CCN
Centro Criptológico Nacional

Spanish Certification Body

"New Challenges on Biometric Vulnerability Analysis on Fingerprint Devices"

Esquema de Evaluación y Certificación de la Seguridad de las Tecnologías de Información

Technical Manager
September 2008

Contents

Introduction: Biometric Technology Security Evaluation

New Challenges in the VA of Fingerprint TOEs

Part 1: Methodological point of view

1) General overview

2) Fingerprint attacks methodologies

3) Characterizing attacks to fingerprint devices

Part 2: Technical point of view

1) Reverse engineering on biometric standards

2) Match on Card (MoC) fingerprint devices

Future challenges

Introduction: Biometric Technology Security Evaluation

(1) **Performance evaluation**:

- NIST, ISO
- E.g. ISO/IEC 19795

Objective:

FAR: False Acceptance Rate.
FRR: False Rejection Rate.
ROC: Receiver Operating Characteristics.
EER: Equal Error Rate.
FTE: Failure to Enroll.

(2) **Security evaluation**:

- ISO/IEC 19792 “Security Evaluation of Biometrics”
- Common Criteria: “Biometric Evaluation Methodology” (BEM) U.K.
- PPs and STs: German, U.S. and U.K. Schemes.
- Fingerprint Attack Methodology: Spanish Scheme

Methodological Evaluation Challenges

General overview in terms of evaluation methodology

Common Evaluation Methodology (CEM) provides a general technology-independent framework, more detailed methods to evaluate the security of <u>specific technologies</u> are a clear necessity.

In the <u>area of biometric security</u> several attempts to standardize a generic biometric evaluation methodology have been developed, but until now the same situation than in the general field of IT security evaluation has been achieved i.e. very <u>generic methods</u> that are only a general approach for the experts belonging to evaluation facilities that have to deal with this kind of technical testing procedures.

The key part of CC/CEM applied to specific technology types is AVA_VAN: <u>penetration testing</u>

Previous success cases in <u>other technologies</u> like Smartcards and similar devices can be extended to fingerprint devices.

Methodological Evaluation Challenges

Previous experience in the SP CB: Fingerprint Attack Methodology (FAM)

- Challenge: provide detailed guidance for evaluators doing pen-testing with fingerprint authentication devices

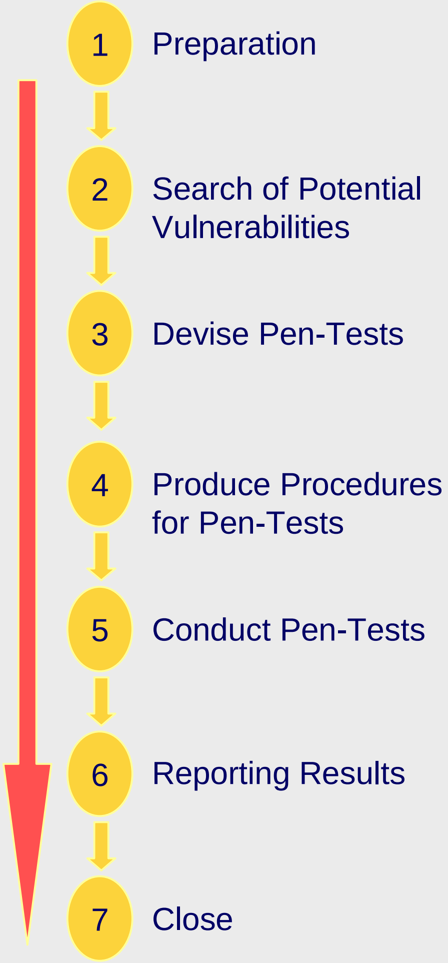
- Applicable to CC v2.3 and v3.1

- Biometrics state-of-the-art review: performace / security evaluation

- Link to CEM, fingerprint-specific issues:
  - Search of Potential Vulnerabilities
  - Devise of Pen-Test Cases
  - Conduct Pen-Test Cases

- Attack types:
  - Type 1, sensors: fake fingers / optical, thermal sweep, solid-state
  - Type 4, input to the matcher: brute-force, hill-climbing

- Presented in ICCC 2006



Methodological Evaluation Challenges

CAFD supporting document: “Characterizing Attacks to Fingerprint Devices”

Proposal: guidance supporting document - CCDB-2008-nn-nnn

First draft released: Versión 1.0 Release 1 January 2008

Field of special use: Fingerprint and Biometric devices.

Main necessities that are the objective of CAFD:

1) guidance about attack methods to be considered in a fingerprint based biometric product evaluation.

2) standardization of the security rating: guidelines & examples for the attack rating.

Methodological Evaluation Challenges

CAFD supporting document: “Characterizing Attacks to Fingerprint Devices”

CEM versions used in CAFD examples:

- CC v3.1 attack potential rate tables for AVA.
- CC v2.3 approach of attack = ID + Exploitation

Template filled for each type of attack:

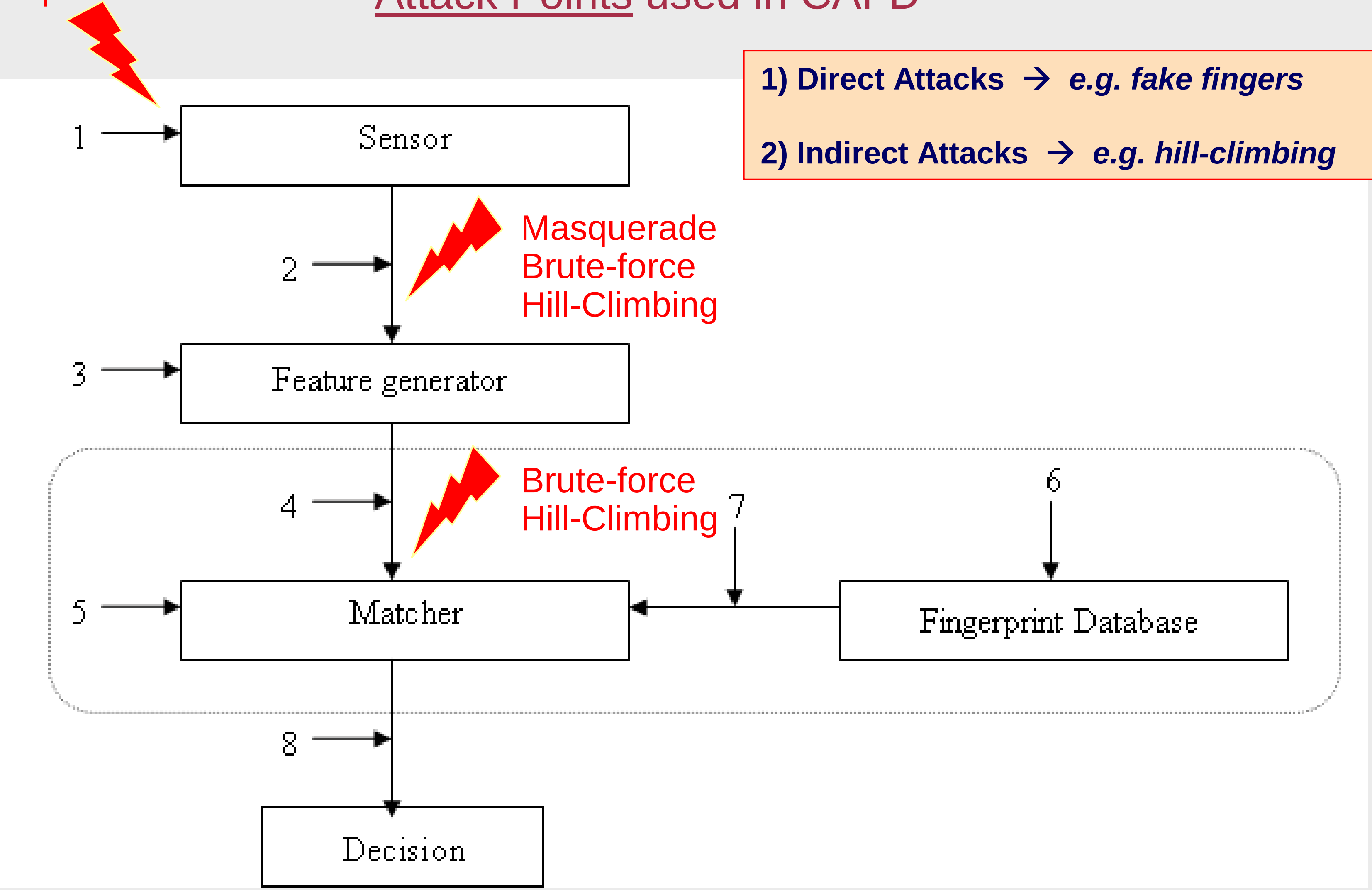
- Description of the attack
- Effect of the Attack
- Impact on TOE
- Characteristics of the Attack
- Examples of attack types
- Examples of attack potential ratings

Methodological Evaluation Challenges

Attack Points used in CAFD

1) Direct Attacks → *e.g. fake fingers*

2) Indirect Attacks → *e.g. hill-climbing*



Fake fingers
Masquerade

Masquerade
Brute-force
Hill-Climbing

Brute-force
Hill-Climbing

Methodological Evaluation Challenges

CAFD supporting document: “Characterizing Attacks to Fingerprint Devices”

Table of Contents: FINGERPRINT ATTACK METHODS

1) Direct Attacks: Fake Fingerprints
   - Example: Direct Attack with Cooperation
   - Example: Direct Attack without Cooperation

2) Brute Force indirect attacks
   - Example: Brute Force attack to the feature extractor input
   - Example: Brute Force attack to the matcher input

3) Hill-Climbing indirect attacks
   - Example: hill-climbing attack to the matcher input
   - Example: hill-climbing attack to the feature extractor input

4) Masquerade attacks
   - Example: masquerade attack to the feature extractor input
   - Example: masquerade attack to the sensor

Methodological Evaluation Challenges

CAFD supporting document: “Characterizing Attacks to Fingerprint Devices”

Biometric mechanisms are analysed basically isolated in CAFD:

- Focused on explaining the relevant biometric aspects related to the attack potential rate estimation.
- Final or absolute rates could be different depending on the TOE but guidance is provided in order to give evaluators a tool to make their own estimations based on examples.
- Real access control functions in TOEs usually will involve other mechanisms complementing the biometric ones.

Attack potential rates for fingerprint attacks included in CAFD are achieving ratings BASIC/MODERATE.

CCMC: proposal for a new subject area for “Biometrics” supporting documents

Technical Evaluation Challenges

Using standards in biometric devices: project examples

1) **EEUU**
   - PIV (Personal Identity Verification)
   - NPIVP (NIST Personal Identity Verification Program)
   - MINEX (Minutiae Interoperability Exchange Test)
   - SBMoC (Secure Biometric Match-on-Card)

2) **Europe**
   - VIS (Visa Information System)

3) **Spain**
   - DNIe (electronic National ID)

4) **International**
   - ILO Seafarers ID
   - The ICAO MRTD initiative: e-passport

Technical Evaluation Challenges

ISO and ANSI fingerprint minutiae data interchange standards

Field	ISO/IEC 19794-2	ANSI/NIST-ITL 1-2000
Data type	Binary	ASCII
Minutiae type	Ridge ending, ridge bifurcation, and points of interest	Ridge ending, ridge bifurcation, compound and undetermined
Minutiae placement	Ridge ending, ridge bifurcation, and other types	Not specified for this standard
Minutiae origin	Upper left corner	Lower left corner
Minutiae coordination system	Based on number of pixels per centimeter	Based upon unit of 0.01 millimeters in a Cartesian coordinate system located in Quadrant 1
Minutiae angle	Granularity of 1.4 degrees	Granularity of 1 degree

Technical Evaluation Challenges

Reverse Engineering: how to attack an ISO matcher

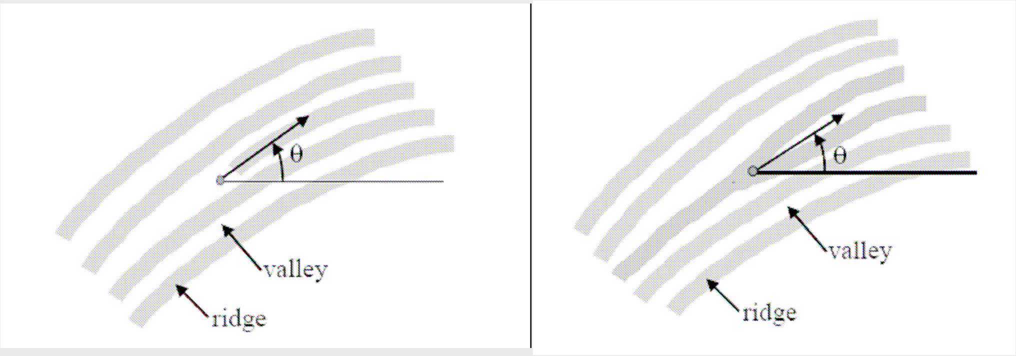
The ISO/IEC 19794-2 standard: minutiae-based

Two formats:

1) general storage and transport
2) compact for use in card-based systems

Minutiae encoding:

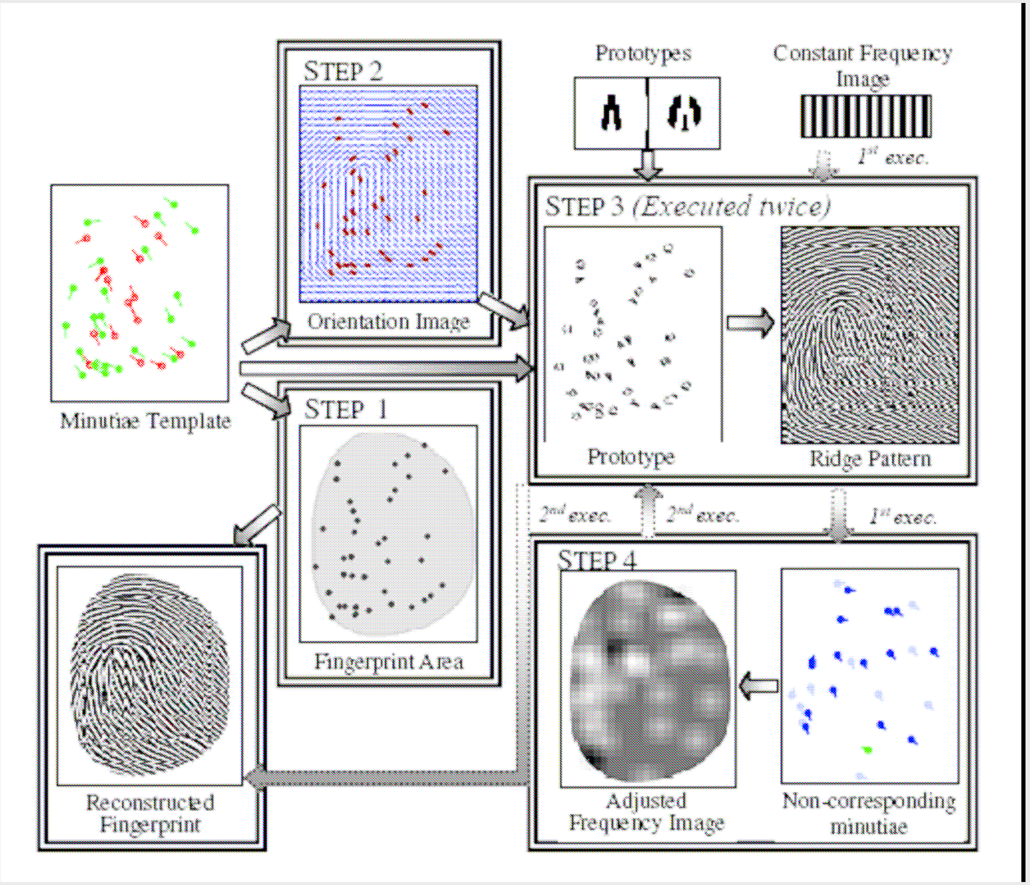
1) coordinate system
2) angle convention



Minutia placement on a ridge ending (left) and on a ridge bifurcation (right).

Technical Evaluation Challenges

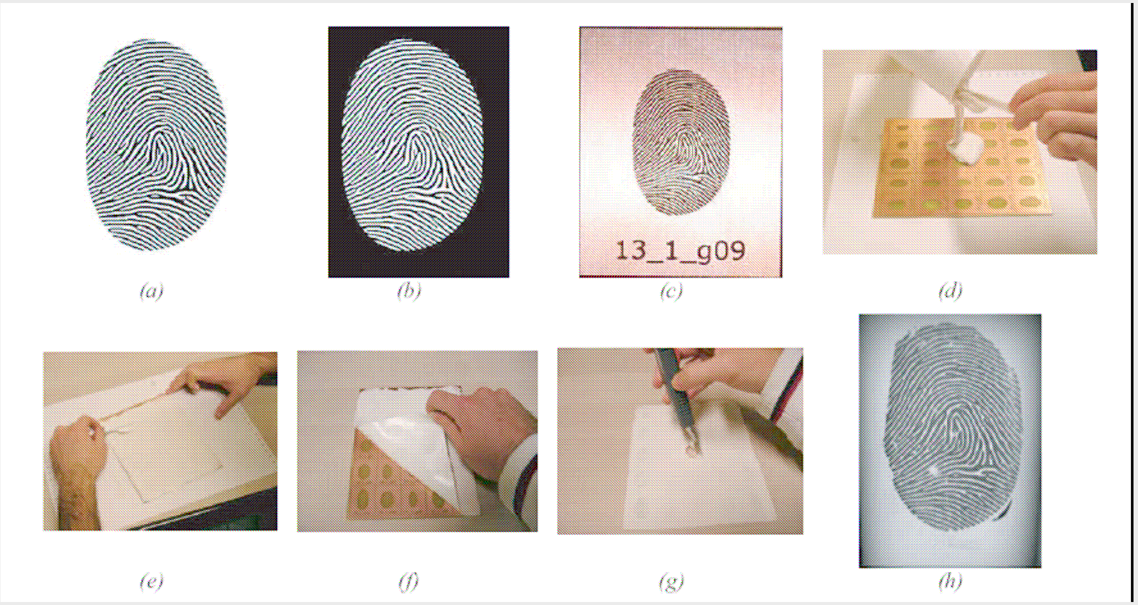
Reverse Engineering



Steps followed to reconstruct the fingerprint image from the ISO minutiae template

Technical Evaluation Challenges

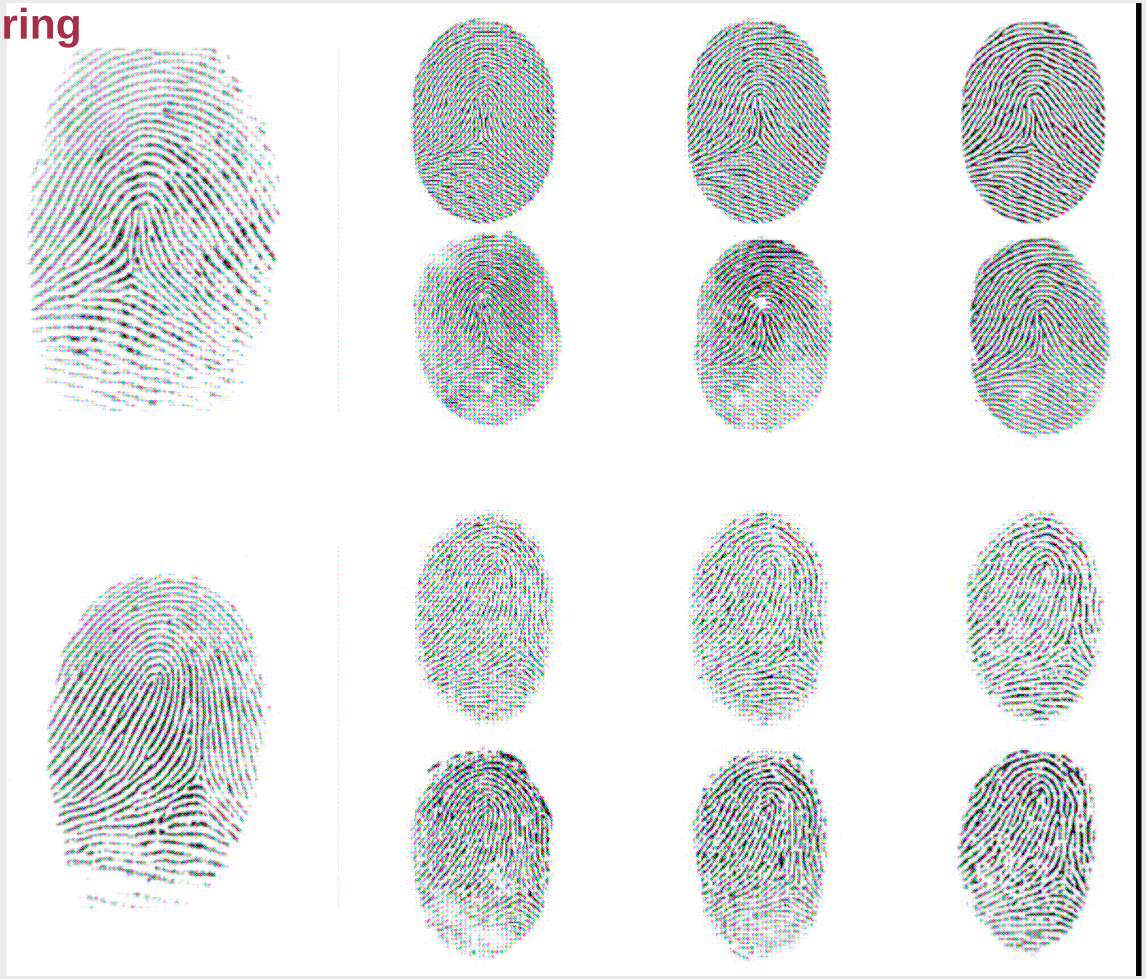
Reverse Engineering



Process followed to generate the fake fingerprint: reconstructed image (a), negative of the reconstructed image (b), fingerprint on the PCB (c), pour the silicone and catalyst mixture on the PCB (d), spread the mixture over the PCB (e), detach when it hardens (f), cut out each fake finger (g), final fake fingerprint acquired (h)

Technical Evaluation Challenges

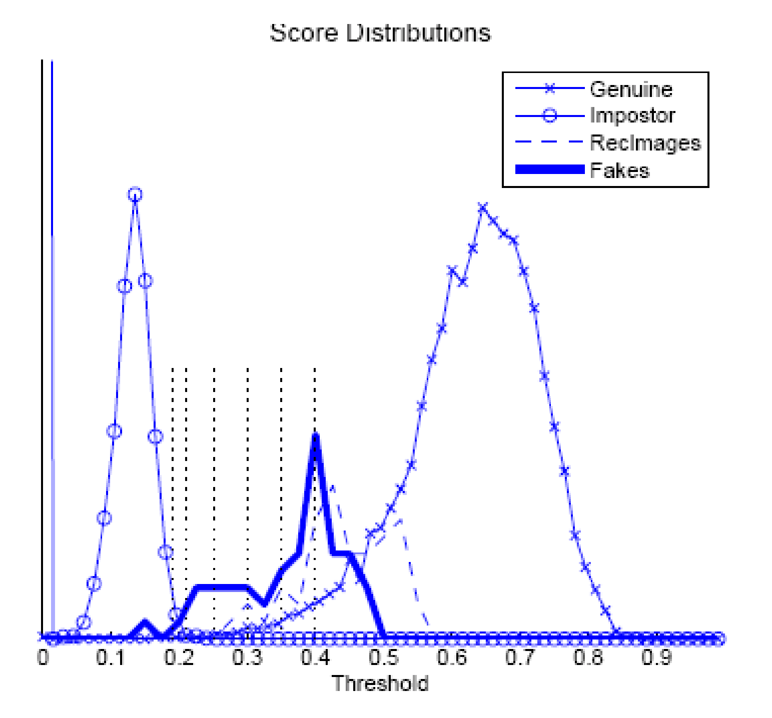
Reverse Engineering



Original fingerprints (left). Reconstructed images without noise (row 1) and with noise (row 3). The respective final fake fingerprints without noise (row 2), and with noise (row 4)

Technical Evaluation Challenges

Reverse Engineering



Matching score distributions and selected thresholds (dotted lines)

Technical Evaluation Challenges

MoC Fingerprint Devices (Match-on-Card) vs. ToC (Template-on-Card)

Spanish Scheme Example: Spanish National eID (“DNIe”)

Contents:

- Authentication certificate & keys
- E-Signature certificate & keys
- CA certificate
- Personal data of the citizen
- Face picture (image)
- Handwritten signature picture (image)
- Fingerprint template
- MoC application included in the smartcard O.S.

Biometric functions in DNIe

1. Update of the citizen’s certificates
2. PIN: Unlock / change
3. ID Applications

Technical Evaluation Challenges

Match-on-Card

→ ***Specific MoC Standards***

1) ISO/IEC 7816

2) ISO/IEC 19785-3: CBEFF patron formats

3) DIN V66400: Finger minutiae encoding format and parameters for on-card matching

→ ***Other Related Biometric Standards***

1) ISO/IEC 19794: Biometric Format Standards

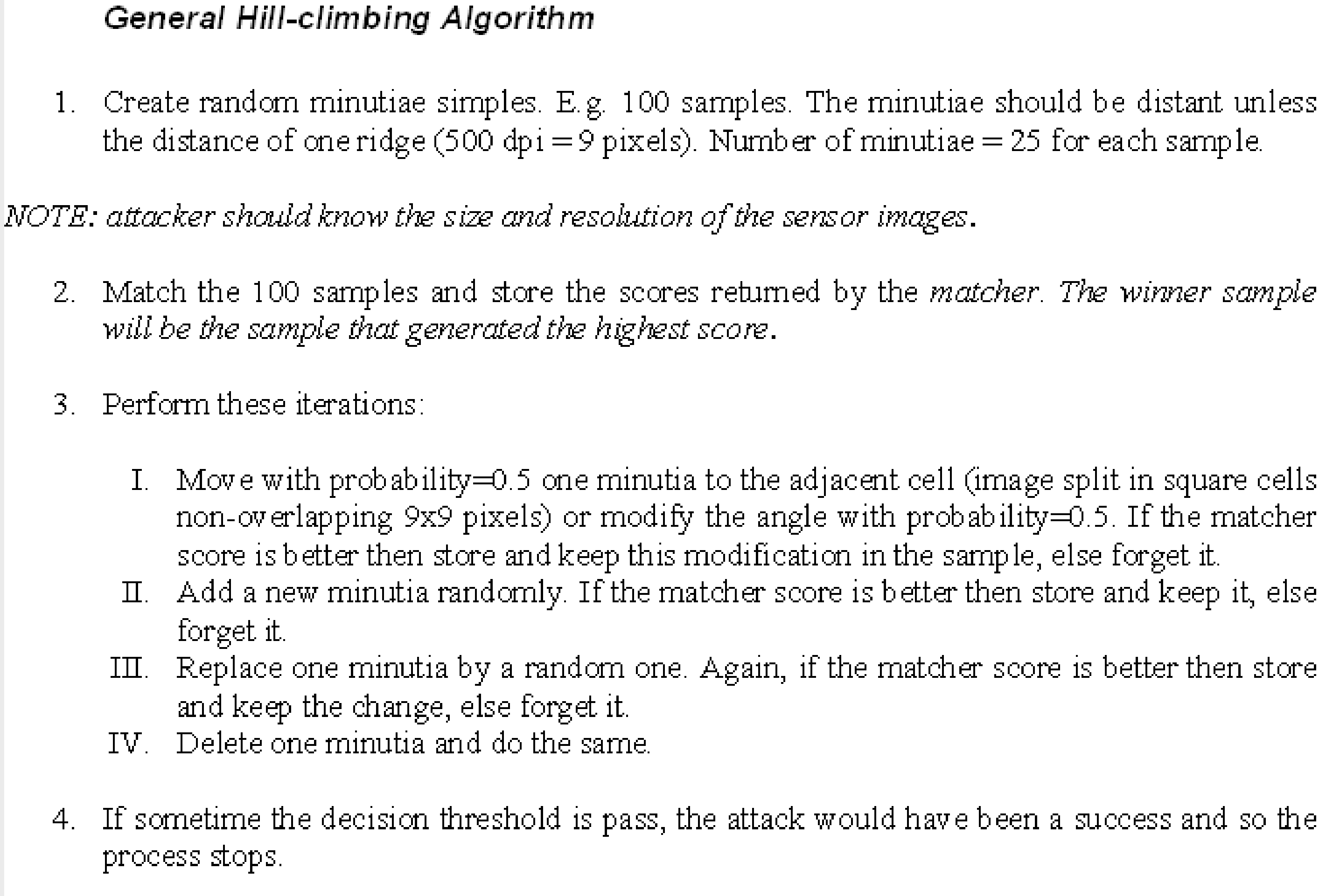
2) ANSI/NIST ITL 1-2007

Technical Evaluation Challenges

Match-on-Card: attacking directly to the matcher

Hill-climbing matching

→ Brute-force attack modified to use some kind of feedback provided by the device.



General Hill-climbing Algorithm

1. Create random minutiae simples. E.g. 100 samples. The minutiae should be distant unless the distance of one ridge (500 dpi = 9 pixels). Number of minutiae = 25 for each sample.

NOTE: attacker should know the size and resolution of the sensor images.

2. Match the 100 samples and store the scores returned by the *matcher*. *The winner sample will be the sample that generated the highest score.*

3. Perform these iterations:

   I. Move with probability=0.5 one minutia to the adjacent cell (image split in square cells non-overlapping 9x9 pixels) or modify the angle with probability=0.5. If the matcher score is better then store and keep this modification in the sample, else forget it.
   II. Add a new minutia randomly. If the matcher score is better then store and keep it, else forget it.
   III. Replace one minutia by a random one. Again, if the matcher score is better then store and keep the change, else forget it.
   IV. Delete one minutia and do the same.

4. If sometime the decision threshold is pass, the attack would have been a success and so the process stops.

Technical Evaluation Challenges

Match-on-Card: attacking directly to the matcher

Hill-climbing matching

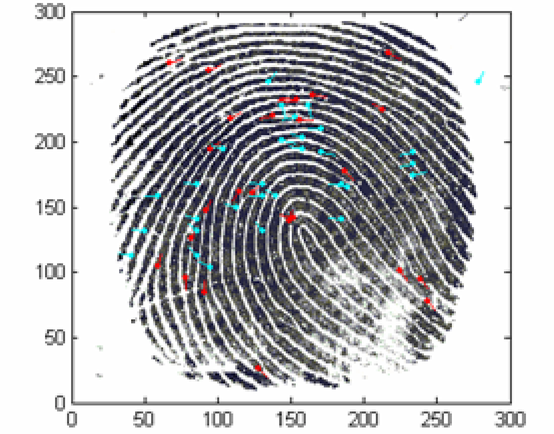


Fig. : Original fingerprint, original minutiae (red), and synthetic minutiae (blue)

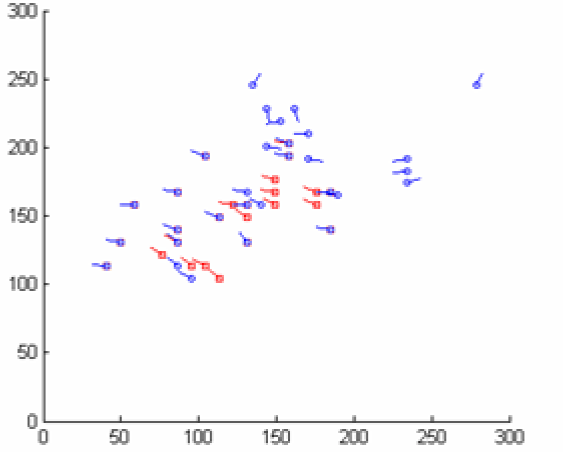


Fig. : Evolution of the minutiae pattern during hill-climbing

Future Challenges

- Hash methods for template storage formats in standards

- Matching algoritms in hash-spaces

- Cripto-Biometrics

- Multimodal devices

- Creation of fake fingerprints for
  - for new types of sensors (ultrasound, etc)
  - to avoid vitality checks

- Methods to “lift” fingerprints from latents

- Vulnerability Analysis focused in other attack points

- Automatic evaluation tools for brute-force attacks

- Methods to get alternative feedbacks from the matching algorithms: DPAs, etc.

Thank you by your attention

Questions?

**** Contact*:**

http://www.oc.ccn.cni.es

organismo.certificacion@cni.es

ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN