UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

PROYECTO FIN DE CARRERA

Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica

Sara Carballo Domínguez

Mayo de 2009

Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica

AUTOR: Sara Carballo Domínguez
TUTOR: Javier Galbally Herrero
PONENTE: Javier Ortega García

Área de Tratamiento de Voz y Señales
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Mayo de 2009

Resumen

La identificación personal es una tarea fundamental en nuestra vida cotidiana y la necesidad de técnicas de autenticación de usuario automáticas y fiables es una realidad. A este respecto, los sistemas de reconocimiento biométrico suponen una nueva dimensión si los comparamos con los sistemas clásicos de reconocimiento automático, ya que los primeros permiten que el usuario sea reconocido mediante un rasgo único e inherente a él mismo. La huella dactilar es, sin duda, uno de los rasgos biométricos más importantes y es por ello que la realización de este proyecto está basada en ella.

Por otro lado, para poder prevenir y evitar los riesgos derivados de las vulnerabilidades que presentan los sistemas de reconocimiento biométrico, es muy importante conocerlas en detalle y profundizar en ellas, con el objetivo final de que un usuario malintencionado nunca pueda hacer uso de datos protegidos u obtener acceso fraudulento al sistema atacado.

Así, este proyecto se centra en el análisis de la información temporal de los sistemas de reconocimiento automático de huella dactilar y en su aplicación a ataques tipo *hill-climbing* sobre sistemas de reconocimiento biométrico de huella dactilar. Esta clase de ataque consiste en modificar sucesivamente un patrón sintético de minucias de tal forma que la puntuación devuelta por el sistema vaya incrementándose paulatinamente hasta lograr que dicho sistema acepte nuestro patrón como válido y nos permita el acceso al mismo.

En la literatura existente sobre huella dactilar se han propuesto diversos ataques *hill-climbing* basados en la puntuación obtenida en el comparador para modificar sucesivamente los patrones sintéticos en base a ella y así lograr el acceso al sistema. Teniendo en cuenta que no todos los sistemas de reconocimiento de huella devuelven esta puntuación o *score*, lo que se propone en este proyecto es la realización de ataques *hill-climbing* en base al tiempo de comparación algorítmica que emplea el sistema. Es decir, trataremos de establecer si el tiempo que tarda el sistema en aceptarnos o denegarnos el acceso está de alguna manera relacionado con la respuesta afirmativa o negativa del sistema. Una vez establecida la relación entre esta respuesta y el tiempo de cómputo, acometeremos diferentes ataques contra el sistema, evaluaremos su comportamiento y comprobaremos la eficiencia de los algoritmos de ataque desarrollados.

El análisis temporal y los ataques se realizan sobre dos sistemas 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*, el cual 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.

Tras la realización de diversos experimentos, los sistemas atacados se han mostrado robustos frente a los ataques implementados. Sin embargo, sí se ha descubierto una considerable correlación entre la puntuación generada por el comparador de los sistemas y el tiempo que tardan los sistemas en devolver dicha puntuación, por lo que no se descarta que ataques más complejos también basados en tiempo sean capaces de vulnerar ambos sistemas.

Abstract

Personal identification is a fundamental task in everyday life, which has lead to an increasing need for automatic and reliable user authentication techniques in our current networked society. In this field, biometric systems represent a new point of view, for they allow the user to be recognized by a unique personal physiological feature. The fingerprint is the most widely used biometric trait and will be the object of research of the present work.

In order to be able to avoid the risks which result from biometric systems' vulnerabilities, it is important to get to know them thoroughly, with the aim of preventing an attacker from accessing our system and protected data.

This research is focused on the analysis of the time information obtained from the monitoring of automatic fingerprint recognition systems, and the application of this information on "hill-climbing" attacks. These attacks iteratively modify a synthetic minutiae template so that the score given by the system increases until access to the system is granted.

However, in many biometric systems the score might not be accessible. Hence a time-based hill-climbing attack is proposed. Firstly, it is studied whether the matching time is related to the resulting score in any way. Once a relation is established, different attacks will be performed against the system, and the developed algorithm's behavior and efficiency will be evaluated.

The time analysis and the attacks will be performed against two different systems: NIST's NFIS reference software, developed for fingerprint automatic processing and based on modules to be 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 data-base for storing the user's templates and thus solves all communication issues between the system and the data-base.

The experimental results showed that the systems are robust to the developed attacks. Nonetheless, it is also proven a clear relation between the given score and the matching time. Therefore, an enhanced algorithm and more complex attacks will possibly be able to break both systems.

Palabras clave

Reconocimiento biométrico, huella dactilar, seguridad, *hill-climbing*, ataques basados en tiempo, NFIS2, tarjeta inteligente.

Key Words

Biometric recognition, fingerprint, security, hill-climbing, timing-attacks, NFIS2, Match-on-Card.

Agradecimientos

Quisiera comenzar agradeciendo a mí ponente, Javier Ortega, haberme dado la oportunidad de colaborar con el ATVS durante todo este tiempo y poder así haber llevado a cabo este proyecto, con el que he disfrutado tanto.

Quiero agradecer, por supuesto, a mi tutor, Javier Galbally, por todo el tiempo que me ha dedicado, por haberme dejado interrumpirle una y mil veces, y por haberme llenado la hoja de rojo; pero, sobre todo, por hacer de todo un poco más divertido.

Gracias a todos y cada uno de los miembros del ATVS, que durante todo este tiempo me han prestado su ayuda siempre que la he necesitado, especialmente Manuel Freire, que hizo las veces de padrino cuando llegué al Grupo y que me ha ayudado siempre que lo he necesitado con la mejor predisposición; Julián Fiérrez, por su ayuda guiando la realización del proyecto; Marcos Martínez, que se tomó siempre el tiempo de resolver mis dudas y proporcionarme el material que necesitaba; y Jesús Marcos, por acompañarme en este último tramo de la carrera y por cuidar tan bien de mi ordenador durante mis ausencias.

Durante todo el tiempo que he estado estudiando la carrera he tenido la oportunidad de conocer a gente maravillosa. Han sido unos años agotadores, pero esta será una experiencia de vida que no olvidaré jamás. Gracias, chic@s, por todo el tiempo compartido, por las infinitas horas que hemos pasado en la uni y por haberme hecho ver la vida de todos los colores. Los mejores años de mi vida vienen con vosotros de regalo. Nunca os olvidaré.

Quisiera, por último, agradecer a mi familia la confianza y la paciencia que ha tenido durante estos años, sobre todo en los peores momentos; a mis amigos, por estar siempre de mi lado, y a Aitor, por estar ahí cada vez, por apoyarme siempre, por sufrir conmigo cuando las cosas iban mal y por hacerme más feliz cuando todo iba bien: gracias por ser quien eres y ayudarme a ser quien soy.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

1. Introducción

1.1. Motivación

La identificación personal es una tarea fundamental en nuestra vida cotidiana. El ser humano identifica a su familia, amigos y conocidos con facilidad. Sin embargo, debido al crecimiento de las industrias del transporte y la comunicación, y los rápidos avances en redes y movilidad, la tarea de identificación personal se ha vuelto mucho más complicada. Esto, unido al aumento de la preocupación por la seguridad en multitud de ámbitos, genera la necesidad de técnicas de autenticación de usuario automáticas y fiables.

Los sistemas de reconocimiento biométrico suponen una nueva dimensión respecto a los sistemas clásicos de reconocimiento automático como tarjetas magnéticas, claves, etc., pues permiten que el usuario sea reconocido mediante un rasgo único e inherente a él mismo y no por la posesión o conocimiento de una llave o clave. De entre los rasgos biométricos más utilizados en la actualidad para el reconocimiento personal, la huella dactilar cobra especial importancia gracias a su alta eficiencia como método identificativo, su reducido tamaño - lo que permite que los sistemas de reconocimiento basados en huella sean fácilmente integrables -, su bajo coste, su relativo sencillo funcionamiento y su probada eficacia. La huella dactilar es, de hecho, el rasgo biométrico con mayor ocupación de mercado en la actualidad.

Por otro lado, en el mundo global en el que vivimos es importante la existencia de cierta compatibilidad entre dispositivos y sistemas, la cual no hace sino aumentar la vulnerabilidad de los sistemas de reconocimiento - incluidos aquéllos basados en rasgos biométricos - frente a ataques externos. Precisamente para poder prevenir y evitar los riesgos derivados de estas vulnerabilidades, es muy importante conocerlas en detalle y profundizar en ellas, con el objetivo final de que un usuario malintencionado nunca pueda hacer uso de datos protegidos u obtener acceso fraudulento al sistema.

Dentro de este contexto, en el presente proyecto se pretende realizar un análisis de la información temporal de los sistemas de reconocimiento automático de huella dactilar y comprobar si dicha información puede representar una amenaza real para el sistema cuando ésta es utilizada para intentar acceder fraudulentamente al mismo.

1.2. Objetivos

A partir de las motivaciones expuestas en la sección anterior, se plantean como objetivos del presente proyecto los siguientes:

- Revisión del estado del arte de las vulnerabilidades de los sistemas de reconocimiento biométrico, prestando especial atención a los ataques tipo *hill-climbing*.
- 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 extraída del cómputo del tiempo que tarda un sistema de reconocimiento automático de huella dactilar en el proceso de comparación algorítmica, y estudio de la posibilidad de que dicha información represente una

vulnerabilidad en este tipo de aplicaciones y pueda ser utilizada para desarrollar ataques que permitan acceder fraudulentamente al sistema.
- Desarrollo de ataques tipo *hill-climbing* basados en el tiempo que emplea el comparador y análisis de su efectividad para atacar con éxito sistemas de reconocimiento automático de huella dactilar.

Para cumplir estos objetivos se analizará el comportamiento de dos sistemas de reconocimiento de huella distintos: el software de referencia NFIS2 del NIST americano y un sistema basado en tarjeta inteligente *Match-on-Card* (MoC).

1.3. Organización de la memoria

La memoria consta de los siguientes capítulos:

1. Introducción.
2. Reconocimiento biométrico.
3. Reconocimiento de huella dactilar.
4. Ataques a sistemas de reconocimiento biométrico.
5. Entorno experimental.
6. Análisis temporal de los sistemas.
7. Resultados de los ataques.
8. Conclusiones y trabajo futuro.

En el capítulo de **introducción** se ha realizado una exposición acerca de la motivación y objetivos de este proyecto.

En el capítulo 2 se profundiza en el estado del arte del **reconocimiento biométrico**, haciendo especial hincapié en la huella dactilar como método identificativo.

El capítulo 3 se centra en el estudio de la huella dactilar y en detallar el funcionamiento de los sistemas de **reconocimiento de huella dactilar**, de nuevo con especial atención sobre aquellos sistemas basados en huella dactilar.

En el capítulo 4 se presentan las amenazas a las que están expuestos los sistemas de reconocimiento automático y los tipos de **ataques** que se pueden llevar a cabo sobre los sistemas de reconocimiento biométrico, dedicando un apartado a los ataques tipo *hill-climbing*, en el cual se cita la literatura existente al respecto. Se presentan igualmente los ataques conocidos en criptografía como ataques *side-channel*, entre los que se encuentran los ataques basados en tiempo (*timing-attacks*).

En el capítulo 5 se detallan las características del **entorno experimental**, es decir, se presentan los sistemas que serán analizados – el software de referencia NFIS2 del NIST y un sistema integrado en una tarjeta inteligente o MoC - y la base de datos utilizada. Además, se proporciona una estimación del rendimiento que presentan los sistemas a estudio con dicha base de datos. Se detalla en este capítulo el algoritmo de ataque implementado para atacar los sistemas presentados.

El capítulo 6 muestra los resultados obtenidos tras la realización de dos experimentos cuyo objetivo es el **análisis temporal de los sistemas** descritos para establecer si existe alguna relación entre la puntuación devuelta por la aplicación y el tiempo que tarda en generarla.

En el capítulo 7 se muestran los **resultados** que obtienen los **ataques** implementados sobre los sistemas descritos - analizados en apartados anteriores -, que consisten en una serie de ataques *hill-climbing* a los dos sistemas de reconocimiento biométrico mencionados.

En el capítulo final de la memoria se presentan las **conclusiones y** el **trabajo futuro**. En él se detallan las conclusiones extraídas de todo el trabajo realizado y se proponen posibles directrices a seguir en futuros trabajos en la misma línea de investigación o similares.

2. Reconocimiento biométrico

2.1. Introducción

Hoy en día, las técnicas de identificación personal más utilizadas son aquellas basadas en contraseñas, tarjetas magnéticas, PINs y otros elementos basados en la posesión o conocimiento de cierta información.

Figura 1: Diferentes aparatos comerciales que utilizan sistemas de identificación personal clásicos.

El problema es que las contraseñas se pueden olvidar, las tarjetas magnéticas se pueden perder y ambas pueden ser robadas. Además, estos sistemas tradicionales de reconocimiento no son capaces de distinguir entre un impostor que obtiene fraudulentamente el acceso a estos privilegios – tarjetas, contraseñas - del propietario legítimo de éstos. De este hecho surge la importancia del reconocimiento personal a partir de uno o varios rasgos biométricos. Así, en lugar de comprobar el conocimiento o la posesión del usuario, éste es identificado comprobando un rasgo o comportamiento inherente a él mismo.

Figura 2: Ejemplos de sistemas comerciales que utilizan sistemas biométricos de identificación personal.

2.2. Características de los rasgos biométricos

Para que un rasgo biométrico pueda ser utilizado para la identificación personal debe cumplir una serie de características, como son (1):

- **Unicidad**: dos personas cualesquiera pueden ser distinguidas suficientemente una de otra basándose en ese rasgo.
- **Universalidad**: todas las personas deben presentar dicho rasgo.
- **Permanencia** en tiempo a corto plazo.
- **Estabilidad** a largo plazo y en condiciones ambientales diversas.
- **Cuantificabilidad**: debe ser un rasgo que se pueda caracterizar cuantitativamente.

Además, son también deseables características como una alta aceptabilidad, rendimiento y robustez frente a ataques externos.

2.3. Rasgos biométricos

Los principales rasgos biométricos utilizados en la actualidad son (1): el ADN, la voz, la cara, la huella, la firma, el iris y la mano.

En menor medida también se pueden encontrar estudios sobre la retina, la oreja, el termograma de la cara, el termograma de la mano, la distribución de las venas en la mano e, incluso, otros rasgos menos distintivos como el olor, la forma de caminar y la forma de teclear.

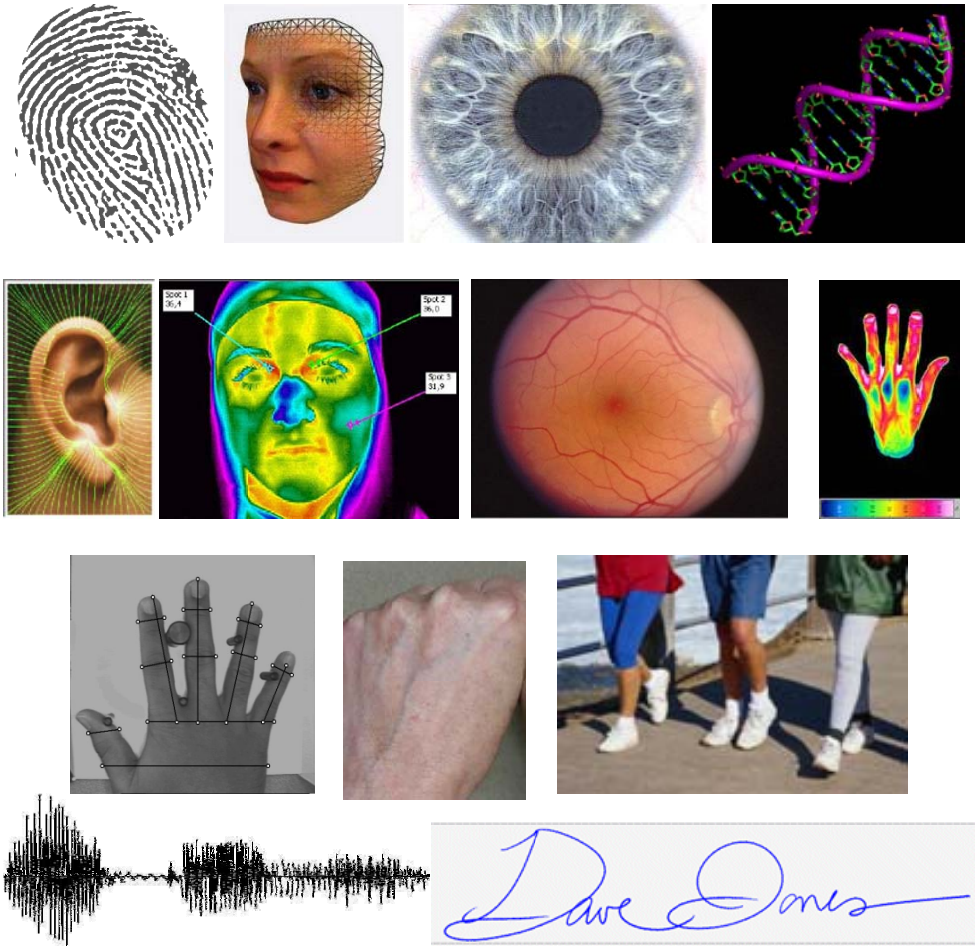
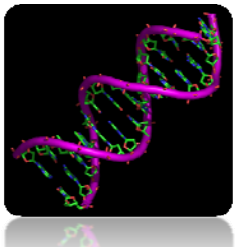


Figura 3 : Algunos rasgos biométricos utilizados en la actualidad: Huella dactilar, Cara, Iris, ADN, Oreja, Termograma de la cara, Retina, Termograma de la mano, Geometría de la mano, Venas de la mano, Forma de caminar, Voz y Firma; de iquierda a derecha y de arriba abajo.

Dentro de la totalidad de rasgos biométricos existentes distinguimos entre **rasgos fisiológicos** o morfológicos y **rasgos biométricos conductuales**. Los primeros son rasgos personales que pueden obtenerse incluso sin la cooperación del usuario, como el ADN, la huella dactilar, el iris, etc. Para obtener los segundos, sin embargo, necesitamos que el usuario realice un comportamiento determinado, y entre ellos se encuentran la firma, la voz, el modo de teclear, el modo de caminar, etc.

Ahora veamos algunos de estos rasgos, listados por orden alfabético, con mayor profundidad (1):

ADN



Único para cada individuo – excepto para los gemelos monocigóticos –, el ADN es utilizado en la actualidad para el reconocimiento de personas principalmente en aplicaciones forenses. Sin embargo, la posible contaminación de la muestra, su sensibilidad – es fácil "robar" una porción de ADN -, así como la imposibilidad de utilizarlo como método de reconocimiento *on-line* no invasivo – son necesarios métodos químicos y un experto en la materia, además de la colaboración del usuario -, le impiden ser una técnica apropiada para su utilización en sistemas de reconocimiento biométrico automático. Por otro lado, el ADN como método de reconocimiento presenta graves problemas de privacidad, ya que puede provocar la discriminación de personas al salir a la luz ciertos aspectos de su genética.

Dinámica del tecleo

Hipotéticamente, cada persona tiene una forma de teclear característica. Si bien este rasgo conductual no es único para cada individuo, sí ofrece suficiente información discriminatoria como para permitir la verificación de identidad. La dinámica de tecleo de una persona puede monitorizarse no invasivamente mientras la persona teclea.

Escáner de retina

La rica estructura vascular de la retina es una característica propia de cada individuo y de cada ojo. Éste es considerado el rasgo biométrico más seguro, pues no es fácil cambiar o duplicar la estructura vascular de la retina. La captura de la imagen requiere una considerable cooperación del sujeto y supone contacto con el sensor, lo que, unido a problemas de privacidad – la estructura vascular de la retina puede revelar ciertas condiciones de salud del individuo -, provoca que los sistemas biométricos basados en este rasgo carezcan de alta aceptación entre los usuarios.

Firma

El modo en que firma una persona es característico de cada individuo. Aunque firmar requiere contacto y un relativo esfuerzo por parte del usuario, es un proceso altamente aceptado en gran variedad de transacciones legales,

gubernamentales y comerciales como método de verificación. Sin embargo, la firma es un rasgo biométrico conductual que cambia a lo largo del tiempo y sufre la influencia de las condiciones físicas y emocionales del firmante. Es, por ello, un rasgo con alta intra-variabilidad (diferencias entre muestras generadas por un mismo individuo) - lo que le supone una desventaja como método de reconocimiento biométrico - y, además, los falsificadores profesionales son capaces de reproducir firmas que logran engañar al ojo inexperto.

Forma de caminar

No es éste un rasgo biométrico especialmente distintivo, pero sí lo suficientemente característico como para permitir la verificación en algunas aplicaciones de baja seguridad. Al ser un rasgo conductual puede no ser invariante, especialmente a largo plazo, por culpa de fluctuaciones importantes en el peso, o lesiones en las articulaciones o el cerebro.
La adquisición de este rasgo es similar a la adquisición de fotografías faciales, por lo que puede considerarse un rasgo biométrico aceptable. No obstante, debido a que los sistemas biométricos basados en este rasgo utilizan secuencias de vídeo de la persona caminando para medir los diferentes movimientos de cada punto de articulación, su carga computacional es más bien alta.

Geometría de la mano

Algunas características de la mano humana - por ejemplo, el largo de los dedos - son relativamente invariantes y características de cada individuo, aunque no demasiado distintivas. El sistema de adquisición de la imagen de la mano requiere cooperación del sujeto, aunque, por otro lado, los requisitos para su representación son pequeños, lo cual supone un atractivo para sistemas limitados en memoria y/o ancho de banda.

Debido a su limitada distintividad, los sistemas basados en geometría de la mano son utilizados típicamente en aplicaciones de verificación, pero no para identificación. Los conceptos de verificación e identificación se definen en la sección 2.4.1.

Huella dactilar

La huella dactilar en un ser humano se forma a partir del séptimo mes fetal, es invariable hasta la descomposición *post-mortem* – salvo por accidentes - y tiene capacidad regenerativa. Las huellas dactilares constituyen un rasgo biométrico altamente identificativo, pues son totalmente propias de cada individuo y cada dedo: no existen dos huellas dactilares exactamente iguales. Además, la huella cobra especial importancia como rasgo biométrico porque puede adquirirse en forma de huella latente en la escena de un crimen.

Ya que éste será el rasgo biométrico con el que se trabaje en el presente proyecto, en el capítulo 3 de la memoria se presenta un estudio más profundo y detallado de la huella dactilar como método identificativo.

Iris

La textura visual del iris humano se determina durante el desarrollo embrionario y, según se propone en (2), es única para cada individuo y para cada ojo. Típicamente, una imagen de iris se captura mediante un proceso con ausencia de contacto, aunque sí es necesaria la cooperación del usuario, tanto para que la imagen del iris se registre en la zona deseada, como para asegurar que el iris está a una distancia determinada del plano focal de la cámara. Se considera que la tecnología de reconocimiento de iris es sumamente precisa y rápida.

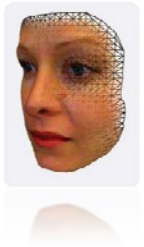
Olor

El olor emanado por el cuerpo de un ser humano es distintivo de cada individuo. En un sistema biométrico basado en este rasgo, el olor del aire que rodea al individuo es captado por una serie de sensores químicos, cada uno de ellos sensible a cierto grupo de componentes (aromáticos). No está claro si la utilización de desodorantes o la composición química del entorno pueden afectar a la capacidad de distintiva de estos sistemas.

Oreja

Se sabe que la forma de la oreja y la estructura del tejido cartilaginoso de la aurícula son distintivos de cada individuo. El reconocimiento de oreja se centra en la comparación de la distancia existente entre puntos salientes de la aurícula y un punto determinado de la oreja.

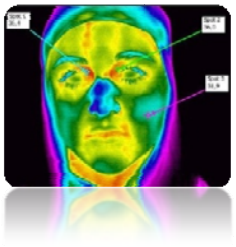
Rostro



La cara es uno de los rasgos biométricos más aceptados por tratarse del método más comúnmente empleado por el ser humano para el reconocimiento visual de sus semejantes. Además, el método empleado en la adquisición de imágenes de la cara es un método no intrusivo, lo que le permite ser una técnica con buena aceptación entre los usuarios.

El reto para este tipo de aplicaciones es lograr desarrollar técnicas de reconocimiento capaces de tolerar cambios por los efectos de la edad, las expresiones faciales, ligeras variaciones en las condiciones de iluminación del entorno y variaciones en la posición de la cara con respecto a la cámara (rotaciones 2D y 3D).

Termogramas



El patrón de calor radiado por el cuerpo humano es una característica propia de cada individuo y es posible capturarlo no intrusivamente mediante una cámara infrarroja de un modo similar

a como se toma una fotografía normal (espectro visible). Este tipo de tecnología puede utilizarse para el reconocimiento biométrico encubierto y, además, permite distinguir entre gemelos idénticos.

Una tecnología similar que usa imágenes cercanas a las de infrarrojos se usa para escanear el dorso del puño cerrado para así determinar la estructura de venas de la mano.

La ventaja del termograma frente a otras técnicas de reconocimiento, como ya hemos dicho, es que esta técnica no requiere ningún contacto con el individuo y no resulta invasiva. Como desventaja cabría destacar que es una técnica sensible a entornos no controlados, aquellos en los que las superficies emisoras de calor cercanas al cuerpo afecten drásticamente a la fase de adquisición de imagen. Además, los sensores de infrarrojos son prohibitivamente caros, factor que afecta considerablemente a la expansión de los termogramas como técnica de reconocimiento biométrico comercial.

Voz

La distintividad de la voz es una característica ampliamente reconocida socialmente. Además, su captura se realiza mediante un proceso no invasivo, lo que la convierte en un rasgo biométrico bien aceptado. La voz puede ser el único rasgo biométrico viable en aplicaciones que requieren el reconocimiento de personas al teléfono. No se considera, sin embargo, que sea lo suficientemente distintiva como para permitir la identificación de un individuo en una gran base de datos de identidades. Por otro lado, la señal de voz que está disponible para su reconocimiento ha sufrido degradación de calidad por el micrófono, el canal de comunicación y la digitalización. La voz se ve afectada, además, por la salud de la persona – por ejemplo, si tiene un catarro -, el estrés, las emociones, etc.

2.4. Sistemas de reconocimiento biométrico

La necesidad de técnicas de autenticación de usuario automáticas, fiables y seguras es una realidad patente en el mundo global en el que vivimos. Para atender esta necesidad aparecen los sistemas automáticos de reconocimiento biométrico, que utilizan alguno de los rasgos descritos en la sección anterior para la identificación del individuo. Es deseable que estos sistemas presenten:

- Alto **rendimiento**: precisión en el proceso de identificación.
- Alta **aceptabilidad**: grado de aceptación personal y social del sistema biométrico.
- Alta **evitabilidad**: capacidad de eludir ser puenteado mediante procedimientos fraudulentos.

En la Figura 4 se muestra la estructura general de funcionamiento de un sistema de reconocimiento biométrico.

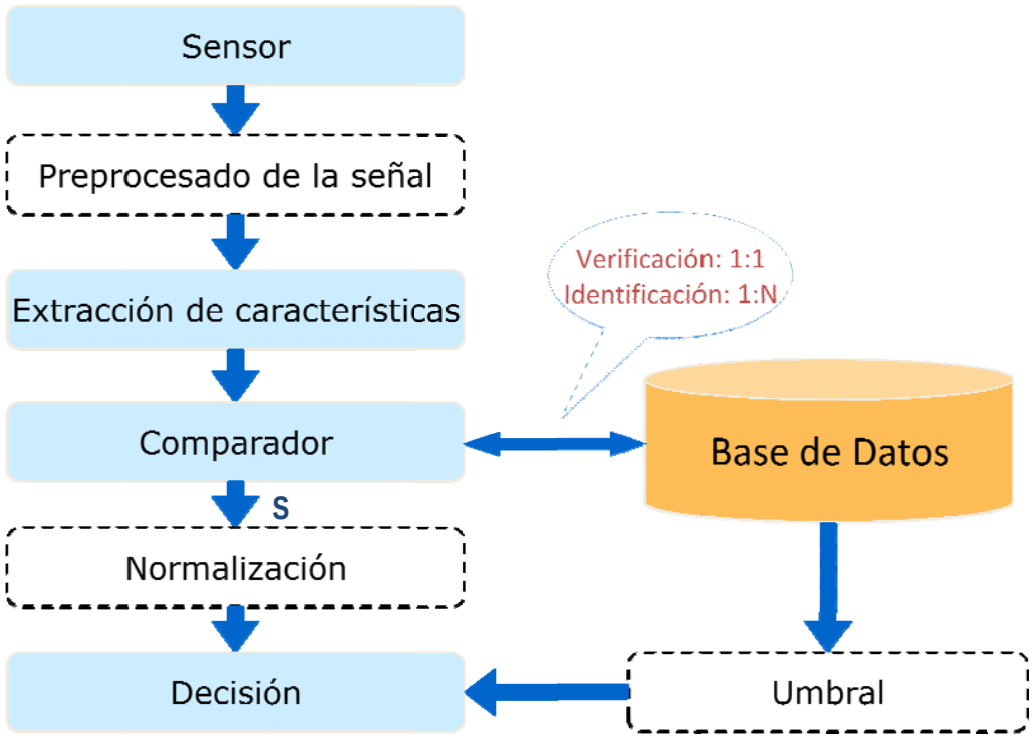


Figura 4: Funcionamiento general de un sistema de reconocimiento biométrico.

Como se observa en el esquema, el rasgo biométrico es capturado por el sensor y, tras procesar la señal, son extraídas sus características. Este patrón de características es comparado con el que está almacenado en la base de datos y que recibe el nombre de "plantilla" o *template* de usuario. El sistema toma entonces la decisión de aceptar nuestro patrón de características de entrada como válido o no, en función del valor devuelto por el comparador – que puede haber sido normalizado – y un umbral de decisión que se ha fijado previamente.

2.4.1. Modos de funcionamiento

Desde el punto de vista de su funcionamiento, podemos clasificar las dos perspectivas fundamentales de trabajo de los sistemas biométricos en dos modos (3):

- **Modo verificación**: comparación 1 a 1.
- **Modo identificación**: comparación 1 a N.

Cuando en la memoria se emplea el término "reconocimiento", se hace con la intención de no distinguir entre verificación e identificación, es decir, se utiliza para hacer referencia a ambos.

Además de los modos de identificación y verificación se puede hablar también del **modo registro**, en el cual los usuarios son dados de alta en la base de datos del sistema, quedando almacenados sus datos como plantillas de usuario.

En la Figura 5 se muestra un esquema de cada uno de los modos de funcionamiento de un sistema biométrico.

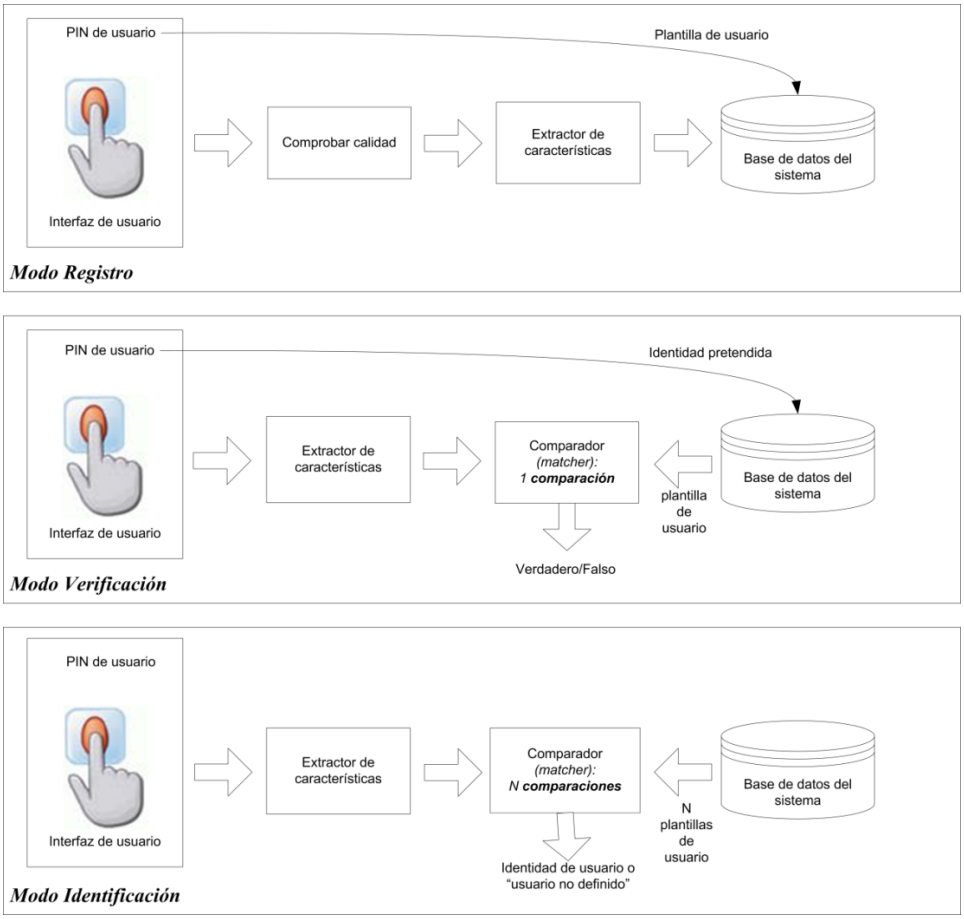


Figura 5: Modos de funcionamiento de un sistema automático de reconocimiento biométrico. Figura adaptada de (3).

A continuación, se describen los dos primeros modos de funcionamiento – verificación e identificación - con mayor detalle:

Modo verificación

En este modo de funcionamiento el sistema recibe dos entradas:

- Una realización del rasgo biométrico a verificar.
- Una identidad: que puede recibir a través de la lectura de una tarjeta magnética individual, la introducción mediante teclado o voz de un código, etc.

Así, las dos únicas salidas o decisiones del sistema son la aceptación o el rechazo del individuo como aquel que pretende ser, quedando el solicitante catalogado como usuario auténtico o como impostor, respectivamente.

La decisión de aceptar o rechazar el rasgo de entrada como correspondiente a la identidad solicitada dependerá de si el valor de parecido o verosimilitud obtenida supera o no un determinado umbral de decisión.

En el presente proyecto trabajaremos siempre en modo verificación.

Modo identificación

El objetivo de este modo de funcionamiento es el de clasificar una realización determinada de un rasgo biométrico de identidad desconocida como perteneciente a uno de entre un conjunto de N posibles individuos. Dentro de este sistema podemos diferenciar dos posibles casos:

- **Identificación en conjunto cerrado**: el resultado del proceso es una asignación de identidad a uno de los individuos modelados por el sistema, conocidos como usuarios. Existen, por tanto, N decisiones de salida posibles.
- **Identificación en conjunto abierto**: aquí debe considerarse una posibilidad adicional a las N del caso anterior: que el individuo que pretende ser identificado no pertenezca al grupo de usuarios, con lo que el sistema de identificación debe considerar la posibilidad de no clasificar la realización de entrada como perteneciente a las N posibles. Tenemos, entonces, (N+1) salidas posibles.

El proceso de identificación de conjunto abierto puede ser observado como un esquema en dos etapas: en la primera se realiza un proceso de identificación en conjunto cerrado – N decisiones o salidas posibles – y, a continuación, se realiza un proceso de verificación respecto al individuo seleccionado en el proceso de identificación. Así, la salida del sistema será la aceptación o el rechazo del individuo, lo que da lugar a un total de (N+1) decisiones posibles.

2.4.2. Rendimiento de los sistemas biométricos

Como se puede observar en la Figura 4, el módulo comparador del sistema biométrico devuelve una puntuación o *score* en el proceso de reconocimiento del rasgo biométrico de entrada. Dicha puntuación será función del parecido entre dicha muestra de entrada y la muestra del usuario que dice ser - la muestra perteneciente a la base de datos con la que la estamos comparando. En el caso concreto de los sistemas basados en reconocimiento de huella dactilar con los que trabajaremos en este proyecto, esta puntuación será mayor cuanto mayor sea el parecido entre las dos huellas.

El sistema dispone de un llamado umbral de decisión, superado el cual, el sistema considerará que las muestras de entrada y de la base de datos son iguales o, más bien, lo suficientemente parecidas. Es por ello que el sistema puede equivocarse: puede que considere que dos muestras corresponden al mismo usuario cuando no es así – falsa aceptación – o, por el contrario, puede considerar que dos muestras no pertenecen al mismo usuario, cuando en realidad sí pertenecen – falso rechazo.

Así, a la hora de caracterizar un sistema biométrico será imprescindible conocer la **tasa de falsa aceptación** o **FAR** (*False Acceptance Rate*), que es la probabilidad de que un impostor sea aceptado en el sistema; y la **tasa de falso rechazo** o **FRR** (*False Rejection Rate*), que es la probabilidad de que un usuario registrado no sea aceptado en el sistema.

En la Figura 6 se han representado densidades de probabilidad de las puntuaciones de impostores y puntuaciones de usuarios válidos de un sistema imaginario (izquierda). Fijado 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. Por ello, tanto la FAR como la FRR variarán según lo haga el umbral de decisión del sistema (derecha).

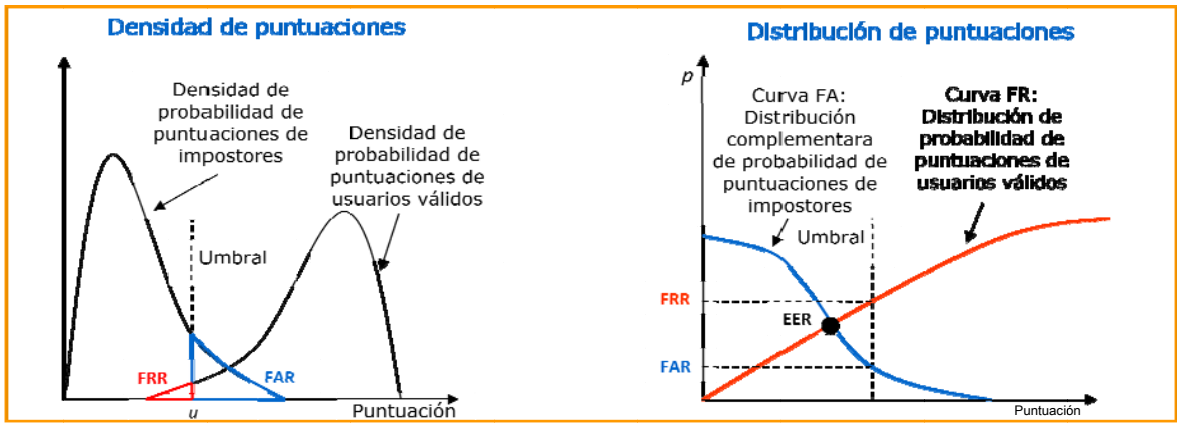


Figura 6: Densidad de probabilidad de puntuaciones de usuarios e impostores (izquierda), y curvas FA y FR (derecha).

El punto en el que la FAR y la FRR son iguales se denomina *Equal Error Rate* (*EER*) y es empleado a menudo para comparar el rendimiento de diferentes sistemas a través de una sola medida de rendimiento.

Otro método que resulta útil para describir el rendimiento de un sistema biométrico es la representación de las curvas ROC (*Reciever Operating Curve*). Este tipo de gráficas se genera representando la FAR frente a (1 - FRR) en función de diferentes valores del umbral, aunque, en ocasiones, se representa bajo el mismo nombre de curva ROC la FAR frente a la FRR.

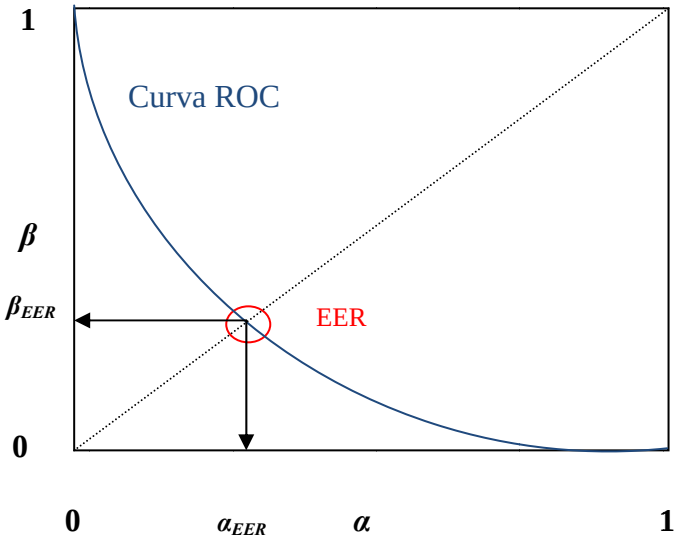


Figura 7: Curva ROC y EER.

Una alternativa comúnmente utilizada frente a las curvas ROC, son las curvas DET (*Detection Error Tradeoff*), cuya única diferencia respecto a las ROC es un cambio de escala en los ejes, que pasan a ser logarítmicos, con lo que las curvas ROC tienden a convertirse en rectas y así es más fácil la comparación de distintos sistemas: un sistema será mejor cuanto más cerca del origen de coordenadas se encuentre su curva DET.

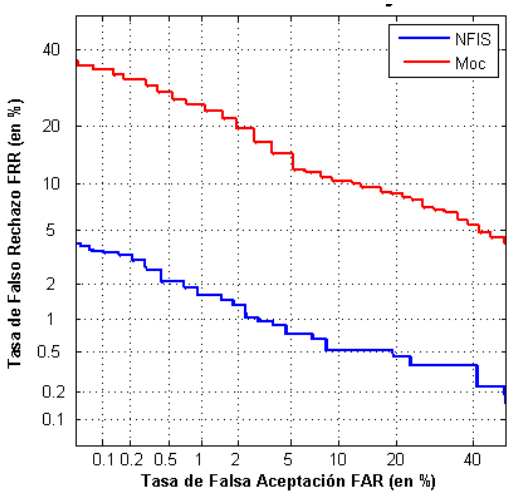
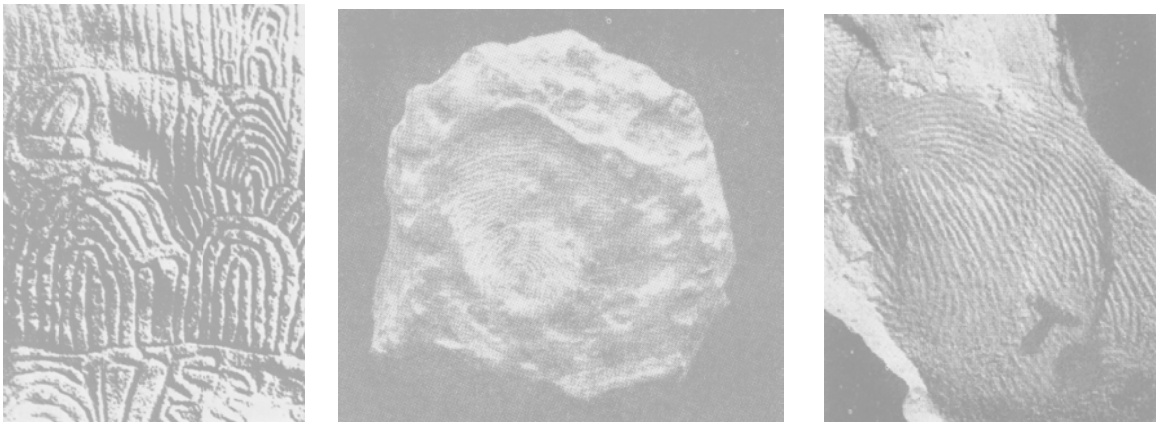


Figura 8: Ejemplo de curvas DET de dos sistemas de reconocimiento biométrico.

3. Reconocimiento de huella dactilar

3.1. Introducción

Dentro del abanico de rasgos biométricos existentes – expuestos en la sección 2.3 de la memoria -, la huella dactilar es uno de los más utilizados en la actualidad. Por un lado, precisamente por la importancia que este rasgo ha tenido tradicionalmente, pues ya algunos hallazgos arqueológicos sugieren que en la antigüedad las personas eran conscientes de la singularidad de la huella dactilar (1), como se puede ver en la Figura 9; y, por otro lado, porque, en las últimas décadas, la investigación y el uso activo de la huella dactilar como rasgo identificativo, su indexado y la mejora de su procesamiento, han contribuido a un mayor conocimiento y comprensión de la información distintiva contenida en la huella.



a **b** **c**

Figura 9 : Ejemplos de impresiones arqueológicas de huellas (4). a) Una escultura neolítica, b) Un sello chino de arcilla y c) Una impresión en una lámpara palestina.

La huella dactilar se aceptó formalmente como método de identificación personal a principios del siglo XX y es utilizada actualmente por agencias gubernamentales y en grandes y pequeñas bases de datos (DNI, criminales,…). A partir de los años 60 del siglo pasado comenzaron a aparecer los primeros sistemas de reconocimiento de huella dactilar automáticos. A lo largo de los años, el FBI ha acumulado más de 40 millones de tarjetas de huellas en archivos y recibe miles de peticiones diarias de identificación (5). Por otro lado, el rápido crecimiento sufrido por las aplicaciones comerciales civiles, gracias a su exactitud, tamaño, coste, funcionamiento y probada eficacia, así como el gran aumento de publicaciones científicas al respecto en los últimos treinta años, no ha hecho sino potenciar su importancia como método de reconocimiento (1).

Figura 10: Sistemas de reconocimiento biométrico basados en huella dactilar integrados en diferentes aparatos.

A día de hoy, la huella dactilar sigue acaparando la mayoría del mercado frente al resto de rasgos biométricos utilizados para el reconocimiento personal. En la Figura 11 se muestra la división del mercado para los distintos rasgos biométricos en 2008:

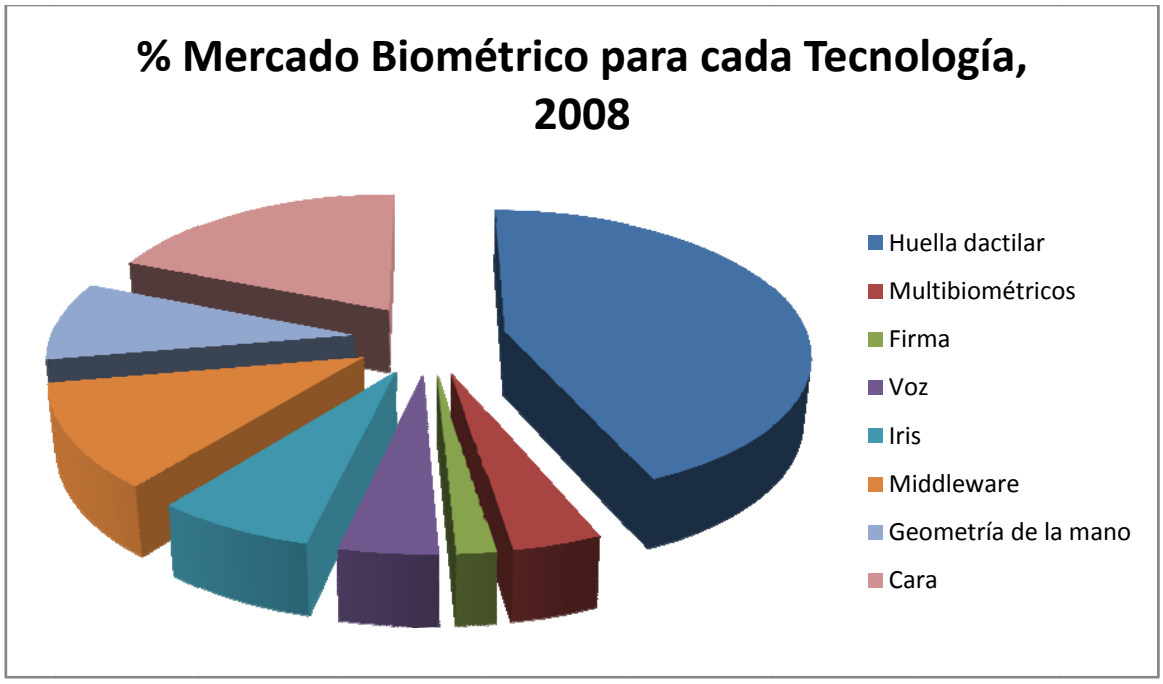


Figura 11: Porcentaje del mercado de biométricos actual correspondiente a cada tipo de tecnología (6).

3.2. Conceptos básicos sobre huellas dactilares

A la imagen formada por el relieve de las yemas del dedo se le denomina dactilograma. Éste está formado por una serie de crestas y valles característicos y únicos de cada individuo, y puede encontrarse en tres estados distintos.

- Natural: observado directamente en las huellas de los dedos.
- Latente: huella dactilar – impresión por contacto en una superficie.
- Artificial: reproducción gráfica del natural – impresión digital.

La observación de este dactilograma será esencial para la clasificación y el reconocimiento de huella dactilar.

Para empezar, en la huella se pueden observar dos tipos de puntos característicos a nivel global que nos permitirán su clasificación en varios tipos: núcleo y deltas.

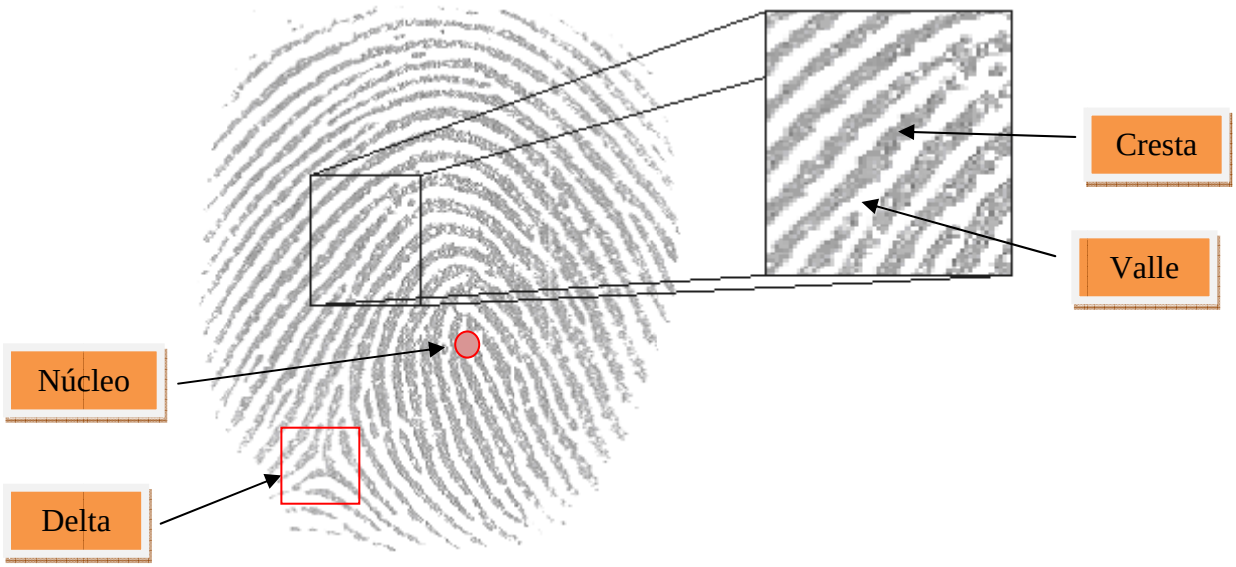


Figura 12: Núcleos, deltas, crestas y valles en una huella.

Así, en base a su núcleo y a sus deltas en (1) se definen las siguientes clases de huellas:

Figura 13 : Clases más comunes de huellas.

3.3. Adquisición de huellas dactilares

La adquisición de huellas dactilares se puede realizar de dos maneras: *off-line*, que consiste en la adquisición tradicional de la huella mojando el dedo en tinta, y *on-line*, método consistente en la captura de la huella mediante sensores que guardan una

imagen digitalizada de la huella. En este proyecto nos centraremos en el estudio de sistemas que trabajan con sensores de captura *on-line* de huella.

En la Figura 14 se muestran las capturas realizadas mediante tres tipos de sensores distintos, correspondientes a las tres principales tecnologías de adquisición de huella dactilar existentes en el mercado: óptico, térmico de desplazamiento y capacitivo.

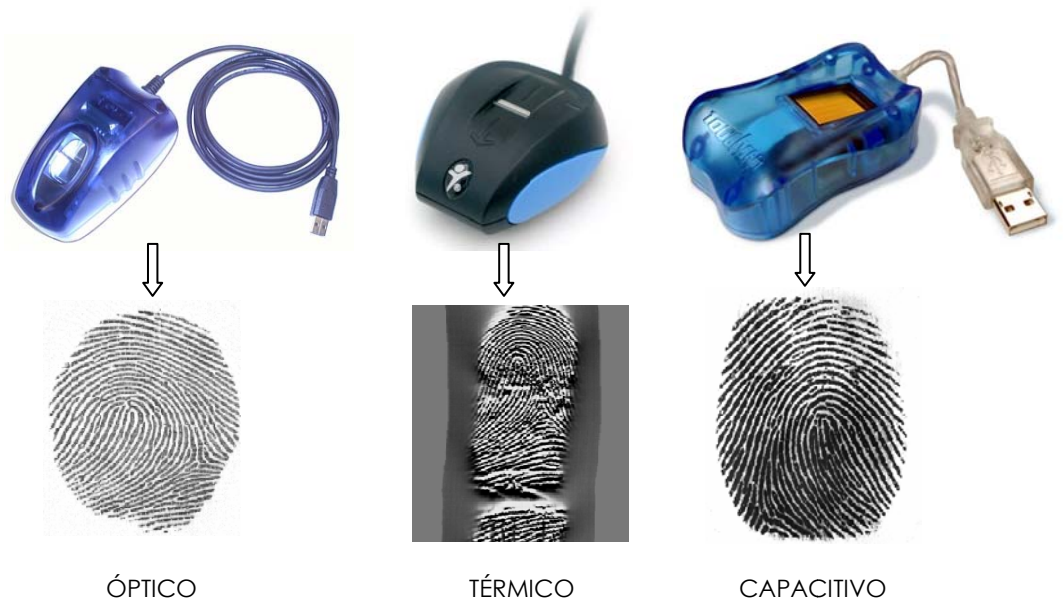
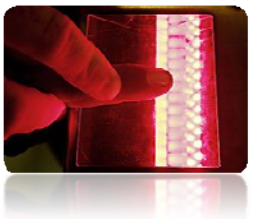


Figura 14: Sensores óptico (Fx2000 de Biometrika), térmico de desplazamiento (de Yubee) y capacitivo (TCRU1C de UPEK), y ejemplos de huellas capturadas con cada uno de ellos.

A continuación se describen los principales tipos de sensores *on-line* existentes en la actualidad: sensores ópticos, sensores de estado sólido y sensores de ultrasonidos.

3.3.1. Sensores ópticos

Reflexión



Éste es el escáner *on-line* más antiguo. Se sirve del efecto de refracción frustrada sobre un prisma de vidrio. El dedo es iluminado desde un lateral con un LED y, mientras que las crestas entran en contacto con la superficie – la luz se refleja, zonas claras -, los valles permanecen a cierta distancia – la luz es absorbida, zonas oscuras. Los rayos de luz salen por el otro lado del prisma y se transmite la imagen a través de una lente y hacia un sensor de imagen CCD o CMOS. Los sensores ópticos por reflexión se conocen también como FTIR (*Frustrated Total Internal Reflection*). Debido a que los dispositivos FTIR captan una superficie tridimensional, no son fácilmente engañados mediante la presentación de una imagen impresa de una huella. Sin embargo, aunque, en general, presentan una muy buena calidad de imagen y son capaces de captar grandes áreas, estos dispositivos no pueden miniaturizarse, pues la reducción de la longitud del camino óptico (distancia entre la superficie externa del prisma y el sensor de imagen) introduciría importantes distorsiones en la imagen capturada. Empresas como Compaq o Biometrika fabrican sensores de este tipo.

Basándose en el mismo principio de reflexión frustrada, Kinetic Sciences y Cecrop/Sannaedle han propuesto 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.

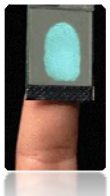
Reflexión sin contacto

Esta técnica, que no requiere contacto, consiste en tomar una fotografía de muy alta calidad de la huella y post-procesarla para corregir posibles distorsiones. TST elimina el prisma que se utilizaba en métodos anteriores, leyendo directamente la huella, sin que se requiera ningún tipo de contacto, aunque sí una guía para lograr la distancia óptica correcta. Thales (Thomson-CSF) también propone algo parecido, pero utiliza un polvo especial para poner en el dedo.

Transmisión

El dedo entra en contacto con una serie de fibras ópticas verticales y la luz residual transmitida por el dedo es leída directamente por un sensor CCD o CMOS que registra la imagen. Mitsubishi propone leer el dedo con una cámara normal. NEC y Delsy utilizan una cámara CMOS del tamaño del dedo, con una fibra óptica en medio, y la luz proviene de los bordes en este caso. Mitsumi y NEC proponen lo mismo pero con un sensor de desplazamiento.

Electro-ópticos



Algunos polímeros son capaces de emitir luz cuando son excitados con el voltaje adecuado, generalmente bastante alto. Este polímero está en contacto directo con una cámara CMOS, que tiene necesariamente el tamaño del dedo. Generalmente el dedo actúa como la tierra y el polímero emite luz donde las crestas hacen contacto. Ethentica y TesTech proponen diferentes soluciones para este tipo de sensor.

3.3.2. Sensores de estado sólido

Capacitivos

Tras la detección óptica, la medida de la capacitancia entre la piel y el píxel es el mayor efecto físico empleado para la adquisición de huellas. Así, este tipo de sensores consiste en una superficie compuesta por una serie bidimensional de placas de pequeños condensadores; la piel del dedo actúa como la segunda placa de los condensadores y, dependiendo de la distancia, la capacitancia será diferente, con lo que es posible distinguir con facilidad crestas y valles. La capa protectora debe ser lo más pequeña posible – pocos µm -, ya que hay que medir un campo eléctrico, y la distancia entre la piel y el píxel debe ser muy pequeña para proporcionar suficiente sensibilidad. Esto, unido al hecho de que sea un método vulnerable a campos eléctricos fuertes, supone su mayor desventaja. Empresas como Veridicom, Fujitsu, Sony o Upek han propuesto sensores de este tipo.

De presión

El material piezoeléctrico que se utiliza para este tipo de sensores ha existido durante años, aunque, desafortunadamente, su sensibilidad es muy baja. Además, cuando se añade una capa protectora, la imagen resultante queda borrosa porque el relieve de la huella se ha suavizado. Actualmente parece que estos problemas han sido resueltos y existen ya algunos dispositivos que utilizan métodos de presión para adquirir la imagen de huella. Según el material empleado se han propuesto distintas soluciones: membrana conductora sobre un chip de silicio CMOS, membrana conductora sobre una TFT y *switches* micro-electromecánicos sobre un chip de silicio. Compañías como Opsis, BMF, Fidelica y Alps Electric comercializan sensores de esta clase.

Térmicos

Este tipo de sensor está fabricado con material piro-eléctrico, el cual es capaz de convertir cambios de temperatura en un voltaje específico. Esta clase de sensor no mide la diferencia de temperatura entre la piel en las crestas y los valles, ya que ésta es muy pequeña. En realidad, ya que el dedo se coloca directamente sobre el material, lo que mide es la temperatura de las crestas, que son las que están en contacto; los valles, sin embargo, no hacen contacto con el material y por ello la temperatura de éste permanece invariable en esos puntos. La gran desventaja que presentan estos sensores es que la imagen desaparece rápidamente: cuando se coloca el dedo sobre el sensor, se produce un cambio muy grande de temperatura y por lo tanto de la señal, pero, tras un corto periodo de tiempo – menos de una décima de segundo -, el dedo y el chip alcanzan un equilibrio térmico y, como no hay cambio en la temperatura, no hay señal y, por tanto, la imagen desaparece. Este efecto desaparece en los sensores térmicos de desplazamiento, pues el barrido del dedo logra que se mantenga la variación de temperatura. Atmel comercializa sensores térmicos.

Campo eléctrico

Esta clase de sensores tiene incorporada un anillo que genera una señal eléctrica sinusoidal y una matriz de antenas activas recibe la señal modulada por la superficie del dedo. El dedo debe estar en contacto con el anillo y el sensor para su correcto funcionamiento. La señal recibida es amplificada, integrada y digitalizada para formar la imagen. Authnec y Fingerprints Cards proponen sensores basados en esta tecnología.

3.3.3. Sensores de ultrasonidos

La lectura de huellas mediante ultrasonidos no es muy común. El funcionamiento de estos sensores es parecido al de un ecógrafo: envían señales acústicas a la superficie del dedo y captan la señal de eco recibida. Esta señal de eco permite reconstruir la forma de la huella y la estructura de crestas y valles. La detección por ultrasonidos requiere dispositivos muy grandes con partes mecánicas, son complejos y muy caros. Además, tarda algunos segundos en captar la imagen, con lo que la adquisición resulta relativamente lenta. Su principal ventaja es que "lee" la dermis (capa inferior de la piel), en lugar de la epidermis (capa superior), con lo que es inmune a la suciedad o, incluso, a materiales que se interpongan entre el dedo y el sensor como guantes finos. Optel y Ultrascan proponen sus propios modelos de sensores de ultrasonidos.

3.4. Reconocimiento automático de huellas basado en minucias

Además de núcleo y delta, en una huella se pueden apreciar a nivel local una serie de puntos característicos o singularidades en las crestas de la huella.

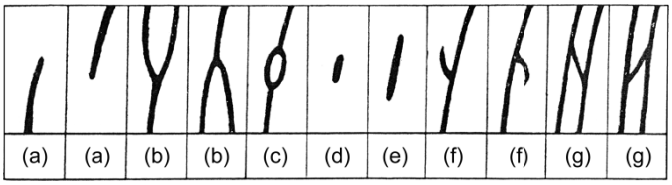


Figura 15: Algunos tipos de puntos característicos en una huella dactilar. a) Abrupta; b) Bifurcación; c) Círculo; d) Punto; e) Fragmento; f) Gancho; g) Empeine.

En teoría, existen multitud de tipos de estas singularidades; sin embargo, en la práctica, los sistemas automáticos suelen considerar exclusivamente dos: terminación y bifurcación de cresta.

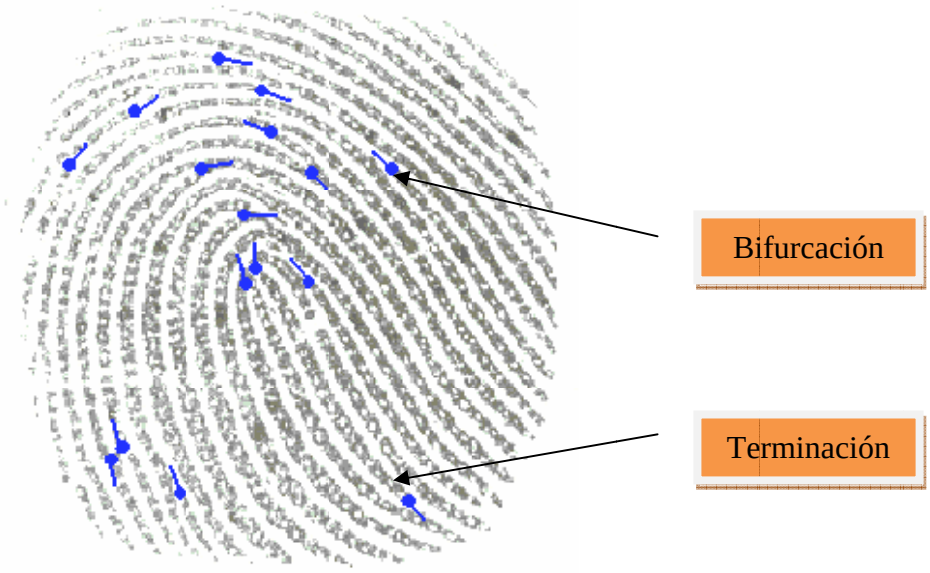


Figura 16: Minucias en una huella dactilar.

Una coincidencia en un número suficiente de puntos característicos - tipo, ubicación, tamaño y orientación - entre dos huellas implica que ambas pertenecen inequívocamente a la misma persona. El sistema judicial español fija este número en 12.

Las marcas azules que se observan en la Figura 16 y que corresponden a los puntos singulares de la huella – bifurcación o terminación -, es lo que denominamos minucias.

Las minucias se suelen caracterizar al menos por sus coordenadas e , y por el ángulo θ que forma la recta tangente a la cresta con el eje horizontal.

Como se observaba en la Figura 4, el proceso de reconocimiento biométrico consta básicamente de los módulos de adquisición del rasgo biométrico, extracción de características y comparación. El proceso de adquisición de huella dactilar se ha detallado previamente en la sección 3.3. Así, a continuación, se profundizará en el

funcionamiento de los módulos de extracción de características y comparación en un sistema de reconocimiento biométrico de huella basado en minucias.

3.4.1. Extracción de minucias

En la Figura 17 se muestra un esquema del módulo extractor de características típico de un sistema de reconocimiento de huella dactilar basado en minucias. Cada una de las etapas del proceso de extracción de minucias está marcada de la 'A' a la 'E' en dicha figura.

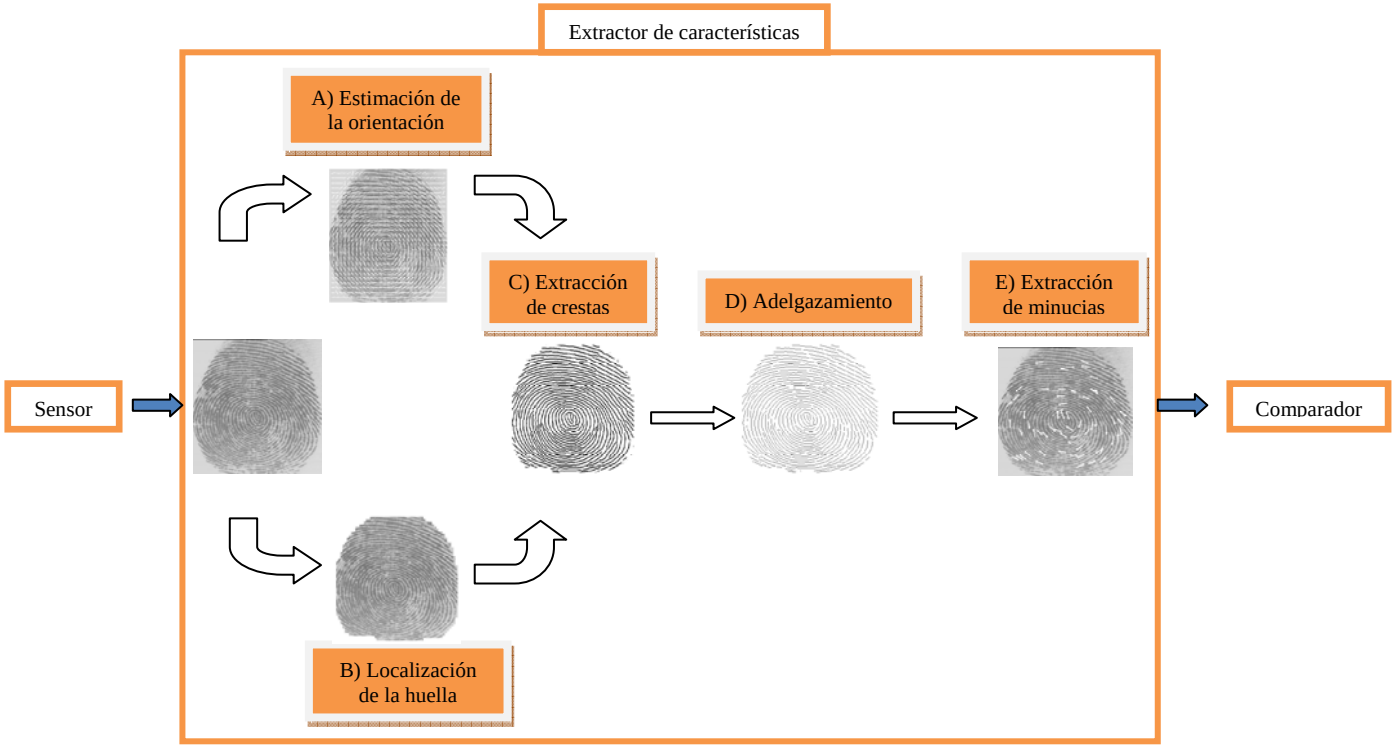


Figura 17: Proceso general de extracción de minucias de una huella dactilar.

A. Estimación de la orientación y detección de singularidades

El campo o imagen de orientación de una huella dactilar representa la naturaleza intrínseca de dicha huella y define 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 (3).

La imagen de orientación es una matriz cuyos elementos codifican la orientación local de las crestas de la huella. Cada elemento θ_{ij} - correspondiente al punto [i,j] de una cuadrícula localizado en el píxel $[x_i,y_j]$ - denota la orientación media de las crestas en los alrededores del píxel $[x_i,y_j]$.

El campo de orientación local viene determinado, entonces, por la dirección fundamental de las crestas de la huella, esto es, el ángulo de dichas crestas con la

horizontal. La estimación de la orientación local se hace preferiblemente en bloques, en lugar de hacerlo en cada píxel, pues así se consigue reducir la carga computacional del algoritmo (1).

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, ya que estamos considerando el entorno.

Una vez obtenido el campo o imagen de orientación, éste es utilizado para la detección de singularidades a nivel global: núcleos y deltas.

La detección de singularidades en huellas ruidosas o de baja calidad es complicada y puede llevar a la detección de falsas singularidades. 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 la huella: Segmentación

Para localizar la región de interés en nuestra imagen de entrada es necesario proceder a la segmentación de dicha imagen, es decir, debemos separar la huella del fondo de la imagen.

En la imagen de una huella sabemos que, en la región de interés – la zona de crestas y valles -, existen grandes variaciones del nivel de gris en la dirección perpendicular a las crestas, mientras que en el resto hay variaciones de gris en todas direcciones, sin el predominio de ninguna de ellas.

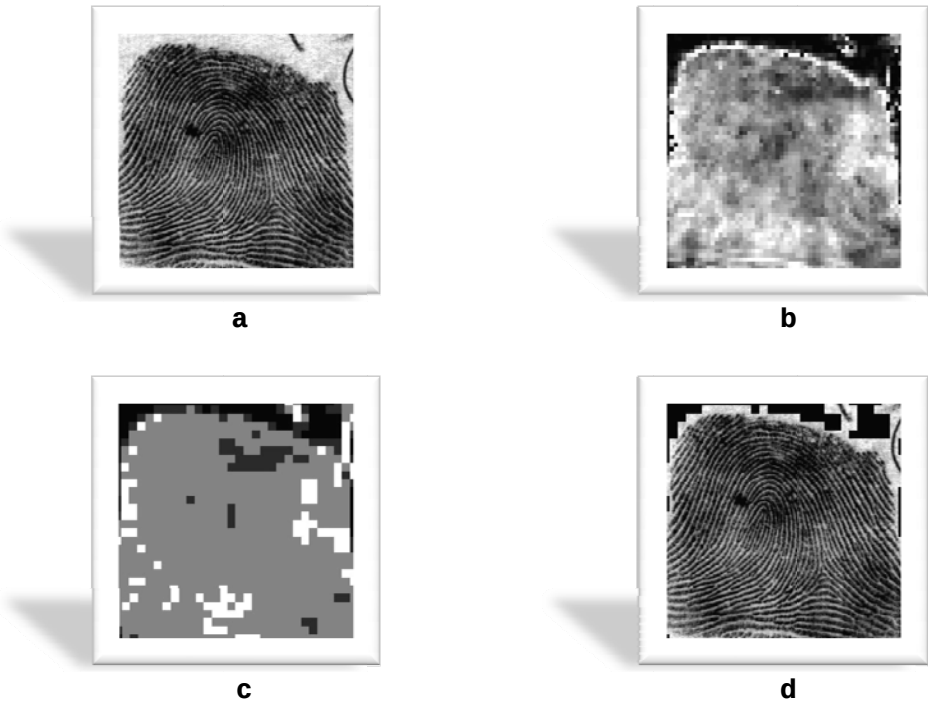


Figura 18: Segmentación de una imagen de huella propuesta en (7): a) Imagen original; b) Campo de variación; c) Imagen de calidad derivada del campo de variación: un valor de calidad "bueno", "medio", "bajo" o "fondo" es asignado a cada bloque, de acuerdo a su varianza; d) Imagen segmentada.

C. Extracción de crestas: Mejora y Binarización.

La mejora de las imágenes obtenidas mediante el sensor tiene como finalidad aumentar la claridad de la estructura de crestas y valles para facilitar la extracción de crestas primero y de minucias más adelante, y descartar zonas demasiado ruidosas o de baja calidad.

Existen varios tipos de degradación asociada con las imágenes de huella: crestas que no son estrictamente continuas, es decir, que contienen pequeños saltos; crestas paralelas que no están bien separadas debido a la presencia de ruido; y cortes, arrugas o quemaduras. Estas degradaciones provocan que la extracción de crestas sea extremadamente difícil 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 (posición y orientación) de minucias. Por todas estas razones, es necesario aplicar algoritmos de mejora para aumentar la claridad de la estructura de crestas.

Las técnicas clásicas de aumento de contraste o claridad que se emplean en imágenes genéricas no logran resultados satisfactorios en imágenes de huellas dactilares. Por ello, la técnica más usada para la mejora de la imagen de huella está basada en filtros contextuales, los cuales varían sus características en función de la zona que estén filtrando. Los filtros que se emplean tienen una estructura sinusoidal con diferentes frecuencias y orientaciones. Una clase de filtros muy extendida en el ámbito de la mejora de las huellas dactilares son los filtros de Gabor - ver Figura 19.

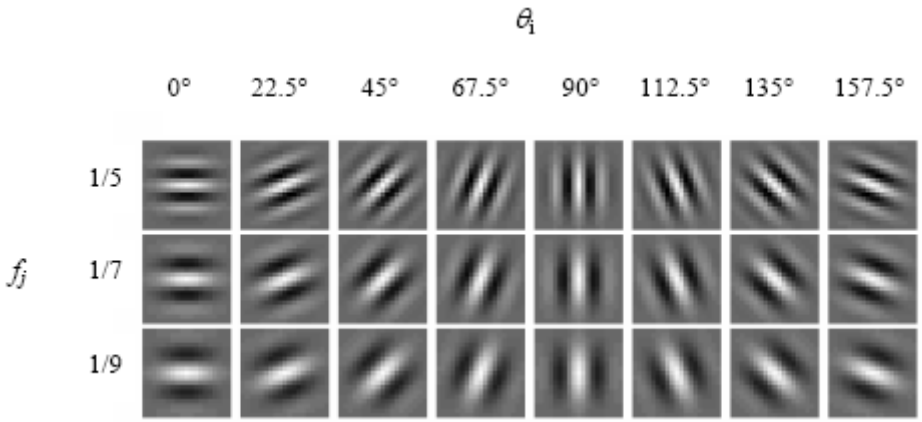


Figura 19. Representación gráfica de 24 filtros de Gabor. Imagen extraída de (8).

Una vez mejorada la imagen, se puede binarizar, es decir convertir sus píxeles en blancos o negros puros exclusivamente, estableciendo un umbral para ello. De hecho, muchos de los algoritmos empleados en la actualidad para la mejora de las imágenes producen como salida la imagen ya binarizada, como el que se propone en (4).

Figura 20: Ejemplo de huella antes (izquierda) y después (derecha) de la binarización. Imágenes extraídas de (4).

Algunos autores proponen no realizar la binarización, ya que es un proceso lento y complejo que puede provocar la pérdida de información importante. Téngase en cuenta, pues, que, si la imagen de la huella no es de suficiente calidad, la binarización puede empeorar los resultados del sistema.

D. Adelgazamiento

La imagen binarizada obtenida en el paso anterior entra ahora en un proceso de adelgazamiento, es decir, se reduce la anchura de la crestas al tamaño de un píxel. Con este paso logramos eliminar ciertas imperfecciones. En la Figura 21 se muestra la imagen de huella antes y después del proceso de adelgazamiento.

Figura 21 : Mapa de crestas (izquierda) y mapa de crestas adelgazadas (derecha). Imágenes extraídas de (4).

E. Extracción de minucias

Aunque, como ya hemos comentado, algunos autores han propuesto métodos de extracción de minucias que trabajan directamente con la imagen de escala de grises sin binarizar ni adelgazar, como en (9), la mayoría de métodos conocidos requieren estos dos procesos previos.

A partir de la imagen binarizada y adelgazada es fácil detectar las minucias existentes: si un píxel negro tiene sólo un píxel negro alrededor, es una terminación; si tiene tres píxeles negros alrededor, entonces será una bifurcación. En (10) se caracteriza cada píxel correspondiente a una minucia mediante un número 'cn' distinto de 2. Este número es definido como la mitad de la suma de las diferencias entre pares de píxeles adyacentes en una región de 8 píxeles vecinos. Así, un punto intermedio de una cresta tendrá un cn=2. Si el píxel corresponde a una terminación tendrá un cn=1, mientras que $cn \geq 3$ define un tipo de minucia más complejo - bifurcación, cruce, etc.

Tras esta primera detección de minucias, suele existir una etapa de post-procesado que incluye eliminar las minucias de los bordes y agrupar – o, incluso, eliminar – en una sola minucia varias de ellas cuando hay muchas juntas. También es posible que se eliminen minucias que se hayan localizado en zonas de baja calidad.

3.4.2. Comparación de patrones de minucias

Una vez extraídas las minucias de la huella es posible crear un patrón de minucias. 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 de comparación. La mayoría de algoritmos de comparación presentan, no obstante, una etapa de alineamiento previa a la de comparación.

A. Alineamiento

Aunque existen múltiples posibilidades, la más común consiste en elegir un par de minucias – una de cada huella -, aquéllas cuyas crestas asociadas sean más parecidas, y se estima entonces traslación, rotación y distorsión. A las minucias en función de las cuales se realiza el alineamiento se las conoce como minucias de referencia.

B. Comparación

En la bibliografía se pueden encontrar multitud de algoritmos con los que calcular la medida de similitud. Uno de los más utilizados consiste en pasar las minucias a coordenadas polares, tomando como origen la minucia de referencia. A continuación, se ordenan las minucias en orden creciente de ángulo y distancia, obteniendo así cadenas que se van comparando, y se calcula entonces el número de minucias coincidentes M_{PQ} - para cada par de puntos de las cadenas se define un entorno capaz de indicar si dos minucias forman pareja o no. Por último se calcula una medida global de similitud:

$$S = \frac{100 x M_{PQ} M_{PQ}}{MxN},$$

donde M y N son el número de minucias de cada huella a comparar. S tendrá un valor de 100 si todas las minucias son coincidentes y de 0, si no existe ninguna coincidencia.

3.5. Otros métodos de reconocimiento de huellas

Si bien este proyecto se basa en el reconocimiento de huella dactilar basado en minucias, existen otros métodos de reconocimiento de huella que comentaremos sin entrar en detalle: reconocimiento basado en texturas y reconocimiento basado en correlación. Ambos métodos se utilizan menos habitualmente que el reconocimiento por minucias, que presenta un mejor rendimiento – menor tasa de error –, aunque peor funcionamiento en condiciones de baja calidad y mayor carga computacional. En muchas ocasiones estos algoritmos se utilizan como medida complementaria a la proporcionada por un comparador basado en minucias.

3.5.1. Reconocimiento basado en texturas

Este método se sirve del patrón de campo de orientación – cómo se comportan las crestas -, sabiendo que en un patrón de crestas y valles existe una estructura orientada con frecuencia espacial y orientación localmente constantes. Se emplean filtros de Gabor con diferente orientación. Este método de reconocimiento tiene la ventaja frente al método de minucias de ser más robusto en presencia de ruido o al trabajar con huellas de baja calidad. Además, el vector de características es constante – en el método de minucias depende del número de minucias – y la carga computacional es menor, ya que no es necesario binarizar ni adelgazar. Como característica negativa cabe mencionar que tiene una menor capacidad discriminativa, es decir, mayor tasa de error.

3.5.2. Reconocimiento basado en correlación

Los métodos de reconocimiento basados en correlación consisten en establecer la correlación directamente entre imágenes de escala de grises. Se seleccionan una serie de regiones locales y la correlación se calcula sólo en esas regiones.

La imagen de escala de grises contiene toda la información original de la huella, al contrario de lo que sucede en el método de minucias, en el cual sólo se conservan un número finito de características. Por otro lado, ya que la correlación se hace localmente, existe cierta robustez frente a las deformaciones no lineales.

4. Ataques a sistemas de reconocimiento biométrico

En el marco de creciente implantación de los sistemas de reconocimiento automático de personas, cobra una especial importancia la evaluación de su seguridad y robustez frente a ataques externos. Las consecuencias de un sistema de reconocimiento inseguro pueden llegar a ser muy graves, ya que puede suponer la pérdida, robo o modificación de información confidencial. Además, la necesidad de identificación del usuario de un modo fiable no está sólo limitada al acceso a ordenadores y redes, sino que muchas actividades de la vida cotidiana requieren la identificación personal positiva: identificación del cliente en el punto de venta, acceso físico a edificios, puntos de entrada/salida restringidos, control de puesta en marcha de vehículos, etc.; lo que no hace sino reforzar la necesidad de estudiar y evaluar las fortalezas y debilidades de este tipo de sistemas (11).

Se ha hablado extensamente de las virtudes de los sistemas biométricos frente a los sistemas tradicionales de reconocimiento, basados en la posesión de un objeto o un conocimiento. Si bien las ventajas de los primeros frente a estos últimos son numerosas, no hay que olvidar que también los sistemas de reconocimiento biométrico presentan vulnerabilidades. Entre otras cosas, se asume que los rasgos biométricos no pueden ser robados, si bien esto no es del todo cierto: por ejemplo, cada día las personas dejamos nuestras huellas en las superficies que tocamos. El mayor problema de que esto ocurra es que, una vez que nuestros datos biométricos han sido comprometidos, es muy complicado volver a un estado seguro.

En (1) se presentan las distintas amenazas a las que están expuestos los sistemas de seguridad en general y, por tanto, también las aplicaciones basadas en reconocimiento biométrico. Estas amenazas son las siguientes:

- **Puenteo del sistema:** un usuario no autorizado logra acceso ilegítimo a los datos y al sistema.
- **Repudio:** negación de acceso al sistema a un usuario legítimo.
- **Contaminación o adquisición encubierta:** los medios de reconocimiento se ven comprometidos – y utilizados en beneficio del impostor - sin el conocimiento del usuario legítimo.
- **Colusión:** un usuario no autorizado logra estatus de súper-usuario, lo cual le permite eludir el componente de reconocimiento y gobernar así las decisiones que toma el sistema.
- **Coerción:** un usuario genuino es forzado a identificarse a sí mismo en el sistema.

4.1. Tipos de ataques a sistemas de reconocimiento biométrico

Las amenazas que acabamos de describir son generalmente el resultado de ataques sobre los distintos puntos vulnerables de un sistema de reconocimiento biométrico, llevados a cabo por un agente externo.

En (12) se identifican ocho potenciales puntos de ataque sobre un sistema biométrico - mostrados en la Figura 22 –, que son los siguientes:

- Ataques directo al sensor o escáner (punto 1 en la Figura 22).
- Ataques al módulo de extracción 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 existentes entre los módulos (puntos 2, 4, 7 y 8).

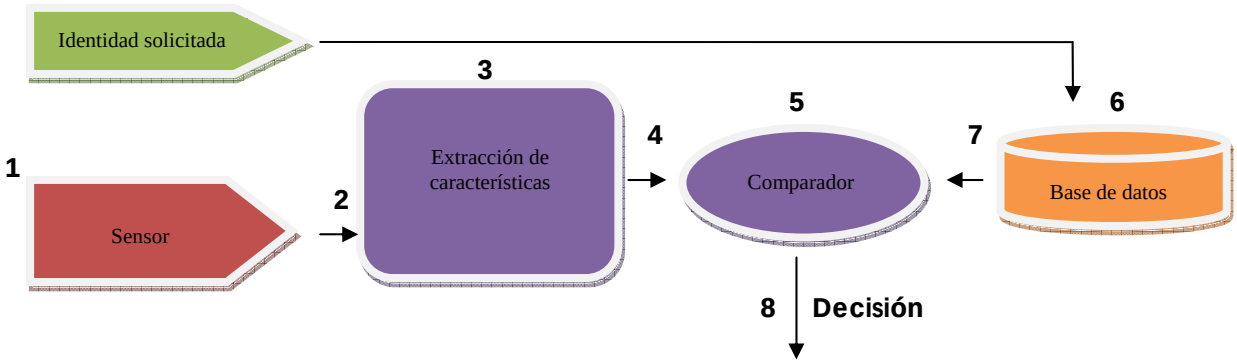


Figura 22: Arquitectura y flujo de datos de un sistema automático de verificación biométrico. Los potenciales puntos de ataque se encuentran numerados del 1 al 8.

El primer tipo de ataque – al sensor - es un **ataque directo** al sistema: el atacante no tiene ningún conocimiento sobre el funcionamiento de dicho sistema; mientras que el resto son **ataques indirectos**: el impostor tiene algún tipo de conocimiento sobre el funcionamiento o la estructura interna del sistema.

Los ataques 1, 3, 5 y 6 se lanzan sobre los módulos del sistema y se les conoce como ataques Troyanos. Los ataques 2, 4, 7 y 8 se lanzan sobre los canales de comunicación entre módulos y son referenciados como ataques de repetición.

En los siguientes apartados se presenta una recopilación de diferentes trabajos en los que se analizan distintos ataques pertenecientes a cada una de las ocho categorías expuestas anteriormente.

Ataques directos al sensor

Este tipo de ataques, marcados como de tipo 1 en la Figura 22, consiste en presentar un rasgo biométrico falso al sensor. En sistemas de reconocimiento de huella puede llevarse a cabo de distintas maneras. Por un lado, la superficie del sensor puede ser físicamente destruida, dando lugar a la negación del servicio. Por otro lado, una huella dactilar falsa, como una huella latente dejada sobre un papel, una imagen de huella impresa en un papel, una fina membrana de goma que contenga una impresión de una huella o un molde tridimensional de plástico, goma o gelatina, pueden ser presentados al sensor como entrada. Por último, una imagen puede ser introducida entre el elemento sensor - un chip de silicio, por ejemplo - y el resto de la electrónica del escáner - conversor A/D, microprocesador, módulo interfaz, etc.

Estos ataques han demostrado ser muy exitosos. Su viabilidad comparada con otro tipo de ataques es alta, ya que no necesitan más que la generación de un rasgo biométrico falso: no son necesarios conocimientos del módulo comparador, de las especificaciones de las plantillas, ni son necesarios privilegios de acceso a la base de datos de plantillas. 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 (13).

Si bien siempre se había pensado que las plantillas biométricas son representaciones tan compactas de las características de la imagen original que no contienen información suficiente como para poder reconstruir la imagen original a partir de ellas, recientemente, en estudios como el presentado en (14), se han cuestionado estas teorías.

A partir de las conclusiones extraídas en (14), en (15) se presenta un estudio preliminar sobre la evaluación de la vulnerabilidad de los sistemas de verificación de huella frente a ataques directos utilizando huellas falsas creadas a partir de plantillas estándar de minucias, y se demuestra que el esquema de ataque propuesto es perfectamente factible y supone una amenaza de seguridad sobre el uso de plantillas de minucias no encriptadas.

En (16) se prueba la vulnerabilidad de varios sensores de huella frente a dedos de goma (plastilina y silicona) creados artificialmente. En sus experimentos cinco de los seis sensores probados aceptaron el dedo de goma como real.

En (17) se atacan 11 sistemas de verificación diferentes con dedos de goma (gelatina) creados artificialmente. Cuando el usuario colabora, los dedos de goma logran engañar a todos los sistemas y son aceptados en él con una probabilidad de entre el 68-100%. Cuando el usuario no colabora – los dedos de goma se generan a partir de una huella latente recuperada de una superficie -, también todos los sistemas son engañados y los dedos de goma son aceptados con una probabilidad de más del 67%.

En (18) se presenta otro método de generación de dedos de goma. Se evalúan sobre una base de datos de tamaño medio dos sistemas de verificación diferentes, uno basado en minucias y otro basado en patrón de crestas, y se consideran tres escenarios distintos. Se concluye que, en general, el funcionamiento del sistema basado en crestas es peor que el basado en minucias, aunque menos vulnerable a los ataques directos y más resistente a muestras de baja calidad.

Para evitar estos ataques se han propuesto diferentes **técnicas de detección de vida**, cuyo objetivo es diferenciar entre una huella real (viva) y una artificial. Estas técnicas deben ser, por norma general, no invasivas, rápidas y de coste razonablemente bajo, y no causar rechazo por parte del usuario (1). Los métodos propuestos tradicionalmente están basados en la medición de características fisiológicas, tales como el pulso, la temperatura, el sudor (19) (20), la elasticidad de la piel (21) (22) o el olor (23).

Métodos más recientes, como el descrito en (24), proponen métodos software que analizan características medibles de la imagen de huella que sean capaces de diferenciar una huella real de una huella fabricada artificialmente.

En (25) se introduce un método de detección de vida basado en múltiples características estáticas (espaciado individual entre poros, ruido residual y otras estadísticas de primer orden), que se obtienen de una sola imagen de la huella.

Otros métodos de detección de vida incluyen los trabajos presentados en (26), donde se estudia la textura superficial de las huellas a través de su análisis *wavelet* (ondícula), y en

(27), donde se propone la utilización del espectro de Fourier en banda selectiva como técnica de detección de vida.

Ataques al canal entre el sensor y el extractor de características

En este tipo de ataques – tipo 2 en la Figura 22 - el canal entre el sensor y el extractor de características es interceptado y la imagen de huella digital de un usuario legítimo originada en el escáner es almacenada para replicarla posteriormente y presentarla al extractor de características, eludiendo así el sensor.

En la sección 4.2 de la memoria se presentan algunos ejemplos de estudios que profundizan en el análisis de este tipo de ataques.

Ataques al módulo extractor de características.

Un programa tipo Caballo de Troya (código ejecutable que no es directamente la traducción del programa original, sino que ha sido añadido con posterioridad, generalmente malintencionadamente, y que entra en el sistema simulando ser el programa original) puede suplantar al extractor de características y enviar características del rasgo biométrico – huella, en nuestro caso -, generadas artificialmente, al módulo comparador.

Para eliminar este tipo de ataques - marcados como de tipo 3 en la Figura 22 -, donde la realización biométrica previamente interceptada es duplicada, en (12) se propone un sistema basado en desafío/respuesta.

Ataques al canal entre el extractor de características y el módulo comparador

El canal entre el extractor de características y el comparador puede ser interferido para obtener el conjunto de características del rasgo biométrico de un usuario legítimo. Esta información puede ser guardada para poder reproducirla en cualquier otro momento, o bien, puede reemplazarse por otro conjunto distinto y fraudulento de características (plantilla sintética). Habitualmente las etapas de extracción y comparación son inseparables y por ello este tipo de ataque resulta complicado. Sin embargo, en ataques a sistemas de reconocimiento de huella, cuando las minucias son transmitidas a un comparador remoto, puede convertirse en una amenaza a considerar.

Dado que los ataques desarrollados en el presente proyecto pertenecen a esta categoría, en la sección 4.2 de la memoria se describen diversos ejemplos de estudios que analizan la eficiencia de este tipo de ataques.

Ataques al módulo comparador.

Un programa Troyano se hace pasar por el comparador y envía puntuaciones de comparación o decisiones (sí o no) artificiales a la aplicación que pedía la autenticación.

Cuando el Troyano genera siempre puntuaciones altas o respuestas afirmativas, se está produciendo un puenteo del sistema (1). Por el contrario, si el programa genera siempre puntuaciones bajas o respuestas negativas, estamos hablando de una negación del servicio. Este ataque se muestra en la Figura 22 como de tipo 5.

Ataques a la base de datos

Un programa Troyano simula ser la base de datos del sistema y envía información generada artificialmente - generalmente plantillas, nombres de usuario, privilegios de acceso, etc. Este ataque – de tipo 6 en la Figura 22 - puede lanzarse durante el proceso de registro, durante la etapa de verificación o directamente sobre la base de datos en cualquier otro momento. En una aplicación de tarjeta de inteligente, en la cual la plantilla de usuario (*template*) reside en la tarjeta que porta el usuario, si la tarjeta se pierde y ésta no está protegida adecuadamente, el impostor podría tener acceso directo a la plantilla.

En (28) se muestra un estudio relacionado con la seguridad de la base de datos de plantillas. Es necesario que las plantillas biométricas estén protegidas usando, por ejemplo, encriptación. Otro método de protección de uso fraudulento de plantillas supone utilizar una versión distorsionada de la señal biométrica no invertible o el vector de características (29). Así, si una representación concreta de la plantilla se ve comprometida, la transformación de distorsión puede ser cambiada por otra.

La ocultación de datos y técnicas de "marcas de agua" también se han propuesto como métodos para incrementar la seguridad de las imágenes de huella detectando modificaciones, escondiendo un rasgo biométrico dentro de otro u ocultando mensajes en el dominio comprimido (28), (29), (30), (31).

Ataques al canal entre la base de datos y el comparador

El canal entre la base de datos y el comparador – ataque tipo 7 en la Figura 22 - puede ser interceptado para robar el registro de un usuario legítimo, el cual es reproducido posteriormente en el canal de comunicación.

Ataques al canal entre el comparador y la aplicación

La comunicación entre el comparador y la aplicación que solicita la verificación puede ser interceptada para acceder a la respuesta de una verificación previa y guardarla. Esta respuesta es repetida más adelante en el canal. Es decir, la decisión final del sistema (Sí/No) queda a merced de la voluntad del intruso. Estos ataques están marcados como de tipo 8 en la Figura 22.

4.2. Ataques *hill-climbing* a sistemas de reconocimiento biométrico

Los ataques ***hill-climbing*** consisten en la modificación sucesiva de un patrón de características obtenido sintéticamente hasta que el sistema acepte dicho patrón como válido.

Este tipo de ataques puede realizarse contra el canal de comunicación entre el sensor y el extractor de características - ataque tipo 2 en la Figura 22 -, o bien entre el extractor de características y el comparador - ataque tipo 4 en la Figura 22. Cuando el ataque se realiza sobre este último punto es necesario conocer información relativa al formato de las plantillas.

En la Figura 23 se muestra el esquema general de un ataque ***hill-climbing*** tipo 4 basado en puntuación.

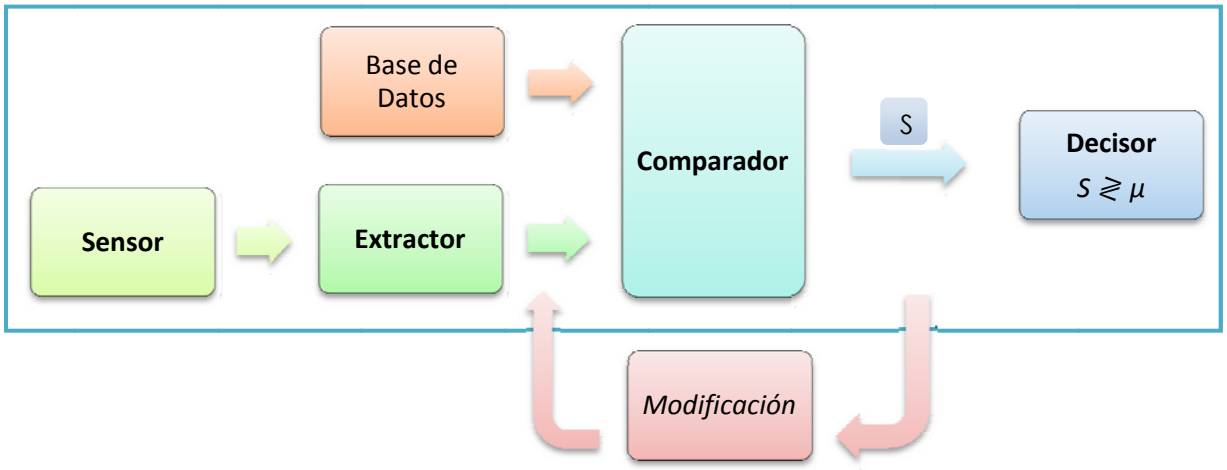


Figura 23: Esquema general de un ataque *hill-climbing* tipo 4 basado en puntuación.

En (32) se propone un ataque de tipo 2 – ver Figura 22 - a un sistema de reconocimiento de cara donde la cuenta de un usuario específico de la base datos es atacada generando sintéticamente imágenes de cara. Se describe un sencillo algoritmo que permite la recreación de una imagen a partir de una plantilla de cara empleando simplemente puntuaciones devueltas por el comparador. En cada paso, una imagen candidata es modificada ligeramente por una *eigen-face* y se conservan aquellas modificaciones que mejoran la puntuación. Aunque la sencillez del algoritmo propuesto sugiere que es extensible a otras modalidades biométricas, para atacar sistemas de reconocimiento de huella podrían necesitarse un tipo de funciones básicas diferente, debido a que en una huella la información discriminatoria no está sujeta a relaciones geométricas específicas, como sí ocurre en los sistemas de reconocimiento de cara - distancia entre ojos, nariz, boca, etc. - (13).

En (33) se propone un algoritmo de ataque ***hill-climbing*** basado en adaptación bayesiana. El método utiliza las puntuaciones proporcionadas por el comparador para adaptar una distribución global calculada a partir de un conjunto de usuarios de desarrollo a las particularidades del usuario atacado. Los resultados muestran una alta eficiencia del algoritmo, el cual logra atacar con éxito el sistema en más del 95% de los intentos.

En (34) se presenta un estudio sobre las vulnerabilidades que dos sistemas de reconocimiento biométrico basados en minucias presentan frente a un determinado ataque *hill-climbing* y se deduce que, permitiendo un número suficiente de iteraciones, la tasa de éxito de los ataques se encuentra por encima del 90%.

Nuestra aproximación al ataque

El ataque *hill-climbing* que se implementa en este proyecto es de tipo 4 – ver Figura 22 - sobre sistemas de reconocimiento de huella basados en minucias y su implementación está basada en el algoritmo propuesto en (13) y analizado en profundidad en (34). No obstante, como, en general, los sistemas de reconocimiento biométrico no devuelven la puntuación obtenida en el comparador, nuestro algoritmo basará su funcionamiento en el tiempo que emplea el sistema en realizar la comparación.

4.3. Ataques *Side-Channel*

Aunque no se trate propiamente de ataques que exploten las vulnerabilidades específicas de los sistemas biométricos, introduciremos en esta sección los conocidos como ataques *Side-Channel*, dada su gran relevancia dentro del desarrollo experimental de este proyecto.

En criptografía, este tipo de ataques utiliza información obtenida de la implementación física de un sistema criptográfico, como el tiempo (*timing-attacks*) (35), el consumo de energía (*power-attacks*) (36), las pérdidas electromagnéticas o, incluso, el ruido del sistema, para romper dicho sistema. No son, por tanto, ataques por fuerza bruta – los cuales aprovechan la existencia de una cierta tasa de falsa aceptación en los sistemas -, ni ataques que hagan uso de la debilidad teórica de los algoritmos utilizados por la aplicación. Muchos de estos ataques requieren un conocimiento técnico considerable sobre el modo de funcionamiento interno del sistema sobre el cual se implementa la criptografía.

En (37) se discute el concepto de ataques *side-channel* y las vulnerabilidades que éstos introducen en los sistemas. Además, se demuestra el éxito de varios tipos de ataques *side-channel* contra tres sistemas de cifrado distintos y se generaliza el estudio para otros sistemas criptográficos.

Dentro de los ataques *side-channel*, aquéllos basados en la información temporal del sistema – conocidos como *timing-attacks* – han demostrado una gran eficiencia, con lo que se han convertido en una amenaza real a tener en cuenta a la hora de implementar este tipo de sistemas.

4.3.1. Ataques *Side-Channel* basados en tiempo: *Timing-Attacks*

Los sistemas criptográficos habitualmente requieren tiempos ligeramente distintos para procesar diferentes entradas. Entre las razones para que esto ocurra se incluyen la optimización de la ejecución para evitar operaciones innecesarias, saltos e instrucciones condicionales, aciertos en la caché, instrucciones del procesador - como multiplicación y división - que se ejecutan en un tiempo que no es fijo.

Si bien las características temporales que se generan no intencionadamente sólo revelan, en principio, una pequeña cantidad de información sobre un sistema criptográfico - como el peso *Hamming* de la clave -, está demostrado que ciertos ataques que aprovechan las medidas de tiempo tienen éxito encontrando la totalidad de la clave secreta.

Así, los ataques *side-channel* basados en tiempo (*timing-attacks*) basan su funcionamiento en la monitorización del movimiento de datos que entra y sale de la CPU o la memoria del hardware que está ejecutando el sistema criptográfico. De este modo, simplemente observando cuánto tiempo se tarda en transferir cierta información, por ejemplo, una clave, en ocasiones es posible determinar cómo de larga es esa clave o, al menos, se pueden descartar ciertas longitudes, lo cual también puede ser útil para el análisis criptográfico. En general, se puede decir que los sistemas proporcionan cierta información que puede ser deducida simplemente observando el tiempo que emplea dicho sistema en la ejecución del algoritmo o de alguna operación interna.

En (35), donde este tipo de ataques se introducen por primera vez, se sugiere que, midiendo cuidadosamente el tiempo requerido para ejecutar operaciones de clave privada, un atacante es capaz de romper ciertos sistemas criptográficos. Se afirma que, contra un sistema vulnerable, este tipo de ataques no tiene una excesiva carga computacional y generalmente sólo requiere que se conozca el texto cifrado. Por ello, se sugiere que sistemas criptográficos reales, como los basados en testigo (*token*) o en red, y otras aplicaciones en las que el atacante puede realizar medidas de tiempo mínimamente precisas, están potencialmente en riesgo. Por último, se presentan técnicas para evitar este tipo de ataques y se sugiere la revisión de los sistemas criptográficos, algoritmos y protocolos, para que incorporen medidas que eviten esta amenaza.

En (38) se propone un *timing-attack* contra sistemas de claves encriptadas basado en medidas del tiempo total de ejecución y en el cual se supone un conocimiento muy limitado de los detalles de implementación del sistema. Se demuestra que, en general, el ataque permite romper claves criptográficas de 512 bits con tan solo 5000 medidas de tiempo, lo que lo convierte una amenaza factible y efectiva sobre dispositivos criptográficos reales.

En (39), por otro lado, se presenta un estudio que demuestra que los *timing-attacks* sobre servidores de red son factibles. Sus experimentos muestran que, al contrario de lo que se pensaba hasta entonces, el *timing-attack* es efectivo cuando se lleva a cabo entre máquinas separadas por múltiples enrutadores. Del mismo modo, el ataque es efectivo entre dos procesos que se ejecutan en la misma máquina y dos máquinas virtuales que se encuentran en el mismo ordenador.

Es un hecho, por tanto, que, al menos en sistemas criptográficos, este tipo de ataques es posible. El objetivo de la parte experimental de nuestro proyecto será, en primer lugar, comprobar si existe alguna relación entre la información temporal que se puede extraer de los sistemas de reconocimiento de huella dactilar y su funcionamiento, y, en segundo lugar, estudiar la viabilidad de combinar el conocimiento que se tiene sobre las vulnerabilidades de los sistemas biométricos y sobre los *timing-attacks* para intentar desarrollar ataques tipo *hill-climbing* basados en el tiempo de comparación algorítmica que permitan el acceso fraudulento al sistema atacado.

5. Entorno experimental

5.1. Sistemas analizados

Los sistemas de reconocimiento automático de huella dactilar que vamos a analizar son el software de referencia NFIS2 del NIST americano y un sistema integrado de tarjeta inteligente o *Match-on-Card* (MoC).

Los ataques se realizarán en un PC que disponga, por un lado, del software NIFS2 instalado y, por otro lado, de los drivers necesarios para el funcionamiento de la tarjeta inteligente. Las pruebas se automatizarán mediante Matlab, permitiendo así realizar ataques masivos de forma continuada.

5.1.1. Software de referencia NFIS2 del NIST

El software de referencia NFIS2 del NIST (Instituto Nacional de Estándares y Tecnología) es un software de imagen de huella desarrollado para el FBI y el DHS (Departamento de Seguridad Nacional) de los Estados Unidos. El sistema NFIS es reconocido a nivel mundial como una referencia en verificación de huella dactilar y los sistemas de reconocimiento de huella dactilar que se diseñan en la actualidad suelen compararse con este sistema para tener una primera medida comparativa de rendimiento.

La tecnología software contenida en NFIS2 es, pues, la culminación de más de una década de trabajo productivo del NIST para el FBI y el DHS. El software NFIS2 es una colección de aplicaciones, programas, utilidades y librerías de código fuente, organizados en una serie de módulos que realizan funciones como la clasificación y la segmentación de huellas, la detección de minucias y la determinación de la calidad de imágenes de huella.

La funcionalidad de los paquetes utilizados para el desarrollo de este proyecto se describe a continuación y puede observarse en la Figura 24.

- **MINDTCT:** localiza minucias - terminación y bifurcación, solamente - en las crestas de la imagen de huella que recibe como entrada. Se almacenan la ubicación, el tipo, la orientación y la calidad de las minucias de la huella.
- **BOZORTH3:** es un sistema de comparación de huellas que usa las minucias detectadas por MINDTCT para determinar si dos huellas pertenecen a la misma persona y el mismo dedo. Puede funcionar tanto en modo verificación como en modo identificación.

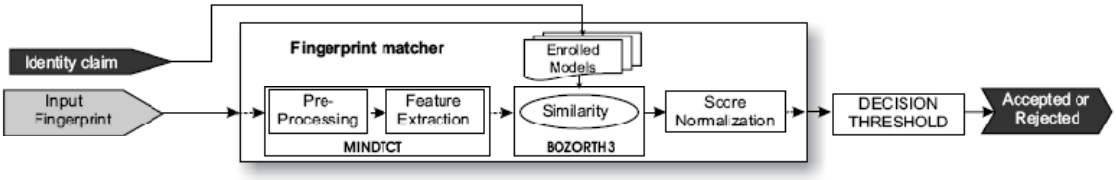


Figura 24: Arquitectura de un sistema NFIS2.

A continuación se profundiza en el funcionamiento de estos dos paquetes software.

MINDTCT

El módulo MINDTCT permite la detección de minucias en la imagen de huella, asignando a cada minucia sus coordenadas, su orientación, su tipo y su calidad. Los pasos más importantes que sigue el algoritmo se muestran en la Figura 25.

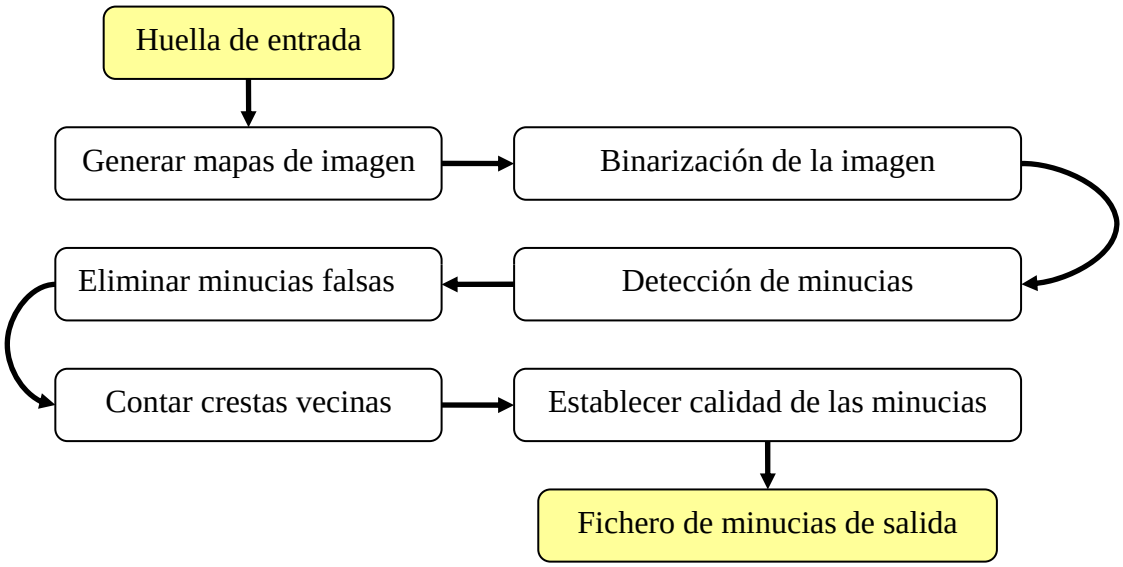


Figura 25: Arquitectura del módulo MINDTCT.

1. **Generación de mapas de calidad de imagen.** Debido a que la calidad de la imagen de una huella puede ser variable, especialmente en el caso de huellas latentes, es importante determinar qué áreas de la imagen están degradadas y es más probable que causen problemas. Las características que se utilizan para determinar la calidad de las áreas de la imagen incluyen la detección de regiones de bajo contraste, bajo flujo de crestas y alta curvatura. Estas tres condiciones representan áreas inestables de la imagen en las que la detección de minucias no es fiable y se usan para representar niveles de calidad en la imagen.
2. **Binarización de la imagen.** El algoritmo de detección de minucias está diseñado para operar con una imagen binaria, donde los píxeles negros representan las crestas y los blancos los valles del dactilograma. Para crear la imagen binarizada, cada píxel de la imagen de escala de grises es analizado para determinar si debe asignársele un píxel negro o uno blanco, en base a la dirección del flujo de crestas asociada con el bloque en el que se encuentra el píxel.
3. **Detección de minucias.** Este paso consiste en el escaneo metódico de la imagen para identificar patrones que indiquen el fin o la bifurcación de una cresta.
4. **Eliminación de minucias falsas.** El paso anterior supone un ambicioso esquema de detección de minucias que minimiza la posibilidad de omitir una minucia real. Por ello, muchas minucias falsas son incluidas como candidatas a la lista de minucias. Esta etapa tiene como objetivo eliminar estas falsas minucias, entre las que se incluyen islas, lagos, agujeros, minucias en regiones de baja calidad, minucias muy cercanas, ganchos, solapamientos, minucias muy anchas y minucias muy estrechas (poros).

5. **Conteo de crestas vecinas.** Los comparadores de minucias de huellas utilizan habitualmente información adicional a las propias minucias. Esta información auxiliar incluye normalmente la dirección de las minucias, el tipo o información perteneciente a las minucias vecinas. Un atributo común es el número de crestas intermedias entre una minucia y cada una de sus vecinas.
6. **Establecimiento de la calidad de las minucias.** Incluso tras el paso de eliminación de minucias falsas, puede quedar alguna en la lista de minucias candidatas. Establecer la calidad de las minucias puede ayudar a solucionar este problema - las minucias falsas tienen en teoría menor calidad que las verdaderas. Para establecer la calidad de cada minucia candidata se tiene en cuenta la ubicación de la minucia dentro del mapa de calidad descrito en el primer paso y los parámetros estadísticos - media y desviación estándar - de la intensidad del píxel dentro de su entorno inmediato. Una región de alta calidad tendrá un contraste significativo que cubrirá completamente el espectro de escala de grises.
7. **Fichero de salida.** Se crean ficheros de salida con los mapas de calidad y con los mapas de minucias. El mapa de minucias es un fichero de texto que contiene un listado de minucias en filas formado por sus coordenadas, su orientación y su nivel de calidad.

BOZORTH3

Como ya hemos comentado, este módulo software contiene el algoritmo que compara las características extraídas de dos huellas - detectadas con MINDTCT -, o bien compara las características de una huella con un conjunto de otras.

El algoritmo de comparación consta básicamente de tres pasos:

1. **Construcción de tablas de comparación de minucias dentro de la huella.** Se construye una tabla para la huella de *test* y una tabla por cada huella de la galería con la que vaya a ser comparada. Estas tablas de comparación contienen las distancias y ángulos relativos entre minucias de la misma huella – ver Figura 26 - y dotan al algoritmo de invarianza frente a rotaciones y traslaciones.

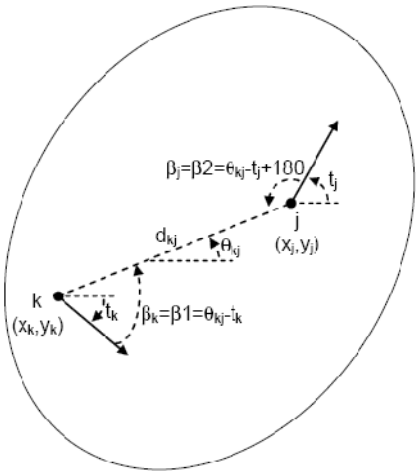


Figura 26: Comparación de minucias intra-huella. Imagen extraída de (5).

2. **Construcción de una tabla de compatibilidad entre huellas.** Se buscan entradas compatibles entre la tabla de comparación de minucias de la huella de *test* y la tabla de comparación de minucias del *template*. La tabla de compatibilidad

contiene, pues, una lista de asociación de compatibilidad entre dos pares de minucias potencialmente correspondientes.

3. **Búsqueda en la tabla de compatibilidad entre huellas.** Primero se recorren y se enlazan entradas de la tabla, formando agrupaciones. A continuación, se combinan las agrupaciones compatibles y se van acumulando las puntuaciones de comparación.

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

La segunda aplicación que analizaremos en este proyecto consiste en un sistema de tarjeta inteligente *Match-on-Card* – ver Figura 27. Este sistema permite la ejecución del algoritmo de comparación 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 (*templates*) y solventa, por tanto, el problema de las comunicaciones - que pueden ser interceptadas - entre el sistema y dicha base de datos.

Entre las ventajas de este tipo de sistemas debemos destacar:

- **Seguridad.** Aunque no añade nada nuevo respecto a otros sistemas, el sistema de MoC asegura que la comparación entre la plantilla y la huella a comprobar se realiza en un entorno cerrado, elemento éste indispensable para que sea considerado un sistema seguro.
- **Privacidad.** El usuario genuino tiene en su poder la única muestra de su plantilla. No es necesaria, pues, una base de datos externa, con lo que se evitan los problemas derivados de su mantenimiento y actualización.
- **Consistencia.** Solamente la tecnología MoC garantiza que el proceso de comparación sea siempre correcto y consistente, precisamente porque éste se realiza dentro de la tarjeta y nadie puede modificarla.
- **Escalabilidad.** Gracias a que el proceso de verificación de huella se realiza localmente en la tarjeta inteligente sin la necesidad de recursos de red o servidores, el sistema MoC crea una base de datos altamente escalable, distribuida y transportable, donde cada activo biométrico es mantenido en su propio entorno seguro de tarjeta inteligente. Esto le permite ser válido para la implementación de grandes sistemas, donde mantener una base de datos que almacene todas las plantillas es impracticable y muy caro.
- **Integración.** El algoritmo de MoC requiere para su código poco espacio. Sólo se requiere espacio de memoria adicional para cada plantilla almacenada en la tarjeta. Además, la implementación de MoC no interfiere con otras aplicaciones basadas en tarjeta (tarjetas de banco, de identificación, etc.). De hecho, estas otras aplicaciones pueden aprovecharse del sistema MoC, utilizando interfaces compartidas y añadiendo seguridad biométrica a su funcionalidad independiente.

Si bien, como se acaba de exponer, las ventajas de los sistemas basados en tarjeta inteligente son numerosas, no podemos olvidar que este tipo de sistemas presentan también una serie de inconvenientes, si los comparamos con los sistemas tradicionales, que básicamente se derivan de sus limitaciones hardware en cuanto a capacidad de almacenamiento y de cómputo. Las dos más importantes son:

- **Rendimiento**: los sistemas de reconocimiento basados en tarjeta inteligente presentan un peor rendimiento que los sistemas clásicos, es decir, se equivocan más a menudo - FAR y FRR mayores. Esto se debe a que el algoritmo de reconocimiento que se puede ejecutar en un hardware con limitaciones en su

capacidad de almacenamiento y de cómputo debe ser necesariamente mucho menos complejo.

- **Eficiencia**: de nuevo, las limitaciones hardware de este tipo de sistemas provocan que la ejecución del algoritmo de comparación y la comunicación con ellos sea mucho más lenta en comparación con los sistemas tradicionales.

Figura 27: Sistema *Match-on-Card* empleado en el proyecto.

5.2. Base de datos

Las huellas empleadas en el desarrollo de la parte experimental del proyecto proceden de un subconjunto de la base de datos MCYT (40), la cual consta de 330 usuarios, cada uno con 10 huellas, de las cuales se toman 12 muestras con 2 tipos de sensores – capacitivo y óptico.

Como base de datos para la realización de este proyecto se toman tan sólo 75 usuarios. De cada uno de ellos se toman 10 muestras - adquiridas con el sensor óptico - de las 2 huellas de los índices de ambas manos. Con esto obtenemos un total de 1500 huellas para la base de datos de nuestro entorno de pruebas – ver Figura 28.

Figura 28: Base de datos utilizada en los experimentos.

La base de datos MCYT fue adquirida con distintos niveles de control. Para determinar el nivel de control de cada huella se situó un rectángulo en el área de captura, de modo que el núcleo de la huella en cuestión se encontrase en el interior del rectángulo; cuanto menor era el área del rectángulo, mayor era el nivel de control en la adquisición y, por lo tanto, existía una menor rotación y desplazamiento entre las huellas adquiridas – ver Figura 29. De las 10 muestras escogidas en este proyecto, 2 son de bajo control, 2 de control medio y 6 de alto control.

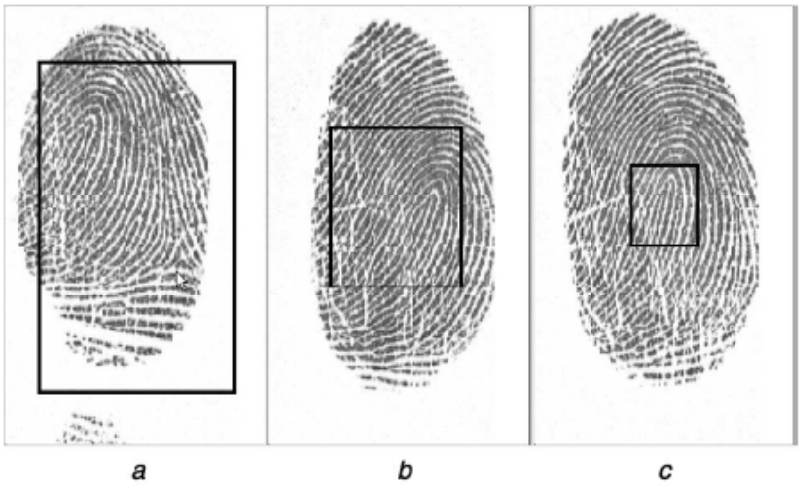


Figura 29: Ejemplo de imágenes adquiridas de una misma huella dactilar con diferentes grados de control (40). a) Bajo control; b) Control medio; c) Alto control.

5.3. Rendimiento de los sistemas

Sobre la base de datos descrita se ha estimado el rendimiento de los sistemas que se analizarán en la parte experimental del proyecto – NFIS y MoC. Para ello, como plantillas de usuario hemos tomado 150 muestras de bajo control – una de cada dedo que forma la base de datos. Teniendo en cuenta que tenemos 10 muestras de cada huella, las

puntuaciones genuinas se calcularán comparando cada plantilla con las 9 muestras restantes del usuario, lo que hace un total de 9x150 = 1350 puntuaciones genuinas. Para las puntuaciones de impostores compararemos cada una de las plantillas con una muestra de cada uno de los 149 usuarios restantes, con lo que el conjunto de puntuaciones de impostor estará formado por 150x149 = 22350 medidas de similitud – ver Figura 30.

Figura 30: Esquema de puntuaciones de genuinos e impostores.

A partir de las puntuaciones generadas, se pueden obtener las densidades de probabilidad para usuarios e impostores que caracterizan un sistema. En la Figura 31 se muestran dichas fdp's para los dos sistemas que se analizarán en el presente proyecto: NFIS y MoC.

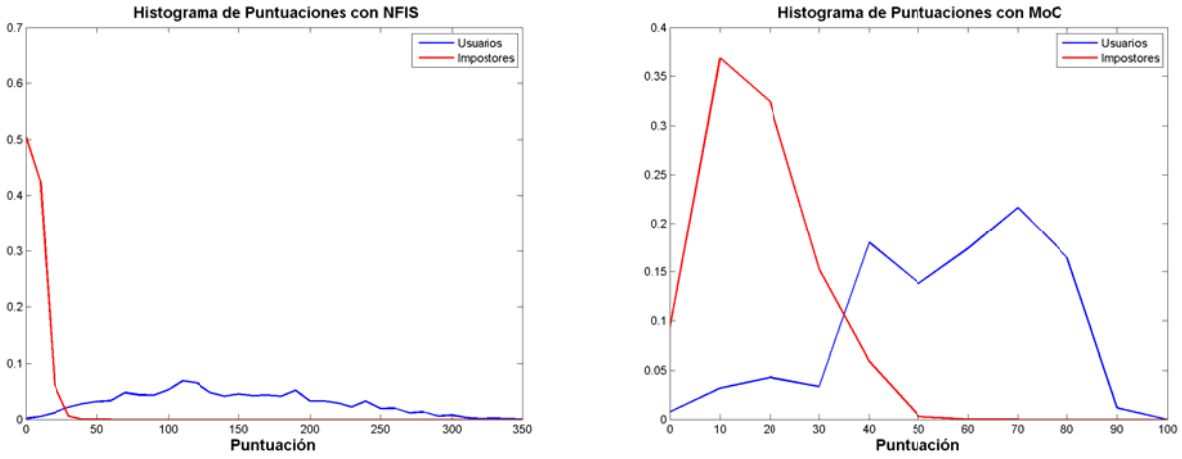


Figura 31 : Densidad de probabilidad de puntuaciones de usuarios e impostores para el sistema NFIS (izquierda) y el sistema MoC (derecha).

Como se puede observar, en la gráfica del NFIS – Figura 31 izquierda - los impostores se acumulan mayoritariamente en puntuaciones por debajo de 40, mientras que los usuarios están más distribuidos a lo largo de toda la banda de puntuaciones (0 – 350), aunque podría considerarse que tienen mayor preponderancia las puntuaciones alrededor de 120.

Para el sistema de tarjeta inteligente *Match-on-Card* – Figura 31 derecha -, las puntuaciones de impostores presentan una densidad de probabilidad más o menos *gaussiana* alrededor de 20, mientras que la densidad de probabilidad de los usuarios se asemeja a la suma de dos *gaussianas*, una centrada en 20 - que cubre el rango de

puntuaciones típico de impostor -, y otra centrada en 60 - que cubre el rango de puntuaciones típicas de usuario. Todo ello implica que este sistema presenta un comportamiento bimodal, es decir, su funcionamiento varía dependiendo de si se encuentra trabajando en el rango de puntuaciones que considera de impostor o de usuario.

En la Figura 32 se muestran también las curvas FR y FA obtenidas para los dos sistemas.

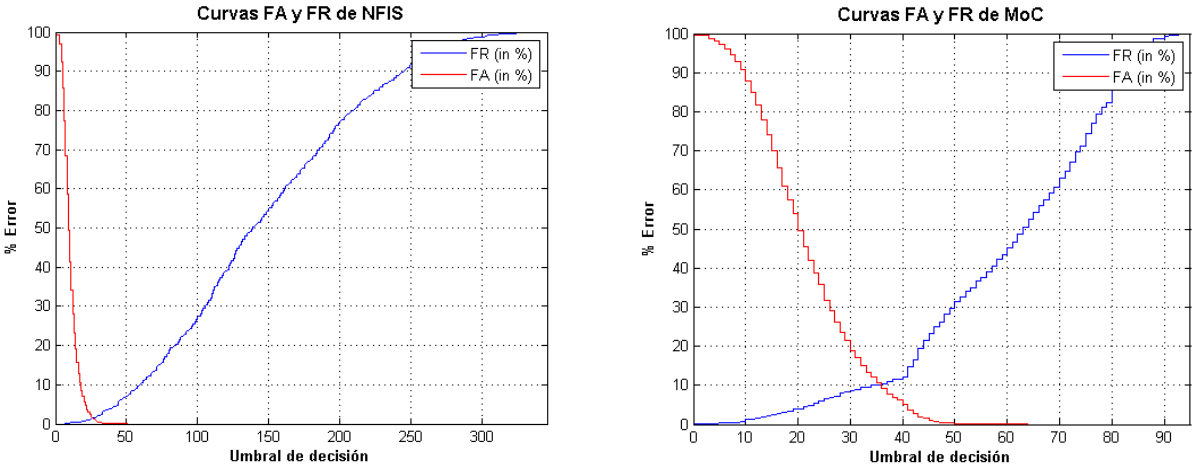


Figura 32 : Curvas FA y FR obtenidas con los sistemas NFIS2 (izquierda) y MoC (derecha).

Como cabía esperar, debido a sus limitaciones hardware – todo el proceso de comparación debe realizarse en el interior del espacio restringido del chip de la tarjeta -, el sistema MoC presenta un rendimiento sensiblemente peor al del sistema NFIS, con un EER del 9,78% y 1,47%, respectivamente.

Por otra parte, tal y como ya se había observado en la Figura 31 derecha, para puntuaciones menores que 40 (puntuaciones típicas de impostor), se puede apreciar que la curva de FR del sistema MoC cambia su comportamiento para puntuaciones mayores que 40 (puntuaciones típicas de usuario). Así pues, queda patente, de nuevo, un fuerte comportamiento bimodal del sistema MoC, dependiendo de la zona en que esté trabajando dicho sistema.

Para terminar esta sección, en la Figura 33 se muestran las curvas DET de los dos sistemas analizados, donde queda patente un peor funcionamiento del sistema MoC frente al sistema NFIS para todo el rango de funcionamiento: la curva del NFIS siempre se mantiene por debajo de la del MoC – ver sección 2.4.2.

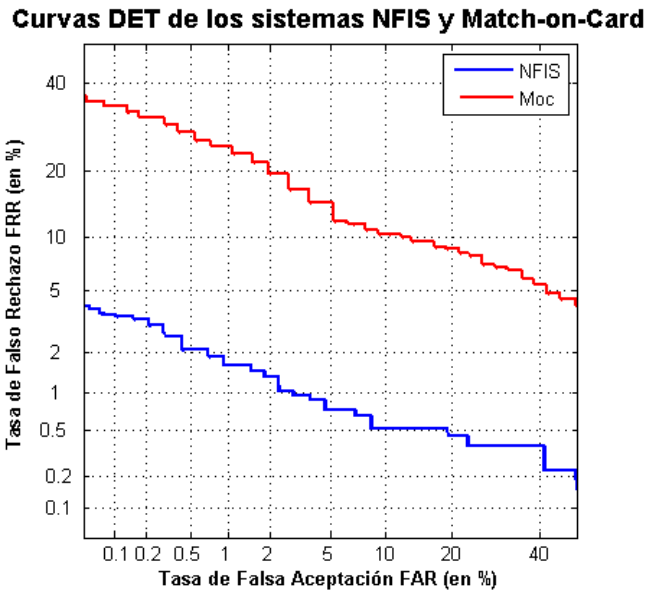


Figura 33 : Curvas DET del sistema Match-on-Card y del sistema NFIS2.

En el sistema del NIST, el EER se encuentra en una puntuación de 26,5 con un valor de 1,47%, como se observa en la Figura 32 izquierda. En la parte experimental del presente proyecto se ha considerado que un umbral de funcionamiento adecuado para este sistema es 35, que da lugar a una FAR del 0.1% y una FRR del 3.33%.

El EER del sistema MoC, por su parte, es del 9,78% para una puntuación de 36,5. El umbral de funcionamiento escogido para este sistema es de 55, que da lugar a una FAR del 0.16% y una FRR del 37.33% - ver Figura 32 derecha.

5.4. Algoritmo de ataque

El objetivo de este proyecto es, además de analizar la relación que existe entre la puntuación devuelta por los sistemas analizados y el tiempo que tardan en generarla, comprobar si dicha relación se puede aprovechar para desarrollar un ataque *hill-climbing* basado, no en la puntuación devuelta por el sistema – a la que no siempre se tiene acceso –, sino en el tiempo Tm que tarda el comparador en procesar dicha información. Para ello asumiremos que el tiempo empleado por el módulo decisor, Tc, es constante.

En la Figura 34 se muestra un esquema genérico del problema al que nos enfrentamos.

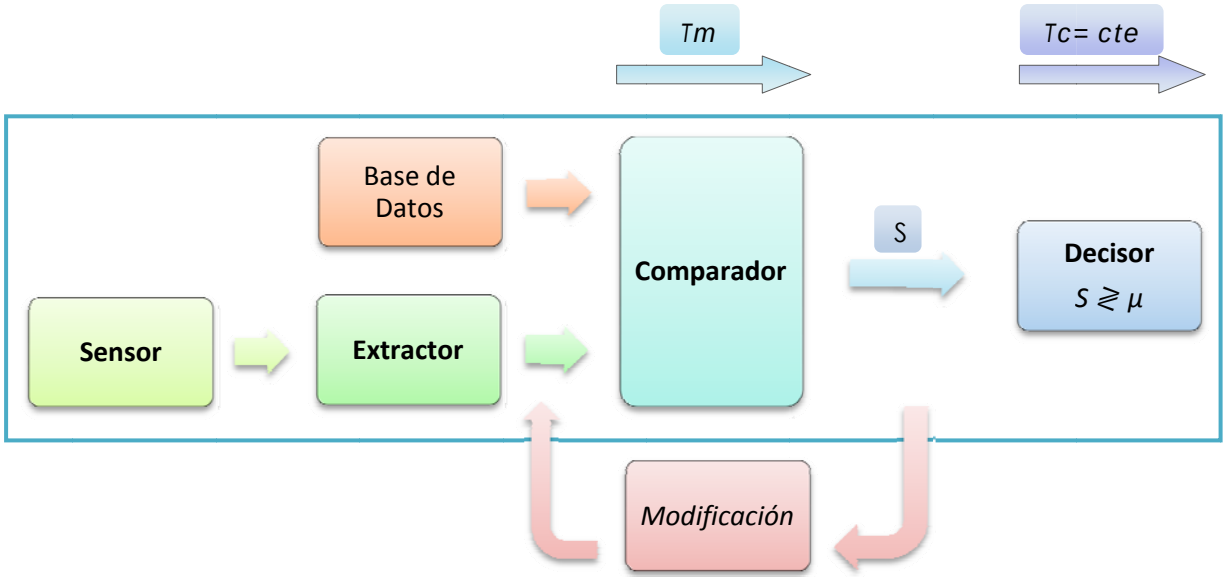


Figura 34 : Esquema general del algoritmo *hill-climbing* basado en tiempo que se desarrollará en el proyecto.

El algoritmo *hill-climbing* que utilizamos para atacar los sistemas descritos es una versión mejorada (34) del algoritmo propuesto en (13) y adaptada para atacar en función del tiempo Tm – ver Figura 34 -, en lugar de en función de la puntuación.

Como ya habíamos adelantado, para analizar y atacar un sistema entre el extractor de características y el módulo comparador – ataque tipo 4 en la Figura 22 - es necesario conocer la estructura de las plantillas de usuario. En nuestro caso, cada minucia de cada plantilla de la base de datos del sistema es guardada como un vector de tres componentes: dos relativas a su posición en el plano (2 dimensiones) y una tercera que se corresponde con el ángulo de la minucia respecto a la horizontal.

En el inicio del ataque propuesto en (13), para cada huella atacada se crean 100 patrones de minucias aleatorios y se comienza a atacar la huella del usuario con aquel patrón que haya generado la puntuación más alta. Este patrón – huella de *test* – se irá modificando sucesivamente hasta que se logre superar el umbral de decisión del sistema. Las modificaciones permitidas sobre el patrón de características creado artificialmente son:

A. Perturbar una minucia existente.
B. Añadir una minucia.
C. Sustituir una minucia elegida al azar.
D. Eliminar una minucia al azar.

En (34) se implementa este ataque *hill-climbing* basado en puntuación sobre los mismos sistemas analizados en el presente proyecto – NFIS2 y MoC. En dicho estudio se alcanzan una serie de conclusiones que nos servirán de apoyo durante la realización de nuestro proyecto:

- Tras la extracción de minucias mediante MINDTCT, se observó que existe una alta concentración de minucias en los bordes de la huella. Esto afecta negativamente al funcionamiento del sistema completo, pues se están introduciendo minucias artificiales. Por esta razón se realizó una etapa de post-procesado en la que se eliminaron todas las minucias que se encontraban en las cercanías de la frontera entre las zonas de alta calidad y baja calidad.
- La mayor parte de las minucias se localizan en un área elíptica centrada en la imagen de la huella, que es la zona más probable en la que se encuentren las minucias de una huella. A esta área se le denominará en adelante ROI (*Region of Interest*) o Región de Interés. Se concluye que los ataques tienen más éxito si se trabaja solamente con la ROI de las huellas.
- Se determina que el número inicial de minucias ideal es de 38 para NFIS2 y de 25 para MoC.
- Se concluye que el ataque que obtiene mejores resultados es el que permite solamente las modificaciones tipo B y C: añadir minucia y sustituir minucia.

El algoritmo de ataque implementado en el presente proyecto partirá, pues, del esquema presentado en (13) y de las conclusiones obtenidas en (34) para tratar de explotar la información temporal de los sistemas analizados. Así, las etapas de las que consta nuestro algoritmo son:

1. Generación de 100 plantillas sintéticas iniciales con un número predeterminado de minucias, todas ellas situadas dentro de la ROI.
2. Comparación de las 100 plantillas sintéticas con la del usuario atacado (cada una de estas comparaciones producirá un tiempo Tm_i con i=1,…,100) y elección de la mejor plantilla sintética – aquella que creamos que ha generado un mayor valor de puntuación – en función del tiempo Tm.
3. Modificación de la plantilla sintética permitiendo uno de los siguientes cambios:
    b. Añadir una minucia.
    c. Sustituir una minucia elegida al azar.

   Se considera que las plantillas están divididas en celdas de 9x9 píxeles y que sólo se puede colocar una minucia por celda. En general, se permitirán M cambios antes de realizar una nueva comparación.
4. Nueva comparación y cálculo del nuevo tiempo Tm tras los M cambios realizados. Si Tm indica que la puntuación ha aumentado con los cambios introducidos, los mantenemos; si no, los desechamos. Volvemos al paso 3.
5. El algoritmo termina cuando el sistema devuelve una respuesta positiva y nos permite el acceso al mismo – el ataque ha tenido éxito –, o cuando se alcanza un límite máximo de iteraciones - el ataque no ha tenido éxito.

6. Análisis temporal de los sistemas

El primer objetivo del presente proyecto es analizar si existe alguna relación entre la puntuación devuelta por los sistemas analizados y el tiempo de comparación Tm, de tal forma que éste pueda ser utilizado en el ataque *hill-climbing* que se describe en la sección 5.4.

Para la caracterización temporal de los sistemas analizados se han llevado a cabo dos experimentos: uno para determinar la relación entre Tm y la puntuación (Experimento 1) y un segundo que ilustra la relación entre Tm - ver Figura 34 - y el incremento en la puntuación (Experimento 2).

6.1. Experimento 1: Relación entre Tiempo y Puntuación

El objetivo de este primer experimento es averiguar si existe alguna relación entre el tiempo empleado en el comparador y la puntuación obtenida.

Como se mostraba en la Figura 30, con la base de datos utilizada, en el entorno de pruebas vamos a obtener 1.350 valores de puntuaciones genuinas y 22.350 valores de puntuaciones impostoras. A cada una de estas puntuaciones se le asocia un tiempo: el que tarda el sistema en devolver cada una de esas puntuaciones. Así pues, obtendremos otros tantos valores de tiempos genuinos y de tiempos impostores.

En la Figura 35 se observa que, aunque el solapamiento de las densidades de probabilidad del tiempo de usuarios e impostores es mayor que el obtenido para las densidades de probabilidad de la puntuación – Figura 31 –, sigue existiendo una clara separación entre la distribución de usuarios y la de impostores, tanto para el sistema NFIS como para el sistema MoC.

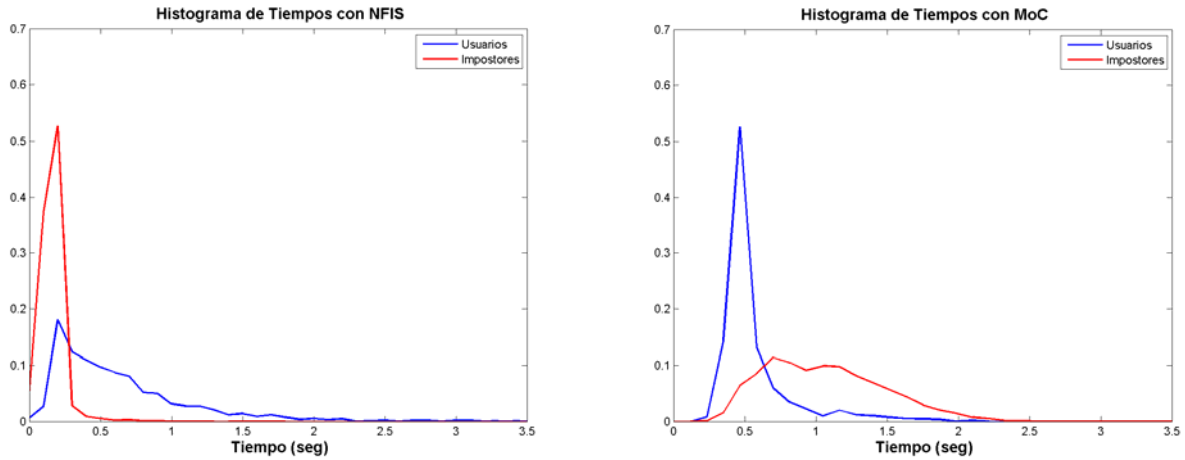


Figura 35: Densidad de probabilidad de tiempos para usuarios e impostores para el sistema NFIS (izquierda) y el sistema MoC (derecha).

A partir de las observaciones realizadas sobre la Figura 35, y con el objetivo de definir más claramente la relación entre tiempo y puntuación, se dividirá el rango total de

puntuaciones (R_T) - definido como la diferencia entre la puntuación máxima y mínima del sistema ($R_T = S_{máx} – S_{mín}$) -, en 10 regiones iguales, como se puede apreciar en la Figura 36:

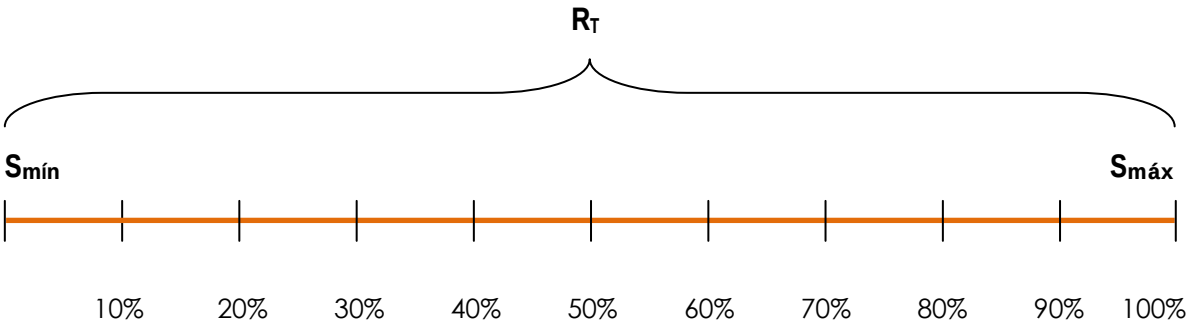


Figura 36 : División del espacio de puntuaciones en 10 regiones iguales.

Para cada una de estas 10 regiones representaremos la densidad de probabilidad (histogramas) de puntuaciones y la densidad de probabilidad de tiempos correspondientes a esas mismas puntuaciones, con el objetivo de averiguar si a rangos de puntuaciones más alejados les corresponden densidades de probabilidad de tiempos menos solapadas.

6.1.1. Resultados para el software NFIS

Tal y como se exponía en la introducción de esta misma sección, comenzamos representando en una misma gráfica el histograma de la primera región y de la última. Como ya habíamos indicado antes, la primera región estará constituida por las puntuaciones - y tiempos correspondientes –, tanto de usuarios como de impostores, que pertenecen al primer 10% del rango total de puntuación R_T. La última región es aquella en la que la puntuación pertenece al último 10% del rango total de puntuación R_T (entre el 90% y el 100%).

Continuaremos representando las regiones dos a dos, pero acumulativamente, es decir, comparamos la primera región con la última, la primera y la segunda con la última y la penúltima, y así sucesivamente.

El resultado obtenido para este experimento se muestra en la Figura 37:

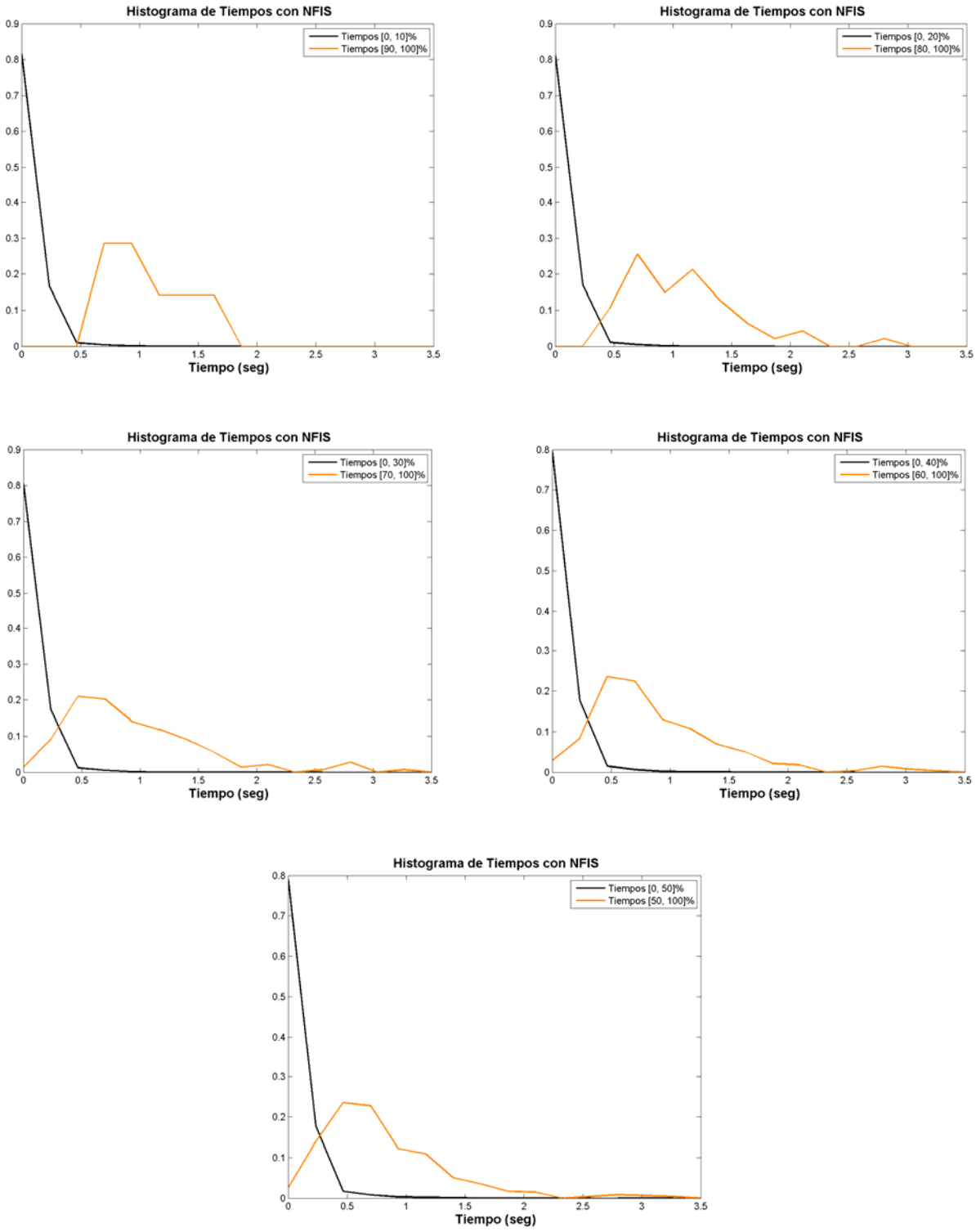


Figura 37: Puntuaciones (izquierda) y Tiempos (derecha) para la división por regiones detallada en la Figura 36 en NFIS.

Como se puede observar en las gráficas de la Figura 37, a medida que vamos incluyendo puntuaciones más cercanas entre sí, los tiempos se van solapando cada vez más. No obstante, cuando las puntuaciones están muy separadas – regiones [0 10]% y [90 100]% -,

los tiempos prácticamente no se solapan y sería posible establecer un umbral de separación bastante fiable entre ambas regiones. Además, se puede apreciar que la fdp de la región de puntuaciones inferiores - en negro – tiene siempre una forma muy similar, y es la fdp de puntuaciones superiores – en naranja – la que va variando su forma y su valor medio. Por último, cabe destacar que los tiempos inferiores corresponden siempre con las puntuaciones más bajas.

Conclusión

Del experimento que se acaba de describir se puede extraer como conclusión que en el sistema NFIS existe una correlación clara entre el tiempo de comparación Tm y la puntuación devuelta S: a mayor puntuación (S), en general, mayor tiempo de comparación (Tm). Esta relación entre puntuación y tiempo se podrá explotar a la hora de desarrollar un ataque hill-climbing basado en el tiempo de comparación algorítmica.

6.1.2. Resultados para el sistema MoC

En la Figura 38 se muestran, de forma análoga a como se representaron para el sistema del NIST, los resultados obtenidos para este primer experimento sobre el sistema MoC.

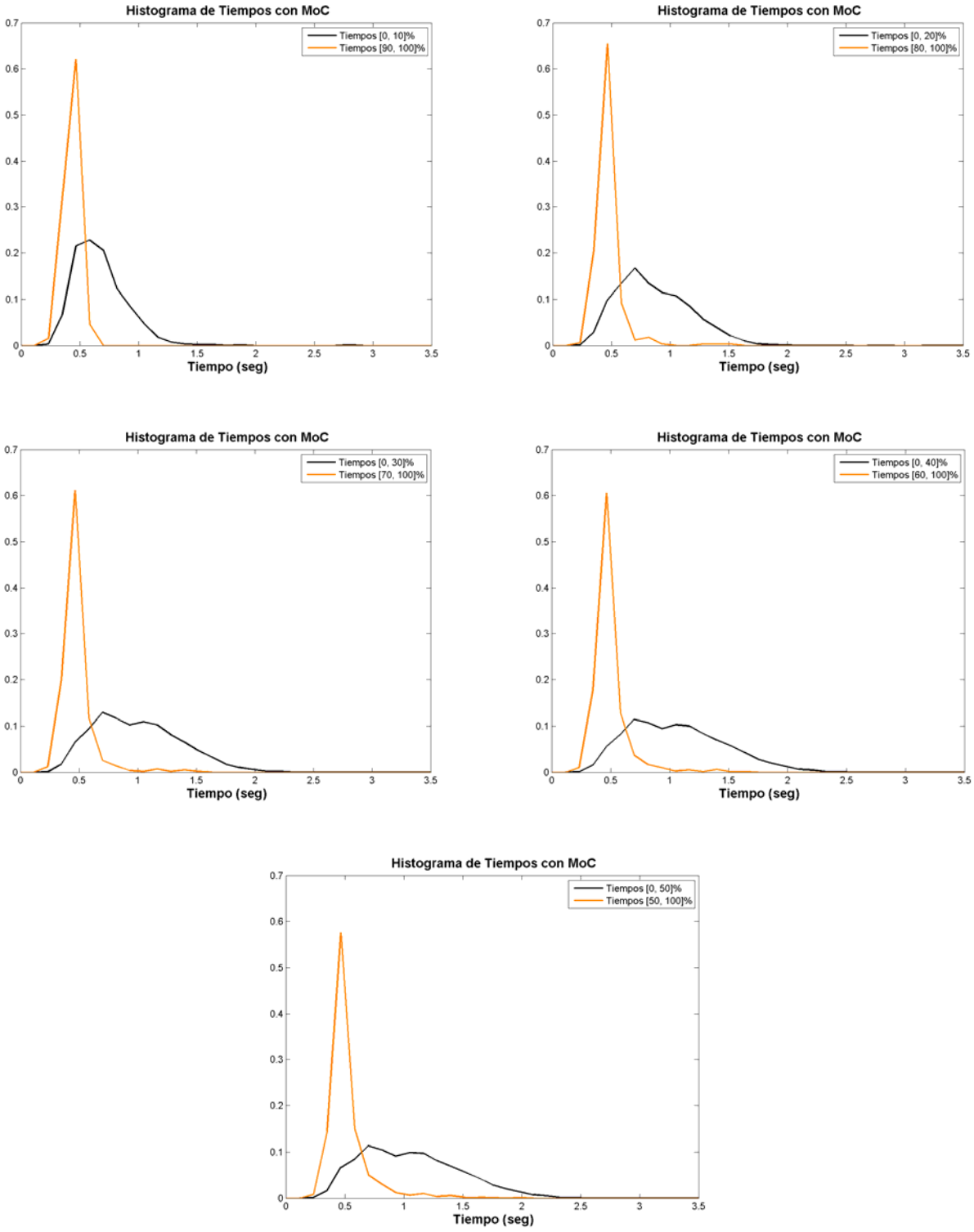


Figura 38: Puntuaciones (izquierda) y Tiempos (derecha) para la división por regiones detallada en la Figura 36 en MoC.

En el caso de la tarjeta inteligente, se puede observar que, para puntuaciones muy alejadas entre sí, como es el caso de la primera división, los tiempos están más solapados que para divisiones posteriores. Se observa en este caso que la fdp de las puntuaciones de la región superior – en naranja - se mantiene prácticamente invariable para las 5 divisiones mostradas, mientras que la fdp de puntuaciones de la región inferior – en negro – sí varía su forma, aunque menos pronunciadamente a partir de la tercera división. Esto implica que el tiempo que tarda el sistema en devolver una puntuación alta es siempre prácticamente el mismo (en torno a 0.5 segundos), mientras que el tiempo que tarda en devolver una puntuación baja varía dependiendo de cómo de baja sea dicha puntuación: cuanto menor la puntuación, más rápida la respuesta, independientemente de que se trate de un usuario o de un impostor. Por otro lado, se observa que los tiempos más pequeños corresponden siempre a puntuaciones mayores - en el software NFIS ocurría justo lo contrario.

Conclusión

Del experimento anterior se deriva que, aunque de un modo diferente que en el NFIS, existe una relación entre el tiempo Tm y la puntuación S: en general, a mayor puntuación (S), menor tiempo de comparación (Tm) es requerido por el sistema.

En el Experimento 2 – sección 6.2 de la memoria – se comprobará si, efectivamente, tal y como parecen mostrar los resultados de este primer experimento, un incremento en la puntuación implica un decremento en el tiempo, relación que podría utilizarse en el desarrollo de un ataque hill-climbing basado en el tiempo de comparación algorítmica.

6.2. Experimento 2: Relación entre la variación del Tiempo y de la Puntuación

En esta segunda prueba trataremos de averiguar si existe alguna relación entre la variación de la puntuación y la variación del tiempo provocada por el cambio de la puntuación, para huellas ligeramente diferentes.

Para llevar a cabo el experimento, tomaremos una huella real y la iremos degradando sucesivamente, al tiempo que observaremos la evolución que siguen puntuación y tiempo. Esto lo repetiremos para un número determinado de huellas originales y permitiremos un número máximo de modificaciones, suficientes para lograr que la puntuación baje hasta valores típicos producidos por dos huellas provenientes de dos usuarios diferentes.

En las gráficas del experimento se representa la evolución de puntuaciones y tiempos tras cada modificación para poder comparar más fácilmente su evolución conjunta. Así, ha de tenerse en cuenta que la escala de representación para la puntuación es distinta de la utilizada para la representación del tiempo. Para una mejor identificación, la escala y la curva de puntuaciones se representan en color azul, y la escala y curva de tiempos en rojo.

En cada iteración modificamos el patrón de entrada mediante una de las cuatro modificaciones planteadas en investigaciones anteriores (34):

A. Perturbar una minucia existente.
B. Añadir una minucia.
C. Sustituir una minucia elegida al azar.
D. Eliminar una minucia.

Dos de estas modificaciones - B y D - incluyen la variación del número de minucias. Precisamente por ello, hay que tener en cuenta que, si el tiempo efectivamente sigue un patrón de variación determinado en nuestro experimento, puede deberse a la variación de la puntuación, a la variación en el número de minucias, o a ambas. Por esta razón, seguiremos también la evolución del número de minucias durante el experimento y la representaremos junto con la evolución del tiempo en color verde.

6.2.1. Resultados para el software NFIS

El experimento se ha llevado a cabo con 50 huellas originales (plantillas), sobre las que se realizan 300 modificaciones. La elección del cambio a realizar en cada iteración se realiza aleatoriamente.

Tras observar los resultados obtenidos, se deduce que, tal y como se podía intuir a partir de los resultados del Experimento 1, para algunas de las huellas escogidas – cuatro de las cuales se muestran en la Figura 39 – existe una tendencia de disminución del tiempo de comparación Tm a medida que la puntuación va disminuyendo. Sin embargo, para otras huellas, la evolución del tiempo de comparación Tm no parece tener ninguna relación con la evolución de la puntuación – ver Figura 40.

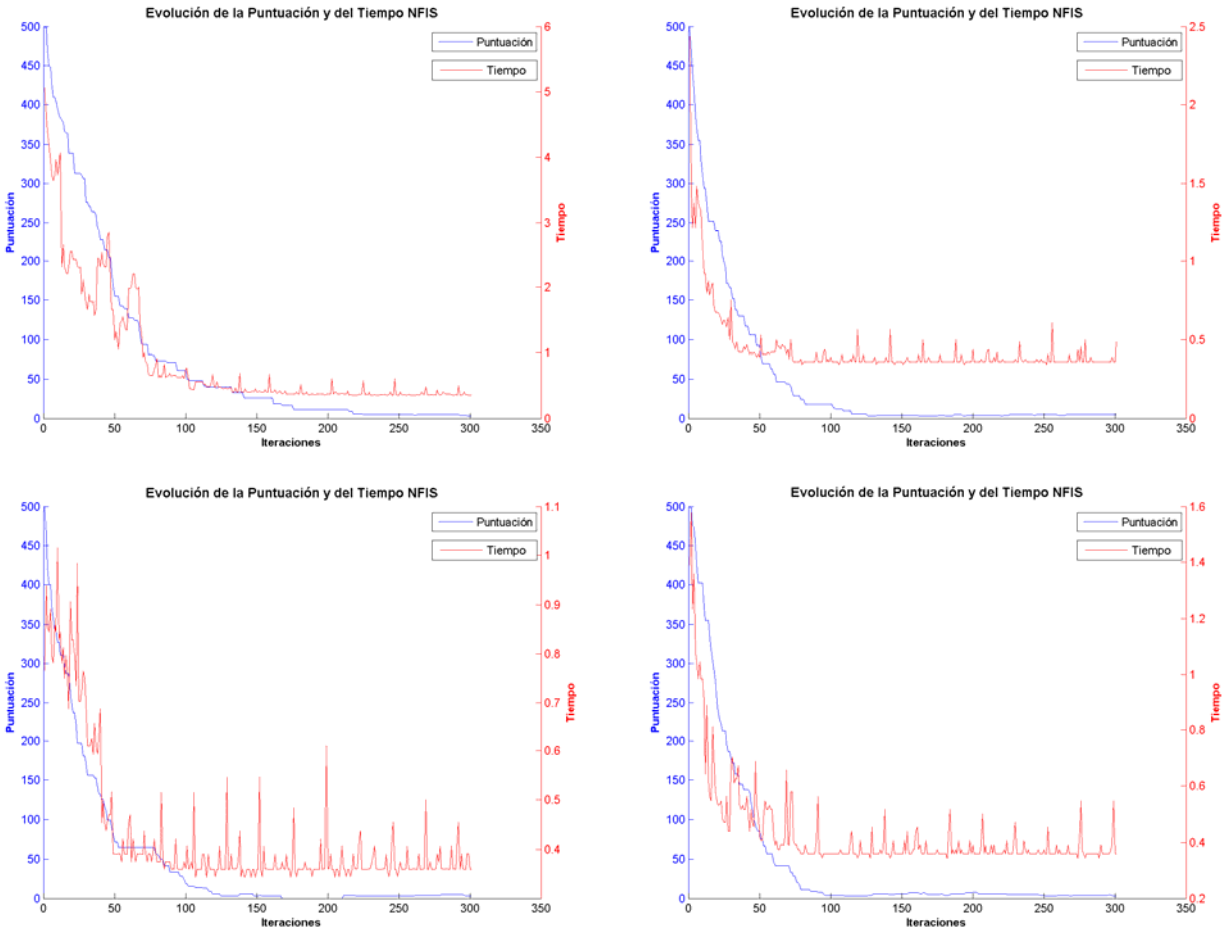


Figura 39 : Ejemplos para el software NFIS de 4 plantillas en las que las evoluciones de la Puntuación y el Tiempo presentan una correlación en su comportamiento: un decremento en la puntuación lleva a una disminución en el tiempo.

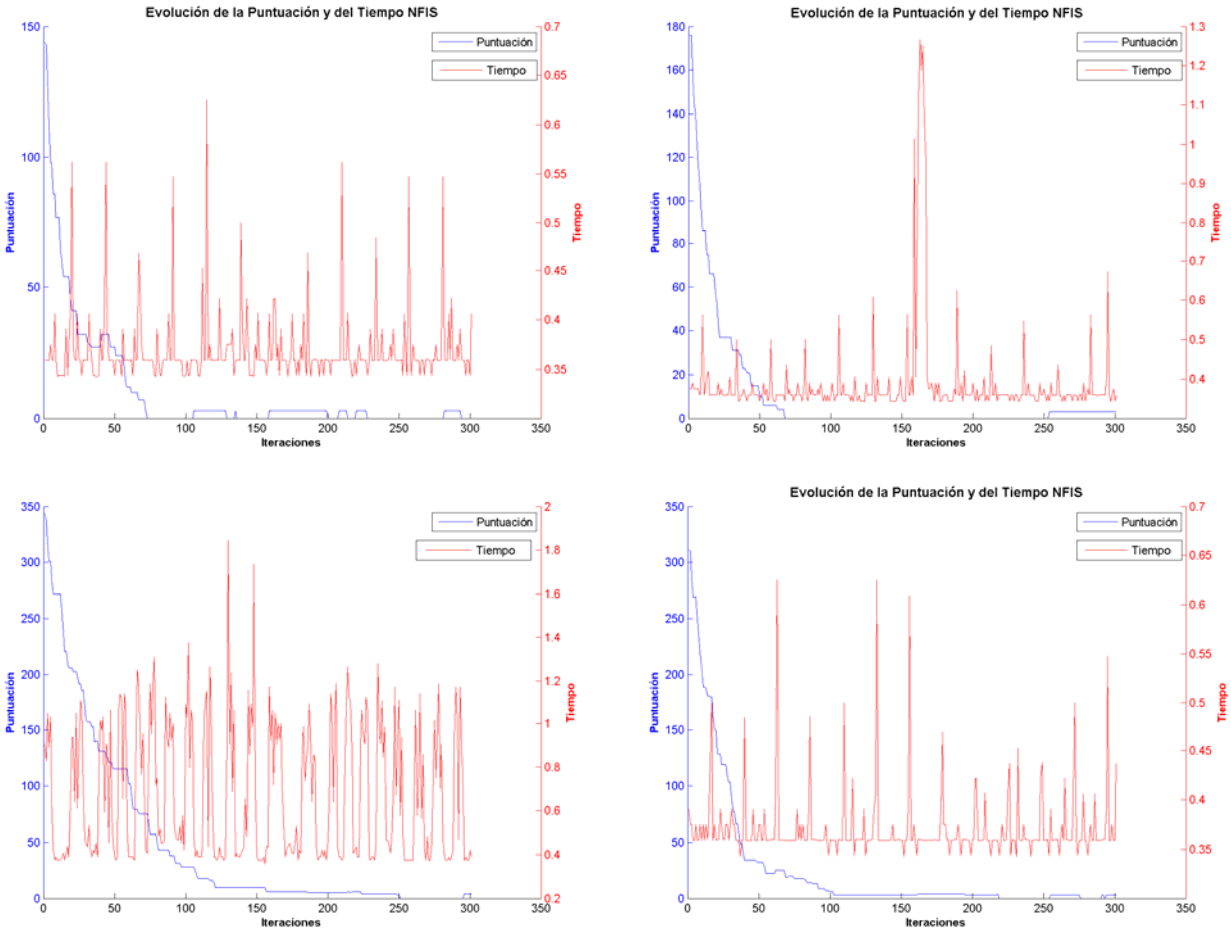


Figura 40 : Ejemplos para el software NFIS de 4 plantillas en las que las evoluciones de la Puntuación y el Tiempo no presentan una correlación aparente.

A la vista de esta disparidad de resultados, y con el objetivo de estudiar ambas evoluciones (puntuación y tiempo) desde un punto de vista estadístico - como corresponde a la naturaleza de los sistemas biométricos -, a continuación se calculan las medias de puntuaciones, tiempos y número de minucias que se obtienen tras cada modificación en las 50 huellas probadas. Las gráficas resultantes de evolución de tiempo frente a puntuación y frente al número de minucias se muestran en la Figura 41.

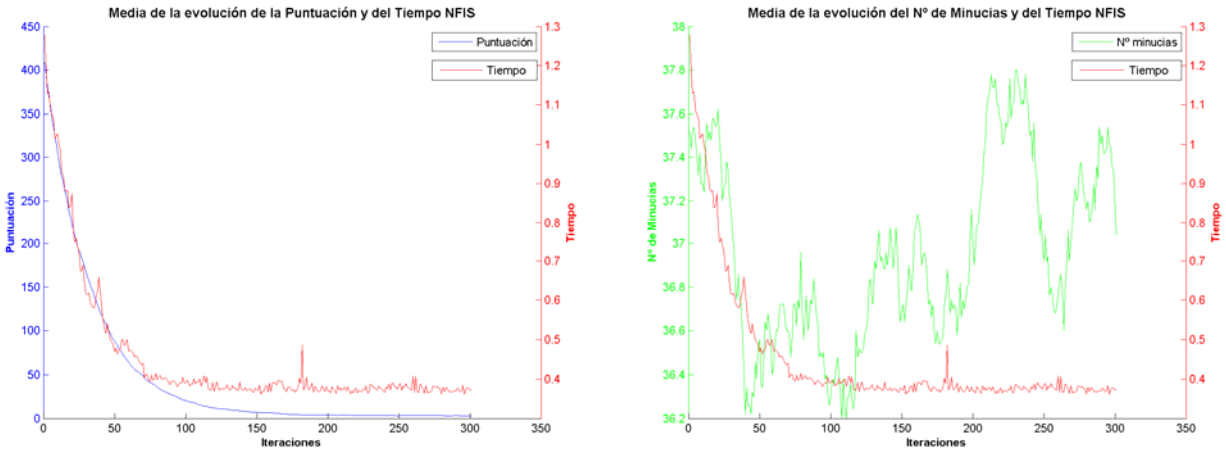


Figura 41: Media de la evolución para el software NFIS de la Puntuación y el Tiempo (izquierda), y del Nº de Minucias y el Tiempo (derecha) de 50 plantillas durante 300 modificaciones.

En la Figura 41 izquierda se observa que, hasta una puntuación de 50 aproximadamente, existe una clara correlación entre puntuaciones y tiempos, de tal forma que, a medida que disminuye la puntuación, lo hace también el tiempo. Sin embargo, también es posible apreciar que, cuando la puntuación baja de este punto, esta relación desaparece, pues, si bien la puntuación sigue bajando, el tiempo permanece prácticamente invariante, fluctuando alrededor de un valor. Este resultado implica, por tanto, que existe un valor de puntuación por debajo del cual el valor de la puntuación y el tiempo que el sistema tarda en calcularla son independientes.

Podríamos, entonces, caracterizar el sistema con dos regiones de funcionamiento: una para puntuaciones altas, en la que es posible extraer una relación entre tiempo y puntuación – una disminución de la puntuación produce una disminución del tiempo -; y otra región para puntuaciones bajas, en la cual el tiempo tiene un comportamiento independiente de la puntación. Una consecuencia de este resultado es que un ataque *hill-climbing* basado en el tiempo sólo podría tener éxito, en principio, en la zona de puntuaciones altas, donde puntuación y tiempo sí están relacionados.

Otro aspecto a señalar es que el hecho de añadir o quitar minucias aleatoriamente - tal y como se describe en la sección 6.2 - no influye en el comportamiento del tiempo de comparación, pues, como se observa en la Figura 41 derecha, un aumento o disminución del número de minucias no repercute en el tiempo medio de comparación.

No obstante, para descartar la influencia del número de minucias sobre la evolución del tiempo de comparación observado en la Figura 41, se ha repetido el experimento permitiendo realizar sólo las modificaciones: A) Perturbar minucia existente y C) Sustituir minucia elegida al azar; es decir, manteniendo el número de minucias constante durante todo el experimento.

Los resultados obtenidos – ver Figura 42 - confirman que, efectivamente, el número de minucias de la huella no influye en el tiempo que tarda el sistema en devolver la puntuación y que, por lo tanto, sí existe una relación considerable entre puntuación y tiempo, independientemente del número de minucias, al menos en la mencionada región de puntuaciones altas.

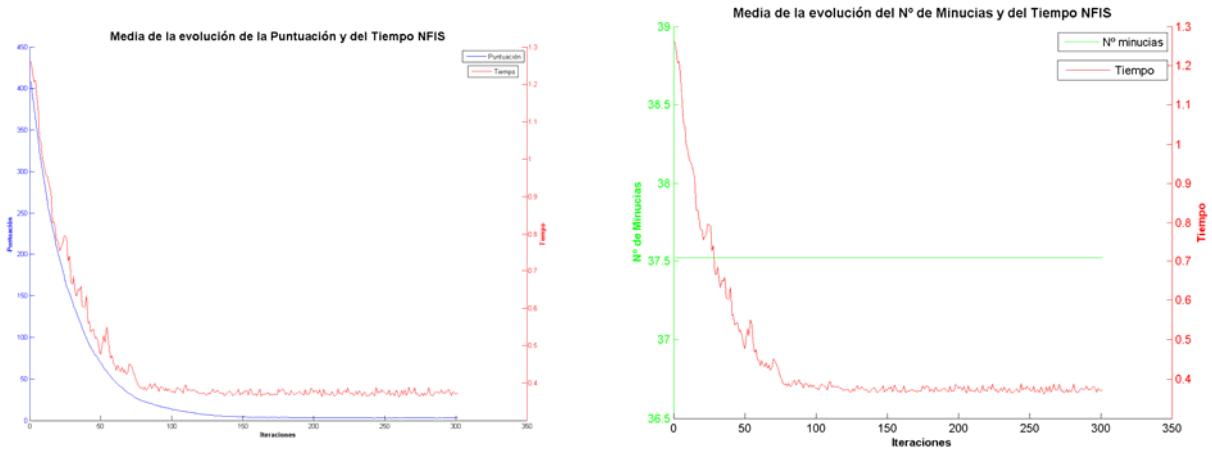


Figura 42: Media de la evolución para el software NFIS de Puntuación y Tiempo (izquierda), y Nº de Minucias y Tiempo (derecha) de 50 plantillas durante 300 modificaciones y con el nº de minucias constante.

Conclusión

A partir de los resultados mostrados, se puede concluir que en el sistema NFIS, y siempre desde un punto de vista promedio, el tiempo disminuye cuando lo hace la puntuación hasta un valor determinado – alrededor de 50 -, sin que el número de minucias tenga influencia en este comportamiento; y que, por debajo de este valor, puntuación y tiempo son independientes.

6.2.2. Resultados para el sistema MoC

Este experimento se ha realizado sobre las mismas 50 plantillas utilizadas con el NFIS, permitiendo un máximo de 100 modificaciones (suficientes para alcanzar una puntuación típica de dos huellas de usuarios diferentes). El algoritmo de modificación de huella es el mismo que el que se utilizó para NFIS, si bien se ha observado que la puntuación no disminuye de un modo tan lineal como lo hacía en aquél. Por otra parte, en las gráficas se puede apreciar que esta puntuación presenta habitualmente un salto brusco en su evolución, ocasionado, probablemente, por el fuerte comportamiento bimodal del sistema MoC que ya habíamos observado en las Figuras 31 y 32. Todo esto puede ser un indicativo de que el algoritmo de comparación que otorga la puntuación de la huella en la tarjeta es más sencillo que el del sistema del NIST – tal y como cabe esperar en una aplicación MoC con fuertes restricciones hardware.

Algunos de los resultados obtenidos para plantillas individuales parecen indicar que el tiempo sufre una evolución contraria a la puntuación, es decir, aumenta cuando ésta disminuye - tal y como se puede observar en la Figura 43.

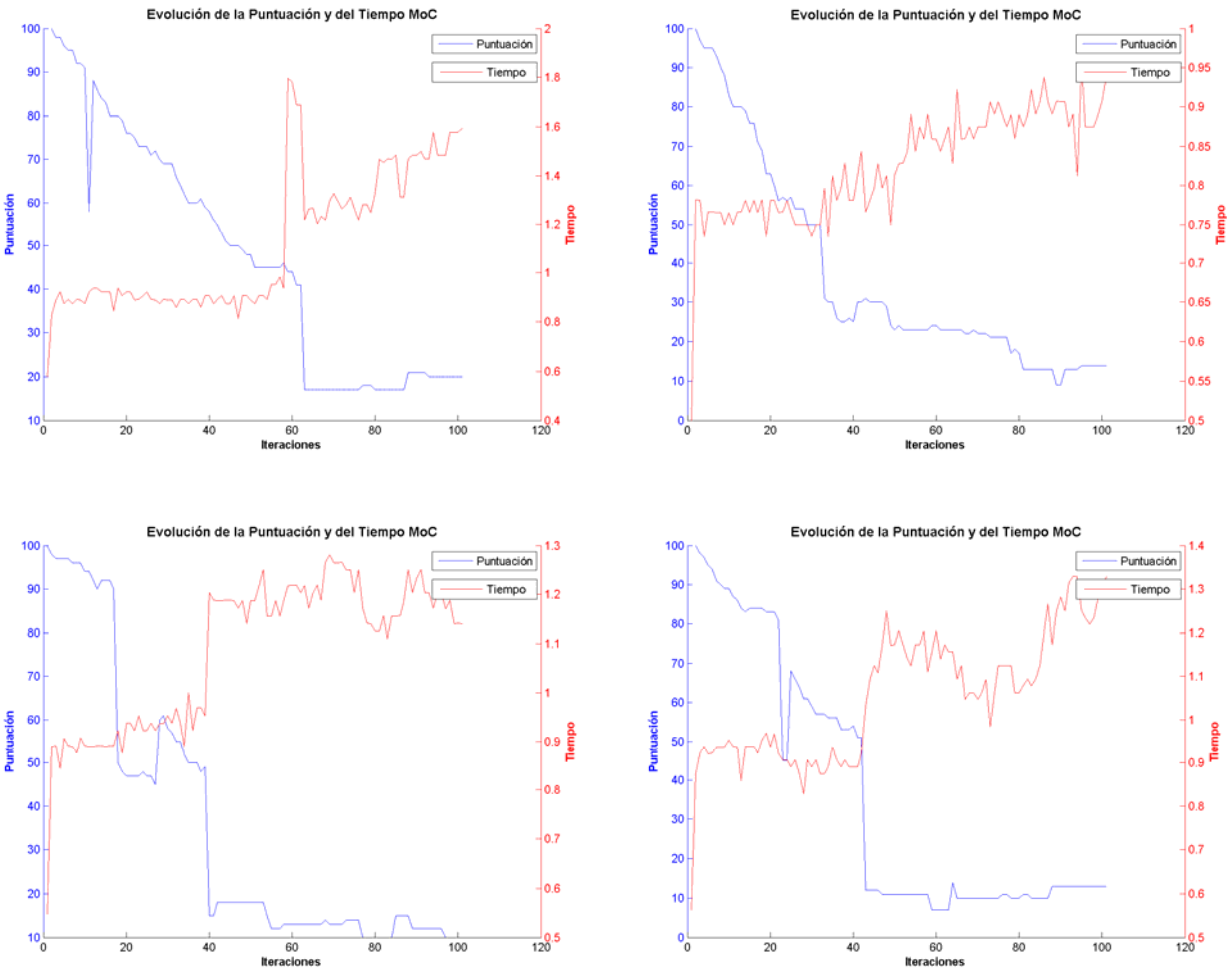


Figura 43: Ejemplos para el sistema MoC de 4 plantillas en las que las evoluciones de Puntuación y Tiempo presentan correlación en su comportamiento: un decremento en la puntuación lleva a un aumento del tiempo.

Sin embargo, al igual que sucedía con el sistema NFIS, en las gráficas generadas para varias de las 50 plantillas utilizadas no parece existir ninguna relación entre puntuación y tiempo – ver Figura 44.

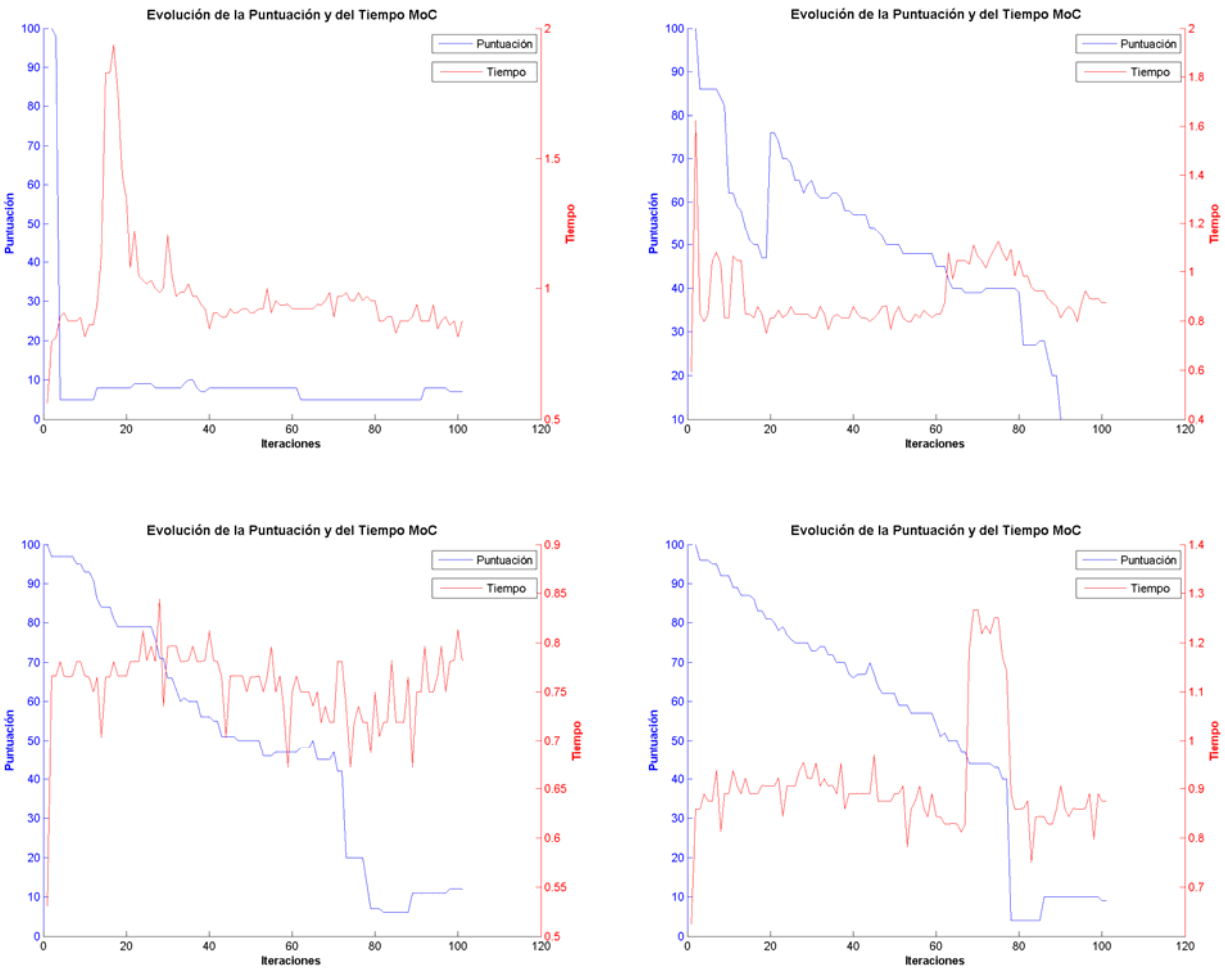


Figura 44: Ejemplos para el sistema MoC de 4 plantillas en las que las evoluciones de Puntuación y Tiempo parecen independientes.

Así pues, para analizar el problema desde un punto de vista promedio – y no desde la perspectiva de las particularidades de cada caso –, se ha calculado la media de la puntuación, el tiempo y las minucias en cada una de las 100 iteraciones para las 50 huellas consideradas. Estos resultados promedio se muestran en la Figura 45.

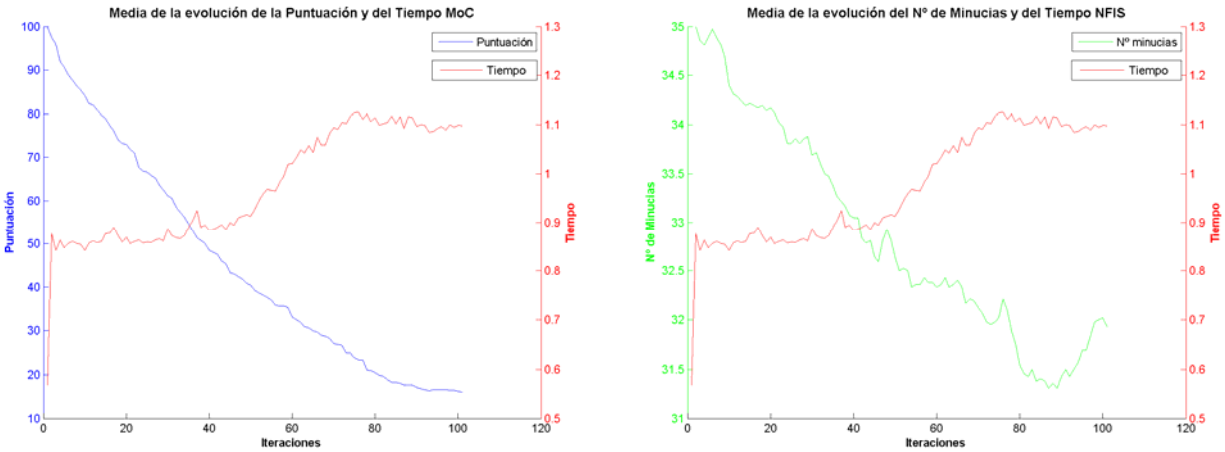


Figura 45: Media de la evolución para el sistema MoC de Puntuación y Tiempo (izquierda), y Nº de Minucias y Tiempo (derecha) de 50 plantillas durante 100 modificaciones.

Como se observa en la Figura 45 izquierda, parece que, en media, el tiempo aumenta cuando disminuye la puntuación. Sin embargo, a la vista de la gráfica del número de minucias frente al tiempo – Figura 45 derecha -, no queda claro que este comportamiento del tiempo no esté motivado por la variación del número de minucias.

Para descartar la influencia del número de minucias, se ha repetido el mismo experimento manteniendo el número de minucias constante para cada huella probada, es decir, sólo se permiten las modificaciones A) Perturbar minucia existente y C) Sustituir minucia elegida al azar.

Los resultados de la ejecución de esta versión modificada del experimento demuestran que el número de minucias no es el factor que determinaba el comportamiento del tiempo, como se puede observar en la Figura 46.

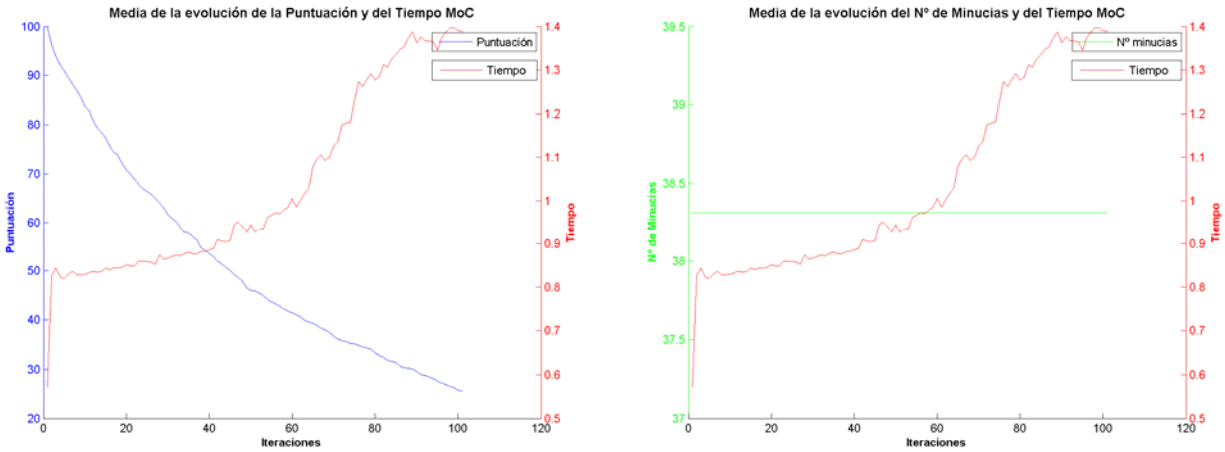


Figura 46: Media de la evolución para el sistema MoC de Puntuación y Tiempo (izquierda), y Nº de Minucias y Tiempo (derecha) de 50 huellas durante 100 modificaciones, manteniendo el nº de minucias constante.

Conclusión

Podemos concluir, entonces, que para el sistema MoC, al menos a nivel promedio, un decremento en la puntuación implica un incremento del tiempo, independientemente del número de minucias.

Debemos añadir que, si bien, tanto en la Figura 41 (NFIS) como en la 45 (MoC), se aprecia claramente que el tiempo sigue un patrón de comportamiento dependiente de la puntuación, es importante tener en cuenta que estas figuras muestran una media estadística, es decir, un comportamiento general y probabilístico de dicho tiempo frente a la puntuación, lo cual no asegura que al atacar una huella en particular el tiempo siga esta misma tendencia.

6.3. Conclusiones del análisis temporal de los sistemas

A tenor de los resultados obtenidos tras la realización de los Experimentos 1 y 2 (análisis temporal de ambos sistemas), podemos concluir que existe una relación patente entre tiempo y puntuación y, por tanto, existe un riesgo potencial de que ambos sistemas sean vulnerables a algún tipo de ataque side-channel basado en tiempo, como, por ejemplo, el ataque hill-climbing descrito en la sección 5.4 y cuyos resultados se presentan en el siguiente capítulo.

7. Resultados de los ataques

Tal y como ya se describió en la sección 5.4, el ataque base implementado es de tipo ***hill-climbing*** y está basado en un algoritmo propuesto en (13) y mejorado en (34). No obstante, en nuestro caso, no nos basaremos en la puntuación devuelta por el sistema – no siempre accesible - para realizar las modificaciones en las plantillas sintéticas, sino en el tiempo de comparación – parámetro mucho más sencillo de obtener que la puntuación.

Como ya se explicó en la descripción del algoritmo – sección 5.4 –, el ataque comenzará con la creación de 100 plantillas sintéticas que serán enviadas al comparador y entre las que se elegirá aquélla que presente un mejor comportamiento en base a las conclusiones extraídas de los experimentos llevados a cabo en el capítulo 6. El criterio de selección será entonces:

- **Sistema NFIS**: nos quedaremos con la plantilla sintética que genere un mayor tiempo de comparación – que, en principio, también será aquélla que genere una puntuación más alta.
- **Sistema MoC**: nos quedaremos con la plantilla sintética que genere un tiempo menor – ya que los resultados experimentales descritos en el capítulo 6 sugerían que a este tiempo le corresponde la mayor puntuación.

Los ataques se lanzarán sobre T plantillas de la base de datos y, en ocasiones, se partirá de una puntuación predefinida alrededor de un valor S_{ini}.

Se permitirán exclusivamente dos tipos de modificaciones sobre estas plantillas:

- Añadir una nueva minucia.
- Sustituir una minucia elegida al azar.

En cada iteración del algoritmo, el cambio puede ser aceptado o no. Esta decisión se tomará en función de la media de los M últimos tiempos obtenidos y, teniendo en cuenta los resultados experimentales extraídos del análisis del temporal de ambos sistemas - descrito en el capítulo 6 -, el criterio seguido para aceptar o desechar los sucesivos cambios será el siguiente:

- **Sistema NFIS**: los cambios serán aceptados si provocan un aumento en Tm – lo que, según el análisis temporal previo, debería implicar un aumento en la puntuación.
- **Sistema MoC**: los cambios serán aceptados si el tiempo de comparación disminuye – lo que, según el análisis temporal previo, debería implicar un aumento en la puntuación.

Se establece un umbral de puntuación U y un número máximo de Q intentos de modificación. Si se supera alguno de ellos, el algoritmo se detiene.

El número medio de intentos que necesita un ataque por fuerza bruta para romper la cuenta de un usuario puede deducirse a partir de la FAR del sistema.

$$N_{fuerza\_bruta} = \frac{100}{FAR\ (\%)}$$

Para el sistema NFIS, se considera que un umbral de puntuación U de 35 presenta una FAR y una FRR razonables de 0.1% y 3.33%, respectivamente. Así pues, el número medio de iteraciones que un ataque por fuerza bruta necesitará para vulnerar este sistema será:

$$N_{fuerza\_bruta\_NFIS} = \frac{100}{0{,}1} = 1000\ iteraciones$$

Para el sistema MoC, por su parte, se ha elegido un umbral de puntuación U de 55, que conlleva una FAR de 0.16% y una FRR de 17.33%. Por ello, el número medio de iteraciones que un ataque por fuerza bruta necesitará para romper este sistema será:

$$N_{fuerza\_bruta\_MoC} = \frac{100}{0{,}16} = 625\ iteraciones$$

Hay que tener en cuenta que la FAR se calcula a partir de plantillas reales, mientras que los ataques se llevan a cabo mediante plantillas sintéticas, de forma que la comparación entre ambos no es directa. Por último, se ha considerado que un número máximo de 10.000 iteraciones permitidas (Q) es adecuado para ambos sistemas.

7.1. Ataque 1: Ataque básico

En este ataque los parámetros definidos en la introducción del capítulo toman los siguientes valores:

- Plantillas: T = 50.
- Iteraciones: Q = 10.000.
- Cambios: M = 1.

7.1.1 Resultados para el software NFIS

- Umbral: U = 35.

Al finalizar este primer ataque comprobamos que nuestro algoritmo no ha sido capaz de atacar con éxito ninguna de las 50 huellas.

Observamos que la puntuación prácticamente no varía durante el ataque, sino que oscila tomando valores muy bajos. En concreto, al patrón de minucias que elegimos como inicial - el que nos da un tiempo mayor - para la primera huella atacada, le corresponde una puntuación de 3; tras 10.000 iteraciones, dicha puntuación ha tomando casi siempre valores comprendidos entre 0 y 3. El resto de huellas sufren situaciones similares respecto a la puntuación. El tiempo, por su parte, también se mantiene oscilando alrededor de un mismo valor a lo largo de todo el ataque.

En la Figura 47 se muestran cuatro ejemplos de progresión de la puntuación y del tiempo a lo largo del primer ataque a NFIS.

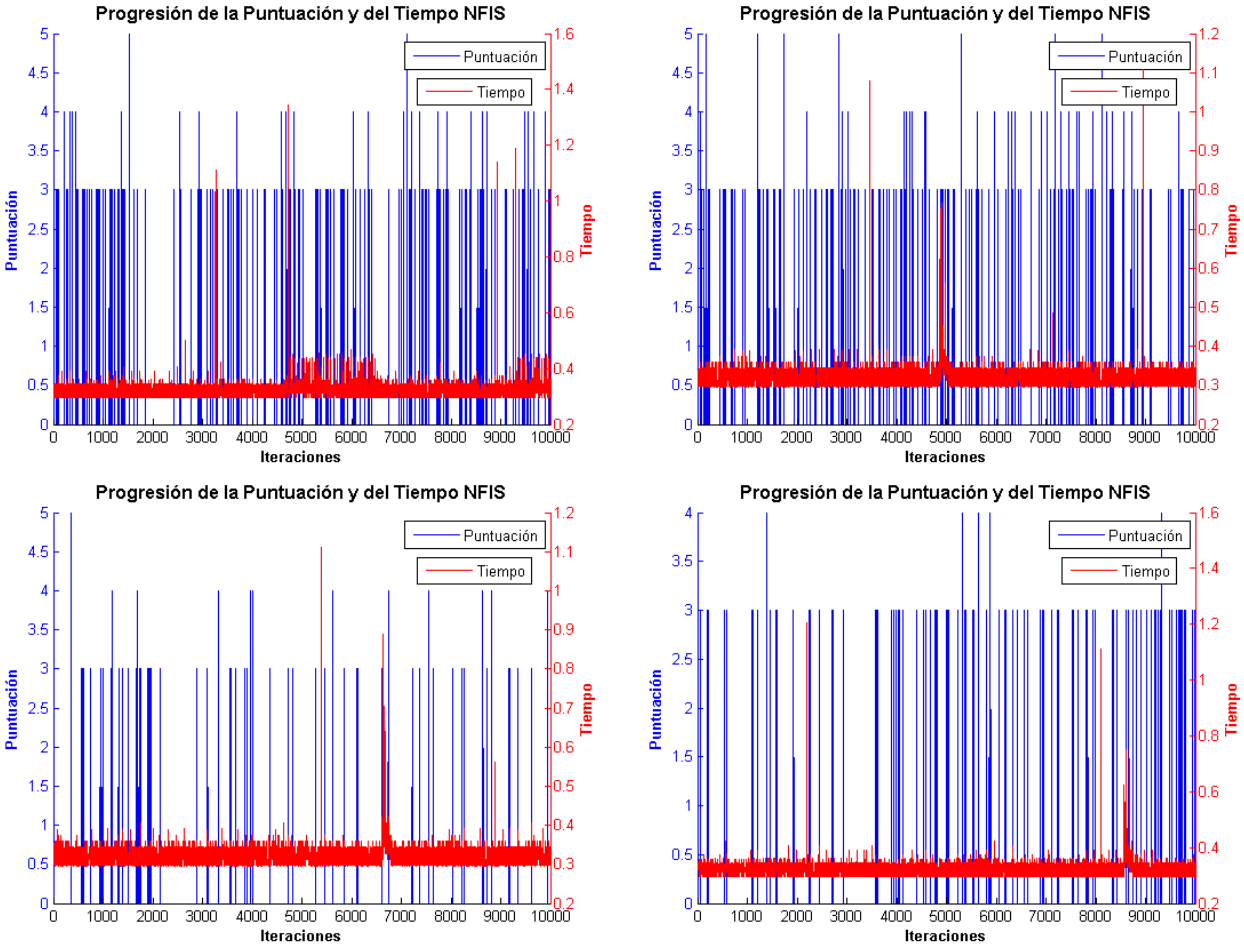


Figura 47 : Ejemplos de la progresión de la Puntuación y del Tiempo en el Ataque 1 a NFIS

El hecho de que la puntuación oscile en torno al valor con el que se inicia el experimento – una puntuación baja -, confirma las conclusiones extraídas del Experimento 2 (relación entre ΔS y ΔTm), en el que observábamos que, si bien, cuando la puntuación es alta, el tiempo parece seguir la tendencia de ésta, es decir, disminuye cuando ésta disminuye; cuando la puntuación es menor que cierto valor, el tiempo se estabiliza y oscila alrededor de un valor determinado, de forma que su comportamiento es independiente de la puntuación – ver Figura 41.

Conclusión

Observando los resultados, lo que parece estar ocurriendo es que nuestro ataque comienza con un valor de puntuación bajo y se queda estancado en los alrededores de esa puntuación, con lo que no somos capaces de romper el sistema. Observando la Figura 41 podemos afirmar que, aunque nuestra puntuación inicial fuera relativamente alta – por ejemplo, 15 –, tampoco seríamos capaces de atacar con éxito el sistema, porque seguiríamos encontrándonos en la región de funcionamiento en la que el tiempo es independiente de la puntuación.

7.1.2. Resultados para el sistema MoC

- Umbral: U = 55.

Como ocurría para en el ataque al sistema del NIST, tampoco los ataques implementados sobre la tarjeta inteligente logran romper ninguna de las 50 huellas probadas. Además, se observa que la puntuación y el tiempo no siguen el comportamiento que cabría esperar a la vista de la Figura 45 - aumentar y disminuir, respectivamente.

En la Figura 48 se muestran cuatro ejemplos de progresión de la puntuación y del tiempo a lo largo del primer ataque a MoC.

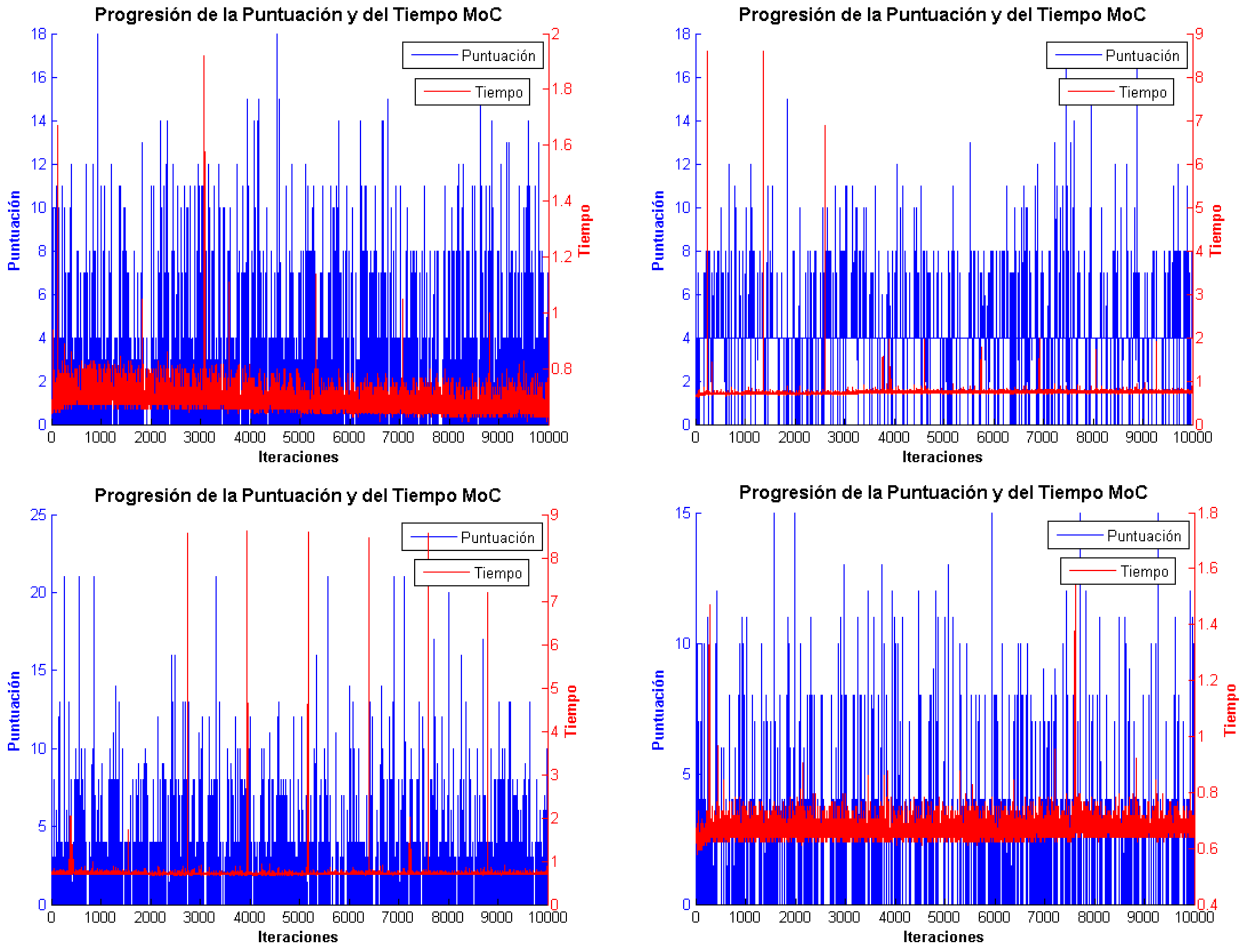


Figura 48 : Ejemplos de la progresión de la Puntuación y del Tiempo en el Ataque 1 a MoC

Tomando como tiempo inicial el menor de los 100 correspondientes a los candidatos creados inicialmente, la puntuación correspondiente es relativamente baja. No obstante, es interesante observar que, al contrario de lo que ocurría con el software NIST, en cuyo ataque la puntuación permanecía siempre en valores muy bajos, en el ataque a la tarjeta inteligente se llegan a obtener puntuaciones relativamente altas – en torno a 20. Sin embargo, más que ser el resultado de una evolución continuada y corresponderse con tiempos cada vez más bajos, parece que estas puntuaciones altas se consiguen de forma aleatoria. Este hecho puede ser un indicativo de que el sistema de tarjeta

inteligente es más susceptible de cometer errores que el sistema del NIST, como ya se observaba en la Figura 33.

7.2. Ataque 2: Ataque a la región de puntuaciones altas

Teniendo en cuenta que atacar las huellas en la región de puntuaciones bajas del sistema NFIS2 no ha tenido éxito, probaremos ahora a atacar el sistema en la región de puntuaciones altas, donde, en principio, tiempo y puntuación están correlacionados – ver Figura 41. Así, partiremos de una huella con una puntuación inicial alta e intentaremos hacer subir esta puntuación hasta el umbral de decisión U.

Para generar el patrón inicial de minucias con una puntuación inicial alta, partimos de una huella original y le aplicamos el siguiente algoritmo:

1. Modificación de la huella mediante uno de los siguientes cambios:
    a. Perturbar minucia.
    b. Añadir minucia.
    c. Sustituir minucia.
    d. Eliminar minucia.
2. Obtención de la nueva puntuación de la huella modificada.
    a. Si la puntuación es mayor que S_{ini}, volvemos al paso 1.
    b. Si la puntuación es menor o igual que S_{ini}, continuamos al paso 4.
3. Almacenamiento del patrón de minucias final obtenido y comienzo del ataque a partir de éste

Una vez que hemos generado este primer patrón de minucias con puntuación inicial alta, pasaremos a ejecutar el algoritmo ***hill-climbing*** descrito en la sección 5.4, obviando los pasos de generación de 100 plantillas sintéticas y elección de la mejor de ellas – que ya no son necesarios.

Este ataque sólo se lleva a cabo sobre el sistema NFIS y los parámetros descritos al inicio del capítulo toman los siguientes valores:

- Plantillas: T = 50.
- Iteraciones: Q = 10.000.
- Cambios: M = 1.
- Puntuación inicial: S_{ini} = 100.
- Umbral: U = 300.

7.2.1. Resultados para el software NFIS

De las 50 huellas atacadas, en ningún caso se logra sobrepasar el umbral establecido después de 10.000 intentos de modificación, aunque sí se observa que la puntuación sube acorde con el tiempo durante un número considerable de iteraciones.

En la Figura 49 se muestran cuatro ejemplos de progresión de la puntuación y del tiempo a lo largo del segundo ataque a NFIS.

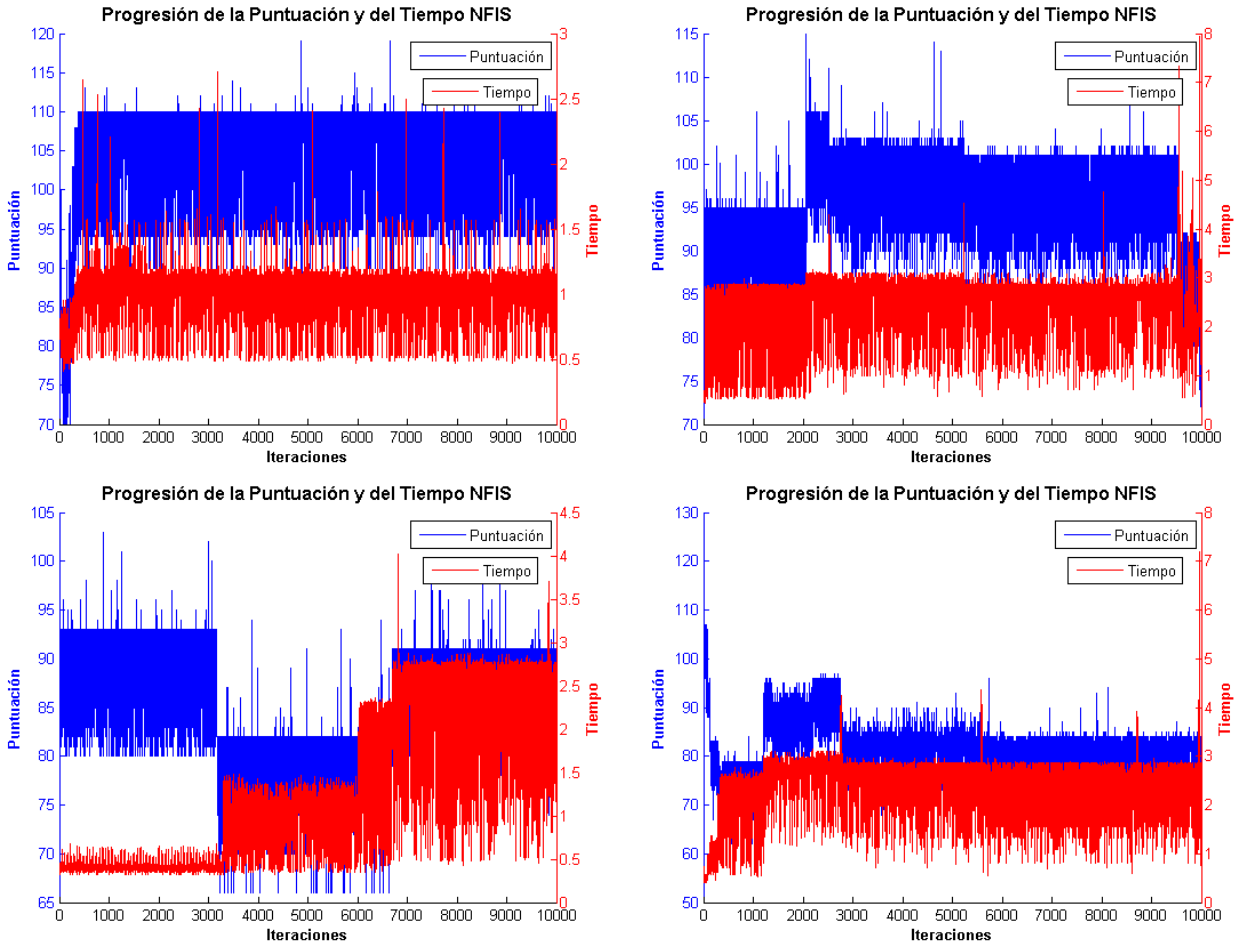


Figura 49: Ejemplos de la progresión de la Puntuación y del Tiempo en el Ataque 2 a NFIS

Conclusión

Teniendo en cuenta los resultados obtenidos hasta ahora, podemos concluir que puntuación y tiempo están más correlacionados cuando trabajamos con puntuaciones altas – tal y como se había observado en los resultados del Experimento 2 -, pero no lo suficiente como para que el ataque tenga éxito.

7.3. Ataque 3: Ataque utilizando valores medios

Como vemos, los ataques implementados hasta ahora no han sido capaces de romper ninguno de los dos sistemas probados. Una posible razón que explique esta situación es que, como se observaba en las figuras del Experimento 2 – de la 39 a la 46 -, el tiempo tiene en promedio un comportamiento ascendente (NFIS) – Figura 41 - o descendente (MoC) – Figura 45 - respecto a la puntuación, pero oscila considerablemente en lo que a sus valores concretos se refiere.

Por este motivo, intentaremos atacar el sistema utilizando las medias de ciertos valores de tiempo, en lugar de cada valor concreto. Así, dejaremos que nuestro algoritmo de ataque realice M cambios seguidos y elija quedarse con dichos cambios si la media de los tiempos obtenidos tras cada uno de esos M cambios mejora la media correspondiente a los últimos cambios aceptados.

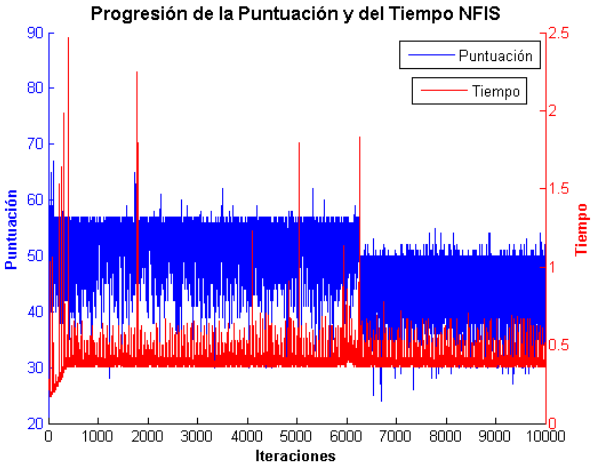
Ya que parece más probable tener éxito en el ataque trabajando en regiones de puntuación altas, trabajaremos en esa región de puntuaciones, empleando el mismo método de generación del patrón inicial de minucias con puntuación elevada que describíamos en la sección 7.2 (Ataque 2).

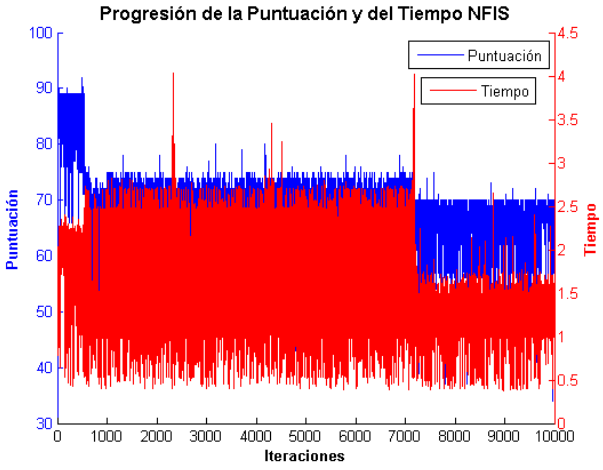
Este ataque sólo se realiza sobre el software NFIS y las características del ataque son las siguientes:

- Plantillas: T = 20.
- Iteraciones: Q = 10.000.
- Puntuación inicial: S_{ini} = 100.
- Umbral: U = 200.
- Cambios: M = 5, 10.

7.3.1. Resultados para el software NFIS

En las Figuras 50 y 51 se muestran los resultados obtenidos para este experimento sobre el software NFIS con M igual a 5 y 10, respectivamente.





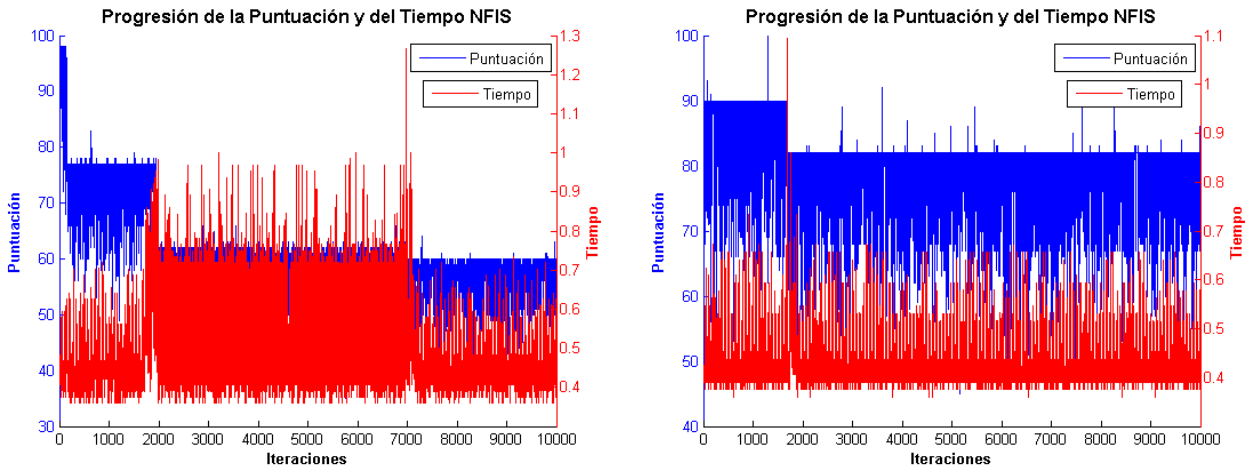


Figura 50 : Ejemplos de progresión de la Puntuación y del Tiempo en el Ataque 3 a NFIS con M=5.

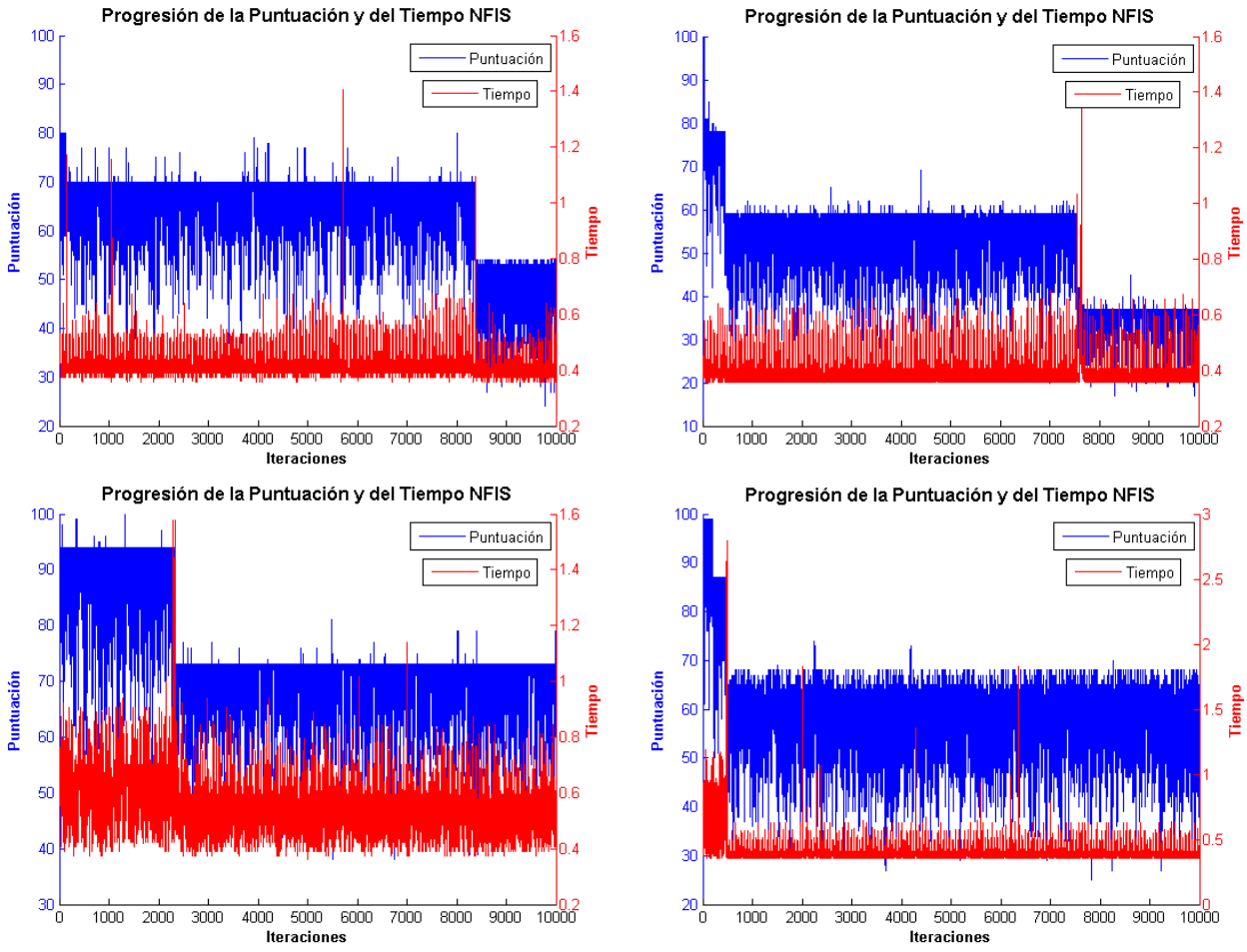


Figura 51 : Ejemplos de progresión de la Puntuación y del Tiempo en el Ataque 3 a NFIS con M=10.

Sólo se ha realizado este experimento permitiendo 5 o 10 cambios a la vez – Figuras 50 y 51, respectivamente -, ya que, teniendo en cuenta que estamos trabajando con plantillas sintéticas que inicialmente constan de 38 minucias, permitir más de 10 cambios de una vez sería prácticamente como crear una nueva plantilla en cada iteración, lo que lo convertiría en un ataque por fuerza bruta.

Conclusión

Si bien, como se observaba en la Figura 41, el tiempo de comparación tiene en promedio una clara relación con la puntuación, no parece que trabajar con valores medios de los tiempos obtenidos tras M cambios mejore el ataque.

8. Conclusiones y trabajo futuro

8.1. Conclusiones

Con el objetivo de comprobar la viabilidad teórica de implementar ataques *hill-climbing* basados en el tiempo que tarda el comparador de un sistema biométrico en generar la puntuación del patrón de minucias de entrada - en lugar de en la propia puntuación -, se ha llevado a cabo una revisión del estado del arte, por un lado, de las vulnerabilidades de los sistemas biométricos en general, prestando especial atención a los conocidos como ataques *hill-climbing*; y, por otro lado, de los ataques conocidos en criptografía como *timing-attacks* - pertenecientes a la categoría de ataques *side-channel*.

Tras el estudio, ha quedado establecido que, tanto los ataques *hill-climbing* sobre sistemas de reconocimiento automático de huella dactilar, como los *timing-attacks* sobre sistemas criptográficos, tienen un éxito probado, con lo que se plantea la posibilidad de implementar ataques *hill-climbing* basados en tiempo sobre sistemas de reconocimiento biométrico de huella.

Para establecer las vulnerabilidades concretas de tipo temporal que presentan ciertos sistemas de reconocimiento de huella, se ha decidido llevar a cabo un análisis temporal de dichos sistemas, con el objetivo de utilizar los conocimientos adquiridos en dicho análisis para el desarrollo de ataques *hill-climbing* basados en tiempo.

Los dos **sistemas** analizados y atacados son:

- **NFIS:** software de referencia en verificación de huella dactilar, creado por el NIST americano. Ver sección 5.1.1.
- ***Match-on-Card*:** sistema integrado de tarjeta inteligente. Ver sección 5.1.2.

La **base de datos** de huellas empleada durante toda la parte experimental del proyecto es un subconjunto de la base de datos del MCYT que consta de un total de 1500 huellas (75 usuarios, 10 muestras, 2 dedos, 1 sensor), a partir de las cuales hemos obtenido 22.350 puntuaciones de impostores y 1.350 puntuaciones de usuarios. Tras el análisis del rendimiento de los sistemas se observa que el sistema NFIS tiene un mejor rendimiento que el sistema MoC, el cual presenta, por otro lado, dos modos de funcionamiento bien diferenciados – dependiendo de si nos encontramos en el rango de puntuaciones típico de impostor o de usuario.

Para el **análisis temporal de los sistemas** hemos llevado a cabo dos experimentos. El primero de ellos - sección 6.1 de la memoria - tiene como objetivo establecer una relación directa entre el tiempo del comparador y la puntuación obtenida. Tras su realización, se concluye que en el sistema NFIS existe una correlación clara entre el tiempo de comparación y la puntuación devuelta por el sistema: a mayor puntuación, en general, mayor tiempo de comparación. En el sistema MoC, por su parte, se observa que, aunque de manera menos clara que en el NFIS, existe también una relación entre el tiempo y la puntuación: en general, a mayor puntuación, menor tiempo de comparación es requerido por el sistema.

En el segundo experimento – sección 6.2 de la memoria – se pretende comprobar si, efectivamente, tal y como parecen mostrar los resultados del primer experimento, existe

alguna relación entre la variación de la puntuación y la variación del tiempo provocada por el cambio de la puntuación de huellas ligeramente diferentes. Para llevar a cabo el experimento se aplica sobre las huellas un algoritmo de degradación.

A la vista de la disparidad de resultados para cada caso concreto (cada huella), y con el objetivo de estudiar las evoluciones de puntuación y tiempo desde un punto de vista estadístico - como corresponde a la naturaleza de los sistemas biométricos -, se calculan las medias de puntuaciones, tiempos y número de minucias que se obtienen tras cada paso del algoritmo de degradación.

Descartada la influencia del número de minucias en el comportamiento del tiempo, se concluye que, en el sistema NFIS, y siempre desde un punto de vista promedio, el tiempo disminuye cuando lo hace la puntuación hasta un valor determinado (alrededor de 50) y que, por debajo de este valor, puntuación y tiempo son independientes. Para el sistema MoC, se observa que, al contrario de lo que sucede en el sistema del NIST, el tiempo aumenta cuando disminuye la puntuación.

Es importante tener en cuenta que, para ambos sistemas, ya que estamos hablando de comportamientos a nivel promedio, no podemos asegurar que al atacar una huella en particular se cumplan las tendencias esperadas.

Una vez llevado a cabo el análisis temporal de los sistemas mediante dos experimentos concretos, podemos concluir que existe una relación patente entre tiempo y puntuación y, por tanto, existe un riesgo potencial de que ambos sistemas sean vulnerables a algún tipo de ataque *side-channel* basado en tiempo. Hemos establecido, además, qué relaciones concretas existen entre la puntuación devuelta por el sistema y el tiempo que tarda éste en generarla, con lo que ya estamos en disposición de desarrollar **ataques *hill-climbing*** que exploten esta vulnerabilidad temporal.

El algoritmo de ataque *hill-climbing* implementado en este proyecto es una versión del algoritmo propuesto en (13), que incluye, además, las mejoras propuestas en (34) y que está adaptado para atacar en función del tiempo, en lugar de en función de la puntuación – ver sección 5.4 para mayores detalles sobre el algoritmo.

Se lleva a cabo un primer ataque sobre el sistema MoC – ver sección 7.1 -, aunque no se logra romper ninguna de las huellas atacadas, y la puntuación y el tiempo no siguen el comportamiento que cabría esperar a la vista de resultados anteriores (aumentar y disminuir, respectivamente). Se observa, por otro lado, que durante el ataque se alcanzan puntuaciones relativamente altas, lo cual parece responder, no obstante, a la sencillez del algoritmo de comparación utilizado por el sistema, más que a la obtención de tiempos cada vez más bajos.

Los resultados obtenidos tras el mismo ataque sobre el sistema NFIS confirman las conclusiones obtenidas durante el segundo experimento del análisis temporal sobre este sistema: el ataque, que comienza con un valor de puntuación muy bajo, se queda estancado en la región de puntuaciones en la que tiempo y puntuación no están relacionados, con lo que no somos capaces de romper el sistema.

Ya que habíamos comprobado que sí existe una relación entre puntuación y tiempo en la región de puntuaciones altas, se ha desarrollado un segundo ataque sobre el sistema del NIST de similares características al primero, que parte de una plantilla capaz de generar una puntuación alta – ver sección 7.2 para mayor detalle.

Los resultados de este segundo ataque muestran que, si bien la puntuación sí que tiende a aumentar cuando lo hace el tiempo – como era de esperar a la vista de los resultados del experimento 2 -, no aumenta lo suficiente como para romper el sistema.

Tras observar que los dos ataques implementados hasta el momento no han tenido el éxito esperado, pero sabiendo que sí existe, de hecho, una relación a nivel promedio entre la puntuación y el tiempo, se decide llevar a cabo un tercer ataque sobre el sistema NFIS2 en el cual la decisión de conservar o no el cambio se realiza en base a la media de los tiempos obtenidos tras cada M cambios – ver sección 7.3. Se ha probado con M igual a 5 y 10 cambios. Los resultados obtenidos, no obstante, no parecen indicar que atacar de este modo ayude a mejorar los resultados.

A modo de **resumen**, presentamos las siguientes **conclusiones**:

- En ambos sistemas existe una relación entre la puntuación devuelta por el sistema y el tiempo que tarda dicho sistema en devolver la puntuación.
- Los sistemas analizados son resistentes a un esquema de ataque *hill-climbing* clásico basado en tiempo en lugar de en puntuación.
- Aunque estos sistemas se hayan mostrado resistentes a los ataques implementados, la relación entre puntuación y tiempo es patente y, por tanto, sigue existiendo un riesgo potencial de que un ataque basado en tiempo (*timing-attack*) pueda romper ambos sistemas.
- Esta amenaza ha de tenerse en cuenta a la hora de desarrollar este tipo de sistemas, implementando las contramedidas que sean necesarias para evitarlos, como podría ser la aleatorización del tiempo de respuesta del sistema.

8.2. Trabajo futuro

Como trabajo futuro se propone el desarrollo de ataques basados en los tiempos de comparación algorítmica que no sigan esquemas clásicos de ataques tipo *hill-climbing* sobre sistemas biométricos, sino que adapten los algoritmos de *timing-attacks* desarrollados para sistemas criptográficos a las particularidades de los sistemas de reconocimiento biométrico automático.

El estudio de este tipo de amenazas es de vital importancia para la evaluación de los sistemas de seguridad. En este contexto, se están desarrollando a nivel internacional varios estándares que permitan la comparación objetiva de los niveles de seguridad ofrecidos al usuario por los sistemas del campo de las Tecnologías de la Información - entre los que se encuentran las aplicaciones biométricas. Algunos ejemplos de estos proyectos de estandarización son el *Common Criteria* (41), que se complementa con la *Common Evaluation Methodology* (42), o la *Biometric Evaluation Methodology* (43) desarrollada por el gobierno británico.

Todas estas iniciativas intentan cubrir un amplio rango de sistemas y tecnologías, por lo que dan indicaciones muy generales sobre los diferentes aspectos que han de tenerse en cuenta en una evaluación de seguridad. Por esta razón, se necesitan documentos complementarios - los conocidos como *Supporting Documents* - que permitan aplicar las indicaciones generales dadas en las normas anteriores a las particularidades de una determinada tecnología.

Así pues, dentro del trabajo futuro que se deriva de este proyecto se encuentra, no sólo el estudio de otros ataques y vulnerabilidades derivados del análisis temporal que se ha realizado de los sistemas biométricos en este trabajo, sino, también, la organización de estas observaciones y algoritmos en una metodología de evaluación que pueda servir a las distintas partes interesadas (usuarios, empresas y evaluadores) para conocer de forma objetiva las ventajas e inconvenientes de cada producto.

Esta mejora en el conocimiento de los sistemas de seguridad biométrico permitirá, además, también como trabajo futuro derivado de las conclusiones obtenidas en el proyecto, desarrollar contramedidas eficientes a las vulnerabilidades derivadas de la información temporal que se puede obtener de los sistemas.

Referencias

1. **Maltoni, D., et al.** Handbook of Fingerprint Recognition. Springer. 2003.
2. **Daugman, J.** *"Recognizing Persons by Their Iris Patterns"*. Biometrics: Personal identification in a Networdek Society. Kluwer Academic. 1999.
3. **Jain, A.K., Ross, A. and Prabhakar, S.** *"Biometrics: a tool for information security"*. IEEE Trans. on Information Forensics and Security. 1(2). pp. 125-143. 2006.
4. **Hong, L.** Automatic Personal Identification Using Fingerprints. Michigan State University, East Lansing, MI, USA. 1998.
5. **Watson, G.I., et al.** *"User's Guide to NIST Fingerprint Image Software 2 (NFIS2)"*. National Institute of Standards and Technology. 2004.
6. **International Biometric Group.** *"Biometrics Market and Industry Report 2006-2010"*. [Online] http://www.biometricgroup.com. 2008.
7. **Ratha, N.K., Chen, S.Y. and Jain, A.K.** *"Adaptive Flow Orientation-Based feature Extraction in Fingerprint Images"*. Pattern Recognition. Vol. 28 no. 11. pp. 1657-1672. 1995.
8. **Maltoni, D.** *"A Tutorial on Fingerprint Recognition, Advanced Studies in Biometrics. Summer School on Biometrics, Alghero, Italy, June 2003"*. Springer LNCS 3161. 2005.
9. **Maio, D. and Maltoni, D.** *"Direct Gray-Scale Minutiae Detection in Fingerprints"*. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 19 no. 1. pp. 27-40. 1997.
10. **Arcelli, C. and Baja, G.S.D.** *"A Width Independent Fast Thinning Algorithm"*. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 4 no. 7, pp. 463-474. 1984.
11. **Schneier, B.** Secrets and Lies: Digital Security in a Networking World. Jonh Wiley & Sons. 2000.
12. **Ratha, N., Connell, J.H. and Bolle, R.** *"An analysis of minutiae matching strength"*. Springer LNCS 2091. pp. 223-228. 2001.
13. **Udulag, U. and Jain, A.K.** *"Attack on biometric systems: A case study in fingerprint"*. Proc. SPIE. Vol. 5306. pp. 622-633. 2004.
14. **Capelli, R., et al.** *"Fingerprint image reconstruction from standard templates"*. IEEE Trans. on pattern Analysis and Machine Inteligenc. Vol. 29. pp. 1489-1503. 2007.
15. **Galbally, J., et al.** "*Fake fingertip generation from a minutiae template"*. 2008.
16. **Putte, T. and Keuning, J.** *"Biometrical fingerprint recognition: don't ger your fingers burned"*. Proc. IFIP. pp. 289-303. 2000.
17. **Matsumoto, T., et al.** *"Impact of Artificial Gummy Fingers on Fingerprint Systems"*. Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV. Vol. 4677. pp. 275-289. 2002.
18. **Galbally-Herrero, J., et al.** *"On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprint Attacks"*. Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST, IEEE Press. Vol. 1. pp. 130-136. 2006.
19. **Derakhshani, R., et al.** *"Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners"*. Pattern Recognition. Vol. 36. pp. 386-396. 2003.
20. **Tan, B. and Schuckers, S.** *"Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners"*. Proc. SPIE BTHI IV. Vol. 6202, volsect. 62020A. 2006.

21. **Capelli, R., Maio, D. and Maltoni, D.** *"Modelling plastic distortion in Fingerprint Images"*. Proc. ICAPR. Springer LNCS-2013. pp. 369-376. 2009.
22. **Antonelli A., Capelli R., et al.** *"Fake Finger detection by skin distortion analysis"*. IEEE Trans. on Information Forensics and Security. Vol. 1. pp. 360-373. 2006.
23. **Baldiserra D., et al.** *"Fake Fingerprint detection by odor analysis"*. Proc. IAPR ICB. Springer LNCS-3832. pp. 265-272. 2006.
24. **Tan, B., Lewicke, A. and Schuckers, S.** *"Novel methods for fingerprint image analysis to detect fake fingers"*. Proc. SPIE. 2008. Vol. 6202, volsect. 62020A.
25. **Choi, H., et al.** *"Aliveness Detection of Fingerprints using Multiple Stactic Features"*. Proc. of Worlds Academy of Science, Engineering and Technology. Vol. 22. 2007.
26. **Moon, Y.S., et al.** *"Wavelet based fingerprint liveness detection"*. Electronics Letters. Vol. 41 no. 20. pp. 1112-1113. 2005.
27. **Jin, C., Kim, H. and Elliott, S.** *"Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum"*. Springer. Vol. 4817. pp. 168-179. 2007.
28. **Hill, C.J.** Risk of masquerade arising from the storage of biometrics. B.S. Thesis. 2001.
29. **Ratha, N.K., Connell, J.H. and Bolle, R.M.** *"Enhancing security and privacy in biometrics-based authentication systems"*. IBM Systems Journal. Vol. 40 no. 3. pp. 614-634. 2001.
30. **Udulag, U. and Jain, A.K.** *"Hiding biometric data"*. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 25 no. 11. pp. 1494-1498. 2003.
31. **Tuyls, P. and Linnartz, J-P.** *"New shielding functions to enhance privacy and prevent misuse of biometric templates"*. Proc. AVBPA 2003. International Conference on Audio- and Video-Based biometric Person Authentication. pp. 393-402. 2003.
32. **Adler, A.** *"Sample Images can be Independently Restored from Face Recognition Templates"*. Proc. CCECE. Vol. 2. pp. 1163-1166. 2003.
33. **Galbally, J., Fierrez, J. and Ortega-Garcia, J.** *"Bayesian Hill-Climbing Attack and its Application to Signature Verification"*. Proc. ICB. LNCS 4642. pp. 386-395. 2007.
34. **Martinez-Diaz, M., et al.** *"Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification"*. Proc. IEEE Intl. Carnahan Conf. on Security Technology. Vol. 1. pp. 151-159. 2006.
35. **Kocher, P.** "*Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems"*. Proc. ICCAC, LNCS 1109. pp. 104-113. 1995.
36. **Kocher, P. and Ja, J.** *"Differential Power Analysis"*. Proc. Crypto 99, LNCS 1666. 1998.
37. **Kelsey, J., et al.** *"Side Channel Cryptanalysis of Product Ciphers"*. Journal of Computer Security. pp. 97-110. 1998.
38. **Schindler, Werner, Koeune, Fraçois and Quisquater, Jean-Jacques.** *"Unleashing the full power of timing attacks"*. Technical Report, Universite Catholique de Louvain. 2001.
39. **Brumley, David y Boneh, Dan.** *"Remote Timing Attacks are Practical"*. Proc. USENIX SS. 2003.
40. **Ortega, J., et al.** *"MCYT Baseline Corpus: A Bimodal Biometric Database"*. IEEE Proc. Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet. Vol. 6. pp. 395-401. 2003.
41. Common Criteria for Information Technology Security Evaluation. v3.1. CC Press, 2006.
42. Common Methodology for Information Technology Evaluation. v3.1. CC Press. 2006.
43. Biometric Evaluation Methodology. v1.0. 2002.

Glosario

ADN	Ácido 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

Presupuesto

1. Ejecución Material

- Compra de ordenador personal (Software básico incluido)..... 2.000 €
- Licencia Matlab…….....8.000 €
- Sistema *Match-on-Card* .....200 €
- Alquiler de impresora láser durante 6 meses .....50 €
- Material de oficina .....150 €
- Total de ejecución material..... 10.400 €

2. Gastos generales

- 16 % sobre Ejecución Material..... 352 €

3. Beneficio Industrial

- 6 % sobre Ejecución Material..... 132 €

4. Honorarios Proyecto

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

5. Material fungible

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

6. Subtotal del presupuesto

- Subtotal Presupuesto..... 20260 €

7. I.V.A. aplicable

- 16% Subtotal Presupuesto..... 3241,6 €

8. Total presupuesto

- Total Presupuesto ..... 23501,6 €

Madrid, Mayo de 2009

El Ingeniero Jefe de Proyecto

Fdo: Sara Carballo Domínguez

Ingeniero Superior de Telecomunicación

PLIEGO DE CONDICIONES

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un sistema de análisis temporal de sistemas de reconocimiento biométrico de huella dactilar. 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.