UNIVERSIDAD AUTÓNOMA DE MADRID
ESCUELA POLITÉCNICA SUPERIOR

VULNERABILIDADES EN SISTEMAS DE RECONOCIMIENTO BASADOS EN HUELLA DACTILAR: ATAQUES HILL-CLIMBING

-RESUMEN DEL PROYECTO FIN DE CARRERA-

XXVII Convocatoria premios "Ingenieros de Telecomunicación"

Marcos Martínez Díaz

Febrero de 2007

1 Descripción del proyecto

1.1 Origen

Hoy en día los sistemas basados en reconocimiento biométrico han cobrado gran relevancia en entornos seguros que requieren la identificación de usuarios o accesos restringidos. En comparación con otros métodos como llaves o claves, los rasgos biométricos no pueden, en general, ser prestados, robados o copiados [1].

Los rasgos biométricos pueden clasificarse según varias características. Entre ellas cabe mencionar su unicidad, su distintividad o individualidad, su universalidad, su facilidad de proceso y adquisición o su variabilidad con el tiempo. La huella dactilar reúne muchas de estas características y por ello ha sido muy utilizada tradicionalmente en el ámbito forense y más recientemente en los sistemas de autenticación automática [2]. Otra ventaja del reconocimiento automático de personas basado en huella dactilar es el reducido tamaño físico de los sensores de huella (especialmente los más modernos, como los de tecnología capacitiva o térmica), el cual permite la incorporación de sistemas reconocedores de huella en dispositivos portátiles o de bajo consumo y en emplazamientos donde otro sistema de reconocimiento no podría situarse. Son ejemplos de ello las PDAs, los ordenadores portátiles, los *Tablet* PC, y los teléfonos móviles 3G, entre otros. En la Figura 1 se muestran algunas de las aplicaciones comerciales de reconocimiento biométrico basado en huella dactilar existentes en la actualidad.

Figura 1. Ejemplos de aplicación comercial de sistemas de reconocimiento biométrico basados en huella dactilar.

El reconocimiento biométrico, al presentarse como una alternativa a sistemas de verificación tradicionales de usuarios, se ha convertido en pocos años en un foco de atención en cuanto a su seguridad. Recientemente se ha comenzado a estudiar las vulnerabilidades que presentan los sistemas biométricos ante diferentes tipos de ataque.

1.2 Objetivos y enfoque

Como ya se ha mencionado, la proliferación de sistemas basados en reconocimiento de huella dactilar ha suscitado gran interés en aplicaciones de seguridad; y los posibles ataques a sistemas de huella dactilar han sido clasificados y documentados. Los ataques hasta ahora conocidos se han clasificado y documentado, existiendo dos clases principales [2]: *ataques directos*, dirigidos al sensor de huella dactilar presentando huellas sintéticas y *ataques indirectos*, dirigidos a una parte interna del sistema de verificación.

El objetivo de este proyecto es el estudio de las vulnerabilidades de sistemas de reconocimiento de huella dactilar, implementando ataques de tipo indirecto y estudiando la robustez de sistemas de verificación reales frente a los mismos.

En el proyecto se estudia, desarrolla, implementa y documenta una clase de ataques indirectos *software* denominada *hill-climbing* [3]. Este tipo de ataques consiste en enviar al sistema comparador la información suficiente para que calcule la similitud con la huella que se está atacando y devuelva una puntuación. La puntuación de similitud obtenida se utiliza en un proceso iterativo para realizar modificaciones sucesivas de la información enviada al comparador de forma que se logra incrementar progresivamente la similitud hasta llegar al umbral de decisión establecido.

Se realizan ataques contra dos sistemas de verificación de huella dactilar: el sistema de referencia NFIS2 del NIST americano (*National Institute of Standards and Technology)* y un sistema embebido basado en tarjeta inteligente (*Match-on-Card*) [4], en un entorno más realista en el que se desconoce el funcionamiento interno del sistema y únicamente se dispone del formato de entrada y salida de datos del sistema.

El método de ataque *hill-climbing* presenta varias ventajas dado que, como se verá en el apartado 1.3, requiere muy poca información acerca del sistema que se está atacando. En el proyecto se exponen los resultados obtenidos en los experimentos realizados sobre ambos sistemas y se discuten los resultados extrayendo conclusiones, planteando posibles contramedidas, y proponiendo posibles vías para trabajo futuro.

1.3 Desarrollo

El proyecto comienza con una exposición del estado del arte del reconocimiento biométrico. Se clasifican e introducen los rasgos biométricos en función de sus características y se desarrollan con más profundidad los aspectos relacionados con el reconocimiento de huella dactilar. En la Figura 2 se muestra la arquitectura básica de un sistema de verificación de huella dactilar y se señala el punto en el que se realizan los ataques *hill-climbing*.

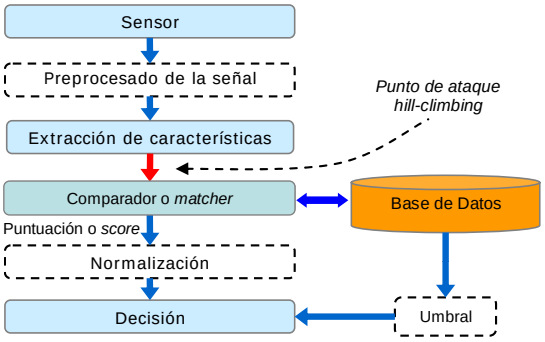


Figura 2. Arquitectura de un sistema de verificación de huella dactilar

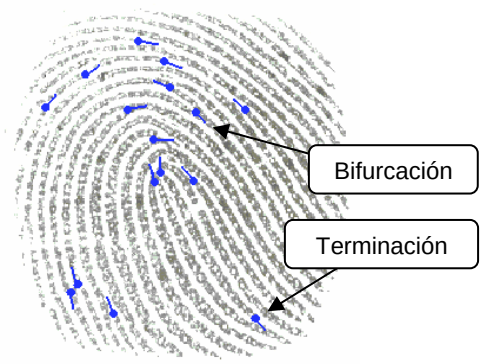


Figura 3. Ejemplos de localización y orientación de las minucias de una huella dactilar

La mayoría de los sistemas de reconocimiento actuales emplean las minucias (*minutiae,* en inglés) de la huella dactilar para comparar dos huellas. Una minucia es una terminación o bifurcación en el flujo de una cresta papilar epidérmica de una huella dactilar (véase Figura 3). Los ataques que se van a realizar estarán dirigidos a este tipo de sistemas. A continuación se detalla el protocolo establecido para la elaboración de los ataques y las características de las huellas empleadas para los mismos.

1.3.1 Ataques *hill-climbing*

Los ataques *hill-climbing* se realizan directamente sobre el *matcher* y no utilizan información alguna de la imagen de la huella [3]. Emplean exclusivamente patrones sintéticos de minu-

cias generados aleatoriamente. Únicamente es necesario conocer la resolución y el tamaño de las imágenes que genera el sensor del sistema. Esta premisa es fácil de cumplir ya que los sensores suelen estar expuestos a la vista y la información necesaria de los mismos es publicada por los fabricantes.

Sea D_i la plantilla de minucias del usuario *i*, con n_i minucias. T_i^j es la *j*-ésima plantilla sintética generada por el sistema de ataque para la huella de la base de datos del usuario *i*. Se emplean únicamente las coordenadas de cada minucia y su orientación, por ser estos datos comunes a la mayoría de los sistemas de reconocimiento actuales basados en minucias. El formato de las plantillas resultante es el siguiente:

$$T_i^j = \begin{bmatrix} {}^1x_i^j & {}^1y_i^j & {}^1\theta_i^j \\ {}^2x_i^j & {}^2y_i^j & {}^2\theta_i^j \\ \vdots & \vdots & \vdots \\ {}^{n_{ij}}x_i^j & {}^{n_{ij}}y_i^j & {}^{n_{ij}}\theta_i^j \end{bmatrix}$$

Donde, en cada fila, x e y representan la posición horizontal y vertical respectivamente de una minucia y θ es el ángulo de la orientación de la minucia (que se corresponde con la dirección de la tangente de la cresta asociada a la minucia en la terminación o bifurcación). Una huella D_i será aceptada por el sistema si su puntuación $S(D_i, T_i^j)$ con respecto a la plantilla T_i^j supera un umbral S_{umbral}. El ataque descrito efectúa las siguientes operaciones:

1) Crear 100 patrones de 25 minucias $T_i^1, T_i^2, T_i^3 ..., T_i^{100}$ completamente aleatorios del mismo tamaño que las imágenes de la huella.
2) Atacar con los 100 patrones la huella víctima y almacenar todas las puntuaciones $S(D_i, T_i^j)$ devueltas por el *matcher*. Se escogerá como patrón ganador $T_i^{ganador}$ aquél que haya generado la puntuación más alta $S_{ganadora}(D_i, T_i^j)$
3) Realizar las siguientes iteraciones:
    a. Desplazar con probabilidad 0.5 una minucia de $T_i^{ganador}$ a una celda adyacente (9×9 píxeles) o modificar su ángulo con probabilidad 0.5.
    b. Añadir una nueva minucia.
    c. Reemplazar una minucia por otra aleatoria.
    d. Eliminar una minucia.

    Entre cada una de estas iteraciones, si la puntuación en el *matcher* mejora, almacenar esta modificación en el patrón, si no, se desecha.
4) Si en algún momento se supera la puntuación umbral, el ataque habrá tenido éxito y por lo tanto se detiene.

En los ataques se estudia la influencia de sus posibles variables. Un ataque *hill-climbing* se puede considerar más eficaz cuantas menos iteraciones requiera. De hecho, para un sistema concreto del cual se conocen sus características de funcionamiento (tasas de Falsa Aceptación FAR y de Falso Rechazo FRR o curva DET), un ataque *hill-climbing* se podrá considerar eficaz si no excede el número de intentos teóricos necesarios para un ataque de fuerza bruta (en el que se presentan huellas reales tomadas aleatoriamente de una base de datos al sistema hasta que una de ellas es aceptada). El número de intentos teóricos para un ataque de fuerza bruta se obtiene de la propia definición de la FAR del siguiente modo:

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

Por lo tanto, si un ataque *hill-climbing* requiere más de $N_{fuerzabruta}$ iteraciones, será teóricamente menos eficiente que un ataque de fuerza bruta.

1.3.2 Sistemas estudiados

Se han realizado los ataques *hill-climbing* frente a dos sistemas de reconocimiento de huella dactilar, el *NIST Fingerprint Image Software 2*, reconocido como sistema de referencia y un sistema embebido basado en *smart-card* que realiza la comparación dentro del propio chip *(Match-on-Card)*. A continuación se describe brevemente cada sistema y su rendimiento.

NIST Fingerprint Image Software 2. El sistema NFIS2 (Figura 4) es reconocido como una referencia en verificación de huella dactilar de tal modo que los sistemas de reconocimiento de huella dactilar que se diseñan en la actualidad se suelen comparar con el *software* de NIST para tener una primera medida comparativa de rendimiento. El sistema NFIS2 fue creado por el *National Institue of Standards and Technology* americano (NIST) y fue diseñado para facilitar y apoyar la manipulación y el procesado de imágenes de huellas dactilares. Los ataques se realizaan en un PC que disponga del *software* NIFS2 instalado. Las pruebas se pueden automatizar permitiendo así realizar ataques masivos de forma continuada.

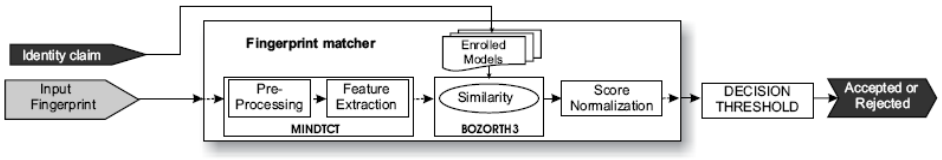


Figura 4. Arquitectura del sistema NFIS2.

Sistema basado en tarjeta inteligente Match-on-Card. El segundo escenario considerado en el presente proyecto es un sistema basado en tarjeta inteligente o *smart-card* en el que la comparación entre huellas se realiza en el propio *chip* de la tarjeta [4] (véase Figura 5). Los sistemas basados en tarjeta inteligente han cobrado gran relevancia en los últimos años. La huella del usuario se encuentra almacenada en la tarjeta y protegida de cualquier acceso, por lo que el poseedor de la tarjeta es portador tanto de su huella como del sistema de comparación necesario para la verificación de la huella. Las *smart-card* poseen pocos centenares de KB de memoria y un microprocesador de capacidad limitada. El algoritmo de comparación era en este caso desconocido, y el acceso a la tarjeta se programó a partir de su *driver* y librerías de Windows. Al igual que en el caso del sistema NFIS2, se automatizan ataques masivos mediante su programación en un PC para realizar los experimentos.

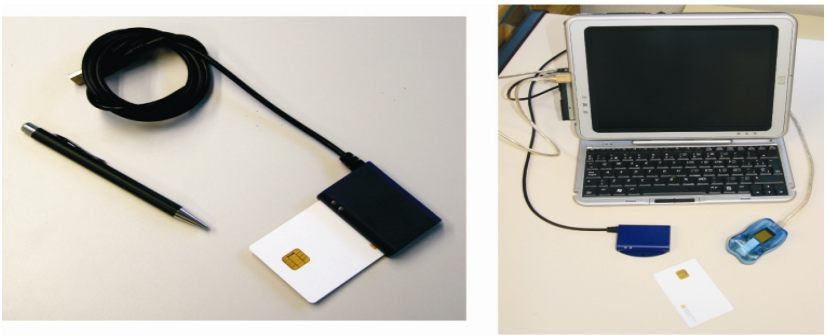
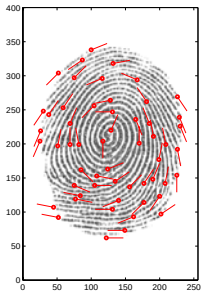


Figura 5. Sistema *Match-on-Card* empleado en el proyecto. Nótese en la fotografía de la izquierda que la tarjeta inteligente ha sido insertada al revés para poder observar el *chip*.

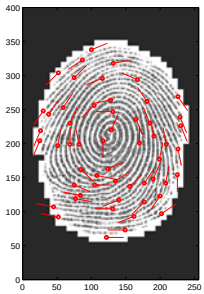
1.3.3 Base de datos y protocolo experimental

Es necesario establecer un protocolo de pruebas para extraer estadísticas del funcionamiento de un sistema biométrico y así poder determinar su rendimiento. Los ataques fueron probados sobre un sub-corpus de la base de datos MCYT [5]. Se consideraron 10 muestras del dedo índice derecho e izquierdo de 75 usuarios adquiridas mediante un sensor óptico de 500 dpi contando por lo tanto con $2 \times 75 \times 10 = 1500$ muestras. Se realizó etapa de preprocesado en las huellas para eliminar las minucias detectadas en los bordes, al tratarse de minucias espurias que disminuyen el rendimiento del sistema (véase Figura 6). Se calculó el histograma bidimensional de minucias (Figura 7) de las huellas seleccionadas y se observó que la una elevada proporción de las minucias se encontraban dentro de una zona elíptica, con una distribución relativamente uniforme. A partir de esta zona, se definió heurísticamente una región de interés (ROI) utilizada en los ataques para generar minucias solamente en su interior.

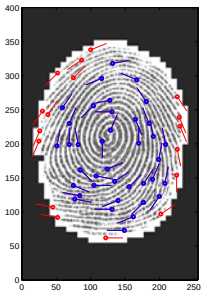
Para calcular el rendimiento de los sistemas a evaluar se ha procedido del siguiente modo: Las puntuaciones de usuario se han definido como las obtenidas por las distintas muestras de un dedo de un mismo usuario comparadas con una muestra de ese mismo dedo (plantilla de usuario). Por lo tanto, dadas las 150 plantillas de usuario, se obtienen $150 \times 9 = 1350$ puntuaciones de usuario que permitirán obtener la tasa de Falso Rechazo o FRR (*False Rejection Rate)*.



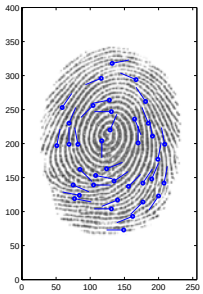
a) Extracción de minucias



b) Zona de baja calidad



c) Detección de las minucias artificiales



d) Eliminación de las minucias artificiales

Figura 6. Proceso de eliminación de minucias en los bordes de la huella

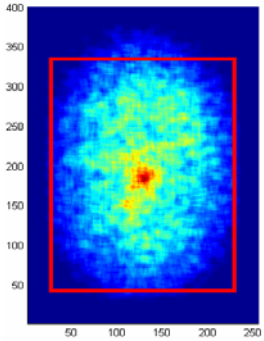


Figura 7. Histograma de minucias de las huellas utilizadas

Para obtener las puntuaciones de impostor se ha comparado una muestra de cada usuario con la plantilla del resto de usuarios. Por lo tanto, se dispone de $150 \times 149 = 22350$ puntuaciones de impostor.

En la Figura 8 se muestran las curvas de funcionamiento de los sistemas según el protocolo descrito. Para el sistema NFIS2, la tasa de igual error o *Equal Error Rate* (EER) se encuentra en un *score* de 26,5 con un valor de 1,47%. Las curvas de funcionamiento del sistema basado en *Match-on-Card* revelan, como cabía esperar dada su limitación, un rendimiento peor que el sistema NFIS2. La EER es del 9,78% para un *score* de 36,5 puntos. Ambos sistemas son comparados en la curva DET de la Figura 8.

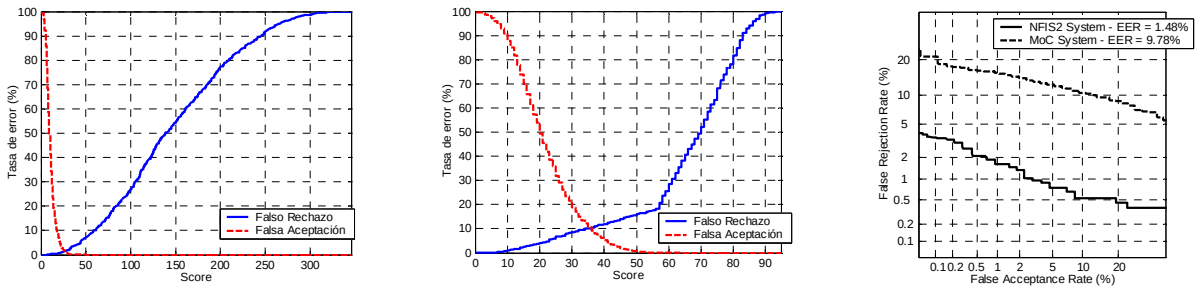


Figura 8. Curvas FA y FR obtenidas con el sistema NFIS2 (izquierda) y el sistema *Match-on-Card* (centro). Curvas DET de ambos sistemas (derecha)

El umbral de decisión establecido para el sistema NFIS2 es de 35 puntos, dando lugar a una FAR del 0.1% y una FRR del 3.33%. Por lo tanto, el número de intentos teóricos de un potencial ataque de fuerza bruta equivalente es de 1000. Para el sistema *Match-on-Card* se establece un umbral de 55 puntos, dando lugar a una FAR del 0.16% y una FRR del 17.33%. El número medio de iteraciones de un ataque de fuerza bruta equivalente será de 640 aproximadamente. La tasa de éxito de los ataques *hill-climbing* realizados se calculará en función de estos valores, considerando como ataques exitosos aquéllos que requieran un número inferior de iteraciones al mencionado para fuerza bruta.

El protocolo de ataques *hill-climbing* consiste en realizar ataques a cada una de las 150 huellas de usuario disponibles empleando en todas ellas la misma estrategia. Los resultados de los ataques se resumen en el apartado 3 del presente documento.

1.4 Conclusiones

En el presente proyecto se han estudiado las vulnerabilidades que presentan los sistemas basado en reconocimiento biométrico de huella dactilar. En concreto, se han implementado una clase de ataques *software* denominados *hill-climbing*.

Los resultados experimentales, descritos en el apartado 3 del presente documento, muestran que los dos sistemas bajo estudio son vulnerables ante ataques *hill-climbing*. El sistema *Match-on-Card* resulta menos robusto ante los ataques, proporcionando tasas de éxito del ataque considerablemente mayores. Este resultado está condicionado por las restricciones *hardware* del sistema, que obligan a que el algoritmo de verificación de los patrones de minucias sea lo suficientemente simple y eficiente como para ocupar pocos centenares de KB y ejecutarse en un tiempo razonable para el usuario.

Para ambos sistemas se ha llegado a una configuración de los ataques que permite elevar la tasa de éxito, a través de la modificación de los parámetros iniciales. Se observa que una parte de los ataques finalizados con éxito requiere un número mayor de iteraciones que las teóricas de fuerza bruta. Debe tenerse en cuenta que, a pesar de ser éste un valor teórico del número medio de intentos con huellas aleatorias, los ataques *hill-climbing* presentan numerosas ventajas con respecto a los de fuerza bruta. La principal ventaja es que no es necesario disponer de una base de datos de huellas reales con miles de ejemplares, como es el caso en ataques de fuerza bruta.

El éxito de los ataques frente a sistemas reales de verificación de huella dactilar abre un nuevo campo de investigación en lo referente a su seguridad. La información transferida en el interior del sistema de verificación debe ser ocultada para evitar estos ataques, lo cual no es siempre posible en sistemas que emplean más de un rasgo biométrico o requieren una configuración distribuida.

2 Originalidad

En este proyecto se ha implementado una técnica de ataque a sistemas biométricos basados en reconocimiento de huella dactilar. Los estudios acerca de ataques a sistemas de verificación de huella dactilar datan en general de la última década, proponiendo y analizando en su mayoría técnicas de ataque directo, es decir, presentando huellas falsas de algún material al sensor. Los ataques indirectos se comenzaron a estudiar más recientemente. En concreto, los ataques *hill-climbing* se han estudiado previamente para sistemas de reconocimiento de imágenes y de reconocimiento facial.

En el ámbito de la huella dactilar, esta técnica sólo se había documentado hasta ahora sobre un desarrollo de laboratorio no funcional, por lo que resultaba especialmente interesante analizarla sobre prototipos de reconocimiento de huella dactilar más cercanos a la aplicación final: un sistema de referencia a nivel mundial, del cual no se habían estudiado vulnerabilidades de esta clase hasta la fecha y un sistema basado en tarjeta inteligente *Match-on-Card,* el cual pertenece a una clase de sistemas sobre el que está generándose un creciente interés en la actualidad.

Las aportaciones de este proyecto al estado del arte y al diseño de sistemas de seguridad basados en huella dactilar son las siguientes:

- **En los experimentos se demuestra la aplicabilidad de los ataques, probando que los sistemas considerados son vulnerables frente a ellos.** Se comprueba por lo tanto la posibilidad de realización de los ataques en entornos realistas.

- **Se aborda una nueva perspectiva de estudio de la fiabilidad de los sistemas de verificación biométricos**: su vulnerabilidad frente a ataques y la penetrabilidad de los mismos. La evaluación del rendimiento de los sistemas biométricos suele hacerse únicamente en términos de tasas de error FAR (*False Acceptance Rate*), FRR (*False Rejection Rate*) y EER (*Equal Error Rate*), parámetros que son comúnmente utilizados en la literatura científica para describir el rendimiento de un sistema.

- **Este trabajo contempla una problemática nueva en los sistemas de verificación basados en tarjeta inteligente**: los sistemas basados en *smart-card* deben ser más simples para permitir que sean embebidos en un *chip*, por lo que resultan a priori más vulnerables frente a ataques en caso de que sea interceptado el canal de comunicaciones con el sistema de verificación.

- **Los ataques se realizan sobre una base de datos de huellas reconocida dentro de la literatura científica**, accesible y utilizada en numerosos estudios científicos por diferentes grupos de investigación, proporcionando resultados que pueden ser contrastados.

- **Se realiza un análisis sistemático de la influencia de los parámetros de configuración de los ataques.** Se modifican los ataques en función de la influencia de los parámetros en su rendimiento para lograr mejorar su tasa de éxito y adaptarlos a cada sistema.

3 Resultados

3.1 Resultados con el sistema NFIS2

En primer lugar se ha atacado el sistema NFIS2 utilizando los cuatro tipos de iteración descritos en el apartado 1.3.1. Como se puede observar en la Tabla 1, únicamente 2 huellas de las 150 son atacadas con éxito, y en 5000 iteraciones tan sólo 64 ataques logran superar el umbral. Si se establece la ROI descrita en el apartado 1.3.3 generando, añadiendo y desplazando minucias sólo en su interior, los resultados mejoran, sobre todo en el número de ataques finalizados antes de 5000 iteraciones (véase Tabla 1).

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
No	*a,b,c,d*	38	1,87	5,16	6,13	0,90	2/150	64/150
Sí	*a,b,c,d*	38	2,41	4,93	5,60	1,35	7/150	85/150

Tabla 1. Estadísticas de los ataques *hill-climbing* sobre NFIS2 empleando y sin emplear la ROI.

Como se puede observar en la Tabla 1, las iteraciones *b* y *c* logran más a menudo un ascenso de la puntuación que las iteraciones *a* y *d*, siendo la iteración *d* la que menos ascensos logra. En consecuencia, se estudia el rendimiento de los ataques eliminando las iteraciones que menos ascensos consiguen en media. Los resultados se muestran en la Tabla 2: se observa una clara mejoría en el rendimiento de los ataques, logrando una tasa de éxito de 40 sobre 150 ataques. El número de ataques finalizados es de 143, quedando únicamente 7 huellas tras 5000 iteraciones que no han logrado ser atacadas con éxito.

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
Sí	*a,b,c,d*	38	2,41	4,93	5,60	1,35	7/150	85/150
Sí	*a,b,c*	38	3,18	7,70	7,91	-	28/150	136/150
Sí	***b,c***	**38**	**-**	**9,25**	**9,76**	**-**	**40/150**	**143/150**

Tabla 2. Estadísticas de los ataques *hill-climbing* sobre NFIS2 eliminando las iteraciones que peor rendimiento presentan.

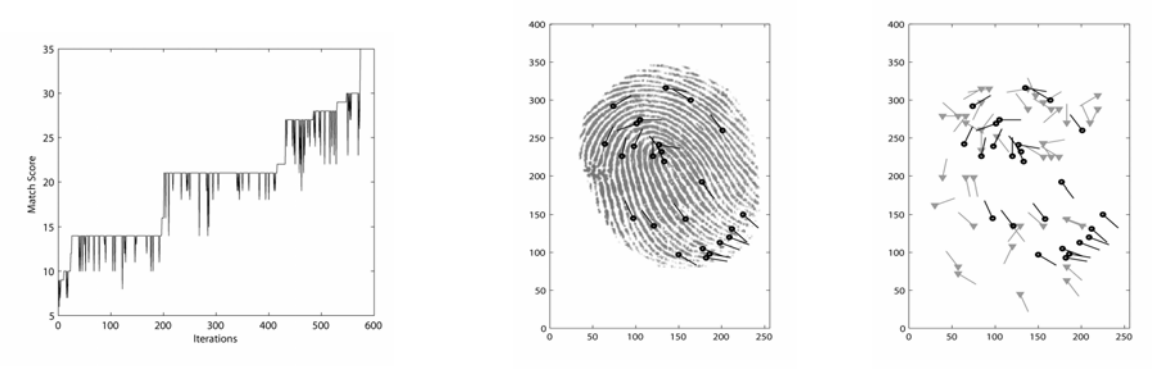
En último lugar, se estudia la influencia del número de minucias iniciales en el rendimiento de los ataques. Se lanzan ataques con un número inicial superior y otro inferior que la media de minucias previamente calculada (38 minucias) y se observa (véase la Tabla 3) que su rendimiento es peor. Por lo tanto, el hecho de comenzar el ataque con un número de minucias correspondiente a la media es de gran relevancia en ataques frente al sistema NFIS2.

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
Sí	*b,c*	25	-	10,85	8,95	-	28/150	136/150
Sí	*b,c*	38	-	9,25	9,76	-	40/150	143/150
Sí	*b,c*	55	-	5,68	13,67	-	12/150	132/150

Tabla 3. Estadísticas de los ataques *hill-climbing* sobre NFIS2 empleando diferentes números de minucias iniciales.

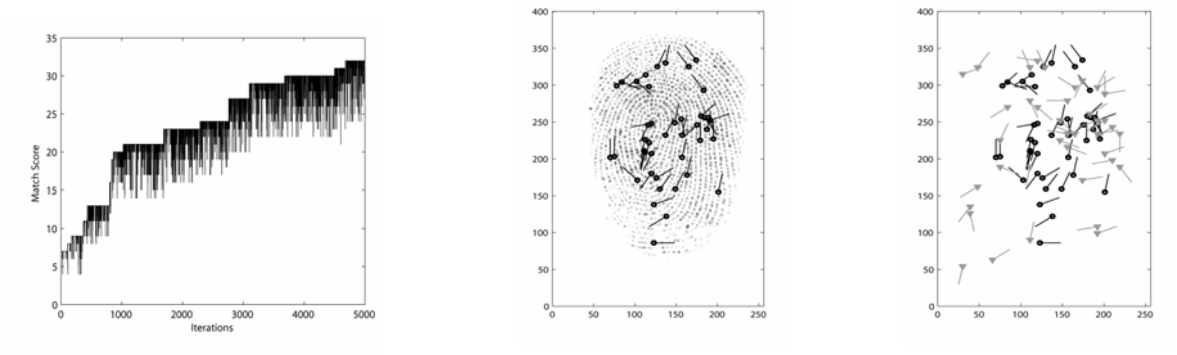
En la Figura 9 se muestra la progresión de la puntuación, la huella atacada y las minucias de la huella sintética que logra una puntuación superior al umbral frente a las originales de un ataque relativamente rápido frente al sistema NFIS2. Visualmente, la relación existente entre ambos patrones es escasa o nula, lo cual está condicionado por la técnica de *matching* que

emplea el sistema NFIS2, invariante a rotaciones y desplazamientos. La Figura 10 muestra los mismos datos para un ataque sin éxito.



(a) (b) (c)

Figura 2. (a) Progresión de la puntuación, (b) minucias originales de la huella y (c) minucias originales (círculos negros) vs, minucias sintéticas que logran una puntuación mayor que el umbral (35 puntos) de decisión en un ataque relativamente rápido a NFIS2 (menos de 600 iteraciones).



(a) (b) (c)

Figura 3. (a) Progresión de la puntuación, (b) minucias originales de la huella y (c) minucias originales (círculos negros) vs, minucias sintéticas finales en un ataque que no logra superar el umbral frente a NFIS2 en menos de 5000 iteraciones.

3.2 Resultados con el sistema basado en *Match-on-Card*

En los ataques realizados al sistema basado en *Match-on-Card*, se parte de los resultados previamente obtenidos frente a NFIS2: se emplean únicamente las iteraciones *b* y *c*, y se emplea la ROI establecida. Se comienza observando la influencia del número de minucias iniciales en la tasa de éxito. En la Tabla 4 se observa un nuevo fenómeno: los ataques con un número inicial de minucias menor que la media, concretamente de 25, obtienen una tasa de éxito mucho mayor que los que comienzan con 38. Se observa que un descenso mayor, hasta 10 minucias iniciales empeora los resultados.

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
Sí	*b,c*	10	-	7,70	5,30	-	65/150	133/150
Sí	*b,c*	25	-	5,53	10,08	-	123/150	146/150
Sí	*b,c*	38	-	3,55	13,27	-	78/150	139/150

Tabla 4. Estadísticas de los ataques *hill-climbing* sobre el sistema *Match-on-Card* variando el número inicial de minucias.

El ataque con 25 minucias iniciales logra una tasa de éxito de 123 sobre 150 huellas totales y en menos de 2000 iteraciones lograr atacar con éxito a 146 huellas. Posteriormente, empleando 25 minucias iniciales se comprueba si realmente en el sistema *Match-on-Card* la influencia de cada tipo de iteración es similar al caso de NFIS2.

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
Sí	*a,b,c,d*	25	1,22	4,60	5,71	4,68	52/150	132/150
Sí	*b,c,d*	25	-	5,24	5,98	5,03	79/150	138/150
Sí	***b,c***	**25**	**-**	**5,53**	**10,08**	**-**	**123/150**	**146/150**

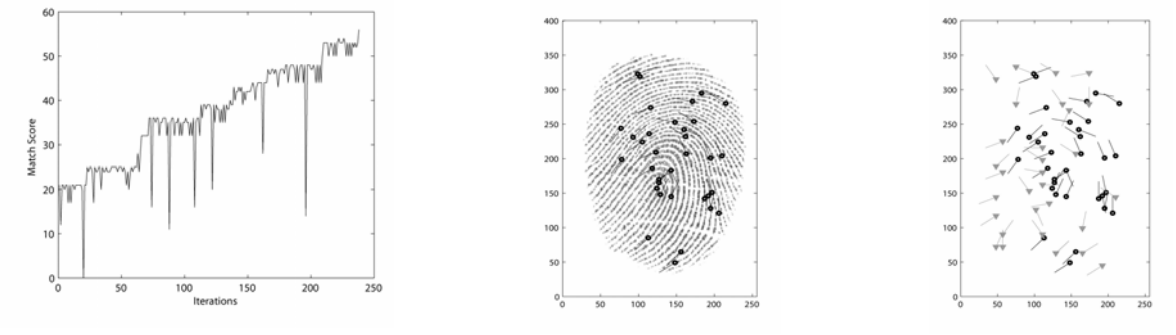
Tabla 5. Estadísticas de los ataques *hill-climbing* sobre el sistema *Match-on-Card* en función del tipo de las iteraciones empleadas

Se puede observar en la Tabla 5 cómo de nuevo las iteraciones *b* y *c*, son las que logran una tasa de éxito mucho mayor. Finalmente, se comprueba si realmente el hecho de establecer una ROI para el sistema basado en *Match-on-Card* es positivo, confirmándolo con el experimento reflejado en la Tabla 6.

ROI	Iteraciones	Minucias Iniciales	Número medio de mejoras				Tasa de éxito	Ataques finalizados en 5000 iteraciones
			a	*b*	*c*	*d*		
Sí	*b,c*	25	-	5,53	10,08	-	123/150	146/150
No	*b,c*	25	-	6,13	9,15	-	91/150	148/150

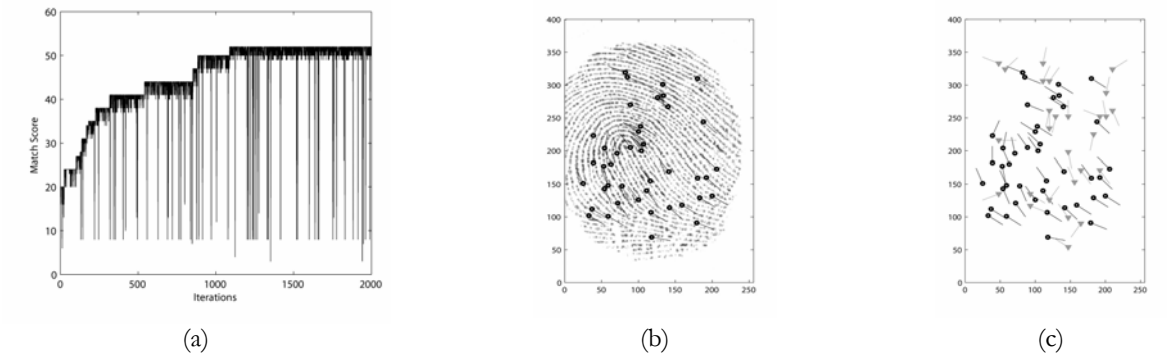
Tabla 6. Estadísticas de los ataques *hill-climbing* sobre el sistema *Match-on-Card* empleando y sin emplear la ROI.

En las Figuras 11 y 12 se muestran de nuevo dos ejemplos de ataque en el caso del sistema *Match-on-Card*. En todos los casos, las huellas para las que no se logra llevar a cabo un ataque con éxito parecen no guardar una relación entre sí ni se repiten en cada ataque.



(a) (b) (c)

Figura 4. (a) Progresión de la puntuación, (b) minucias originales de la huella y (c) minucias originales (círculos negros) vs, minucias sintéticas que logran una puntuación mayor que el umbral (55 puntos) de decisión en un ataque relativamente rápido a el sistema *Match-on-Card.*



(a) (b) (c)

Figura 5. (a) Progresión de la puntuación, (b) minucias originales de la huella y (c) minucias originales (círculos negros) vs, minucias sintéticas finales en un ataque que no logra superar el umbral frente al sistema basado en *Match-on-Card.*

4 Aplicabilidad

En el diseño de sistemas de seguridad basados en reconocimiento biométrico, la evaluación de sus posibles vulnerabilidades es una parte clave. Generalmente los sistemas de reconocimiento biométrico son evaluados según su tasa de error, sin tener en cuenta las vulnerabilidades a ataques directos o indirectos.

Los sistemas de reconocimiento de huella dactilar están experimentando un fuerte crecimiento en su campo de implementación, sustituyendo a *passwords* en numerosos dispositivos electrónicos. Por lo tanto, una **evaluación integral de su seguridad** es necesaria. Dentro de esta ámbito, la aplicabilidad del proyecto se puede resumir en los siguientes aspectos:

- Este trabajo **proporciona un marco de evaluación de la seguridad de sistemas biométricos basados en huella dactilar**, describiendo los algoritmos y protocolos necesarios para implementar ataques *hill-climbing*. Se presentan además otras técnicas de ataque a los sistemas biométricos, que son propuestas para la evaluación conjunta de la vulnerabilidad de los sistemas basados en huella dactilar frente a ataques.

- A partir de los resultados obtenidos, en los que **se demuestra la vulnerabilidad** de ambos sistemas, se pueden extender nuevos ataques de este tipo a otros sistemas de reconocimiento biométrico. Las conclusiones extraídas de este trabajo, **proponen considerar un punto más de evaluación de la seguridad en el diseño de un sistema** de reconocimiento de huella comercial. La vulnerabilidad frente a ataques de esta clase deberá ser evaluada, o se deberán tomar medidas para evitar que este tipo de ataques puedan producirse.

Los ataques *hill-climbing* propuestos **pueden encuadrarse dentro de un protocolo de evaluación de la seguridad** de sistemas basados en reconocimiento dactilar. De hecho, tras el creciente interés comercial que ha surgido en la última década en relación a los sistemas automáticos de identificación personal basados en rasgos biométricos se ha creado un subcomité dedicado a la identificación biométrica (SC37), dentro del comité conjunto ISO/IEC sobre tecnologías de la información (JTC1).

Adicionalmente se ha propuesto la estandarización en la evaluación de la seguridad de sistemas biométricos a través de la iniciativa CC (***Common Criteria***). Esta iniciativa es la de mayor éxito y aceptación a nivel internacional para la evaluación de la seguridad en Tecnologías de la Información.

La estructura de CC permite gran flexibilidad para la caracterización de módulos o productos de seguridad. Como resultado, tanto consumidores como desarrolladores y evaluadores tienen herramientas para definir, caracterizar, evaluar y garantizar las funciones de seguridad o la seguridad objetivo (*Security Target* –ST) de módulos o productos (*Target of Evaluation* –TOE) de acuerdo a una serie de perfiles de seguridad estándar (*Protection Profile* –PP), y asegurar un determinado nivel de seguridad (*Evaluation Assurance Levels* –EAL) de entre los predefinidos. Por lo tanto, **las nuevas técnicas de ataque que se propongan, podrán encuadrarse dentro de protocolos de test de seguridad** en los sistemas biométricos.

El estudio de los ataques a un sistema de seguridad, tiene como finalidad **proponer contramedidas ante potenciales ataques**. En el proyecto se proponen algunas medidas de seguridad para proteger los sistemas de verificación ante esta clase de ataques:

- La aproximación más básica es la **ocultación de los resultado**s, algo no siempre posible en entornos que requieran sistemas sencillos (como es el caso del sistema *Match-on-Card* evaluado), en sistemas que se empleen puntuaciones de varios *matchers* para obtener una puntuación global (sistemas multimodales, que utilizan varios rasgos biométricos o sistemas que empleen fusión de *scores* obtenidos en diferentes comparadores*)* o en sistemas distribuidos, que envían la información entre los diferentes módulos a través de canales accesibles, como redes IP.

- Otro método propuesto es la **cuantificación de los resultados**, que provoca que las leves modificaciones introducidas por el atacante en la huella no supongan un incremento o decremento de la puntación, impidiendo la progresión del ataque. De todos modos, este método puede resultar ineficiente si se diseñan correctamente los ataques.

- Existe adicionalmente la posibilidad de **reducir el número máximo de intentos** de acceso a un sistema en un determinado periodo de tiempo, por ejemplo, en un día. En este caso, al estar basados los ataques en sucesivos intentos, sería más complicada su aplicación. A pesar de ello, esta técnica consigue únicamente alargar en el tiempo la progresión de los ataques, pero un atacante podría lograr acceder al sistema tras varios días.

Apéndice I: Referencias

[1] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security* Vol. 1, No. 2, pp. 125-143, June 2006

[2] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar. "Handbook of Fingerprint Recognition", *Springer* 2003.

[3] U. Uludag, A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints", *Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents* VI, 5306:622-633, San Jose, CA, January 2004.

[4] R. Sanchez-Reillo, L. Mengihar-Pozo, and C. Sanchez-Avila. "Microprocessor smart cards with fingerprint user authentication". *IEEE AESS Systems Magazine*, 18(3):22–24, March 2003.

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

Apéndice II: Financiación

Este proyecto ha contado con la siguiente financiación:

Proyecto: Vulnerabilidad de Sistemas de Seguridad Basados en Sensores de Huella Dactilar
Entidad financiadora: Subsecretaría de Defensa, Ministerio de Defensa (Procedimiento negociado sin publicidad –concurso público)

Proyecto: BIOSECURE NoE, Biometrics for Secure Authentication
Entidad financiadora: Comisión Europea, Red de Excelencia del 6º Programa Marco, IST-2002-507634

Proyecto: BIOSECUR-ID, Seguridad Multimodal basada en Autenticación Biométrica mediante Fusión de Expertos Unimodales
Entidad financiadora: Ministerio de Ciencia y Tecnología, Plan Nacional de I+D+i, TIC2003-08382-C05

Apéndice III: Publicaciones

El proyecto ha dado lugar a la publicación del trabajo "*Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification*" en el congreso internacional 40th Annual IEEE International Carnahan Conferences Security Technology, anexado a continuación y publicado bajo la siguiente referencia:

> M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia and J. A. Siguenza, "Hill-climbing and brute-force attacks on biometric systems: A case study in Match-on-Card fingerprint verification", in Proc. *IEEE Intl. Carnahan Conf. on Security Technology, ICCST*, pp. 151-159, Lexington, USA, October 2006.

Adicionalmente, ha dado pie al envío de un artículo a la revista IEEE Transactions on Information Forensics and Security, aún en proceso de revisión:

> J. Galbally, J. Fierrez, M. Martinez-Diaz, J. Ortega-García, J. Gonzalez-Rodriguez, "An Analysis of Direct and Indirect Attacks to Fingerprint Verification Systems", under review *IEEE Trans. on Information Forensics and Security,* 2007.

Anexos

"Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification"

Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification

M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia, J.A. Siguenza
ATVS/Biometrics Research Lab, Escuela Politecnica Superior - Universidad Autonoma de Madrid
C/ Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, Spain
{julian.fierrez, fernando.alonso, javier.ortega}@uam.es

Abstract

In this paper, we study the robustness of state-of-the-art automatic fingerprint verification systems against hill-climbing and brute-force attacks. We compare the performance of this type of attacks against two different minutiae-based systems, the NIST Fingerprint Image Software 2 (NFIS2) reference system and a Match-on-Card based system. In order to study their success rate, the attacks are analyzed and modified in each scenario. We focus on the influence of initial conditions in hill-climbing attacks, like the number of minutiae in the synthetically generated templates or the performance of each type of modification in the template. We demonstrate how slight modifications in the hill-climbing algorithm lead to very different success rates.

1. Introduction

Biometrics is becoming an important issue in our society [1]. The heightened interest in biometrics-based automated personal identification has resulted in the development of several commercial biometric recognition systems. Fingerprints are one of the most commonly used biometrics due to their reduced size and acceptability [2]. Despite the development of fingerprint recognition techniques, there are many security concerns [3] which still make it a topic for discussion.

One of the hot topics within biometrics are Match-on-Devices, and in particular Match-on-Card based systems for fingerprint recognition. Smart-cards allow to encrypt and protect stored information and to execute matching algorithms [4]. Thus, the user's fingerprint template and the matching algorithm can be stored in a smart-card without compromising its security. Corroborating this increasing interest in Match-on-Card systems, in the Fingerprint Verification Competition (FVC) 2004 [5], a special evaluation track for matching systems with reduced time and memory restrictions was introduced. Furthermore, in this year's competition, FVC 2006 [6], a new category including Match-on-Card systems has been proposed.

A fingerprint recognition system is vulnerable to attacks which may decrease its security level. Ratha *et al.* [7] have studied and classified these attacks in 8 different types. Attacks from type 1 are aimed at the sensor and can be carried out using fake fingerprints. Types 3, 5 and 6 may be performed as Trojan Horse attacks, bypassing the feature extractor, the matcher, and the system database respectively. Types 2, 4, 7 and 8 attack communication channels and can either try to intercept information or insert it into the channel. Possible attack points in a general biometric recognition system are depicted in Fig. 1.

In this study, we focus on attacks known as *hill-climbing* attacks [8]. Hill-climbing attacks consist of an application that sends synthetically generated minutiae templates to the matcher and, according to the match score, randomly modifies the templates until the decision threshold is exceeded. We implement hill-climbing attacks against both the NFIS2 reference system [9] and a Match-on-Card (MoC) system, and then study some factors involved in the success rate of the attack. A direct comparison is also made between our hill-climbing attacks and brute-force attacks.

Using smart-card embedded matching systems for fingerprint recognition has already been studied [4, 10] but, to the best of our knowledge, no attacks aimed directly to the smart-card matcher have been reported in the literature.

The rest of the paper is organized as follows. Hill-climbing and brute force attacks are explained in Sect. 2, the fingerprint recognition systems under attack are presented in Sect. 3, experiments are described in Sect. 4, and conclusions are finally drawn in Sect. 5.

2. Hill-climbing and Brute-Force Attacks

Hill-climbing attacks against automated fingerprint recognition systems have been studied by Uludag and Jain [8] and Soutar [12]. A hill-climbing attack may be performed by an application that sends random templates to the system, which are perturbed iteratively. The application reads the output match score and continues with the perturbed template only when the matching score increases until the decision threshold is exceeded.

A hill-climbing attack may be of type 2 or 4, depending on the point of attack. Soutar proposed in [12] a type

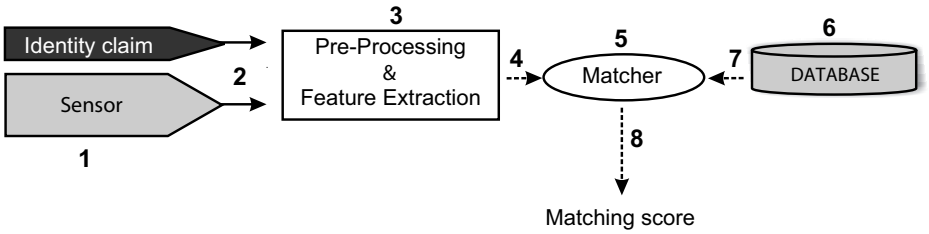


Figure 1. Architecture and dataflow paths of an automated biometric verification system. Possible attack points are numbered from 1 to 8.

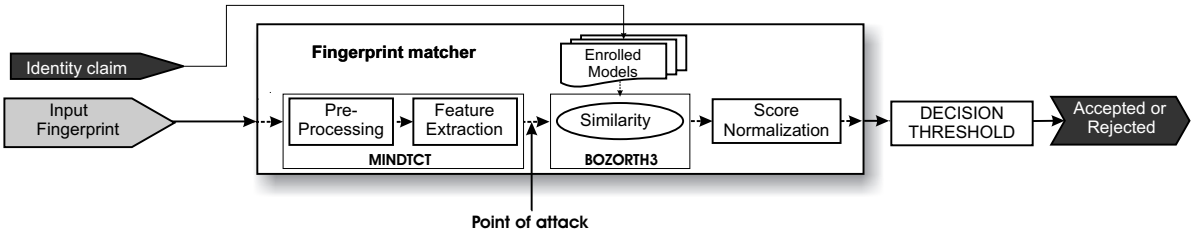


Figure 2. Architecture, dataflow paths and point of attack of the NFIS2 system.

2 attack with a face recognition system. The input image is conveniently modified until a desired matching score is attained. In [8], a type 4 attack against a minutiae-based fingerprint recognition system is described. Uludag and Jain [8] propose an attack based on synthetic random minutiae templates which are modified, one minutia at a time, until the decision threshold is exceeded.

In this paper, we study a hill-climbing attack based on the one presented by Uludag and Jain [8]. The template format of the matching systems must be known by the attacker as well as the input image size. Note that the image size is easy to obtain in general as it is normally made public by the fingerprint sensor vendors.

The efficiency of a hill-climbing attack may be evaluated by comparing the mean number of iterations needed to break each user account with the estimated number of attempts a brute-force attack would require [8]. The average number of attempts needed by a brute-force attack can be derived from the FAR of the system. A type 4 brute-force attack may be performed by sending real minutiae templates to the matcher until the system wrongly accepts one as corresponding to the template from the user's account under attack. Note that a brute-force attack using random synthetic templates would need more iterations than the number derived from the FAR as the FAR is calculated using real minutiae templates as inputs, not synthetic random ones.

3. Fingerprint Matching Systems

3.1. Reference System

We use the minutiae-based verification system from the NIST Fingerprint Image Software package (NFIS2) [9] as a reference system for our attacks. The architecture of the system and the point of attack, where the synthetic templates shall be introduced, are depicted in Fig. 2.

NFIS2 is a PC-based fingerprint processing and recognition system composed of independent software modules. In our experiments we will use two of the software modules included in NFIS2: MINDTCT and BOZORTH3. MINDTCT is the minutiae extraction subsystem. It generates an output text file containing the location, orientation and quality of each minutia from a fingerprint image input file. Direction maps and quality maps, among other output files are also generated for each image file.

BOZORTH3 performs the matching between any number of fingerprint templates which must have the same format as the output of MINDTCT. It is a rotation and translation invariant algorithm since it computes only relative distances and orientations. BOZORTH3 first constructs intra-compatibility tables, which are lists of associations between pairs of minutiae and their relative distance from the same fingerprint. It then looks for potential compatible minutiae pairs from the two fingerprints based on a specified tolerance and stores them in an inter-compatibility table. In the last step, it first traverses the inter-compatibility table, combining its entries into clusters, and then combines the clusters, building graphs. The larger the graph, the larger the match score will be. In our system, the match score is not normalized.

3.2. Match-on-Card (MoC) System

The Match-on-Card (MoC) system under consideration is a proprietary prototype. The matcher is fully embedded in a smart-card and may only be accessed via a smart-card reader connected to a PC.

One of the main differences between this system and the

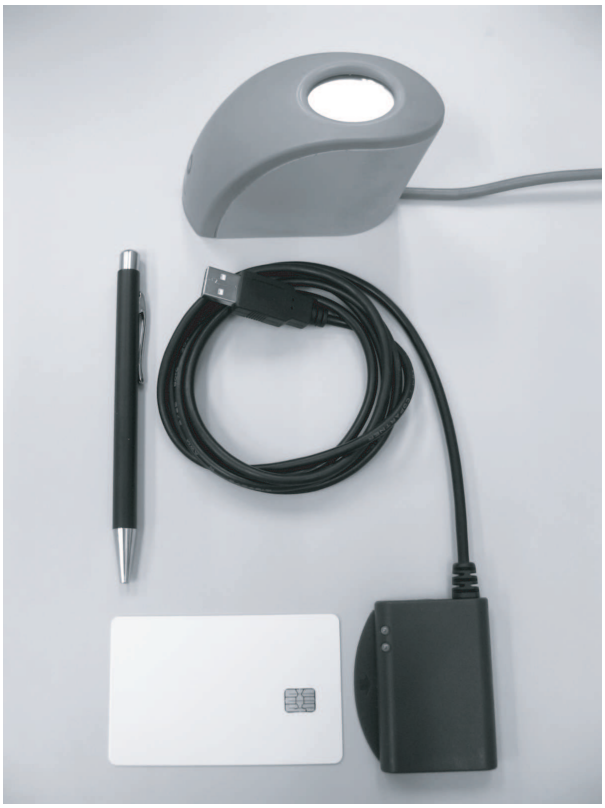


Figure 3. Top: Digital Persona fingerprint sensor used for acquiring the fingerprints used in our experiment [11]. Bottom: Smart-card and smart-card reader used in our experiments.

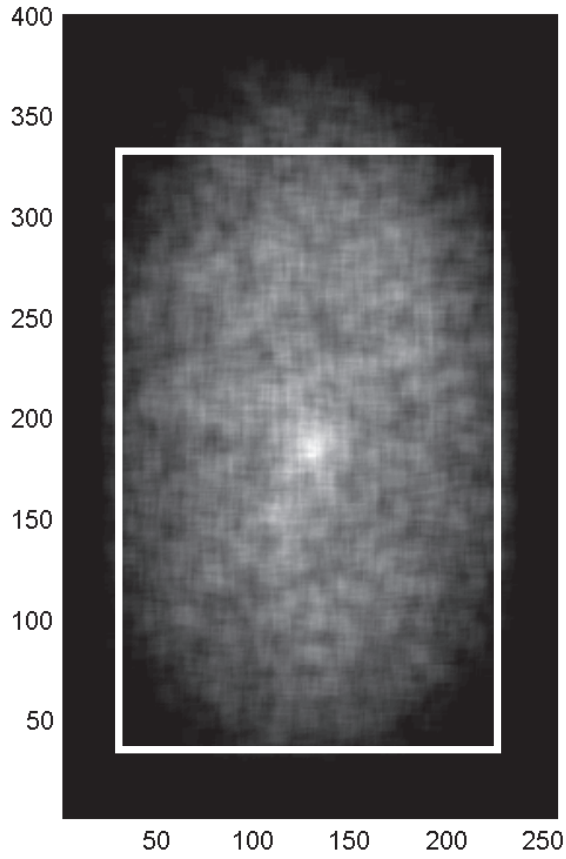


Figure 4. Minutiae location histogram from the selected subcorpus of MCYT [11]

reference system explained in Sect. 3.1 is that a MoC system is hardware limited. A smart-card has a very limited processing capacity and the matching algorithm should be efficient enough to perform the match in a reasonably short time. There has been much work in this field resulting in many algorithm proposals which try to reduce the matching computational cost [4, 10, 13]. The MoC system used in our experiments is shown in Fig. 3.

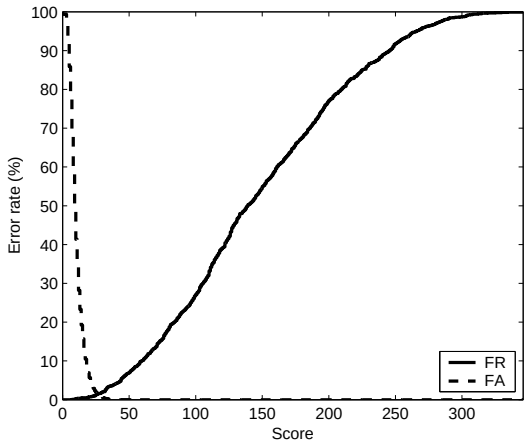
The smart-card reader is attached to a PC via USB, so the attacks can be performed from the PC. The user's fingerprint template is also stored in the smart-card memory. We only know the template storing format, which is also minutiae-based. In our experiments, we use the NFIS2 MINTDCT module (see Sect. 3.1) for the minutiae extraction phase and then perform the required transformations to the output file to make it compatible with this system. Note that the minutiae extraction phase would never be carried out by the smart-card, it must be done by an external application. The matcher returns the score as an integer value in a range from 0 to 100, 100 being the maximum likelihood between both fingerprints. The matching algorithm is unknown, but as the template format and the matching score are accessible, a hill-climbing attack may be performed.

4. Experiments

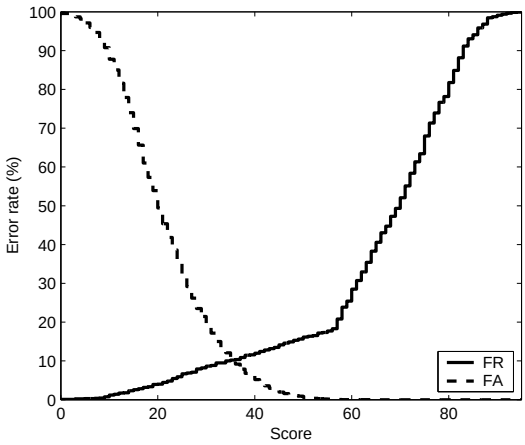
4.1. Database

The attack algorithms presented above have been tested on a sub-corpus from the MCYT database [11]. The fingerprint images are acquired with a 500 dpi optical sensor, model UareU by Digital Persona (see Fig. 3). We consider 10 samples from the right and left index fingers of 75 users, with 6 samples acquired with a high level of control [11] (i.e. small rotation or displacement from the center of the sensor), 2 with medium control level, and the last 2 samples with low control level. Therefore there are $75 \times 2 \times 10 = 1500$ samples.

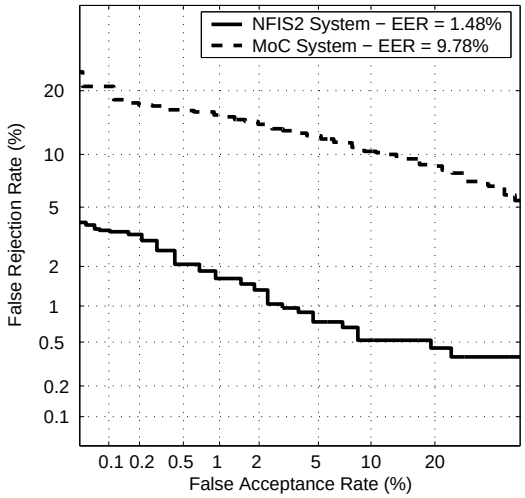
We compute the two-dimensional histogram of the minutia locations of all the fingerprints of the considered subcorpus. Fig. 4 depicts this histogram and a rectangle obtained heuristically that contains most minutiae. It can be seen that there are nearly no minutiae outside an elliptic region. Minutiae are nearly uniformly distributed in the rectangle with a higher concentration at its center. This rectangle will be used in our hill-climbing attacks as explained in Sect. 4.2. In the selected sub-corpus from the database



(a) FA and FR curves for the NFIS2 system



(b) FA and FR curves for the MoC system



(c) DET curves

Figure 5. Verification performance of both systems

described in Sect. 4.1, the mean number of minutiae is 38.

The verification performance of both systems is also studied. We use one of the low control samples as a template and the other 9 samples from the same finger as probes to test genuine matches, leading to $150 \times 9 = 1350$ genuine user scores. Impostor scores are obtained comparing each template to one sample from each other finger of the subcorpus, thus we have $150 \times 149 = 22350$ impostor scores. Fig. 5 depicts the FA, FR and DET curves from both systems.

4.2. Experimental Protocol

Our experiments are based on the ones presented in [8]. A number of 100 initial synthetic random templates are generated and sent to the matcher to attack a specific user account. Synthetic templates are generated with a fixed number of minutiae which is the mean number of minutiae in the fingerprints from the database (25 in [8]) and dividing the template into 9×9 pixel cells. A cell can contain only one minutia to avoid generating minutia which are closer than the inter-ridge distance.

The template that attains the highest matching score is saved. This template is iteratively modified by:

a) Perturbing an existing minutia by moving it to an adjacent cell or by changing its orientation.
b) Adding a minutia.
c) Substituting a minutia.
d) Deleting a minutia from the template.

If the matching score increases in any of these iterations, the modified template is saved, otherwise it is not.

In our experiments, we study the effects of different attack parameters by observing which iterations achieve, on average, more matching score increases during the attacks. We also study the influence of the initial number of minutiae and how these can be generated to improve the perfor-

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
No	a, b, c, d	38	1,87	5,16	6,13	0,90	2/150	64/150
Yes	a, b, c, d	38	2,41	4,93	5,60	1,35	7/150	85/150

(a) Hill-climbing statistics using all iterations with and without ROI.

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
Yes	a, b, c, d	38	2,41	4,93	5,60	1,35	7/150	85/150
Yes	a, b, c	38	3,18	7,70	7,91	-	28/150	145/150
Yes	b, c	38	-	9,25	9,76	-	40/150	143/150

(b) Hill-climbing statistics deleting low performing iterations.

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
Yes	b, c	25	-	10,85	8,95	-	28/150	136/150
Yes	b, c	38	-	9,25	9,76	-	40/150	143/150
Yes	b, c	55	-	5,68	13,67	-	12/150	132/150

(c) Hill-climbing statistics using a different number of initial minutiae.

Table 1. Hill-climbing results on NFIS2

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
Yes	b, c	10	-	7,70	5,30	-	65/150	133/150
Yes	b, c	25	-	5,53	10,08	-	123/150	146/150
Yes	b, c	38	-	3,55	13,27	-	78/150	139/150

(a) Hill-climbing statistics using a different number of initial minutiae.

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
Yes	a, b, c, d	25	1,22	4,60	5,71	4,68	52/150	132/150
Yes	b, c, d	25	-	5,24	5,98	5,03	79/150	138/150
Yes	b, c	25	-	5,53	10,08	-	123/150	146/150

(b) Hill-climbing statistics deleting low performing iterations.

ROI	Iterations	Initial Minutiae	Mean score raises				Success Rate	Total accounts broken in 5000 iterations
			a	b	c	d		
Yes	b, c	25	-	5,53	10,08	-	123/150	146/150
No	b, c	25	-	6,13	9,15	-	91/150	148/150

(c) Hill-climbing statistics with and without rectangular ROI.

Table 2. Hill-climbing results on the Match-on-Card system

mance of our attacks. A first attack will be performed using the mean number of minutiae in our database and the four types of iterations.

In each attack, the 150 user templates are attacked using the same method (same initial minutiae generating scheme, same type of iterations and decision point) and statistics are gathered about the success rate of the attack. According to the results, the attacks are modified in order to better understand the factors involved in the success rate.

The synthetically generated templates will first have a random uniform minutiae distribution of 38 minutiae, which is the mean number of minutiae in our database.

For the NFIS2 system, we choose a decision threshold of 35 for the match score, leading to a 0.10% FAR and a 3.33% FRR. This means that a brute-force attack would theoretically need an average of 1000 iterations. For the Match-on-Card system a decision threshold of 55 is selected, resulting in a FAR of approximately 0.16% and a FRR of 17.33%. Thus, for the MoC system, 640 iterations would be needed by a brute-force attack.

We define the *success-rate* of an attack as the proportion of fingerprints for which the decision threshold is reached using less iterations than a brute-force attack. We establish a maximum of 5000 and 2000 iterations for the NFIS2 and the MoC system respectively.

4.3. Experimental Results

We first attack the NFIS2 system using the method described in [8]. As it has been said in Sect. 4.1, there is a region where it is most probable to find minutiae. From now on, we will refer to this region as the Region Of Interest (ROI). We subsequently run the algorithm considering only minutiae in the inside of the ROI, i.e. without generating, adding or displacing any minutia outside the ROI. Table 1.(a) studies the introduction of the ROI in the basic configuration of the attack, showing an improvement in the attack success rate when considering minutiae only within the ROI (from 2/150 to 7/150).

Next we focus on the influence of the different types of iterations. As it can be seen in Table 1.(a), each type of iteration achieves a different mean number of score raises during the attacks. Table 1.(b) shows the success improvements using only the best performing iterations. Iterations b and c, (add and substitute a minutia respectively) are the ones which achieve a higher rate of score raises, achieving a success rate of 40/150.

Finally, for the NFIS2 system, we study how the initial number of minutiae in the 100 synthetic initial random templates affect the attack performance. Table 1.(c) shows the different success rates for three different initial configurations. It can be seen that attacks with a number of initial minutiae different to the average in the database (38 in our case) perform much worse than those with this average number of initial minutiae. Fig. 6 shows the score progression and the minutiae maps of a successful hill-climbing attack on NFIS2 while Fig. 7 shows the same data for an unsuccessful attack.

For the Match-On-Card system, we start with the best configuration obtained by the NFIS2 system. We first study the influence of the initial number of minutiae, see Table 2.(a). As it can be seen, 25 initial minutia achieve better results (success rate of 123/150) than the mean number of minutiae (success rate of 78/150). This may be an effect of the limited capacity of the MoC matching algorithm.

In the next experiment, we study the influence of each iteration. Table 2.b shows the results obtained. Again, as on the NFIS2 system, iterations b and c are the most effective ones. The poor performance of iteration a points out that the MoC system is not very sensitive to small minutiae displacements or rotations. The attack score progression and the minutiae maps of a successful attack are depicted Fig. 8. The same data same data for an unsuccessful attack is shown in Fig. 9.

Finally we study the relevance of using the ROI under this configuration. In Table 2.(c) we see the decrease in performance without using the ROI (from 123/150 to 91/150 success rate).

5. Conclusions

In this paper, we have performed and studied hill-climbing attacks on the NFIS2 reference system and a Match-on-Card embedded system. NFIS2 is a PC-based fingerprint recognition system while the MoC system is a hardware limited system.

As it has been shown, the performance of hill-climbing attacks is heavily dependent upon the system under attack and the iterations that are performed. Attacks with a reduced number of minutiae are highly successful against the MoC system, while their performance against NFIS2 is very poor.

NFIS2 has proven to be more robust against hill-climbing attacks, at least with a reduced number of iterations. On the other hand, if we allow for a higher number of iterations (such as 5000 in our experiments), most accounts can be broken. It may be derived from the results that hill-climbing attacks are less effective than brute-force attacks, at least in the case of NFIS2. This statement must be taken with care, as hill-climbing attacks require much less resources than the ones needed by a brute-force attack. In fact, to perform an efficient brute force attack, the attacker must have a database of more than a thousand of real fingerprint templates, whereas there is no need for real templates in the case of a hill-climbing attack.

Acknowledgments

This work has been supported by the Spanish Ministry of Defense, BioSecure NoE and the TIC2003-08382-C05-01 project of the Spanish Ministry of Science and Technology. F. A.-F. and J. F.-A. thank Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting their studies.

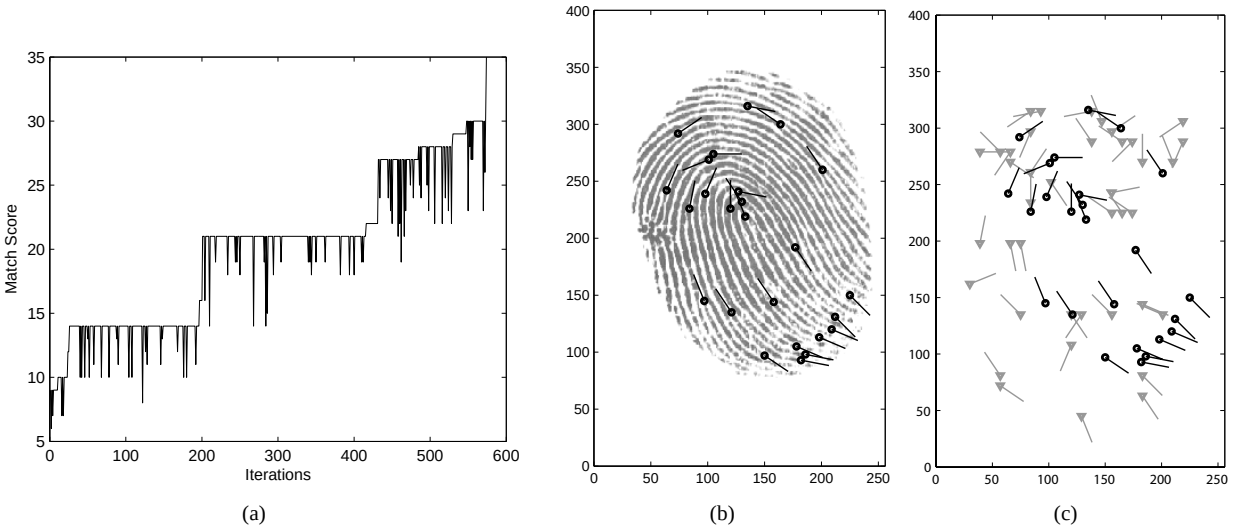


Figure 6. (a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) that achieve a higher score than the decision point on NFIS2 in a relatively short attack

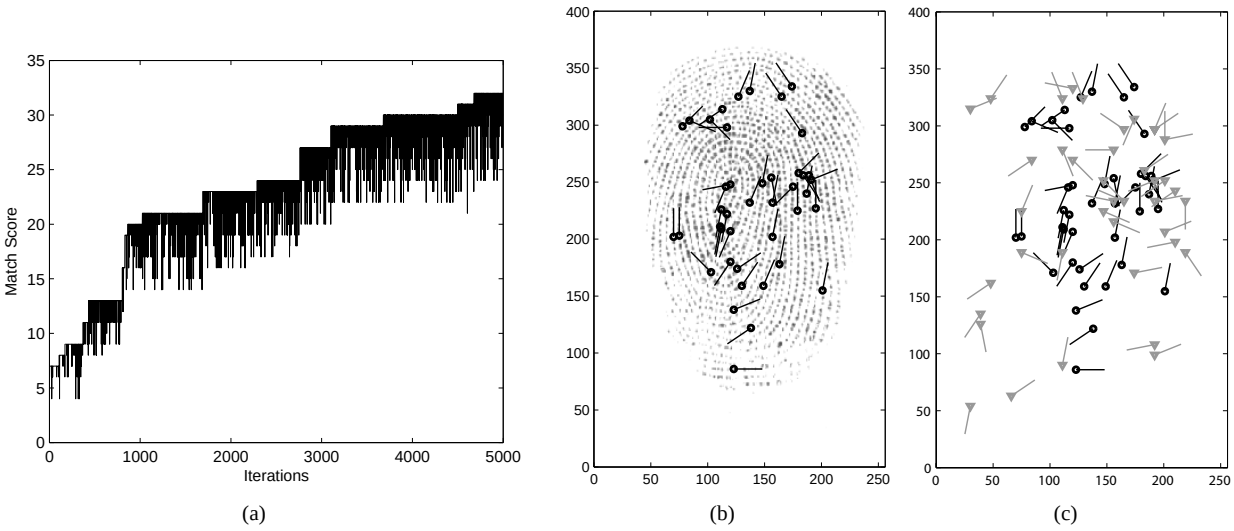
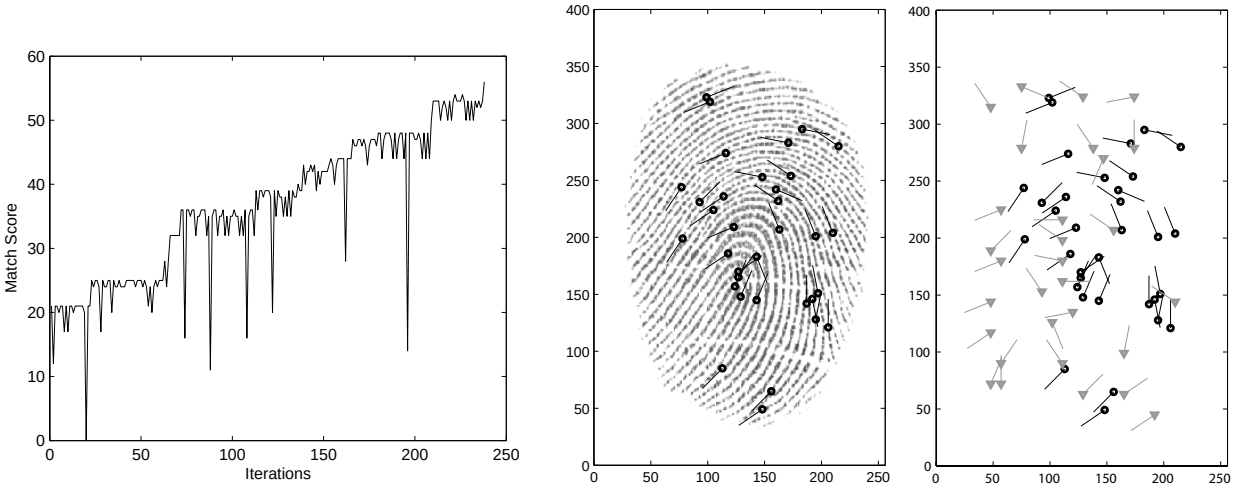
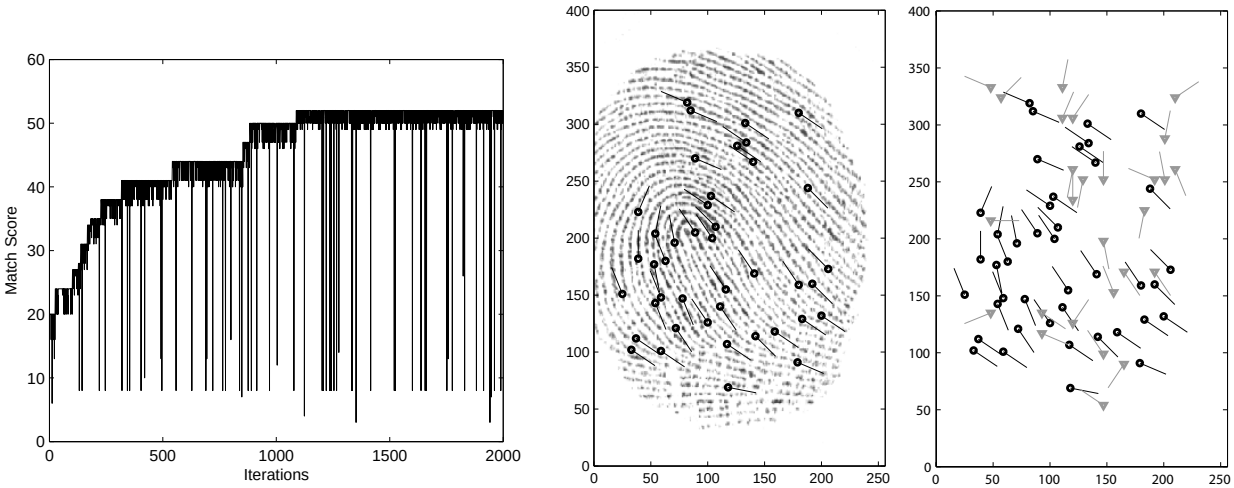


Figure 7. (a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) after 5000 iterations on NFIS2 in an unsuccessful attack



(a) (b) (c)

Figure 8. (a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) that achieve a higher score than the decision point on the MoC system in a relatively short attack



(a) (b) (c)

Figure 9. (a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) after 2000 iterations on the MoC system in an unsuccessful attack

6 References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[3] A. K. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," *Proc. of 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey*, 2005.

[4] R. Sanchez-Reillo, L. Mengihar-Pozo, and C. Sanchez-Avila, "Microprocessor smart cards with fingerprint user authentication," *IEEE AESS Systems Magazine*, vol. 18(3), pp. 22–24, March 2003.

[5] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, pp. 3–18, 2006.

[6] FVC, "Fingerprint Verification Competition," 2006, (http://bias.csr.unibo.it/fvc2006).

[7] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength," *Third International Conference on Audio- and Video-Based Biometric Person Authentication, Proc. AVBPA 2001*, pp. 223–228, 2001.

[8] U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, San Jose, CA*, pp. 622–633, 2004.

[9] G.I. Watson, M.D. Garris, E. Tabassi, C.L. Wilson, R.M. McCabe, and S. Janet, *User's Guide to NIST Fingerprint Image Software 2 (NFIS2)*, National Institute of Standards and Technology (http://fingerprint.nist.gov/NFIS), 2004.

[10] M. Mimura, S. Ishida, and Y. Y. Seto, "Fingerprint verification system on smart card," *ICCE Digest of Technical Papers*, pp. 182–183, June 2002.

[11] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, C. Escudero, and Q.-I. Moro, "MCYT baseline corpus: a bimodal biometric database," *IEE Proc. Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 391–401, December 2003.

[12] Colin Soutar, "Biometric system security. http://www.bioscrypt.com/assets/security_soutar.pdf," 2002.

[13] FVC, "Fingerprint Verification Competition," 2004, (http://bias.csr.unibo.it/fvc2004).