Seguretat en sistemes biomètrics

Albert Solé Ribalta

PID_00200894

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Tal com s'ha anat comentant al llarg dels mòduls anteriors, l'objectiu dels sistemes biomètrics és proporcionar un mecanisme d'identificació. Aquest mecanisme d'identificació pot estar adreçat a diversos objectius. Els més comuns, relacionats perquè proporcionen seguretat a un recurs, solen ser l'autenticació o la detecció de personal autoritzat i la detecció de personal no autoritzat. Des del punt de vista tècnic, aquests dos objectius es poden englobar en un sol punt, ja que la majoria de funcionalitats s'assoleixen fent cerques de persones identificades prèviament a la base de dades del sistema en qüestió. En el primer cas, es dóna accés a les persones introduïdes a la base de dades i, en el segon, a les persones que no estan introduïdes a la base de dades. Tot i que aquests són els dos atacs més comuns, també n'existeixen d'altres que seran comentats al llarg del mòdul.

L'estructura del mòdul és la següent:

- La primera part pretén fer una descripció general dels tipus bàsics d'atacs i també descriure les mesures habituals de protecció (apartats "Objectius de l'atac a un sistema biomètric", "Punts febles dels sistemes biomètrics" i "Defenses específiques per a millorar la seguretat en sistemes biomètrics").

- La segona part descriu diversos atacs aplicables a sistemes basats en empremta dactilar, reconeixement de cares i reconeixement d'iris.

- Una vegada descrites cadascuna de les metodologies d'atac es comenten també algunes mesures específiques de protecció (apartats "Atacs directes" i "Atacs indirectes (generació sintètica de dades biomètriques)").

- Finalment, es descriuen els atacs *side channel* i les seves utilitats en combinació amb els altres possibles atacs (apartat "Atacs *side channel*").

Objectius

Els objectius bàsics d'aquest mòdul són els següents:

1. Conèixer els tipus bàsics d'atacs que es poden produir en un sistema biomètric.

2. Conèixer les mesures bàsiques de protecció contra atacs en sistemes de seguretat basats en biometria.

3. Conèixer una sèrie de casos pràctics d'atacs (atacs directes i atacs indirectes), juntament amb els seves mesures de protecció.

1. Objectius de l'atac a un sistema biomètric

Un sistema de seguretat, utilitzi o no informació biomètrica, pot ser objecte d'una sèrie d'atacs. En aquest apartat en descriurem els principals tipus sense tenir en compte ni l'arquitectura del sistema ni els seus detalls tècnics. S'intentarà centrar els tipus d'atac en els sistemes biomètrics tot i que, a causa de la seva generalitat, molts tenen molts punts en comú amb els atacs típics a sistemes de seguretat. Per a cada atac es descriuran els principals objectius i exemples reals documentats.

1.1. Atacs de suplantació de la persona

El tipus d'atacs de **suplantació de la persona** (***spoofing***) van dirigits a obtenir accés il·lícit a un recurs. El tipus d'atac consisteix a suplantar la identitat d'un usuari amb accés al recurs desitjat.

Hi ha diverses variants de l'atac segons el punt de l'arquitectura al qual vagin dirigits. Deixant de banda els atacs tradicionals a sistemes informàtics i centrant-nos específicament en sistemes biomètrics, cal dir que la manera més habitual de dur a terme aquest atac és mitjançant còpies sintètiques de dades biomètriques de l'usuari objectiu. Per tal d'obtenir les còpies sintètiques de les dades hi ha diversos mecanismes que seran comentats específicament al llarg del mòdul. A grans trets, el principal objectiu de l'atacant es dirigeix a dos punts principals:

Vegeu també

Les variants de l'atac segons el punt de l'arquitectura al qual vagi dirigit s'estudien en els apartats 2, 4 i 5 d'aquest mòdul.

1) Obtenir accés a les dades biomètriques de l'usuari.

2) Fer una còpia sintètica de les dades obtingudes.

A causa de la gran difusió dels sistemes d'autenticació biomètrica, no és difícil trobar-hi notícies relacionades.

Empremta dactilar

Un primer exemple el podem trobar en un lladre de cotxes que li va tallar el dit al propietari per tal d'arrencar el seu cotxe, protegit amb un sistema de seguretat basat en empremta dactilar. En aquest cas, l'atacant va ser capaç d'arrencar el cotxe la primera vegada, amb l'empremta sense vida del propietari. Tot i que posteriorment la mateixa empremta ja no permetia engegar el cotxe a causa dels sistemes de protecció contra mostres mortes de què disposava el cotxe.

Font: extret de "Malaysia car thieves steal finger". *BBC News*.

Còpies sintètiques

Un segon exemple el podem trobar en un usuari de la Seguretat Social mexicana, que mitjançant còpies sintètiques d'empremtes falsificava la presència d'altres usuaris al lloc de treball. En aquest cas, el falsejament es feia mitjançant còpies sintètiques fetes amb làtex (similars a un segell) impreses en una impremta.

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

1.2. Ofuscació biomètrica

La majoria d'atacs a sistemes biomètrics estan dirigits a la suplantació d'un individu per tal d'obtenir accés a un recurs protegit. Tot i així, hi ha altres tipus d'atac que cal tenir en compte.

L'**ofuscació biomètrica (*obfuscation*)** està adreçada a falsejar o emmascarar les dades biomètriques, abans o després que el sistema les adquireixi, per tal d'evitar que el sistema reconegui un individu.

Les conseqüències d'un atac d'ofuscació poden ser tan o més greus que les d'un atac de suplantació, per tant aquest tipus d'atacs tampoc no s'ha de desestimar en la protecció dels sistemes. S'ha de tenir en compte que la majoria de les persones que duen a terme aquest tipus d'atac acostumen a ser presents en llistes de control i la majoria, buscades per les forces de l'ordre. Per tant, aquestes persones acostumen a tenir fortes raons per tal de modificar les seves dades biomètriques. Per fer-nos una idea de la gravetat de l'atac podem considerar els sistemes biomètric situats a les fronteres entre països. En aquest cas, a un individu que vol entrar al país se li requereix que introdueixi dades biomètriques (habitualment empremtes dactilars o dades facials) per tal de garantir que no ha comès delictes dins del país o que no està sent buscat per la policia.

Hi ha diverses maneres de dur a terme aquest atac segons la metodologia aplicada; les dues principals són les següents:

1) L'alteració física de les dades biomètriques pròpies ja sigui per deterioració o mitjançant cirurgia.

2) L'ús de tècniques de suplantació per a suplantar un individu i ofuscar la identitat pròpia. Aquesta segona metodologia també inclou l'ús de dades sintètiques per tal d'ofuscar la identitat.

Tot i que no hi ha gaires casos reals publicats d'aquests tipus d'atacs, segurament per tal d'evitar proves de debilitat en els sistemes de seguretat, és possible trobar-hi algunes notícies relacionades.

Exemples d'ofuscació biomètrica

El primer exemple d'ofuscació biomètrica que es coneix data del 1933, en què un assassí i lladre de bancs va ser trobat amb les empremtes de la mà esquerra mutilades. Hi ha casos similars amb alguns famosos delinqüents com John Dillinger. Un altre cas el podem trobar el juny del 2009, en què quatre persones van ser detingudes en intentar entrar al Japó amb les empremtes alterades quirúrgicament.

Un dels casos més actuals fa referència a la violació de les mesures de seguretat de l'aeroport principal de Londres. Aquest aeroport aplica diversos sistemes de protecció biomètrica per tal de garantir, d'una banda, que el passatger i el passaport corresponen a la mateixa persona i, de l'altra, que la persona no representa cap perill per al país. Aquestes mesures es basen en reconeixement per empremta dactilar i reconeixement facial. La notícia, destacada per la FOX, fa referència a un grup de persones que va evadir els mecanismes de seguretat tot i estar incloses en una llista de seguiment. El document no deixa clares les tècniques usades per a violar el sistema de seguretat, tot i que és un exemple clar del que es pot aconseguir mitjançant tècniques d'ofuscació. Clarament, els atacants van usar l'esdeveniment dels Jocs Olímpics del 2012 amb força habilitat, ja que segurament els llindars d'acceptació van ser reduïts per tal de permetre una fluïdesa més gran dels punts de control.

Referència web

Trobareu la notícia de la violació de les mesures de seguretat a l'aeroport principal de Londres a "Members of terror watch list reportedly pass through London airport security ahead of Olympics". *Fox*.

1.3. Atacs de denegació de servei

L'objectiu de l'**atac de denegació de servei** (***denial of service***) està dirigit a alentir, parar o degradar la qualitat del sistema.

Un sistema afectat per aquest tipus d'atac impedeix que els usuaris legítims el puguin usar amb normalitat. Aquest mal funcionament del sistema pot ser usat per l'atacant amb dos fins clarament diferenciats:

1) Fer un atac secundari de suplantació o ofuscació.

2) Dur a terme un atac secundari d'extorsió.

Reflexió

Pel context de l'assignatura, aquest segon tipus d'atac secundari no serà comentat al llarg del mòdul.

Una metodologia senzilla per a dur a terme aquest tipus d'atac és la inserció de gran quantitat de dades amb molt de soroll que segurament baixarà el llindar d'acceptació i, conseqüentment, augmentarà la taxa de falsos acceptats. En aquest cas, l'atac secundari podria correspondre a un atac de suplantació, ja que el sistema podria acceptar mostres biomètriques no lícites com a lícites. En cas que l'atac de denegació de servei anés més enllà d'una degradació lleu del sistema i n'aturés el funcionament, el personal administrador es podria veure obligat a reemplaçar els sistemes biomètrics amb mesures més tradicionals com un guarda de seguretat. S'ha de considerar que, en alguns aspectes, aquests sistemes tradicionals són burlats més fàcilment que un sistema biomètric.

Atac secundari d'ofuscació

Un clar exemple el podríem trobar en un escenari en què es vol fer un atac secundari d'ofuscació. Suposem que l'atacant vol accedir a un recurs protegit per un sistema de reconeixement dactilar i refermat per un reconeixement facial. En aquest escenari podria ser difícil enganyar un sistema automàtic ben calibrat, però no tan difícil enganyar un guarda de seguretat.

1.4. Conspiració i coacció

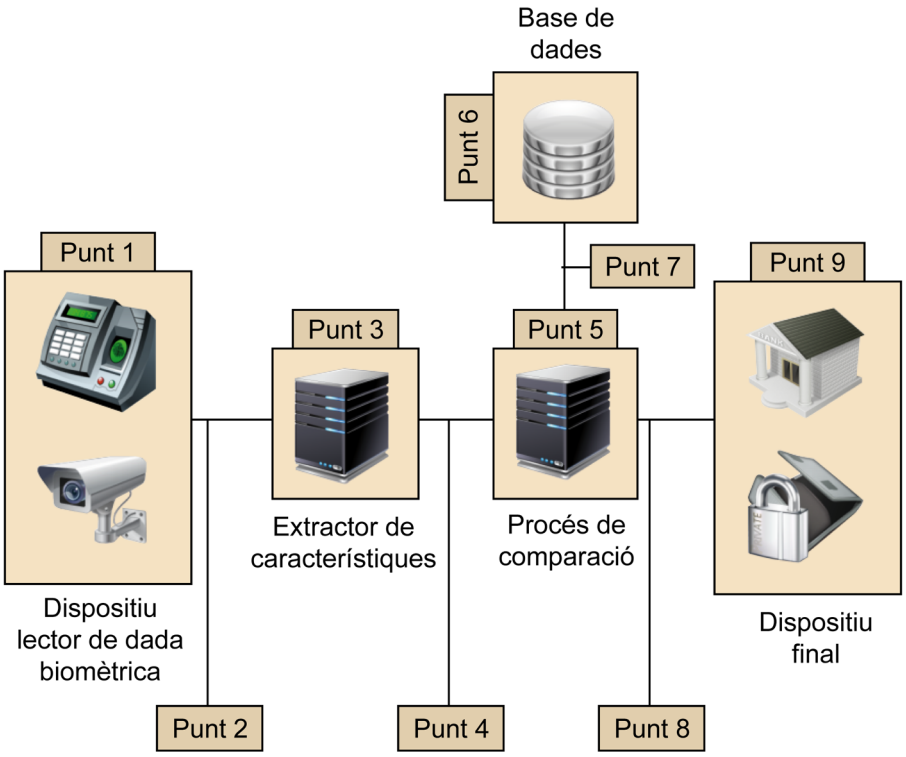
La principal diferència entre la **conspiració** i la **coacció** i els anteriors és que aquests tipus d'atacs els duen a terme usuaris legítims del sistema.

En els atacs de conspiració, l'usuari, possiblement per suborn, facilita l'accés al sistema. En els atacs de coacció, la víctima, possiblement sota amenaça o xantatge, facilita l'accés al sistema. Aquestes vulnerabilitats evadeixen el sistema de seguretat, ja que les dades són vertaderes. El tipus d'atac pot variar en severitat depenent de l'usuari atacat. Cal considerar que no té la mateixa importància atacar un administrador que un usuari sense privilegis.

2. Punts febles dels sistemes biomètrics

En aquest apartat, analitzarem l'arquitectura d'un sistema de seguretat basat en biometria per tal de detectar-ne els punts més febles i poder presentar una sèrie de mecanismes per mitigar-ne les possibles deficiències. La figura 1 presenta l'esquema habitual d'un sistema de seguretat basat en biometria.

Figura 1. Esquema i punts d'atac en un sistema biomètric



El sistema de la figura es basa en cinc equips físics i diversos sistemes de comunicació entre ells. Els cinc equips són els següents: el sensor, dedicat a capturar les dades biomètriques; dues màquines dedicades a extraure les característiques biomètriques de les dades capturades pel sensor i a comparar les dades biomètriques amb les dades del possible usuari; una base de dades que conté les dades dels usuaris registrats en el sistema, i finalment un dispositiu que interpreta la sortida del sistema i dóna accés al recurs o el denega. Hi ha tant extensions com simplificacions del sistema mostrat. Les simplificacions poden ser determinades per la fusió dels diversos mòduls del sistema, i per tant també per l'eliminació dels canals de comunicació relacionats. Possibles extensions poden ser determinades per la combinació de diversos dispositius de captura de dades (per exemple, cara, empremta i veu), distribució de la base de dades en un clúster de màquines, execució dels processos de comparació en màquines paral·leles, etc.

Analitzant la figura 1 no és complicat detectar els punts d'atac més evidents. Aquests punts es poden classificar en dos grans grups: les **màquines físiques** i els **canals de comunicació**.

En els subapartats següents es descriuran els atacs que es poden produir en cadascun dels punts destacats de la figura 1. Per a cada punt es descriuran els atacs més habituals i també s'introduiran alguns dels mecanismes més habituals per a evitar els tipus d'atac.

2.1. Biometria falsa

L'atac de **biometria falsa** (punt 1 de la figura 1), dirigit al procés d'extracció de les dades biomètriques, es basa a introduir dades falses al sensor.

Segons el tipus de sistema biomètric, els atacs poden presentar diverses formes. Un dels més habituals, atesa la gran popularitat del seu ús, és la presentació d'una empremta dactilar falsa al sistema. Aquestes empremtes poden provenir de gran varietat de llocs: empremtes de cadàvers, empremtes de silicona, gelatina, plàstic o, simplement, fotocòpies d'empremtes dactilars. També és habitual l'activació del sensor mitjançat la respiració sobre els residus acumulats sobre el sensor, tot i que cada cop més sensors són robustos a aquest tipus d'atacs. En els sistemes basats en la detecció del rostre, els atacs més habituals solen ser la presentació de fotografies, originals o amb petites modificacions, de persones autoritzades. Altres exemples de presentació de biometria falsa poden ser: presentació de gravacions d'alta qualitat en sistemes de detecció de veu o la presentació de fotografies sobre suports bidimensionals o impreses sobre lents de contacte en sistemes basats en l'iris.

Vegeu també

En l'apartat 4 d'aquest mòdul es descriuran alguns del mecanismes més usats per a dur a terme aquests atacs.

Una solució bastant genèrica per a protegir el sistema davant la presentació de biometria falsa és la detecció de si la mostra adquirida i comparada prové d'un teixit viu o no. Aquest mecanisme s'anomena **detecció de vida**. Tot i així, s'ha de tenir en compte que en cada tipus de sistema les seves característiques implícites fan que els tipus de problemes, i per tant les solucions que cal aplicar, siguin diverses.

La vida de la mostra

Dos exemples oposats relacionats amb el tema de la vida de la mostra podrien ser un sistema d'autenticació basat en empremta instal·lat en un dispositiu portàtil i el control d'immigració d'un aeroport. En el dispositiu portàtil és molt difícil detectar la presentació d'una empremta falsa en comparació d'un control d'immigració en un aeroport, on un operari pot analitzar els dits de les persones per tal de detectar-hi qualsevol anomalia.

2.2. Injecció de paquets falsos i atacs de reenviament

La **injecció de paquets falsos i els atacs de reenviament** (punts 2, 4, 7 i 8 de la figura 1) consisteixen en la captura de paquets de dades procedents de diversos mòduls del sistema i que viatgen per algun canal de comunicació.

Els paquets capturats poden ser utilitzats amb posterioritat per tal d'autentificar-se en un sistema biomètric. Els paquets capturats poden ser enviats sense modificació, utilitzats per tal de crear dades noves o prototips de dades biomètriques i també per a extraure les dades biomètriques adreçades a la creació de biometria falsa i fer atacs de biometria falsa sobre els punts 1, 3, 5 o 6 de la figura 1.

En els atacs en el punt 2, les dades biomètriques prèviament enregistrades són repetides sobre el canal i eviten el sensor. Alguns exemples clars en serien la intrusió de dades corresponents a empremtes dactilars o senyals d'àudio. Aquest tipus d'atac s'anomena ***atac per repetició***. S'ha de comentar que en sistemes en què el sensor i l'extractor de característiques formen part d'un mateix dispositiu físic aquest atac resulta bastant complicat.

En els atacs en el punt 4, posteriorment a l'extracció de característiques biomètriques, les dades provinents de l'extractor de característiques amb destinació al mòdul de comparació són alterades o substituïdes per un conjunt nou de característiques. Igual que en el cas anterior, si l'extractor de característiques i el mòdul de comparació formen part del mateix bloc físic, aquest atac és extremament difícil. En canvi, si el procés de comparació es fa en una altra màquina i les dades s'han de transmetre per canals no segurs (per exemple, via HTTP) aquest atac és molt factible i perillós.

Igual que en els atacs en el punt 4, en els atacs en el punt 7 les dades corresponents a les plantilles dels usuaris registrats poden ser modificades mitjançant el canal de comunicació.

Finalment, els atacs en el punt 8 estan adreçats a modificar el resultat final del sistema. S'ha de tenir en compte que aquest tipus d'atac és molt perillós, ja que independentment de l'eficiència de tot el sistema, si un atacant pot modificar la sortida final, totes les mesures aplicades prèviament no tenen cap tipus d'utilitat.

Sense tenir en compte les tècniques de generació de dades biomètriques falses, les tècniques aplicades en aquests tipus d'atacs són més aviat tècniques clàssiques de captura i injecció de paquets en un mitjà de transmissió, que no pas tècniques específiques per a sistemes biomètrics. Per tant, els sistemes de

protecció sobre aquests atacs són anàlegs als sistemes de protecció del mitjà de transmissió com poden ser detectors de *sniffers*, encriptació, signatura dels paquets, etc.

2.3. Reutilització de residus

La realització d'aquest tipus d'atac necessita accés físic al maquinari involucrat en el sistema de seguretat.

La **reutilització de residus** es basa en la captura de dades temporals del maquinari tant siguin residents a memòria principal, fitxers temporals emmagatzemats a un disc com fitxers no esborrats a baix nivell.

Aquest tipus d'atac es pot dur a terme a qualsevol dels punts que formen part del maquinari usat: sensor, extractor de característiques, bloc de comparació o base de dades. La captura d'aquestes dades podria permetre a un possible atacant fer atacs de biometria falsa, injecció de paquets sobre el mitjà, atacs de reenviament, atacs sobre el sensor o també al mòdul de comparació.

Les mesures específiques de protecció sobre aquest tipus d'atacs acostumen a ser força similars a les tècniques bàsiques per a evitar intrusions i modificacions a una màquina sensible. La principal consisteix en la protecció de la màquina en si, cosa que inclou les mesures bàsiques de protecció d'un sistema informàtic, com poden ser tenir el programari actualitzat per a evitar intrusió a partir d'errors en el programari. Antivirus en cas que sigui necessari, cerques periòdiques contra eines d'intrusió (*rootkits*), instal·lació de sistemes de detecció d'intrusos (IDS[1]), instal·lació de la màquina en DMZ (zona desmilitaritzada). Un altre mètode senzill i complementari de protecció sobre aquests tipus d'atacs consisteix a assegurar que s'esborren a baix nivell totes les dades sensibles utilitzades.

(1)Sigla de l'anglès *intrusion detection system*.

2.4. Interferència en el procés d'extracció

Els **atacs en el procés d'extracció** (punt 3 de la figura 1) estan adreçats a la sobreescriptura de les dades extretes per l'extractor de característiques.

L'atac és equivalent a l'atac en el punt 4 explicat anteriorment, però usant mecanismes diferents. En aquest cas, un troià podria ser el responsable de mantenir una porta oberta entre l'atacant i l'extractor de característiques perquè l'extractor generi les dades que es volen.

Una altra tipologia d'atac que pot rebre aquest punt està dirigida a evitar que el procés d'extracció pugui detectar característiques vitals o de referència de la dada biomètrica, cosa que impediria la validació correcta de la identitat. En aquest cas, l'atac correspon a un atac d'ofuscació.

De la mateixa manera que en la reutilització de residus, és molt important mantenir un control dels usuaris i del programari instal·lat a la màquina i també l'ús d'IDS per tal de garantir la protecció de la màquina.

2.5. Atacs al mòdul de comparació

Els atacs dirigits al mòdul de comparació (punt 5 de la figura 1) poden tenir diverses formes. La primera i més senzilla correspon a un atac similar al d'interferència en el procés d'extracció, en la qual l'atacant modifica les dades generades pel mòdul de comparació. Un altre tipus d'atac més complicat correspon a un atac a l'algorisme de comparació. En aquest cas, l'algorisme de comparació és enganyat per un conjunt de característiques generades sintèticament (possiblement basant-se en característiques reals). Aquest conjunt de característiques presentades a l'algorisme de comparació poden anar adreçades o bé a substituir un usuari concret o bé adreçades a substituir algun usuari desconegut buscant el límit de falsos positius del sistema.

Vegeu també

En l'apartat 5 es descriuran una sèrie de mecanismes usats per a dur a terme aquest tipus d'atacs.

2.6. Atacs a la base de dades de plantilles

Els **atacs a la base de dades de plantilles** (punt 6 de la figura 1) estan adreçats a modificar les dades biomètriques dels usuaris registrats en el sistema.

S'ha de tenir en compte que la base de dades pot ser accessible localment o remotament, i també pot estar distribuïda en diversos servidors. Depenent del tipus d'arquitectura es poden aplicar diversos tipus d'atac. L'objectiu dels atacs pot ser molt divers. En els atacs de suplantació, un atacant modifica les dades de les plantilles enregistrades per tal que es corresponguin amb les seves. Un altre possible atac destinat a la base de dades està dirigit a registrar un usuari no autoritzat, cosa que permetria un accés futur al recurs protegit. Un tercer possible atac està dirigit a denegar-los el servei a un o diversos usuaris concrets.

3. Defenses específiques per a millorar la seguretat en sistemes biomètrics

Hi ha una sèrie de mesures per a impedir/dificultar els atacs comentats anteriorment. Les metodologies descrites a continuació no van totes dirigides a un punt concret del sistema, sinó que formen part d'un conjunt de sistemes de protecció/recomanacions i bones pràctiques que cal seguir perquè el sistema de seguretat funcioni de manera correcta i eficient.

Com a metodologia general, s'ha de considerar que un **sistema de seguretat** no s'ha de centrar mai en un únic mètode de seguretat, sinó que s'ha d'aplicar amb combinació d'altres de secundaris o de complementaris.

3.1. Autenticació per combinació de dades aleatòries i biometria múltiple

La idea principal del mecanisme està basada en el fet que l'usuari disposa de diferents característiques biomètriques que poden ser sol·licitades, segons la implementació del sistema, aleatòriament o de manera seqüencial. L'augment de seguretat és determinat pel fet que el possible atacant ha de poder reproduir de manera correcta totes les possibles dades que es poden demanar a l'usuari. En el cas d'introduir aleatorietat al procés, l'atac es complica encara més, ja que no és possible conèixer ni la seqüència ni la quantitat de dades que seran sol·licitades.

Empremta dactilar

Un exemple senzill d'implementació sobre un sistema d'empremta dactilar seria la verificació de l'empremta de diversos dits de manera aleatòria. El possible atacant ha de tenir en possessió una còpia de totes les empremtes dactilars. En aquest cas, a més, es fa impossible l'atac mitjançant els residus al dispositiu de captura de dades, ja que les empremtes dels diversos dits se solaparan.

Reconeixement de veu

Un altre possible exemple d'implementació més elaborada podria ser un sistema de reconeixement de veu en què se sol·licita a l'usuari que repeteixi una seqüència aleatòria de paraules. En aquest cas, l'atacant hauria de disposar d'una gran quantitat de paraules enregistrades per tal de poder reproduir qualsevol combinació sol·licitada.

Sistema de seguretat de l'aeroport de Londres

Un últim exemple basat en un exemple de sistema de seguretat real en què s'aplica biometria múltiple sense aleatorització en la demanda de dades es podria veure en el sistema de seguretat de l'aeroport de Londres, on els usuaris han de presentar de manera seqüencial les empremtes dactilars i una imatge de la cara.

Vegeu també

Aquest exemple s'ha explicat en el subapartat 1.2 d'aquest mòdul.

3.2. Retenció de dades

Una gran font d'informació susceptible de ser usada per a un presumpte atac és la informació temporal que usen els sistemes biomètrics. Considerant el sistema tècnicament, s'ha de tenir en compte que tant en l'extracció de les característiques com en el sistema d'identificació és necessari desar certa informació temporal per fer les operacions pròpies del sistema. Aquesta informació temporal, en cas de ser capturada, pot donar molta informació a un possible atacant, perquè dugui a terme una gran diversitat d'atacs. Per tant, per protegir l'accés a aquesta informació s'han de garantir, amb mesures severes, l'accés il·lícit al maquinari del sistema. D'altra banda, el sistema en si també ha de considerar la necessitat de no mantenir la informació temporal més temps del necessari. Aquests mecanismes poden ser utilitzats amb combinació d'esborraments de la memòria a baix nivell de manera periòdica.

Cal destacar que per a poder desar històrics dels accessos autoritzats i no autoritzats pel sistema biomètric és necessari emmagatzemar dades històriques de manera temporal. Sense considerar que aquestes dades s'haurien de desar de manera codificada al sistema, l'administrador ha de considerar, mitjançant una anàlisi de cada cas en particular, un bon equilibri entre seguretat i utilitat de la informació emmagatzemada.

3.3. Detecció de la vida de la mostra

Com s'ha anat veient al llarg de tot el mòdul, l'atac de suplantació de la persona és un dels atacs més típics sobre un sistema biomètric. Considerant que la metodologia més habitual és la còpia sintètica de dades biomètriques de la persona que es vol suplantar, una de les defenses més utilitzades per tal d'evitar aquests tipus d'atacs és la **detecció de vida de la mostra**. És habitual incorporar aquests mecanismes al dispositiu de captació de dades. També és important detectar la vida de la mostra en atacs d'ofuscació, ja que l'atacant pot intentar no ser detectat pel sistema usant mostres sintètiques que pertanyen a altres usuaris.

Hi ha moltes maneres de detectar la vida de la mostra. Aquestes depenen en gran manera de la dada biomètrica usada pel sistema. A continuació, es descriuen algunes mesures concretes per tal de detectar la vida de diversos tipus de mostres biomètriques.

1) Per a **sistemes basats en detecció de veu** una mesura per a la detecció de la vida de la mostra pot ser mesurar l'aire expulsat en la parla. Aquest patró facilita molta informació de la persona i també fa més difícil violar el sistema mitjançant còpies gravades de la veu original.

2) En **sistemes basats en empremtes dactilars**, mesures de fàcil detecció com poden ser la temperatura, oximetria, conductivitat de la pell, detecció de capil·lars sota l'epidermis o el pols, poden donar molta informació sobre la vida de la mostra.

3) En **sistemes basats en reconeixement facial** es podria combinar el reconeixement de la cara amb imatges espectroscòpiques o tèrmiques.

4) Finalment, val la pena comentar el cas de **sistemes biomètrics basats en reconeixement de l'iris**. Fer una còpia sintètica d'un iris sobre una lent de contacte comporta grans dificultats tècniques, tant sigui una còpia obtinguda d'un original com simplement una de generada aleatòriament. Tot i així, hi ha alguns mètodes per a detectar la vida d'un iris. La majoria estan basats en l'anàlisi estadística de simetries en el patró de l'iris llegit.

Vegeu també

Trobareu més informació referent als sistemes biomètrics basats en reconeixement de l'iris en el subapartat 4.3 d'aquest mòdul.

3.4. Autenticació multifactor

L'**autentificació multifactor** podria ser considerada una generalització de la biometria múltiple, en què diversos mecanismes, no necessàriament biomètrics, són sol·licitats pel sistema en la validació d'un individu.

Aquests mecanismes podrien ser mecanismes físics com targetes intel·ligents (*smart cards*), *DONGLE*[2] o qualsevol altre tipus de *token*, o mecanismes com **claus d'accés**. L'augment de la seguretat d'aquest tipus de mecanismes, igual que en el cas de la biometria múltiple, és determinat per la combinació dels diversos elements que cal poder plagiar per fer un atac de suplantació.

(2)En trobareu la definició en el glossari de l'assignatura.

Els possibles inconvenients d'utilitzar autenticacions multifactor serien determinats per un augment del temps de validació, cosa que forçaria el personal responsable del disseny del sistema a buscar un equilibri entre la seguretat i la usabilitat del sistema.

3.5. Criptografia i signatura digital

Tant els criptosistemes com les signatures digitals poden ser utilitzats a molts nivells en un sistema complex com pot ser un sistema biomètric. En aquest cas, atesa la generalitat del mecanisme, ens centrem només en la protecció de les dades que circulen pels mecanismes de comunicació entre les diverses màquines que formen el sistema. L'encriptació i el xifratge de les dades que circulen per la xarxa permet al sistema protegir-se d'atacs produïts per la lectura/escriptura dels paquets de dades que circulen per la xarxa de comunicació del sistema. L'objectiu principal del xifratge és evitar que cap possible atacant

(3)En trobareu la definició en el glossari de l'assignatura.

pugui analitzar la informació que circula pel canal de comunicació. D'altra banda, la signatura digital està adreçada a verificar l'emissor de la informació, i evitar en aquest cas atacs d'intercepció (*man-in-the-middle*)[3].

3.6. Estàndards

Com en la majoria de sistemes o organitzacions de treball, hi ha una sèrie d'estàndards que proporcionen seguretat i eficiència al sistema. En aquest cas, deixant de banda altres estàndards aplicables en organitzacions, com poden ser la ISO 9001, hi ha una sèrie d'estàndards relacionats amb el bon funcionament i la seguretat dels sistemes informàtics. Alguns de relacionats amb la seguretat de sistemes en general poden ser: ITIL capítol 4 o ISO/IEC 17799. D'altres de relacionats específicament amb sistemes biomètrics poden ser: ANSI X.9.84 o PIV-071006. L'estàndard **ANSI X.9.84**, dissenyat específicament per a sistemes financers, engloba conceptes de seguretat en la transmissió d'informació biomètrica i també sobre el seu emmagatzematge i els requisits de seguretat que ha de complir el maquinari utilitzat en el sistema biomètric. A causa de la gran utilització de sistemes basts en empremta dactilar, un estàndard bastant important és PIV-071006. Aquest estàndard especifica els requeriments dels sensors de captura de dades utilitzats en els sistemes governamentals dels Estats Units.

Altres estàndards relacionats amb sistemes biomètrics poden ser els següents:

- **ANSI/INCITS 358**, que motiva l'estandarditzación de la interoperabilitat dels sistemes biomètrics.

- **NISTIR 6529**, el qual especifica el format de les dades en les interfícies de sortida dels sistemes biomètrics.

- **ISO/IEC 19794-2:2005**, que especifica el format de les dades en sistemes basats en empremta dactilar.

- **INCITS 378-2009** també adreçat a estandarditzar l'intercanvi de dades en sistemes basats en empremta dactilar.

Amb relació als estàndards d'interoperabilitat, s'han de tenir en compte les dues cares de la moneda. D'una banda, els estàndards milloren la seguretat del sistema ja que han estat dissenyats per un equip d'especialistes i, per tant, molts dels punts febles relacionats amb la seguretat han estat eliminats. De l'altra, un sistema que compleixi un estàndard d'interoperabilitat facilita l'accés a les dades ja que tant el seu format com els mitjans de transmissió es coneixen.

3.7. Agents de seguretat i personal de control

Els sistemes tecnològics actuals encara no tenen certes qualitats o funcionalitats que una persona pot fer amb extrema facilitat. En aquest cas, molts dels mecanismes de protecció comentats al llarg d'aquest mòdul poden ser efectuats per un agent de seguretat d'una manera més eficient i econòmica que un sistema automàtic. La principal mesura de seguretat, i que ajuda a prevenir en gran manera la violació del sistema, és la **detecció de la vida de les dades biomètriques**. Per tant, en un sistema de seguretat basat en biometria, és molt important la combinació de mètodes automàtics per a la identificació de les dades biomètriques amb personal de seguretat per tal de verificar les mostres. Per il·lustrar aquest fet només cal considerar que per a qualsevol persona és molt fàcil identificar si una mostra és una simple fotocòpia o la cara d'una persona humana. Un altre mecanisme de seguretat que un agent pot proporcionar per augmentar la seguretat del sistema és la identificació d'atacs coercitius, en què un usuari lícit del sistema és obligat a introduir les seves dades biomètriques al sistema per tal de donar accés a un usuari no autoritzat.

3.8. Seguretat per desconeixement

La **seguretat per desconeixement**[4] és un mecanisme per a proporcionar seguretat en un sistema i està basat a no revelar-ne detalls de disseny i implementació.

[(4)]En anglès, *security through obscurity*.

S'ha de tenir en compte que habitualment un sistema basat en aquest tipus de seguretat acostuma a tenir vulnerabilitats conegudes, però que per desconeixement de la seva arquitectura i implementació no es poden explotar. Aquest sistema de protecció acostuma a ser una bona mesura complementària de protecció.

4. Atacs directes

Els **atacs directes** són atacs dirigits al mecanisme d'adquisició de dades biomètriques (punt 1 de la figura 1). Aquests tipus d'atacs es basen a introduir dades biomètriques generades sintèticament al mecanisme d'adquisició.

Hi ha una gran quantitat de variants de l'atac segons l'objectiu de l'atacant, el tipus de dada biomètrica usada pel sistema de seguretat, i també els mecanismes de seguretat que el sistema apliqui. Per a dur a terme un atac satisfactori sobre el sensor un atacant necessita en un primer pas obtenir dades biomètriques, tant sigui per còpia de dades reals d'un usuari registrat al sistema, com per creació de dades aleatòries. En un segon pas fer una còpia sintètica de les dades obtingudes i, finalment, presentar les dades noves al sistema pel sensor.

Aquests tipus d'atacs han demostrat ser força reeixits si la còpia de dades biomètriques és de prou qualitat. Part de la gran popularitat d'aquest tipus d'atacs rau en el fet que no és necessari conèixer ni l'arquitectura del sistema, ni detalls del maquinari, ni detalls dels algoritmes utilitzats, ni tampoc accés físic al maquinari del sistema de seguretat.

Com a punt general, s'ha de tenir en compte que en molts dels casos que es presentaran no és possible protegir l'usuari perquè un possible atacant no pugui obtenir/robar certes dades biomètriques. Com es veurà, en aquests casos la seguretat es mou cap a evitar que l'atacant pugui introduir una còpia de les dades al sistema.

En aquest apartat, comentarem diverses maneres utilitzades per a aconseguir informació biomètrica i utilitzar-la per a fer un atac directe. Per a cadascuna de les tècniques explicades també es comentaran la validesa de les mostres i les proteccions més utilitzades.

4.1. Empremta dactilar

En aquest apartat es presentaran dues maneres de generar empremtes dactilars sintètiques, la primera considerant que l'usuari objectiu col·labora en la lectura de les seves empremtes dactilars i la segona considerant que l'usuari no hi col·labora. A continuació, es comentaran com de perilloses poden ser les còpies generades en un atac real, juntament amb els mecanismes de protecció més habituals. Finalment, es comentaran breument els mecanismes usats per a fer atacs d'ofuscació en el punt 1 de la figura 1.

4.1.1. Duplicats amb cooperació

Els duplicats d'empremtes dactilars amb cooperació del propietari són, sens dubte, els més fàcils i reeixits, ja que a causa de l'accés físic a la dada biomètrica és possible comparar la còpia amb la dada real per a una rectificació posterior o una còpia nova en cas que no sigui de prou qualitat.

Per tal de fer-ne una còpia els passos més habituals són els següents: el primer pas, molt important, consisteix a netejar bé l'empremta dactilar tant del greix propi de la pell com de petits residus que hi pugui haver. Aquesta neteja s'acostuma a fer usant simplement sabó. Aquest pas és bàsic, ja que el material de suport de la còpia ha de ser capaç de penetrar a les valls de l'empremta dactilar amb facilitat. Els motlles de les còpies de qualitat s'acostumen a fer en petits recipients usant, habitualment, guix odontològic. Un cop sec el motlle, s'unta la part de l'empremta amb silicona impermeable o làtex i es col·loca el dit destinació de l'empremta damunt del material de suport. Un cop seca, l'empremta ja es pot retirar amb compte i ser col·locada sobre el dit del portador.

Tal com es pot veure, la còpia d'una empremta dactilar amb cooperació és relativament simple de fer i és d'alta qualitat segons els materials utilitzats. Per tant, a causa de la simplicitat en la realització de còpies, és molt comú que els sistemes de seguretat utilitzin contramesures per a evitar aquest tipus d'intrusions.

4.1.2. Duplicats sense cooperació

Per tal de duplicar una empremta dactilar sense cooperació del propietari, és necessari obtenir-ne una còpia mitjançant alguna superfície de contacte. Una de les millors maneres d'obtenir la còpia acostuma a ser mitjançant el mateix sensor o una superfície llisa i rígida. S'ha de tenir en compte que en cas que l'escàner hagi estat netejat abans del seu ús i només hi hagi una sola empremta a la superfície, aquesta empremta acostuma a ser de molt bona qualitat i a més correspon al dit usat per a la verificació. Tot i així, crear còpies en relleu d'aquestes empremtes no és tan fàcil com en el cas amb cooperació, però tampoc no requereix grans mitjans tècnics.

Un dels possibles procediments és el següent: primer de tot s'ha de fer una còpia de l'empremta dactilar. Per a fer aquesta còpia habitualment s'usa algun tipus de tint, com pot ser pols de grafit. Aquest tint és dipositat sobre la superfície que conté l'empremta i aquesta és retirada utilitzant algun tipus de superfície adherent transparent. Tradicionalment, es feia una còpia en negatiu de l'empremta amb cel·luloide (usant una càmera de fotografia amb rodet); actualment, el negatiu es pot generar amb una impressora convencional (després d'haver escanejat la mostra). Una vegada obtingut el negatiu de l'empremta se'n fa una còpia en relleu mitjançant un procediment semblant a la creació

de circuits impresos. Aquesta còpia posteriorment es pot perfeccionar usant algun tipus de fresadora. Una vegada creat el motlle, se'n fa la còpia amb silicona impermeable o sobre el material desitjat.

MythBusters Fingerprints Busted.

4.1.3. Validesa dels duplicats i mètodes per tal d'evitar l'atac

Els mètodes comentats amb anterioritat, o variants d'aquests mètodes, proporcionen còpies de gran qualitat si l'empremta font és de qualitat. Els mètodes comentats han estat provats amb èxit en diversos dispositius actuals.

Tal com s'ha vist, fer còpies d'empremtes dactilars és factible i no excessivament complicat, per tant la inclusió de mètodes per a detectar la naturalesa sintètica de les mostres és de vital importància. La principal manera d'evitar aquest tipus d'atacs està basada en la detecció de vida de la mostra. Els mecanismes més usats inclouen test de temperatura, conductivitat, batec del cor, pressió sanguínia, etc. Tot i així, s'ha de tenir en compte que aquests mètodes són difícils d'aplicar en sistemes que operen a l'exterior. Les condicions climatològiques obliguen a mantenir marges d'acceptació alts per tal de facilitar l'accés a personal autoritzat, cosa que facilita bastant un atac exitós. En aquests casos, la detecció de la vida de la mostra és fàcilment controlada per un agent de seguretat.

A continuació, es descriuran un conjunt de possibles mesures que cal aplicar per tal de detectar la vida en una empremta dactilar. Tal com veurem, la naturalesa del suport usat per a crear les còpies de les empremtes dactilars dificulta molt la implementació de mesures de seguretat.

1) Temperatura

En un entorn normal la temperatura de l'epidermis acostuma a ser entorn de 8 a 10 graus per sobre de la temperatura exterior. Si el sensor disposa de termòmetre, és possible fer controls de temperatura de les mostres. Tenint en compte que l'empremta sintètica, enganxada sobre el dit, ha de tenir un cert gruix la temperatura de contacte amb el sensor hauria de ser alterada i per tant facilitar la detecció que l'empremta no correspon a una epidermis humana.

Tot i així, com que les còpies de les empremtes acostumen a ser molt primes, la detecció per temperatura és difícil. En dispositius localitzats a l'exterior, les condicions climatològiques dificulten encara més la implementació d'aquest mecanisme en particular.

2) Conductivitat

Alguns sensors incorporen mètodes per tal de detectar la conductivitat del dit. Un dels problemes més grans d'aquest mètode és la variabilitat de la conductivitat de la pell. Estudis demostren que la conductivitat en condicions normals de la pell és aproximadament de 200 kΩ. Tot i així, en dies de fred, en el mateix dit, aquesta conductivitat pot baixar fins a diversos milions d'ohms o augmentar fins a pocs milers d'ohms en dies de calor. Tenint en compte aquesta variabilitat, els marges acostumen a ser massa amplis per a detectar empremtes fetes amb silicona i humitejades amb saliva.

3) Batec del cor

Alguns mecanismes implementen metodologies per tal de detectar el batec del cor en la mostra presentada. Tot i així, aquest mètode presenta diversos problemes a causa de la variabilitat del ritme cardíac. Individus practicants d'esport poden tenir un ritme cardíac inferior a quaranta batecs per minut, cosa que segons diversos estudis obliga a tenir el dit immòbil entorn de quatre segons, fet que alenteix molt l'autenticació de l'usuari. També s'ha de tenir en compte que la variabilitat del ritme cardíac en una mateixa persona fa virtualment impossible la seva aplicació com a mesura biomètrica complementària per tal de comprovar que el ritme cardíac no correspon a l'usuari registrat.

Condicionants del ritme cardíac

Un exemple clar el podem trobar en la variació del ritme cardíac depenent de si l'usuari ha agafat l'ascensor o ha pujat per les escales de l'edifici abans de fer la validació biomètrica.

Un altre punt que cal considerar en cas que només es vulgui detectar si hi ha batec o no és l'extrema primesa de la còpia sintètica feta. És habitual que el batec sigui detectable amb la còpia.

4) Constant dielèctrica

S'anomena **constant dielèctrica** la permissivitat d'un medi continu a transmetre ones electromagnètiques.

Alguns fabricants implementen mesures per detectar la vida de la mostra basada en aquesta constant de la pell humana, que és diferent de la constant dielèctrica de la silicona. Com en els mecanismes anteriors, s'ha de tenir en compte que per tal de no obtenir un *false rejection rate* excessiu el marge d'acceptació ha de ser configurat bastant alt.

Tot i la fiabilitat del mètode, hi ha mecanismes teòrics per a sobrepassar la protecció. Un dels més elaborats consisteix en la utilització d'alcohol per a impregnar l'empremta sintètica. Es coneix que l'alcohol 90% està format per un 90% d'alcohol i un 10% d'aigua i les seves constants dielèctriques respectives són aproximadament de 24 i 80. També es coneix que la constant dielèctrica d'un dit humà és entre aquests dos valors. Tenint en compte que l'alcohol s'evapora més ràpidament que l'aigua, durant l'evaporació hi haurà un moment en què la constant dielèctrica de la còpia caurà dins els marges d'acceptació i el lector hauria d'acceptar la mostra com a vertadera. El mètode sembla tenir validesa teòrica tot i que no se n'ha demostrat la validesa pràctica.

5) Pressió sanguínia

Alguns sensors existents al mercat són capaços de mesurar la pressió sanguínia usant mostres preses en dues posicions separades del cos. Aquestes mesures es basen a detectar el batec del cor en dos punts del cos i determinar la velocitat de propagació del batec per les venes. Sense considerar els desavantatges de la detecció del batec del cor, s'ha de considerar que s'ha de llegir el batec en dues posicions diferents, cosa que dificulta la validació de l'usuari. D'altra banda, com s'ha comentat, les còpies prou primes fetes amb silicona permeten llegir el batec del cor.

6) Detecció sota l'epidermis

Alguns sistemes avançats de reconeixement d'empremtes dactilars usen patrons de línies detectats sota l'epidermis. Aquests patrons són equivalents als patrons de línies detectats en l'empremta dactilar. Tot i així, aquests tipus de proteccions no són totalment segurs, ja que una vegada es coneix el tipus de protecció que usa el sistema es poden prendre mesures per tal de violar la seguretat del sistema.

Altres mètodes basats en els mateixos principis de prendre lectures del material existent sota la possible epidermis es basen en sensors ultrasònics per tal de mesurar la duresa i flexibilitat del material i també en la comprovació de la seva conductivitat.

4.1.4. Tècniques d'ofuscació per a evitar el reconeixement

Habitualment, les tècniques d'ofuscació basades en atacs al sensor es basen en la impressió de dades biomètriques sobre un suport sintètic. Aquestes dades biomètriques poden ser dades obtingudes d'altres individus o dades generades aleatòriament. Les tècniques d'impressió són equivalents a les tècniques de còpia sense cooperació.

Reflexió

Les tècniques de generació d'aquest tipus de dades són equivalents a algunes de les comentades en l'apartat 5 i per tant es reprendran en aquell apartat.

4.2. Reconeixement de cares

Com en la majoria d'atacs dirigits al sensor un dels primers passos que un possible atacant vol fer és obtenir les dades de l'usuari que es vol suplantar. En el cas de reconeixement de cares, aquesta tasca és extremament fàcil. Per adonar-se del fet, un només ha de considerar la quantitat de fotografies en què apareix. No sols les fotografies en què un posa sinó també totes les fotografies en les quals un apareix en l'escena, les fotografies preses per les càmeres d'entitats bancàries i comerços, gasolineres, autopistes, etc.

En aquest tipus d'identificació biomètrica sovint se suposa que no es pot evitar la captura de dades biomètriques sense autorització. Per tant, com en la majoria de casos, per tal d'evitar l'engany, els sistemes intenten detectar la vida de la mostra.

4.2.1. Imatges bidimensionals

En aquest tipus d'atac la còpia de les dades biomètriques es fa mitjançant una fotografia. La còpia és presentada a l'escàner o càmera que han de llegir les dades biomètriques. Aquest mètode acostuma a funcionar bé sobre sistemes en els quals no es detecten els ulls mitjançant els reflexos de les pupil·les o que no consideren la profunditat de les imatges preses. Els reflexos de la pupil·la sovint són usats per a obtenir la posició dels ulls i, amb aquestes, les altres característiques de la cara. Les imatges habitualment no retenen aquesta refractivitat i, per tant, no poden enganyar sistemes amb aquestes característiques.

4.2.2. Imatges bidimensionals amb forats per als ulls

En aquest tipus de còpia, la dada biomètrica, com en el cas anterior, és duplicada sobre un suport bidimensional. Per tal de ser robust en l'adquisició de dades mitjançant les pupil·les, en la imatge es retallen els ulls. Aquesta còpia és presentada a l'escàner sobre la cara del suplantador, per tal que el dispositiu detecti la còpia de la cara i els ulls del suplantador.

4.2.3. Imatges en vídeo

Aquest tipus d'atac es fa mitjançant seqüències de vídeo preses sense autorització de la víctima. Posteriorment a la captura del vídeo, les imatges són editades per destacar les característiques facials de la víctima. Habitualment, les imatges resultants acaben sent un conjunt d'imatges presentades com una seqüència de vídeo iteratiu de la cara de la víctima. Aquest conjunt d'imatges no cal que correspongui a una seqüència real de la cara, ja que la majoria de sistemes de detecció facial es basen en imatges fixes i no consideren imatges preses amb anterioritat de la cara analitzada. Les imatges es presenten al lector o càmera usant un dispositiu portàtil que tant pot ser un ordinador portàtil, un marc de

fotografies digitals o qualsevol dispositiu que pugui reproduir vídeo o seqüències de fotografies. Considerant la gran qualitat actual dels enregistradors de vídeo digital i dels dispositius de visualització, aquest atac és altament efectiu.

4.2.4. Validesa dels duplicats i mètodes per a evitar l'atac

Tot i que no tots els atacs són sempre efectius, molts dels comentats comprometen altament l'efectivitat de la majoria de sistemes de seguretat. Alguns dels atacs tenen diverses contramesures que efectivament eviten l'atac. Tot i que, una vegada l'atacant coneix les contramesures, aquestes poden ser compromeses novament.

Un primer mètode específic per a evitar que un atacant pugui presentar cares en un suport bidimensional consisteix en la **detecció de la profunditat de la imatge**. Sense necessitat d'usar càmeres tridimensionals, la percepció de la profunditat sovint és implementada variant el pla d'enfocament de la lent de la càmera per enfocar diferents profunditats de la imatge. En aquest cas, considerant que la dada biomètrica està copiada en un suport bidimensional, no conté profunditat i per tant el sistema no pot ser enganyat. Un possible truc, provat en alguns estudis, consisteix a apropar i allunyar la imatge per tal de simular la profunditat.

Altres tècniques per a evitar atacs més elaborats en què les dades són presentades al sensor mitjançant seqüències de vídeo estan basades en la detecció del moviment de les pestanyes, de la boca o d'altres parts de la cara. Tot i així, un atacant possiblement podria simular aquests moviments mitjançant seqüències de vídeo. Basats en el mateix principi de detectar moviment en la mostra, mètodes més eficaços es basen a sol·licitar que l'usuari faci una seqüència de moviments sol·licitats pel sistema, com poden ser parpellejar una sèrie de vegades, moure el cap fent els moviments requerits o fer moviments amb la boca. Tot i que, segurament, aquests tipus d'accions també poden ser plagiades, la complexitat de l'atac i les tècniques que cal usar per a fer la còpia de dades augmenta considerablement.

Com a comentari general, com que no hi ha una metodologia global per tal d'implementar una mesura de protecció eficaç, és aconsellable usar, com s'ha comentat en l'apartat "Defenses específiques per a millorar la seguretat en sistemes biomètrics", un conjunt de mesures complementàries com poden ser les anteriors o també la comparació no sols d'imatges estàtiques sinó seqüències de vídeo, captura d'imatges tèrmiques, etc.

4.2.5. Tècniques d'ofuscació per a evitar reconeixement

Les tècniques d'ofuscació per a reconeixement de cares tenen els mateixos principis que en el cas de l'empremta dactilar.

4.3. Reconeixement de l'iris

El **reconeixement de l'iris** és una de les característiques biomètriques més difícils de capturar sense consentiment, i també és molt difícil fer-ne còpies efectives. Tot i així, si es té la cooperació de l'usuari que cal suplantar és possible suplantar l'iris d'una víctima usant fotografies amb una qualitat raonable fetes amb microscopis digitals o càmeres amb alta resolució. En els mètodes d'atac més simples el suport de la imatge sintètica acostuma a ser paper mat imprès amb impressores de tinta. Per tal de millorar l'eficiència de l'atac, equivalent als mètodes de detecció de cares, en aquests casos també és habitual retallar la pupil·la en les imatges, ja que molts sensors usen la reflexió de la pupil·la per a detectar que la mostra és real. Tot i així, aquesta mesura depèn de la qualitat del sistema de seguretat.

Alguns experiments que apliquen el mètode anterior han demostrat l'efectivitat d'aquest atac en sensors comercials. Després de fer diversos tests, els experiments demostren la gran perillositat de l'atac i s'apropa al 100% d'acceptació de les dades generades. Tot i així, s'ha de considerar que els sensors usats són sensors no actuals i estan adreçats a l'àmbit domèstic.

Altres metodologies més avançades usades per a fer suplantacions de l'iris estan basades en lents de contacte. Sobre aquestes lents es pinten els patrons volguts. La més sofisticada de les tecnologies es basa a fer iris artificials mitjançant tècniques usades per a fer pròtesis oculars. Aquestes metodologies superposen una sèrie de patrons impresos en diverses capes semitransparents. Els resultats són d'alta qualitat, tot i que és difícil fer una captura i una impressió posterior de la retina capturada per dur a terme un atac de suplantació.

En casos com en el cas del mètode anterior, en què no és possible fer còpies fidels de les imatges fetes, és habitual usar els mecanismes per a crear identitats transferibles. En aquest cas, la lectura / el registre de l'usuari al sistema es fa amb una lent de contacte impresa prèviament. S'ha de tenir en compte que aquesta lent pot ser reimpresa i transferida tantes vegades com es vulgui atesa la seva naturalesa sintètica.

4.3.1. Validesa dels duplicats i mètodes per a evitar l'atac

Dos són els principals inconvenients o dificultats per a fer un atac de suplantació en un sistema basat en reconeixement de l'iris.

1) Cal considerar que és altament difícil capturar dades biomètriques d'una víctima sense la seva col·laboració (els dispositius de fotografia actuals no són tan avançats).

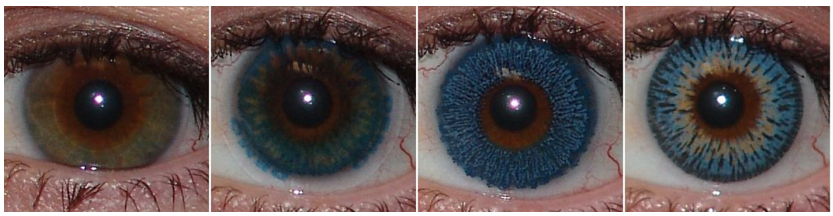
2) D'altra banda, tant els mètodes d'escaneig d'iris com la majoria dels mètodes de síntesi d'iris són molt especialitzats, la qual cosa en dificulta molt la còpia a personal no especialitzat.

Tot i que alguns experiments demostren la viabilitat de les còpies sintètiques de l'iris, la seva eficàcia és dubtable. Tot i així, hi ha mètodes per a detectar que l'iris presentat a l'escàner és sintètic. Un mètode bastant simple que els fabricants de sensors d'iris asseguren que funciona és la creació de bases de dades amb models de lents de contacte i la comparació de patrons, introduïts a les lents en temps de construcció, amb patrons detectats en les mostres capturades pel sensor. El principal inconvenient d'aquest mètode, en el cas hipotètic que funcionés, és que les bases de dades de patrons s'haurien de mantenir actualitzades per tal de garantir-ne l'eficiència, fet que implica la creació d'organitzacions de constructors de lents de contacte i la col·laboració de gran quantitat de països.

Iridian Technologies, Inc.

Una de les empreses que ha estudiat aquest tipus de mètodes amb combinació a la detecció de patrons no habituals (l'empresa no revela detalls de la tecnologia usada) és Iridian Technologies, Inc. En un estudi, elaborat el 2005, va estudiar diversos tipus de lents de contacte diferents adreçades a destacar o modificar el color de l'iris. La figura 2 mostra diversos tipus de lents usats en l'experiment. La primera imatge mostra l'ull sense lent de contacte.

Figura 2. Exemples d'imatges usades en l'estudi elaborat per Iridian Technologies, Inc. La primera imatge correspon a l'iris sense lent de contacte



Font: imatges obtingudes de Ph. D. Ulf Cahn von Seeles. *Countermeasures Against Iris Spoofing with Contact Lenses.* Iridian Technologies, Inc.

L'empresa assegura aconseguir errors d'un 12% en la detecció del tipus de lent i d'un 5% en la detecció de l'existència de lent.

Referència web

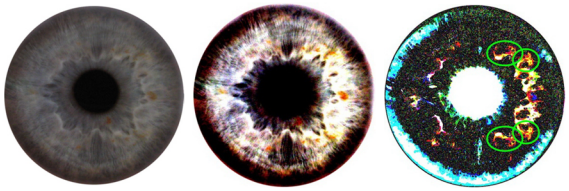
Aquesta informació es va extreure d'"Iris analysis & iris comparison". *ForBrains*.

Mètodes que també semblen eficaços per a la detecció de lents de contacte estan basats en models estadístics d'anàlisi de les textures. Aquests models poden ser tan usats per a la detecció de patrons repetits com també per a detectar altres tipus de patrons que no apareixen en retines reals. Un exemple d'aquest tipus de patrons són simetries en les dades capturades. Hi ha diverses maneres de detectar aquests patrons. A continuació es descriurà, a trets generals, la solució aplicada per l'empresa ForBrains.

En aquest cas, per a detectar possibles canvis de l'iris, és a dir, si l'usuari porta lents de contacte o no, aquesta empresa es basa a detectar petites reflexions que es produeixen entre la part interior de la (possible) lent de contacte i la còrnia de l'ull. La llum, en passar d'un medi a un altre, fa petits canvis de direcció (refracció). Quan la llum incideix sobre la lent de contacte, aquesta fa un petit canvi de direcció i continua en línia recta per tot el polímer que forma la lent. Una vegada arriba a la còrnia, considerant que aquesta es parcialment

reflexiva, no passa tota la llum, una part rebota sense arribar a entrar a la còrnia. Usant diverses càmeres d'alta velocitat (no necessàriament amb alta definició) situades en diferents angles, és possible aconseguir recuperar l'iris real i el fals. En aquest iris fals es detecten petites repeticions de patrons. En podem veure un exemple en la seqüència de figures següent. La figura 3a mostra un possible iris fals. Una vegada combinades les imatges i augmentat el contrast de l'iris, vegeu la figura 3b, és aplicat un algorisme de detecció d'arestes, figura 3c. Atesa la baixa probabilitat de simetries en un iris real, aquesta imatge és considerada alterada per una lent de contacte.

Figura 3



a. Iris capturat, potencialment fals. **b.** Combinació de diverses imatges preses en diferents angles amb un augment de contrast. **c.** Imatge original en la qual s'han detectat diverses simetries, potencialment corresponents a una lent de contacte
Font: imatge obtinguda d'"Iris analysis & iris comparison". *ForBrains*.

4.3.2. Tècniques d'ofuscació per a evitar reconeixement

Les tècniques d'ofuscació per a reconeixement d'iris tenen els mateixos principis que en el cas d'empremta dactilar.

5. Atacs indirectes (generació sintètica de dades biomètriques)

Aquesta tipologia inclou els atacs en els punts 2, 3, 4, 6, 7, 8 de la figura 1, és a dir, els que no van adreçats al sensor. En aquest apartat només ens centrarem en atacs sobre l'algorisme d'**extracció de característiques** (punt 3) i l'algorisme de **comparació** (punt 5).

Els atacs en el punt 3 que es comentaran estan dirigits a dur a terme un atac d'ofuscació. L'objectiu serà modificar l'aparença del suport de la dada biomètrica per tal que l'algorisme extractor no en pugui detectar les característiques biomètriques. En els atacs en el punt 5 l'engany és determinat per un conjunt de característiques biomètriques sintètiques presentades al sistema mitjançant el sensor, per tant aquest atac és aplicat amb combinació d'un atac directe. A diferència dels atacs en l'àmbit del sensor, l'atacant necessita conèixer informació addicional del sistema, i també detalls de funcionament intern i del procés de reconeixement. En alguns casos d'atacs en el punt 5, l'atacant també necessita tenir accés físic als components del sistema.

Reflexió

Els altres punts habitualment són atacats usant tècniques clàssiques de *hacking* i per tant no seran comentats.

5.1. Atac per ascens de turons

Un dels algorismes més coneguts per tal d'atacar el mòdul de comparació (punt 5) és l'algorisme basat en el **mètode *hill climbing***, traduït com a **ascens de turons**. El mètode és habitualment usat en el camp de les matemàtiques dedicat a l'optimització de funcions i correspon al grup dels mètodes d'optimització local. Atès que alguns dels algorismes presentats a continuació usen aquest mètode com a eina bàsica d'atac, se'n descriurà el funcionament bàsic. A trets generals, la idea bàsica d'un atac usant el mètode consisteix a generar dades biomètriques sintètiques que siguin acceptades pel sistema d'autenticació.

5.1.1. Descripció del mètode

L'objectiu principal de l'algorisme d'ascens de turons és trobar el màxim d'una funció d'una o diverses variables. Considerem que la funció de la qual es vol trobar el màxim correspon a $f(\mathbf{x})$, en què $\mathbf{x}$ correspon a un vector que tant pot ser discret com continu. En l'aplicació que estem estudiant, aquesta funció f modela les respostes de l'algorisme de comparació i el domini de la funció, és a dir, els possibles valors de $\mathbf{x}$, correspon a totes les possibles característiques biomètriques. A cada iteració t l'algorisme varia els valors del vector $\mathbf{x^t}$ i obté un vector nou, $\mathbf{x^{t+1}}$. Aquest vector nou s'ha obtingut variant una de les components del vector $\mathbf{x^t}$, per tal que el vector nou millori el valor de la funció. És a dir:

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

L'algorisme finalitza quan no hi ha cap variació del vector **x** que millori la funció objectiu, és a dir, hem arribat a un màxim.

S'ha de considerar que aquest mètode és bastant poc robust a màxims locals, crestes, valls o altiplans de la funció objectiu.

5.2. Atacs per ascens de turons en sistemes basats en empremtes dactilars

A continuació, es descriuran dues metodologies per a generar dades dactilars sintètiques que siguin acceptades per un sistema de seguretat basat en biometria i una metodologia per a fer un atac d'ofuscació.

5.2.1. Atac en el punt 5 de la figura 1 mitjançant ascens de turons

És habitual que els sistemes d'autenticació basat en empremtes dactilars utilitzin solament *minutiae* referents a terminacions i bifurcacions. Els més simples es basen en la localització de les *minutiae* (posició (x, y) en la imatge) i l'orientació associada. La possible aplicació de l'atac basat en *hill climbing* descrita a continuació està basada només en aquests tres atributs, tot i que és fàcilment extensible per a considerar una quantitat d'atributs més gran.

L'objectiu principal de l'atac consisteix a generar una sèrie de *minutiae* sintètiques amb les quals els resultats d'autenticació siguin prou elevats perquè el sistema de seguretat reconegui les empremtes com a correctes. L'atac va dirigit a suplantar un usuari D concret, tot i que la informació sobre els usuaris no és coneguda per l'atacant. L'atacant únicament té accés als resultats de l'algorisme de comparació.

L'atac que s'il·lustra es basa en cinc passos que es repeteixen iterativament fins que el resultat és el volgut:

1) Inicialització. El primer pas consisteix en la generació d'una sèrie de *minutiae* de manera aleatòria formada per tal de formar una empremta dactilar fictícia. Cada *minutia* està formada per la posició en la imatge i l'orientació, *i.e*(x, y, θ). Generarem P empremtes dactilars, que anomenarem T^i, $i \in \{1 \ldots P\}$.

2) Comprovació del resultat de comparació al sistema. S'ataca l'usuari seleccionat amb cadascuna de les dades generades en el pas 1, *biometric_compare*(D, T^i), en què D correspon a l'usuari objectiu. Els resultats corresponents a cada comparació es guarden.

3) Escollir el millor resultat T^*, en què:

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

4) Si algun dels patrons T^* és acceptat pel sistema, seleccionar el patró com a bona aproximació de les dades biomètriques de l'usuari *D*. Si no, passar al pas 5.

5) A partir del millor patró sintètic T^*, generar una sèrie de patrons auxiliars T^i modificant aleatòriament *minutiae* existents, afegint *minutiae* i esborrant *minutiae* noves. Passar al pas 2.

L'atac presentat està dirigit únicament a un sol usuari, tot i que per tal de millorar l'eficiència de l'atac sovint s'ataquen diversos usuaris en paral·lel.

L'atac basat en *hill climbing* acostuma a ser molt efectiu per a aconseguir accés al sistema, tot i que requereix temps i accés al sistema o almenys a una còpia. Tot i l'efectivitat d'aquest tipus d'atac, hi ha diverses maneres de protegir-se.

La manera més intuïtiva de protecció es basa a no mostrar la taxa d'acceptació de la mostra, tot i que aquesta solució no és sempre efectiva, ja que en alguns casos aquesta taxa és utilitzada fora del dispositiu de comparació. Un exemple el podríem trobar en sistemes que usen múltiples dades biomètriques que són obtingudes de diversos dispositius i un sistema central decideix si l'usuari és vàlid o no. En sistemes que usen resultats quantificats és habitual mesurar la taxa d'acceptació amb relació al temps que l'algorisme de comparació ha necessitat per a comparar les dades introduïdes amb les dades registrades al sistema (*side channel attack*).

Una altra solució possible per a evitar atacs basats en *hill climbing* és retornar resultats ficticis que no alterin el resultat d'acceptació de les dades introduïdes. Aquests resultats semialeatoris estan adreçats a trencar possibles correlacions entre les dades introduïdes i el resultat produït.

Finalment, val la pena comentar que una de les solucions més simples però efectives d'evitar aquest tipus d'atacs és limitar el nombre de comparacions per usuari que es poden fer en un dia. S'ha de considerar que habitualment els atacs per *hill climbing* necessiten un gran nombre de comparacions. Per tant, limitar el nombre de comparacions possibles elimina en gran manera la utilització d'aquest tipus d'atacs.

5.2.2. Reconstrucció de dades dactilars usant informació de plantilles

Referència bibliogràfica

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

El la primera metodologia d'atac que s'ha comentat no es coneixia cap tipus d'informació de l'usuari. En aquest cas, el mètode que es descriurà considera coneguda la **informació corresponent a les *minutiae* d'un usuari** per tal de generar una possible empremta dactilar (és a dir, reconstruir un conjunt possible d'arestes que continguin les *minutiae* volgudes) que sigui acceptada pel sistema d'autenticació biomètrica. El mètode, proposat per Cappelli i altres, està basat en tres punts principals:

1) Es dedueix l'àrea de la imatge que cal construir.

2) Es dedueix l'orientació de les arestes mitjançant una anàlisi de l'orientació de les *minutiae*.

3) Es genera la imatge donades les *minutiae*, la mida i orientació de les arestes.

1) Informació obtinguda de la plantilla

En la metodologia proposada per Cappelli i altres les dades són obtingudes d'una plantilla basada en l'estàndard ISO/IEC 19794-2:2005. Podríem imaginar que capturada mitjançant un atac d'intrusió a la base de dades o un atac d'anàlisi al mitjà de comunicació. En aquest cas, la plantilla aporta la informació general sobre la imatge següent: amplària i alçària de la imatge i resolució. A més, per a cada una de les n *minutiae* m_i aporta informació sobre:

- tipus t_i (en aquest cas només es consideren terminació i bifurcació),
- posició (x_i, y_i) i
- orientació θ_i

2) Detecció de l'àrea de la imatge

És fàcil veure que la mida de les empremtes dactilars varia segons la mida del dit i la pressió exercida sobre el sensor. Per tant, si es pretén generar una imatge que s'assembli a una empremta dactilar real, la mida de la imatge correspon a una de les característiques bàsiques que cal determinar. Una possible manera d'estimar-ne la mida seria usant un model genèric configurable usant un conjunt reduït de paràmetres. En aquest cas, Cappelli i altres proposen fer servir un model que usa quatre paràmetres. Com es mostra en la figura 4, el model conté quatre arcs el·líptics i un rectangle que són configurables mitjançant els quatre paràmetres comentats (b_1, b_2, a_1, a_2).

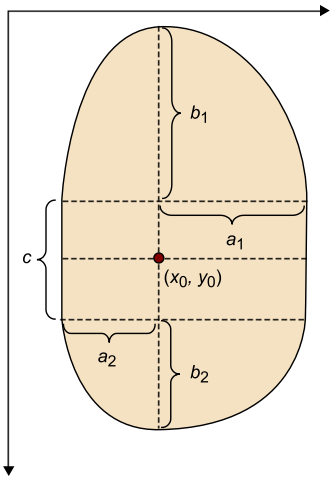


Figura 4. Possible prototip de l'àrea d'una empremta dactilar

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

Aquests quatre paràmetres poden ser obtinguts mitjançant diversos procediments considerant la posició coneguda de les *minutiae* que han de ser presents en la imatge. Un dels algorismes més senzills està basat en un algorisme *Greedy* que simplement incrementa els valors dels paràmetres b_1, b_2, a_1, a_2 fins que totes les *minutiae* són contingudes dins l'àrea generada. Altres algorismes més avançats podrien, per exemple, considerar petites rotacions de la imatge per tal de generar una àrea millor aproximada.

3) Detecció de l'orientació de les arestes

L'orientació de les arestes en la imatge en defineix el moviment al llarg de la imatge. Aquesta dada representa una informació crucial per a obtenir una bona imatge final. Per a obtenir una possible orientació de les arestes de la imatge només basant-nos en informació obtinguda a partir de l'orientació de les *minutiae* hi ha diversos mètodes. Un dels més senzills es basa a triangular la imatge considerant la posició de les *minutiae* i deduir l'orientació per separat en cada triangle format. Aquest mètode necessita un postprocessament per tal de generar imatges d'orientació suaus. Altres mètodes, més eficaços, usen altres tipus d'informació per a generar models més acurats, com, per exemple, la posició de possibles singularitats que defineixen el tipus d'empremta. Sense considerar el mètode usat en la detecció de l'orientació de les arestes, el resultat ha de ser l'orientació de les arestes per a cada punt de la imatge que es vol generar. En el nostre cas, definirem aquesta orientació com un angle $\theta_{x,y}$.

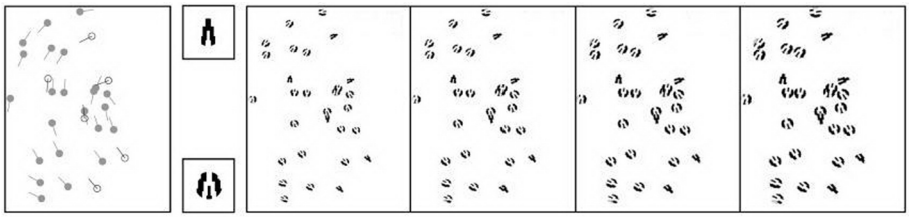
4) Generació de la imatge

Considerant la informació obtinguda en els punts anteriors, un mètode eficaç per a generar una imatge només considerant la informació donada per les ***minutiae*** de la imatge es basa en dos passos.

En el primer pas, partint d'una imatge de l'àrea requerida, es col·loquen prototips de les *minutiae* a les posicions indicades per les dades inicials del problema. Aquests prototips acostumen a ser imatges d'una possible *minutia*. Aquestes imatges prototip són escalades considerant la mida requerida i el nombre

d'arestes per unitat de mesura requerida en la imatge resultant. La figura 5 mostra diverses imatges en què els patrons de *minutiae* bifurcació i terminal han estat introduïts en diverses mides.

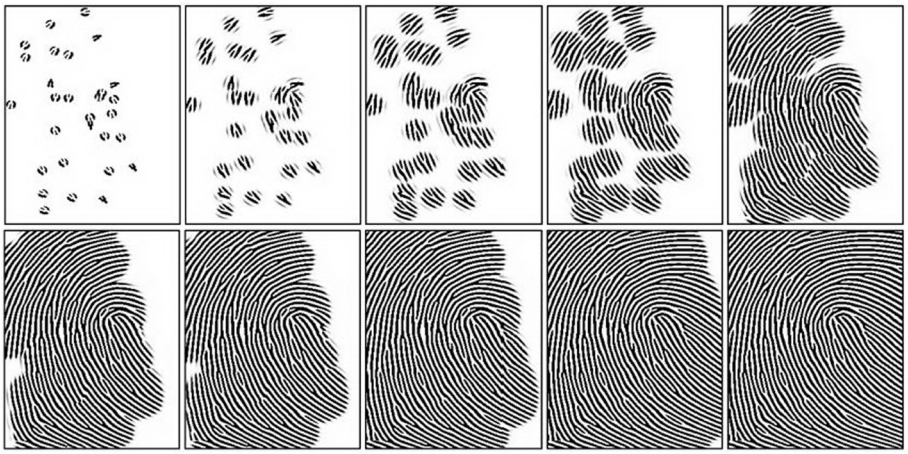
Figura 5. Inserció de patrons mitjançant imatges



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

Una vegada aquests patrons de les *minutiae* han estat introduïts en la imatge, aquesta es completa introduint arestes fictícies (recordem que no se'n coneix l'orientació real) usant la informació d'orientació de les arestes obtinguda $\theta_{x,y}$. Una manera bastant efectiva de fer-ho és usant filtres de Gabor que són aplicats a l'entorn de les zones conegudes per tal d'engrandir-les. Inicialment, només les *minutiae* són zones conegudes. La figura 6 mostra un exemple d'aquest procés iteratiu.

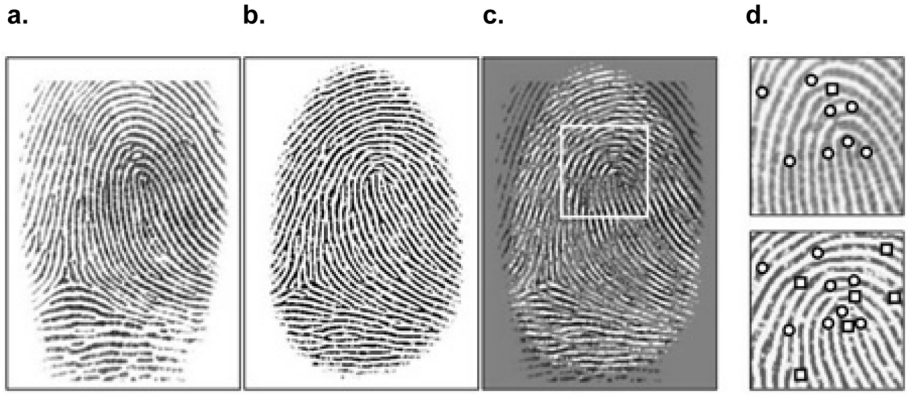
Figura 6. Algoritme de generació d'arestes



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

Tot i l'efectivitat demostrada de la metodologia descrita, és probable que mètodes d'identificació biomètrica, humans o automàtics, siguin capaços de detectar que la mostra ha estat generada de manera sintètica. La figura 7 mostra una empremta real i el seu equivalent generat sintèticament amb el procediment descrit.

Figura 7. Emprenta real i equivalent sintètic



a. Imatge original. **b.** Equivalent generat sintèticament. **c.** Solapament de les dues imatges. **d.** Característiques detectades
Font: R. Cappelli; A. Lumini; D. Maio; D. Maltoni (2007). "Fingerprint image reconstruction from standard templates". A: *IEEE Transactions on Pattern Analysis and Machine Intelligence* (núm. 29, pàg. 1489-1503).

Des del punt de vista humà, la imatge generada pot no correspondre a una imatge real, ja que es detecta molta repetició de patrons generada pel procés de creació d'arestes. Des del punt de vista d'un sistema automàtic, pot ser fàcilment detectable que l'empremta és sintètica si les arestes són massa sòlides per a tractar-se d'una mostra real. També es podria tenir en compte el soroll de la imatge, que en podria delatar en gran manera la naturalesa sintètica. Per tal de solucionar aquests problemes habitualment abans de la utilització de la imatge se'n fa un postprocessament, en el qual s'hi afegeix soroll. Diverses tècniques poden ser emprades per tal de generar soroll sobre la imatge resultant, dues de les més clàssiques són les següents:

- Introducció de soroll en forma de punts blancs de diferents formes i mides al llarg de tota la imatge resultant. Aquest tipus de soroll està adreçat a simular irregularitats en l'adquisició de les imatges, tant siguin degudes al sensor o explícites a l'empremta dactilar.

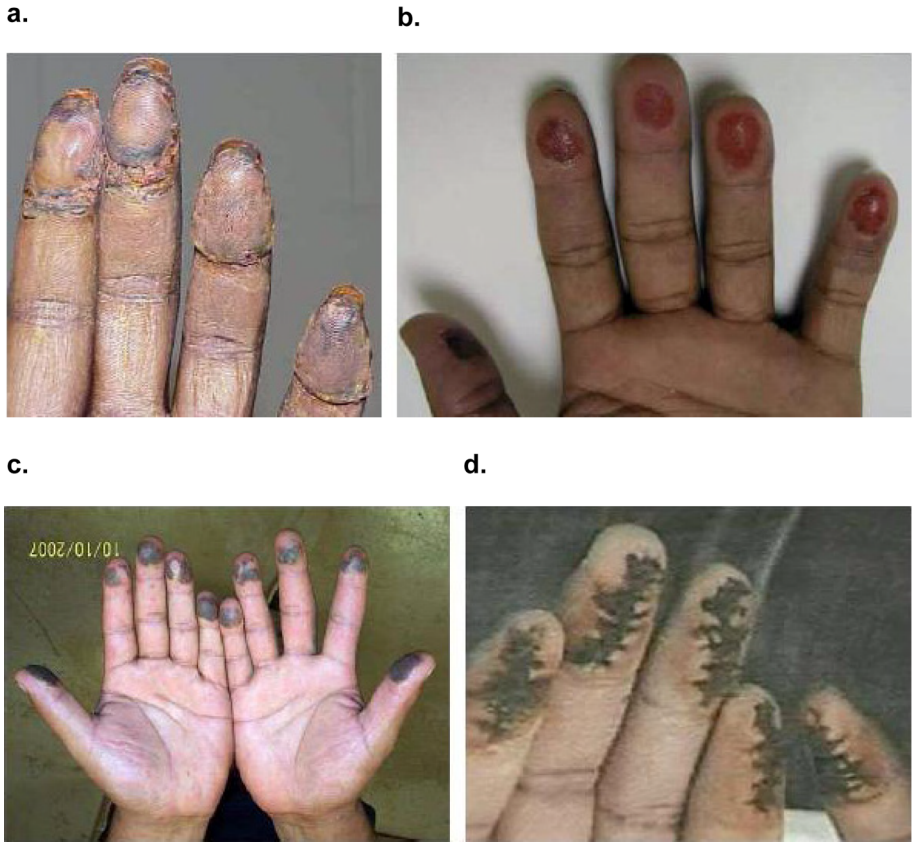
- Suavització del resultat mitjançant filtres d'allisat.

5.2.3. Tècniques d'ofuscació per a evitar reconeixement

Les tècniques d'ofuscació aplicades a empremtes dactilars es divideixen en tres categories: obliteració, distorsió i imitació.

En els **atacs per obliteració** les empremtes dactilars o únicament les arestes són extirpades o mutilades usant diverses metodologies, com poden ser: abrasió, talls, cremades químiques o transplantaments de pell. Alguns exemples d'obliteració d'empremtes es poden veure en la figura 8.

Figura 8. Exemples d'alteració d'empremtes dactilars.



a. Empremtes trasplantades. **b.** Empremtes mossegades. **c.** Empremtes cremades mitjançant àcid. **d.** Empremtes extirpades
Font: J. Feng; A. K. Jain; A. Ross (2009). *Fingerprint alteration*.

Les empremtes obliterades, depenent de la profunditat i de l'àrea malmesa, enganyen fàcilment els sistemes automàtics de detecció i passen també mecanismes de control de qualitat. Per aplicar aquest tipus d'atacs s'ha de considerar que l'epidermis és regenerarà correctament si la profunditat de la lesió produïda no supera el mil·límetre de profunditat. En aquest tipus d'atacs, s'ha de considerar un bon equilibri entre l'àrea lesionada i l'àrea no lesionada. Una lesió massa extensa probablement enganyarà l'algorisme de comparació però no passarà els controls de qualitat suficients i serà fàcilment detectable tant per mitjans automàtics com per mitjans humans. D'altra banda, si la lesió no és prou extensa, és possible que el sistema encara sigui capaç de recuperar la identitat real de l'atacant.

En els **atacs per distorsió** les arestes de l'empremta dactilar són modificades mitjançant cirurgia plàstica. Aquestes modificacions es basen en amputacions de part de la pell, i re-col·locació d'altres. Els procediments quirúrgics per a fer modificacions en les empremtes dactilars no acostumen a ser difícils. Les empremtes dactilars resultants no acostumen a coincidir amb l'original i en molts casos són difícilment detectables; tot i així, la qualitat de les distorsions depèn en gran manera de la qualitat de la cirurgia. Podem veure dos exemples d'empremtes distorsionades en la figura 9. En el primer cas es pot veure

que la qualitat de la cirurgia no és gaire bona i per tant l'engany és fàcilment detectable; en el segon cas es pot veure una millor qualitat en la distorsió de l'empremta.

Figura 9. Dues imatges d'empremtes obliterades proporcionades per la Michigan State Police i el DHS

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

En els **atacs per imitació** les empremtes dactilars són substituïdes, usant mitjans quirúrgics, per empremtes d'altres parts del cos, com poden ser altres dits de les mans o dels peus. En aquest tipus d'atacs, les empremtes acostumen a tenir un aspecte molt natural i si les cicatrius són discretes poden fins i tot enganyar usuaris humans experts.

Els mecanismes automàtics de detecció d'empremtes ofuscades es basen en la detecció de patrons no naturals en les arestes de l'empremta. Aquests patrons són detectats usant l'orientació de les arestes. En un primer pas s'extreuen un conjunt de característiques que descriuen l'empremta per, en un segon pas, usant un classificador binari, classificar les empremtes entre alterades i no alterades.

5.3. Reconeixement de cares

5.3.1. Atac en el punt 5 de la figura 1 mitjançant ascens de turons

En aquest apartat es descriu una possible manera de generar un atac basat en *hill climbing* en un sistema de reconeixement de cares basat en valors propis. Igual que en l'atac a empremtes dactilars, l'atac està adreçat a un usuari concret. En aquest cas, l'atacant té accés a una base de dades amb fotografies de cares ($LI = \{IM_0, IM_1, \ldots, IM_M\}$), una imatge de la cara que es vol

atacar (IM_{targ}), accés a l'algorisme de comparació i al resultat que retorna ($MS = biometric\_compare(IM_i, IM_{targ})$). L'algorisme és, en certa manera, equivalent al donat per empremtes dactilars.

L'algoritme bàsic per a aplicar un atac per *hill climbing* pot ser descrit en quatre punts:

1) Preparació de la base de dades que s'utilitzarà per a fer l'atac. En aquest punt l'atacant prepara la base de dades. Igual que en els sistemes de reconeixement basats en vectors propis, les imatges han de tenir la mateix mida i estan alineades. En aquest cas, podríem suposar que les imatges estan alineades mitjançant la posició dels ulls.

2) Càlcul de les *eigenfaces*. En aquest punt es calculen un conjunt d'*eigenfaces* donades les imatges descrites en el punt 1. Cada *eigenface* serà identificada amb el símbol EF_i.

3) Inicialització de l'atac. Una imatge de la base de dades és seleccionada aleatòriament (IM_0). Aquesta imatge serà modificada posteriorment per tal d'adaptar-se tant com sigui possible a la imatge destinació (IM_{targ}). La imatge seleccionada és la que correspon a una similitud inicial màxima a IM_{targ}.

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

a) Escollir aleatòriament una *eigenface* de la base de dades *LI*; anomenarem la imatge EF_k.

b) Calcular per a un conjunt petit de valors $c = \{c_1, \ldots c_j\}$ el valor de l'algorisme de comparació:

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

c) Seleccionar c_{max} com el valor que dóna millor resultat MS_j.

d) Actualitzar la imatge actual:

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

e) Truncar valors de la nova imatge generada IM_{i+1} en cas que surtin del rang establert (0..255).

f) Anar al pas **a)** fins a $i = i\_max$ o fins que no hi hagi millora.

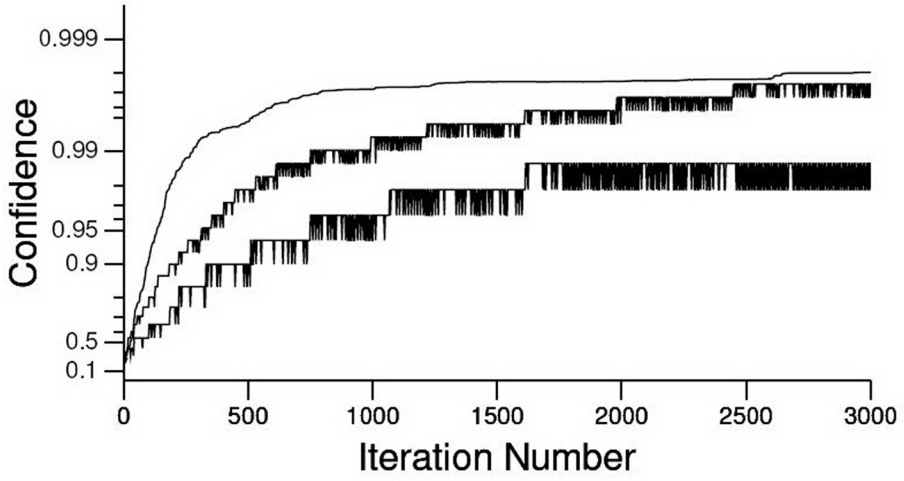
Una primer metodologia per a fer front a aquest atac va ser la implantació de resultats quantificats de l'algorisme de comparació (The BioAPI Consortium, BioAPI Specification (Version 1.1) març del 2001). Tot i així, s'ha demostrat que amb modificacions a l'algorisme de *hill climbing* que s'ha explicat prèviament encara es poden generar dades que s'assemblin a un usuari concret.

En un estudi elaborat per Andy Adler, mitjançant una modificació de l'algorisme presentat, s'obtenen resultats més que satisfactoris. Els resultats obtinguts es mostren en la figura 10. Es pot observar que, tot i que la quantificació dels resultats retornats per l'algorisme de comparació no alteren gaire l'efectivitat de l'atac, l'algorisme obté en tots els casos una confidència de coincidència superior al 95%.

Referència bibliogràfica

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

Figura 10. Resultants de confidència de l'algorisme proposat per Andy Adler



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

Figura 10

Les diferents corbes corresponen a diversos nivells de quantificació dels resultats retornats per l'algorisme; la corba superior correspon a resultats sense quantificació.

5.3.2. Tècniques d'ofuscació per a evitar el reconeixement

Tot i que en la majoria de casos els atacs efectuats són atacs de suplantació, també hi ha atacs o metodologies per a evitar que un usuari sigui reconegut per un sistema de detecció automàtic. Hi ha diverses metodologies, tot i que en aquest apartat només ens centrarem en dues.

La primera metodologia està adreçada a evitar que càmeres de seguretat col·locades estratègicament a la via pública o a comerços puguin capturar dades biomètriques dels usuaris. Per tal de veure l'efectivitat de la metodologia cal considerar que en la majoria de casos les càmeres estan situades en posicions elevades per a evitar obstacles i tenir una millor perspectiva. Un mètode de baixa tecnologia i altament eficaç és l'ús de dessuadores, en què la cara va amagada dins la caputxa. Considerant la posició prou elevada de les càmeres, és bastant difícil obtenir imatges de qualitat a causa de les ombres i de la mala visualització que s'obté.

Lectura recomanada

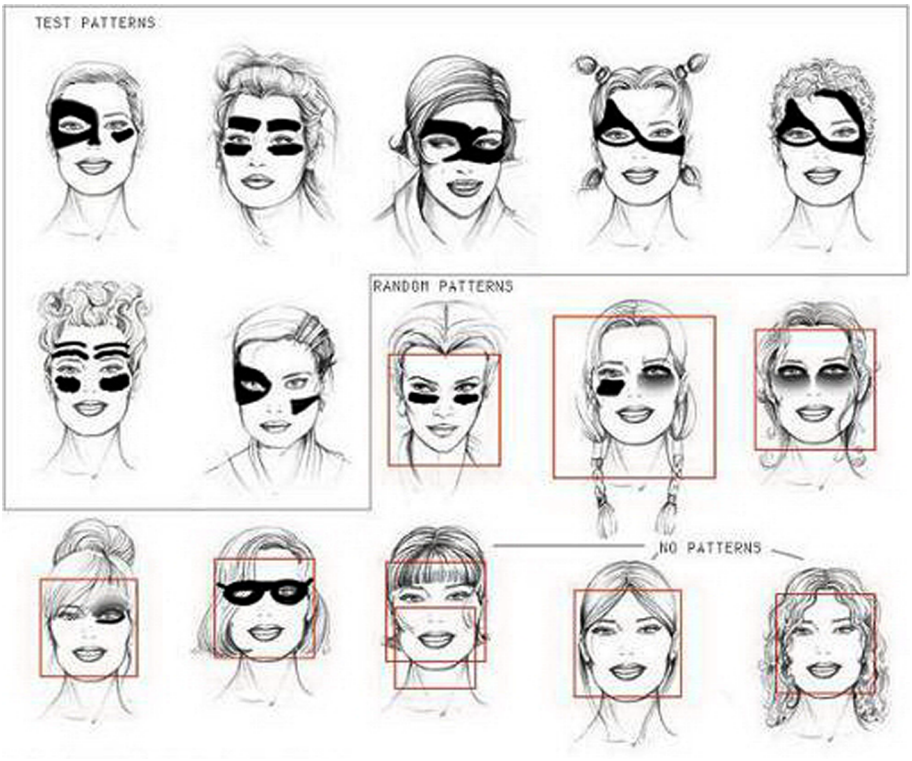
B. Rounds (2010). "Fool facial recognition technology". *How to vanish*.

Una altra metodologia bastant eficaç per a evitar la detecció automàtica és l'ús de maquillatge. Hi ha estudis, un dels més interessants dels quals elaborat per Adam Harvey, en què s'han estudiat diversos patrons de maquillatge per tal d'ofuscar diverses característiques facials. Les tècniques de reconeixement basades en característiques permet aplicar maquillatge per tal de manipular i distorsionar els punts de referència usats per a detectar la cara i evitar per tant aquesta detecció. Alguns del patrons estudiats es presenten en la figura 11.

Referència web

Per a més informació sobre l'estudi d'Adam Harvey podeu visitar CV Dazzle.

Figura 11. Patrons estudiats per Adam Harvey



Font: A. Harvey. *CV Dazzle.*

Els estudis elaborats amb els patrons descrits mostren la gran efectivitat del sistema. En cap dels patrons estudiats els sistemes de detecció no aconsegueixen detectar la cara.

6. Atacs *side channel*

Com s'ha vist en l'apartat "Atacs indirectes (generació sintètica de dades biomètriques)", la majoria d'atacs es basen a adaptar el model generat considerant el resultat obtingut per l'algorisme comparador. Considerant que moltes de les vegades l'atacant no disposa d'aquesta informació, ja que els algorismes i metodologies de reconeixement acostumen a ser secrets, és habitual aplicar atacs de tipus *side channel*.

Els **atacs *side channel*** es basen a obtenir aquest resultat de l'algorisme de comparació que quantifica la validesa de la dada biomètrica presentada al sistema, analitzant el temps d'execució, el consum d'energia de la màquina, les ones electromagnètiques despreses o simplement el soroll produït.

Aquests tipus d'atacs són habitualment aplicats a sistemes criptogràfics, tot i que poden ser fàcilment adaptats per ser aplicats a sistemes biomètrics. Els **atacs basats en temps**[5] consisteixen en l'anàlisi del temps de càlcul usat per a executar l'algorisme de comparació. És fàcil veure que aquest temps depèn fortament de les dades d'entrada. Diversos experiments han demostrat que els algorismes usats en les comparacions de les dades acostumen a usar més temps en la comparació de dades incorrectes que en la comparació de dades correctes. Els **atacs basats en anàlisis de la quantitat d'energia**, **pèrdues electromagnètiques** i de **soroll** van en la mateixa direcció.

(5)En anglès, *timing attack*.

Activitats

1. Com creieu que es podrien detectar automàticament atacs basats en coacció? I els basats en conspiració? Com creieu que afectarien les solucions que proposeu a la usabilitat del sistema?

2. Amplieu la informació relacionada amb els estàndards llegint els documents següents:

- 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. Amb relació a la síntesi d'empremtes dactilars comentada en el subapartat "Empremta dactilar", què penseu de la validesa dels duplicats? Us sembla que les mesures de protecció comentades proporcionen un percentatge de seguretat prou alt? Considerant que sou el dissenyador del sistema, quines utilitzaríeu? N'afegiríeu alguna de no comentada?

4. Visiteu les pàgines web esmentades al llarg del mòdul. Quina de les tècniques creieu que és la més fàcil d'implementar per fer un atac de suplantació? I d'ofuscació? Què penseu que és més senzill: fer un atac dirigit al sensor, a l'extractor de característiques o a l'algorisme de comparació?

5. Amb relació als atacs indirectes dirigits a l'algorisme de comparació, creieu que es podria millorar l'eficiència del mecanisme proposat (*hill climbing*) amb combinació d'altres tècniques com la cerca tabú? Creieu que altres mètodes d'optimització, com, per exemple, algorismes genètics o *simulated annealing*, funcionarien millor? En cas que la metodologia sigui aplicable, intenteu generar un pseudocodi dels algorismes resultants.

6. Poseu en funcionament el sistema de reconeixement de cares de Picassa o, en el cas de disposar-ne el del telèfon mòbil, intenteu aplicar un atac d'ofuscació basat en els patrons dissenyats per Adam Harvey.

7. Dissenyeu alguna metodologia per tal d'aplicar un atac *side channel* al sistema de reconeixement facial del Picassa. Com transformaríeu les dades obtingudes en dades usables per a fer un atac de suplantació basat en *hill climbing*?

Abreviatures

ANSI American National Standards Institute ('Institut Nacional Nord-americà de Normalització')

DHS Department of Homeland Security

IDS Intrusion detection system

ISO International Organization for Standardization ('Organització Internacional per a la Normalització')

PIV Personal identity verification

Glossari

constant dielèctrica *f* Relacionada amb l'electromagnetisme. És la mesura de resistència que té un medi quan s'hi aplica un camp electromagnètic.

dongle *m* Equivalent a clau electrònica o cadenat electrònic.

falsejament d'identitat *m* Atac de suplantació d'identitat.
en spoofing

hill climbing *m* Tècnica d'optimització matemàtica que pertany a la família de cerca local.

intercepció *f* Atac en què s'adquireix el poder de modificar els missatges entre dues parts que es comuniquen.
en man-in-the-middle

man-in-the-middle *m* Vegeu **intercepció**.

obliteració *f* Acció de fer illegible un element.

pesca *f* Atac amb l'objectiu d'aconseguir informació privada d'un usuari mitjançat la suplantació d'una entitat confiable.
en phishing

phishing *m* Vegeu **pesca**.

sniffing *m* Acció d'analitzar els paquets que es transmeten per un mitjà de comunicació.

spoofing *m* Vegeu **falsejament d'identitat**.

Bibliografia

Bibliografia bàsica

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

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

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

Harvey, A. *CV Dazzle*

"Iris analysis & iris comparison". *ForBrains*.

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

Ulf Cahn von Seeles, Ph. D. *Countermeasures Against Iris Spoofing with Contact Lenses*. Iridian Technologies, Inc.

Bibliografia complementària

Galbally, J.; Cappelli, R.; Lumini, A.; Maltoni, D.; Fierrez, J. (2008). "Fake fingertip generation from a minutiae template". A: *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". A: *International Congress on Pattern 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". A: *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-Garcia, J. (2008). "Ataques directos usando imágenes falsas en verificación de iris". A: *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". A: *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents*.