Seguridad en los sistemas biométricos

Albert Solé Ribalta

PID_00200719

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Tal y como hemos ido comentando a lo largo de los módulos anteriores, el objetivo de los sistemas biométricos es proporcionar un mecanismo de identificación. Este mecanismo de identificación puede estar dirigido a varios objetivos. Los más comunes, relacionados con proporcionar seguridad a un recurso, suelen ser la autentificación o la detección de personal autorizado y la detección de personal no autorizado. Desde el punto de vista técnico, estos dos objetivos se pueden englobar en un solo punto puesto que la mayoría de las funcionalidades se logran haciendo buscas de personas previamente identificadas en la base de datos del sistema en cuestión. En el primer caso, se da acceso a las personas introducidas en la base de datos y, en el segundo caso, a las personas que no están introducidas en la base de datos. A pesar de que estos son los dos ataques más comunes también existen otros que se van a tratar a lo largo del módulo.

La estructura del módulo es la siguiente:

- La primera parte pretende dar una descripción general de los tipos básicos de ataques como también describir las medidas habituales de protección (apartados "Objetivos del ataque a un sistema biométrico", "Puntos débiles de los sistemas biométricos" y "Defensas específicas para mejorar la seguridad en los sistemas biométricos").

- La segunda parte describe varios ataques aplicables a sistemas basados en la huella dactilar, el reconocimiento de caras y el reconocimiento del iris.

- Una vez descritas cada una de las metodologías de ataque, se tratan también algunas medidas específicas de protección (apartados "Ataques directos" y "Ataques indirectos (generación sintética de datos biométricos)").

- Finalmente se describen los ataques *side channel* y sus utilidades en combinación con los otros posibles ataques (apartado "Ataques *side channel*").

Objetivos

Los objetivos básicos de este módulo son los siguientes:

1. Conocer los tipos básicos de ataques que se pueden producir en un sistema biométrico.

2. Conocer las medidas básicas de protección contra ataques en los sistemas de seguridad basados en la biometría.

3. Conocer una serie de casos prácticos de ataques (ataques directos y ataques indirectos) junto con sus medidas de protección.

1. Objetivos del ataque a un sistema biométrico

Un sistema de seguridad, utilice o no información biométrica, puede ser objeto de una serie de ataques. En este apartado, vamos a describir los principales tipos sin tener en cuenta ni la arquitectura del sistema ni detalles técnicos de estos. Intentaremos centrar los tipos de ataque en los sistemas biométricos a pesar de que, debido a la generalidad de estos, muchos tienen la mayoría de los puntos en común con los ataques típicos a los sistemas de seguridad. Para cada ataque, se van a describir los principales objetivos y ejemplos reales documentados.

1.1. Ataques de suplantación de la persona

El tipo de ataques de **suplantación de la persona (*spoofing*)** va dirigido a obtener acceso ilícito a un recurso. El tipo de ataque consiste en suplantar la identidad de un usuario con acceso al recurso deseado.

Existen varias variantes del ataque según el punto de la arquitectura al que vayan dirigidos. Dejando de lado los ataques tradicionales a sistemas informáticos y centrándonos específicamente en los sistemas biométricos, hay que decir que la forma más habitual de llevar a cabo este ataque es mediante copias sintéticas de datos biométricos del usuario objetivo. Para obtener las copias sintéticas de los datos, hay varios mecanismos que se van a comentar específicamente a lo largo del módulo. A rasgos generales, el principal objetivo del atacante se dirige a dos puntos principales:

Ved también

Las variantes del ataque según el punto de la arquitectura al que vayan dirigidos se tratan en los apartados 2, 4 y 5 del presente módulo.

1) obtener acceso a los datos biométricos del usuario; y

2) realizar una copia sintética de los datos obtenidos.

Debido a la gran difusión de los sistemas de autentificación biométrica, no es difícil encontrar noticias relacionadas.

La huella dactilar

Un primer ejemplo lo podemos encontrar en un ladrón de coches que cortó el dedo al propietario para arrancar su coche, protegido con un sistema de seguridad basado en una huella dactilar. En este caso, el atacante fue capaz de arrancar el coche la primera vez con la huella sin vida del propietario. A pesar de que con posterioridad la misma huella ya no permitía el arranque del coche debido a los sistemas de protección contra muestras muertas de los que disponía el coche.

Fuente: extraído de "Malaysia car thieves steal finger". *BBC News*.

Copias sintéticas

Un segundo ejemplo lo podemos encontrar en un usuario de la Seguridad Social mexicana, quien, mediante copias sintéticas de huellas, falsificaba la presencia de otros usuarios en el puesto de trabajo. En este caso, la suplantación se llevaba a cabo mediante copias sintéticas realizadas con látex (similares a un sello) imprimidas en una imprenta.

Fuente: extraído de "Detienen a empleado de IMSS que duplicaba huellas digitales para «checar» asistencias". *Milenio*.

1.2. Ofuscación biométrica

La mayoría de los ataques a sistemas biométricos están dirigidos a la suplantación de un individuo para obtener el acceso a un recurso protegido. Aun así, existen otros tipos de ataque que hay que tener en cuenta.

La **ofuscación biométrica (*obfuscation*)** va dirigida a falsear o enmascarar los datos biométricos, antes o después de la adquisición de estos por parte del sistema, para evitar que el sistema reconozca a un individuo.

Las consecuencias de un ataque de ofuscación pueden ser tanto o más graves que las de un ataque de suplantación, por lo tanto este tipo de ataques tampoco se tiene que desestimar en la protección de los sistemas. Se debe tener en cuenta que la mayoría de las personas que llevan a cabo este tipo de ataque suelen estar presentes en listas de control y la mayoría están buscadas por las fuerzas del orden. Por lo tanto, estas personas suelen tener bastantes razones para modificar sus datos biométricos. Para hacerse una idea de la gravedad del ataque, podemos considerar los sistemas biométricos situados en las fronteras entre países. En este caso, se requiere que un individuo que desea entrar al país introduzca datos biométricos (habitualmente huellas dactilares o datos faciales) para garantizar que el individuo no ha cometido delitos dentro del país o que no está siendo buscado por la policía.

Hay varias formas de llevar a cabo este ataque según la metodología aplicada, las dos principales son las siguientes:

1) la alteración física de los datos biométricos propios ya sea por deterioro o mediante cirugía, y

2) el uso de técnicas de suplantación para suplantar a un individuo y ofuscar la identidad propia. Esta segunda metodología también incluye el uso de datos sintéticos para ofuscar la identidad.

A pesar de que no hay demasiados casos reales publicados de estos tipos de ataques, seguramente para evitar mostrar pruebas de debilidad en los sistemas de seguridad, es posible encontrar algunas noticias relacionadas.

Ejemplos de ofuscación biométrica

El primer caso que se conoce data de 1933, cuando un asesino y ladrón de bancos fue encontrado con las huellas de la mano izquierda mutiladas. Existen casos similares con algunos famosos delincuentes, como John Dillinger. Otro caso lo podemos encontrar en junio del 2009, cuando cuatro personas fueron detenidas intentando entrar en Japón con las huellas alteradas quirúrgicamente.

Uno de los casos más actuales hace referencia a la violación de las medidas de seguridad del aeropuerto principal de Londres. Este aeropuerto aplica varios sistemas de protección biométrica para garantizar, por un lado, que el pasajero y el pasaporte corresponden a la misma persona y, por el otro lado, para garantizar que la persona no supone ningún peligro para el país. Estas medidas se basan en el reconocimiento por huella dactilar y reconocimiento facial. La noticia, resaltada por la FOX, hace referencia a un grupo de personas que evadió los mecanismos de seguridad a pesar de estar incluidos en una lista de seguimiento. El documento no deja claras las técnicas usadas para violar el sistema de seguridad a pesar de que es un claro ejemplo de lo que se puede conseguir mediante técnicas de ofuscación. Claramente, los atacantes usaron el acontecimiento de los Juegos Olímpicos del 2012 con bastante habilidad, puesto que con seguridad los umbrales de aceptación fueron reducidos para permitir una mayor fluidez de los puntos de control.

Referencia web

Encontraréis la noticia de la violación de las medidas de seguridad en el aeropuerto principal de Londres en "Members of terror watch list reportedly pass through London airport security ahead of Olympics". *Fox*.

1.3. Ataques de denegación de servicio

El objetivo del **ataque de denegación de servicio (*denial of service*)** está dirigido a retrasar, detener o degradar la calidad del sistema.

Un sistema afectado por este tipo de ataque impide que los usuarios legítimos lo puedan usar con normalidad. Este mal funcionamiento del sistema puede ser usado por el atacante con dos fines claramente diferenciados:

1) llevar a cabo un ataque secundario de suplantación u ofuscación, y

2) llevar a cabo un ataque secundario de extorsión.

Reflexión

Debido al contexto de la asignatura, este segundo tipo de ataque secundario no se va a tratar a lo largo del módulo.

Una metodología sencilla para ejecutar este tipo de ataque es la inserción de gran cantidad de datos con mucho ruido que seguramente bajaría el umbral de aceptación y, en consecuencia, aumentaría la tasa de falsos aceptados. En este caso, el ataque secundario podría corresponder a un ataque de suplantación, puesto que muestras biométricas no lícitas podrían ser aceptadas como lícitas por el sistema. En el caso de que el ataque de denegación de servicio fuera más allá de una degradación leve del sistema y detuviera el funcionamiento, el personal administrador se podría ver obligado a reemplazar los sistemas biométricos con medidas más tradicionales como un guardia de seguridad. Se tiene que considerar que, en algunos aspectos, estos sistemas tradicionales son más fácilmente burlados que un sistema biométrico.

Ataque secundario de ofuscación

Un claro ejemplo lo podríamos encontrar en un escenario donde se desea ejecutar un ataque secundario de ofuscación. Supongamos que el atacante desea el acceso a un recurso protegido por un sistema de reconocimiento dactilar y apoyado por un reconocimiento facial. En este escenario, podría ser difícil engañar a un sistema automático bien calibrado, pero no tan difícil engañar a un guardia de seguridad.

1.4. Conspiración y coacción

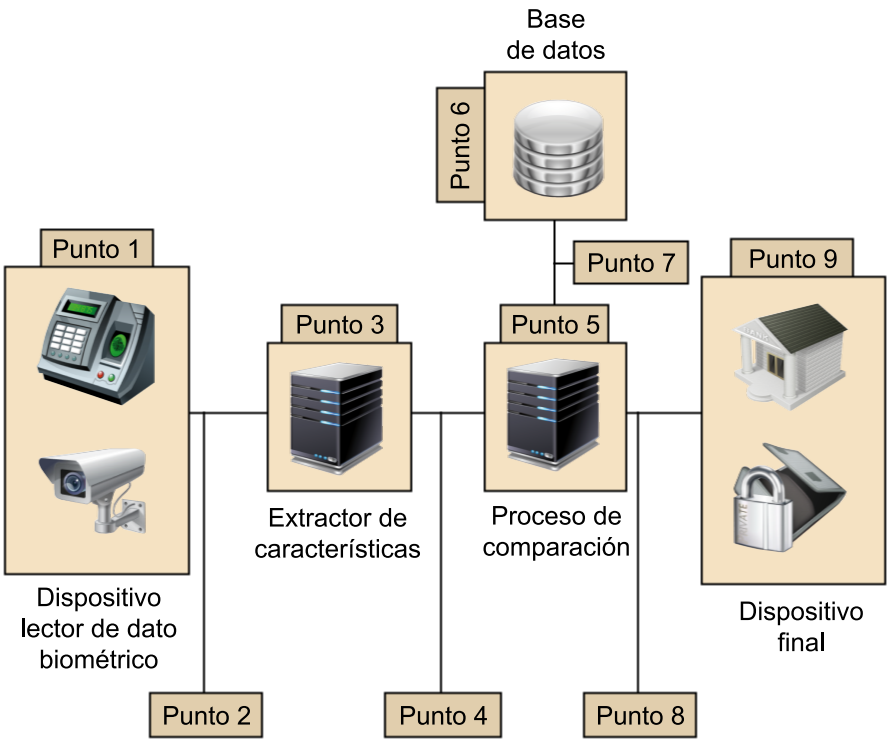
La principal diferencia entre la **conspiración** y la **coacción** y los anteriores es que este tipo de ataques los ejecutan usuarios legítimos del sistema.

En los ataques de conspiración, el usuario, posiblemente por soborno, facilita el acceso al sistema. En los ataques de coacción, la víctima, posiblemente bajo amenaza o chantaje, facilita el acceso al sistema. Estas vulnerabilidades evaden el sistema de seguridad, puesto que los datos son verdaderos. El tipo de ataque puede variar en gravedad dependiendo del usuario atacado. Hay que considerar que no tiene la misma importancia atacar a un administrador que a un usuario sin privilegios.

2. Puntos débiles de los sistemas biométricos

En este apartado, vamos a analizar la arquitectura de un sistema de seguridad basado en biometría para detectar los puntos más débiles y poder presentar una serie de mecanismos para mitigar las posibles deficiencias. La figura 1 presenta el esquema habitual de un sistema de seguridad basado en biometría.

Figura 1. Esquema y puntos de ataque en un sistema biométrico



El sistema de la figura se basa en cinco equipos físicos y varios sistemas de comunicación entre ellos. Los cinco equipos son los siguientes: el sensor, dedicado a capturar los datos biométricos, dos máquinas dedicadas a extraer las características biométricas de los datos capturados por el sensor y a realizar la comparación de los datos biométricos con los datos del posible usuario, una base de datos que contiene los datos de los usuarios registrados en el sistema y, finalmente, un dispositivo que interpreta la salida del sistema y da o deniega acceso al recurso. Existen tanto extensiones como simplificaciones del sistema mostrado. Las simplificaciones pueden venir dadas por la fusión de los distintos módulos del sistema y, por lo tanto, también en la eliminación de los canales de comunicación relacionados. Posibles extensiones pueden venir dadas por la combinación de varios dispositivos de captura de datos (por ejemplo, cara, huella y voz), la distribución de la base de datos en un clúster de máquinas o la ejecución de los procesos de comparación en máquinas paralelas, entre otros.

Analizando la figura 1 no es complicado detectar los puntos de ataque más evidentes. Estos puntos se pueden clasificar en dos grandes grupos, las **máquinas físicas** y los **canales de comunicación**.

En los subapartados siguientes, vamos a describir los ataques que se pueden producir en cada uno de los puntos destacados de la figura 1. Para cada punto se describirán los ataques más habituales como también se introducirán algunos de los mecanismos más habituales para evitar los tipos de ataque.

2.1. Biometría falsa

El ataque de **biometría falsa** (punto 1 de la figura 1), dirigido al proceso de extracción de los datos biométricos, se basa en introducir datos falsos en el sensor.

Según el tipo de sistema biométrico, los ataques pueden presentar varias formas. Uno de los más habituales, dada su gran popularidad de uso, es la presentación de una huella dactilar falsa en el sistema. Estas huellas pueden provenir de gran variedad de lugares: huellas de cadáveres, huellas de silicona, gelatina, plástico o simplemente fotocopias de huellas dactilares. También es habitual la activación del sensor mediante la respiración sobre los residuos acumulados sobre el sensor a pesar de que cada vez más sensores son robustos a este tipo de ataques. En los sistemas basados en la detección del rostro, los ataques más habituales suelen ser la presentación de fotografías, originales o con pequeñas modificaciones, de personas autorizadas. Otros ejemplos de presentación de biometría falsa pueden ser la presentación de grabaciones de alta calidad en sistemas de detección de voz o la presentación de fotografías sobre soportes bidimensionales o impresas sobre lentes de contacto en sistemas basados en el iris.

Ved también

En el apartado 4 del presente módulo describimos algunos de los mecanismos más usados para llevar a cabo estos ataques.

Una solución bastante genérica para proteger el sistema en la presentación de biometría falsa es la detección de si la muestra adquirida y comparada proviene de un tejido vivo o no. Este mecanismo se denomina **detección de vida**. Aun así, se deben tener en cuenta que, en cada tipo de sistema, las características implícitas de estos hacen que los tipos de problemas y, por lo tanto, las soluciones que se vayan a aplicar sean diversas.

La vida de la muestra

Dos ejemplos opuestos relacionados con el tema de la vida de la muestra podrían ser un sistema de autentificación basado en la huella instalado en un dispositivo portátil y el control de inmigración de un aeropuerto. En el dispositivo portátil, es de gran dificultad la detección de la presentación de una huella falsa en comparación con un control de inmigración en un aeropuerto, donde un operario puede analizar los dedos de las personas para detectar cualquier anomalía.

2.2. Inyección de paquetes falsos y ataques de reenvío

La **inyección de paquetes falsos y los ataques de reenvío** (puntos 2, 4, 7 y 8 de la figura 1) consisten en la captura de paquetes de datos procedentes de varios módulos del sistema y que viajan por algún canal de comunicación.

Los paquetes capturados pueden ser utilizados con posterioridad para autentificarse en un sistema biométrico. Los paquetes capturados se pueden enviar sin modificación, utilizar para crear nuevos datos o prototipos de datos biométricos así como también para extraer los datos biométricos dirigidos a la creación de biometría falsa y ejecutar ataques de biometría falsa sobre los puntos 1, 3, 5 o 6 de la figura 1.

En los ataques al punto 2, los datos biométricos previamente grabados se repiten sobre el canal para evitar el sensor. Claros ejemplos de ello serían la intrusión de datos correspondientes a huellas dactilares o señales de audio. Este tipo de ataque se denomina **ataque por repetición**. Se debe comentar que, en sistemas donde el sensor y el extractor de características forman parte de un mismo dispositivo físico, este ataque resulta bastante complicado.

En los ataques al punto 4, después de la extracción de características biométricas, los datos provenientes del extractor de características con destino al módulo de comparación se alteran o se sustituyen por un conjunto nuevo de características. Igual que en el caso anterior, si el extractor de características y el módulo de comparación forman parte del mismo bloque físico este ataque es extremadamente difícil. En cambio, si el proceso de comparación se realiza en otra máquina y los datos se tienen que transmitir por canales no seguros (por ejemplo, via HTTP) este ataque es muy factible y peligroso.

Como en los ataques al punto 4, en los ataques al punto 7 los datos correspondientes a las plantillas de los usuarios registrados se pueden modificar a través del canal de comunicación.

Finalmente, los ataques al punto 8 están dirigidos a modificar el resultado final del sistema. Se debe tener en cuenta que este tipo de ataque es muy peligroso, puesto que independientemente de la eficiencia de todo el sistema, si un atacante puede modificar la salida final, todas las medidas previamente aplicadas no tienen ningún tipo de utilidad.

Sin tener en cuenta las técnicas de generación de datos biométricos falsos, las técnicas aplicadas a este tipo de ataques son más bien técnicas clásicas de captura e inyección de paquetes en un medio de transmisión que técnicas específicas para sistemas biométricos. Por lo tanto, los sistemas de protección

sobre estos ataques son análogos a los sistemas de protección del medio de transmisión como pueden ser detectores de *sniffers*, encriptación o firma de los paquetes.

2.3. Reutilización de residuos

La ejecución de este tipo de ataque necesita el acceso físico al hardware involucrado en el sistema de seguridad.

La **reutilización de residuos** se basa en la captura de datos temporales del hardware ya sean residentes en la memoria principal, en ficheros temporales almacenados en un disco o en ficheros no borrados a bajo nivel.

Este tipo de ataque se puede llevar a cabo en cualquiera de los puntos que forman parte del hardware usado: sensor, extractor de características, bloque de comparación o base de datos. La captura de estos datos podría permitir a un posible atacante ejecutar ataques de biometría falsa, inyección de paquetes sobre el medio, ataques de reenvío, ataques sobre el sensor o también al módulo de comparación.

Las medidas específicas de protección sobre este tipo de ataques suelen ser bastante similares a las técnicas básicas para evitar intrusiones y modificaciones en una máquina sensible. La principal consiste en la protección de la máquina en sí, lo que incluye las medidas básicas de protección de un sistema informático, como pueden ser tener el software actualizado para evitar la intrusión a través de errores en él, un antivirus en caso de que sea necesario, buscas periódicas contra *rootkits*, instalación de sistemas de detección de intrusos (IDS[1]) o la instalación de la máquina en una DMZ (zona desmilitarizada). Otro método sencillo y complementario de protección para estos tipos de ataques consiste en asegurar la ejecución de borrados de bajo nivel de todos los datos sensibles utilizados.

[(1)]Acrónimo del inglés *intrusion detection system*.

2.4. Interferencia en el proceso de extracción

Los **ataques en el proceso de extracción** (punto 3 de la figura 1) van dirigidos a la sobreescritura de los datos extraídos por el extractor de características.

El ataque es equivalente al ataque al punto 4 ya explicado, pero usando mecanismos diferentes. En este caso, un troyano podría ser el responsable de mantener una puerta abierta entre el atacante y el extractor de características para que el extractor genere los datos deseados.

Otra tipología de ataque que puede recibir este punto va dirigida a evitar que el proceso de extracción pueda detectar características vitales o de referencia del dato biométrico, lo que impediría la correcta validación de la identidad. En este caso, el ataque corresponde a un ataque de ofuscación.

De la misma forma que en la reutilización de residuos, es muy importante mantener un control de los usuarios y del software instalado en la máquina como también el uso de *IDS* para garantizar la protección de la máquina.

2.5. Ataques al módulo de comparación

Los ataques dirigidos al módulo de comparación (punto 5 de la figura 1) pueden tener varias formas. La primera y más sencilla corresponde a un ataque similar al de la interferencia en el proceso de extracción, donde el atacante modifica los datos generados por el módulo de comparación. Otro tipo de ataque más complicado corresponde a un ataque al algoritmo de comparación. En este caso, el algoritmo de comparación es engañado por un conjunto de características generadas sintéticamente (con alta probabilidad basándose en características reales). Este conjunto de características presentadas al algoritmo de comparación puede ir dirigido o bien a sustituir a un usuario en concreto o bien a sustituir a algún usuario desconocido buscando el límite de falsos positivos del sistema.

Ved también

En el apartado 5 se describirán una serie de mecanismos usados para ejecutar este tipo de ataques.

2.6. Ataques a la base de datos de plantillas

Los **ataques a la base de datos de plantillas** (punto 6 de la figura 1) van dirigidos a modificar los datos biométricos de los usuarios registrados en el sistema.

Se debe tener en cuenta que la base de datos puede ser accesible local o remotamente, como también puede estar distribuida en varios servidores. En función del tipo de arquitectura, se pueden aplicar varios tipos de ataque. El objetivo de los ataques puede ser muy diverso. En los ataques de suplantación, un atacante modifica los datos de las plantillas grabadas para que correspondan con las suyas. Otro posible ataque destinado a la base de datos va dirigido a registrar a un usuario no autorizado, lo que permitiría un futuro acceso al recurso protegido. Un tercer posible ataque va dirigido a realizar una denegación de servicio a uno o varios usuarios en concreto.

3. Defensas específicas para mejorar la seguridad en los sistemas biométricos

Existen una serie de medidas para impedir/dificultar los ataques antes comentados. Las metodologías descritas a continuación no van todas dirigidas a un punto en concreto del sistema sino que forman parte de un conjunto de sistemas de protección/recomendaciones y buenas prácticas que se deben seguir para que los sistema de seguridad funcionen de manera correcta y eficiente.

Como metodología general, se debe considerar que un **sistema de seguridad** no tiene que centrarse nunca en un único método de seguridad sino que se debe aplicar en combinación con otros secundarios o complementarios.

3.1. Autentificación por combinación de datos aleatorios y biometría múltiple

La idea principal del mecanismo está basada en que el usuario dispone de diferentes características biométricas que pueden ser solicitadas, según la implementación del sistema, aleatoriamente o de forma secuencial. El aumento de seguridad viene dado por el hecho de que el posible atacante tiene que poder reproducir de forma correcta todos los posibles datos que se pueden pedir al usuario. En el caso de introducir aleatoriedad en el proceso, el ataque se complica todavía más puesto que no es posible conocer ni la secuencia ni la cantidad de datos que se van a solicitar.

La huella dactilar

Un sencillo ejemplo de implementación sobre un sistema de huella dactilar sería la verificación de la huella de varios dedos de forma aleatoria. El posible atacante debe tener en posesión una copia de todas las huellas dactilares. En este caso, además, se hace imposible el ataque mediante los residuos en el dispositivo de captura de datos puesto que las huellas de los diferentes dedos se solaparán.

Reconocimiento de voz

Otro posible ejemplo, de implementación más elaborada, podría ser un sistema de reconocimiento de voz en el que se solicita al usuario repetir una secuencia aleatoria de palabras. En este caso, el atacante debería disponer de una gran cantidad de palabras grabadas para poder reproducir cualquier combinación solicitada.

Sistema de seguridad del aeropuerto de Londres

Como último ejemplo basado en un ejemplo de sistema de seguridad real donde se aplica la biometría múltiple sin aleatorización en la demanda de datos podría verse el sistema de seguridad del aeropuerto de Londres, donde los usuarios tienen que presentar de forma secuencial las huellas dactilares y una imagen de la cara.

Ved también

Este ejemplo ya se ha tratado en el subapartado 1.2 del presente módulo.

3.2. Retención de datos

Una gran fuente de información susceptible de ser usada por un presunto ataque es la información temporal que usan los sistemas biométricos. Considerando el sistema a escala técnica se debe tener en cuenta que tanto en la extracción de las características como en el sistema de identificación es necesario guardar cierta información temporal para llevar a cabo las operaciones propias del sistema. Esta información temporal, en el caso de ser capturada, puede dar mucha información a un posible atacante para ejecutar una gran variedad de ataques. Por lo tanto, para proteger el acceso a esta información se tienen que garantizar, con medidas severas, el acceso ilícito al hardware del sistema. Por otro lado, el sistema en sí también debe considerar la necesidad de no mantener la información temporal más tiempo del necesario. Estos mecanismos se pueden usar en combinación con borrados de la memoria a bajo nivel de forma periódica.

Hay que destacar que, para poder guardar históricos de los accesos autorizados y no autorizados por el sistema biométrico, es necesario almacenar datos históricos de forma temporal. Sin considerar que estos datos se tendrían que guardar de forma codificada en el sistema, el administrador debe considerar, mediante un análisis de cada caso en particular, un buen equilibrio entre seguridad y utilidad de la información almacenada.

3.3. Detección de la vida de la muestra

Tal como se ha ido viendo a lo largo de todo el módulo, el ataque de suplantación de la persona es uno de los ataques más típicos sobre un sistema biométrico. Considerando que la metodología más habitual es la copia sintética de datos biométricos de la persona que se quiere suplantar, una de las defensas más utilizadas para evitar estos tipos de ataques es la **detección de vida de la muestra**. Es habitual la incorporación de estos mecanismos al dispositivo de captación de datos. También es importante la detección de la vida de la muestra en ataques de ofuscación, ya que el atacante puede intentar no ser detectado por el sistema usando muestras sintéticas pertenecientes a otros usuarios.

Existen muchas formas para detectar la vida de la muestra. Estas dependen en gran medida del dato biométrico usado por el sistema. A continuación, describimos algunas medidas concretas para detectar la vida de varios tipos de muestras biométricas.

1) Para **sistemas basados en la detección de voz** una medida para detectar la vida de la muestra puede ser la medición del aire expulsado en el habla. Este patrón facilita mucha información de la persona así como también hace más difícil la violación del sistema mediante copias grabadas de la voz original.

2) En **sistemas basados en huellas dactilares**, medidas de fácil detección como pueden ser la temperatura, la oximetría, la conductividad de la piel y la detección de capilares bajo la epidermis o el pulso cardíaco pueden dar mucha información sobre la vida de la muestra.

3) En **sistemas basados en el reconocimiento facial**, se podría combinar el reconocimiento de la cara con combinación de imágenes espectroscópicas o térmicas.

4) Finalmente, vale la pena exponer el caso de los **sistemas biométricos basados en el reconocimiento del iris**, donde ejecutar una copia sintética de un iris sobre una lente de contacto comporta grandes dificultades técnicas, ya sea una copia obtenida de un original o simplemente una generada aleatoriamente. Aun así, existen algunos métodos para detectar la vida de un iris. La mayoría están basados en el análisis estadístico de simetrías en el patrón del iris leído.

Ved también

Encontraréis más información referente a los sistemas biométricos basados en reconocimiento del iris en el subapartado 4.3 del presente módulo.

3.4. Autenticación multifactor

La **autentificación multifactor** podría ser considerada una generalización de la biometría múltiple donde varios mecanismos, no necesariamente biométricos, son solicitados por el sistema en la validación de un individuo.

Estos mecanismos podrían ser mecanismos físicos como tarjetas inteligentes (*SmartCards*), *DONGLE*[2] o cualquier otro tipo de *token* o mecanismos como **claves de acceso**. El aumento de la seguridad de este tipo de mecanismos, igual que en el caso de la biometría múltiple, viene dado por la combinación de los diversos elementos que hay que poder plagiar para practicar un ataque de suplantación.

(2)Encontraréis la definición en el glosario de la asignatura.

Los posibles inconvenientes de utilizar autentificaciones multifactor vendrían dados por un aumento del tiempo de validación. Este aumento forzaría al personal responsable del diseño del sistema a buscar un equilibrio entre seguridad y usabilidad de este.

3.5. Criptografía y firma digital

Tanto los criptosistemas como las firmas digitales se pueden utilizar a muchos niveles en un sistema complejo como puede ser un sistema biométrico. En este caso, dada la generalidad del mecanismo, nos centramos solo en la protección de los datos que circulan por los mecanismos de comunicación entre las diversas máquinas que forman el sistema. La encriptación y el cifrado de los datos que circulan por la red permiten al sistema protegerse de ataques producidos por la lectura/escritura de los paquetes de datos que circulan por

(3)Encontraréis la definición en el glosario de la asignatura.

la red de comunicación del sistema. El objetivo principal del cifrado es evitar que cualquier posible atacante pueda analizar la información que circula por el canal de comunicación. Por otro lado, la firma digital va dirigida a verificar al emisor de la información y evitar en este caso ataques de tipo *man-in-the-middle*[3].

3.6. Los estándares

Como en la mayoría de los sistemas u organizaciones de trabajo, hay una serie de estándares que proporcionan seguridad y eficiencia al sistema. En este caso, dejando de lado otros estándares aplicables a organizaciones, como pueden ser la ISO 9001, hay una serie de estándares relacionados con el buen funcionamiento y la seguridad de los sistemas informáticos. Algunos relacionados con la seguridad de sistemas en general pueden ser el ITIL capítulo 4 o el ISO/IEC 17799. Otros relacionados específicamente con los sistemas biométricos pueden ser el ANSI X.9.84 y el PIV-071006. El estándar **ANSI X.9.84**, diseñado específicamente para sistemas financieros, engloba conceptos de seguridad en la transmisión de información biométrica como también sobre el almacenamiento de esta y los requisitos de seguridad que tiene que cumplir el hardware utilizado en el sistema biométrico. Debido a la gran utilización de los sistemas basados en la huella dactilar, un estándar bastante importante es el PIV-071006. Este estándar especifica los requerimientos de los sensores de captura de datos utilizados en los sistemas gubernamentales de Estados Unidos.

Otros estándares relacionados con sistemas biométricos pueden ser los siguientes:

- **ANSI/INCITS 358**, que motiva la estandarización de la interoperabilidad de los sistemas biométricos.

- **NISTIR 6529**, que especifica el formato de los datos en las interfaces de salida de los sistemas biométricos.

- **ISO/IEC 19794-2:2005**, que especifica el formato de los datos en los sistemas basados en la huella dactilar.

- **INCITS 378-2009**, también dirigido a estandarizar el intercambio de datos en los sistemas basados en la huella dactilar.

Relacionado con los estándares de interoperabilidad, se deben tener en cuenta las dos caras de la moneda. Por un lado, los estándares mejoran la seguridad del sistema puesto que han sido diseñados por un equipo de especialistas y, por lo tanto, se han eliminado muchos de los puntos débiles relacionados con la seguridad. Por el otro lado, un sistema que cumpla el estándar de interoperabilidad facilita el acceso a los datos puesto que tanto el formato de estos como los medios de transmisión se conocen.

3.7. Agentes de seguridad y personal de control

Los sistemas tecnológicos actuales todavía carecen de ciertas cualidades o funcionalidades que una persona puede desempeñar con extrema facilidad. En este caso, muchos de los mecanismos de protección comentados a lo largo de este módulo los puede llevar a cabo un agente de seguridad de una forma más eficiente y económica que un sistema automático. La principal medida de seguridad, y que ayuda a prevenir en gran medida la violación del sistema, es la **detección de la vida de los datos biométricos**. Por lo tanto, en un sistema de seguridad basado en la biometría, es muy importante la combinación de métodos automáticos, para la identificación de datos biométricos, con personal de seguridad para verificar las muestras. Para ilustrar este hecho, basta con considerar que, para cualquier persona, es muy fácil identificar si una muestra es una simple fotocopia o la cara de una persona humana. Otro mecanismo de seguridad que un agente puede proporcionar para aumentar la seguridad del sistema es la identificación de ataques coercitivos, donde un usuario lícito del sistema es obligado a introducir sus datos biométricos en el sistema para dar acceso a un usuario no autorizado.

3.8. La seguridad por desconocimiento

La **seguridad por desconocimiento**[4] es un mecanismo para proporcionar seguridad a un sistema y está basado en no revelar detalles del diseño y la implementación de este.

(4)En inglés, *security through obscurity*.

Se debe tener en cuenta que habitualmente un sistema basado en este tipo de seguridad suele tener vulnerabilidades conocidas, pero que por desconocimiento de su arquitectura e implementación no se pueden explotar. Este sistema de protección suele ser una buena medida complementaria de protección.

4. Ataques directos

Los **ataques directos** son ataques dirigidos al mecanismo de adquisición de los datos biométricos (punto 1 de la figura 1). Este tipo de ataques se basan en introducir datos biométricos generados sintéticamente en el mecanismo de adquisición.

Hay una gran cantidad de variantes del ataque según el objetivo del atacante, el tipo de dato biométrico usado por el sistema de seguridad, como también de los mecanismos de seguridad que el sistema aplique. Para ejecutar un ataque satisfactorio sobre el sensor, un atacante necesita en un primer paso obtener datos biométricos, ya sea por copia de datos reales de un usuario registrado en el sistema como por creación de datos aleatorios, y en un segundo paso producir una copia sintética de los datos obtenidos. Finalmente, presentar los nuevos datos al sistema a través del sensor.

Estos tipos de ataques han demostrado ser bastante exitosos si la copia de datos biométricos es de suficiente calidad. Parte de la gran popularidad de este tipo de ataques radica en que no es necesario conocer ni la arquitectura del sistema, ni detalles del hardware, ni detalles de los algoritmos utilizados, como tampoco el acceso físico al hardware del sistema de seguridad.

Como punto general, se debe tener en cuenta que en muchos de los casos que se presentarán no es posible proteger al usuario para que un posible atacante pueda obtener/robar ciertos datos biométricos. Tal como vamos a ver, en estos casos la seguridad se mueve hacia evitar que el atacante pueda introducir una copia de los datos en el sistema.

En este apartado, vamos a comentar varias de las formas utilizadas para lograr obtener información biométrica y utilizarla para ejecutar un ataque directo. Para cada una de las técnicas explicadas, también comentaremos la validez de las muestras y las protecciones más utilizadas.

4.1. La huella dactilar

En este apartado, vamos a presentar dos formas para generar huellas dactilares sintéticas, la primera considerando que el usuario objetivo colabora en la lectura de sus huellas dactilares y la segunda considerando que el usuario no colabora. A continuación, se comentarán lo peligrosas que pueden ser las copias

generadas en un ataque real junto con los mecanismos de protección más habituales. Finalmente, se comentarán brevemente los mecanismos usados para llevar a cabo ataques de ofuscación al punto 1 de la figura 1.

4.1.1. Duplicados con cooperación

Los duplicados de huellas dactilares con cooperación del propietario son, sin duda, los más fáciles y exitosos, puesto que debido al acceso físico al dato biométrico es posible comparar la copia con el dato real para una rectificación posterior o una nueva copia en caso de no ser de suficiente calidad.

Para ejecutar una copia, los pasos más habituales son los siguientes: el primer paso, de alta importancia, consiste en limpiar bien la huella dactilar tanto de la grasa propia de la piel como de pequeños residuos que puedan existir. Esta limpieza se suele hacer usando simplemente jabón. Este paso es básico puesto que el material de soporte de la copia debe ser capaz de penetrar en los valles de la huella dactilar con facilidad. Los moldes de las copias de calidad suelen hacerse en pequeños recipientes usando, habitualmente, yeso odontológico. Una vez seco el molde se unta la parte de la huella con silicona impermeable o látex y se coloca el dedo destino de la huella encima del material de soporte. Una vez seca, la huella ya se puede retirar con cuidado y colocarse sobre el dedo del portador.

Tal como se puede ver, la copia de una huella dactilar con cooperación tiene una ejecución relativamente sencilla y de alta calidad según los materiales utilizados. Por lo tanto, debido a la simplicidad en la ejecución de copias es muy común que los sistemas de seguridad utilicen contramedidas para evitar este tipo de intrusiones.

4.1.2. Duplicados sin cooperación

Para duplicar una huella dactilar sin cooperación del propietario, es necesario obtener una copia de esta mediante alguna superficie de contacto. Una de las mejores maneras de obtener la copia suele ser mediante el propio sensor o una superficie lisa y rígida. Se debe tener en cuenta que, en el caso de que el escáner se haya limpiado antes de su uso y solo haya una sola huella en la superficie, esta huella suele ser de muy buena calidad y además corresponde al dedo usado para la verificación. Aun así, crear copias en relieve de estas huellas no es tan fácil como en el caso con cooperación, pero tampoco requiere grandes medios técnicos.

Uno de los posibles procedimientos es el siguiente: antes de nada, se debe hacer una copia de la huella dactilar. Para realizar esta copia, habitualmente se usa algún tipo de tinte como puede ser polvo de grafito. Este tinte se deposita sobre la superficie que contiene la huella y esta se retira utilizando algún tipo de superficie adherente transparente. Tradicionalmente, se hacía una copia en negativo de la huella con celuloide (usando una cámara de fotografía

con carrete), en la actualidad el negativo se puede generar con una impresora convencional (tras haber escaneado la muestra). Una vez obtenido el negativo de la huella, se hace una copia en relieve mediante un procedimiento parecido a la creación de circuitos impresos. Esta copia se puede perfeccionar luego usando algún tipo de fresadora. Una vez creado el molde se realiza la copia con silicona impermeable o sobre el material deseado.

MythBusters Fingerprints Busted.

4.1.3. Validez de los duplicados y métodos para evitar el ataque

Los métodos ya comentados, o las variantes de este, dan copias de gran calidad si la huella fuente es de calidad. Los métodos comentados han sido probados con éxito en varios dispositivos actuales.

Tal y como se ha visto, ejecutar copias de huellas dactilares es factible y no excesivamente complicado, por lo tanto la inclusión de métodos para detectar la naturaleza sintética de las muestras es de vital importancia. La principal forma para evitar este tipo de ataques se basa en la detección de vida de la muestra. Los mecanismos más usados incluyen tests de temperatura, conductividad, latido del corazón y presión sanguínea, entre otros. Aun así, se debe tener en cuenta que estos métodos son difícilmente aplicables en sistemas que operan en el exterior. Las condiciones climatológicas obligan a mantener márgenes de aceptación altos para facilitar el acceso a personal autorizado, lo que facilita bastante un ataque exitoso. En estos casos, la detección de la vida de la muestra es fácilmente controlada por un agente de seguridad.

A continuación, se van a describir un conjunto de posibles medidas de aplicación para detectar la vida en una huella dactilar. Tal y como vamos a ver, la naturaleza del soporte usado para crear las copias de las huellas dactilares dificulta mucho la aplicabilidad de estas medidas.

1) Temperatura

En un entorno normal, la temperatura de la epidermis suele estar en torno a los 8 a 10 grados por encima de la temperatura exterior; si el sensor dispone de termómetro es posible realizar controles de temperatura de las muestras.

Teniendo en cuenta que la huella sintética, pegada sobre el dedo, debe tener un cierto grosor, la temperatura de contacto con el sensor tendría que verse alterada y por lo tanto facilitar la detección de que la huella no corresponde a una epidermis humana. Aun así, debido a que las copias de las huellas suelen ser muy finas, la detección por temperatura es difícil. En dispositivos localizados en el exterior, las condiciones climatológicas dificultan todavía más la implementación de este mecanismo en particular.

2) Conductividad

Algunos sensores incorporan métodos para detectar la conductividad del dedo. Uno de los problemas más grandes de este método es la variabilidad de la conductividad de la piel. Estudios demuestran que la conductividad en condiciones normales de la piel es aproximadamente de 200 kΩ. Aun así, en días de frío, en el mismo dedo, esta conductividad puede bajar hasta varios millones de ohmios o aumentar hasta pocos miles de ohmios en días de calor. Teniendo en cuenta esta variabilidad, los márgenes suelen ser demasiado amplios para detectar huellas realizadas con silicona y humedecidas con saliva.

3) El latido del corazón

Algunos mecanismos implementan metodologías para detectar el latido del corazón en la muestra presentada. Aun así, este método presenta varios problemas debido a la variabilidad del ritmo cardiaco. Los individuos que practican deporte pueden tener un ritmo cardiaco inferior a cuarenta latidos por minuto, lo que según varios estudios obliga a tener el dedo inmóvil en torno a cuatro segundos, hecho que retrasa mucho la autentificación del usuario. También se debe tener en cuenta que la variabilidad del ritmo cardiaco en una misma persona hace virtualmente imposible su aplicación como medida biométrica complementaria para comprobar que el ritmo cardiaco no corresponde al usuario registrado.

Condicionantes del ritmo cardiaco

Un claro ejemplo lo podemos encontrar en la variación del ritmo cardiaco en función de si el usuario ha tomado el ascensor o ha subido por las escaleras del edificio antes de llevar a cabo la validación biométrica.

Otro punto que debemos considerar en el caso de que solo se desee detectar si existe latido o no es la extrema delgadez de la copia sintética realizada. Es habitual que el latido sea detectable a través de la copia.

4) La constante dieléctrica

Se denomina **constante dieléctrica** a la permisividad de un medio continuo a transmitir ondas electromagnéticas.

Algunos fabricantes implementan medidas para detectar la vida de la muestra basada en esta constante de la piel humana, que es diferente de la constante dieléctrica de la silicona. Como en los mecanismos anteriores, se debe tener en cuenta que, para no obtener una *false rejection rate* excesiva, el margen de aceptación se debe configurar bastante alto.

A pesar de la fiabilidad del método, existen mecanismos teóricos para sobrepasar la protección. Uno de los más elaborados consiste en la utilización de alcohol para impregnar la huella sintética. Se conoce que el alcohol 90% está formado por un 90% de alcohol y un 10% de agua y sus constantes dieléctricas respectivas son aproximadamente de 24 y 80. También se conoce que la constante dieléctrica de un dedo humano está entre estos dos valores. Teniendo en cuenta que el alcohol se evapora más rápido que el agua, durante la evaporación habrá un momento en el que la constante dieléctrica de la copia caerá dentro de los márgenes de aceptación y el lector tendría que aceptar la muestra como verdadera. El método parece tener validez teórica a pesar de que no se ha demostrado la validez práctica.

5) La presión sanguínea

Algunos sensores existentes en el mercado son capaces de medir la presión sanguínea usando muestras tomadas en dos posiciones separadas del cuerpo. Estas medidas se basan en detectar el latido del corazón en dos puntos del cuerpo y determinar la velocidad de propagación del latido a través de las venas. Sin considerar las desventajas de la detección del latido del corazón, se tiene que considerar que se debe leer el latido en dos posiciones diferentes, lo que dificulta la validación en el usuario. Por otro lado, como ya hemos indicado, las copias suficientemente delgadas ejecutadas con silicona permiten leer el latido del corazón.

6) Detección bajo la epidermis

Algunos sistemas avanzados de reconocimiento de huellas dactilares usan patrones de líneas detectados bajo la epidermis. Estos patrones son equivalentes a los patrones de líneas detectados en la huella dactilar. Aun así, este tipo de protecciones no son totalmente seguros, puesto que una vez se conoce el tipo de protección que usa el sistema se pueden tomar medidas para violar la seguridad del sistema.

Otros métodos basados en los mismos principios de tomar lecturas del material existente bajo la posible epidermis se basan en sensores ultrasónicos para medir la dureza y flexibilidad del material como también en la comprobación de su conductividad.

4.1.4. Técnicas de ofuscación para evitar el reconocimiento

Habitualmente, las técnicas de ofuscación basadas en ataques al sensor se basan en la impresión de datos biométricos sobre un soporte sintético. Estos datos biométricos pueden ser datos obtenidos de otros individuos o datos generados aleatoriamente. Las técnicas de impresión son equivalentes a las técnicas de copia sin cooperación.

Reflexión

Las técnicas de generación de este tipo de datos son equivalentes a algunas de las tratadas en el apartado 5 y, por lo tanto, allí es donde se van a comentar.

4.2. Reconocimiento de caras

Como en la mayoría de los ataques dirigidos al sensor, uno de los primeros pasos que un posible atacante quiere dar es la obtención de los datos del usuario al que desea suplantar. En el caso del reconocimiento de caras, esta tarea es de extrema facilidad. Para darse cuenta del hecho, uno solo debe considerar la cantidad de fotografías en las que aparece. No solo las fotografías en las que uno posa sino también todas las fotografías en las que uno aparece en la escena, las fotografías tomadas por las cámaras de entidades bancarias y comercios, gasolineras, autopistas, entre otras.

En este tipo de identificación biométrica, habitualmente se supone que no se puede evitar la captura de datos biométricos sin autorización. Por lo tanto, como en la mayoría de los casos, para evitar el engaño, los sistemas intentan detectar la vida de la muestra.

4.2.1. Imágenes bidimensionales

En este tipo de ataque, la copia de los datos biométricos tiene lugar mediante una fotografía. La copia se presenta en el escáner o cámara dirigida a llevar a cabo la lectura de los datos biométricos. Este método suele funcionar bien sobre sistemas en los que no se detectan los ojos mediante los reflejos de las pupilas o que no consideran la profundidad de las imágenes tomadas. Los reflejos de la pupila se usan habitualmente para obtener la posición de los ojos y, con estas, las demás características de la cara. Las imágenes carecen habitualmente de esta refractividad y, por lo tanto, no pueden engañar a los sistemas con estas características.

4.2.2. Imágenes bidimensionales con agujeros para los ojos

En este tipo de copia, el dato biométrico, como en el caso anterior, se duplica sobre un soporte bidimensional. Para ser robusto en la adquisición de datos mediante las pupilas, en la imagen se recortan los ojos. Esta copia se presenta en el escáner sobre la cara del suplantador para que el dispositivo detecte la copia de la cara y los ojos del suplantador.

4.2.3. Imágenes en vídeo

Este tipo de ataque tiene lugar mediante secuencias de vídeo de la víctima tomadas sin autorización. Con posterioridad a la captura del vídeo, se editan las imágenes para resaltar las características faciales de la víctima. Habitualmente, las imágenes resultantes acaban siendo un conjunto de imágenes presentadas como una secuencia de vídeo iterativo de la cara de la víctima. No es necesario que este conjunto de imágenes corresponda a una secuencia real de la cara, ya que la mayoría de los sistemas de detección facial se basan en imágenes fijas y no consideran imágenes tomadas con anterioridad de la cara analizada. Las imágenes se presentan al lector o cámara usando un dispositivo portátil que tanto puede ser un ordenador portátil, un marco de fotografías digitales como cualquier dispositivo que pueda reproducir vídeo o secuencias de fotografías. Considerando la gran calidad actual de los grabadores de vídeo digital y de los dispositivos de visualización, este ataque es altamente efectivo.

4.2.4. Validez de los duplicados y métodos para evitar el ataque

A pesar de que no todos los ataques son siempre eficaces, muchos de los comentados comprometen altamente la efectividad de la mayoría de los sistemas de seguridad. Algunos de los ataques tienen varias contramedidas que evitan el ataque de forma eficaz, a pesar de que una vez el atacante conoce las contramedidas estas pueden ser nuevamente comprometidas.

Un primer método específico para evitar que un atacante pueda presentar caras en un soporte bidimensional consiste en la **detección de la profundidad de la imagen**. Sin necesidad de usar cámaras tridimensionales, la percepción de la profundidad se implementa habitualmente variando el plano de enfoque de la lente de la cámara para enfocar diferentes profundidades de la imagen. En este caso, considerando que el dato biométrico está copiado en un soporte bidimensional no contiene profundidad y por lo tanto el sistema no puede ser engañado. Un posible truco, probado en algunos estudios, consiste en acercar y alejar la imagen para simular la profundidad.

Otras técnicas para evitar ataques más elaborados en los que los datos se presentan al sensor mediante secuencias de vídeo se basan en la detección del movimiento de las pestañas, de la boca u otras partes de la cara. Aun así, un atacante posiblemente podría simular estos movimientos mediante secuencias de vídeo. Basados en el mismo principio de detectar movimiento en la muestra, métodos más eficaces se basan en solicitar que el usuario realice una secuencia de movimientos solicitados por el sistema, como puede ser parpadear una serie de veces, mover la cabeza ejecutando los movimientos requeridos o introducir movimientos con la boca. Aunque seguramente estos tipos de acciones también se pueden plagiar, la complejidad del ataque y las técnicas que se pueden usar para realizar la copia de datos aumenta considerablemente.

Como comentario general, puesto que no existe una metodología global para implementar una medida de protección eficaz, es aconsejable usar, como se ha indicado en el apartado "Defensas específicas para mejorar la seguridad en sistemas biométricos", un conjunto de medidas complementarias como pueden ser las anteriores o también la comparación no solo de imágenes estáticas sino de secuencias de vídeo o captura de imágenes térmicas, entre otros.

4.2.5. Técnicas de ofuscación para evitar el reconocimiento

Las técnicas de ofuscación para el reconocimiento de caras tienen los mismos principios que en el caso de la huella dactilar.

4.3. Reconocimiento del iris

El **reconocimiento del iris** es una de las características biométricas más difíciles de capturar sin consentimiento como también es de gran dificultad realizar copias efectivas. Aun así, si se tiene la cooperación del usuario que se pretende suplantar, es posible suplantar el iris de una víctima usando fotografías con una calidad razonable tomadas con microscopios digitales o cámaras con alta resolución. En los métodos de ataque más simples, el soporte de la imagen sintética suele ser papel mate impreso con impresoras de tinta. Para mejorar la eficiencia del ataque, equivalente a los métodos de detección de caras, en estos casos también es habitual recortar la pupila a las imágenes, puesto que muchos sensores usan la reflexión de la pupila para detectar que la muestra es real. Aun así, esta medida depende de la calidad del sistema de seguridad.

Algunos experimentos que aplican el método anterior han demostrado la efectividad de este ataque en sensores comerciales. Tras realizar varios tests, los experimentos demuestran la gran peligrosidad del ataque y se acercan al 100% de aceptación de los datos generados. Aun así, se debe considerar que los sensores usados son sensores no actuales y están dirigidos al ámbito doméstico.

Otras metodologías más avanzadas usadas para llevar a cabo suplantaciones del iris están basadas en lentes de contacto. Sobre estas lentes se pintan los patrones deseados. La más sofisticada de las tecnologías se basa en crear iris artificiales mediante técnicas usadas para elaborar prótesis oculares. Estas metodologías superponen una serie de patrones impresos en varias capas semitransparentes. Los resultados son de alta calidad, a pesar de que es difícil realizar una captura y una posterior impresión de la retina capturada para llevar a cabo un ataque de suplantación.

En casos en los que no es posible realizar copias fieles a las imágenes tomadas, como es el caso del método anterior, es habitual usar los mecanismos para crear identidades transferibles. En este caso, la lectura/registro del usuario en

el sistema se hace con una lente de contacto previamente impresa. Se debe tener en cuenta que esta lente puede ser reimpresa y transferida tantas veces como se quiera dada su naturaleza sintética.

4.3.1. Validez de los duplicados y métodos para evitar el ataque

Dos son los principales inconvenientes o dificultades para realizar un ataque de suplantación en un sistema basado en el reconocimiento del iris.

1) Hay que considerar que es altamente difícil capturar datos biométricos de una víctima sin su colaboración (los dispositivos de fotografía actuales no son tan avanzados).

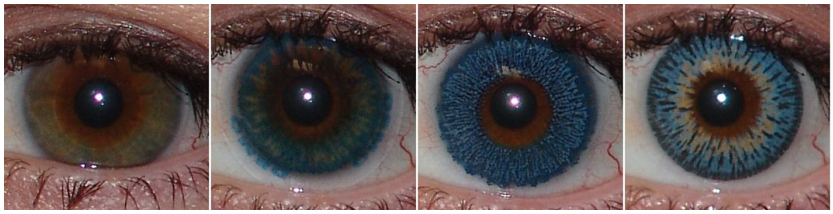
2) Por otro lado, tanto los métodos de escaneo del iris como la mayoría de los métodos de síntesis del iris son muy especializados, lo que dificulta mucho la copia a personal no especializado.

A pesar de que algunos experimentos demuestran la viabilidad de las copias sintéticas de iris, su eficacia es dudable. Aun así, existen métodos para detectar que el iris presentado en el escáner es sintético. Un método bastante simple que los fabricantes de sensores de iris aseguran que funciona es la creación de bases de datos con modelos de lentes de contacto y la comparación de patrones, introducidos en las lentes en el momento de la construcción, con patrones detectados en las muestras capturadas por el sensor. El principal inconveniente de este método, en el hipotético caso de que funcionara, recae en que las bases de datos de patrones se tendrían que mantener actualizadas para garantizar su eficiencia, hecho que implica la creación de organizaciones de constructores de lentes de contacto y la colaboración de gran cantidad de países.

Iridian Technologies Inc.

Una de las empresas que ha estudiado este tipo de métodos con combinación en la detección de patrones no habituales (la empresa no revela detalles de la tecnología usada) es Iridian Technologies Inc. En un estudio, llevado a cabo en el 2005, estudió varios tipos de lentes de contacto diferentes dirigidas a resaltar o modificar el color del iris. La figura 2 muestra varios tipos de lentes usadas en el experimento. La primera imagen muestra el ojo sin la lente de contacto.

Figura 2. Ejemplos de imágenes usadas en el estudio llevado a cabo por Iridian Technologies Inc. La primera imagen corresponde al iris sin la lente de contacto.



Fuente: imágenes obtenidas del doctor Ulf Cahn von Seeles*Countermeasures against iris spoofing with contact lenses.* Iridian Technologies Inc.

La empresa asegura lograr errores de un 12% en la detección del tipo de lente y de un 5% en la detección de la existencia de lente.

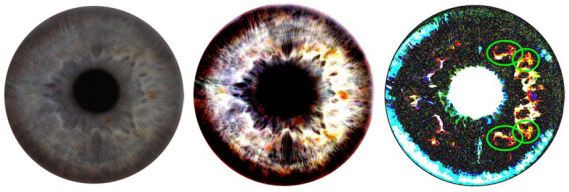
Métodos que también parecen eficaces para la detección de lentes de contacto se basan en modelos estadísticos de análisis de las texturas. Estos modelos se pueden usar tanto para la detección de patrones repetidos como también para detectar otros tipos de patrones que no aparecen en retinas reales. Un ejemplo de este tipo de patrones son simetrías en los datos capturados. Hay varias formas de detección de estos patrones. A continuación, vamos a describir, a rasgos generales, la solución aplicada por la empresa ForBrains.

Referencia web

Esta información se extrajo de "Iris analysis & iris comparison" de ForBrains.

En este caso, para detectar posibles cambios del iris, es decir, si el usuario lleva lentes de contacto o no, esta empresa se basa en detectar pequeñas reflexiones que se producen entre la parte interior de la (posible) lente de contacto y la córnea del ojo. La luz, al pasar de un medio al otro, realiza pequeños cambios de dirección (refracción). Cuando la luz incide sobre la lente de contacto, esta realiza un pequeño cambio de dirección y continúa en línea recta por todo el polímero que forma la lente. Una vez llega a la córnea, considerando que esta es parcialmente reflexiva, no pasa toda la luz, parte rebota sin llegar a entrar en la córnea. Usando varias cámaras de alta velocidad (no necesariamente con alta definición) situadas en diferentes ángulos, es posible conseguir recuperar el iris real y el falso. En este iris falso, se detectan pequeñas repeticiones de patrones. Podemos ver un ejemplo en la secuencia de figuras siguiente. La figura 3a muestra un posible iris falso. Una vez combinadas las imágenes y aumentado el contraste del iris, ved la figura 3b, se aplica un algoritmo de detección de aristas, figura 3c. Dada la baja probabilidad de simetrías en un iris real, esta imagen se considera como alterada por una lente de contacto.

Figura 3



a. Iris capturado, potencialmente falso. **b.** Combinación de varias imágenes tomadas a diferentes ángulos con un aumento de contraste. **c.** Imagen original en la que se han detectado varias simetrías, potencialmente correspondientes a una lente de contacto
Fuente: imagen obtenida de "Iris analysis & iris comparison". *ForBrains*.

4.3.2. Técnicas de ofuscación para evitar el reconocimiento

Las técnicas de ofuscación para el reconocimiento del iris tienen los mismos principios que en el caso de la huella dactilar.

5. Ataques indirectos (generación sintética de datos biométricos)

Esta tipología incluye los ataques a los puntos 2, 3, 4, 6, 7, 8 de la figura 1, es decir a los que no van dirigidos al sensor. En este apartado, solo nos vamos a centrar en ataques sobre el algoritmo de **extracción de características** (punto 3) y el algoritmo de comparación (punto 5).

Los ataques al punto 3 que se van a tratar van dirigidos a realizar un ataque de ofuscación. El objetivo será modificar la apariencia del soporte del dato biométrico para que el algoritmo extractor no pueda detectar las características biométricas de esta. En los ataques al punto 5, el engaño viene dado por un conjunto de características biométricas sintéticas presentadas en el sistema a través del sensor, por lo tanto este ataque viene aplicado con combinación de un ataque directo. A diferencia de los ataques en cuanto al sensor, el atacante necesita conocer información adicional del sistema, como también detalles de funcionamiento interno y del proceso de reconocimiento. En algunos casos de ataques al punto 5, el atacante también necesita tener acceso físico a los componentes del sistema.

Reflexión

Los otros puntos se atacan habitualmente usando técnicas clásicas de Hacking y, por lo tanto, no los vamos a tratar.

5.1. Ataque por ascenso de colinas

Uno de los algoritmos más conocidos para atacar al módulo de comparación (punto 5) es el algoritmo basado en el **método *hill climbing***, traducido como **ascenso de colinas**. El método se usa habitualmente en el campo de las matemáticas dedicado a la optimización de funciones y corresponde al grupo de los métodos de optimización local. Dado que algunos de los algoritmos presentados a continuación usan este método como herramienta básica de ataque, a continuación vamos a describir el funcionamiento básico de este. A rasgos generales, la idea básica de un ataque usando este método consiste en generar datos biométricos sintéticos que sean aceptados por el sistema de autenticación.

5.1.1. Descripción del método

El objetivo principal del algoritmo de ascenso de colinas es encontrar el máximo de una función de una o varias variables. Consideremos que la función de la que se quiere encontrar el máximo corresponde a $f(\mathbf{x})$, donde $\mathbf{x}$ corresponde a un vector que tanto puede ser discreto como continuo. En la aplicación que estamos estudiando, esta función f modela las respuestas del algoritmo de comparación y el dominio de la función, es decir los posibles valores de $\mathbf{x}$, corresponde a todas las posibles características biométricas. En cada iteración

t, el algoritmo varía los valores del vector $\mathbf{x^t}$ y obtiene un nuevo vector $\mathbf{x^{t+1}}$. Este nuevo vector se ha obtenido variando una de las componentes del vector $\mathbf{x^t}$ para que el nuevo vector mejore el valor de la función. Es decir:

$$f(x^{t+1}) > f(x^t) \qquad (1)$$

El algoritmo finaliza cuando no existe ninguna variación del vector x que mejore la función objetivo, es decir cuando hemos llegado a un máximo.

Se tiene que considerar que este método es bastante poco robusto en máximos locales, crestas, valles o mesetas de la función objetivo.

5.2. Ataques por ascenso de colinas en sistemas basados en huellas dactilares

A continuación, describimos dos metodologías para generar datos dactilares sintéticos que sean aceptadas por un sistema de seguridad basado en biometría y una metodología para realizar un ataque de ofuscación.

5.2.1. Ataque al punto 5 de la figura 1 mediante ascenso de colinas

Es habitual que los sistemas de autenticación basados en huellas dactilares utilicen solamente *minutiae* referentes a terminaciones y bifurcaciones. Los más simples se basan en la localización de las *minutiae* (posición (x, y) en la imagen) y la orientación asociada. La posible aplicación del ataque basado en *hill climbing* descrita a continuación se basa solo en estos tres atributos, a pesar de que es fácilmente extensible para considerar una mayor cantidad de atributos.

El objetivo principal del ataque consiste en generar una serie de *minutiae* sintéticas con las que los resultados de autenticación sean suficientemente elevados para que el sistema de seguridad reconozca las huellas como correctas. El ataque va dirigido a suplantar a un usuario D en concreto a pesar de que la información sobre los usuarios no es conocida por el atacante. El atacante únicamente tiene acceso a los resultados del algoritmo de comparación.

El ataque que se ilustra se basa en cinco pasos que se repiten iterativamente hasta que el resultado es el deseado:

1) Inicialización. El primer paso consiste en la generación de una serie de *minutiae* de forma aleatoria para formar una huella dactilar ficticia. Cada *minutia* está formada por la posición en la imagen y la orientación, es decir (x, y, θ). Generaremos P huellas dactilares, que denominaremos T^i, $i \in \{1 \ldots P\}$.

2) Comprobación del resultado de comparación al sistema. Se ataca el usuario seleccionado con cada uno de los datos generados en el paso 1, $biometric\_compare(D, T^i)$, donde D corresponde al usuario objetivo. Los resultados correspondientes a cada comparación se guardan.

3) Escoger el mejor resultado T^* donde:

$$T^* = \min_{T^i} biometric\_compare(D, T^i) \qquad (2)$$

4) Si alguno de los patrones T^* es aceptado por el sistema, seleccionar el patrón como buena aproximación de los datos biométricos del usuario D. En caso contrario, ir a 5.

5) A partir del mejor patrón sintético T^*, generar una serie de patrones auxiliares T^i modificando aleatoriamente *minutiae* existentes, añadiendo nuevas *minutiae* y borrando *minutiae*. Ir a 2.

El ataque presentado va únicamente dirigido a un solo usuario, a pesar de que para mejorar la eficiencia del ataque habitualmente se ataca a varios usuarios en paralelo.

El ataque basado en *hill climbing* suele ser de gran efectividad para conseguir acceso al sistema, a pesar de que requiere tiempo y acceso al propio sistema o al menos una copia de él. A pesar de la efectividad de este tipo de ataque, hay varias formas de protegerse.

La forma más intuitiva de protección se basa en no mostrar la tasa de aceptación de la muestra, a pesar de que esta solución no es siempre efectiva, puesto que en algunos casos esta tasa se utiliza fuera del dispositivo de comparación. Un ejemplo lo podríamos encontrar en sistemas que usan múltiples datos biométricos que se obtienen de varios dispositivos y un sistema central decide si el usuario es válido o no. En sistemas que usan resultados cuantificados, es habitual medir la tasa de aceptación en relación con el tiempo que el algoritmo de comparación ha necesitado para comparar los datos introducidos con los datos registrados en el sistema (*side channel attack*).

Otra posible solución para evitar ataques basados en *hill climbing* recae en devolver resultados ficticios que no alteren el resultado de aceptación de los datos introducidos. Estos resultados semialeatorios están dirigidos a romper posibles correlaciones entre los datos introducidos y el resultado producido.

Por último, vale la pena comentar que una de las soluciones más simples pero efectivas de evitar este tipo de ataque consiste en limitar el número de comparaciones por usuario que se pueden establecer en un día. Se tiene que conside-

rar que habitualmente los ataques por *hill climbing* necesitan de gran número de comparaciones. Por lo tanto, limitar el número de comparaciones posibles elimina en gran medida la utilización de este tipo de ataques.

5.2.2. Reconstrucción de datos dactilares usando información de plantillas

En la primera metodología de ataque que se ha tratado no se conocía ningún tipo de información del usuario. En este caso, el método que se describirá considera conocida la **información correspondiente a las *minutiae* de un usuario** para generar una posible huella dactilar (es decir reconstruir un conjunto posible de aristas que contengan las *minutiae* deseadas) que sea aceptada por el sistema de autenticación biométrica. El método, propuesto por Cappelli y otros, está basado en tres puntos principales:

Referencia bibliográfica

R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n.º 29, págs.1489-1503).

1) se deduce el área de la imagen que se va a construir;

2) se deduce la orientación de las aristas mediante un análisis de la orientación de las *minutiae*;

3) se genera la imagen dadas las *minutiae*, el tamaño y la orientación de las aristas.

1) Información obtenida de la plantilla

En la metodología propuesta por Cappelli y otros, los datos se obtienen de una plantilla basada en el estándar ISO/IEC 19794-2:2005. Podríamos imaginar que se captura mediante un ataque de intrusión en la base de datos o un ataque de análisis al medio de comunicación. En este caso, la plantilla aporta la información general sobre la imagen siguiente: anchura y altura de la imagen y resolución. Además, para cada una de las *n minutiae* m_i aporta información sobre:

- tipo t_i (en este caso solo se consideran terminación y bifurcación),
- posición (x_i, y_i), y
- orientación θ_i.

2) Detección del área de la imagen

Es fácil ver que el tamaño de las huellas dactilares varía según el tamaño del dedo y la presión ejercida sobre el sensor. Por lo tanto, si se pretende generar una imagen que se asemeje a una huella dactilar real, el tamaño de la imagen corresponde a una de las características básicas por determinar. Una posible forma de estimar el tamaño sería usando un modelo genérico configurable mediante un conjunto reducido de parámetros. En este caso, Cappelli y otros proponen usar un modelo que usa cuatro parámetros. Tal como se muestra en la figura 4, el modelo contiene cuatro arcos elípticos y un rectángulo que son configurables mediante los cuatro parámetros comentados (b_1, b_2, a_1, a_2).

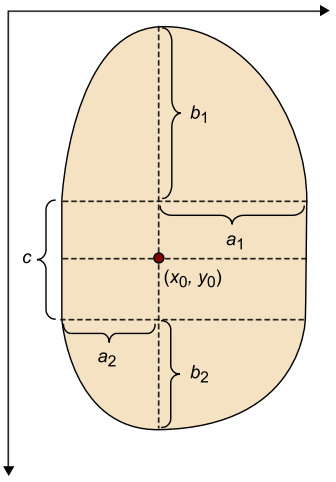


Figura 4. Posible prototipo del área de una huella dactilar

Fuente: R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n.º 29, págs.1489-1503).

Estos cuatro parámetros se pueden obtener mediante varios procedimientos considerando la posición conocida de las *minutiae* que tienen que estar presentes en la imagen. Uno de los algoritmos más sencillos está basado en un algoritmo *greedy*, que simplemente incrementa los valores de los parámetros b_1, b_2, a_1, a_2 hasta que todas las *minutiae* son contenidas dentro del área generada. Otros algoritmos más avanzados podrían, por ejemplo, considerar pequeñas rotaciones de la imagen para generar un área mejor aproximada.

3) Detección de la orientación de las aristas

La orientación de las aristas en la imagen define el movimiento de estas a lo largo de la imagen. Este dato representa una información crucial para obtener una buena imagen final. Para obtener una posible orientación de las aristas de la imagen solo basándonos en información obtenida a partir de la orientación de las *minutiae* hay varios métodos. Uno de los más sencillos se basa en triangular la imagen considerando la posición de las *minutiae* y deducir la orientación por separado en cada triángulo formado. Este método necesita posprocesado para generar imágenes de orientación suaves. Otros métodos más eficaces usan otros tipos de información para generar modelos más precisos como por ejemplo la posición de posibles singularidades que definen el tipo de huella. Sin considerar el método usado en la detección de la orientación de las aristas proceso, el resultado tiene que ser la orientación de las aristas para cada punto de la imagen que se quiere generar. En nuestro caso, definiremos esta orientación como un ángulo $\theta_{x,y}$.

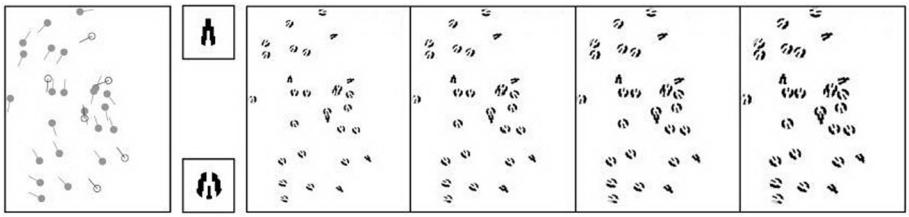
4) Generación de la imagen

Considerando la información obtenida en los puntos anteriores, un método eficaz para generar una imagen solo considerando la información dada por las ***minutiae*** de la imagen se basa en dos pasos.

En el primer paso, partiendo de una imagen del área requerida, se colocan prototipos de las *minutiae* en las posiciones indicadas por los datos iniciales del problema. Estos prototipos suelen ser imágenes de una posible *minutia*. Estas imágenes prototipo se escalan considerando el tamaño requerido y el

número de aristas por unidad de medida requerida en la imagen resultante. La figura 5 muestra varias imágenes donde los patrones de *minutiae* bifurcación y terminal han sido introducidas en varias medidas.

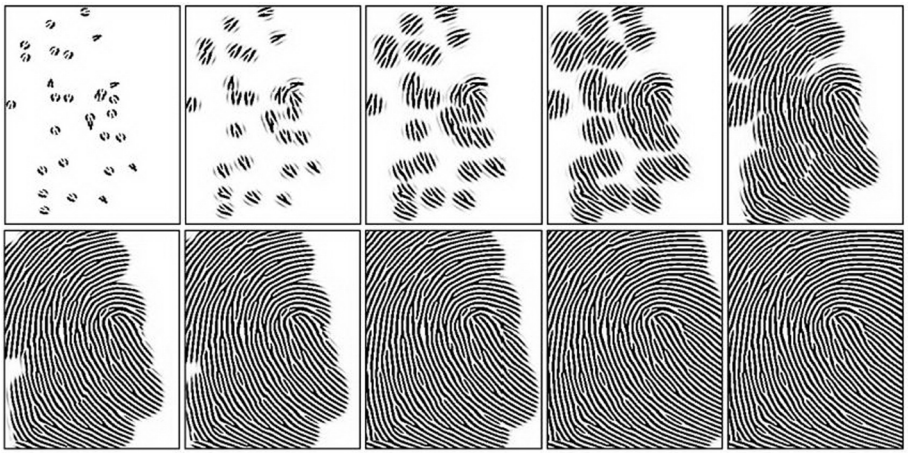
Figura 5. Inserción de patrones mediante imágenes



Fuente: R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n.º 29, págs.1489-1503).

Una vez estos patrones de las *minutiae* se han introducido en la imagen, esta se completa introduciendo aristas ficticias (recordemos que no se conoce la orientación real) usando la información de orientación de las aristas obtenida $\theta_{x,y}$. Una manera bastante efectiva de llevar a cabo este llenado es usando filtros de Gabor, que se aplican en el entorno de las zonas conocidas para agrandarlas. Inicialmente, solo las *minutiae* son zonas conocidas. La figura 6 muestra un ejemplo de este proceso iterativo.

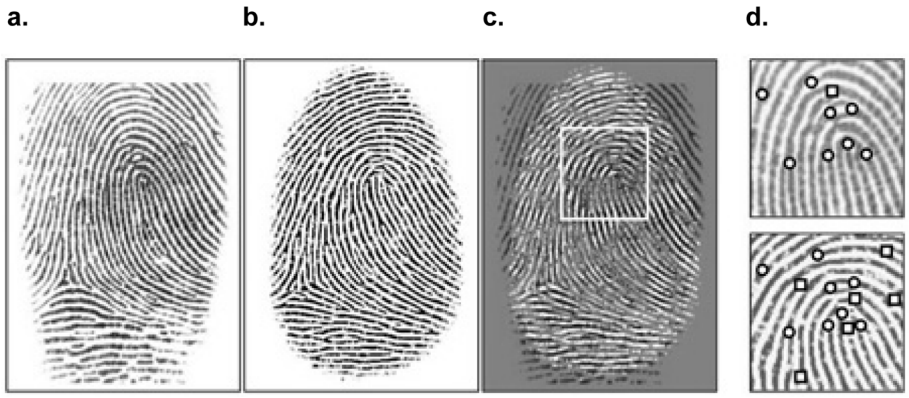
Figura 6. Algoritmo de generación de aristas



Fuente: R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n.º 29, págs.1489-1503).

A pesar de la efectividad demostrada de la metodología descrita, es probable que métodos de identificación biométrica, humana o automática sean capaces de detectar que la muestra se ha generado de forma sintética. La figura 7 muestra una huella real y su equivalente generada sintéticamente con el procedimiento descrito.

Figura 7. Huella real y equivalente sintética



a. Imagen original; b. equivalente generado sintéticamente; c. solapado de las dos imágenes; d. características detectadas
Fuente: R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n.º 29, págs.1489-1503).

Desde el punto de vista humano, la imagen generada puede no corresponder a una imagen real puesto que se detecta mucha repetición de patrones generada por el proceso de creación de aristas. Desde el punto de vista de un sistema automático, puede ser fácilmente detectable que la huella es sintética si las aristas son demasiado sólidas para tratarse de una muestra real. También se podría tener en cuenta el ruido de la imagen que podría delatar en alta medida su naturaleza sintética. Para solucionar estos problemas, habitualmente antes de la utilización de la imagen se ejecuta un posprocesado en el que se añade ruido a esta. Varias técnicas pueden ser empleadas para generar ruido sobre la imagen resultante, dos de las más clásicas son las siguientes:

- introducción de ruido en forma de puntos blancos de diferentes formas y medidas a lo largo de toda la imagen resultante; este tipo de ruido viene dirigido a simular irregularidades en la adquisición de las imágenes, ya sea debido al sensor o explícitas en la huella dactilar;

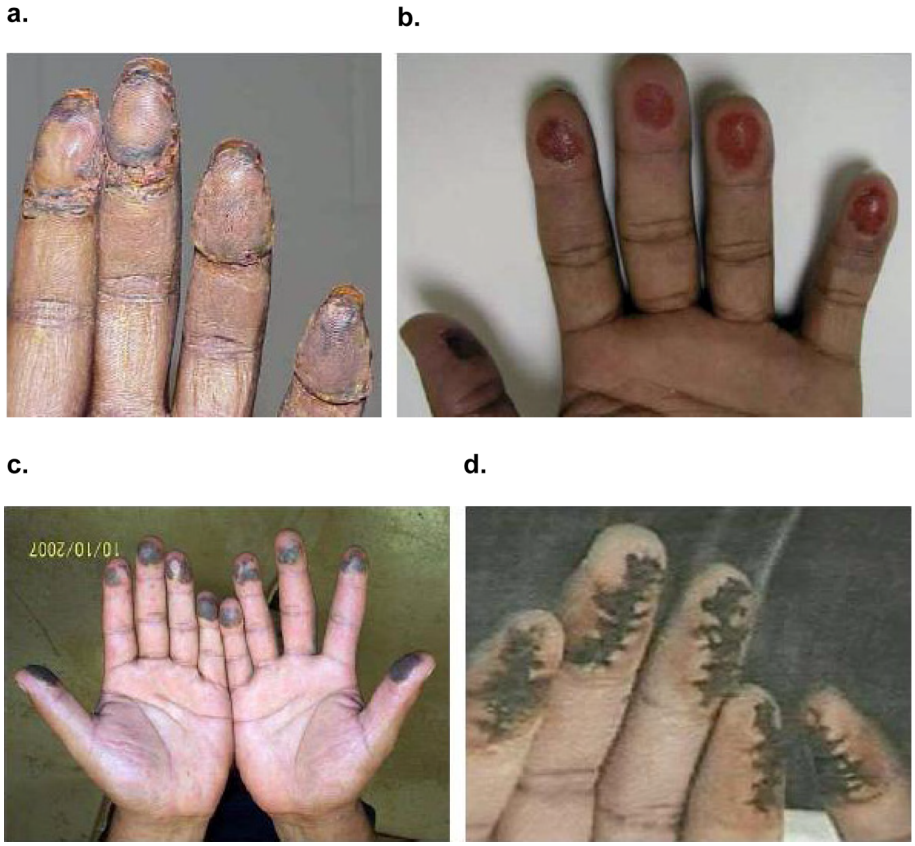
- suavizado del resultado mediante filtros de alisado.

5.2.3. Técnicas de ofuscación para evitar el reconocimiento

Las técnicas de ofuscación aplicadas a huellas dactilares se dividen en tres categorías: obliteración, distorsión e imitación.

En los **ataques por obliteración**, las huellas dactilares o únicamente las aristas son extirpadas o mutiladas usando varias metodologías como pueden ser: abrasión, cortes, quemaduras químicas o transplantes de piel. Algunos ejemplos de obliteración de huellas se pueden ver en la figura 8.

Figura 8. Ejemplos de alteración de huellas dactilares



a. huellas trasplantadas; b. huellas mordidas; c. huellas quemadas mediante ácido; d. huellas extirpadas.
Fuente: J. Feng; A. K. Jain; A. Ross (2009). *Fingerprint alteration.*

Las huellas obliteradas, dependiendo de la profundidad y del área dañada, engañan fácilmente a los sistemas automáticos de detección y pasan también mecanismos de control de calidad. Para aplicar este tipo de ataques se tiene que considerar que la epidermis se va a regenerar correctamente si la profundidad de la lesión producida no supera el milímetro de profundidad. En este tipo de ataques, se tiene que considerar un buen equilibrio entre el área lesionada y el área no lesionada. Una lesión demasiado extensa probablemente engañará al algoritmo de comparación pero no pasará los controles de calidad suficientes y será fácilmente detectable tanto por medios automáticos como por medios humanos. Por otro lado, si la lesión no es lo bastante extensa es posible que el sistema todavía sea capaz de recuperar la identidad verdadera del atacante.

En los **ataques por distorsión**, las aristas de la huella dactilar se modifican mediante cirugía plástica. Estas modificaciones se basan en amputaciones de parte de la piel y recolocación de otras. Los procedimientos quirúrgicos para llevar a cabo modificaciones en las huellas dactilares no suelen ser difíciles. Las huellas dactilares resultantes no suelen coincidir con el original y en muchos casos son difícilmente detectables, aun así la calidad de las distorsiones depende en alta medida de la calidad de la cirugía. Podemos ver dos ejemplos de huellas distorsionadas en la figura 9. En el primer caso, se puede ver que

la calidad de la cirugía no es demasiado buena y, por lo tanto, el engaño es fácilmente detectable, en el segundo caso se puede ver una mejor calidad en la distorsión de la huellas.

Figura 9. Dos imágenes de huellas obliteradas proporcionadas por la Michigan State Police y la DHS

Fuente: J. Feng; A. K. Jain; A. Ross (2009). *Fingerprint alteration.*

En los **ataques por imitación**, las huellas dactilares son sustituidas, usando medios quirúrgicos, por huellas de otras partes del cuerpo, como pueden ser otros dedos de las manos o de los pies. En este tipo de ataques, las huellas suelen tener un aspecto muy natural y si las cicatrices son discretas pueden incluso engañar a usuarios humanos expertos.

Los mecanismos automáticos de detección de huellas ofuscadas se basan en la detección de patrones no naturales en las aristas de la huellas. Estos patrones se detectan usando la orientación de las aristas. En un primer paso, se extrae un conjunto de características que describen las huellas para posteriormente, usando un clasificador binario, clasificar las huellas entre alteradas y no alteradas.

5.3. Reconocimiento de caras

5.3.1. Ataque al punto 5 de la figura 1 mediante ascenso de colinas

En este apartado, describimos una posible forma para generar un ataque basado en *hill climbing* en un sistema de reconocimiento de caras basado en valores propios. Igual que en el ataque a huellas dactilares, el ataque está dirigido a un usuario en concreto. En este caso, el atacante tiene acceso a una base de datos con fotografías de caras ($LI = \{IM_0, IM_1, \ldots, IM_M\}$), imagen de la cara que se

quiere atacar (IM_{targ}), acceso al algoritmo de comparación y al resultado devuelto de este ($MS = biometric\_compare(IM_i, IM_{targ})$). El algoritmo es, en cierta medida, equivalente al dado por huellas dactilares.

El algoritmo básico para aplicar un ataque por *hill climbing* puede ser descrito en cuatro puntos:

1) Preparación de la base de datos que se utilizará para realizar el ataque. En este punto, el atacante prepara la base de datos. Igual que en los sistemas de reconocimiento basados en vectores propios, las imágenes deben tener el mismo tamaño y están alineadas. En este caso, podríamos suponer que las imágenes están alineadas mediante la posición de los ojos.

2) Cálculo de las *eigenfaces*. En este punto, se calcula un conjunto de *eigenfaces* dadas las imágenes descritas en el punto 1. Cada *eigenface* será identificada con el símbolo EF_i.

3) Inicialización del ataque. Se selecciona aleatoriamente una imagen de la base de datos (IM_0). Esta imagen será modificada posteriormente para adaptarse lo más posible a la imagen destino (IM_{targ}). La imagen seleccionada es la que corresponde a una similitud inicial máxima a IM_{targ}.

4) Fase de mejora iterativa $i = \{0,\ldots,i_{max}\}$:

a) Elegir aleatoriamente una *eigenface* de la base de datos *LI*, denominaremos la imagen EF_k.

b) Calcular para un conjunto pequeño de valores $c = \{c_1, \ldots c_j\}$ el valor del algoritmo de comparación:

$$MS_j = biometric\_compare\left(IM_i + c_j * EF_k, IM_{targ}\right) \qquad (3)$$

c) Seleccionar c_{max} como el valor que da mejor resultado MS_j.

d) Actualizar la imagen actual:

$$IM_{i+1} = IM_i + c_{max} * EF_k \qquad (4)$$

e) Truncar valores de la nueva imagen generada IM_{i+1} en el caso de que salgan del rango establecido (0..255).

f) Ir al punto a) hasta $i = i\_max$ o hasta que no haya mejora.

Una primera metodología para hacer frente a este ataque fue la implantación de resultados cuantificados del algoritmo de comparación (The BioAPI Consortium, BioAPI Specification, versión 1.1, marzo del 2001). Aun así, se ha de-

mostrado que con modificaciones al algoritmo de *hill climbing* previamente explicado todavía se pueden generar datos que se asemejen a un usuario en concreto.

En un estudio llevado a cabo por Andy Adler mediante una modificación del algoritmo presentado, se obtienen resultados más que satisfactorios. Los resultados obtenidos se muestran en la figura 10. Se puede observar que, a pesar de que la cuantificación de los resultados devueltos por el algoritmo de comparación, no alteran demasiado la efectividad del ataque. El algoritmo obtiene en todos los casos una confidencia de coincidencia superior al 95%.

Referencia bibliográfica

A. Adler (2004). "Images can be regenerated from quantized biometric match score data". *Canadian Conference on Electrical and Computer Engineering* (págs. 469-472).

Figura 10. Resultantes de confidencia del algoritmo propuesto por Andy Adler

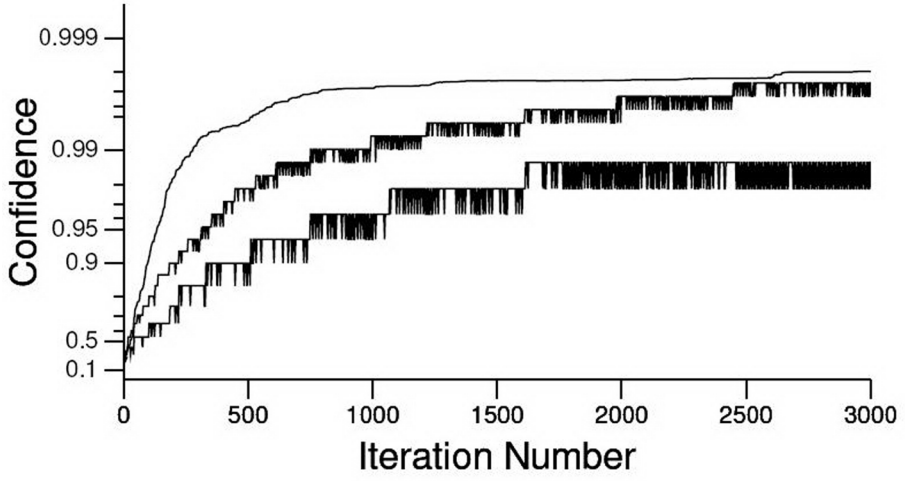


Figura 10

Las diferentes curvas corresponden a varios niveles de cuantificación de los resultados devueltos por el algoritmo; la curva superior corresponde a resultados sin cuantificación.

5.3.2. Técnicas de ofuscación para evitar el reconocimiento

A pesar de que en la mayoría de los casos los ataques sufridos son ataques de suplantación, también hay ataques o metodologías para evitar que un usuario sea reconocido por un sistema de detección automático. Existen varias metodologías, aunque en este apartado solo nos vamos a centrar en dos.

La primera metodología está dirigida a evitar que las cámaras de seguridad colocadas estratégicamente en la vía pública o comercios puedan capturar datos biométricos de los usuarios. Para ver la efectividad de la metodología, hay que considerar que en la mayoría de los casos las cámaras están situadas en posiciones elevadas para evitar obstáculos y tener una mejor perspectiva. Un método de baja tecnología y altamente eficaz es el uso de sudaderas, donde la cara va escondida dentro de la capucha. Considerando la posición suficientemente elevada de las cámaras es bastante difícil obtener imágenes de calidad debido a las sombras y a la mala visual que se obtiene.

Lectura recomendada

B. Rounds (2010). "Fool facial recognition technology". *How to vanish*.

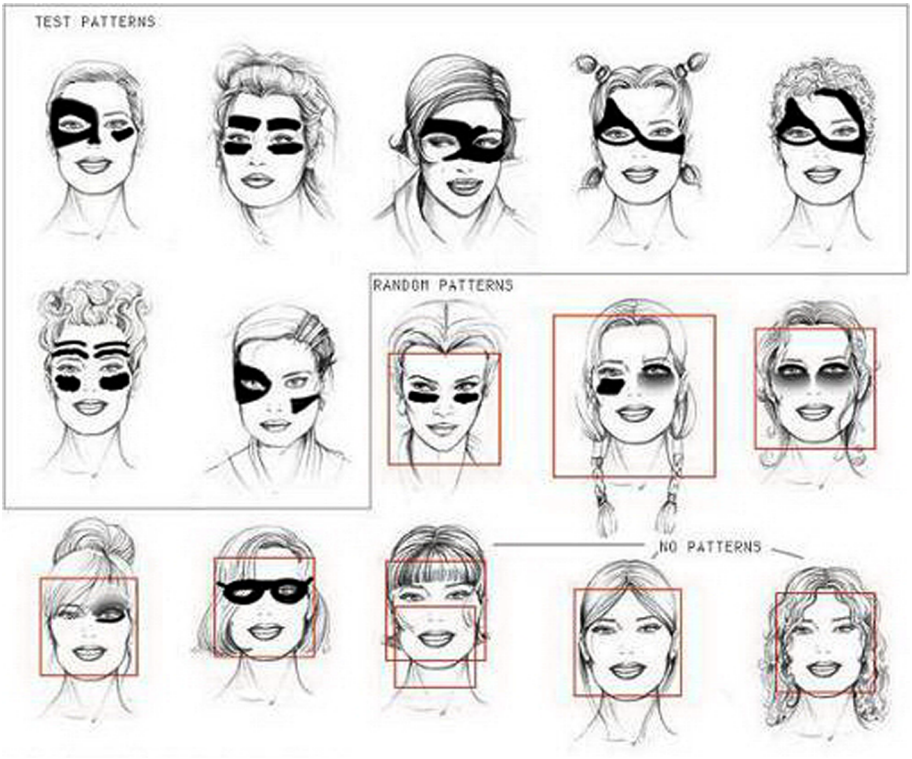
Otra metodología bastante eficaz para evitar la detección automática es el uso de maquillaje. Existen estudios, uno de los más interesantes realizado por Adam Harvey, donde se han estudiado varios patrones de maquillaje para ofuscar varias características faciales. Las técnicas de reconocimiento basadas en

Referencia web

Para más información sobre el estudio de Adam Harvey, podéis visitar CV Dazzle.

características permiten aplicar maquillaje para manipular y distorsionar los puntos de referencia usados para detectar la cara y evitar por lo tanto esta detección. Algunos de los patrones estudiados se presentan en la figura 11.

Figura 11. Patrones estudiados por Adam Harvey



Los estudios llevados a cabo con los patrones descritos muestran la gran efectividad del sistema. En ninguno de los patrones estudiados, los sistemas de detección consiguen detectar la cara.

6. Ataques *side channel*

Tal como se ha visto en el apartado "Ataques indirectos (generación sintética de datos biométricos)", la mayoría de los ataques se basan en adaptar el modelo generado considerando el resultado obtenido por el algoritmo comparador. Considerando que muchas de las veces el atacante no dispone de esta información, puesto que los algoritmos y metodologías de reconocimiento suelen ser secretos, es habitual aplicar ataques del tipo *side channel*.

Los **ataques *side channel*** se basan en obtener este resultado del algoritmo de comparación que cuantifica la validez del dato biométrico presentado en el sistema, analizando el tiempo de ejecución, el consumo de energía de la máquina, las ondas electromagnéticas desprendidas o simplemente el ruido producido.

Estos tipos de ataques se aplican habitualmente a sistemas criptográficos a pesar de que se pueden adaptar fácilmente para ser aplicados a sistemas biométricos. Los **ataques basados en tiempo**[5] consisten en el análisis del tiempo de cálculo usado para ejecutar el algoritmo de comparación. Es fácil ver que este tiempo depende fuertemente de los datos de entrada. Varios experimentos han demostrado que los algoritmos usados en las comparaciones de los datos suelen usar más tiempo en la comparación de datos incorrectos que en la comparación de datos correctos. Los **ataques basados en el análisis de la cantidad de energía**, **pérdidas electromagnéticas** y de **ruido** van dirigidos en la misma dirección.

(5)En inglés, *timing attack*.

Actividades

1. ¿Cómo creéis que se podrían detectar automáticamente ataques basados en la coacción? ¿Y los basados en la conspiración? ¿Cómo creéis que afectarían las soluciones que proponéis a la usabilidad del sistema?

2. Extended la información relacionada con los estándares, leyendo los documentos siguientes:

- Biometrics standards
- Common biometric exchange file format
- Common biometric exchange formats framework
- Image quality specifications for single finger capture devices
- https://dev.issa.org/library/journals/2007/january/griffin%20-%20ISO%2019092.pdf

3. Relacionado con la síntesis de las huellas dactilares comentada en el subapartado "Huella dactilar", ¿qué pensáis de la validez de los duplicados? ¿Os parece que las medidas de protección señaladas proporcionan un porcentaje de seguridad bastante alto? Considerando que sois los diseñadores del sistema, ¿cuáles utilizaríais? ¿Añadiríais alguna no comentada?

4. Visitad las páginas web citadas a lo largo del módulo. ¿Cuál de las técnicas creéis que es la más fácil de implementar para llevar a cabo un ataque de suplantación? ¿Y de ofuscación? ¿Qué pensáis que es más sencillo, realizar un ataque dirigido al sensor, al extractor de características o al algoritmo de comparación?

5. Relacionado con los ataques indirectos dirigidos al algoritmo de comparación, ¿creéis que se podría mejorar la eficiencia del mecanismo propuesto (*hill climbing*) en combinación con otras técnicas como la busca tabú? ¿Creéis que otros métodos de optimización como por ejemplo algoritmos genéticos o *simulated annealing* funcionarían mejor? En el caso de que la metodología sea aplicable, intentad generar un pseudocódigo de los algoritmos resultantes.

6. Poned en funcionamiento el sistema de reconocimiento de caras de Picassa o, en el caso de que disponga de él, el del teléfono móvil. Intentad aplicar un ataque de ofuscación basado en los patrones diseñados por Adam Harvey.

7. Diseñad alguna metodología para aplicar un ataque *side channel* al sistema de reconocimiento facial del Picassa. ¿Cómo transformaríais los datos obtenidos en datos usables para llevar a cabo un ataque de suplantación basado en *hill climbing*?

Abreviaturas

ANSI American National Standards Institute

DHS Department of Homeland Security

IDS *intrusion detection system*

ISO International Organization for Standardization

PIV *personal identity verification*

Glosario

constante dieléctrica *f* Relacionada con el electromagnetismo. Es la medida de resistencia que tiene un medio cuando se le aplica un campo electromagnético.

dongle *m* Equivalente a clave electrónica o candado electrónico.

hill climbing *f* Técnica de optimización matemática que pertenece a la familia de la busca local.

man-in-the-middle *m* Ataque en el que se adquiere el poder de modificar los mensajes entre dos partes que se comunican.

obliteración *f* Acción de hacer ilegible un elemento.

phishing *m* Ataque con el objetivo de obtener información privada de un usuario mediante la suplantación de una entidad confiable.

sniffing *m* Acción de analizar los paquetes que se transmiten por un medio de comunicación.

spoofing *m* Ataque de suplantación de identidad.

Bibliografía

Bibliografía básica

Adler, A. (2004). "Images can be regenerated from quantized biometric match score data". *Canadian Conference on Electrical and Computer Engineering* (págs. 469-472).

Cappelli, R.; Lumini, A.; Maio, D.; Maltoni, D. (2007). "Fingerprint image reconstruction from standard templates". *IEEE Transactions on Pattern Analysis and Machine Intelligence* (n. 29, págs.1489-1503).

Feng, J.; Jain, A. K.; Ross, A. (2009). *Fingerprint alteration*.

ForBrains. "Iris Analysis & Iris Comparison".

Harvey, A. *CV Dazzle*

Rounds, B. (2010). "Fool facial recognition technology". *How to vanish*.

Cahn von Seeles, Ulf. *Countermeasures against iris spoofing with contact lenses*. Iridian Technologies Inc.

Bibliografía complementaria

Galbally, J.; Cappelli, R.; Lumini, A.; Maltoni, D.; Fierrez, J. (2008). "Fake fingertip generation from a minutiae template".*International Conference on Pattern Recognition*.

Herrero, J. G. (2009). *Vulnerabilities and attack protection in security systems based on biometric recognition*.

Kiviharju, M. *Hacking fingerprint scanners*.

Lefohn, A.; Caruso, R.; Reinhard, E.; Budge, B. (2003). *An ocularist's approach to human Iris synthesis, computer graphics and applications*.

Mohanty, P.; Sarkar, S.; Kasturi, R. (2006). "A non-iterative approach to reconstruct face templates from match scores".*International Congress on Patern Recognition*.

Nanavati, S.; Thieme, M.; Nanavati, R. (2002). *Biometrics*.

Nixon, K. A.; Aimale, V.; Rowe, R. K. (2007). "Spoof detection schemes".*White Paper*.

Ratha, N. K.; Connell, J. H.; Bolle, R. M. (2001). "An analysis of minutiae matching strength".*Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*.

Reid, P (2004). *Biometrics for network security*.

Ruiz-Albacete, V.; Tome-González, P.; Alonso-Fernández, F.; Galbally, J.; Fierrez, J.; Ortega-García, J. (2008). "Ataques directos usando imágenes falsas en verificación de iris".*IV Jornadas de Reconocimiento Biométrico de Personas*.

Thalheim, L.; Krissler, J.; Ziegler, P.-M. (2002). "Body check: biometric access protection devices and their programs put to the test".*C't Magazine*.

Uludag, U.; Jain, A. K. (2004). "Attacks on biometric systems: a case study in fingerprints".*Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents*.