"LOOKING FOR A COMMON ATTACK METHODOLOGY FOCUSED ON FINGERPRINT AUTHENTICATION DEVICES“

Dr. Marino Tapiador
Technical Manager of the Certification Area

Spanish Certification Body
National Cryptologic Center

TABLE OF CONTENTS

Introduction

Nowadays the information security evaluation field demands common methodologies and, although a global framework has been agreed in relationship to the Common Evaluation Methodology (CEM), more detailed methods to evaluate the security of specific technologies are a clear necessity.

In the area of biometric security 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 generic methods that are only a general approach for the experts belonging to evaluation facilities that have to deal with this kind of technical testing procedures.

This paper presents a proposal for an attack methodology focused on fingerprint authentication devices. It is a detailed recipe for evaluators and it enables them to execute a step-by-step procedure to analyze a fingerprint verification system, devise penetration testing, execute the penetration test cases, and properly understand and document the results of these attacks.

State-of-the-art

Two different areas:

(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.**

State-of-the-art

These are some useful sources about performance evaluation:

- **J. Wayman, A. Jain, D. Maltoni, and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation***
- **R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. W. Senior, *Guide to biometrics***
- **H. Kang, B. Lee, H. Kim, D. Shin and J. Kim, "A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules,"**
- **BioAPI Specification, American National Standards Institute (ANSI)**
- **Best Practices in Testing and Reporting Performance of Biometric Devices, Tony Mansfield and Jim Wayman for the UK Biometrics Working Group**
- **Common Biometric Exchange File Format (CBEFF), National Institute of Standards and Technology (NIST)**

- http://fingerprint.nist.gov/NFIS/

State-of-the-art

These are some useful sources about <u>security</u> evaluation:

- **Common Methodology for Information Technology Security Evaluation – "Biometric Evaluation Methodology Supplement [BEM]". v1.0**

- **Biometric Technology Security Evaluation under the Common Criteria, Version 1.2, (CSE, Canada)**

- **UK Government Biometrics Working Group, "Biometric Device Protection Profile (BDPP)", Draft Issue 0.82, 2001**

- **BSI, "Common Criteria Protection Profile: Biometric Verification Mechanisms", BSI-PP-0016, v1.04. 2005**

- **US Information Assurance Directorate, "Biometric Verification Mode Protection Profile for Basic Robustness Environments", v1.0. 2006**

- **US Information Assurance Directorate, "Biometric Verification Mode Protection Profile for Medium Robustness Environments", v1.0. 2003**

- **EWA Ltd, "Security Target for BioscryptTM Inc. BioscryptTM Enterprise for NT Logon", v3.2 EWA-1360-013-350. 2001**

Link to CEM

1. Inter-version differential analysis

1) VLA versus VAN:

- AVA class v2.3: CCA, MSU, SOF, VLA

- AVA class v3.1: VAN

2) Developer Vulnerability Analysis ¿yes or no?

3) Attack Potential Tables changes:

- identification + exploitation

- attack potential levels

v2.3 → low, moderate, high

v3.1 → basic, enhanced-basic, moderate, high

- numerical values

Link to CEM

2. Intra-version differential analysis

Version 2.3: VLA.1 to VLA.4

VLA	EAL	Method	VA	Attack Potential
VLA.1	2,3	CEM	D	(*Obvious*)
VLA.2	4	CEM	D+E	Low
VLA.3	5	-	D+E	Moderate
VLA.4	6	BSI: AIS34	D+E	High

Version 3.1: VAN.1 to VAN.5

VAN	EAL	Method	VA	Sources	Search	Attack Potential
VAN.1	1	CEM	E	P	-	Basic
VAN.2	2,3	CEM	E	P+T	Search	Basic
VAN.3	4	CEM	E	P+T	Focused	Enhanced-basic
VAN.4	5	CEM	E	P+T	Methodical	Moderate
VAN.5	6,7	-	E	P+T	Advanced	High

Link to CEM

Vulnerability Analysis Workflow: VAW

Considering the results of inter-version and intra-version comparison, this methodology is been designed to :

- be uncoupled
- general enough to be technical guidance version 2.3 and 3.1
- possible to link to work units of VLA and VAN

The underlying idea is the Vulnerability Analysis of CEM has a general structure under the specific work units that compose VLA or VAN, and also some general parameters that can concrete this structure.

The general structure is been called in this method “Vulnerability Analysis Workflow” (VAW) and it can be connected or mapped to any sub-activity of VLA v2.3 or VAN v3.1 easily by the evaluator.

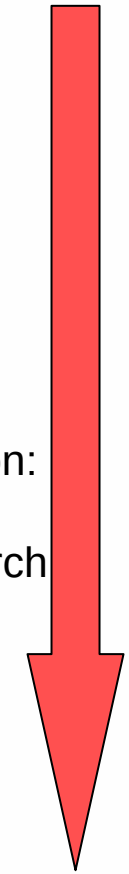
The VAW consist of the general phases described below and a set of general parameters.

Link to CEM

Vulnerability Analysis Workflow VAW : PHASES

Parameters:

- Developer VA: Yes, No
- Vulnerability Identification:
  - a) Source
  - b) Type of Search
- Attack Potential:



1. Preparation
2. Search of Potential Vulnerabilities
3. Devise Pen-Tests
4. Produce Procedures for Pen-Tests
5. Conduct Pen-Tests
6. Reporting Results
7. Close

Vulnerability Assessment

Class AVA: Vulnerability assessment

The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or weaknesses in the TOE in the operational environment. This determination is based upon analysis of the evaluation evidence and a search of publicly available material by the evaluator and is supported by evaluator penetration testing.

***Example*: Evaluation of Methodical Vulnerability Analysis (AVA_VAN.4)**

The objective of this sub-activity is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing Moderate attack potential.

A methodical vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Moderate.

Vulnerability Assessment

Inputs:

a) the ST;
b) the functional specification;
c) the TOE design;
d) the security architecture description;
e) the implementation representation;
f) the guidance documentation;
g) the TOE suitable for testing;

Work units for the Evaluation:

AVA_VAN.4-1 The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

AVA_VAN.4-2 The evaluator **shall examine** the TOE to determine that it has been installed properly and is in a known state

Vulnerability Assessment

AVA_VAN.4-3 The evaluator **shall examine** sources of information publicly available to identify potential vulnerabilities in the TOE.

As a *minimum* the evaluator should examine the following FRS specific vulnerability sources:

a) fingerprint specialist publications:

•VAW LINK: Phase 2 – Search of PV

- **"Securing Fingerprint Systems" in Handbook of Fingerprint Recognition.**
- **"Security considerations for the implementation of biometric systems" in Automatic fingerprint recognition systems.**
- **Guide to biometrics.**
- **Biometric Systems: Technology, Design and Performance Evaluation.**

Books

- **IEEE Transactions on Image Processing.**
- **IEEE Transactions on Pattern Analysis and Machine Intelligence.**
- **IEEE Transactions on Systems, Man and Cybernetics.**
- **Communications of the ACM.**
- **Journal of Forensic Sciences.**

Journals

Vulnerability Assessment

•VAW LINK: Phase 2 – Search of PV

b) research papers:

- "Impact of Artificial Gummy Fingers on Fingerprint Systems," T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino.
- “Attacks on Biometric Systems: A Case Study in Fingerprints,” U. Uludag, A.K. Jain.
- “Biometrical Fingerprint Recognition Don't Get Your Fingers Burned”, T. van der Putte, J. Keuning.
- “How to fake fingerprints?”.
- “Fake fingerprint detection by odor analysis”, D. Baldiserra, A. Franco, D. Maio, and D. Maltoni.
- “A new approach to fake finger detection based on skin distortion”, A. Antonelli, R. Capelli, D. Maio, and D. Maltoni.
- “Vulnerabilities in biometric encryption systems”, A. Adler.
- “Biometrics: yes or no?” , M. Kàkona.
- “Body Check: Biometric Access Protection Devices and their Programs Put to the Test”, L. Thalheim, J. Krissler, P. M. Ziegler.
- “A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules,” H. Kang, B. Lee, H. Kim, D. Shin and J. Kim.
- “Evaluation of biometric security systems against artificial fingers”, J. Blommè.
- “Attacking Fingerprint Sensors”, A. Wiehe, T. Sondrol, O. Kasper, F. Skarderud.

Vulnerability Assessment

b) research papers: *part II*

•VAW LINK: Phase 2 – Search of PV

- **“Biometric system security”, C. Soutar.**
- **“Risk of masquerade arising from the storage of Biometrics”, C. J. Hill.**
- **“Image quality and position variability assessment in minutiae-based fingerprint verification”, D. Simon-Zorita, J. Ortega-Garcia, J. Fierrez-Aguilar and J. Gonzalez-Rodriguez.**
- **"On the effects of image quality degradation on minutiae- and ridge-based automatic fingerprint recognition", J. Fierrez-Aguilar, L. M. Muñoz-Serrano, F. Alonso-Fernandez and J. Ortega-Garcia.**
- **"Incorporating image quality in multi-algorithm fingerprint verification", J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia and A. K. Jain.**
- **“An identity authentication system using fingerprints”, A.K. Jain, L. Hong, S. Pankanti, and R. Bolle.**
- **“Modelling Plastic Distortion in Fingerprint Images”, R. Cappelli, D. Maio and D. Maltoni.**
- **“An análisis of minutiae matching strength”, N. K. Ratha, J. H. Connell, and R. M. Bolle.**

Vulnerability Assessment

c) conference proceedings:

- **Proceedings of AVBPA, Audio and Video based Biometric Person Authentication.**
- **Proceedings of ICB, International Conference on Biometrics.**
- **Proceedings of ICBA, International Conference on Biometric Authentication.**
- **Proceedings of ICCST, IEEE International Carnahan Conference on Security Technology.**
- **Proceedings of IEEE Vision, Image and Signal Processing.**
- **Proceedings of SPIE.**
- **Proceedings of International Conference on Pattern Recognition.**
- **Proceedings of International Conference on Advances in Pattern Recognition.**
- **Proceedings of Conference on Science of Fingerprints.**

d) internet websites:

- **http://www.cesg.gov.uk/site/ast/biometrics**
- **http://www.biometrics.org**
- **http://fingerprint.nist.gov**
- **http://www.nist.gov**
- **http://www.engr.sjsu.edu/biometrics**
- **http://www.securityfocus.com**
- **http://www.biometrika.it**
- **http://www.bioapi.org**
- **http://www.cse-cst.gc.ca**
- **http://www.commoncriteria.org**

•VAW LINK: Phase 2 – Search of PV

Vulnerability Assessment

AVA_VAN.4-4 The evaluator shall conduct a methodical analysis of ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

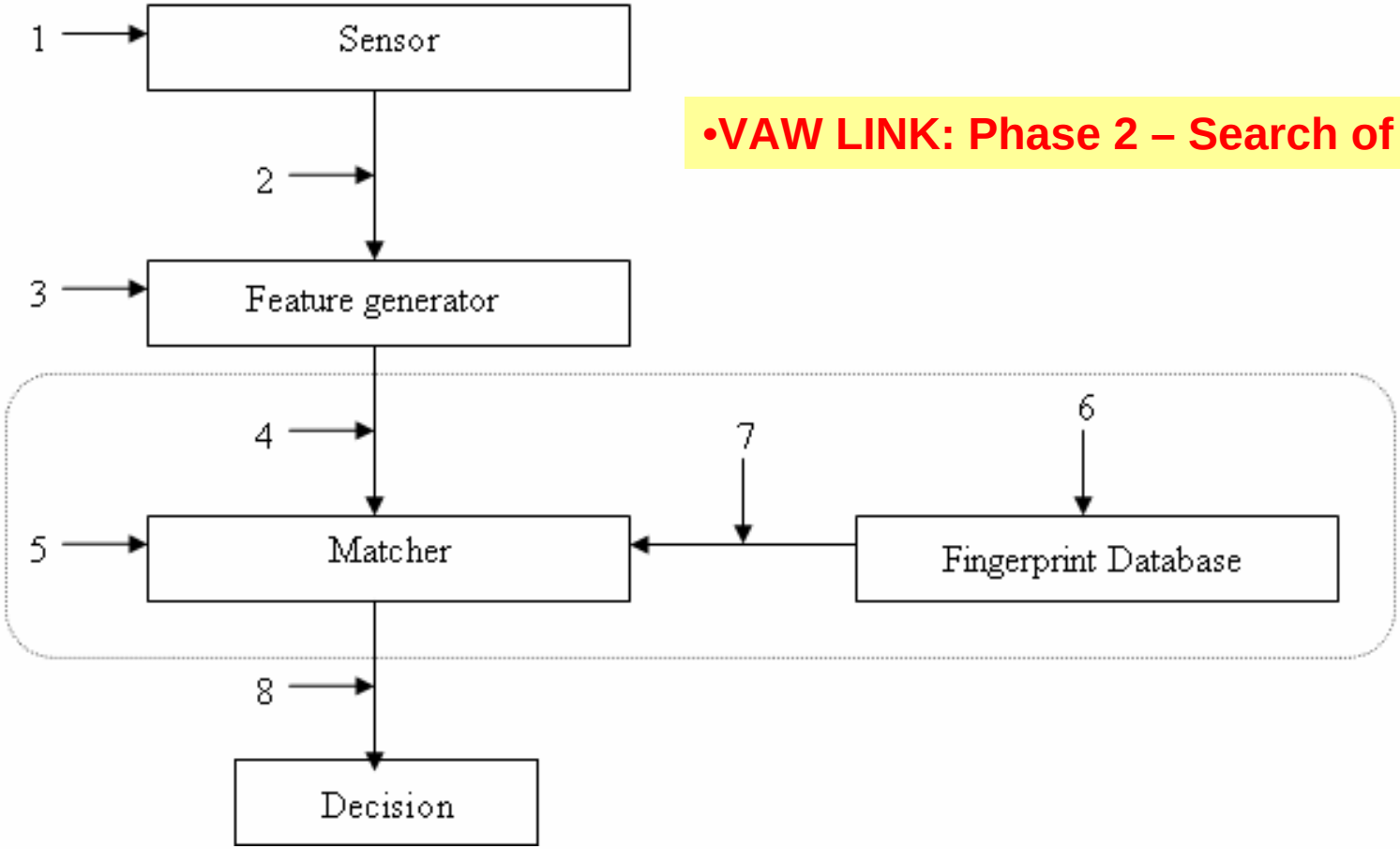
•VAW LINK: Phase 2 – Search of PV

Conducting the analysis of potential vulnerabilities with a FRS-type TOE, the evaluator should identify potential vulnerabilities using an approach based on a general security structure for the FRS as described by the logical model proposed by Ratha et al. In this approach the potential attack points can be located in these areas or attack point types:

1) Sensor.
2) Internal communication channel between the sensor and the feature generator.
3) Feature generator.
4) Internal communication channel between the feature generator and the matcher.
5) Matcher.
6) Fingerprint Database.
7) Internal communication channel between the database and the matcher.
8) Decision subsystem.

Vulnerability Assessment

Logical model for an FRS-type TOE with eight potential attack points.



- **VAW LINK: Phase 2 – Search of PV**

Vulnerability Assessment

AVA_VAN.4-5 The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.

AVA_VAN.4-6 The evaluator **shall devise** penetration tests, based on the independent search for potential vulnerabilities.

As a *minimum*, during the process of devising penetration test cases for a FRS-type TOE, the evaluator should devise penetration tests to conduct this type of attacks:

- **Type 1 attacks: focused on the sensor or scanner.**
- **Type 4 attacks: focused on the input to the matcher.**

•VAW LINK: Phase 3 – Devise Pen-Tests

Vulnerability Assessment

For type 1 attacks the evaluator should devise penetration test cases to perform direct attacks to the sensor using fake fingerprints.

For each fake fingerprint to make, the evaluator should create a negative fingerprint from a real sample or from a latent fingerprint.

For each negative fingerprint, the evaluator should create a positive fingerprint that will be used as the final fake fingerprint in penetration test cases.

If the TOE includes a thermal sensor, the evaluator should devise penetration tests with actions oriented to warm up the fake fingerprints using heat-resistant materials and some kind of heat source.

If the TOE includes a solid-state sensor, the evaluator should devise penetration tests with actions oriented to increase the conductivity of the fake fingerprints using some liquid or spray to be applied on the samples (water could be enough, the idea is to get a wet surface in the fake fingerprint).

The evaluator should create a fake fingerprint database. This database is to be used to compute the False Acceptance Rate (FAR) of the TOE using fake samples, in order to calculate the statistical probability of exploiting this type of vulnerabilities.

•VAW LINK: Phase 3 – Devise Pen-Tests

Appendix A: Procedure to Create Fake Fingerprints

Fig. : Epoxy putty for a mould

Fig. : Mixed Epoxy putty

Fig. : Spread it on a piece of paper

Fig. : Smooth down it with a latex globe

Fig. : Smooth green stuff

Fig. : Press with the genuine finger on the putty

Create 'Negative' fake fingerprint

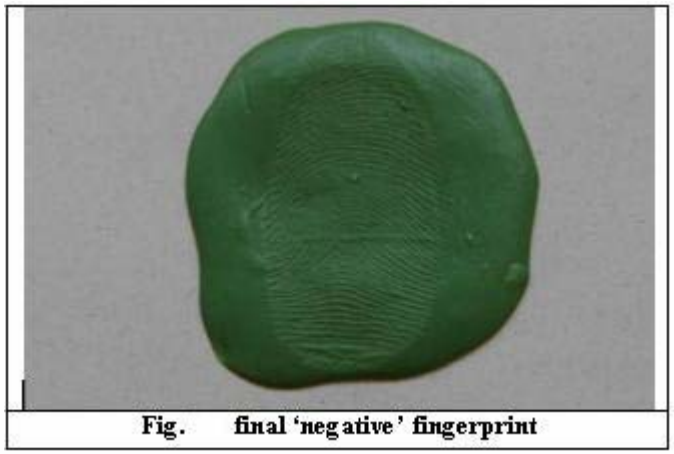


Fig. final 'negative' fingerprint

Appendix A: Procedure to Create Fake Fingerprints

Fig. : Move the silicone

Fig. : Drop down the silicone in the cup with the volume scale

Fig. : Get the right catalyst volume

Fig. : Combine silicone and catalyst

Fig. : Pour the combined substance over the green stuff

Fig. : Mould covered with the mix

Fig. : Unstick the solid silicone

Fig. : Negative and positive of the fingerprint

Fig. : Cut the positive fingerprint

Fig. : Final positive fingerprint

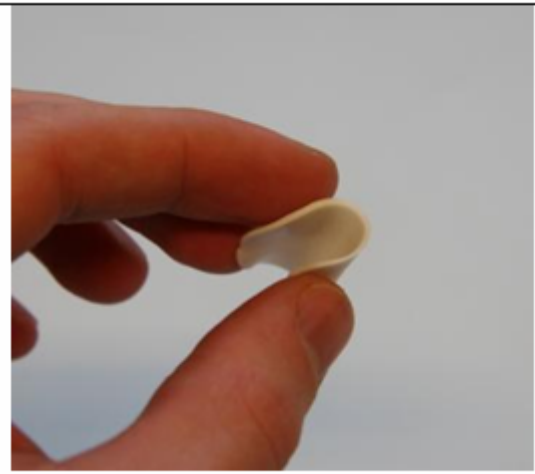


Fig. : Consistency of the positive fingerprint

Create 'Positive' fake fingerprint

Appendix B: Procedure to Create Fingerprint Databases

Generation of evaluation databases

In order to analyse the vulnerabilities of a FRS it is necessary a DB populated of a number high enough of real and fake fingerprints to derive conclusions.

The general characteristics required are:

- Statistically representative of the operational population of the FRS.
- Big enough to have inter-variability between samples of different users.
- Big enough to have intra-variability among samples of the same user.
- Same fingerprints from different times in order to fetch evolutions in the sample.
- Legal aspects:
  - •Biometric data are personal data protected by national laws and regulations.
  - •Volunteers providing simples have to be inform and aware of the procedure of acquiring their fingerprints and the final target use of them.
  - •Volunteers can select to be anonymous and this desire has to be respected.

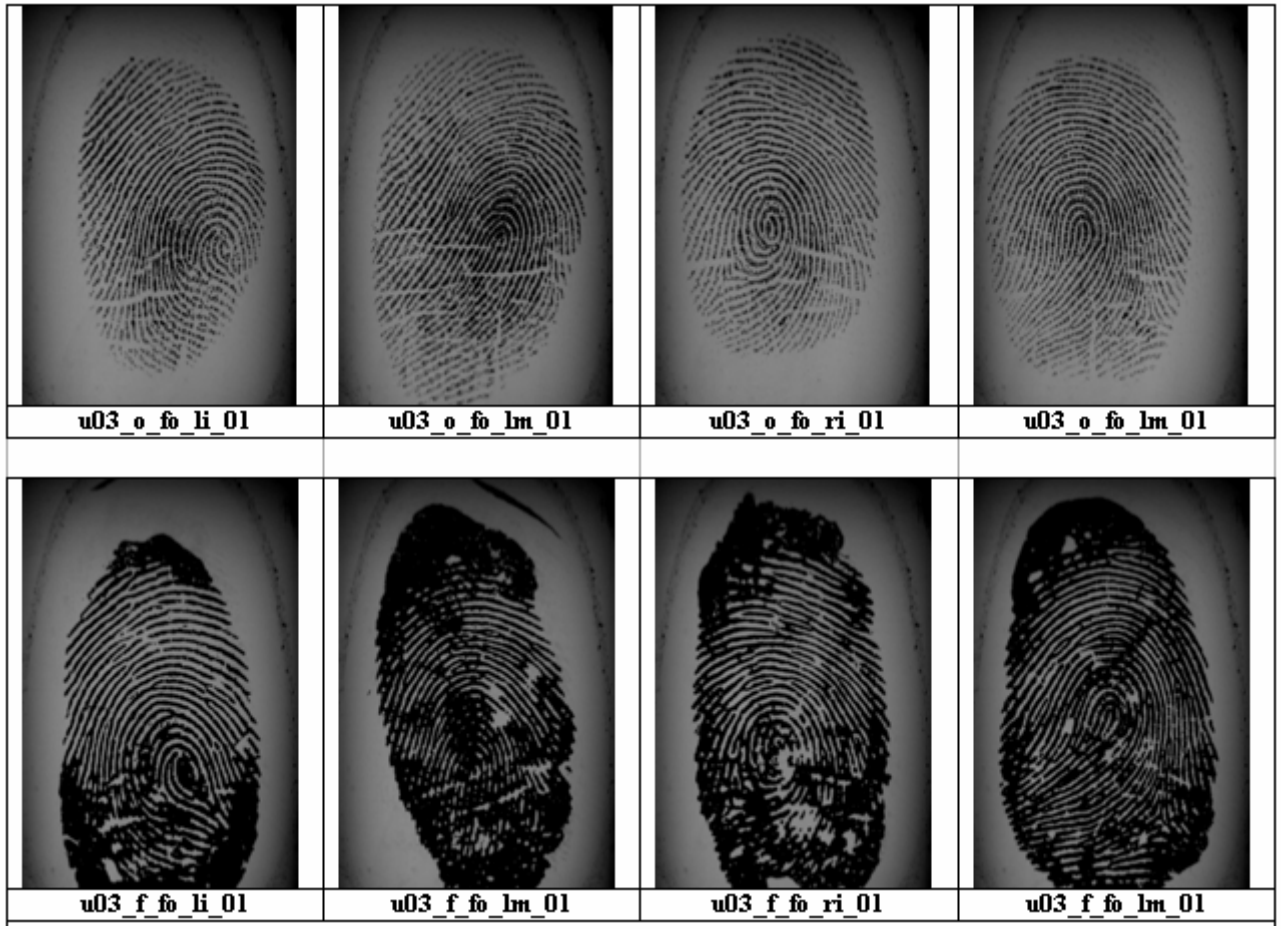
Example protocol to create a reference database

Appendix B: Procedure to Create Fingerprint Databases

E.g. Types of Sensors: optical, thermal sweep, solid-state

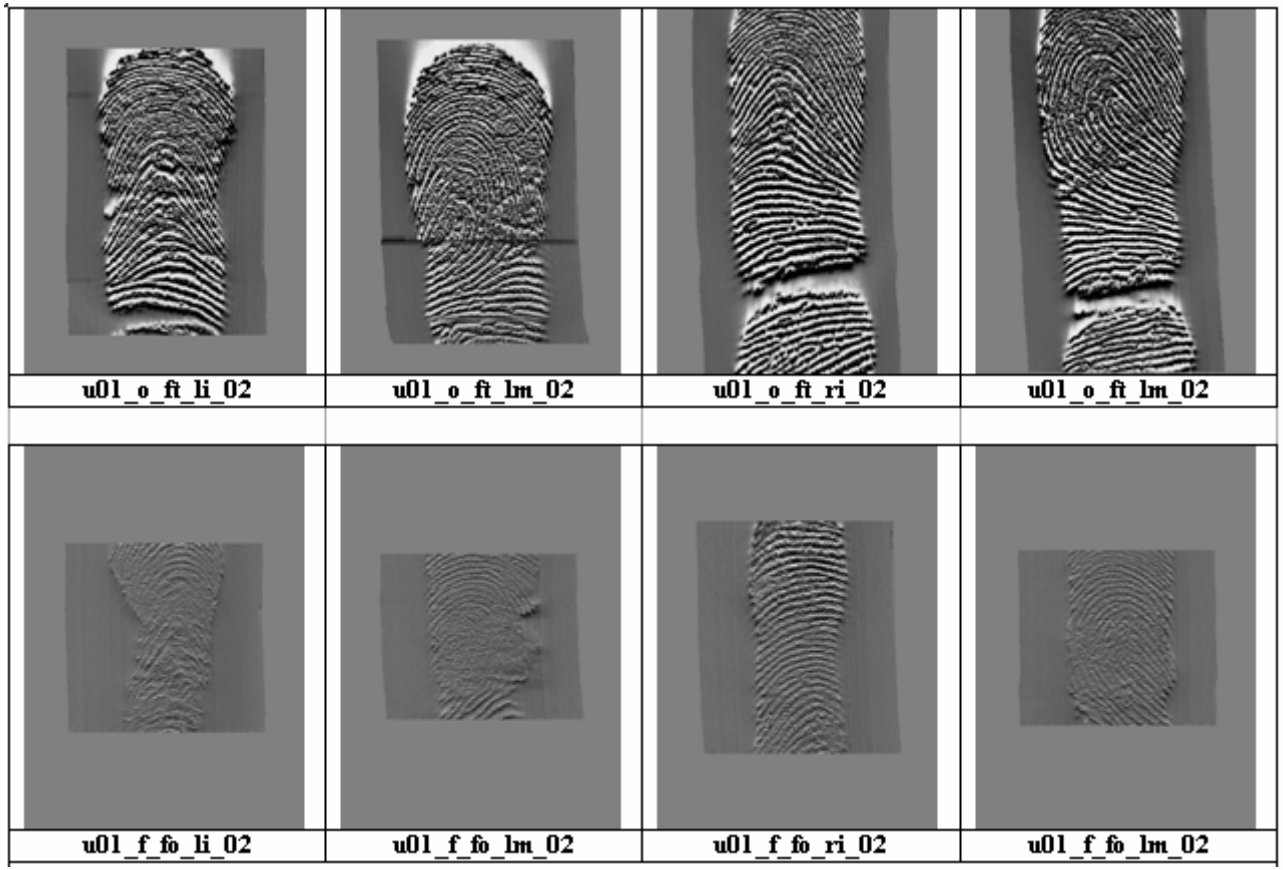
Appendix B: Procedure to Create Fingerprint Databases

E.g. Types of Sensors: optical, real and fake



Appendix B: Procedure to Create Fingerprint Databases

E.g. Types of Sensors: thermal sweep, real and fake



Appendix B: Procedure to Create Fingerprint Databases

E.g. Types of Sensors: solid-state, with and w/o spray

Fig. : Original fingerprint

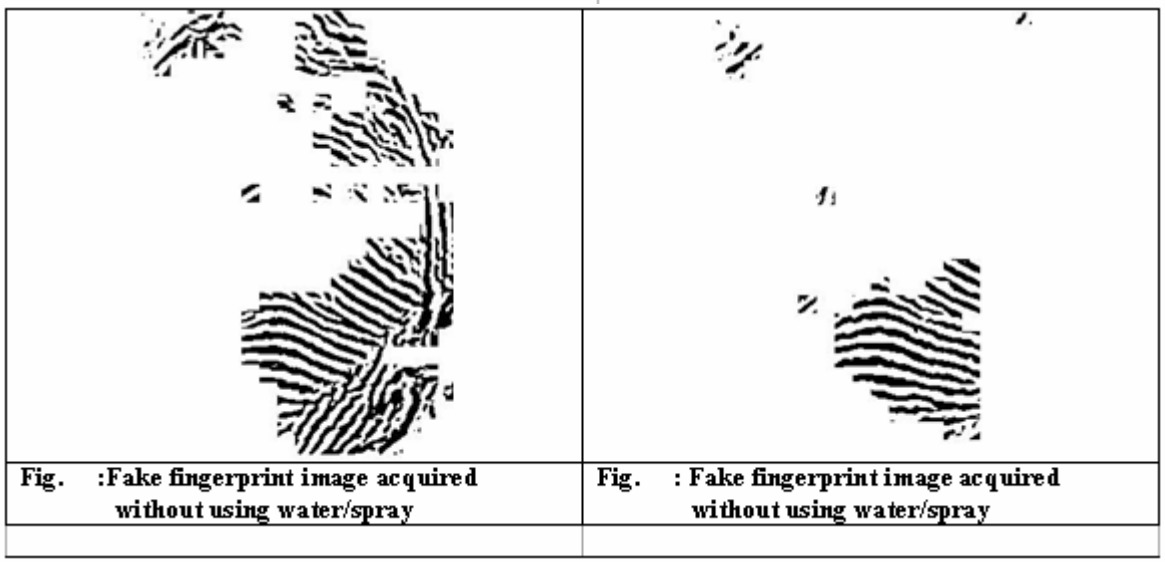


Fig. :Fake fingerprint image acquired without using water/spray

Fig. : Fake fingerprint image acquired without using water/spray

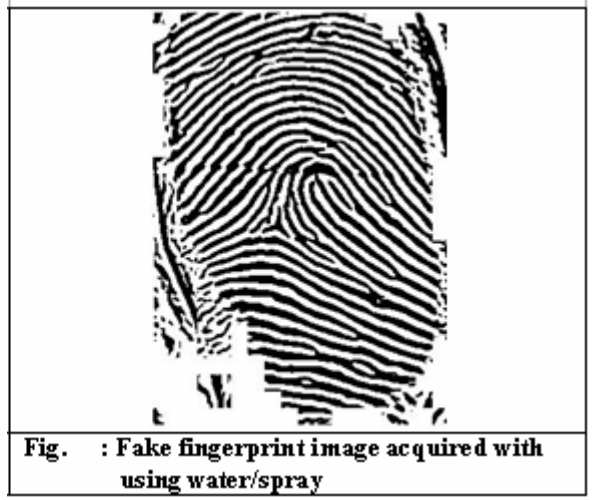


Fig. : Fake fingerprint image acquired with using water/spray

Vulnerability Assessment

For type 4 attacks the evaluator should devise penetration test cases to perform attacks through the input to the matcher using automatic tools to test fingerprint databases against the matcher.

As a *minimum*, during the process of devising penetration test cases for the FRS matcher, the evaluator should devise penetration tests to conduct attacks using:

- ***Brute-force matching***.
- ***Hill-climbing matching.***

•VAW LINK: Phase 3 – Devise Pen-Tests

Vulnerability Assessment

For ***brute-force*** attacks the evaluator should devise penetration test cases to execute matching using a real fingerprint database. This database should be focused on covering aspects that could modify the estimated FAR of the TOE:

- Huge databases.
- Databases from different sources.
- Fingerprint samples from different ethnics, age zones, gender, etc.
- Different image quality levels.

•VAW LINK: Phase 3 – Devise Pen-Tests

For ***hill-climbing*** attacks the evaluator should devise penetration test cases to execute matching using a real fingerprint database and using some procedure to get some level of feed-back about the success of individual matches. Matcher feed-back can be obtained by:

Directly using the matching response when it is a score i.e. when it includes some rate of the confidence or similarity level between the two fingerprint samples compared.

Using time consumption information that could be derived during unsuccessful comparisons.

Using power consumption analysis of the electronic component of the TOE that could be related to the operations involved in the comparison process during the matching.

Appendix C: Procedure to Execute Brute-force Matching

Brute-force matching consist of executing huge volumes of matches, in order to do this during the evaluation of a FRS TOE the evaluator needs to know how to use an automatic tool designed to do this task.

The main objective of this kind of tool is going to be to compute the FAR and FRR (False Acceptance Rate and False Rejection Rate).

The *National Institute of Standards and Technology* (NIST), in EE.UU., provides a freeware that can be downloaded by the Internet.

This software is world-wide well known and used by biometric evaluators, and is called NIST *Fingerprint Image Software 2* (NFIS2).

This tool in combination with MATHLAB is a powerful help to perform automatic fingerprint testing.

The detailed information and instructions of this software can be found in the manual called *User's guide to Fingerprint Image Software 2 – NFIS2* that also can be downloaded for free in the Internet.

Appendix D: Procedure to Execute Hill-climbing Matching

Hill-climbing matching

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

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.

Appendix D: Procedure to Execute Hill-climbing Matching

Hill-climbing matching

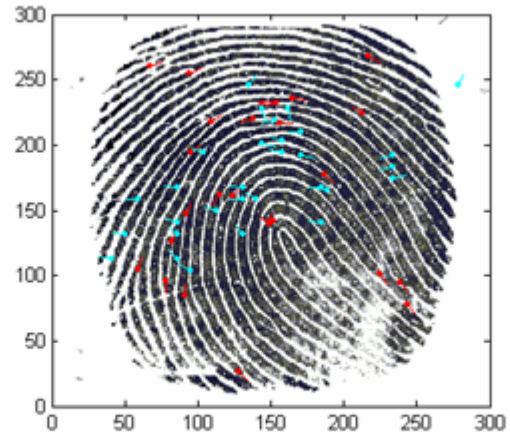


Fig. : Original fingerprint, original minutiae (red), and synthetic minutiae (blue)

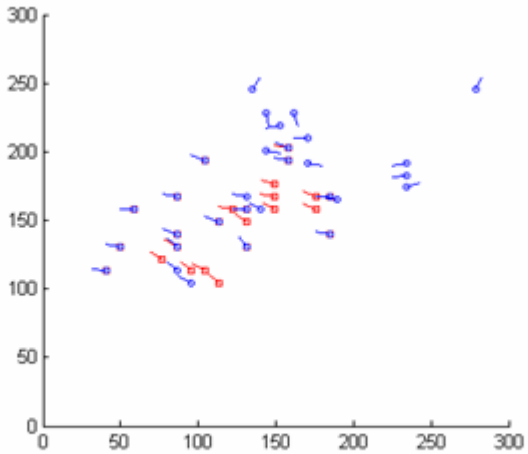


Fig. : Evolution of the minutiae pattern during hill-climbing

Vulnerability Assessment

AVA_VAN.4-7 The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable.

AVA_VAN.4-8 The evaluator **shall conduct** penetration testing.

AVA_VAN.4-9 The evaluator **shall record** the actual results of the penetration tests.

AVA_VAN.4-10 The evaluator **shall report** in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

AVA_VAN.4-11 The evaluator **shall examine** the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a Moderate attack potential.

AVA_VAN.4-12 The evaluator **shall report** in the ETR all exploitable vulnerabilities and residual vulnerabilities

Vulnerability Assessment

NEXT FUTURE

- Creation of fake fingerprints with
    - other types of sensors: ultrasound, etc.
    - to avoid vitality checks

- Methods to “lift” fingerprints from latents

- Vulnerability Analysis focused in other attack points

- Other automatic tools for brute-force attacks

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

Questions welcomed

organismo.certificacion@cni.es