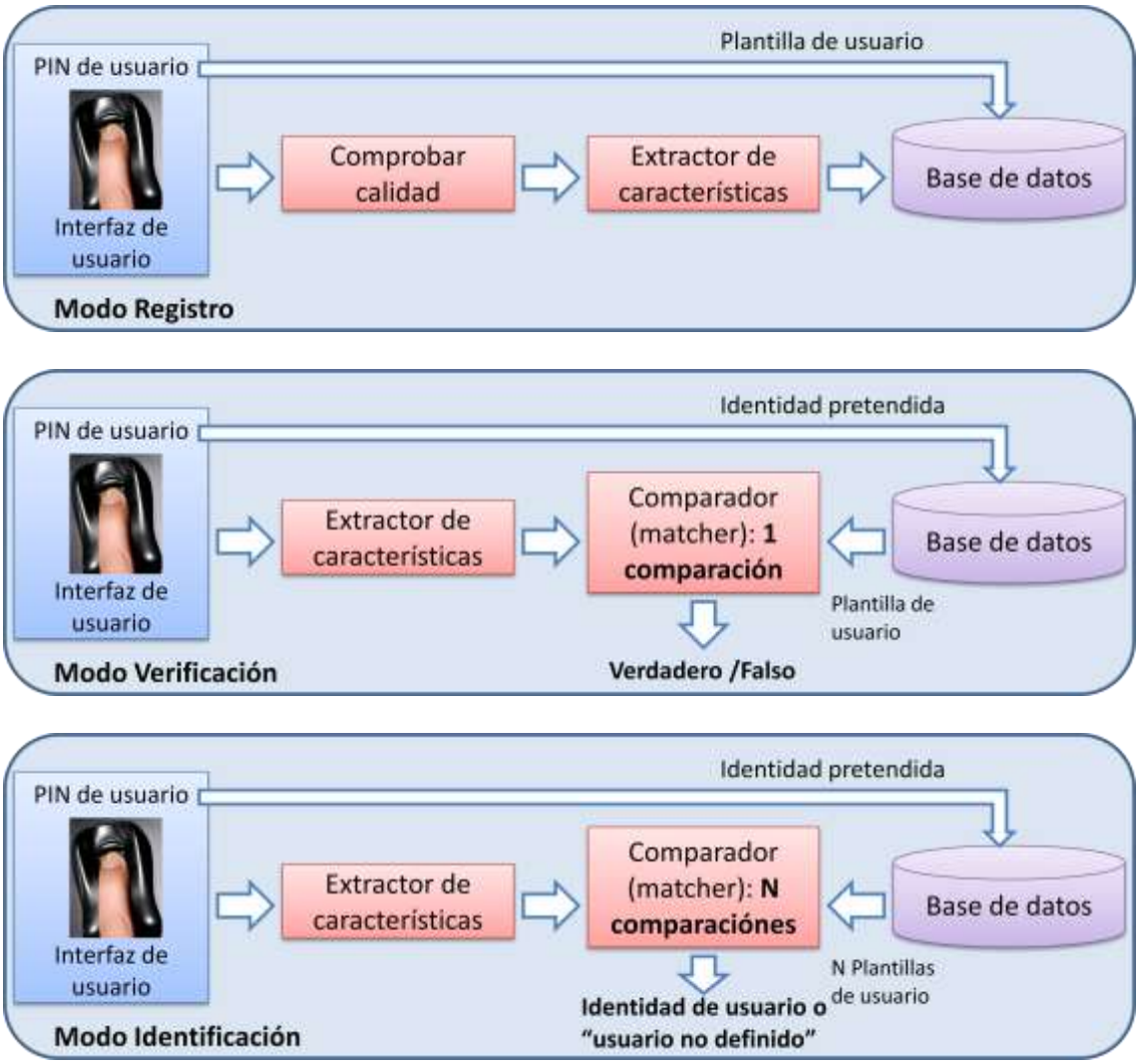


Figura 5: Modos de funcionamiento de un sistema automático de reconocimiento biométrico. Figura adaptada de [2].

2.6. Rendimiento de los sistemas biométricos

El comparador de un sistema de reconocimiento biométrico mostrado en la Figura 4 devuelve una puntuación o *score* en el proceso de verificación del rasgo biométrico. Esta puntuación es el resultado del parecido entre el rasgo introducido con el comparado que se encuentra almacenado en la base de datos (después del registro del usuario, tal y como se ha explicado en el apartado anterior). En el caso concreto de los sistemas basados en huella dactilar con los que trabajaremos en este proyecto, dicha puntuación será mayor cuanto mayor sea el parecido entre las dos huellas.

La salida del sistema está gobernada por el umbral de decisión. Si la puntuación obtenida por el comparador es superior al umbral establecido quiere decir que las huellas comparadas son suficientemente parecidas como para determinar que

pertenecen al mismo dedo o usuario. En caso de que la puntuación no supere el umbral se determina que son de dedos diferentes.

Así pues, un sistema de verificación de huella puede cometer dos tipos de errores:

- **Falsa aceptación (FA):** el sistema considera que dos huellas pertenecen al mismo usuario cuando no es así.
- **Falso rechazo (FR):** el sistema determina que dos huellas pertenecientes al mismo dedo no se corresponden.

Por esta razón, a la hora de caracterizar un sistema para un determinado umbral de funcionamiento es imprescindible conocer la **tasa de falsa aceptación** (FAR o *False Acceptance Rate*), que es la probabilidad de que un impostor sea aceptado en el sistema; y la **tasa de falso rechazo** (FRR o *False Rejection Rate*), que es la probabilidad de que un usuario registrado no sea aceptado en el sistema.

Tanto la FAR como la FRR varían según varíe el umbral de decisión del sistema. Como se puede observar en la Figura 6 (izquierda), fijando un umbral, la FAR será el área bajo la curva de impostores que se sitúa por encima del umbral, mientras que la FRR será el área bajo la curva de usuarios válidos que queda por debajo del umbral.

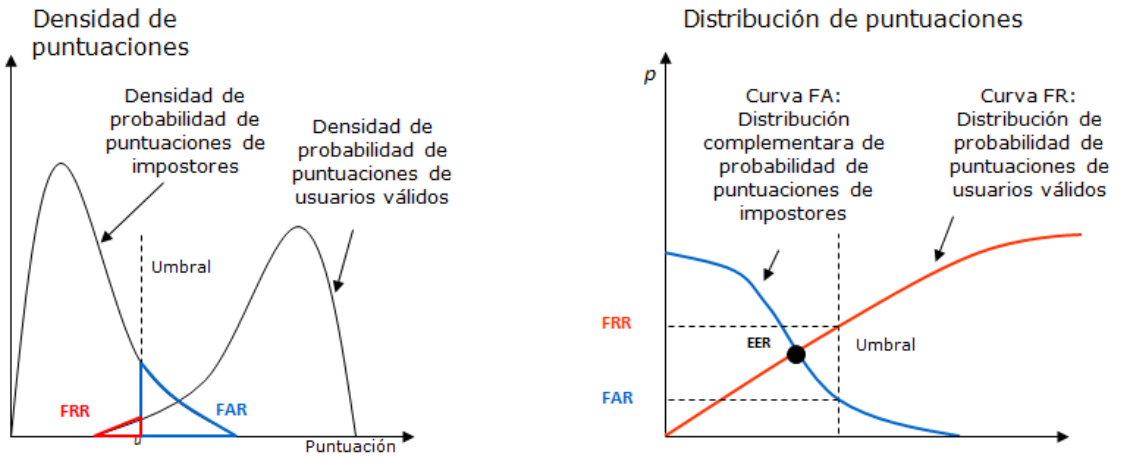


Figura 6: Densidades (izquierda) y distribuciones (derecha) de probabilidad de puntuaciones de usuarios e impostores.

El punto en el que la FAR y la FRR son iguales se denomina *Equal Error Rate (EER)* y a menudo es utilizado para comparar el rendimiento de diferentes sistemas dando un solo valor. Sin embargo, no hay que olvidar que este parámetro no describe completamente el funcionamiento de un sistema.

Otro método de representar el rendimiento de un sistema biométrico es mediante las curvas ROC (*Reciever Operating Curve*). Este tipo de curvas se generan representando la FAR frente a (1 - FRR) en función de diferentes valores del

umbral de decisión. En ocasiones también se denomina curva ROC a la representación de FAR frente a FRR.

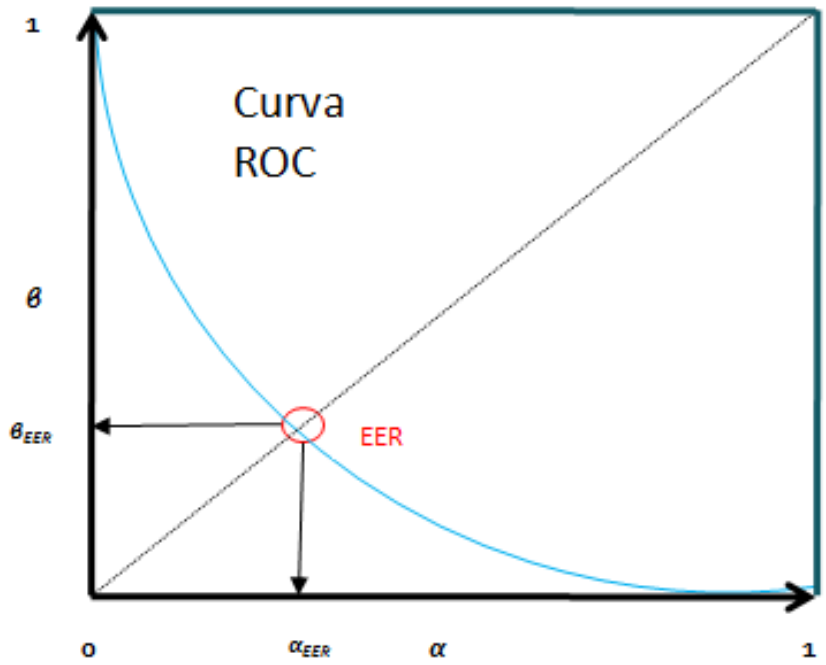


Figura 7:Curva ROC y punto EER.

Una alternativa comúnmente utilizada frente a las curvas ROC son las curvas DET (*Detection Error Tradeoff*) cuyo ejemplo puede visualizarse en la Figura 8**.** La única diferencia es que las curvas DET se representan en una escala de ejes logarítmica, con lo que tienden a convertir las curvas ROC en rectas y facilita la comparación de distintos sistemas: un sistema será mejor cuanto más cerca del origen de coordenadas se encuentren las curvas DET.

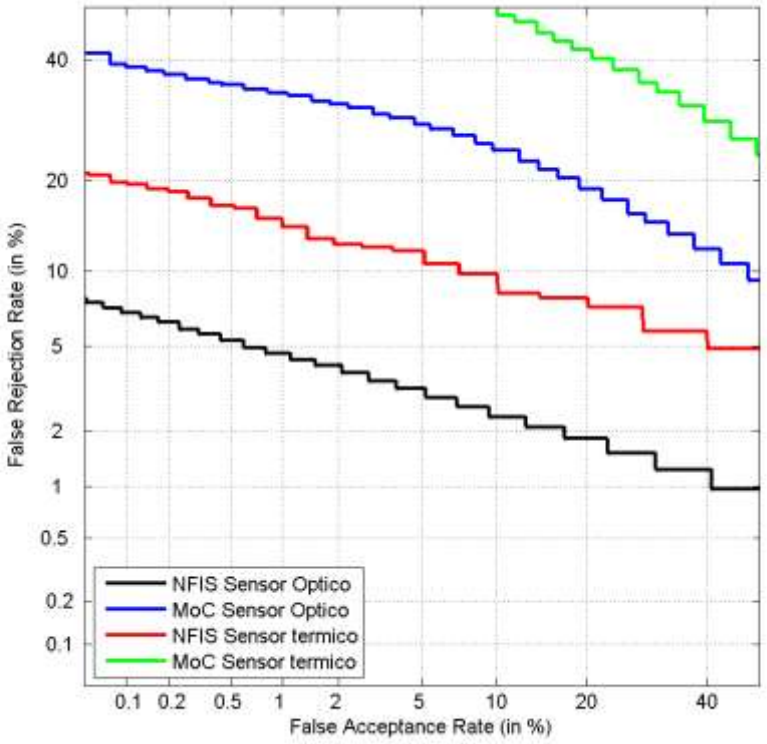


Figura 8: Ejemplo de curvas DET para los dos sistemas tratados en el presente proyecto y para los dos sensores considerados.

3

Reconocimiento basado en huella dactilar

3.1. Introducción

Desde hace siglos existe una evidente relación entre la huella dactilar y la identidad personal. Diferentes hallazgos arqueológicos sugieren que ya en la antigüedad, las personas eran conscientes de la singularidad de este rasgo biométrico [1].

Hasta principios del siglo XX no fue aceptada como método de identificación personal aunque ya se había trabajado con ella anteriormente en investigaciones científicas que habían conseguido esclarecer su naturaleza, caracterización, formación anatómica e individualidad [1].

A parir de los años 60 del siglo pasado, la huella dactilar se empezó a utilizar en sistemas de reconocimiento automáticos por agencias gubernamentales y en bases de datos (DNI, criminales,…), y desde entonces ha tenido un rápido crecimiento en aplicaciones policiales y comerciales civiles (Figura 9). Todos estos avances han sido posibles gracias a que los sistemas de reconocimiento automático basados en huella dactilar poseen características como exactitud, bajo coste, tamaño reducido, funcionalidad, etc.

Además, el interés por la huella dactilar como rasgo biométrico en los últimos treinta años ha producido innumerables publicaciones científicas que han conseguido que actualmente acapare la mayor parte del mercado biométrico frente al resto de rasgos [1].

Figura 9: Ejemplos de aplicaciones comerciales que utilizan reconocimiento biométrico basado en huella dactilar.

3.2. Clasificación de huella dactilar

Las huellas dactilares se forman a partir del séptimo mes fetal y sus características son:

- **perennes:** invariantes hasta la descomposición y con capacidad regenerativa.
- **individuales:** características para cada individuo.

La representación de la huella dactilar se consigue con el **dactilograma**, que es una imagen formada por el relieve de las crestas interpapilares de la yema del dedo. Está formado por una serie de crestas y valles propias de cada individuo y pueden observarse de tres maneras diferentes (Figura 10).

- **Natural:** Observado directamente en las huellas de los dedos.
- **Latente:** Impresión por contacto con una superficie.
- **Artificial:** reproducción gráfica del natural.

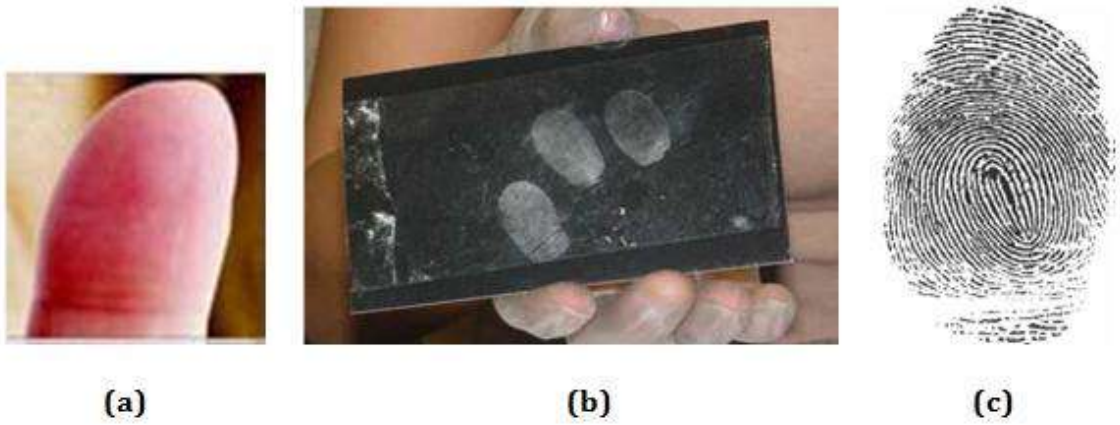


Figura 10: Tipos de dactilogramas existentes. (a) Natural, (b) Latente, (c) Artificial.

El dactilograma es esencial para la clasificación y reconocimiento de la huella dactilar. Generalmente, estas imágenes presentan dos zonas diferenciadas. Las zonas oscuras se denominan ***crestas*** mientras que las claras son los llamados ***valles***. En la Figura 11 se observa un ejemplo de huella dactilar capturada con un sensor capacitivo.

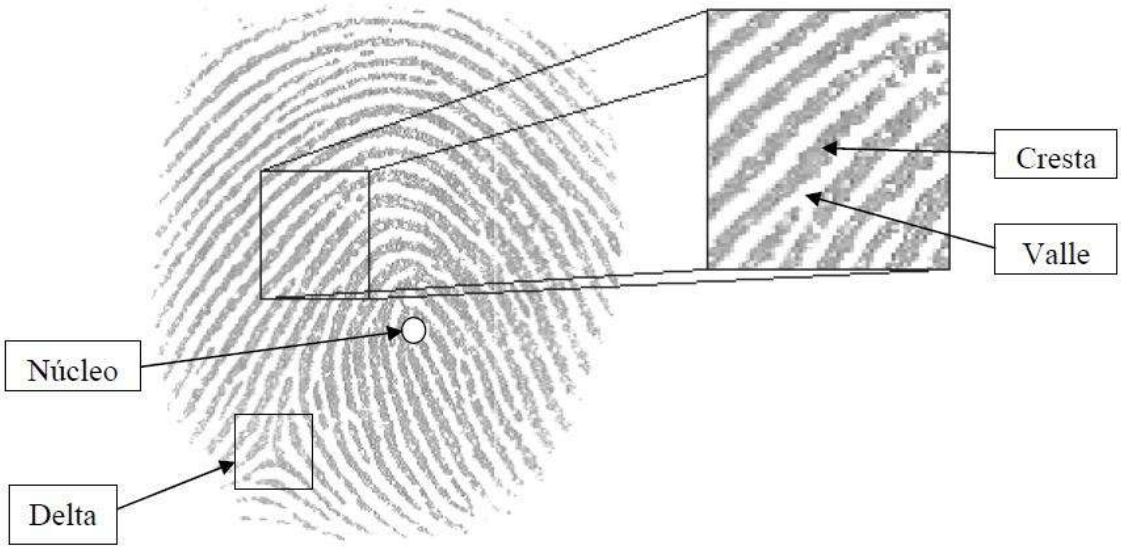


Figura 11: Huella dactilar capturada con un sensor capacitivo.

Las crestas y los valles discurren en paralelo por la superficie de la huella. Las anomalías de las crestas se denominan ***minucias*** y pueden encontrarse en múltiples formas diferentes. En la se muestran los ejemplos de minucias más típicos.

A efectos prácticos, los sistemas automáticos suelen considerar sólo dos tipos de puntos característicos de la cresta: terminación y bifurcación (Figura 13).

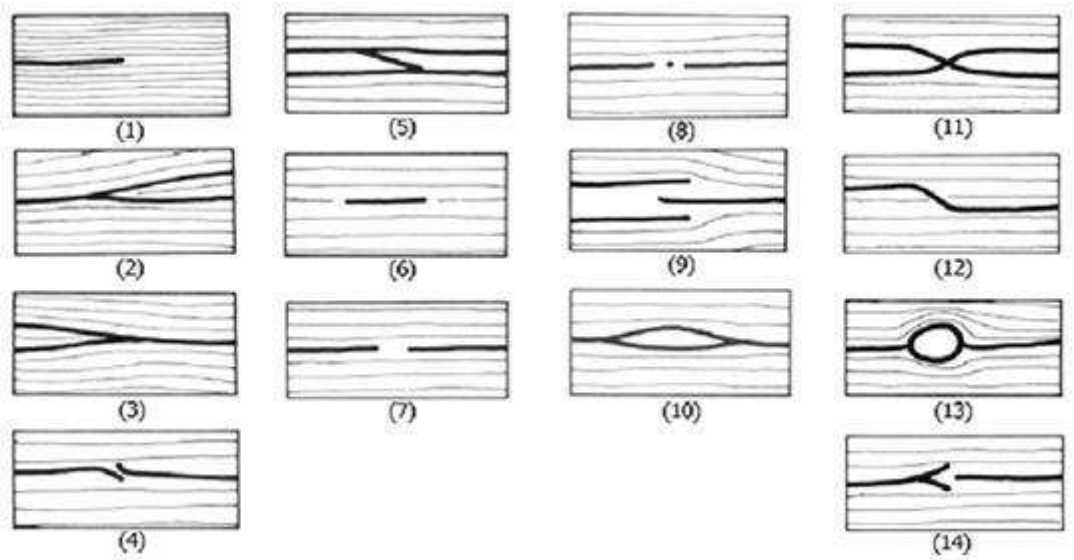


Figura 12: Algunos tipos de crestas: (1) Abrupta, (2) Bifurcación, (3) Convergencia, (4) Desviación, (5) Empalme, (6) Fragmento, (7) Interrupción, (8) Punto, (9) Ensamble, (10) Ojal, (11) Secante, (12) transversal, (13) Círculo, (14) Delta.

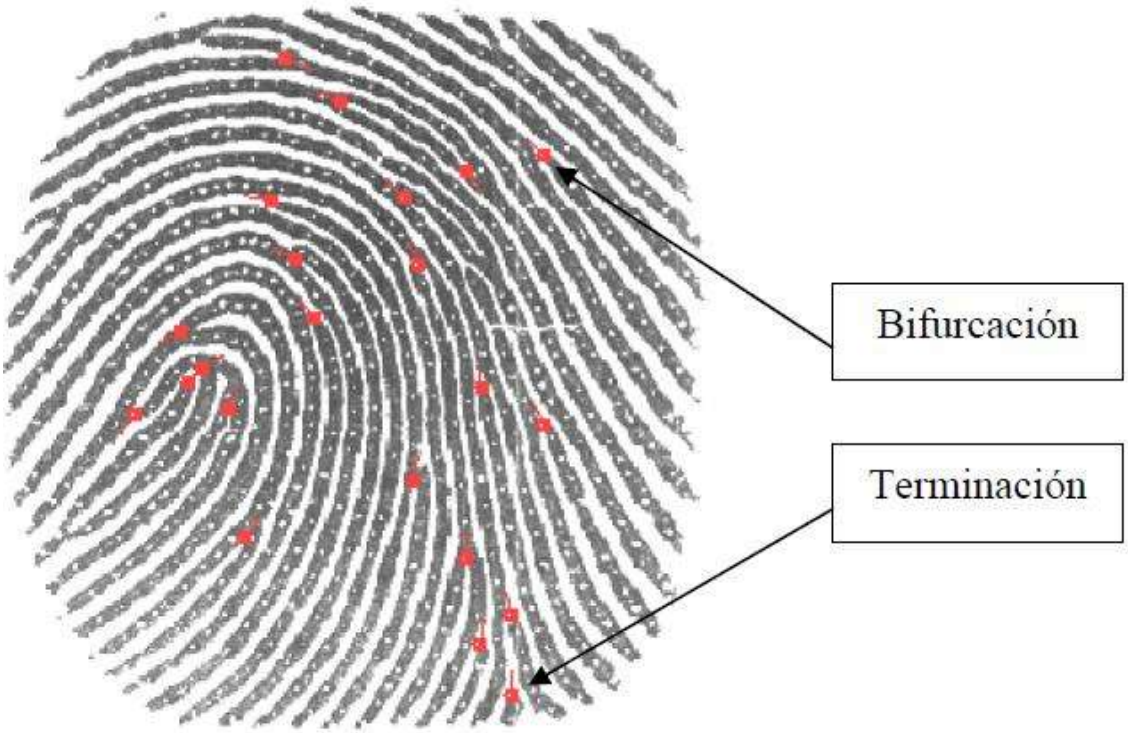


Figura 13: Ejemplo de minucias de tipo bifurcación y terminación en una huella dactilar real.

Otros puntos que permiten clasificar el tipo de huella son el ***núcleo*** y la ***delta*** (Figura 14), siendo posible que existan cero, uno o dos zonas delta en una misma huella dactilar. En función de esta clasificación se definen en [1] las siguientes clases de huella:

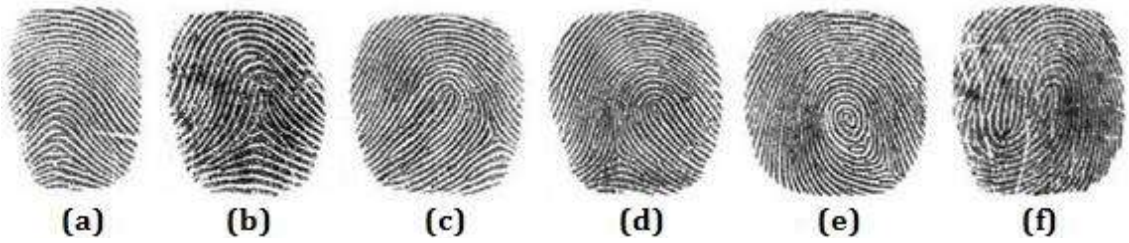


Figura 14: Clases de huellas clasificadas según su núcleo y delta: (a) Arco, (b) Arco tensado, (c) Lazo izquierdo, (d) Lazo derecho, (e) Rizo, (f) Doble lazo.

3.3. Adquisición de la huella dactilar

Existen diferentes maneras de captar una huella dactilar. La adquisición ***off-line*** se trata de un método sencillo que se lleva realizando desde hace siglos. Consiste en humedecer la yema del dedo en tinta y presionar contra una tarjeta de papel. En la adquisición ***on-line***, se presiona la yema del dedo contra una superficie plana de un sensor que guarda la imagen digitalizada de la huella.

Las principales tecnologías de adquisición existentes en el mercado son: óptico, térmico de desplazamiento y capacitivo. Se muestran en la Figura 15 las capturas de la huella dactilar que realiza cada sensor.

Figura 15: Sensores óptico (Fx2000 de Biometrika), térmico de desplazamiento (de Yubee) y capacitivo (TCRU1C de UPEK), y ejemplos de huellas capturadas con dichos sensores.

Para hacernos una idea del funcionamiento de un sensor *on-line*, se explicaran a continuación los sensores existentes en la actualidad: sensores ópticos, sensores de estado sólido y sensores de ultrasonidos.

3.3.1. Sensores ópticos

FTIR (Frustrated Total Internal Reflection)

Es la tecnología existente más antigua y utilizada. El dedo se coloca sobre un prisma de vidrio y es iluminado desde un lateral con un LED. Las zonas que están pegadas a la superficie (crestas) hacen que la luz se refleje y se creen zonas claras, mientras que las zonas más alejadas (valles), absorben la luz y proporcionan zonas oscuras. La diferente reflexión entre las crestas y los valles de la huella es recogida mediante un sensor CCD o CMOS que registrará la huella. En general estos sensores presentan imágenes de muy buena calidad, pero no pueden miniaturizarse ya que introducirían distorsiones en la imagen capturada. Empresas como Compac o Biometrika fabrican sensores de este tipo. Otras como Kinetic Sciences y Ceprop/Sannaedle se basan en el mismo principio para proponer sensores ópticos de desplazamiento. Casio y Alps Electric utilizan para sus sensores de reflexión con desplazamiento una rueda que actúa como prisma con un sensor dentro.

FTIR con prisma laminado

Este sensor busca una reducción en el tamaño del sensor *FTIR* clásico. Para ello se talla la superficie interna del sensor en forma de microprismas que simularán el prisma de mayor tamaño. En general, la calidad de las imágenes se ve reducida.

Fibra óptica

En este tipo de sensores el dedo entra en contacto con una serie de fibras ópticas verticales. La luz residual emitida por el dedo es recogida por un sensor CCD o CMOS que registra la imagen. Mitsubishi propone utilizar una cámara normal, mientras que NEC y Delsy utilizan una cámara CMOS del tamaño del dedo.

Electro-ópticos

Incorporan un polímero que es capaz de emitir luz cuando es excitado con el voltaje adecuado, generalmente bastante alto. El polímero está en contacto directo con la cámara CMOS, que tiene necesariamente el tamaño del dedo. La diferencia de voltaje producida por las crestas y los valles es almacenada en el sensor CMOS.
Existen soluciones diferentes de este tipo de sensores ópticos propuestas por Ethentica y TesTech.

Reflexión sin contacto

Único sensor que no necesita el contacto directo con la huella dactilar. Consiste en tomar una fotografía de muy alta calidad y post-procesarla para corregir posibles distorsiones. Resulta complicado obtener imágenes con la resolución y el contraste necesarios. TST lee la huella utilizando una guía para obtener la distancia óptica

correcta. Thales (Thomson-CSF) propone algo parecido pero utilizando unos polvos especiales para poner en la huella.

3.3.2. Sensores de estado sólido

Capacitivos

Este método de adquisición es utilizado habitualmente en la actualidad. Consiste en una superficie compuesta por una serie bidimensional de placas de condensadores de tamaño reducido. La piel del dedo actúa como una segunda placa de condensadores y dependiendo de la distancia a la que se encuentre, la capacidad será diferente. De esta manera se pueden diferenciar las crestas de los valles. Este tipo de sensores se basa en la medición de un campo eléctrico. En función de esto, el espesor de la capa protectora del sensor debe ser lo suficientemente grueso para soportar campos eléctricos fuertes y, a vez, fino para ser preciso. Adicionalmente, descargas eléctricas pueden causar daños irreversibles al sensor. Empresas como Fujitsu o Sony han propuesto sensores de este tipo.

Térmicos

Son sensores fabricados con material piro-eléctrico, el cual es capaz de convertir cambios de temperatura en un voltaje específico. Estos dispositivos miden la temperatura de las crestas, ya que son las que están en contacto con la superficie, mientras que la zona de los valles permanece con la temperatura de configuración del sensor que habitualmente es elevada para obtener una diferencia de temperatura mayor. El principal problema se presenta cuando ocurre el equilibrio térmico que causa la desaparición de la imagen. Se proponen como solución los sensores térmicos de desplazamiento, donde el dedo es deslizado por el sensor logrando mantener una variación de temperatura. Atmel comercializa estos sensores.

Piezoeléctrico

Se trata de un tipo de sensores para medir presión, fuerza ejercida o aceleración y convertirla en una señal eléctrica. La diferencia entre la presión que ejercen las crestas y los valles wson aprovechadas para formar la imagen. Desafortunadamente, la sensibilidad de estos sensores era muy baja y la imagen resultaba borrosa al añadir una capa protectora. Estos problemas han conseguido solventarse con diferentes métodos: membrana conductora sobre una TFT, membrana conductora sobre un chip de silicio CMOS y switches microelectromecánicos sobre un chip de silicio. Compañías como BMF, Fidelica y Alps Electric comercializan con estos sensores.

Campo eléctrico

Esta clase de sensores incorporan un anillo que genera una señal eléctrica sinusoidal y una matriz de antenas activas recibe la señal modulada por la superficie del dedo. En este caso el dedo debe estar en contacto tanto con el anillo

como con el sensor para un correcto funcionamiento. La señal se amplifica, integra y digitaliza para formar la imagen. Fingerprints Cards propone estos sensores.

3.3.3. Sensores de ultrasonidos

Los sensores de ultrasonidos tienen un funcionamiento parecido al de un ecógrafo: envía señales acústicas a la superficie del dedo y capta las señales de eco recibidas, permitiendo reconstruir la estructura de las crestas y los valles y dando forma a la imagen. La principal ventaja es que "lee" la dermis (capa inferior de la piel) y no la epidermis (capa superior de la piel), con lo que es inmune a suciedad o incluso a materiales que se interpongan entre el dedo y el sensor como unos guantes finos.
Existen también desventajas que han hecho que estos sensores no sean muy comúnmente utilizados. La principal es su complejidad, que hace complicado integrarlo en dispositivos de tamaño reducido y aumenta el coste.

3.4. Extracción de características

El reconocimiento automático de huella dactilar como se muestra en la Figura 4 consta básicamente de los siguientes módulos: adquisición de la imagen, extracción de características y comparación. En el apartado 3.3. se han descrito detalladamente diferentes métodos de adquisición de la imagen. En este apartado profundizaremos en el funcionamiento de los módulos de extracción de características de un sistema basado en minucias.

Antes de entrar en detalle, recordamos que dentro de los diferentes tipos de singularidades, los sistemas automáticos suelen considerar exclusivamente dos: terminación y bifurcación de crestas.

Una coincidencia en un número suficiente de puntos característicos o minucias entre dos huellas, implica que ambas pertenecen a un mismo usuario. Dentro del sistema judicial español 12 minucias coincidentes implica que las huellas pertenecen inequívocamente a una misma persona.

Las minucias suelen estar caracterizadas por las coordenadas **X** e **Y** y por el ángulo que forma la recta tangente a la cresta con el eje horizontal **θ**.

La Figura 16 muestra un esquema general de los módulos de extracción de características enumerados de 'A' a 'E' y explicados en detalle a continuación.

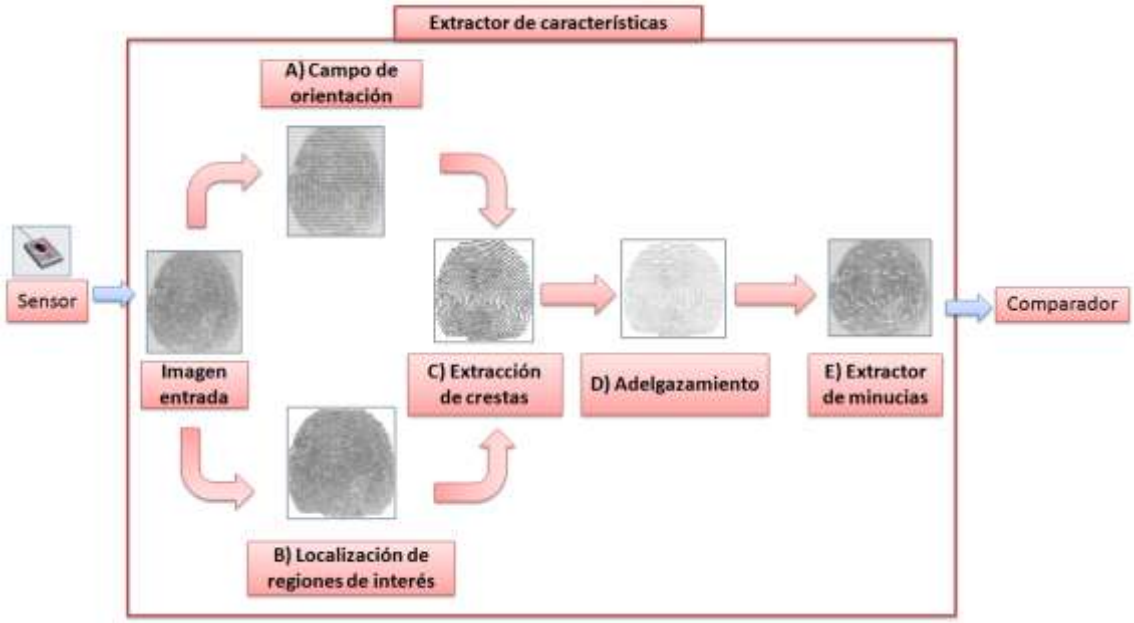


Figura 16: Módulos del extractor de características de un sistema típico de reconocimiento de huella dactilar basado en minucias.

A) Campo de orientación

El campo de orientación de una huella dactilar representa la naturaleza intrínseca de dicha huella y define las coordenadas invariantes para crestas y valles alrededor de cada región local, lo cual juega un papel muy importante en el análisis de la imagen de la huella [2].

Consiste en el cálculo en bloques del ángulo de la cresta respecto a la horizontal. El método más sencillo aparentemente para el cálculo es utilizar el gradiente, pero existen técnicas más robustas empleando medias locales y estimaciones del gradiente. No se realiza pixel a pixel para conseguir una menor sensibilidad con respecto al ruido y una menor carga computacional. De aquí se obtiene una matriz cuyos elementos codifican la orientación local de las crestas y la imagen resultante se utiliza para la detección de puntos singulares: núcleos y deltas.

El cálculo del campo de orientación permite fijar parámetros de funciones adaptativas en los pasos siguientes. Además, al calcularlo se logran corregir las discrepancias entre bloques adyacentes por considerar el entorno.

Con huellas ruidosas o de baja calidad, la detección de singularidades resulta más complicada pudiendo dar lugar a detecciones falsas. La regularización de la imagen de orientación mediante un promediado local suele resultar un método efectivo para evitar la detección de singularidades falsas.

B) Localización de regiones de interés

Para localizar la información es necesario segmentar la imagen separando la región de crestas y valles del fondo de la imagen. Está acción se realiza midiendo la variación de gris de la imagen. En la zona de crestas y valles la variación de gris es

alta en la dirección ortogonal a las crestas. En el fondo de la imagen la varianza de gris es baja para todas las direcciones. Un ejemplo de los pasos a seguir en la segmentación se muestra en la Figura 17 y el resultado final en la Figura 18.

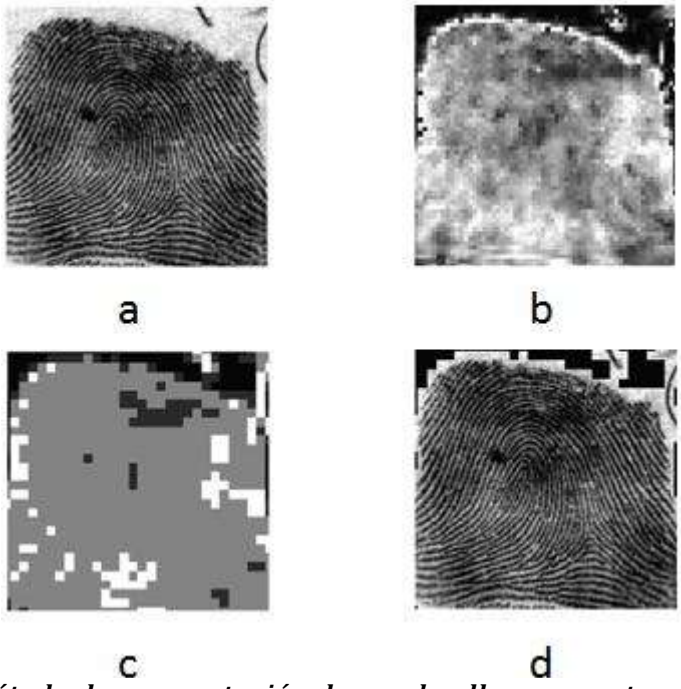


Figura 17: Método de segmentación de una huella propuesto en [34]:a) Imagen original; b) Campo de variación; c) Imagen de calidad derivada del campo de variación: un valor de calidad "bueno", "medio", "bajo" o "fondo" es asignado a cada bloque de acuerdo a su varianza; d) Imagen segmentándose.

Figura 18: Imagen de una huella dactilar a la derecha y su segmentación a la izquierda mediante el uso de máscaras.

C) Extracción de crestas

Para la extracción de crestas es necesario, para empezar, mejorar la imagen para aumentar la claridad de la estructura de crestas y valles. Este paso se lleva a cabo para descartar zonas demasiado ruidosas o de baja calidad producidas por la degradación asociada a las imágenes de huella: crestas que no son estrictamente continuas, crestas paralelas que no se encuentran bien separadas por el ruido, cortes, arrugas o quemaduras.

Las técnicas clásicas de aumento de contraste o claridad empleadas en imágenes genéricas no logran resultados satisfactorios en imágenes de huella dactilar. Por ello se emplean filtros contextuales que modifican sus características en función de la zona que estén filtrando en vez de utilizar un único filtro para toda la imagen.

La estructura de los filtros empleados es 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. En la Figura 19 se muestran filtros de Gabor de diferentes frecuencias utilizados en la actualidad.

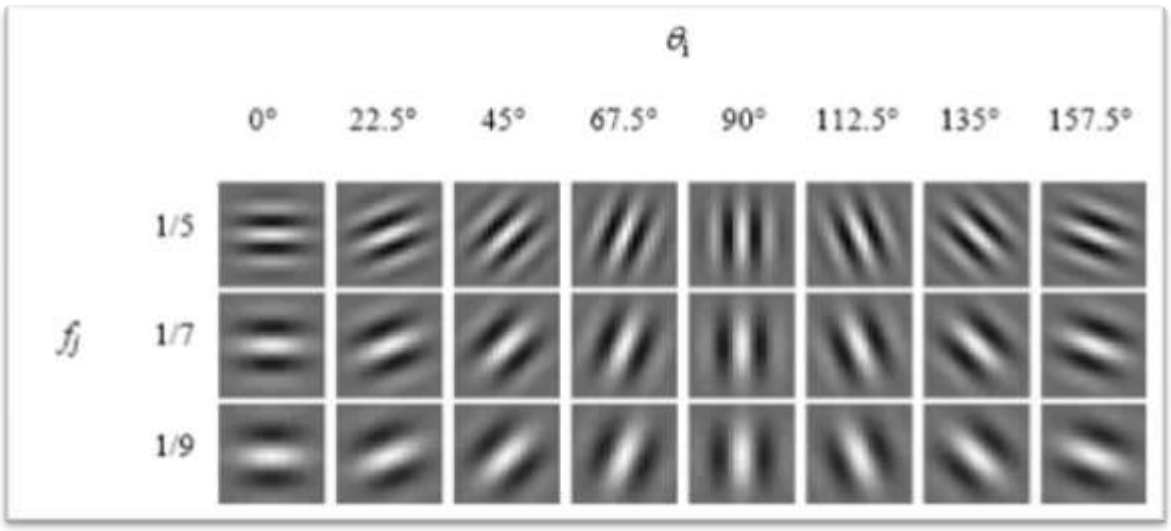


Figura 19: Representación gráfica de 24 filtros de Gabor. Imagen extraída de [35].

La utilización de estos algoritmos de mejora evita que la extracción de crestas sea extremadamente complicada en las regiones corruptas y, en consecuencia, que se extraigan posteriormente minucias espurias, que se obvien minucias verdaderas y que se produzcan errores en la localización de minucias (posición y orientación).

Tras aplicar estas técnicas, se puede binarizar la imagen, es decir, convertir los píxeles en blanco y negro exclusivamente a partir de un umbral establecido. Muchos de los algoritmos utilizados en la actualidad devuelven la imagen ya binarizada, como se propone en [3].

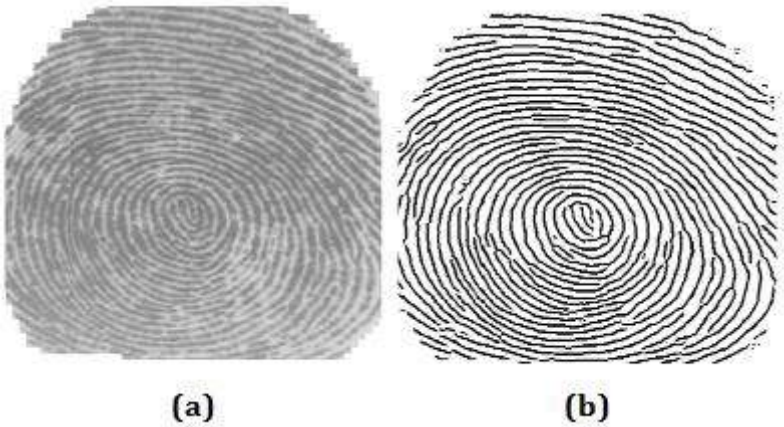


***Figura 20: Ejemplo de huella dactilar: a) tras aplicar filtros de Gabor y b) tras binarizar la imagen. Imágenes extraídas de** [3].*

Algunos autores no realizar la binarización ya que si la imagen no posee la calidad suficiente, la binarización puede empeorar los resultados obtenidos. Además, es un proceso lento y complejo que puede provocar pérdida de información importante.

D) Adelgazamiento

De la imagen binarizada obtenida en el apartado anterior es necesario definir las crestas reduciendo su anchura al tamaño de un pixel. Este proceso ayuda a que la extracción de minucias resulte más factible ya que puede reducir posibles imperfecciones. En la Figura 21 se observa el resultado tras aplicar este módulo.

***Figura 21: Mapa de crestas adelgazadas. Imagen extraída de** [3].*

E) Extractor de minucias

El módulo extractor de minucias parte de la imagen ya binarizada y adelgazada para detectar fácilmente las minucias existentes: si un pixel negro sólo tiene un pixel alrededor, es una terminación; si tiene tres pixeles negros alrededor, entonces será una bifurcación.

Como ya se ha comentado anteriormente, ciertos autores no son partidarios de realizar una binarización y adelgazamiento de la huella y trabajan directamente en escala de gris como ocurre en [4]. Sin embargo, la mayoría de métodos conocidos, como el explicado anteriormente, requieren estos dos pasos previos.

En general, también suele existir una etapa de post-procesado en la cual se eliminan las minucias de los bordes de la huella, se sustituyen grupos muy densos de minucias por una única central y se eliminan minucias que hayan sido localizadas en zonas de baja calidad. Un ejemplo del resultado de los módulos del extractor de características se puede visualizar en la Figura 22.

Figura 22: Mapa de crestas adelgazadas (izquierda), minucias extraídas de la huella adelgazada (centro), minucias válidas tras el post-procesado (derecha).

3.5. 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.

Para averiguar si dos patrones de minucias corresponden a la misma huella necesitamos, como ya se ha expuesto, una medida de similitud o puntuación que constituirá la salida del módulo comparador. Ver Figura 4. La mayoría de algoritmos de comparación presentan, no obstante, una etapa de alineamiento previa a la comparación.

El alineamiento más común, aunque existen muchos tipos, consiste en elegir aquellas minucias (una de cada huella a comparar) cuyas crestas asociadas sean más parecidas. A partir de ese punto de referencia se alinean el resto de minucias estimando la traslación, rotación y distorsión.

Existen en la literatura un gran número de algoritmos automáticos de comparación o *matching* para huellas dactilares [1]. Los desarrollados hasta la fecha pueden clasificarse en: A) Basados en minucias, B) Basados en correlación y C) Basados en texturas.

3.5.1. Basado en minucias

Se trata de la técnica más extendida al ser la que presenta menores tasas de error y en la que se sustenta la comparación manual. El método más común consiste en: pasar las coordenadas de las minucias a polares tomando como origen la minucia de referencia; ordenar las minucias en orden creciente de ángulo y distancia, formando así, sendas cadenas de puntos que serán los patrones a comparar; calcular entonces el número de minucias coincidentes definiendo un entorno capaz de indicar si dos minucias forman pareja o no; y calcular una medida global de similitud.

Los sistemas de verificación de huella dactilar estudiados en el presente proyecto están basados en la comparación de plantillas de minucias.

3.5.2. Basados en correlación

Las imágenes del par de huellas a comparar se superponen y se calcula la correlación entre pixeles equivalentes para diferentes alineamientos (variaciones en la posición y el ángulo). Se suele calcular directamente entre imágenes en escala de grises (sin binarizar y adelgazar) para mantener toda la información de la imagen. Además, normalmente se seleccionan una serie de regiones locales y se calcula la correlación sólo en esos puntos, consiguiendo así, robustez frente a las deformaciones no lineales.

3.5.3. Basados 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 texturas), en general menos distintivas, pueden obtenerse de manera más robusta. Además, la carga computacional es menor ya que no es necesaria la binarización ni adelgazamiento de la imagen.

Este método se sirve del patrón de campo de orientación (comportamiento de las crestas) sabiendo que en un patrón de crestas y valles existe una estructura orientada con frecuencia espacial y orientación localmente constantes. Utiliza filtros de Gabor con diferente orientación.

Cabe mencionar, como característica negativa, que tiene una menor capacidad discriminativa y por tanto mayor tasa de error con respecto a la comparación basada en minucias. Suele utilizarse como método complementario a los comparadores basados en minucias.

4

Ataques a sistemas de reconocimiento biométrico

4.1. Introducción

Tras el alto crecimiento en implantación de sistemas de reconocimiento biométrico, se hace necesario evaluar la seguridad y robustez que proporciona este tipo de tecnología. Como ya habíamos comentado, la identificación de un usuario debe hacerse de forma fiable ya que el acceso no sólo está restringido a ordenadores o redes, sino que también son utilizados en la vida cotidiana para acceso físico a edificios, puntos de entrada/salida restringidos, control de puesta en marcha de vehículos, identificación del cliente en el punto de venta, etc. Las consecuencias de un sistema de reconocimiento inseguro pueden ser muy graves, ya que pueden suponer la pérdida, robo o modificación de información confidencial, lo que refuerza la necesidad de estudiar y evaluar las fortalezas y debilidades de este tipo de sistemas [5].

Se asume que los rasgos biométricos no pueden ser robados, si bien esto no es del todo cierto. Por ejemplo, a diario posamos las manos en superficies dejando nuestras huellas dactilares y comprometiendo así nuestro rasgo biométrico. El mayor problema es que resulta muy complicado volver a un estado seguro (siempre puede regenerarse una clave o un PIN, pero tenemos un número limitado de rasgos biométricos).

Se han comentado extensamente las virtudes que poseen los sistemas biométricos frente a los sistemas tradicionales, pero no nos podemos olvidar de las vulnerabilidades que poseen los sistemas de reconocimiento automático. A continuación se citan las diferentes amenazas [1] a las que se expone un sistema de seguridad en general:

- **Puenteo del sistema:** un usuario no autorizado logra acceso fraudulento al sistema y a los datos que éste posee.

- **Repudio:** el usuario que intenta acceder legítimamente, obtiene negación de acceso al sistema.
- **Contaminación o adquisición encubierta:** los medios de reconocimiento del usuario se ven comprometidos por ser usados por el impostor sin conocimiento del usuario legítimo.
- **Colusión:** acceso al sistema como súper-usuario de un usuario no autorizado dándole privilegios como toma de decisiones.
- **Coerción:** usuario obligado a identificarse a sí mismo en el sistema.

Estas amenazas son generalmente el resultado de posibles ataques al sistema sobre distintos puntos vulnerables de un sistema de reconocimiento biométrico llevados a cabo por un agente externo.

4.2. Tipos de ataques

Diversos grupos de investigación han hecho un esfuerzo por catalogar y clasificar diferentes tipos de ataques a los que puede ser sometido un sistema de reconocimiento biométrico basado en huella dactilar.

En concreto, en [6] se han analizado los posibles puntos de ataque clasificándolos en ocho categorías. En la Figura 23 se pueden ver estos puntos de ataque junto a los componentes básicos de un sistema biométrico. Los puntos potenciales son los siguientes:

- Ataques al sensor o escáner (punto 1 en la Figura 23).
- Ataques al módulo extractor de características (punto 3).
- Ataques al módulo comparador (punto 5).
- Ataques a la base de datos del sistema (punto 6).
- Ataques a los distintos canales de comunicación entre los módulos existentes en el sistema (puntos 2, 4, 7 y 8).

El ataque al sensor o escáner es un tipo de ataque **directo** al sistema, y en él, el atacante no tiene ningún conocimiento sobre el funcionamiento de dicho sistema. El resto de ataque se denominan **indirectos** y van dirigidos a alguno de los módulos internos del sistema. En ellos el imposto necesita de algún tipo de conocimiento sobre el funcionamiento o estructura interna del sistema (por ejemplo, características extraidas o el formato de la plantilla).

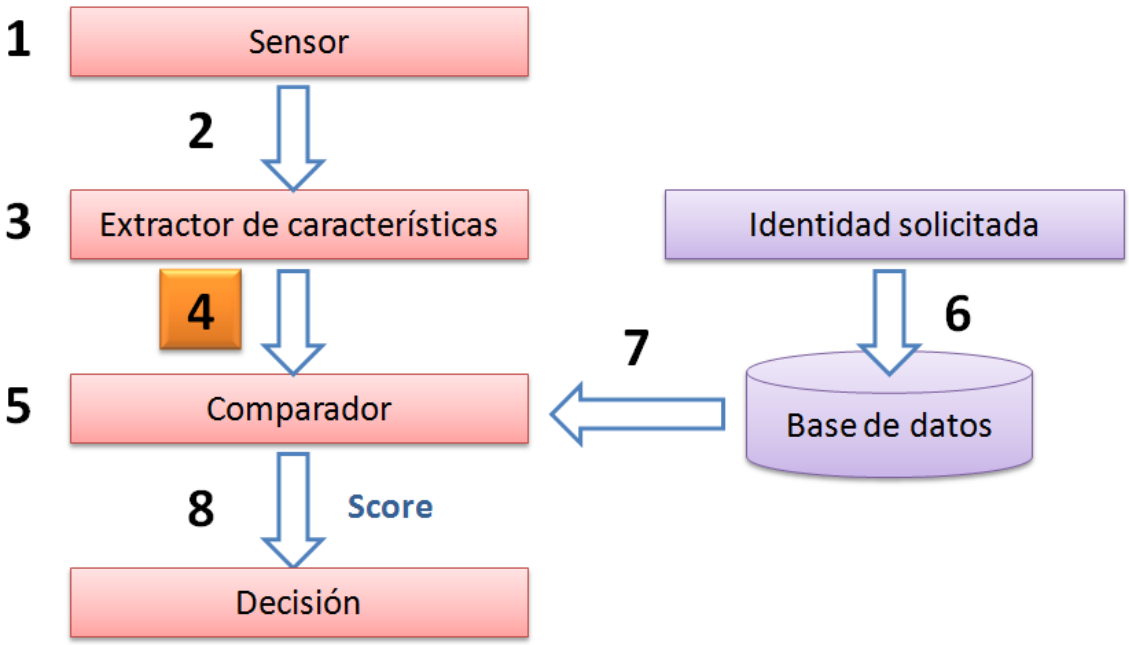


Figura 23: Potenciales puntos de ataque a un sistema de reconocimiento biométrico. Se resalta el punto de ataque que se analizará en el presente proyecto.

Los ataques lanzados directamente sobre los módulos del sistema (1, 3, 5 y 6) se denominan **ataques Troyanos.** En cambio, los que se lanzan sobre los canales de comunicación entre los módulos del sistema (2, 4, 7 y 8) son referenciados como **ataques de repetición**.

1) Ataques al sensor

Existen diversos ejemplos en la literatura sobre ataques basados en la presentación de rasgos biométricos falsos al sensor. Estos ataques han demostrado ser muy exitosos ya que sólo necesitan generar el rasgo biométrico sin tener que conocer el funcionamiento del módulo comparador o las especificaciones de las plantillas. En consecuencia, en el caso concreto de la huella dactilar, para poder llevar a cabo este tipo de ataques sólo se requiere un dedo falso del usuario a suplantar.

Además, al operar en el dominio analógico, los mecanismos de protección digitales como encriptación, *hashing* (técnicas de transformación no invertible), firma digital, etc., no son aplicables.

Normalmente se había pensado que la plantilla de minucias constituía una representación compacta de las características de la imagen original sin suficiente información como para poder reconstruir dicha imagen.

En [7] se cuestionan estas teorías dando lugar a unas conclusiones básicas, utilizadas en [8] para un estudio preliminar sobre la evolución de la vulnerabilidad de los sistemas de verificación de huella dactilar frente a ataques directos. Dichos ataques, se basan en la utilización de huellas falsas creadas a partir de plantillas

estándar de minucias. Se demuestra en [8], que el ataque propuesto es perfectamente factible y supone una amenaza sobre el uso de plantillas de minucias sin encriptación.

La creación de dedos de goma como huella artificial para este tipo de ataques, se puede realizar con o sin la colaboración del dueño del rasgo biométrico. Cabe esperar, que los ataques al sistema serán más exitosos si el dedo artificial se crea con la colaboración del usuario por tener una calidad de imitación mayor.

En [9], se probó la vulnerabilidad de seis sensores de huella frente a dedos de goma (plastilina y silicona) creados artificialmente. Cinco de los seis sensores probados aceptaron al dedo de goma como real.

En [10], se atacaron once sistemas de verificación diferentes con dedos artificiales de goma (gelatina) consiguiendo engañar a todos los sistemas siempre y cuando, el usuario colaborase a la hora de crear la huella artificial.

En [11] se presentó otro método de creación de dedos de goma y se probó para dos sistemas de verificación diferentes, uno basado en minucias y otro en patrones de cresta. Los resultados de estos experimentos, concluyeron que en general el funcionamiento del sistema basado en crestas es peor que el basado en minucias, aunque menos vulnerable a ataques directos y más resistentes a muestras de baja calidad.

Uno de lo métodos frente a ataques directos al sensor que más referencias está adquiriendo en la actualidad es la detección de vida. Los métodos tradicionales en detección de vida utilizan medición de características fisiológicas como el pulso, la temperatura, el sudor [12] [13], la elasticidad de la piel [14] [15] o el olor [16]. Técnicas más recientes utiliza: métodos software para analizar características medibles [17]; múltiples características estáticas (espaciado entre poros, ruido,…) obtenidas de una sola imagen [18]; estudio de la textura superficial de la huella a través de wavelet (ondícula) [19]; o el espectro de Fourier en banda selectiva [20].

2) Ataque al canal entre el sensor y el extractor de características

Se trata de un ataque tipo 2 mostrados en la Figura 23.El canal de comunicación puede ser interceptado y se puede introducir otra información que sustituya a la enviada por el sensor o bien guardar la imagen de la huella digital del usuario legítimo para ser replicada posteriormente y presentada al extractor de características.

3) Ataques al extractor de características

Un programa tipo Troyano (código ejecutable que no es directamente la traducción original del programa, sino que ha sido añadido con posterioridad y que entra simulando ser el original) puede suplantar al extractor de características y enviar características generadas a voluntad del atacante (generadas artificialmente) al comparador.

Para este tipo de ataques tipo 3 representados en la Figura 23, se propone en [6] un sistema basado en desafío/respuesta como método de protección.

4) Ataques al canal entre el extractor de características y el comparador

De forma parecida al ataque 2, se puede intentar enviar información al comparador introducida por el canal. Además, es posible obtener y guardar un conjunto de características del rasgo biométrico de un usuario legítimo y reproducirlas en otro momento o incluso reemplazarlas por un conjunto fraudulento de características.

Habitualmente, las fases de extracción de características y comparación están completamente ligadas y son inseparables. En ataques a sistemas de reconocimiento biométrico donde las minucias son transmitidas a un comparador remoto, puede convertirse en una amenaza considerable.

En el proyecto que nos atañe se trabajará sobre este tipo de ataques, por lo que más adelante se describirán diversos ejemplos de estudio que analizan su eficiencia.

5) Ataques al comparador

Al igual que en los ataques de tipo 3, se trata de introducir un programa Troyano que suplante al comparador modificando las puntuaciones (*scores*) o la decisión final (si o no) que se envía a la aplicación de autenticación.

Si el programa Troyano envía siempre respuestas afirmativas, se dice que estamos ante un **puenteo del sistema**, [1]. Si, por el contrario, la respuesta es siempre negativa o las puntuaciones son bajas, se habla de una **negación del servicio**.

6) Ataques a la base de datos

Este ataque puede lanzarse durante el proceso de registro, etapa de verificación o directamente sobre la base de datos en cualquier momento mediante un programa Troyano que suplante a la base de datos enviando información generada artificialmente (plantillas, nombres de usuarios, etc.)

Para el caso de una aplicación sobre tarjeta inteligente, es importante que esté protegida correctamente mediante por ejemplo, técnicas de encriptación [21], porque la pérdida de la tarjeta permite el acceso directo al impostor a la plantilla (*template*).

Otro método de protección de plantillas biométricas supone la utilización de una versión distorsionada de la señal biométrica no invertible o el vector de características [22]. Esto permite cambiar la transformación de distorsión en el momento en que la plantilla se vea comprometida.

7) Ataques al canal entre la base de datos y el comparador

El canal puede ser interceptado, en este punto, para robar el registro de un usuario legítimo y extraer la información que se envía a través de él. Dicha información puede ser reproducida posteriormente.

8) Ataques al canal entre el comparador y la aplicación

La información que circula por el canal entre la aplicación que solicita una verificación y el comparador puede ser interceptada y guardada para ser utilizada más adelante. Es decir, la decisión final del sistema (si o no) queda en manos de la voluntad del intruso.

4.3. Ataques *hill-climbing*

Los ataques *hill-climbing* a sistemas de reconocimiento biométrico consisten en la sucesiva modificación de un patrón de características obtenido sintéticamente hasta conseguir que el sistema acepte dicho patrón.

Pueden realizarse ataques *hill-climbing* de tipo 2 (según la clasificación de la Figura 23), es decir, atacar al canal de comunicaciones que existe entre el sensor y el extractor de características; o bien se pueden realizar ataques de tipo 4 que consisten en atacar al sistema en el canal de comunicación entre el extractor de características y el módulo comparador.

La Figura 24 muestra un esquema general de ataques *hill-climbing* tipo 4 basado en puntuación o *score*. Para este tipo de ataque se requiere conocer el formato de la plantilla.

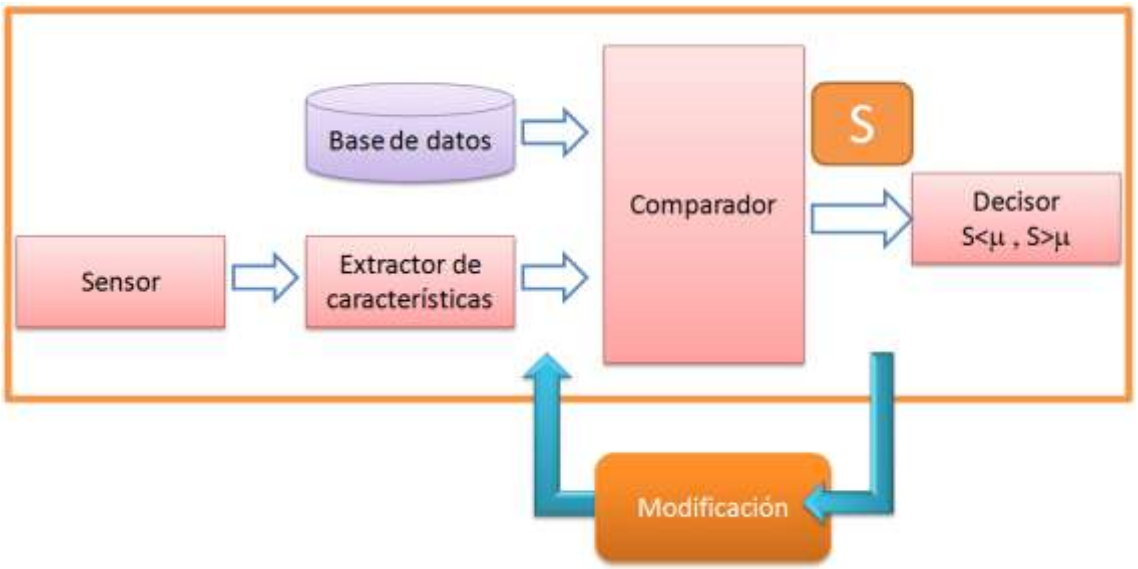


Figura 24: Ataque hill-climbing tipo 4 basado en puntuación.

En el presente proyecto se llevarán a cabo ataques *hill-climbing* entre el extractor de características y el comparador (sobre dos sistemas de reconocimiento de huella dactilar basados en minucias) y cuya implementación se propuso en [23] y se analizó en profundidad en [24]. En aquellos casos, los ataques se centraban en la puntuación obtenida por el comparador.

Como método de protección al sistema, en general, no se revela la puntuación por el sistema biométrico, de esta manera, basaremos nuestro algoritmo en el tiempo que emplea el comparador como se propuso en [25].

4.4. Ataques *side-channel*

Un ataque *side-channel* [26] se produce cuando un atacante es capaz de utilizar información adicional obtenida de la implementación física de un sistema criptográfico. Si la información *side-channel* es suficiente, permitirá romper un sistema cifrado.

No se trata de ataques por fuerza bruta que aprovechan la existencia de una tasa de falsa aceptación, sino que utilizan información de la implementación del sistema como puede ser el tiempo (*timing-attacks*) [27], el consumo de energía (*power-attacks*) [28], las pérdidas electromagnéticas o el ruido del sistema.

Existen varios tipos de ataques *side-channel*, dentro de los cuales, aquellos basados en la información temporal han demostrado tener una gran eficiencia. Estos ataques denominados *timing-attacks* se han convertido en una amenaza real a tener en cuenta a la hora de implementar sistemas de seguridad, por lo que profundizaremos a continuación en su funcionamiento.

4.4.1. Basados en tiempo: *Timing-Attacks*

Estos ataques fueron desarrollados en [27] para romper sistemas criptográficos. En principio, las características temporales sólo revelan una pequeña cantidad de información sobre un sistema criptográfico como puede ser la longitud de una clave, pero está demostrado que algunos ataques son capaces de encontrar la clave secreta en sí.

Los sistemas criptográficos suelen utilizar tiempos diferentes según la entrada que estén procesando. Para que esto no ocurra se suele optimizar el código del algoritmo evitando operaciones innecesarias o aquellas que no se ejecuten en un tiempo fijo.

El funcionamiento de los ataques *side-channel* basados en tiempo consiste en monitorizar el movimiento de datos que entra y sale de la CPU o la memoria. Sabiendo el tiempo que tarda en mover cierta información es posible saber la longitud que puede tener una clave, o de manera más clara, la longitud que seguro no va a tener.

Diferentes estudios sobre sistemas criptográficos basados en el tiempo requerido para efectuar operaciones, el tiempo total de ejecución o el tiempo sobre servidores de red, han demostrado que este tipo de ataques son factibles para estos sistemas [27], [29], [30].

En la parte experimental del proyecto se propone, en primer lugar, implementar ataques *hill-climbing* clásicos con el objetivo de fijar una serie de parámetros iniciales necesarios para realizar los *timming-attacks*. En segundo lugar se comprobará si existe alguna relación entre el tiempo de comparación y la puntuación devuelta por los sistemas de reconocimiento de huella dactilar basado en minucias. Para terminar, se probará a partir de la relación temporal la eficiencia de diferentes ataques *hill-climbing* basados en el tiempo de comparación algorítmica.

5

Entorno experimental

5.1. Introducción

Las pruebas experimentales realizadas en este proyecto se han llevado a cabo sobre dos sistemas reales de reconocimiento de huella dactilar basados en minucias: Software de referencia NFIS2 del NIST americano y un sistema integrado de tarjeta inteligente o, también llamado, *Match-on-Card* (*MoC*).

5.1.1. Software de referencia NFIS2 del NIST

Los ataques se llevarán a cabo, en primer lugar, sobre el sistema de verificación basado en minucias NFIS2 del NIST (*National Institute of Standards and Technology*).

Este software para imagen de huella fue desarrollado por el FBI y el Departamento de Seguridad Nacional de los Estados Unidos. Consiste en una colección de programas, aplicaciones y librerías de código fuente organizadas en módulos para realizar diferentes funciones como clasificar las huellas, segmentarlas, detectar minucias o determinar la calidad de las imágenes.

En definitiva, este software resultante de más de una década de trabajo es reconocido a nivel mundial como referencia de verificación de huella dactilar. Por esta razón, los sistemas diseñados en la actualidad se suelen comparar con el sistema NFIS para obtener una primera medida comparativa del rendimiento.

Dentro de los distintos módulos encontrados en el software NFIS2 vamos a utilizar para desarrollar el proyecto los siguientes:

- **MINDTCT**: detección de minucias en la imagen de huella dactilar de entrada así como asignación de coordenadas, orientación, tipo y calidad a cada minucia. La arquitectura de MINDTCT consta de un preprocesado y un extractor de características como se puede observar en la Figura 25.

- **BOZORTH3**: comparador de huellas dactilares a partir de los patrones de minucias generando una puntuación que resultará mayor cuanto más parecidas sean las huellas dactilares. Este módulo puede funcionar tanto en modo verificación como identificación.
- **NFIQ**: módulo que ejecuta algoritmos de estimación de calidad de las huellas dactilares basándose en la calidad de las minucias resultante de MINDTCT.

Para entender mejor el funcionamiento, vamos a profundizar en cada uno de los módulos nombrados anteriormente que intervienen en el proceso de verificación de usuarios.

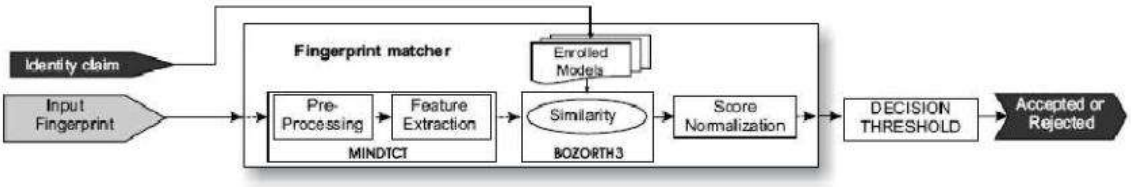


Figura 25: Arquitectura general del sistema NFIS2.

5.1.1.1. MINDTCT

Este módulo permite localizar minucias de tipo terminación y bifurcación de la huella dactilar de entrada almacenando la siguiente información: ubicación, tipo, orientación y calidad.

El proceso de detección de minucias sigue el siguiente algoritmo mostrado en la Figura 26 a partir de la imagen de la huella dactilar de entrada:

Figura 26: Arquitectura del módulo MINDTCT.

1) ***Generar mapas de calidad de la imagen*:** Paso importante para encontrar zonas degradadas de la imagen que pueden dar lugar a problemas. Principalmente, las características utilizadas para detectar la calidad son las áreas de la imagen que incluyen las regiones de bajo contraste(o regiones que no pertenecen a la huella dactilar), bajo flujo de crestas y alta curvatura (donde es probable que se encuentre el núcleo y la detección de minucias resulte más complicada).

2) ***Binarización de la imagen***: El proceso de detección de minucias se realiza en los siguientes pasos para imágenes de dos niveles de color donde los píxeles negros representan las crestas y los blancos los valles de la huella.

3) ***Detección de minucias:*** Escaneo de la imagen para identificar terminaciones o bifurcaciones de una cresta. Esta acción puede introducir muchas minucias que darán lugar a error.

4) ***Eliminar minucias falsas:*** Paso para eliminar todas las minucias de baja calidad, aquellas minucias que están demasiado próximas y minucias que son susceptibles de ser producto de una detección errónea.

5) ***Contar crestas vecinas:*** Se cuentan las crestas existentes entre una minucia y sus minucias vecinas para su utilización en otros módulos del sistema NFIS2. Es habitual guardar información adicional para ser utilizada por el comparador.

6) ***Establecer calidad de las minucias:*** Aunque en pasos anteriores se ha intentado eliminar las minucias falsas, es posible que quede alguna entre las minucias candidatas. Por esa razón, es necesario establecer la calidad a partir de los mapas generados en el apartado 1).

7) ***Fichero de minucias de salida:*** El fichero de salida es un documento de texto que contiene una lista de minucias con sus coordenadas, ángulo de rotación y nivel de calidad.

5.1.1.2. BOZORTH3

Como se ha comentado anteriormente, BOZORTH3 es el módulo comparador entre dos huellas a partir de los patrones de minucias (por lo menos requiere de dos ficheros). El algoritmo que realiza es invariante frente a rotaciones y traslaciones entre las huellas. Se divide en tres fases:

1) ***Construcción de tablas de comparación de minucias intra-huella:*** Se construye una tabla para la huella de test y otra tabla para cada huella plantilla (*template*) con la que se vaya a comparar. El contenido de las tablas es: posición de las minucias, distancia relativa de cada minucia con respecto a las demás de la huella, ángulo de la línea que las une y ángulos de orientación de las minucias con respecto a la línea que las une como muestra la Figura 27.

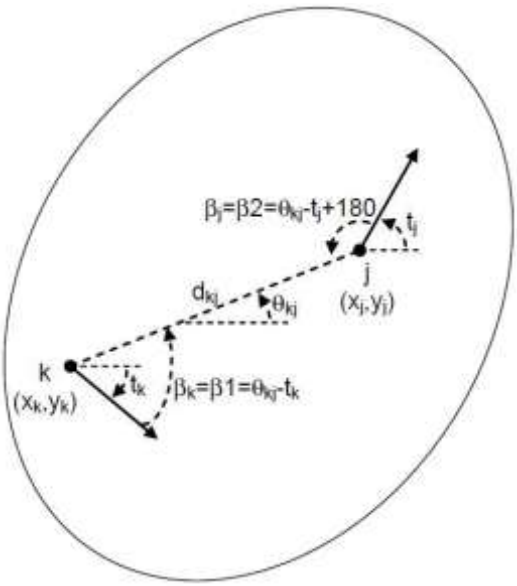


Figura 27: Comparación de minucias intra-huella. Imagen extraída de [36] .

2) ***Construcción de tablas de compatibilidad inter-huella:*** La tabla de compatibilidades se crea buscando entradas compatibles entre la tabla de comparación de minucias de la huella de *test* y la tabla de comparación de minucias del *template*. Las comparaciones se realizan mediante tres *tests*: en primer lugar se comprueba que la distancia relativa entre las minucias es similar aplicando una cierta tolerancia. Posteriormente se comprueba mediante dos *tests* que los dos ángulos de orientación son también similares. Si esto es así, se almacena esta entrada en la tabla de compatibilidades junto con la orientación global para poder agrupar minucias. De esa manera se crea una lista de asociación de compatibilidad entre dos pares de minucias potencialmente correspondientes.

3) ***Recorrer la tabla de compatibilidad inter-huella*:** Se recorre la tabla para enlazar entradas pudiendo formar agrupaciones de minucias. A continuación, se combinan las agrupaciones compatibles y se van acumulando las puntuaciones de comparación. La puntuación devuelta por BOZORTH3 se calcula construyendo grafos y buscando el recorrido que más asociaciones de minucias compatibles produce.

5.1.1.3. NFIQ

Se trata de un algoritmo descrito en [31] que mide la calidad de la imagen de la huella dactilar de entrada tras extraer las características de la misma con el módulo MINDTCT. El algoritmo proporciona como salida valores del 1 al 5 que corresponden a alta y baja calidad respectivamente. Se ha utilizado en el presente proyecto para comparar la calidad de las huellas adquiridas con el sensor óptico y térmico.

5.1.2. Sistema basado en tarjeta inteligente *Match-on-Card*

El segundo escenario considerado en el presente proyecto es un sistema basado en tarjeta inteligente o *Match-on-Card* en el que la comparación entre huellas se realiza en el propio chip de la tarjeta limitando así la capacidad de almacenamiento y de cómputo.

Esta tecnología ha cobrado gran relevancia en los últimos años al evitar utilizar una base de datos centralizada para el almacenamiento de las plantillas y por tanto, solventa problemas de comunicación entre la base de datos y el sistema. De esta manera, el poseedor de la tarjeta es portador tanto de su huella como del sistema de comparación necesario para verificar al usuario.

Existen numerosas ventajas para esta tecnología como la seguridad que aporta el realizar la comparación en un sistema cerrado, la privacidad proporcionada al ser el usuario genuino el único poseedor de su huella dactilar, la consistencia debido a que el proceso de comparación no puede ser modificado al ser realizado dentro de la tarjeta inteligente o la alta facilidad de integración y escalabilidad. El sistema de reconocimiento es propietario, lo que implica que no tenemos conocimiento de su funcionamiento (salvo el formato de la plantilla) y por tanto la simulación del ataque se realiza en un entorno totalmente real.

Al igual que encontramos ventajas claras para este tipo de sistemas, hay que tener en cuenta las limitaciones hardware en cuanto a capacidad de almacenamiento y de cómputo. Dichas limitaciones hacen que el rendimiento y la eficiencia de estos sistemas sean menores que para los sistemas clásicos al emplear, necesariamente, un algoritmo menos complejo y que se va a ejecutar de manera más lenta.

En la Figura 28 se muestra el dispositivo *Match-on-Card* empleado en los experimentos. El sistema está formado por un lector de tarjeta inteligente modelo LTC31 del fabricante C3PO conectado a un ordenador mediante USB y una tarjeta inteligente con un chip integrado.

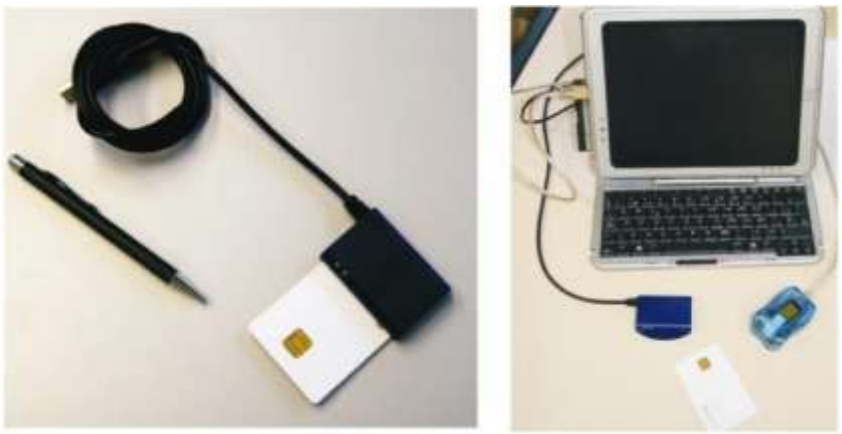


Figura 28: Sistema Match-on-Card empleado en el proyecto. Nótese en la fotografía de la izquierda que la tarjeta inteligente ha sido insertada al revés para poder observar el chip.

La comunicación con la tarjeta se realiza mediante el driver de la misma y librerías de MS Windows para el manejo de *smart-cards*. Todos los ataques están automatizados mediante MATLAB pudiendo así lanzar pruebas masivas y almacenar automáticamente estadísticas de los resultados.

5.2. Base de datos

La base de datos utilizada en el proyecto ha sido BiosecurID [32], presenta una serie de características destacables: 8 rasgos biométricos diferentes (voz, iris, cara, firma y forme de escribir, huella dactilar en dos sensores diferentes, mano y forma de teclear); número alto de sujetos adquiridos (400); 4 sesiones distribuidas en 8 meses; distribución equilibrada de hombres y mujeres; y distribución equilibrada de usuarios por grupos de edades.

Las huellas utilizadas en la parte experimental se obtienen de cada uno de los 400 usuarios. Cada usuario realizó 4 sesiones en cada una de las cuales se adquirieron 4 huellas diferentes (dedos índice y corazón de la mano derecha y de la mano izquierda) y 4 muestras de cada huella. Esta operación se realizó para una adquisición con sensor óptico (BiométricaFX2000) y otra con sensor térmico de barrido (Yubee- Atmel sensor), ambos utilizados en los experimentos.

De esta manera, se obtiene para cada tipo de sensor: 400 usuarios $*$ 4 huellas diferentes por usuario=1600 usuarios con 16 muestras cada uno (Figura 29).

Figura 29: Huellas utilizadas en la parte experimental del proyecto para cada tipo de sensor.

La Figura 30 muestra ejemplos de huellas de la base de datos BiosecurID, así como su organización interna.

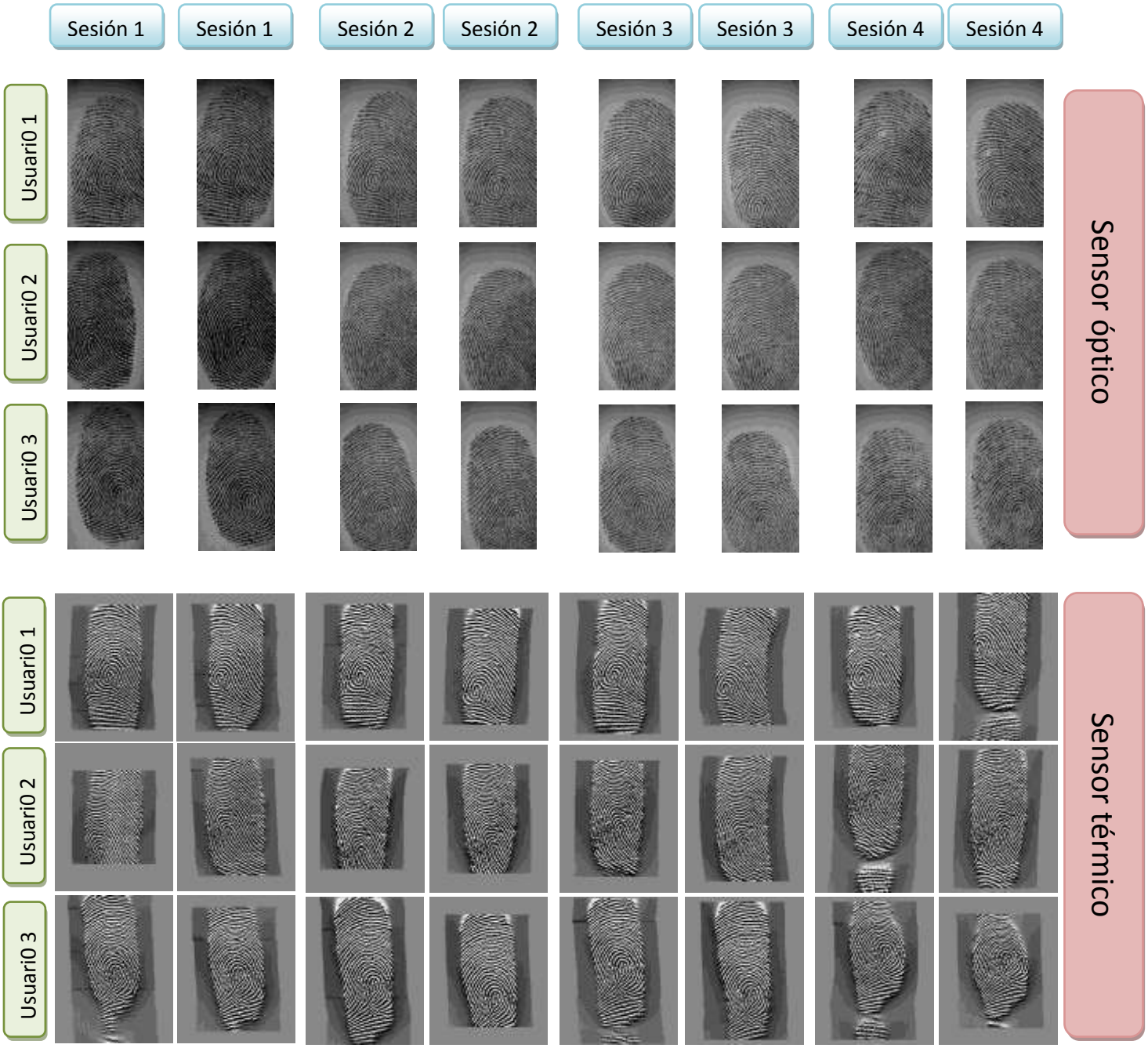


Figura 30: Ejemplos de huellas dactilares pertenecientes a la base de datos BiosecurID adquiridas en cuatro sesiones por usuario y mediante un sensor óptico de presión y un sensor térmico de barrido.

Todas las huellas son empleadas en algún momento en los sistemas propuestos y , por tanto, se introducen en el módulo extractor de características.

Para la extracción de minucias se utiliza el módulo MINDTCT del software NFIS2 explicado en 5.1.1. El patrón de minucias que emplea MoC es equivalente a BOZORTH3 pero limitado por la capacidad del chip, es decir, restringe el número de minucias de la huella a 42. Para cumplir esta restricción, las huellas donde MINDTCT detecta más de 42 minucias se ordenan en orden decreciente de calidad y se escogen únicamente las 42 minucias de mayor calidad.

Tras la extracción de minucias con MINDTCT se observa que existe un alto número de minucias en los bordes de la huella o incluso en zonas del fondo de la imagen. Estas falsas minucias afectan negativamente al rendimiento del sistema y se eliminan mediante una etapa de post-procesado.

En la Figura 31, se puede observar el proceso de eliminación de minucias que realiza los siguientes pasos:

1) Se extraen las minucias.
2) Con la ayuda de los mapas de calidad generados por MINDTCT se detectan las zonas de peor calidad (corresponden a zonas donde no existe huella)
3) Se eliminan las minucias que están cerca de la frontera.

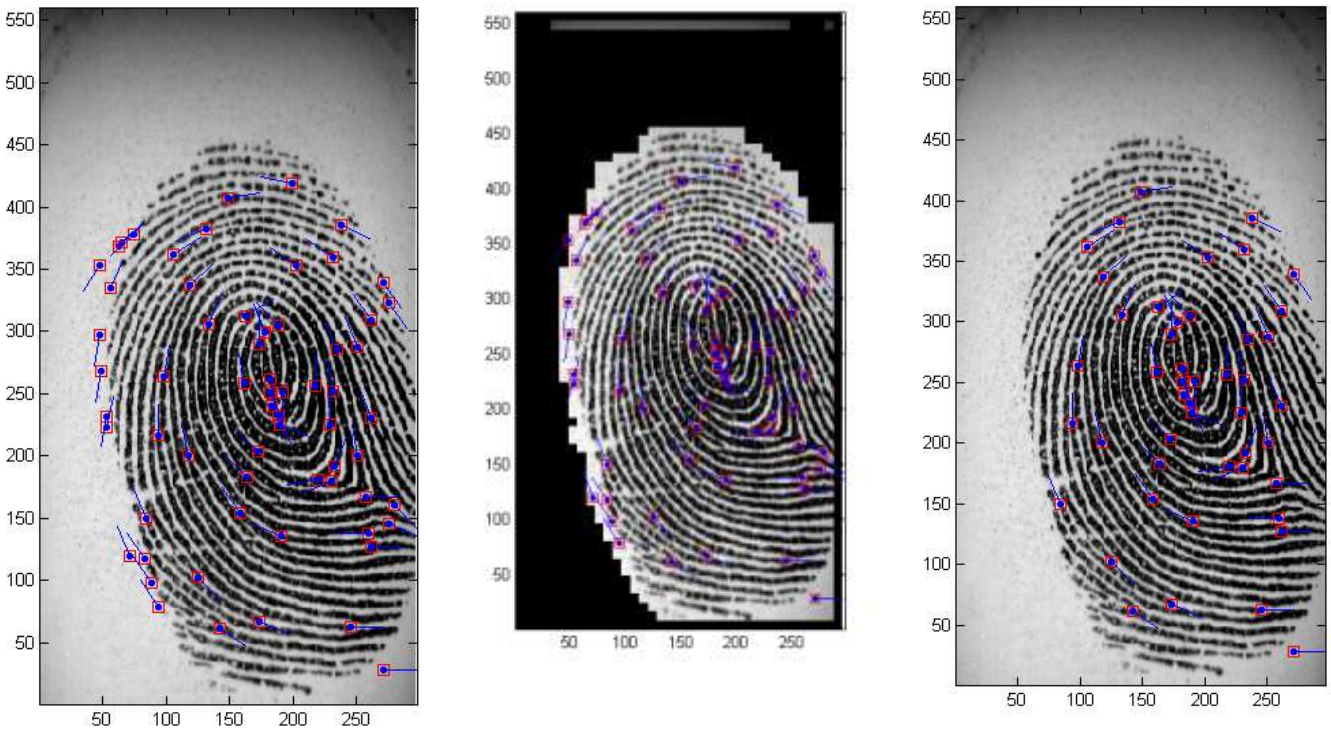


Figura 31: Proceso de eliminación de minucias en los bordes de la huella dactilar. Se muestra de izquierda a derecha los pasos que realiza: extracción de minucias, detección de zonas de peor calidad y eliminación de minucias de la frontera.

La mayor parte de las minucias se localizan dentro de un área elíptica centrada en la imagen de la huella dactilar a la que denominaremos de ahora en adelante ROI (*Region of Interest*) o región de interés.

Este proceso ayuda a mejorar el rendimiento del sistema, por lo que todos los experimentos realizados en este proyecto se han llevado a cabo con las huellas post-procesadas.

5.3. Rendimiento de los sistemas

El primer paso antes de realizar una evaluación de la vulnerabilidad de un sistema biométrico frente a un ataque es determinar el punto de funcionamiento en el que opera el sistema, ya que la tasa de éxito del ataque variará en función de dicho punto de operación.

Así pues, en este apartado se ha estimado el rendimiento para los sistemas NFIS2 y MoC descritos en 5.1. Tomando como plantillas cada uno de los 4 dedos de cada usuario que conforma la base de datos, tenemos 1600 plantillas diferentes. Como cada usuario posee 16 muestra de cada huella dactilar, las puntuaciones genuinas se calcularán comparando cada plantilla con las 15 muestras restantes del usuario, obteniendo 1600x15= 24000 puntuaciones genuinas. Para el caso de los impostores, se ha comparado cada plantilla con 100 muestras de impostores (1 muestra de cada uno de los 100 usuarios siguientes) dando lugar a 1600x100=160000 medidas de similitud. Ver Figura 32.

Figura 32: Conjunto de puntuaciones genuinas y de impostor calculadas para evaluar el rendimiento de los sistemas.

A partir de las puntuaciones obtenidas se han representado las distribuciones de *scores* genuinos y de impostor que caracterizan a los diferentes sistemas. Para organizar los resultados obtenidos se estudiará el rendimiento del sistema tanto para el software NFIS2 como para el software MoC, primero para el sensor óptico y posteriormente para el sensor térmico.

5.3.1. Sensor óptico

A continuación se muestran las densidades de probabilidad de las puntuaciones de usuario e impostor del sensor óptico para los sistemas empleados (Figura 33).

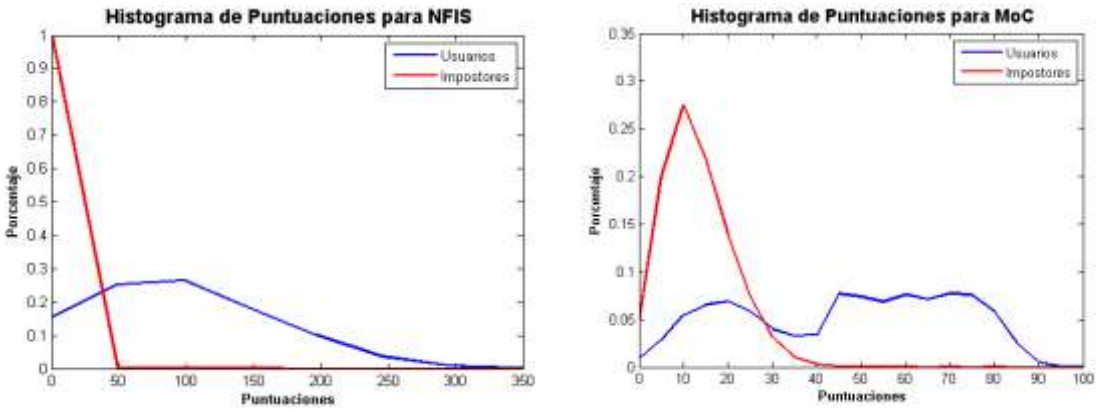


Figura 33: Histograma de puntuaciones para el sistema NFIS (izquierda) y el sistema MoC (derecha) del sensor óptico.

En el sistema NFIS2 (gráfica de la izquierda), se observa que los usuarios están repartidos a lo largo de todo el rango de puntuaciones (0 – 350) y tienen una mayor acumulación entre las puntuaciones 50 y 100. En el caso de los impostores, las puntuaciones quedan acumuladas mayoritariamente por debajo de 50.

Para el sistema *Match-on-Card* (gráfica de la derecha de la Figura 33), las puntuaciones de los usuarios también quedan repartidas en todo el rango (0-100) observándose un comportamiento bimodal del sistema que se traduce en una distribución de *scores* que parece la combinación de una gaussiana centrada aproximadamente en 20 y otra en 60. La función densidad de probabilidad que presentan los impostores tiene forma de gaussiana centrada alrededor de 16 puntos.

A continuación, en la Figura 34, se muestra el rendimiento de los sistemas según las curvas de falso rechazo (FR) y falsa aceptación (FA) obtenidas a partir de las distribuciones de *scores* anteriores.

El software NFIS obtiene un EER (*equal error rate*) del 3,16% para un umbral de decisión de 16,5 mientras que el valor para MoC asciende a un EER del 18,1% para un umbral de 22,5.

Como cabía esperar, el sistema *Match-on-Card* obtiene un rendimiento inferior al sistema NFIS por las limitaciones del chip.

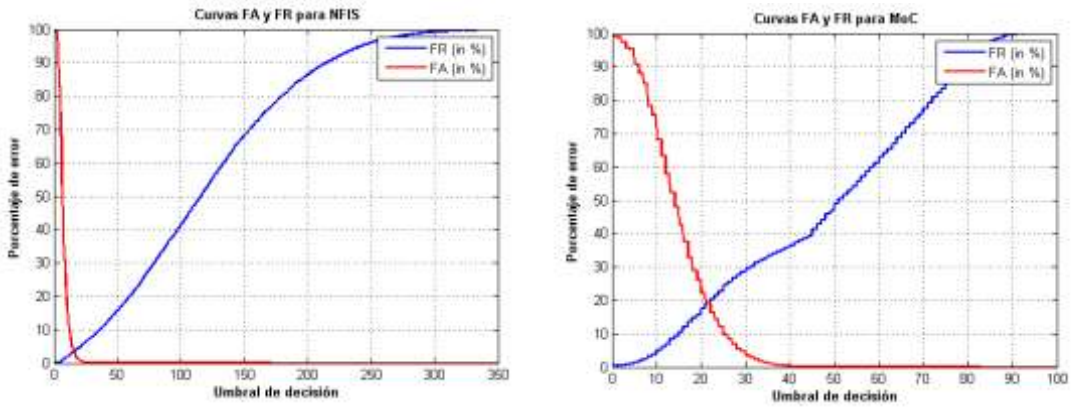


Figura 34: Curvas FA y FR para el sistema NFIS (izquierda) y el sistema MoC (derecha) del sensor óptico.

5.3.2. Sensor térmico

Los histogramas de puntuaciones obtenidos para el sensor térmico se muestran en la Figura 35.

La densidad de probabilidad de puntuaciones del sistema NFIS (Figura 35 izquierda) tiene una acumulación de *scores* por debajo de 30 para los impostores mientras que los usuarios se reparten por puntuaciones entre 0 y 180 aproximadamente.

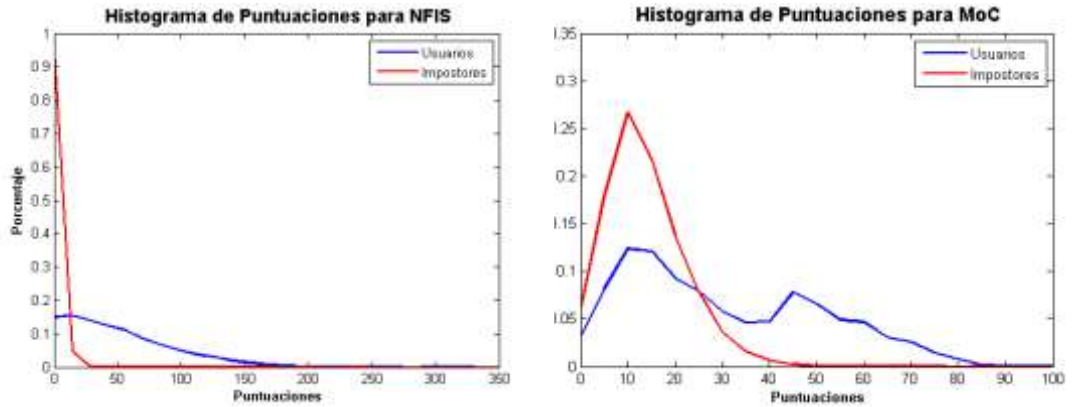


Figura 35: Histograma de puntuaciones para el sistema NFIS (izquierda) y el sistema MoC (derecha) del sensor térmico.

En el sistema MoC, los impostores forman una función densidad de probabilidad en forma de gaussiana centrada alrededor de 16 (Figura 35 derecha) tal y como

sucedía con el sensor óptico. Por su parte, las puntuaciones de usuario se reparten en todo el rango (0-100) observándose, como ocurria en el sensor óptico, dos modos de comportamiento del sistema que se corresponden con una gaussiana centrada en 16 y otra en 45. Las puntuaciones de usuario son, en general, más bajas que las obtenidas para el sensor óptico.

Para averiguar el EER se representan las curvas de falso rechazo (FR) y falsa aceptación (FA) en la Figura 36.

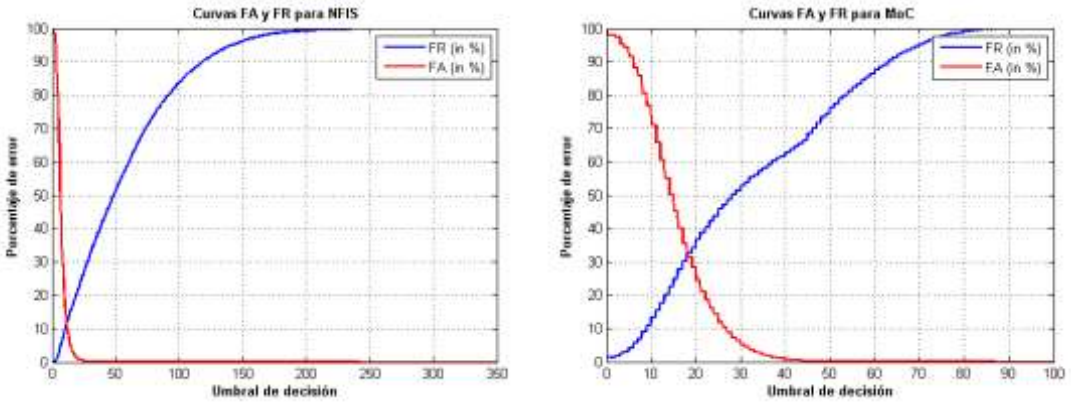


Figura 36: Curvas FA y FR para el sistema NFIS (izquierda) y el sistema MoC (derecha) del sensor térmico.

El sistema NFIS obtiene un EER del 11% aproximadamente para un umbral de decisión de 12,5. En el caso del software MoC el EER asciende hasta un 32% para un umbral de 18,5.

Este caso también muestra un rendimiento menor del sistema MoC causado por las limitaciones de la tarjeta.

5.3.3. Comparativa

En los histogramas obtenidos para el sensor óptico y el sensor térmico se aprecian funciones densidad de probabilidad con una forma muy parecida pero con ciertas diferencias:

- **Software NFIS** (Figura 33 y Figura 35, graficas representadas a la izquierda): El valor de puntuación obtenido tanto para los usuarios como para los impostores en el sensor térmico es menor que en el sensor óptico. Además, el sensor térmico posee un menor rango de puntuación. Las puntuaciones de usuario que tienen una mayor probabilidad de ocurrencia se encuentran entre 50 y 100 para el sensor óptico y entre 0 y 30 en el sensor térmico.
- **Sistema MOC** (Figura 33 y Figura 35, gráficas representadas a la derecha): Los usuarios se encuentran repartidos por todas las puntuaciones. En ambos sensores, la función densidad de probabilidad formada por los impostores tiene forma de gaussiana centrada en 16 y los usuarios

presentan un comportamiento del sistema bimodal formado por dos gaussianas.

- En ningún caso las puntuaciones de los impostores son superiores a 50 puntos y, en general, las puntuaciones de usuario son más bajas en el caso del sensor térmico.
- Los resultados obtenidos con el sensor térmico en ambos sistemas son sensiblemente peores debido a la peor calidad de las imágenes capturadas con este sensor (como se puede apreciar en la Figura 30) causada por la tecnología empleada. En general, las características físicas del dedo son más consistentes que las térmicas. Además, al ser el sensor térmico de barrido, tiene una etapa de post-procesado en la que hace una reconstrucción de la huella donde puede haber errores. Para corroborar estas afirmaciones, se ha utilizado el módulo NFIQ (5.1.1.3) del sistema NFIS que estima la calidad de las huellas devolviendo valores comprendidos entre el 1 y el 5 (alta calidad y baja calidad respectivamente). En la Figura 37 se observan las distribuciones de calidad de ambos sensores evaluados sobre toda la base de datos BiosecurID. La gráfica muestra como, efectivamente, las huellas capturadas con el sensor óptico de contacto presentan en general una mayor calidad que las muestras del sensor térmico de barrido.

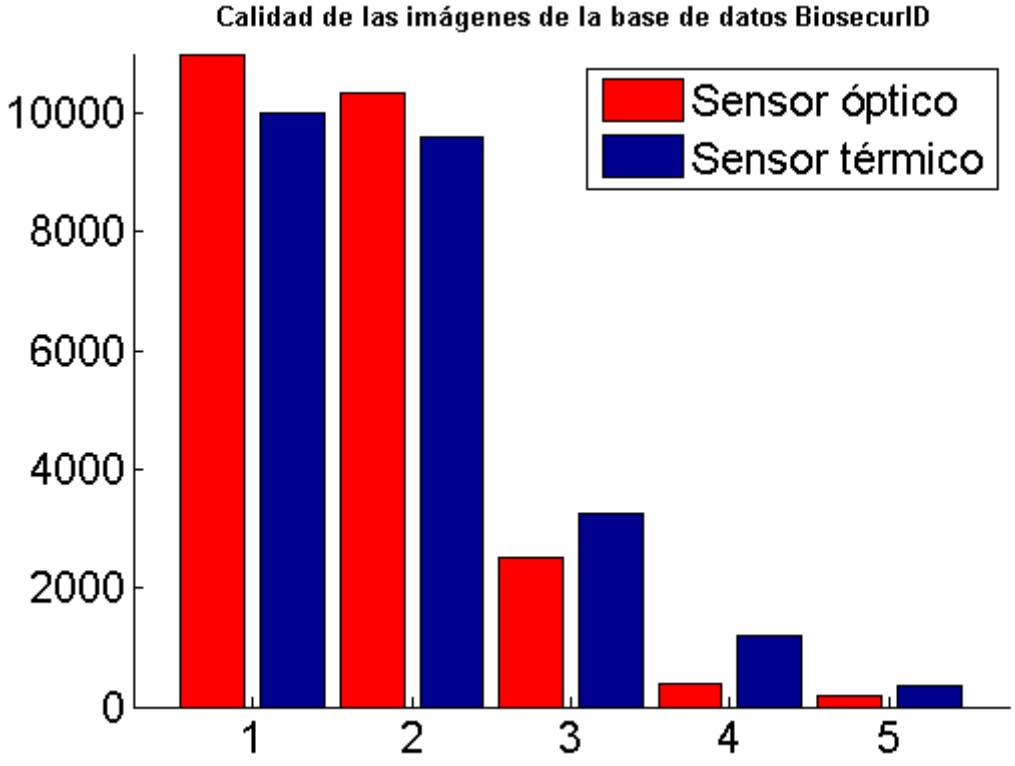


Figura 37: Distribución de calidad de las imágenes adquiridas con el sensor óptico y térmico representadas en escala del 1 al 5 (alta y baja calidad respectivamente).

Por otro lado, las curvas de FA y FR obtienen los siguientes valores de EER:

	Sensor Óptico		**Sensor Térmico**	
Sistema	NFIS	MoC	NFIS	MoC
EER	3,16%	18%	11%	32%
Umbral	16,5	22,5	12,5	18,5

Tabla 2: EER de los sistemas NFIS y MoC para los sensores óptico y térmico.

El sistema que obtiene un mejor rendimiento dentro de los estudiados es NFIS para el sensor óptico con un EER de 3,16% (valor considerablemente bueno comparado con el 32% del sistema MoC para sensor térmico).

La bajada del rendimiento del sistema MoC frente al software NFIS se produce por las limitaciones que posee el chip de la tarjeta inteligente y esto causa un empeoramiento de las puntuaciones de usuario ya que el número de minucias que compara es inferior. Las puntuaciones de los impostores permanecen distribuidas de forma parecida.

El rendimiento también se ve afectado por el tipo de sensor utilizado. Se observa un aumento de probabilidad de error del 3,16% al 11% para el caso de NFIS y del 18% al 32% para MoC al emplear el sensor térmico en vez del óptico. Esto es debido a la peor calidad de las imágenes adquiridas con el sensor térmico y, por tanto, a la mayor probabilidad de localización de falsas minucias en las huellas dactilares.

En la parte experimental del presente proyecto se ha considerado un punto de funcionamiento de los sistemas con FAR del 0,1%. Esto requiere un umbral y una FRR diferente para cada sistema y que se muestra en la Tabla 3.

FAR = 0,1 %	**Sensor Óptico**		**Sensor Térmico**	
Sistema	NFIS	MoC	NFIS	MoC
FRR	6,62%	38,55%	40,6%	73,3%
Umbral	26	45	38	49

Tabla 3: Valores de FRR y umbrales correspondientes a una FAR del 0,1 %.

Se escogen los puntos de funcionamiento en función de una FAR fija ya que la tasa de éxito de los ataques que se analizarán depende precisamente de la FAR en la que esté operando el sistema. De esta manera podemos comparar de forma objetiva los resultados obtenidos para ambos sistemas.

Con estos valores se obtiene una tasa de falsa aceptación considerada buena para un sistema y que implica que será más complicado que un impostor vulnere el sistema. Por otro lado, las tasas elevadas de falso rechazo harán que sea complicada la aceptación de usuarios reales, sin embargo, esta circunstancia no es crítica para el tipo de análisis de vulnerabilidades que es el objetivo del presente proyecto.

Para concluir este capítulo, la Figura 38 muestra una comparación de los dos sistemas estudiados para los dos sensores de adquisición mediante la representación de las curvas DET. Queda reflejado un peor comportamiento para los sistemas MoC frente a NFIS2 y para el sensor térmico frente al óptico.

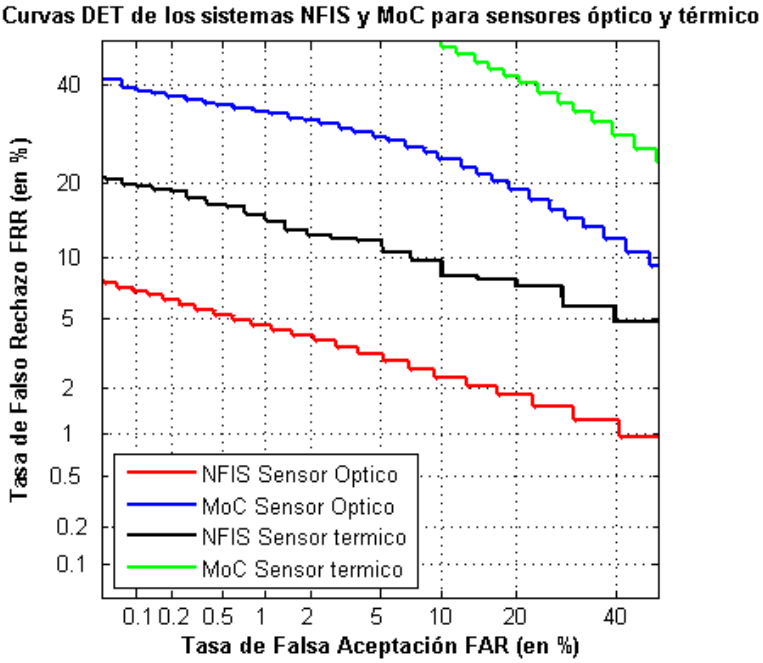


Figura 38: Curvas DET de los sistemas estudiados (MoC y NFIS2) para dos tipos de sensores (óptico y térmico).

6

Métodos de ataque *hill-climbing*

6.1. Algoritmo de ataque

El algoritmo *hill-climbing* que se ha utilizado en el presente proyecto es un ataque al sistema entre el extractor de características y el módulo comparador, es decir, un ataque al canal de comunicaciones de tipo 4 (Figura 24).

Como ya se había comentado anteriormente, este tipo de ataques necesitan saber la estructura de la plantilla y cierta información básica de la imagen de la huella. Es necesario conocer el tipo de sensor que está utilizando el sistema para poder extraer la información de la resolución y el tamaño de la imagen (este requisito es fácil de cumplir ya que los sensores suelen estar expuestos a la vista y la información suele ser aportada por los fabricantes).

Es importante recordar que las plantillas que utilizamos están basadas en minucias. Cada minucia se guarda como un vector con 3 componentes (2 pertenecientes a la posición que ocupa la minucia en el plano y una tercera que informa del ángulo que forma con la horizontal).

El algoritmo utilizado se propuso en [23], y consiste en:

1. Crear 100 patrones sintéticos de minucias aleatorios y del mismo tamaño que la imagen de la huella estudiada. Para que los patrones sean realistas las minucias deben estar separadas el equivalente a una cresta que es aproximadamente una distancia de 9 píxeles (para la resolución de las imágenes utilizadas).
2. Atacar la huella objetivo con los 100 patrones sintéticos y guardar las puntuaciones devueltas por el comparador. El patrón ganador será el que devuelva la mayor puntuación.
3. Realizar diferentes modificaciones al patrón ganador:
    A. Perturbar una minucia existente: desplazar una minucia o modificar su ángulo.
    B. Añadir una nueva minucia.
    C. Sustituir una minucia existente por otra aleatoria.
    D. Eliminar una minucia existente.

Si la puntuación mejora en el comparador tras cualquiera de las modificaciones permitidas, se almacena dicha modificación, si no, se elimina.

4. El algoritmo deja de ejecutarse si en algún momento se supera el umbral estipulado, en cuyo caso el ataque finaliza con éxito, o si se supera el número máximo de iteraciones permitidas.

Una evolución típica de la puntuación en un ataque *hill-climbing* se muestra en la Figura 39, donde el umbral fijado es de 26 y se observa que tras menos de 1000 iteraciones el umbral es superado.

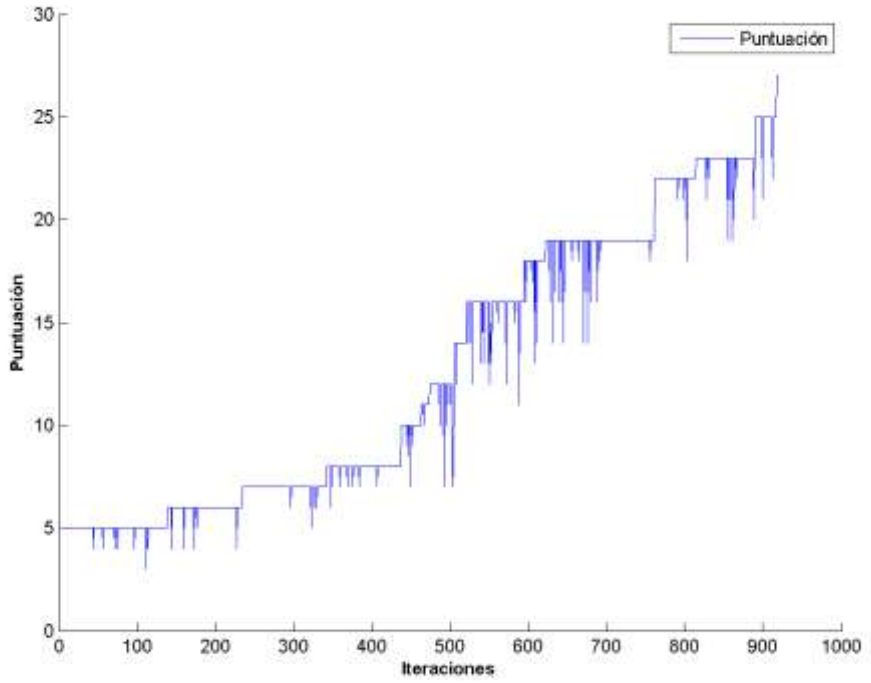


Figura 39: Ejemplo de evolución de la puntuación en un ataque hill-climbing finalizado con éxito para un sistema con un umbral de 26 puntos.

El número de iteraciones necesarias por el ataque *hill-climbing* varía según el sistema de estudio. Debido al alto coste temporal de los ataques al sistema MoC (que requieren una constante comunicación entre tarjeta y sistema) se ha decidido establecer un límite superior diferente para cada sistema. En el sistema NFIS el límite está marcado en 5000 iteraciones mientras que en MoC lo marcamos en 2000 iteraciones. Además de esta forma los resultados son comparables con los obtenidos en [24] de tal forma que se pueden alcanzar nuevas conclusiones sobre el ataque al tiempo que se profundiza en el conocimiento de las vulnerabilidades de este tipo de sistemas.

6.2. Análisis de los ataques

El ataque anteriormente descrito se ha ejecutado contra los sistemas NFIS y MoC sobre la base de datos BiosecurID. Se ha decidido utilizar un subconjunto de la base de datos escogiendo 200 huellas diferentes. Como ya se ha comentado, esta base de datos posee capturas de la huella dactilar utilizando dos tipos de sensores: óptico y térmico.

Los resultados obtenidos con el sensor óptico los hemos querido comparar con la versión mejorada del algoritmo anteriormente propuesto que se encuentra en [24]. En ese caso utilizaban un subconjunto de la base de datos MCYT [33] con las siguientes particularidades:

- De los 330 usuarios que posee la base de datos MCYT se tomo un subconjunto de 75 usuarios.
- Eligieron utilizar las huellas del dedo índice de la mano derecha y la misma mano izquierda por lo que tenían 150 huellas diferentes.
- Las muestras de cada huella fueron adquiridas con diferentes grados de control, es decir, se situaba un rectángulo en el área de captura de modo que el núcleo de la huella se encontrase en el interior. Cuanto menor fuese el rectángulo, mayor es el control ya que existía menor rotación y desplazamiento.
- Se escogieron 10 de las 12 muestras disponibles de cada huella (6 de alto control, 2 de control medio y 2 de control bajo).
- Al igual que en nuestra base de datos se realizó un post-procesado de las imágenes eliminando las minucias falsas que no pertenecían a la huella dactilar.
- El número medio de minucias de las huellas dactilares es de 38 minucias para el sistema NFIS y 25 minucias para MoC. Dicho número corresponde con las mismas minucias que utilizaron para generar los patrones aleatorios.

Para comparar los datos se ha calculado el porcentaje de éxito de cada ataque antes de llegar al número máximo de iteraciones permitido (5000 para NFIS y 2000 para el sistema MoC).

6.2.1. Sensor óptico

Tras el análisis de los sistemas definidos en el capítulo 5 se han realizado los ataques anteriormente descritos para las huellas adquiridas con el sensor óptico.
Se compararán nuestros resultados con los obtenidos en [24] que se muestran en las siguientes tablas. La Tabla 4 muestra los resultados obtenidos para el sistema NFIS.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
SI	B,C	38	-----	9,25	9,76	-----	95,3

Tabla 4: Resultados obtenidos en* [24] *para el ataque hill-climbing descrito sobre el sistema NFIS utilizando la base de datos MCYT y para un punto de operación FAR=0,1%.

La Tabla 5 es un resumen de los experimentos realizados en [24] sobre el sistema MoC.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 2000 iteraciones (%)
			A	B	C	D	
SI	B,C	25	-----	5,53	10,08	-----	97,3

Tabla 5: Resultados obtenidos en* [24] *para el ataque hill-climbing descrito sobre el sistema MoC utilizando la base de datos MCYT y para un punto de operación FAR=0,16%.

En los ataques realizados en este proyecto a ambos sistemas (NFIS y MoC) se han empleado las 4 modificaciones descritas en [23] para comprobar la influencia de cada una sobre los ataques (de forma similar a como se realizó en [24]). Se emplea la nomenclatura 'A', 'B', 'C' y 'D' para los cuatro tipos de modificaciones permitidas en el algoritmo, siendo las mismas, permutar una minucia, añadir una minucia, sustituir una minucia o eliminarla respectivamente.

Se recuerda que los umbrales establecidos para que los sistemas posean una tasa de falsa aceptación del 0,1% son los siguientes:

- **Sistema NFIS:** 26 puntos.
- **Sistema MoC:** 45 puntos.

6.2.1.1. Sistema NFIS

En primer lugar se ha atacado el sistema NFIS donde los patrones aleatorios a comparar con la huella de usuario se han creado con 72 minucias. Este número se ha asignado porque corresponde al número medio de minucias de las huellas dactilares adquiridas con el sensor óptico en la base de datos BiosecurID.

Como primer resultado experimental se analiza la conveniencia de generar minucias sólo en la región de interés (ROI). Como muestra la Tabla 6, sin utilizar la ROI el 61,5% de los ataques finalizan antes de 5000 iteraciones siendo capaces de superar el umbral (26 puntos para este sistema). Si decidimos establecer una ROI de menor tamaño que el de la imagen de la huella, se observa que el número de ataques finalizados antes de 5000 iteraciones es inferior ya que sólo obtiene un 50,5% de porcentaje de éxito.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	72	2,75	4,77	4,71	0,74	61,5
SI	A,B,C,D	72	4,26	1,82	1,53	0,01	50,5

Tabla 6: Estadísticas de los ataques NFIS aplicando y sin aplicar control de calidad para el sensor óptico.

Para continuar, se ha estudiado la influencia del número inicial de minucias en el rendimiento del ataque con mayor porcentaje de éxito. Se han lanzado ataques con un número inicial de minucias superior e inferior a la media previamente calculada en los que se observa una degradación del rendimiento en el porcentaje de éxito en 5000 iteraciones (Tabla 7).

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	90	2,21	3,11	3,69	0,93	20,5
NO	A,B,C,D	72	2,75	4,77	4,71	0,74	61,5
NO	A,B,C,D	58	1,06	4,10	3,54	0,86	47,0

Tabla 7: Estadísticas de los ataques NFIS empleando diferente número de minucias iniciales para el sensor óptico.

Se observa que, efectivamente, al atacar el sistema utilizando patrones con un número de minucias distinto a la media de la base de datos, empeora el rendimiento del algoritmo de ataque.

Para finalizar, se ha analizado la influencia que cada tipo de modificación tiene sobre el porcentaje de éxito de los ataques. La Tabla 6 muestra que las mejoras B y C logran a más a menudo un ascenso de la puntuación que las modificaciones A y D.

A raíz de los resultados, se estudia el rendimiento de los ataques eliminando en primer lugar la modificación que menor número medio de mejoras introduce (D) y posteriormente A. La Tabla 8 muestra una clara mejora (del 14,5%) en el rendimiento de los ataques tras eliminar la modificación D en el porcentaje de éxito. No realizar la modificación A no afecta significativamente al porcentaje de éxito en 5000 iteraciones (se mantiene prácticamente constante).

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	72	2,75	4,77	4,71	0,74	61,5
NO	A,B,C	72	2,91	5,07	5,87	-----	76,0
NO	B,C	72	-----	5,99	7,49	-----	75,0

Tabla 8: Estadísticas de los ataques NFIS eliminando las modificaciones con menor número medio de mejoras para el sensor óptico.

Comparativa

Base de datos	Control	modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
				A	B	C	D	
BiosecurID	NO	B,C	72	-----	5,99	7,49	-----	75,0
MCYT	SI	B,C	38	-----	9,25	9,76	-----	95,3

Tabla 9: Resumen comparativo de las estadísticas de los ataques para el sistema NFIS implementados sobre BiosecurID y MCYT.

Los resultados obtenidos para la base de datos BiosecurID coinciden con los extraídos de [24] salvo por el hecho de la utilización de un área de control de la huella y se muestran en la Tabla 9. En nuestro caso se obtienen mejores resultados sin aplicar un control de la huella dactilar debido a que la adquisición de nuestra base de datos no ha sido con niveles de control y, por tanto, el núcleo de la huella no tiene porqué pertenecer a la región de la huella considerada como ROI.

El porcentaje de éxito en 5000 iteraciones utilizando las cuatro modificaciones es muy similar para ambas bases de datos, pero tiene un 20% menos de probabilidad de éxito al eliminar las modificaciones que menos número de mejoras realizan. Este resultado es la consecuencia de una adquisición de la base de datos sin control pero, a su vez, más realista.

También se observa que las modificaciones que más afectan contribuyen al éxito del ataque sobre los sistemas son B y C (añadir una minucia y sustituir una existente por otra aleatoria tal y como ya ocurría con los ataques ejecutados con MCYT).

Basándonos en todos los resultados experimentales podemos concluir que:

- Las mejoras producidas en el ataque por la inclusión o no de la ROI son altamente dependientes de la base de datos utilizada: la ROI es beneficiosa si la base de datos fue adquirida con un alto nivel de control y no bajo condiciones realistas.

- Igualmente dependiente de los datos utilizados es el número de minucias iniciales con el que se debe lanzar el ataque, aunque se confirma que este debe coincidir con el número medio de minucias de las huellas de la base de datos utilizada.
- Las mejores modificaciones a realizar (B, C) son independientes del entorno experimental.

6.2.1.2. Sistema *Match-on-Card*

Para terminar con el sensor óptico se han realizado los experimentos sobre el sistema MoC. En este caso se ha estudiado la influencia del número de minucias iniciales y el rendimiento de los ataques al eliminar las modificaciones que menor número medio de mejoras producen.

Dichos ataques se han realizado sin aplicar nivel de control de la huella dactilar ya que, como se ha comprobado, no introduce mejoras en los resultados debido a que la distribución de las minucias es menos compacta (no todas las minucias se encuentran en el centro de la imagen) que en el caso de utilizar la base de datos MCYT.

Los patrones de las huellas dactilares deberían crearse con el número medio de minucias de la huella dactilar que corresponde a 72 minucias. Una de las desventajas del sistema MoC, es que está limitado por la capacidad del chip. En consecuencia, el número máximo de minucias que puede introducirse en la tarjeta es 42.

Se ha decidido probar los experimentos con un número inicial de minucias igual a 41 porque existe la probabilidad de que la mejor modificación, en primer lugar, sea B (añadir una minucia). Si el patrón contiene 42 minucias, la opción de añadir una minucia queda descartada.

En primer lugar estudiamos la influencia del número inicial de minucias. El motivo ha sido que en el caso de la base de datos MCYT, cuyos resultados se encuentran en [24], se demostraba que una disminución del número inicial de minucias en un 35-40% (de 38 minucias iniciales a 25) implicaba una mejora en el rendimiento de los ataques mientras que si se descendía hasta 10 minucias (un 74%) el rendimiento volvía a empeorar.

Los resultados obtenidos se muestran en la Tabla 10. Se observa que se obtiene un mejor rendimiento de los ataques para el caso de 41 minucias iniciales obteniendo un 11% de porcentaje de éxito en 2000 iteraciones. En nuestro caso, el número de minucias iniciales ya ha sido reducido un 43% (de 72 a 41 minucias), por lo que si reducimos un porcentaje mayor obtenemos peores resultados como ocurría en la base de datos MCYT.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 2000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	41	0,38	2,39	3,73	0,87	11,0
NO	A,B,C,D	25	0,04	0,50	0,77	0,42	8,2
NO	A,B,C,D	10	0,02	0,21	0,05	0,09	3,0

Tabla 10: Estadísticas de los ataques MoC empleando diferente número de minucias iniciales para el sensor óptico.

En cuanto al efecto de las modificaciones sobre los ataques, observamos en la Tabla 11, que en este caso las modificaciones que mayor número de mejoras aportan vuelven a ser B y C. Al implementar sólo dichas modificaciones, el rendimiento de los ataques aumenta hasta un 81,8%.

Al contrario de lo ocurrido con el sistema NFIS para la misma base de datos, pero al igual que en la base de datos MCYT para el sistema MoC, la modificación D (eliminar una minucia existente) proporciona un mayor número medio de mejoras en comparación con la modificación A, que es en este caso la primera en descartar.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 2000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	41	0,38	2,39	3,73	0,87	11,0
NO	B,C,D	41	-----	3,84	6,52	1,16	39,7
NO	B,C	41	-----	5,08	9,56	-----	81,8

Tabla 11: Estadísticas de los ataques MoC eliminando las modificaciones con menor número medio de mejoras para el sensor óptico.

Comparativa

Base de datos	Control	modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
				A	B	C	D	
BiosecurID	NO	B,C	41	-----	5,08	9,56	-----	81,8
MCYT [24]	SI	B,C	25	-----	5,53	10,08	-----	97,3

Tabla 12: Resumen comparativo de las estadísticas de los ataques para el sistema MoC implementados sobre BiosecurID y MCYT.

Como ocurría en [24], se comprueba que el sistema MoC es más vulnerable al ataque que el sistema NFIS debido a sus restricciones computacionales y de almacenamiento.

El sistema MoC (al igual que el NFIS) presenta mejores resultados sin aplicar un control de la huella dactilar al tratarse de una base de datos adquirida en condiciones reales y sin niveles de control.

Se comprueba que las modificaciones que más afectan a la terminación del ataque en 5000 iteraciones son B y C como ocurre con NFIS y sobre la base de datos MCYT. Empleando exclusivamente esas modificaciones de forma aleatoria la base de datos BiosecurID obtiene un 15,5% menos de probabilidad de éxito en el caso del sistema MoC (el sistema NFIS obtiene un 20% menos de probabilidad de éxito para la base de datos BiosecurID frente a MCYT).

El número inicial de minucias es dependiente de las huellas utilizadas pero se ha podido comprobar con los resultados de BiosecurID y MCYT, que se obtienen mejores resultados al utilizar el 60% (aproximadamente) del número medio de minucias de la base de datos como número de minucias iniciales. A su vez, este número queda restringido por las limitaciones de la capacidad del chip de los sistemas *Match-on-Card*.

6.2.1.3. Conclusiones

Tras realizar los ataques con el sensor óptico se han extraído las siguientes conclusiones que servirán para futuros experimentos.

- Los ataques de la base de datos BiosecurID tienen mayor probabilidad de éxito sin utilizar los niveles de control ya que no se han utilizado dichos niveles a la hora de adquirir las imágenes.
- Se ha comprobado que el número inicial de minucias ideal depende de los datos y la tecnología utilizada. En el caso del sistema NFIS2 corresponde al número medio de minucias de las huellas de la base de datos. Sin embargo, para el sistema MoC se obtiene un rendimiento más efectivo del ataque reduciendo el número inicial de minucias a un 60% del número medio de minucias de la base de datos o, en su defecto, a la capacidad máxima del chip de la tarjeta (42 minucias).
- Se concluye que independientemente de la base de datos utilizada en las pruebas, las modificaciones que aportan mejores resultados son la B y C, es decir, añadir una minucia o sustituir una minucia existente.
- Se ha comprobado que debido a las limitaciones impuestas por el hardware en los sistemas MoC que obliga a una mayor simplicidad del algoritmo de comparación, el ataque *hill-climbing* es más eficiente que sobre el sistema NFIS.
- Se observa que la tasa de éxito del ataque, tanto para el sistema NFIS como para MoC, es ligeramente superior en el caso de la base de datos MCYT. Esto se debe, probablemente, a las limitaciones con que fueron capturadas que

harán que las huellas tengan un menor grado de libertad y por tanto sean más vulnerables al ataque.

6.2.2. Sensor térmico

Tras analizar los ataques obtenidos empleando el sensor óptico para adquirir las imágenes, se han probado los experimentos que mejores resultados han obtenido utilizando esta vez las huellas capturadas con el sensor térmico. Estos resultados nos permitirán obtener nuevas conclusiones sobre el comportamiento del ataque y sus parámetros, más allá de los estudios realizados en [24] donde no se analizó la incidencia del uso de distintos sensores de adquisición en la vulnerabilidad final de los sistemas.

Para realizar los ataques de las huellas del sensor térmico, también se ha utilizado un subconjunto de 200 huellas diferentes (correspondientes a los mismos usuarios que los del óptico) de la base de datos BiosecurID. Los umbrales que se establecieron condicionados a una tasa de falsa aceptación (FAR) del 0,1% son:

- **Sistema NFIS:** 38 puntos.
- **Sistema MoC:** 49 puntos.

6.2.2.1. Sistema NFIS

En primer lugar se ha evaluado la influencia del número de minucias iniciales en el sistema. En el caso de las huellas capturadas con el sensor térmico, el número medio de minucias de las huellas de la base de datos es 70 (aproximadamente las mismas que se obtenían para el sensor óptico).

La Tabla 13 indica los resultados obtenidos. Se comprueba que el número de minucias iniciales que mayor probabilidad de éxito en 5000 iteraciones presenta es la que corresponde al número medio de minucias de las huellas (70 minucias). Se demuestra que, para cualquier número inicial de minucias utilizadas, las modificaciones que mayor número de mejoras provocan son de nuevo B y C (añadir y sustituir minucia), mientras que D (eliminar minucia aleatoria) no parece en ningún caso afectar significativamente al ataque.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	90	3,10	6,01	5,47	0,80	25,0
NO	A,B,C,D	70	3,18	6,36	5,29	0,93	29,0
NO	A,B,C,D	58	1,17	4,81	4,14	0,68	22,5

Tabla 13: Estadísticas de los ataques NFIS empleando diferente número de minucias iniciales para el sensor térmico.

Por esta razón, a continuación estudiamos los ataques realizando sólo las modificaciones que más afectan al rendimiento. En primer lugar eliminamos la modificación D y después A. Se concluye que el rendimiento del ataque aumenta considerablemente, consiguiendo hasta un 63,5% de porcentaje de éxito en 5000 iteraciones.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 5000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	70	3,18	6,36	5,29	0,93	29,0
NO	A,B,C	70	3,57	7,39	7,44	-----	42,5
NO	B,C	70	-----	8,07	11,37	-----	63,5

Tabla 14: Estadísticas de los ataques NFIS eliminando las modificaciones con menor número medio de mejoras para el sensor térmico.

6.2.2.2. Sistema *Match-on-Card*

Para finalizar con los ataques *hill-climbing*, se han realizado los ataques al sistema MoC evaluando las modificaciones que mayor número de mejoras introducen en los ataques.

Como ya se ha comentado anteriormente, el sistema MoC está limitado por la capacidad del chip y obtiene mejores resultados al utilizar como número de minucias iniciales un 60% (aproximadamente) del número medio de minucias de la base de datos. Por estas razones se reduce el número de minucias iniciales hasta 41 minucias. Además, se escoge una minucia menos que el número máximo de minucias aceptadas por la tarjeta (42 minucias) permitiendo así que la primera modificación sea añadir una minucia aleatoria.

Control de la huella	Modificaciones	Minucias Iniciales	Número medio de mejoras				Porcentaje de éxito en 2000 iteraciones (%)
			A	B	C	D	
NO	A,B,C,D	41	0,32	2,46	3,61	0,73	11,1
NO	B,C,D	41	-----	2,92	4,70	1,12	34,0
NO	B,C	41	-----	2,45	8,87	-----	75,8

Tabla 15: Estadísticas de los ataques MoC eliminando las modificaciones con menor número medio de mejoras para el sensor térmico.

Se comprueba en la tabla que el rendimiento de los ataques para el sistema MoC con las huellas adquiridas por un sensor térmico alcanza un 75,8% de éxito tras 2000 iteraciones. Esto implica que el sistema MoC, al igual que sucedía con el sensor óptico, es más vulnerable al ataque que el software NFIS.

6.2.2.3. Conclusiones

Los experimentos realizados con el sensor térmico corroboran que el sistema MoC presenta una mayor vulnerabilidad al ataque que el software NFIS independientemente de la tecnología utilizada en la adquisición (óptica de contacto o térmica de barrido).

Por otra parte, el rendimiento del ataque con el sensor térmico es consistente con el porcentaje de éxito obtenido para el óptico aunque en ambos casos (NFIS y MoC) ligeramente inferior, 63,5% frente a 75% para los ataques realizados sobre el sistema NFIS, y 75,8% con el térmico frente a 81% con el óptico, para MoC. Esta pequeña disminución en el porcentaje de éxito sugiere que el algoritmo es más eficiente a la hora de romper huellas de mejor calidad (como es el caso de las imágenes capturadas con el sensor óptico).

Además, se pone de nuevo de manifiesto que el ataque obtiene un mejor rendimiento cuando utiliza como número inicial de minucias el número medio de minucias de las huellas de la base de datos para el caso del sistema NFIS y una reducción del 40% (aproximadamente) del valor del número medio de minucias de la base de datos utilizada para MoC. Por otro lado, y como ya hemos visto, el sistema MoC también está restringido por la capacidad del dispositivo.

Los resultados obtenidos con el sensor térmico corroboran que las modificaciones más eficientes del ataque *hill-climbing*, independientemente de la base de datos o sensor utilizados, son añadir o sustituir una minucia.

6.2.3. Conclusiones de los ataques *hill-climbing*

Se concluye este capítulo relacionando los resultados obtenidos en los ataques al emplear huellas dactilares de BiosecurID y de MCYT y comparando la utilización de un sensor óptico de contacto frente a uno térmico de barrido para la base de datos BiosecurID.

En general, al utilizar BiosecurID o MCYT obtenemos datos coincidentes que difieren en el hecho de utilizar un área de control. Podemos concluir que la inclusión o no de una ROI depende de la base de datos utilizada ya que en el caso de BiosecurID no es beneficioso emplear la ROI porque las huellas han sido adquiridas bajo condiciones reales mientras que en MCYT, al utilizar la ROI se obtienen mejores resultados porque las imágenes fueron adquiridas con niveles de control.

En cuanto al algoritmo de ataque, se ha demostrado que es ligeramente más eficiente a la hora de romper huellas de mayor calidad (obtenidas con el sensor óptico) como demuestra el porcentaje de éxito del sistema NFIS para el sensor óptico (75%) frente al sensor térmico (63%) y el sistema MoC para los mismos casos (81,8% para el óptico frente a 75,8% del térmico).

Se puede generalizar que los resultados obtenidos muestran que el sistema NFIS2 obtiene una menor vulnerabilidad a los ataques que MoC independientemente de la tecnología de adquisición de las imágenes empleada. Este hecho es achacable a las restricciones del sistema MoC provocadas por las limitaciones del chip donde debe realizarse el almacenamiento y la comparación entre huellas.

Además, se ha comprobado que el número de minucias iniciales que proporcionan un mejor rendimiento es dependiente de la tecnología y la base de datos utilizada. El sistema NFIS obtiene mejores resultados cuando dicho número corresponde con el número medio de minucias de la base de datos empleada. El sistema MoC posee más limitaciones (la capacidad del chip de la tarjeta o una mayor simplicidad del algoritmo de comparación) que provocan que el número inicial de minucias ideal que proporciona resultados más eficientes corresponda a un 60% del número medio de minucias de las huellas utilizadas o bien, a la capacidad máxima del chip.

En cuanto a las modificaciones, añadir y sustituir una minucia (B y C) son las que mayor número de mejoras proporcionan a los ataques independientemente de la base de datos y sensor utilizado mientras que A y D (permutar y eliminar una minucia) no aumentan el porcentaje de éxito y es mejor eliminarlas para reducir el coste computacional.

7

Métodos de ataque *side-channel*

7.1. Algoritmo de ataque

Como ya se ha mencionado, uno de los principales objetivos del proyecto es aplicar los nuevos conocimientos adquiridos tras el análisis de los ataques *hill-climbing*, al desarrollo de ataques tipo *side-channel*.

Para ello en primer lugar se analizará la relación que existe entre la puntuación devuelta por los sistemas analizados y el tiempo que tarda en generarla. Discutiremos el hecho de si se puede aprovechar esta información para generar un ataque *side-channel* basado en tiempo.

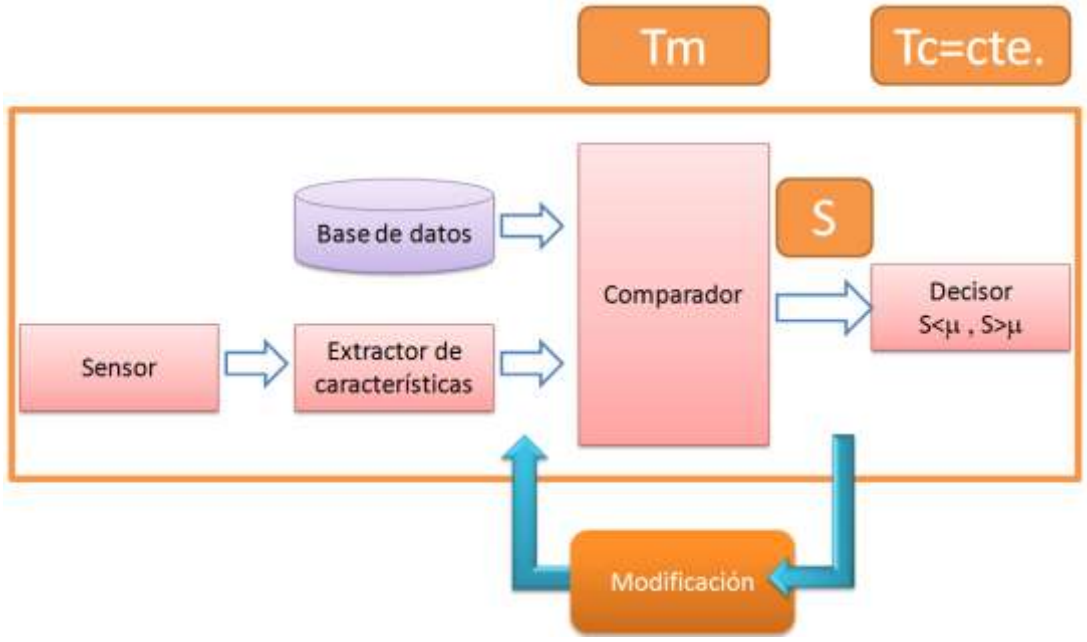


Figura 40: Esquema general del algoritmo hill-climbing basado en tiempo (timming-attacks).

El ataque a realizar se considerará s*ide-channel* porque se va a utilizar información adicional (en este caso temporal) obtenida de la implementación física del sistema. El tiempo que vamos a intentar relacionar con la puntuación es el que tarda el comparador en procesar la información, asumiendo que el tiempo del módulo decisor es constante. En la Figura 40 se muestra el esquema del problema que analizaremos.

Como se puede observar, hemos adaptado un esquema *hill-climbing* tipo 4 descrito en 4.3., donde las modificaciones se realizan sobre el módulo comparador, a un ataque s*ide-channel* basado en tiempo y que fue implementado por primera vez en [25].

De esta manera el algoritmo a utilizar parte de las conclusiones obtenidas en el capítulo 5 y el capítulo 6 y que resumimos brevemente:

- Es necesario realizar una etapa de post-procesado para eliminar las minucias artificiales existentes en los bordes de la huella dactilar para aumentar así el rendimiento de los ataques.
- Crear una ROI con niveles de control en la huella dactilar depende de la base de datos utilizada y de la distribución de las minucias. En nuestra base de datos aplicar los niveles de control empeoran los resultados por lo que no será utilizado.
- El umbral establecido depende del sistema y la base de datos. Para el sensor óptico se utilizara una puntuación de 26 y 45 (NFIS2 y MoC respectivamente), mientras que el sensor térmico emplea un umbral de 38 para el sistema NFIS2 y 49 puntos para MoC.
- Se permitirán exclusivamente las modificaciones que mayor número de mejoras introducen, es decir, B y C (añadir y sustituir minucia).
- El número de minucias iniciales depende de la base de datos y tecnología utilizada.

Partiendo de esta base, emplearemos el siguiente algoritmo de ataque:

1. Crear 100 patrones sintéticos con un número determinado de minucias del tamaño de la imagen de la huella a estudiar.
2. Atacar la huella objetivo con los 100 patrones sintéticos y guardar los tiempos que tarda el comparador en generar una puntuación. Se elige el mejor patrón en función del tiempo Tm.
3. Modificamos el patrón ganador permitiendo uno de los siguientes cambios:
    B. Añadir una nueva minucia.
    C. Sustituir una minucia existente por otra aleatoria.
4. Para que los patrones sean realistas las minucias deben estar separadas el equivalente a una cresta que para la resolución de la imagen con la que se trabaja es de 9 píxeles. En general, se permiten M cambios antes de realizar una nueva comparación.
5. Se realiza una nueva comparación y se calcula el nuevo tiempo Tm tras los M cambios realizados. Si el tiempo Tm indica que la puntuación ha aumentado, se conserva el cambio, si no, se desecha y se vuelve a modificar la huella (paso 3).

6. El algoritmo deja de ejecutarse si el sistema devuelve una respuesta positiva (el ataque finaliza con éxito) o se supera el número máximo de iteraciones (el ataque no ha tenido éxito).

7.2. Estudio de la relación puntuación-tiempo.

En el algoritmo anterior hay dos decisiones para las que es crucial conocer la relación (de haberla) entre la puntuación y el tiempo de comparación:

- Primero, para decidir en el paso 2 cuál es el mejor patrón únicamente en función del tiempo que se tardó en devolver la puntuación.
- Segundo, para decidir en el paso 5 si se conserva o se desecha el cambio realizado.

Así pues, el siguiente objetivo de estudio del presente proyecto, es analizar la puntuación devuelta por el sistema y comprobar si existe alguna relación con el tiempo de comparación del *matcher*.

Para caracterizar los sistemas analizados se ha partido de los trabajos realizados en [25], donde se analizaba la relación entre la variación del tiempo y la variación de la puntuación.

Para conseguir establecer una relación puntuación-tiempo, se partirá de una huella real que va a ser degradada sucesivamente mientras se observa la evolución de ambos parámetros. Este experimento se ha realizado para 100 huellas de la base de datos permitiendo un número máximo de modificaciones (300) suficientes para lograr que la puntuación baje hasta los valores típicos producidos por dos huellas provenientes de dos usuarios diferentes.

Cada iteración tiene permitido realizar una de las 4 modificaciones planteadas en el ataque *hill-climbing* analizado en el capítulo anterior de este proyecto, es decir, permutar una minucia, añadir una minucia, sustituir una minucia o eliminar una minucia.

La organización de los experimentos realizado será como en el capítulo anterior. Veremos los resultados obtenidos para el sensor óptico con los sistemas NFIS y MoC y después, para los mismos sistemas, los obtenidos con el sensor térmico.

Las gráficas representan la evolución del tiempo y la puntuación en cada iteración para poder comprobar más fácilmente si existe alguna correlación entre ellas.

7.2.1. Sensor óptico

Se han realizado los experimentos sobre 100 huellas dactilares reales de la base de datos. El número de modificaciones permitidas ha sido diferente para cada tipo de software (300 para el software NFIS y 100 para MoC), pero suficiente para

alcanzar una puntuación típica de dos huellas de usuarios diferentes. La modificación a realizar en cada iteración ha sido elegida aleatoriamente.

7.2.1.1. Resultados para el software NFIS

Las siguientes figuras muestran los resultados obtenidos para algunas de las huellas analizadas. En la Figura 41, se observa que existe una tendencia de disminución del tiempo de comparación Tm al decrementar la puntuación de la huella dactilar.

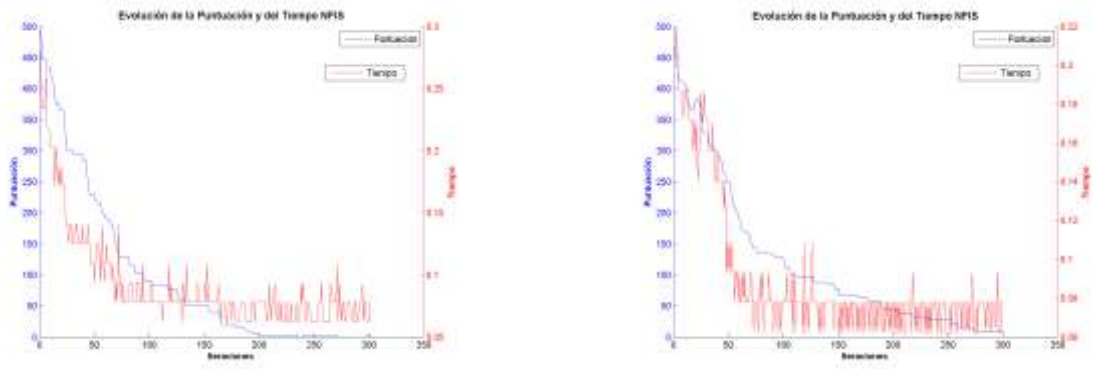


Figura 41: Ejemplos de evolución de las puntuaciones y el tiempo para el software NFIS donde existe una correlación entre ambos parámetros: al decrementar la puntuación se produce una disminución del tiempo.

Por otro lado, en los ejemplos de la Figura 42 no se observa ningún tipo de relación entre la evolución de la puntuación y la del tiempo.

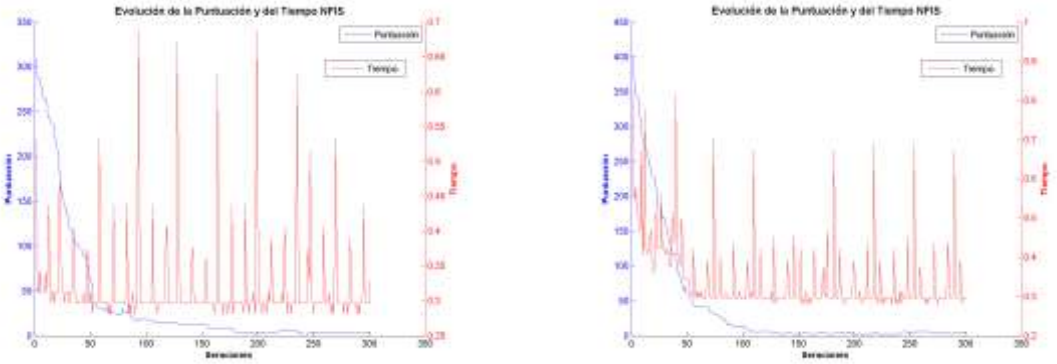


Figura 42: Ejemplos de evolución de las puntuaciones y el tiempo para el software NFIS donde no existe una correlación aparente entre ambos parámetros.

Como consecuencia de no observar una correlación evidente entre la variación de la puntuación y la variación del tiempo para todas las huellas de la base de datos, se recurre a un punto de vista estadístico empleando las medias de las puntuaciones y los tiempos tras cada modificación (ver Figura 43).

Utilizando la media obtenemos una correlación entre el tiempo y la puntuación, de manera que a medida que disminuye la puntuación, lo hace también el tiempo. Se observa que tras 140 iteraciones aproximadamente, la puntuación sigue disminuyendo mientras que el tiempo se queda oscilando alrededor de un valor constante.

Por esta razón se distinguen dos zonas: la primera (Zona A en la Figura 43) pertenece a las iteraciones comprendidas entre 0 y 150 donde para altas puntuaciones se obtiene un tiempo de comparación elevado; La segunda zona (para un número de iteraciones mayor de 150) no muestra una relación entre la puntuación y el tiempo ya que el sistema necesita un tiempo mínimo de ejecutarse (zona B en la Figura 43).

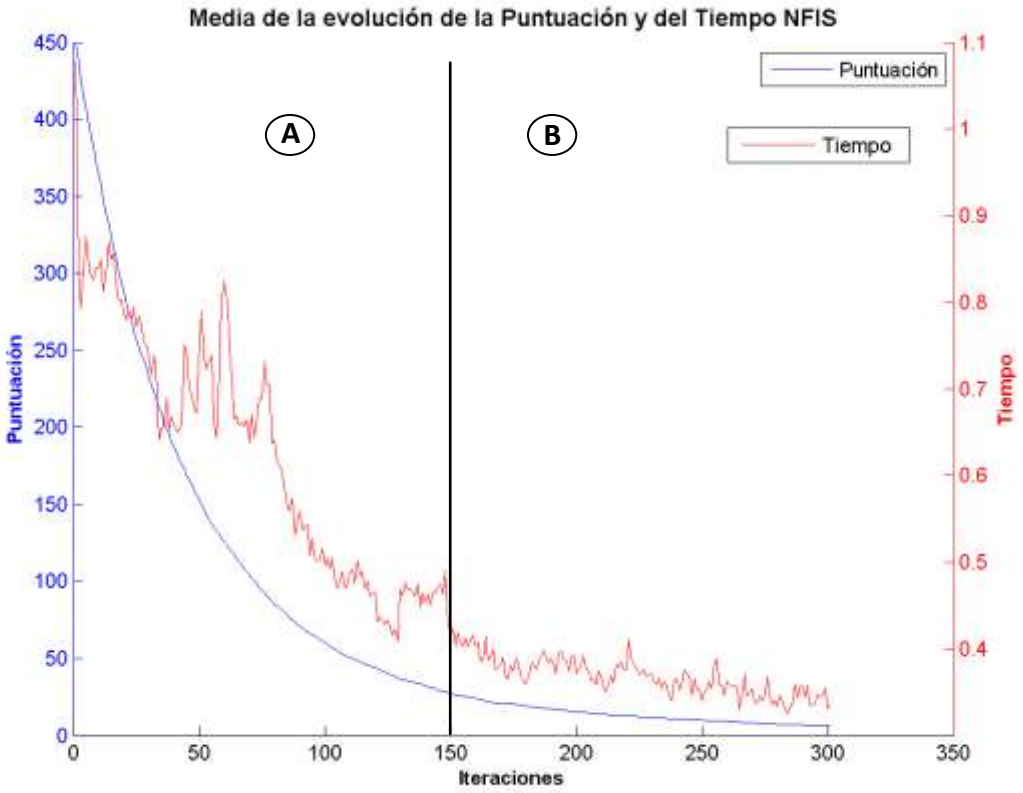


Figura 43: Media de la evolución de la variación de la puntuación y del tiempo para el software NFIS empleando el sensor óptico.

7.2.1.2. Resultados para el software *Match-on-Card.*

Las pruebas se han realizado sobre las mismas 100 huellas que en el caso del NFIS. En este caso el número de modificaciones permitidas es 100 (aplicado para alcanzar una puntuación típica de impostor), que equivale al número máximo de iteraciones ya que se permite una modificación por iteración.

Al igual que ocurría para NFIS con el software MoC no se observa una correlación entre variación de puntuación y de tiempo en todos los usuarios. La Figura 44 muestra dos gráficas de usuarios que presentan una cierta tendencia a que aumente el tiempo a medida que disminuye la puntuación, mientras que los ejemplos de la Figura 45 muestra lo contrario (no se observa ninguna relación).

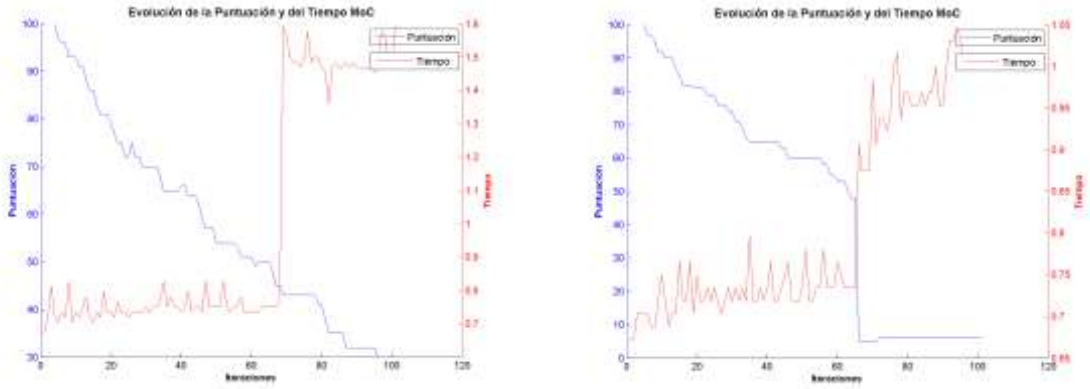


Figura 44: Ejemplos de evolución de las puntuaciones y el tiempo para el software MoC donde existe una correlación entre ambos parámetros: al disminuir la puntuación se produce un incremento del tiempo.

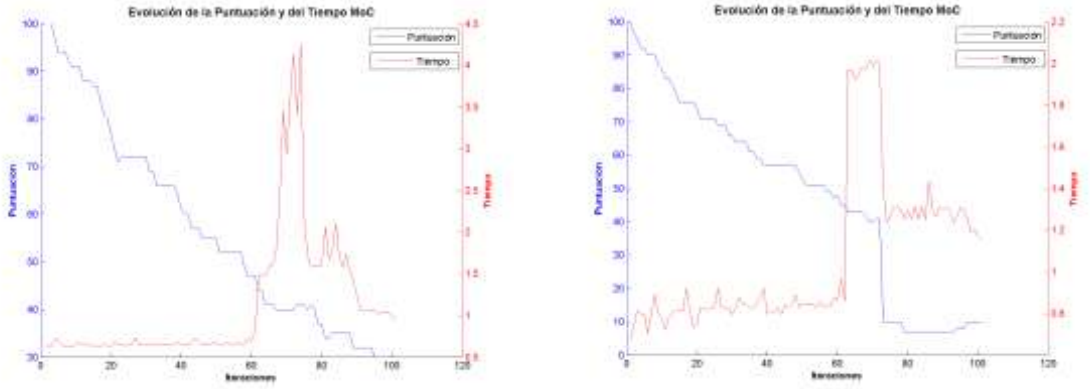


Figura 45: Ejemplos de evolución de las puntuaciones y el tiempo para el software MoC donde no existe una correlación aparente entre ambos parámetros.

Como no se puede generalizar la relación entre puntuación y tiempo, de nuevo se decide recurrir a los estadísticos y calcular la media de la puntuación y el tiempo en cada iteración para obtener una relación cuantitativa.

Se observa en la Figura 46 que la relación producida por la variación de la puntuación y la variación del tiempo es contraria a la observada en NFIS, es decir, a medida que disminuye la puntuación, el tiempo va incrementándose. Esto quiere decir que el sistema tarda un tiempo mayor en procesar la información de dos usuarios distintos que cuando las huellas pertenecen al mismo usuario.

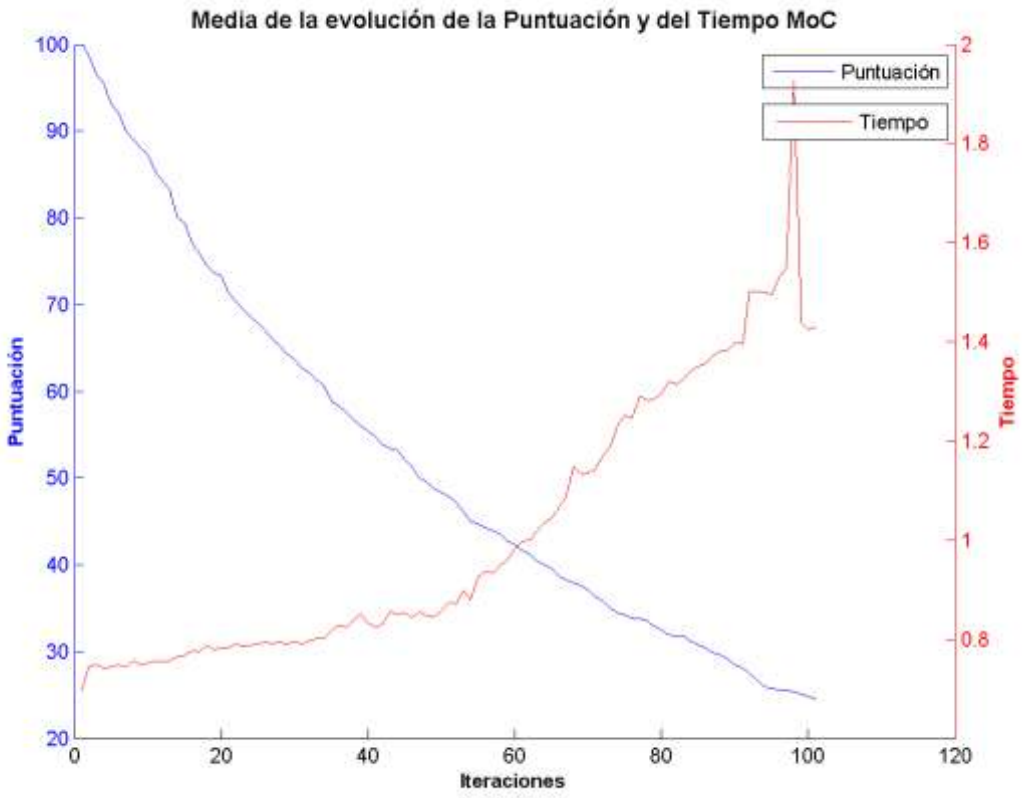


Figura 46: Media de la evolución de la variación de la puntuación y del tiempo para el sistema Match-on-Card con huellas adquiridas con el sensor óptico.

7.2.2. Sensor térmico

Los experimentos que se han realizado con el sensor térmico son análogos a los empleados con el sensor óptico. De esta manera, se ha utilizado un número de modificaciones para cada sistema que permite alcanzar una puntuación realista a la hora de comparar dos huellas diferentes. Las modificaciones realizadas son aleatorias en cada iteración.

7.2.2.1. Resultados para el software NFIS

Se han empleado 300 iteraciones, en cada una de las cuales se permite una única modificación aleatoria para comprobar la relación entre la variación de la puntuación y el tiempo.

La siguiente figura muestra, como ejemplo, dos plantillas en las que la evolución de la puntuación y el tiempo presentan una correlación equivalente a la observada en el caso del sensor óptico: al disminuir la puntuación, lo hace también el tiempo.

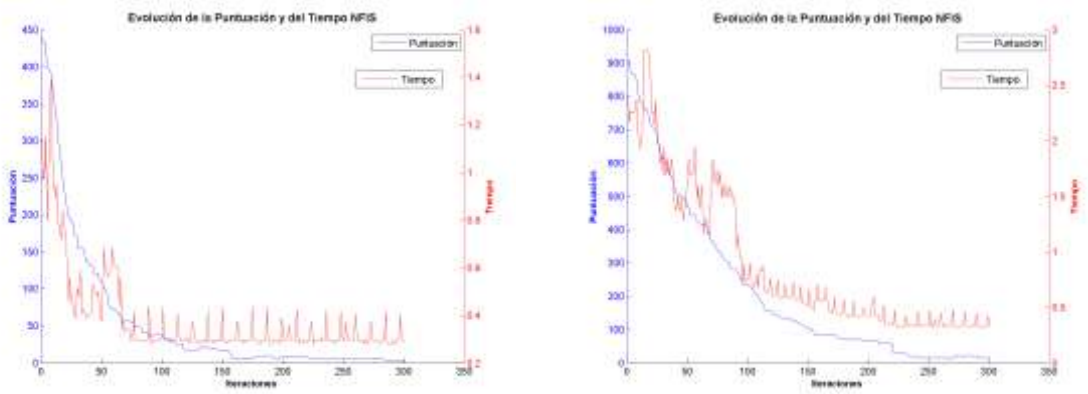


Figura 47: Ejemplos de evolución de las puntuaciones y el tiempo para el software NFIS utilizando el sensor térmico donde existe una correlación: al disminuir la puntuación se produce una disminución del tiempo.

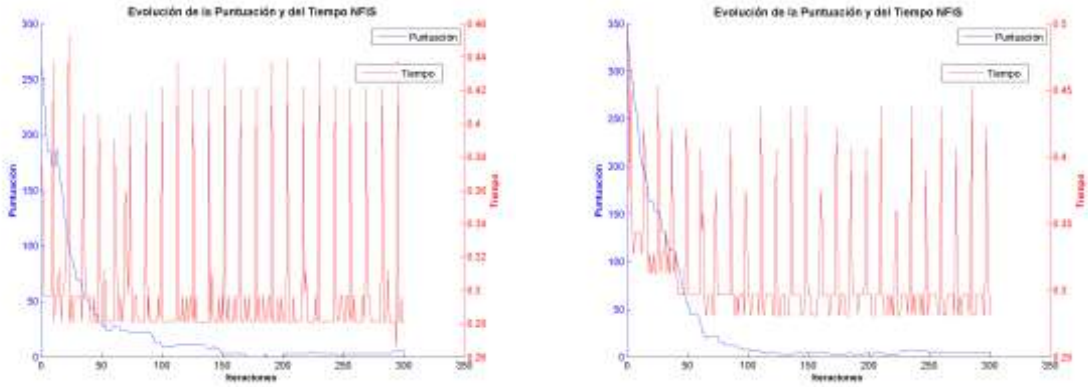


Figura 48: Ejemplos de evolución de las puntuaciones y el tiempo para el software NFIS utilizando el sensor térmico donde no existe una correlación aparente entre ambos parámetros.

Tal y como ocurría en el caso de las huellas capturadas con el sensor óptico la evolución de la puntuación y el tiempo no presenta siempre los resultados de la Figura 47. Algunas plantillas de diferentes usuarios, no muestran una tendencia parecida de las funciones estudiadas (ver Figura 48), por lo que es necesario recurrir a la estadística y utilizar promedios de la variación de puntuación y la variación del tiempo (ver Figura 49).

El promediado de las funciones analizadas indica que tras un decremento de la puntuación, se obtiene una disminución del tiempo. Se puede observar que esta tendencia ocurre hasta la iteración número 150 aproximadamente (zona A). A continuación, el tiempo empleado en realizar la modificación forma valores alrededor de 0,33 segundos (zona B).

Este comportamiento es prácticamente idéntico al observado para el caso del sensor óptico lo que demuestra la consistencia del funcionamiento temporal del sistema NFIS independientemente del sensor utilizado en la captura de las huellas dactilares.

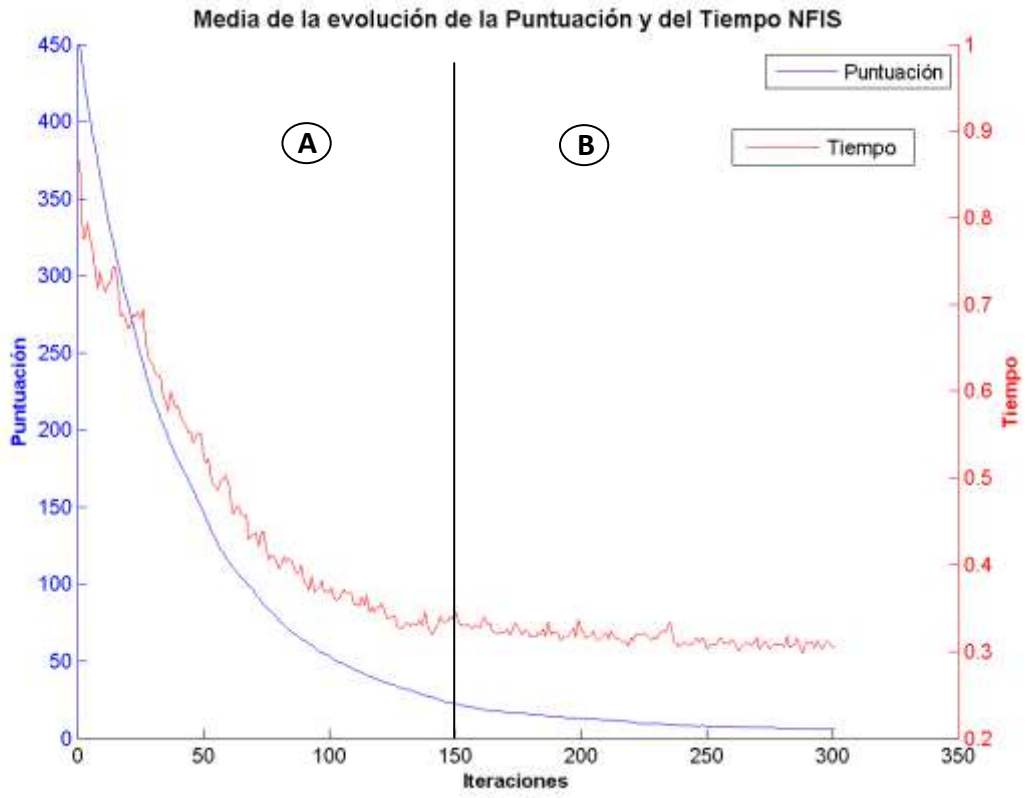


Figura 49: Media de la evolución de la puntuación y el tiempo al aplicar 300 modificaciones al software NFIS empleando el sensor térmico.

7.2.2.2. Resultados para el software *Match-on-Card*

Al igual que en el caso del sensor óptico, en las pruebas realizadas con el software MoC se ejecutan 100 modificaciones. Los resultados obtenidos son análogos a los del sensor óptico: no todas las plantillas presentan una relación entre la puntuación y el tiempo.

Como consecuencia, se decide realizar el promedio de las funciones para obtener una correlación estadística como ocurría en los casos anteriores. La gráfica muestra que el tiempo sufre una evolución contraria a la puntuación, es decir, un decremento de la puntuación causa un incremento en la variación del tiempo (ver Figura 50).

El comportamiento entre la puntuación y el tiempo de los experimentos sobre el software MoC es prácticamente idéntico para el sensor óptico y el térmico mostrando la consistencia del funcionamiento de este sistema.

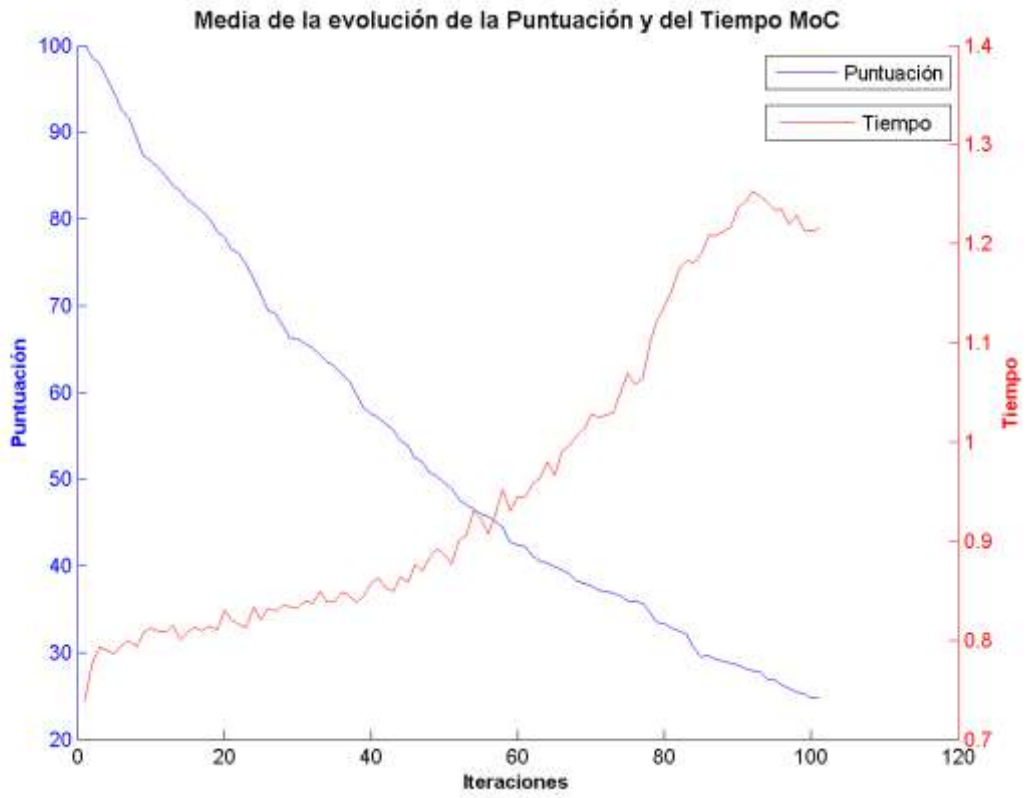


Figura 50: Media de la puntuación y el tiempo para el software MoC empleando el sensor térmico.

7.2.3. Conclusiones

En el apartado 7.2. hemos analizado la relación puntuación-tiempo para los diferentes sistemas empleados en el presente proyecto. Los resultados obtenidos han sido extraídos tanto para plantillas adquiridas con el sensor óptico como térmico y son consistentes con las observaciones realizadas en [25], de donde se concluye que el comportamiento temporal de ambos sistemas es independiente de la base de datos y sensores utilizados. Se han extraído las siguientes conclusiones análogas en ambos sensores:

- No todas las plantillas de la base de datos obtienen una relación entre la variación de la puntuación y la variación del tiempo, por lo que es necesario recurrir a los estadísticos y realizar un promediado de los usuarios analizados para obtener una correlación.
- La media estadística realizada al software NFIS, presenta una correlación directa entre la puntuación y el tiempo (un decremento de la puntuación provoca una disminución del tiempo de comparación) por encima de una determinada puntuación. Por debajo de esa puntuación no se encuentra un patrón de relación.
- El promediado realizado para analizar el sistema *Match-on-Card* muestra una relación contraria a la del NFIS entre puntuación y tiempo (el tiempo aumenta cuando disminuye la puntuación) hasta alcanzar una puntuación relativamente baja.

Es importante remarcar el hecho de que estamos hablando de valores estadísticos, y que no se puede asegurar que el comportamiento general del tiempo al atacar una huella en particular vaya a seguir esa misma tendencia.

En cualquier caso, esto demuestra que existe una relación patente entre puntuación y tiempo y, por tanto, un riesgo potencial de que los sistemas sean vulnerables a ataques *side-channel* basados en tiempo cuyos resultados se presentan en el siguiente apartado.

7.3. Análisis de los ataques

Como se ha descrito en el apartado 7.1., el ataque base del que partimos es un ataque *side-channel* basado en tiempo utilizando la estructura general de un ataque *hill-climbing* tipo 4 analizado en el capítulo anterior.

Los ataques se realizan sobre 100 huellas de la base de datos BiosecurID. Para cada ataque se generarán 100 plantillas con un número inicial de minucias (dependiente de tecnología y base de datos). Dichas plantillas sufrirán dos tipos de modificaciones como consecuencia de los resultados extraídos en los experimentos descritos en el capítulo 6:

B. Añadir una minucia nueva.
C. Sustituir una minucia existente.

Tal y como ya se apuntó al principio de este capítulo, para poder realizar estos ataques necesitábamos obtener una relación entre la puntuación y el tiempo del comparador. La razón es que el sistema elegirá la plantilla que presente un mejor comportamiento en base a las conclusiones extraídas de los resultados descritos en el apartado 7.2. El criterio será entonces:

- **Sistema NFIS:** de las 100 plantillas generadas se escogerá la que genere un mayor tiempo de comparación porque, como se ha estudiado, será la que tenga una mayor probabilidad de haber generado la puntuación más alta.
- **Sistema MoC:** nos quedaremos con la plantilla sintética que genere un tiempo menor ya que, por los resultados de los experimentos llevados a cabo en la sección anterior, son los que en media generarán una mayor puntuación.

Se evaluará también la influencia del número de modificaciones permitidas en cada iteración, es decir, en función de la media de los tiempos obtenidos en las M modificaciones seguiremos un criterio de aceptación o desecho de los cambios (en función de los resultados obtenidos en el análisis temporal):

- **Sistema NFIS:** los cambios realizados serán aceptados si provocan un aumento del tiempo de comparación Tm.
- **Sistema MoC:** los cambios realizados serán aceptados si provocan una disminución del tiempo de comparación Tm.

El umbral de puntuación queda establecido en cada sistema evaluado para obtener una tasa de falsa aceptación (FAR) del 0,1% y los valores se muestran en la Tabla 3.

Se ha considerado que un número máximo de 10.000 iteraciones permitidas para cada ataque es suficiente en ambos sistemas.

Por lo tanto los valores fijos de los ataques son:

- Iteraciones=10.000.
- Plantillas= 100.

Los valores que modificaremos en cada ataque son:

- Umbral.
- Modificaciones permitidas en cada iteración.
- Número inicial de minucias.

7.3.1. Ataque 1: Básico

Este primer experimento se ha realizado utilizando 100 de las plantillas adquiridas con el sensor óptico y las mismas 100 del sensor térmico permitiendo una única modificación por iteración. Como los resultados logrados son muy parecidos, dividiremos este apartado en los dos sistemas descritos en el proyecto.

7.3.1.1. Resultados para el software NFIS

Los umbrales utilizados que fueron calculados en el apartado 5.3.3. para una FAR=0,1% son:

- **Umbral óptico**=26.
- **Umbral térmico**= 38.

Las minucias iniciales ideales para un mejor rendimiento que fueron calculados en el capítulo 6 son:

- **Número de minucias iniciales para plantillas ópticas**=72.
- **Número de minucias iniciales para plantillas térmicas**= 70.

Al finalizar los ataques se puede comprobar que el algoritmo no ha sido capaz de romper el sistema. Se muestran dos ejemplos de ataques para el sensor óptico en la Figura 51 y otros dos ataques probados sobre las mismas plantillas pero adquiridas con el sensor térmico en la Figura 52.

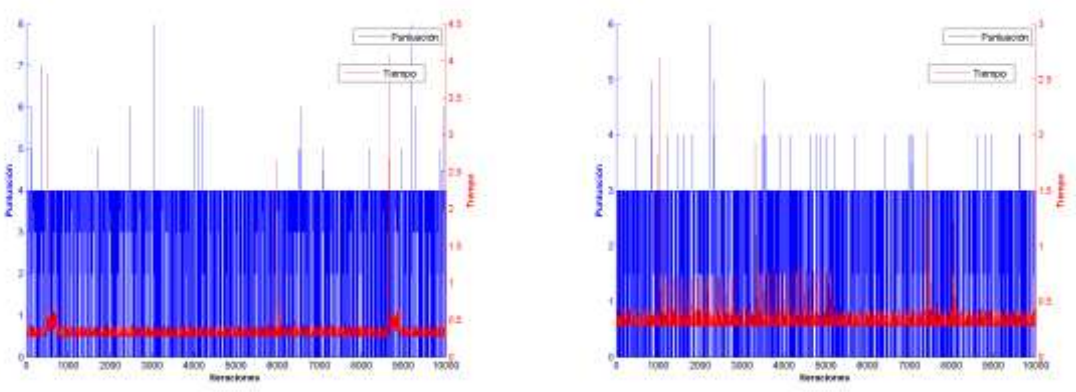


Figura 51: Ejemplos de progresión de puntuación y tiempo para el sistema NFIS con huellas adquiridas por el sensor óptico para un ataque con 1 modificación por iteración.

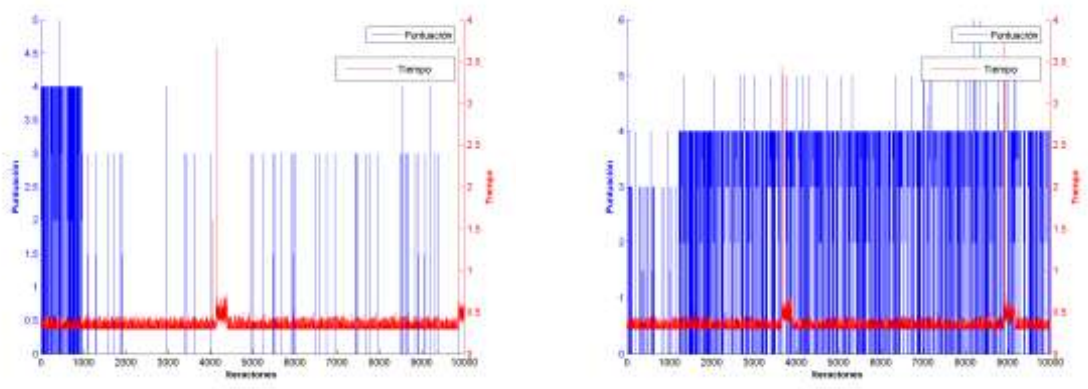


Figura 52: Ejemplos de progresión de puntuación y tiempo para el sistema NFIS con huellas adquiridas por el sensor térmico para un ataque con 1 modificación por iteración.

El resto de huellas sobre las que se ha lanzado el ataque presentan una situación similar.

En los ejemplos se puede apreciar que tanto el tiempo como la puntuación se quedan oscilando alrededor de valores muy bajos. Este hecho se puede explicar con la relación puntuación-tiempo estudiada, donde, para puntuaciones altas (zona A de la Figura 49) existe una relación entre ambos parámetros: si la puntuación disminuye el tiempo desciende pero sólo hasta un valor mínimo en el que se queda oscilando. Como en este caso la puntuación es realmente baja, el ataque se queda estancado y el comportamiento es independiente del tiempo (zona B de la Figura 49).

Mirando los resultados del apartado 7.2. podemos comprobar que la relación entre puntuación y tiempo ocurre para valores de puntuación alrededor de 50 puntos, lo que parece indicar que para que el ataque tuviera éxito necesitamos una puntuación inicial alta para encontrarnos en la región de funcionamiento del sistema donde el tiempo del comparador depende de la puntuación.

7.3.1.2. Resultados para el sistema *Match-on-Card*

Los umbrales utilizados que fueron calculados en el apartado 5.3.3. para una FAR=0,1% son:

- **Umbral óptico**=45.
- **Umbral térmico**= 49.

Las minucias iniciales ideales para un mejor rendimiento que fueron calculados en el capítulo 6 son:

- **Número de minucias iniciales** =41 (limitadas por la capacidad del chip).

Como ocurría con el sistema NFIS, este ataque no consigue romper ninguna de las 100 huellas probadas sobre el sistema de tarjeta inteligente. Diferentes ejemplos se muestran en las siguientes gráficas (Figura 53 y Figura 54).

Por los resultados obtenidos en 7.2., el tiempo inicial de los ataques debe ser relativamente alto ya que irá disminuyendo a medida que aumente la puntuación.

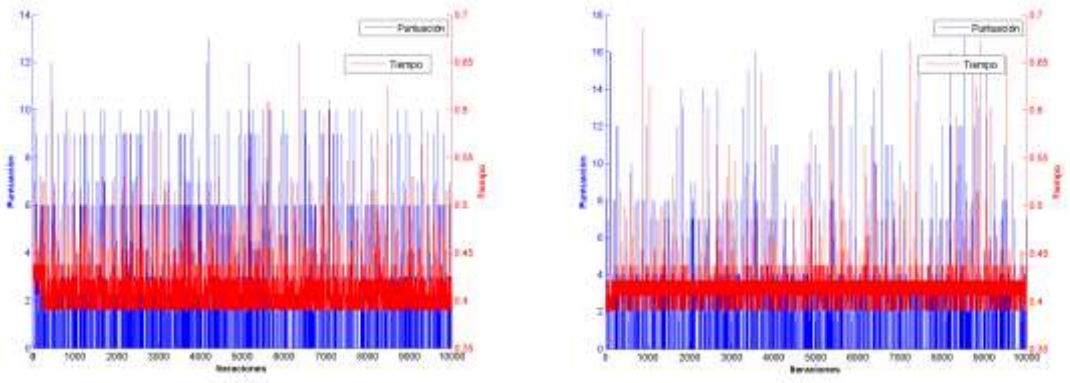


Figura 53: Ejemplos de progresión de puntuación y tiempo para el sistema MoC con huellas adquiridas por el sensor óptico para un ataque con 1 modificación por iteración.

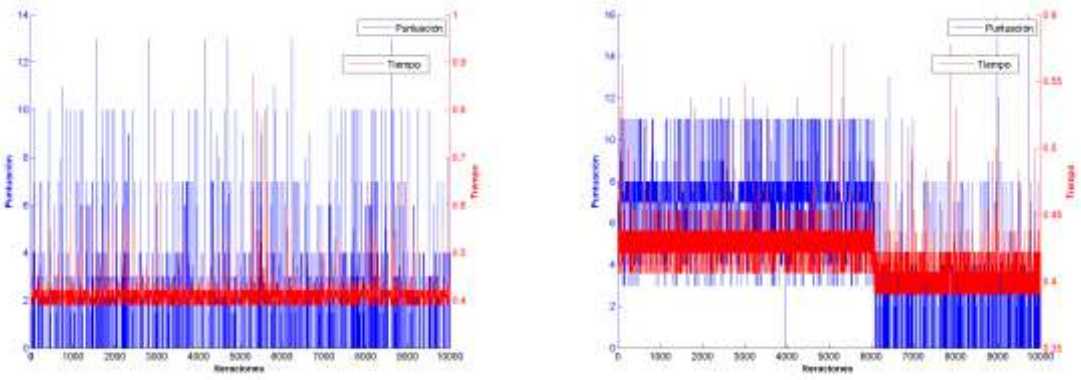


Figura 54: Ejemplos de progresión de puntuación y tiempo para el sistema MoC con huellas adquiridas por el sensor térmico para un ataque con 1 modificación por iteración.

Se observa que las puntuaciones presentan valores ligeramente más elevados que para los casos del sistema NFIS pero esos valores son conseguidos de forma aleatoria y sin evolución continuada. Este hecho ha provocado que desde este momento, y tras no ver una evolución relevante, continuemos realizando experimentos sólo para el sistema NFIS2.

7.3.2. Ataque 2: Puntuaciones altas

Como consecuencia de los resultados del ataque anterior, se excluye de este análisis al sistema *Match-on-Card* y se ha probado a atacar el sistema NFIS2 en la región donde puntuación y tiempo tienen en promedio una relación más o menos clara.

Para realizar estos experimentos se necesita lanzar el ataque empezando en una huella con puntuación inicial relativamente elevada. Para obtener la plantilla inicial se parte de la huella original y se realizan modificaciones sobre ella (perturbar, añadir, sustituir o eliminar una minucia) para conseguir disminuir la puntuación inicial de la huella.

El patrón de minucias obtenido tras aplicar el algoritmo anterior, obtendrá una puntuación inicial alta al compararlo con la huella real. Dicha puntuación dependerá del sistema que estemos analizando y estará basado en el histograma de puntuaciones calculado en el apartado 5.3. de este proyecto.

De esta manera, se decide realizar el ataque partiendo de dos puntuaciones iniciales que muestren el comportamiento del sistema en situaciones diferentes. Se elegirá una puntuación más elevada que en el ataque anterior, pero, a su vez, en la zona donde se solapen las distribuciones de usuarios e impostores. El segundo caso partirá de una puntuación elevada donde sólo exista una distribución de usuarios.

Mirando la Figura 33 (gráfico izquierdo) para el sensor óptico se concluye que dos puntuaciones iniciales razonables para ambos ataques son 30 y 60, mientras que para el sensor térmico corresponden a 20 y 40 (Figura 35, gráfico izquierdo).

En este momento podemos empezar el ataque *side-channel* descrito en el apartado 7.1., obviando la generación de 100 patrones sintéticos aleatorios. Los ataques se han aplicado sobre el sistema NFIS2, permitiendo una sola modificación por iteración y con un umbral de decisión aumentado a 300 puntos (se modifica el umbral objetivo al iniciarse el ataque también desde una puntuación más alta).

7.3.2.1. Resultados para el sistema NFIS

Aunque en el estudio temporal del sistema NFIS se encuentra una relación en promedio entre la puntuación y el tiempo, no se ha conseguido acceder al sistema con este tipo de ataques en ninguna de las 100 plantillas probadas para cada sensor y puntuación inicial. A continuación se muestran varios ejemplos de cada uno de los ataques probados.

- **Ataque a huellas adquiridas con un sensor óptico y una puntuación inicial máxima de 30.**

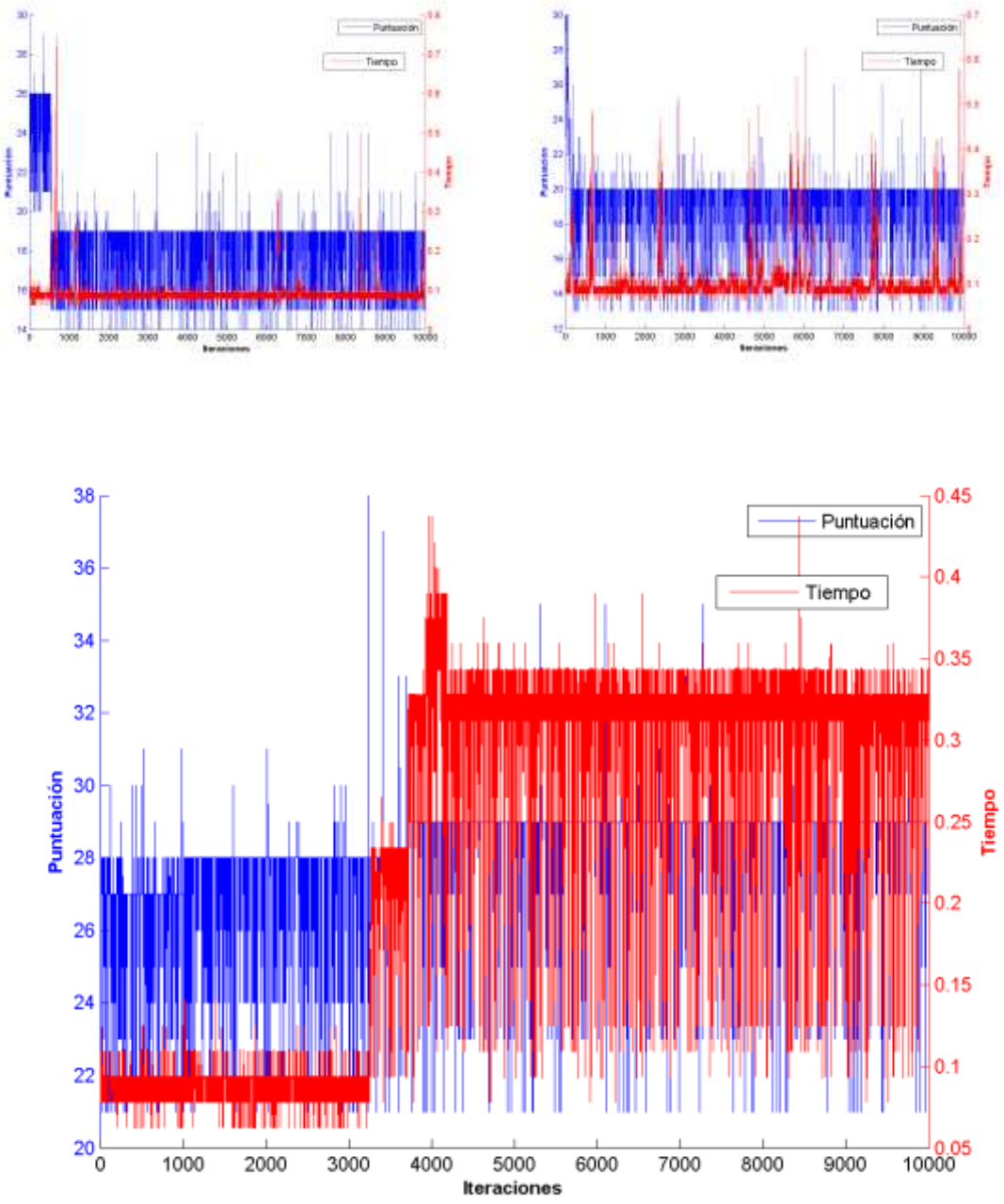


Figura 55: Ejemplos de ataques side-channel para sensor óptico con puntuación inicial máxima de 30, donde no se consigue acceder al sistema.

Las dos gráficas de arriba representan los resultados obtenidos por la mayoría de las huellas dactilares probadas. La puntuación oscila por los valores inferiores al máximo establecido (30 puntos) y no asciende considerablemente en ningún caso. En la Figura 55 abajo se muestra un ataque en el que sí que se consigue un aumento de la puntuación pero no lo suficientemente alto como para romper el sistema.

- **Ataque a huellas adquiridas con un sensor óptico y una puntuación inicial máxima de 60.**

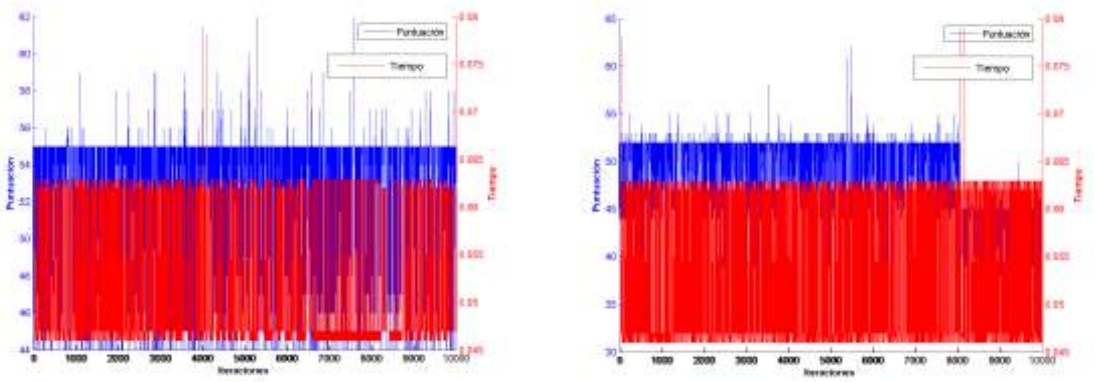


Figura 56: Ejemplos de ataques side-channel para sensor óptico con puntuación inicial máxima de 60, donde no se consigue acceder al sistema.

Los resultados obtenidos demuestran que el ataque no tiene éxito y por tanto no se accede al sistema tras 10.000 iteraciones. Además, se observa (Figura 56, gráfica derecha) que no existe una correlación en algunos de los usuarios probados ya que el tiempo permanece prácticamente constante mientras que la puntuación disminuye.

- **Ataque a huellas adquiridas con un sensor térmico y una puntuación inicial de 20.**

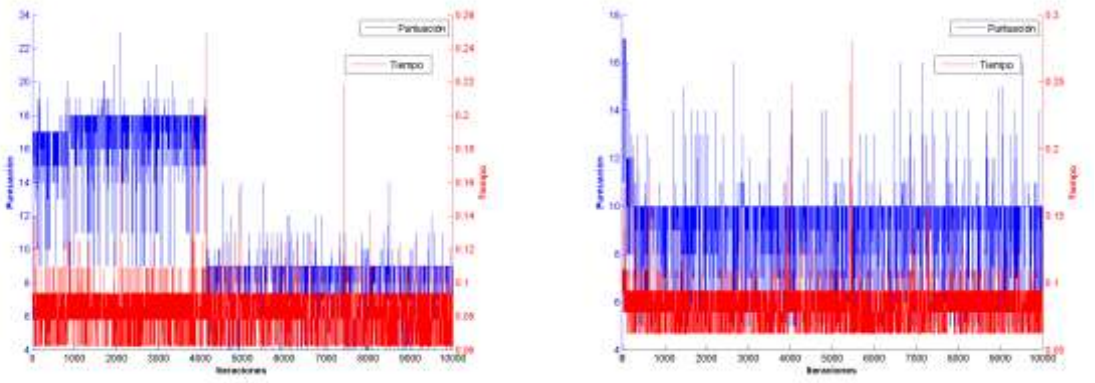
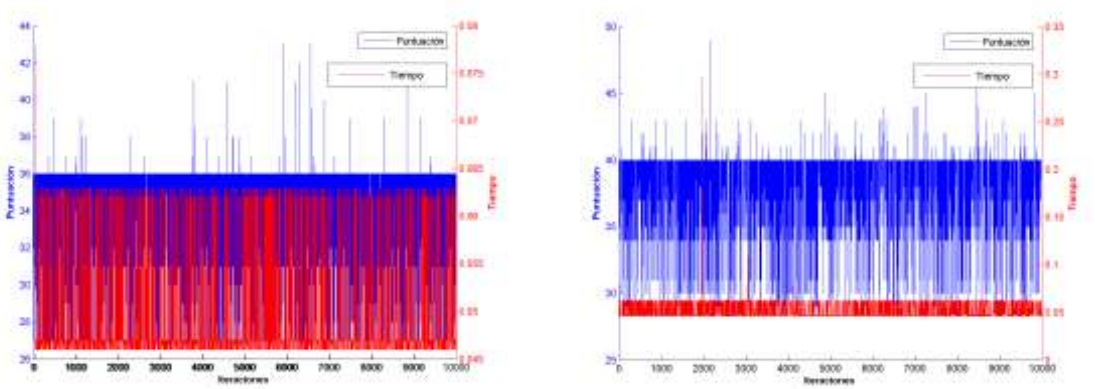


Figura 57: Ejemplos de ataques side-channel para sensor térmico con puntuación inicial máxima de 20, donde no se consigue acceder al sistema.

Las graficas no muestran ninguna correlación directa entre el tiempo y la puntuación ya que un aumento o disminución del tiempo no provoca el comportamiento esperado de la puntuación.

Tras 10.000 iteraciones y partiendo de una puntuación máxima de 20, al realizar diferentes modificaciones la puntuación no aumenta de forma apreciable, lo que indica que el ataque basado en tiempo no ha tenido éxito.

- **Ataque a huellas adquiridas con un sensor térmico y una puntuación inicial de 40.**



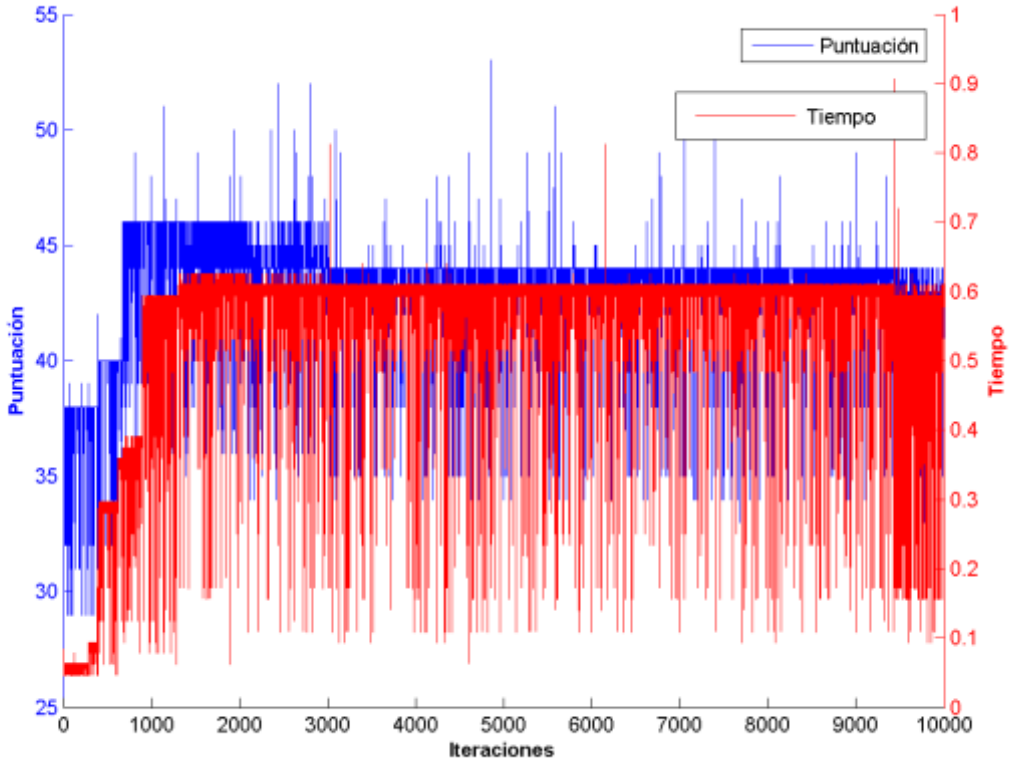


Figura 58: Ejemplos de ataques side-channel para sensor térmico con puntuación inicial máxima de 40, donde no se consigue acceder al sistema.

La Figura 58 es representativa de los usuarios probados. Las dos gráficas de arriba no muestran ninguna relación entre puntuación y tiempo con lo que no se logra acceder al sistema. En la gráfica de debajo se muestra un ejemplo en el que se puede apreciar que un aumento en el tiempo que tarda el comparador involucra un aumento de la puntuación aunque de nuevo no suficiente para romper el sistema.

7.3.3. Conclusiones

Los diferentes ataques *side-channel* implementados han generado diferentes conclusiones que se exponen a continuación.

Para empezar, se ha realizado un ataque denominado básico en el que el sistema era atacado con un algoritmo *hill-climbing* tipo 4 al que se le realizan modificaciones basadas en el tiempo de comparación. Dicho algoritmo no ha permitido un acceso al sistema con ningún software (NFIS o MoC), pero se ha comprobado que la relación entre puntuación y tiempo observada en 7.2. se cumple en el sistema NFIS mientras que no ocurre lo mismo con MoC (el tiempo permanece estable independientemente del comportamiento de la puntuación).

Las puntuaciones obtenidas para MoC son más elevadas, pero son conseguidas de forma aleatoria por lo que se decide continuar sólo realizando experimentos con el sistema NFIS.

En los experimentos en los que se observó la relación puntuación-tiempo (apartado 7.2.) pudimos apreciar que era necesaria una puntuación inicial alta para que dicha relación se produjera. El segundo experimento intenta obtener un acceso al sistema partiendo de la huella original degradada para conseguir una puntuación de comparación inicial determinada. A partir de ese punto se realiza el mismo algoritmo que el empleado en el ataque 1. Este ataque no obtiene ningún acierto, es decir, ninguno de los 100 usuarios de ninguno de los sensores que se han degradado y comparado con la huella real han podido acceder al sistema, pero sí que se ha podido observar que para este ataque en algunos ejemplos se consigue un aumento razonable de la puntuación.

Así pues, sí hemos podido corroborar con este ataque que la correlación entre puntuación y tiempo existe. Por tanto, podemos afirmar que los sistemas de reconocimiento automático de huella dactilar basados en minucias son potencialmente vulnerables a ataques *side-channel* en función del tiempo y que es necesario tenerlos en cuenta a la hora de diseñar este tipo de aplicaciones.

8

Conclusiones y trabajo futuro

8.1. Conclusiones

En el presente proyecto se ha llevado a cabo una revisión del estado del arte de los sistemas de reconocimiento biométrico y de las vulnerabilidades que los mismos pueden presentar. Este estudio se realizó con el objetivo de comparar la viabilidad de transformar los ataques *hill-climing* basados en puntuación, a ataques *side-channel* basados en tiempo (tras un análisis temporal previo de los sistemas).

Se ha estudiado la robustez frente a los ataques de dos sistemas: el sistema de referencia NFIS2 del NIST y un sistema basado en tarjeta inteligente *Match-on-Card*.

La base de datos empleada en el laboratorio es BiosecurID. Consta de 25.600 huellas por cada tipo de sensor (óptico de contacto y térmico de barrido) provenientes de: 400 usuarios, 4 sesiones, 4 dedos, 4 muestras. A partir de esta base de datos se han calculado 24.000 puntuaciones de usuario y 160.000 puntuaciones de impostor para evaluar cada uno de los sistemas. Tras el análisis del rendimiento de cada sistema con la base de datos se obtiene una menor tasa de error para el sistema NFIS2 ante MoC, y en ambos casos, para la captura con sensor óptico frente al térmico (debido a una menor calidad de las muestras capturadas con este último).

El ataque *hill-climbing* muestra tasas de éxito diferentes para cada sistema y sensor empleado. Los experimentos han generado una serie de conclusiones relativas a la eficiencia del algoritmo del ataque en función del entorno experimental (la base de datos, sistemas y sensores utilizados):

- Un mejor rendimiento y probabilidad de éxito del ataque frente al sistema MoC comparado con NFIS, debido a las restricciones de almacenamiento y capacidad de cómputo del sistema distribuido frente al centralizado.
- El algoritmo de ataque resulta ligeramente más eficiente a la hora de romper huellas de mayor calidad (obtenidas con el sensor óptico).

- La utilización de una región de interés (ROI) proporciona mejores resultados sólo en el caso de utilizar una base de datos adquirida con niveles de control.
- Las modificaciones que aumentan la tasa de éxito en mayor proporción son en todo caso añadir minucia y sustituir minucia.
- El número inicial de minucias que proporciona un mayor rendimiento depende de la tecnología empleada. El sistema NFIS es más eficiente si el número inicial de minucias corresponde al número medio de minucias de las huellas de la base de datos empleada. Por su parte el sistema MoC tendrá una mayor probabilidad de atacar al sistema si dicho número está entorno al 60% del número medio de minucias de la base de datos (respetando las limitaciones de la tarjeta).
- El sensor óptico es menos robusto frente al ataque (lo que implica que el ataque es más eficiente contra huellas de menor calidad).

El segundo ataque implementado ha sido el ataque *side-channel* basado en la información temporal de los sistemas y en los datos extraídos del ataque *hill-climbing* clásico analizado anteriormente. Este algoritmo requería un estudio temporal previo en el que se relacionase la variación del tiempo con la variación de la puntuación. Este análisis ha demostrado que en promedio la relación entre ambos parámetros en el software NFIS2 es directa (puntuación y tiempo aumentan o disminuyen al tiempo), mientras que en el sistema MoC es contraria (al aumentar la puntuación disminuye el tiempo y viceversa).

En base a los datos obtenidos en el análisis temporal, se llevan a cabo dos tipos de ataques *side-channel*. Los resultados para las huellas adquiridas con sensor óptico y térmico han sido muy parecidos en ambos ataques.

En primer lugar se ha realizado un ataque básico estableciendo los umbrales en el punto donde la tasa de falsa aceptación (FAR) es del 0,1% y que se han calculado en el capítulo 5. En ninguno de los casos se consigue acceder al sistema pero se puede apreciar que para poder atacarlo es necesaria una puntuación inicial alta. Por otro lado, las puntuaciones obtenidas para MoC son más elevadas pero son conseguidas de forma aleatoria lo que hace que segundo ataque sólo se evalúe el sistema NFIS.

El segundo ataque parte de puntuaciones altas (donde la relación puntuación-tiempo es más marcada) conseguidas utilizando la huella real del usuario degradada. La puntuación de la que parte cada ataque es dependiente del sensor de adquisición empleado.

Los resultados de este segundo ataque no han conseguido acceder al sistema para ninguna huella o puntuación inicial establecida, pero si se ha conseguido un aumento en la puntuación razonable. Además, se ha corroborado que existe una relación entre puntuación y tiempo y por tanto que los sistemas de reconocimiento automático de huella dactilar basados en minucias son potencialmente vulnerables a este tipo de ataques.

8.2. Trabajo futuro

Se propone en primer lugar la optimización de los algoritmos utilizados para un menor tiempo de cómputo y número de iteraciones necesarias en cada ataque. Además podrían adaptarse estos sistemas al estudio de las vulnerabilidades de los sistemas biométricos multimodales combinando por ejemplo cara y huella dactilar para realizar ataques *hill-climbing*.

El estudio de este tipo de amenazas es muy importante para evaluar la seguridad del sistema, por esta razón, existen estándares de comparación de seguridad en el ámbito biométrico. Sería conveniente una comparación objetiva de estos resultados con los estándares.

Unos de los sistemas de seguridad más estudiados en la actualidad son los criptográficos. En este ámbito podría adaptarse los algoritmos *side-channel* basados en tiempo desarrollados en sistemas criptográficos a los sistemas de reconocimiento biométrico automático.

Al conocer el comportamiento de estos sistemas, también se propone desarrollar contramedidas a las vulnerabilidades derivadas de la información temporal que se puede obtener de los sistemas (tales como la aleatorización temporal del comparador).

Bibliografía

1. **D. Maltoni, D. Maio, A. Jain, and S. Prabhakar.** *Handbook of Fingerprint Recognition.* Springer, 2003.

2. **K. Jain, A. Ross, and S. Prabhakar.** "Biometrics: a Tool for Information Security". *IEEE Trans. on Information Forensics and Security.* 1(2): 125-143, 2006.

3. **L. Hong.** *Automatic Personal Identification Using Fingerprints. Michigan State University, East Lansing, MI, USA.* 1998.

4. **D. Maio, and D. Maltoni.** "Direct Gray-Scale Minutiae Detection in Fingerprints". *IEEE Trans. on Pattern Analysis and Machine Intelligence.* Vol. 19 no. 1. pp. 27-40. 1997.

5. **B. Schneier.** *Secrets and Lies: Digital Security in a Networking World.* Jonh Wiley & Sons. 2000.

6. **N. Ratha, J. H. Connell, R. M. Bolle.** "An Analysis of Minutiae Matching Strength". In *Proc. IAPR Audio-and Video- Based Person Authentication (AVBPA),* pages. 223-228. Springer LNCS-2091. 2001.

7. **R. Capelli, D. Maio, A. Lumini, and D. Maltoni.** "Fingerprint Image Reconstruction from Standard Templates". *IEEE Trans. on Pattern Analysis and Machine Inteligenc.* 29:1489-1503, September 2007b.

8. **J. Galbally, R. Capelli, A. Lumini, D. Maltoni, and J. Fierrez.** "Fake Fingertip Generation from a Minutiae Template". In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR),* pages 1-4, 2008a.

9. **Van der Putte and J. Keuning.** "Biometrical Fingerprint Recognition: Don't Ger your Fingers Burned".In *Proc. Conference on Smart Card Research and Advanced Applications (CARDIS),* pages. 289-303, 2000.

10. **T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino.** "Impact of Artificial Gummy Fingers on Fingerprint Systems". In *Proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV, Volume 4677,* pages 275-289, 2002.

11. **J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-García, and M. Tapiador.** "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprint Attacks". In *Proc. IEEE Intl. Carnahan Conf. on Security Technology (ICCST),* volume 1, pages 130-136. 2006.

12. **R. Derakhshani, S. Schuckers, L. Hornak, and L. O'Gorman.** "Determination of Vitality from a Non-Invasive Biomedical Measurement for Use in Iingerprint Scanners". *Pattern Recognition.* 36:386-396, 2003.

13. **B. Tan and S. Schuckers.** "Comparison of Ridge- and Intensity-Based Perspiration Liveness Detection Methods in Fingerprint Scanners". In *Proc. SPIE Biometric Technology for Human Identification III (BTHI III), volume 6202,* page *62020A,* 2006.

14. **R. Capelli, D. Maio, and D. Maltoni.** "Modelling Plastic Distortion in Fingerprint Images". In *Proc. Int. Conf. on Advances in Pattern Recognition (ICAPR),* pages. 369-376. Springer LNCS-2013, 2001.

15. **A. Antonelli , R. Capelli, D. Maio, and D. Maltoniet.** "Fake Finger Detection by Skin Distortion Analysis". *IEEE Trans. on Information Forensics and Security,* 1:360-373, 2006.

16. **D. Baldiserra, A. Franco, D. Maio, and D. Maltoni.** "Fake Fingerprint Detection by Odor Analysis". In *Proc. IAPR Int. Conf. on Biometrics (ICB).* pages. 265-272. Springer LNCS-3832, 2006.

17. **B. Tan, A. Lewicke, and S. Schuckers.** "Novel Methods for Fingerprint Image Analysis to Detect Fake Fingers". *SPIE Newsroom,* 2008.

18. **H. Choi, R. Kang, K. Choi, and J. Kim.** "Aliveness Detection of Fingerprints Using Multiple Stactic Features". In *Proc. of Worlds Academy of Science, Engineering and Technology. Vol. 28.* 2007.

19. **Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo.** "Wavelet Based Fingerprint Liveness Detection". *Electronics Letters,* 41, 2005.

20. **C. Jin, H. Kim, and S. Elliott.** "Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum". In *Proc. Int. Conf. on Information Securety and Cryptology (ICISC),* pages. 168-179. Springer LNCS-4817, 2007.

21. **C. J. Hil.** "Risk of Masquerade Arising from the Storage of Biometrics". Master's Thesis. Australian National University, 2001.

22. **N. K. Ratha, J. H. Connell, and R. M. Bolle.** "Enhancing Security and Privacy in Biometrics-Based Authentication Systems". *IBM Systems Journal.* 40:614-634, 2001b.

23. **U. Uludag, and A. K. Jain. "**Attack on Biometric Systems: A Case Study in Fingerprint". In *Proc. SPIE Seganography and Watermarking of Multimedia Contents VI,* volume 5306, pages. 622-633, 2004.

24. **M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-García, and J. A. Siguenza.** "Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification". In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST), v*olume 1. pages. 151-159, 2006.

25. **J. Galbally, S. Carballo, J. Fierrez and J. Ortega-Garcia.** "Vulnerability Assessment of Fingerprint Matching Based on Time Analysis". *In Proc. Biometric ID Management and Multimodal Communication, BioID, Madrid, SPAIN,* pages. 285--292. Springer LNCS-5707. September 2009.

26. **J. Kelsey,B. Schneier, D. Wagner, and C. Hall.** "Side Channel Cryptanalysis of Product Ciphers*". Journal of Computer Security,* volume 8, pages. 141-158. 2000.

27. **P. Kocher.** "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*". In Proc. Int. Cryptology Conf. on Advances in Cryptology, pages. 104-113.* Springer LNCS-1109, 1995.

28. **P. Kocher, and J. Jaffe, and B. Jun.** "Differential Power Analysis*". In Proc. Advances in Cryptology (Crypto 99), pages 388-397.* Springer LNCS-1666, 1999.

29. **W. Schindler, F. Koeune, and J. J. Quisquater.** "Unleashing the Full Power of Timing Attacks". *Technical Report, Universite Catholique de Louvain.* 2001.

30. **D. Brumley, and D. Boneh.** "Remote Timing Attacks are Practical*". In Proc. USENIX Security Symposium,* volume 12. 2003.

31. **E. Tabassi, C. Wilson, C. Watson.** "Fingerprint Image Quality*", Technical Report 7151.* August 2004.

32. **J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. Gonzalez-de-Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras and J. J. Gracia-Roche.** "BiosecurID: A Multimodal Biometric Database*", Pattern Analysis and Applications.* 2009.

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

34. **N. K. Ratha, S. Y. Chen, and A. K. Jain.** "Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images*". Pattern Recognition,* volume 28, no. 11, pages. 1657-1672. 1995.

35. **D. Maltoni.** "A Tutorial on Fingerprint Recognition, Advanced Studies in Biometrics*". Summer School on Biometrics, Alghero, Italy, June 2003 .* Springer LNCS-3161. 2005.

36. **M. Garris, C. Watson, R. McCabe, and C. Wilson.** "User's Guide to NIST Fingerprint Image Software 2 (NFIS2)".*National Institute of Standards and Technology,* 2004.

Glosario

ADN	Acido Desoxirribo-Nucleico
ATVS	Área de Tratamiento de Voz y Señal
CCD	Charge-Coupled Device
CMOS	Complementary Metal Oxide Semiconductor
DET	Detection Error Trade-off
EER	Error Equal Rate
FAR	False Acceptance Rate
FDP	Función Densidad de Probabilidad
FRR	False Rejection Rate
FTIR	Frustrated Total Internal Reflection
LED	Light-Emitting Diode
MoC	Match on Card
NFIS	NIST Fingerprint Image Software
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
ROC	Receiver Operating Curve

A. Presupuesto

1) Ejecución Material

- Compra de ordenador personal (Software incluido)..... 2.000 €
- Compra de sistema de tarjeta inteligente..... 14 €
- Compra de tarjeta con chip incorporado.....2 €
- Alquiler de impresora láser durante 6 meses ..... 50 €
- Material de oficina.....150 €
- Total de ejecución material ..... 2.216 €

2) Gastos generales

- 16 % sobre Ejecución Material..... 354 €

3) Beneficio Industrial

- 6 % sobre Ejecución Material ..... 133 €

4) Honorarios Proyecto

- 640 horas a 15 € / hora ..... 9600 €

5) Material fungible

- Gastos de impresión ..... 200 €
- Encuadernación..... 60 €

6) Subtotal del presupuesto

- Subtotal Presupuesto ..... 12079 €

7) I.V.A. aplicable

- 16% Subtotal Presupuesto..... 1932.6 €

8) Total presupuesto

- Total Presupuesto ..... 14011,6 €

Madrid, Abril de 2010
El Ingeniero Jefe de Proyecto
Fdo.: Alicia Hortensia Beisner Muñoz
Ingeniero Superior de Telecomunicación

B. Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto. 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.