EVALUATION METHODOLOGY FOR FAKE SAMPLES DETECTION IN BIOMETRICS

Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Raul Alonso-Moreno
University Carlos III of Madrid – Dpt. Electronics Technology
University Group for Identification Technologies (GUTI)
Avda. Universidad, 30
E-28911 – Leganes (Madrid)
SPAIN
{mbfernan, rsreillo, ramoreno}@ing.uc3m.es

Carmen Sanchez-Avila
Polytechnic University of Madrid
E.T.S.I. Telecomunicacion
Ciudad Universitaria, s/n
E-28040 – Madrid
SPAIN
csa@mat.upm.es

Abstract – Nowadays biometrics is being used in many applications where security is required. This fact causes that new threatens have appeared and that the number of attempts to break biometric systems has increased. From all potential attacks, those involving damage or thefts to users are the most worrying. Most of them could be avoided if acquisition sensors would have suitable approaches for aliveness detection at the capture process. Many providers claim that their products support these methods but unfortunately it has been discovered that some products do not detect fake samples. In this paper a methodology based on Common Criteria is given to evaluate, in an independent way, whether biometric capture devices implement methods for fake samples detection, and till which extent such methods are effective. This methodology has been tested with sensors from different modalities.

Index Terms — Biometrics, Aliveness Detection, Fake Samples, Evaluation Methodology

I. INTRODUCTION

Currently the use of Biometrics is increasing as a method to provide security at the identification stage in applications. Following this raise in popularity, new threats have appeared. One of the most important is the use of fake samples to overcome the identity verification step. These fake samples can be obtained from genuine users by different means. One of them is to make an artificial sample similar to a personal characteristic taking the latent information from a previous presentation. Another way is taking by force a real but not life sample. This last alternative is the reason why many people are worried about their personal safety. In order to avoid users to be injured and/or security applications to be overcome, biometric systems must provide mechanisms for aliveness detection.

There have been few works related to aliveness detection. One of the most popular is the work published by L. Thalheim, J. Krissler and P. Ziegler [1]. This study tested eleven biometric products, analyzing their ability to resist potential attacks. Products analyzed were from different modalities: nine products for fingerprint, one for face and one for iris. They tested the use of fake samples or the reactivation of latent images. Other well known experiments are the ones carried out by T. Matsumoto [2] [3], related to "gummy" fingers and iris samples. A. Pacut and A.Czajka [4] have also worked with iris forgeries. Matsumoto proved that commercial fingerprint systems implemented means to reject artificial fingers, but when the technology for building that fingers was changed, and “gummy” fingers are built, then they were not able to detect the lack of aliveness. In addition, both Matsumoto and A. Pacut and A.Czajka made forgery iris using different printers and resolutions to present the samples at different cameras. All of these works disclose that aliveness detection is not enforced in may biometric systems, dealing to the fact that many sensors and algorithms are not able to reject artificial or false samples.

In all these studies, simple suitable methods for each modality were applied to test each sensor. Neither of them followed an evaluation methodology. Each author implements his own approach to demonstrate how biometric sensors are not able to deny fake samples.

In this work, a generic methodology for aliveness detection testing will be shown. Such methodology is based on CEM (*Common Criteria Evaluation Methodology*), and will be used for testing the security level achieved by Biometric Systems.

Next section introduces CEM methodology to analyse vulnerabilities and Section III describes how to adapt such methodology to biometric products. The remaining parts explain the complete procedure applied to sensors from different modalities. Finally, evaluation results and conclusions will be presented.

II. CEM METHODOLOGY

CC (*Common Criteria*) [5] establishes a common base to evaluate security properties of IT products. This multi-part standard is composed by a set of functional and assurance requirements and specific methods to evaluate them. Such methods are detailed at CEM [6]. An evaluation based on CC consists on testing that a certain TOE (*Target of Evaluation*) meets all functional and assurance requirements defined in a ST (*Security Target*), following CEM specific procedures.

One of the most important assurance requirements is the analysis of vulnerabilities (class AVA_VAN). This requirement is included in all evaluations regardless of the EAL (*Evaluation Assurance Level*) chosen for them. Only some details regarding effort, rigour and depth will change depending on the EAL chosen. For an enhanced-basic potential attack (EAL4), the methodology specified at CEM request the following Inputs to be obtained before evaluation:

978-1-4244-1817-6/08/$25.00 ©2008 IEEE

- The ST
- Documentation related to the TOE (design, guidance documentation, functional specification, etc.)
- The TOE suitable for testing
- Information publicly available to support the identification of possible potential vulnerabilities.

Then, the evaluation can take place, by the execution of the following Actions:

1) *TOE configuration and test environment*
   Previously to real evaluation, test equipment, environment and device configuration, has to be defined according to the evaluation specification defined in the ST. In addition, TOE shall be installed and its current state known.
2) *Examine the TOE and sources of information*
   In CEM methodology this part is based on a search of vulnerabilities following a methodical analysis. Based on papers, public documentation, proceedings, conferences and/or other documentation used in the evaluation, TOE design and its implementation are studied in order to find potential vulnerabilities. Once all vulnerabilities have been identified, evaluator has to select which ones could be exploitable considering the ST, operational environment and potential attacks. The rest of them are declared as residual vulnerabilities and it will be not evaluated.
3) *Define penetration test*
   Afterwards evaluator has to define a series of test cases for all exploitable vulnerabilities. From such cases, evaluators should determinate the susceptibility of TOE to each applicable vulnerability. Enough documentation containing any considerations, have to be developed in sufficient detail to guarantee repeatability.
4) *Perform penetration tests and record test results*
   Evaluator has to carry out all penetration tests declared following the approaches previously defined and save all results obtained during the evaluation.
5) *Report results*
   At the end of the evaluation activity, evaluators have to document all steps, considerations and results of each penetration test. These reports have to include the verdict of TOE resistance to the type of attacks considered in the analysis of vulnerabilities.

III. EVALUATION METHODOLOGY FOR BIOMETRIC SYSTEMS

As any other IT product, biometric systems can be evaluated following CC. However, due to special features of them, it is necessary to consider particular details when biometrics products are going to be analysed. In order to evaluate this kind of products according to the analysis of vulnerabilities previously mentioned, authors suggest the next procedure. This procedure will be defined generically for all biometric modalities.

Consider the following specific inputs:

- Biometric system and its respective acquisition device
- Biometric system guidance documentation
- Documentation publicly available of any potential vulnerability
- A set of users
- Material to create forgeries
- Measurement instruments

Then perform the following actions:

1) *Define evaluation objectives and TOE characteristics*
   In CC this is already included at ST and/or TOE documentation before vulnerabilities analysis is done. For this evaluation we have not such documents so it has to be specified in detail at the very first moment. Hence, objectives, assumptions and operational environment have to be defined before evaluation. Furthermore a generic study of the acquisition device has to be carried out. Such study has to include at least: sensor modality, type of data captured (image, audio stream, raw data, etc), main sensor features and how it operates. It has to be identified which sensor parameters are used to capture and recognize such sample like one belonging to the modality under study. In addition at the first step of evaluation, measure instruments have to be calibrated, TOE has to be installed and configured in operational environment and also necessary users and materials have to be prepared. A simple trial of enrolment and verification process must be done to assure biometric system works correctly.
2) *Search and identify potential vulnerabilities*
   Knowing all data mentioned above, a list of potential vulnerabilities has to be done. After that, all exploitable vulnerabilities have to be identified. In addition those non-exploitable and residual vulnerabilities have to be properly justified.
3) *Design penetration test*
   In accordance with exploitable vulnerabilities identified at previous phase, penetration tests have to be described. These tests have to include the entire procedure to perform them and it has to be repeatable. Such tests have to describe its purpose and vulnerability under test, attack mode and how to create fake samples. These have to cover all phases (enrolment and verification), specifying how to present sample to sensor, defining results to be saved and any relevant aspect related to the particular modality under study.
4) *Carry out penetration tests*
   Penetration tests previously described have to be performed. All tests have to be carried out although one test can disclose possible results of others. This is because we never know the resources of an attacker and/or how he/she works. It is possible that it is easier for him/her to execute a complex attack instead a simple one. For the same reason, the execution order of these tests is not relevant. At this part of the evaluation, all results specified for each test have to be saved. Also, unexpected results have to be recorded in order to analyse its cause at the next phase..
5) *Generate reports*
   From all data obtained during evaluation, reports have to be generated where proofs and results are presented. Such reports should include at least:
   1) *A description of the tested biometric system*: modality, type of comparison system (verification or identification), a brief description of capture sensor and how it works.
   2) *For each penetration test*:
      a) Vulnerability to be analyzed and the purpose of the test.

b) Type of fake samples, its special features and how each sample was generated.

c) Number of users that have taken part at the test, how many behave as genuine users and how many as impostors.

d) Results in each phase.

IV. EVALUATION OBJECTIVES AND TOE CHARACTERISTICS

In this paper, authors analyse if biometric acquisition sensors have implemented valid methods to detect fake samples. Some commercial devices of two biometric modalities are being evaluated: one vascular system and three fingerprint based sensors. This global objective involves all remarks explained below.

A. Objectives

TABLE I
OBJECTIVES OF EVALUATION

O.ALIVENESS_ DETECTION	The main objective is analysing if biometric systems have implemented aliveness detection methods and can reject fake samples (e.g. synthetic, dead, latent or imitation samples).
O.SENSOR	Only attacks launched directly against the biometric sensor are going to be evaluated in order to test if sensor and/or biometric system have implemented aliveness detection.

B. Assumptions

TABLE II
ASSUMPTIONS OF EVALUATION

A.USER	User is not hostile.
A.ADMIN	Administrator is not hostile.
A.QUALITY	We consider that sample quality is analysed directly by the sensor or in a later process but quality is not going to be covered in this evaluation. If a fake sample is rejected by quality, result will be as if the sensor has counteracted this vulnerability either by means of quality or aliveness detection methods.
A.VERIFICATION	In order to simplify the evaluation, only biometric system in verification mode will be analysed.
A.ATTACK	For vulnerability analysis, authors have considered an enhanced-basic attack potential.

C. Others considerations

Operational environment for the evaluation presented in this paper is standard laboratory conditions, both in temperature and humidity. Ambient illumination is fluorescent light.

D. TOE characteristics

Biometric sensors and target modalities are detailed in Table III. Only technical and relevant features are mentioned. Companies and sensor trade names will not be disclosed in order to keep its confidentiality.

TABLE III
TOE CHARACTERISTICS

VASCULAR PATTERN	
S.VASCULAR	This sensor is based on near-infrared light to capture the vein pattern image. The deoxidized hemoglobin in the blood palm veins absorbs this kind of light and forms a unique pattern for each user. It works in a non-invasive way because sensor takes the image at low distances.
FINGERPRINT	
S.FINGERP_A	It is an optical high resolution sensor (> 500 dpi) with a large sensing area (> 400 mm^2). Optical sensor use visible light to illuminate the surface of finger and get a digital photography. User just has to touch sensible area. This kind of sensor is very susceptible to dirt, skin type or humidity.
S.FINGERP_B	It is a silicon sensor with a resolution of 500 dpi and a sensible area of 230 mm^2. This sensor uses capacitance to get fingerprint image. As S.FINGERP_A, user just has to touch sensible area and its operation could change with dirt, humidity and damaged skins.
S.FINGERP_C	It is a swipe fingerprint sensor with an image resolution of 500 dpi. Sensor array is of 192 column x 8 row and its acquisition rate is more than 3,700 frames per second. As the previous sensor, It works based on the capacitance principle too, but its use it is completely different. Users have to slide his/her finger over the sensible area at a certain speed.

V. POTENTIAL THREATS AND VULNERABILITIES

Several threats could affect the entire biometric systems and decrease its security. Considering only attacks directed against the capture device (O.SENSOR) and analysing papers, proceedings and public documentation (e.g. [2], [7] and [8]), the threats found are the ones stated in Table IV.

TABLE IV
POTENTIAL THREATS

AUTHORIZED USER	
T.UNKNOWNGLY	Biometric sample is stolen from user without his/her knowledge.
T.WILLINGLY	User presents voluntarily his/her own biometric reference.
T.UNWILLINGLY	User is forced to present his/her biometric reference.

T.DEAD	Biometric sample is obtained by mean of killing user or amputating his/her biometric reference.
T.MODIFY	Modify his/her own sample during enrolment in order to facilitate an impostor attack.
IMPOSTOR	
T.OWN_SAMPLE	Presenting his/her own sample in a zero-effort attempt.
T.IMP_MODIFY	Modifying his/her own sample.
T.CLONE	Using a clone (e.g. twins).
T.FAKE	Presenting a fake sample.
T.LATENT	Reactivating a latent sample.
T.REPLAY	Replay attacks.
T.ENVIRONMENT	Modifying environment conditions
T.HILL_CLIMBING	Hill-climbing attack

Compared to previous attacks the system presents the following vulnerabilities or weaknesses:

TABLE V
VULNERABILITIES

V.SYNTHETIC	If biometric system is unable to detect fake samples (e.g. latex hands, gummy fingers)
V.DEAD	Unable to detect dead or amputated samples.
V.RESIDUAL	Unable to detect residual or latent samples.
V.IMITATION	Unable to detect forgeries (e.g. photographics or videos).
V.QUALITY	Unable to detect low quality samples and/or degraded samples.
V.MULT_CAPTURE	Allowing many consecutive acquisitions or without a limited the number of attempts per user.
V.USER_THREATEN	Unable to detect a threaten user or not.
V.USER_HOSTILE	If user is hostile.
V.ADMIN_HOSTILE	If administrator is hostile.
V.OUTPUT	If biometric system shows scores or other kind of results from some information could be obtained.
V.FAR	If the false acceptance rate of the biometric system allows impostors to access.

There is a relationship between attacks and vulnerabilities. This is shown in Table VI:

TABLE VI
CROSS-TABLE BETWEEN ATTACKS AND VULNERABILITIES

CORRESPONDENCE BETWEEN ATTACKS AND VULNERABILITIES	V.DEAD	V.SYNTHETIC	V.RESIDUAL	V.IMITATION	V.QUALITY	V.MULT_CAPTURE	V.USER_THREATEN	V.USER_HOSTILE	V.ADMIN_HOSTILE	V.OUTPUT	V.FAR
T.UNKNOWNGLY		X	X	X							
T.WILLINGLY								X			
T.UNWILLINGLY							X				
T.DEAD	X										
T.MODIFY								X	X		
T.OWN_SAMPLE					X						X
T.IMP_MODIFY					X						X
T.CLON					X						X
T.FAKE		X		X							
T.LATENT			X								
T.REPLAY						X					X
T.ENVIRONMENT					X						X
T.HILL_CLIMBING					X					X	X

Assuming that users and administrator are not hostile (A.USER and A.ADMIN), all attacks mentioned above have to be counteracted by the overall biometric system.

Removing vulnerabilities related with performance (V.FAR), quality (V.QUALITY) and results (V.OUTPUT), the rest of them could be avoided if acquisition sensors have the capability to detect fake samples.

Considering the objectives and assumptions defined at the beginning of the evaluation, a classification of vulnerabilities is presented in Tables VII, VIII and IX.

TABLE VII
EXPLOITABLE VULNERABILITIES

V.SYNTHETIC	These three vulnerabilities are included as exploitable vulnerabilities because all of them meet with the objectives O.ALIVENESS_DETECTION and O.SENSOR.
V.DEAD	
V.IMITATION	
V.LATENT (Fingerprint)	This vulnerability satisfies the objectives of the evaluation but only for fingerprint modality where the biometric reference can laid down on the sensor.

TABLE VIII
NOT EXPLOITABLE VULNERABILITIES

V.USER_THREATEN	Sensor and algorithms may have implemented methods to detect threaten users. This vulnerability should be analyzed if we consider O.SENSOR objective however, this is out of the scope of this evaluation because of the O.ALIVESSNES_DETECTION objective.

V.USER_HOSTILE	This vulnerability is not exploitable due to A.USER assumption.
V.ADMIN_HOSTILE	In the same way, this vulnerability is not exploitable because of A.ADMIN assumption.
V.OUTPUT	Both vulnerabilities are not exploitable because only vulnerabilities related to aliveness detection are evaluation targets (O.ALIVENESS_DETECTION).
V.FAR	
V.QUALITY	This vulnerability is not exploitable according to A.QUALITY assumption.

The rest of vulnerabilities are classified as residual vulnerabilities because authors believe that it not be possible to be carried out within an enhanced-basic attack potential.

TABLE IX
RESIDUAL VULNERABILITIES

V.MULT_CAPTURE	Sensor and subsequent process algorithms must detect replay attacks. These attacks are a way of inject fake samples to biometric system and could be avoided if aliveness detection methods are implemented. But these attacks need particular equipment and knowledge to perform them. That is why authors consider this vulnerability having a attack potential higher than enhanced-basic (A.ATTACK).
V.LATENT (Vascular Pattern)	This vulnerability is included like a residual vulnerability for vascular biometrics because this biometric reference is located inside the human body. In order to reactivate a latent sample, attackers need to find register where image has been recorded and recover it. This action requires special equipments and a wide knowledge of the system so this vulnerability has an attack potential higher than enhanced-basic (A.ATTACK).

VI. GENERAL PENETRATION TEST FOR EXPLOITABLE VULNERABILITIES

Authors propose the next penetration tests. As above mentioned, only verification biometric systems have been considered (A.VERIFICATION).

A. Penetration test for V.SYNTHETIC and V.IMITATION vulnerabilities

Before this test can be performed and as generic considerations during its achievement:

- It is necessary to have samples of genuine users.
- All kind of potential synthetic/imitation samples must be evaluated.
- All results must show a description of how fake samples have been generated and which materials are needed.
- Fake sample enrolments must not be used for the remaining phases of the evaluation process.

Test procedure entitles the following steps:

1) Enrol a genuine user.
2) Make synthetic/imitation sample from this user.
3) Analyse enrolment process: Evaluator has to start an enrolment process and present synthetic/imitation sample to biometric capture sensor.

   If evaluator could get enrolled with such sample, test result is that sensor and/or biometric system have not implemented an aliveness detection method at enrolment phase.

   On the other hand, if evaluator could not get to enrol with this fake sample or if a FTE (Failure To Enrol) error is given back, test result to save is that sensor and/or biometric system have implemented methods that can detect this fake at enrolment.
4) Analyse verification process: Evaluator has to start a verification claiming genuine user identity and present his/her synthetic/imitation sample to biometric capture sensor. At this point two things may happen:

- A FTA (*Failure To Acquisition*) error is returned because sensor does not capture fake biometric reference. Test result for this case is that sensor and/or biometric system have implemented methods for aliveness detection at verification.
- Biometric sensor permits synthetic/imitation sample capture.
   a) Evaluator does not get a successful verification. Test result is that sensor and/or biometric system have implemented aliveness detection methods that can reject this attack at verification.
   b) On the contrary, if evaluator gets that biometric system accepts, test result is that sensor and/or biometric system have not implemented an aliveness detection method that can reject this kind of synthetic/imitation samples at verification process.

5) Results of different phases have to be recorded.

B. Penetration test for V.DEAD vulnerability

Before this test can be performed and as generic considerations during its achievement:

- Two kinds of samples have to be tested: current amputate samples and dead samples.
- Procedures change depending on whether it is possible to enrol a live sample previously or not.
- Dead/amputate sample enrolment must not be used for the remaining phases of evaluation process.

A procedure with previous enrolment entitles evaluators to follow the following steps:

1) Perform an enrolment with a live biometric reference.
2) Obtain dead/amputate sample from the user enrolled.
3) Analyse enrolment process: In an analogue way as in the penetration test for V.SYNTHETIC AND V.IMITATION vulnerabilities.

4) Analyse verification process: As in the penetration test for V.SYNTHETIC AND V.IMITATION vulnerabilities.
5) Results of different phases have to be recorded.

A procedure without previous enrolment entitles that evaluators do the following stages:

1) Obtain dead/amputate sample from the user enrol previously.
2) Analyse enrolment process: In an analogue way as in the penetration test for V.SYNTHETIC AND V.IMITATION vulnerabilities.
3) Verification process cannot be evaluated because live biometric reference has not been previously enrolled in the system.
4) Results of different phases have to be recorded.

C. Penetration test for V.LATENT vulnerability

Before this test can be performed and as generic considerations during its achievement:

- It is necessary to have samples of genuine users.
- All kind of potential reactivation methods must be evaluated.
- All results must show a description of how to reactivate latent samples.
- Latent sample enrolment must not be used for the remaining phases of the evaluation process.

Test procedure entitles that evaluators follow the next steps:

1) Perform an enrolment of a genuine user.
2) Verify the same user in order to check if previous enrolment has been done correctly.
3) Perform a new presentation of this biometric reference and assure whether this latent information is held on the sensor.
4) Analyse enrolment process: Evaluator has to start an enrolment process and reactivate latent sample. Evaluation is performed in the same way as in previous penetration tests.
5) Perform a new presentation of genuine biometric reference again and assure that latent information is held in the sensor.
6) Analyse verification process: Evaluator has to start a verification claiming genuine user identity and reactivate biometric sample. Evaluation is performed in an analogue way as in previous penetration tests.
7) The results of different phases have to be stored.

VII. EVALUATION RESULTS

After all penetration tests previously mentioned have been defined, reports have to be generated. As sensors and vulnerabilities have already been described, only results obtained will be detailed in this section. In order to keep confidentiality on the sensors tested, results will be given without reference to the specific sensor. This does not limit the interest of this paper, because this work is dealing with the methodology, but not with the particular results of particular sensors.

But what is of great interest is the description of the samples used and the way those were created. Therefore this will be explained first, leaving the overview of results for the last part of this section. Before giving those and a brief description of samples and how to create them will be detailed. Such results are presented at the following tables.

A. Vascular Pattern

TABLE X
V.IMITATION SAMPLES FOR VASCULAR BIOMETRICS

SAMPLE	A sheet of paper with a palm-vein pattern printed. Paper: DIN A4 Printer: HP 1200 LaserJet
PROCESS TO CREATE	Intercepting captured image and post-processing with image processing software. Finally image is printed. Sheet of paper is presented to the system.

TABLE XI
V.DEAD SAMPLES FOR VASCULAR BIOMETRICS

Procedure with previous live enrolment	
SAMPLE	Due to authors do not get a dead or amputate sample, this has been simulated taking out blood of the hand.
PROCESS TO CREATE	Following surgery techniques, we used a blood pressure measure instrument to press arm in order to avoid blood come in to the hand. After we covered hand with an elastic band until taking out all blood. Then that body is presented to the system

B. Fingerprint

TABLE XII
V.IMITATION SAMPLES FOR FINGERPRINTS

SAMPLE 1	Gummy Finger [2]
PROCESS TO CREATE	We made a fingerprint mould with silicone rubber. Then we boiled water and added solid gelatine. When it was liquid, we put it into the mould. Later, we put this mould into a refrigerator and when sample was solid, we put out of the mould [2].
SAMPLE 2	Resine Finger
PROCESS TO CREATE	This sample was made by an special effects expert. He made the mould with alginate of dentist and then used resin to create finger.

TABLE XIII
V.DEAD SAMPLES FOR FINGERPRINTS

V.DEAD (Procedure with previous live enrolment)	
SAMPLE	Authors did not get a dead or amputate finger, therefore this has been simulated taking out blood of the finger as we mentioned previously for vascular modality.
PROCESS TO CREATE	Again following surgery techniques, we used a blood pressure measure instrument to press arm in order to avoid blood come into the hand and fingers. After, we covered finger with an elastic band until taking out all blood.

TABLE XIV
V.LATENT SAMPLES FOR FINGERPRINTS

SAMPLE	Previous genuine user
PROCESS TO CREATE	We breathed out to sensor in order to reactivate latent sample.

C. Overall results

Unfortunately results were not as good as expected. All sensors presented some kind of fail to some of the tests performed. Some of the failures showed that with little adjustments sensor can pass the test, while other failures seem to be far from reaching a solution.

In is a fact to worry about, that although Matsumoto's work on gummy fingers is from 2002, in 2008 there are still some sensors that can fail such test.

As already mentioned, not detailed results can be published, not even the good ones, due to confidentiality reasons. But the most important result of this paper, is that the methodology developed works, and it is clearly defined to be used in CC evaluations.

VIII. CONCLUSIONS

Biometric systems could be attacked by means of presenting fake, dead or latent samples. This vulnerability can be counteracted if acquisition devices and/or process algorithms have implemented aliveness detection methods.

In this paper, authors have defined a general methodology based on analysis of vulnerabilities specified at CEM to evaluate if current commercial sensors and biometric systems have included such methods. Such methodology begins analyzing potential threats and vulnerabilities. Then it describes penetration tests for those vulnerabilities that are considered exploitable.

This methodology has been placed into action with several sensors from different modalities (vascular and fingerprint). Results have disclosed that there are still some test where sensors fail, but that the methodology presented is valid and applicable.

IX. ACKNOWLEDGEMENTS

This work has been partially developed within the PIBES Project (TEC2006-12365), funded by the Spanish Ministry of Science and Education.

Thanks to Dorian for providing us with fake finger used in some experiments.

X. REFERENCES

[1] Lisa Thalheim, Jan Krissler and Peter-Michel Ziegler, “Biometric Access Protection Devices and their Programs Put to the Test”, c’t 11/2002, page 114 http://www.heise.de/ct/English/02/11/114/

[2] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, “Impact of Artificial “Gummy” fingers on Fingerprint Systems”, Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol 4677, pp. 275-289, January 2002.

[3] T. Matsumoto, “Artificial Fingers and Irises: importance of Vulnerability Analysis”, 7th International Biometrics 2004 Conference and Exhibition, London, UK, 2004.

[4] A. Pacut and A. Czajka, “Aliveness Detection for Iris Biometrics”, IEEE Int’l Carnahan Conference on Security Technology, 17-19 October, 2006.

[5] Common Criteria - Common Methodology for Information Technology Security Evaluation v.3.1 – September, 2006.

[6] Common Criteria - Common Methodology for Information Technology Security Evaluation – Evaluation Methodology [CEM]”. v.3.1 – September, 2006.

[7] R. Sanchez-Reillo, J. Liu-Jiménez, M. G. Lorenz, L. Entrena. “Improvement in Security Evaluation of Biometric Systems”. 40th IEEE International Carnahan Conference on Security Technology (ICCST 2006). Proceedings, pp. 137-143. Lexington, KY (EE.UU.) October 16-19, 2006.

[8] Common Criteria - Common Methodology for Information Technology Security Evaluation – “Biometric Evaluation Methodology Supplement [BEM]”. v.1.0 – 2002. http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

XI. VITA

BELEN FERNANDEZ-SAAVEDRA graduated as Electronic Engineer with a Master in Robotics and Electronic Systems, by University Carlos III of Madrid in 2006. She is currently working at the University Group for Identification Technologies (GUTI), as a R&D engineer. Her PhD studies are focused on evaluating the security of biometric systems, following the works done by Common Criteria.

RAUL SANCHEZ-REILLO graduated as Telecommunication Engineer by the Polytechnic University of Madrid, obtaining his PhD in 2000. His Thesis was based on Biometric Authentication in Smart Cards. From 1994 he has been researching at the University Group for Identification Technologies (formerly University Group of Smart Cards), becoming its Director in 2000. He is also currently Associate Professor at University Carlos III of Madrid, member of IEEE and Spanish delegate in ISO/IEC JTC1 SC17, SC27 and SC37 standardization bodies. His interests in R&D cover all Personal Identification Technologies, including smart cards, biometrics and secure authentication systems.

RAUL ALONSO-MORENO graduated as Telecommunication Engineer by University Carlos III of Madrid in 2007. He is currently working at the University Group for Identification Technologies (GUTI), as a R&D engineer. His PhD studies are focused on the evaluation of identification systems, especially on those related to match-on-card technology.

CARMEN SANCHEZ-AVILA received the Ph.D. degree in Mathematical Sciences from the Polytechnic University of Madrid, Spain, in 1993. From 1985 she has been with the Department of Applied Mathematics, Polytechnic University of Madrid, where she conduct research in Digital Signal

Processing, Cryptography and Biometric. At present she is Professor in the above mentioned Department where she has been teaching different undergraduate courses related with Mathematical and Numerical Analysis as well as graduate courses in Wavelets in Signal Processing. She is also active in the research of new Biometric Verification techniques.