Biometric Sensor and Match-On-Card Evaluation platform

Benoît Vibert, John Lebouteiller, Felix Keita, Christophe Rosenberger

▶ **To cite this version:**

Benoît Vibert, John Lebouteiller, Felix Keita, Christophe Rosenberger. Biometric Sensor and Match-On-Card Evaluation platform. International Biometric Performance Testing Conference (IBPC), Apr 2014, gattersburg, United States. hal-00988148

HAL Id: hal-00988148
https://hal.science/hal-00988148

Submitted on 7 May 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Biometric Sensor and Match-On-Card Evaluation platform

B. Vibert, J. Lebouteiller, F. Keita, C. Rosenberger

Normandie Univ, France;
UNICAEN, GREYC F-14032 Caen, France;
ENSICAEN, GREYC, F-14032 Caen, France;
CNRS, UMR 6072, F-14032 Caen, France
{*benoit.vibert,christophe.rosenberger*}*@ensicaen.fr*

I. Introduction

Biometric systems are increasingly used to check or determine the identity of an individual. IT Industry is very interesting to this authentication solution in order to embed it in daily life products. The need of the evaluation of biometric sensors and Match-On-Card (MOC) algorithms is more more important to help them to choose the best system for a specific product. Among the different biometric systems, which one provides the best False Rejection Rate (FRR) given the False Acceptance Rate (FAR) set to a specific value ? How much time is needed to achieve a biometric verification on a smartcard ? Researchers are also interested to improve their MOC algorithm an also to compare it with the ones in the state of the art. These aspects become to be crucial for many applications like e-payment, physical access control...

The purpose of this paper is to propose an evaluation platform on biometric sensors and MOC for testing their performance and security. This platform allows to perform tests given scenarios and benchmarks for comparing MOCs, and permit to test fake biometric data. We illustrate the usefulness of this platform on a commercial MOC, four commercial sensors and attacks on fingerprint (fake and dead fingers).

The paper is organized as follows. Section 2 is devoted to the state of the art on the evaluating platform. Section 3 describes the proposed platform and its different modules. In Section 4, we describe the sensor acquisition platform and attacks on sensor. In section 5, we illustrate results on a commercial sensor and MOC. We conclude and give some perspectives on this work in Section 6.

II. State of the art

In this section, we first give some generalities of biometric systems. We also present the different evaluation methods of a biometric system: quality of biometric data, performance, security and usability. We describe the different existing benchmark databases that can be used for the evaluation task of biometric systems. Finally, we present the existing platforms for testing and characterizing MOC based biometric systems.

In a complete biometric system, we can evaluate each part to quantify its impact on the final result. As for example, a poor fingerprint quality can affect the performance of the system. The evaluation of a complete biometric system is based on several criteria.

The quality of the captured biometric data: In the literature, we find many elements that address the quality of fingerprints [5]. As for example, Alonso-Fernandez and *al.* [6] presented an overview of existing methods to quantify the quality of fingerprints. The authors show the impact of poor image quality on the overall performance of biometric systems. Other methods for measuring the quality of the fingerprints are given in[8], [9]. These methods have proved effective in predicting the quality of fingerprint images. NFIQ metric proposed by NIST is now the reference for this task and is part of all industrial sensors SDK fingerprint [7]. Another metric is used in research it is the metric Q [5] and this method has a better distribution of quality than NFIQ. The metric Q used multi-criteria to determine the quality of the data.

Performance: We intend here to measure the efficiency of a biometric system in terms of recognition errors in a given context of use. It is quantified by statistical measures (error rate, processing time, etc.). The measures proposed by the International Organization for Standardization ISO/IEC 19795-1 [1] to evaluate and compare the performance of biometric systems are effective and comprehensive.

Security: With regard to security, a biometric MOC have vulnerabilities, Ratha and *al.* [10] have combined attacks of a generic biometric system in 8 classes (falsified biometric data, interception of biometric data during its transmission, attack on the extraction module parameters, altered extracted parameters, matching module replaced by a malicious software, alteration of the database, man in the middle attack between the database and the matching module and alteration of the verification decision). For each point, there are different types of attacks. Figure 1 illustrates the

possible locations of the attacks in a generic biometric system.

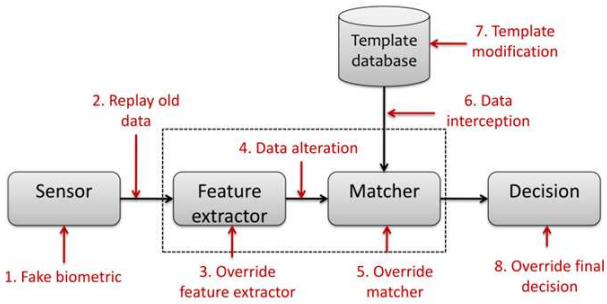

Fig. 1. Vulnerabilities locations of a biometric system (defined from [10])

Usability: This evaluation aspect is to analyze the user perception of the system and to quantify its satisfaction and acceptability. The work presented by El-Abed et *al.* [11], Jain and *al.* [12], Kukula and Proctor [13] and Kubula and *al.* [14] show the importance of this evaluation in the design and comparison of biometric systems [13]. An effective system in terms of performance but not acceptable, is not considered interesting (as in the case of DNA verification systems for physical access control).

Benchmark: To evaluate biometric systems, it is necessary to have a database containing biometric data. This database ensures that the systems are tested under the same conditions and allows for reproducible results to compare biometric MOC. Examples of biometric databases from research competitions are FVC2002 or FVC2004 [15], [16]. Moreover, it is also interesting to perform tests of the same MOC when we use multiple databases acquired under different conditions (biometric sensor, population, environment, etc.). It is also necessary to define test scenarios (number of biometric data for enrollment, number of data for testing ...).

Platforms: With regard to platforms, there are quite a few in the literature. We can already cite the NIST platform [2], which is used in their annual research competitions. It allows manufacturers to test their MOC or minutiae extractors, in terms of interoperability. In the NIST report, information on FAR (False Acceptance Rate) and FRR (False Rejected Rate) rates for every MOC and different extractors are disseminated. We can also mention the online FVC-Ongoing platform [3] dedicated to algorithms for fingerprint verification (evolution of the FCV competitions). The platform offers multiple databases grouped into two parts. The first one (Fingerprint Verification) quantifies both enrollment and verification modules, while the second one (ISO Fingerprint Matching) quantifies only the verification module on ISO Templates [4] based on minutiae. Performance metrics are: the failure to acquire rate (FTA) and the failure to enroll rate (FTE), the false non match rate (FNMR) for a defined false match rate and vice versa, the average enrollment and verification times, the maximum size required to store the biometric template on the SE, the distribution of legitimate and impostors users scores and the ROC curve with the associated equal error rate (EER). The main drawback of this platform is that it is necessary to submit the executable or source code of the MOC to the online platform which can cause confidentiality issues.

The evaluation of biometric verification algorithms is most of time used during the algorithm prototyping by researchers and relatively little by the industrial world. The evaluation methods and platforms fail to satisfy all of our needs. We intend to realize security analysis of a research or a commercial biometric MOC, to measure performance in terms of errors or verification average time.

III. Match On Card Evaluating platform

The proposed platform architecture is presented in figure 2 and is composed of modules.

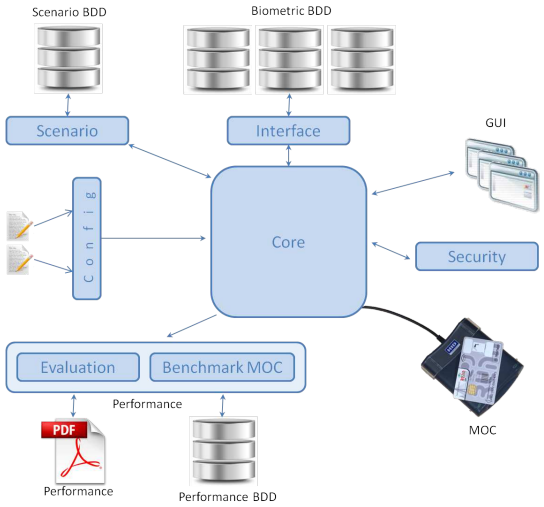

Fig. 2. general schema of the platform

The platform is made up of different modules allowing to make specific treatments, such as the interface to connect biometric databases. The central element is the `Core`, all other modules have no knowledge on others. This allows to modify a module without changing the overall operation of the platform. All modules are independent, we can change one and then see the effect of this change on the results. This will allow us, for example, to quantify the impact of a biometric database on the results or if an algorithm is better than another. The proposed platform uses active mechanisms of communication by event allowing multiple modules simultaneously access data exchanged between the client application and the MOC, thus offering the possibility of analyzing "on the fly" results.

Core: The `Core` is the main module that interfaces and manages all modules. It orchestrates the interaction with the different modules. It only knows the type of data as input of the MOC and the type of data returned by the MOC. As for example, to communicate with the Secure Element, the `Core` transparently manages the connection and communication with the MOC, it is realized by Personal Computer/Smart Card (PCSC) communication or Java Card OpenPlatform (JCOP) simulator with the software library developed through

WSCT in [20].

Database Interface: The module `Interface` manages all biometric databases. The `Core` requests to the interface the next biometric data for processing and delegates to the interface the connection and management of all biometric databases. This allows to abstract the storage format of biometric data for example.

Scenario: The module `Scenario` permits to create or use an evaluation scenario. It defines the biometric database to query, the number of biometric data to be used for enrollment or the number of users to consider. This allows us to make reproducible testing only by setting these elements. The module `Performance` quantifies the impact of these changes.

Performance: This module allows to evaluate the performance of the MOC with different metrics: FAR, FRR, EER, NIFQ value of each capture, ROC curve, enrollment and verification time. It also allows us to save the results in a database to compare several MOC based on the same test scenario.

Security: This module contains various attacks on the MOC. It is possible to use fuzzing approaches [18] consisting in injecting fault data to the biometric MOC. It can be a biometric template respecting the ISO format but containing random biometric data (brute force attack). It is also possible to test the interoperability of the MOC by providing biometric templates ISO in which faults have been injected.

GUI Interface: The proposed platform has a main graphical interface that allows to choose the test scenario and evaluation metrics. From the main interface, you have the option of using "plugins" that allow us to get information about one or more elements (eg minimum, average and maximum time for enrollment and verification). As mentioned earlier, the proposed platform uses active communication by event mechanisms, which provides access to information that you want in just developing a plugin that allows to visualize evaluation results as for example.

A. Evaluation metrics

As a first step, we use classical performance metrics commonly used in the literature and more specific ones:

- False Acceptance Rate (FAR): it measures how many times the biometric data of a user provides positive verifications with biometric data of another user.
- False Rejection Rate (FRR): it measures how many times the biometric data of a user gives a negative verification of biometric data with the same user,
- Success rate of attack: it measures the ratio of successful attacks (number of positive result over a number of transactions).
- Measuring interoperability: it quantifies the ratio of successful tests when providing an ISO template to the MOC.
- ROC curve: It describes the behavior of the biometric MOC for each value of the decision threshold (from which a test is positive). This implies that it is possible to obtain the comparison score from the MOC or to set decision threshold. For industrial MOCs, this is rarely the case but for research ones, this information is always available.
- Verification Time: we measure the time required to achieve a MOC enrollment or to obtain a verification result (after sending the ADPU (Application Data Protocol Unit defined in [19]) to the SE. It is also possible to generate several statistics on computation times such as histogram verification time, average, minimum or maximum time.
- Correlation between verification time and score : In general, a positive verification is slower than a negative one. This information can be exploited by an attacker as it can analyze the response time for the MOC to identify the extent to where the transmitted data is near the biometric reference stored on the SE (approach called Hill Climbing attack in the literature [17]). In order to quantify if a MOC could be attacked by the Hill climbing attack, we measure the Pearson correlation factor between the verification time and score returned by the MOC (when known). A strong correlation highlights a flaw in the biometric MOC, as indication the template is similar to the reference if the time decrease.

IV. Sensor acquisition platform

We have built another platform which permits to acquire biometric templates and raw data and save it on databases. During an acquisition campaign, we have used several sensors and the proposed platform can detect which sensor the finger has been placed. This platforms offer to us the possibility to acquire fingerprint on several sensors during a campaign. Each acquisition generates fingerprint images and minutiae ISO templates. These data are saved with an identification number, the hand, the finger and user's profile information. The sensor acquisition platform is shown in figure 3, we can see the different sensors and the display screen which permits to indicate to the user the hand and finger to used for the capture.

With regard to security, a biometric sensor has vulnerabilities. Ratha and *al.* [10] have combined attacks of a generic biometric system in 8 classes (falsified biometric data, interception of biometric data during its transmission, attack on the extraction module parameters, altered extracted parameters, matching module replaced by a malicious software, alteration of the database, man in the middle attack between the database and the matching module and alteration of the verification decision). For each point, there are different types of attacks. Figure 1 illustrates the possible locations of the attacks in a generic biometric system. We have tested 2 attacks on sensor, one with fake fingerprint data taken on a

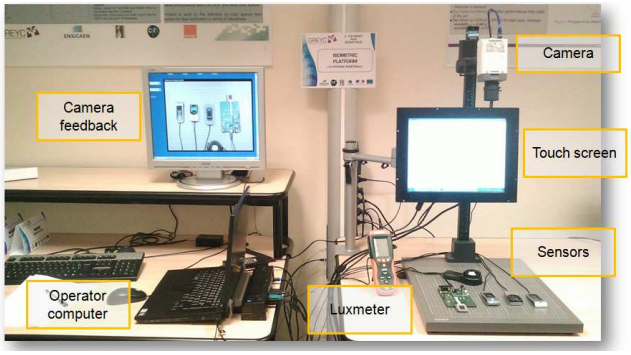

Fig. 3. Sensor acquisition platform in working

genuine user and the other on a dead finger.

Fake fingerprint: We have created a fake fingerprint database with real fingers and fingerprints (see figure 4) and we tested them on sensors face to real ones. To build this database, we have used wax and gelatin because these materials are not thick. With this test, we calculate the FTAR and if the sensors output a negative verification or if they are able to detect fake fingerprints or a spoofing attack (see figure 4).

Fig. 4. Example of fake fingerprint

Dead fingerprint: We have created a fingerprint database with dead fingers. We went on a mortuary at the Caen Hospital and we acquired fingerprints of 4 dead people. The protocol is the following :

- 3 sensors
- 4 fingers (except the thumb)
- 2 hands (left and right)
- 6 captures per individual per finger per sensor

We have 144 (6*2*4*3) data (fingerprint images and ISO template) per individual for all the sensors. For the 4 individuals, we have in total 576 (144*4) data. We have calculated the Failure To Acquire Rate (FTAR) and equals 36.11% (1 - (368/576).

V. Illustrations

To illustrate how the platform works, we have evaluated a commercial MOC on a fingerprint database (home made). We obtained the performance of the MOC, the operating point figure 5 with False Acceptance Rate (FAR) and False Rejection Rate (FRR) , the distribution of FAR FRR vs the Q metric (fingerprint quality metric developed in the GREYC research lab) on figure 7. We also have additional informations such as Q distribution on the database, time distribution figure 6.

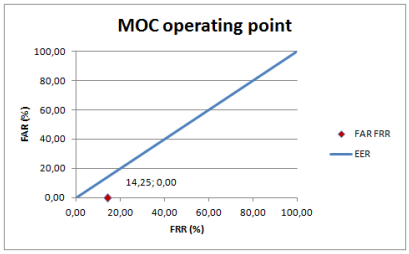

Fig. 5. Operating point for Q metric

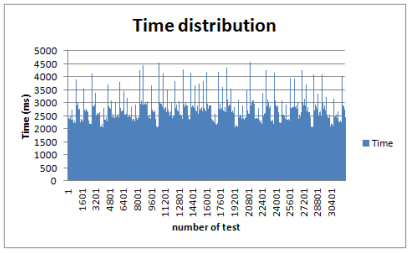

Fig. 6. Time distribution

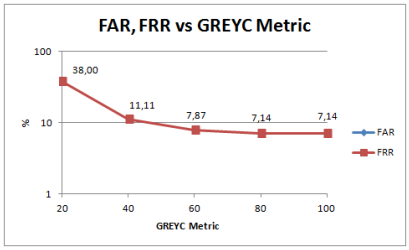

Fig. 7. FAR FRR versus Q metric: the more high is the Q quality metric, the better are the samples, the lower are the FFR values.

Industry wants to know this kind of information because it is important to choose the best MOC for their applications. We are able to compare MOC because we use the same testing scenario for each MOC. When we have a high FRR value, a good user is rejected frequently and it has a high impact on acceptability. If you have a high FAR, an impostor user is accepted by the system and it is a vulnerability. The time is another important information because it has an impact on user acceptance. Considering the evolution of the FRR value face to the quality of samples is important to consider especially during the enrollment to guarantee a good operational performance.

For fake fingerprints, we got a FTAR equal to 100% for sensors 1, 3 and 4. Consequently, for these sensors, the tested spoofing attacks are not working. For the sensor 2, the FTAR is 0% meaning that there is no problem to acquire the biometric data. 96 tests have been performed, 65% led to a negative verification and 35% to a positive one.

For the dead fingers, e have used the Q quality metric, because it has been shown in [5] that it provides a better quality assessment than NFIQ in Table 1.

Metric Q results				
	Sensor 1	Sensor 2	Sensor 3	Sensor 4
Mortuary	38.3	81.9	72.3	68.3
Senior database	32.1	84	78.6	73.7

TABLE I. AVERAGE Q METRIC VALUE FOR FINGERPRINT COMING FROM A SENIOR DATABASE THE DEADE FINGERS ONE.

We note for sensors 2, 3 and 4 that the dead fingers have a lower fingerprint quality (the higher value is Q, the better is the quality). For the sensor 1 (the only swipe sensor), it is not the case and the quality is largely worst than the three others. We think, this is due to its use, the operator for the dead fingers used correctly the sensor (see figure 8) contrary to real users.

Fig. 8. Acquisition in Mortuary

VI. CONCLUSION AND PERSPECTIVES

In this paper, we have presented the proposed platforms which permit the evaluation of biometric sensors (FTAR, quality...) and Match-On-Card algorithms. For the sensors evalution, we have illustrated two attacks on sensors: fake biometric data and fingerprint of dead people. For the dead fingerprint, we have generally observed a lower quality for the data. We have illustrated the possibility of the MOC evaluation platform on commercial MOC. We explained the importance of providing these results for industry in order to help tem to choose a MOC or for research to test if a new development is better than the previous.

In perspectives, we want to improve the attack module by providing new attack scenarios on MOC and to improve the Q metric for fingerprint quality assessment.

REFERENCES

[1] ISO/IEC 19795-1. Information technology - biometric performance testing and reporting - part 1 : Principles and framework, 2006.

[2] P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, MINEX II “Performance of Fingerprint Match-on-Card Algorithms” Phase IV : Report NIST Interagency Report 7477 (Revision II), 2011.

[3] https://biolab.csr.unibo.it/FVCOnGoing

[4] ISO/IEC 19795-2. Information technology - biometric data interchange format - part 2 : Finger minutiae data, 2004.

[5] M. El Abed, B. Hemery, C. Charrier, and C. Rosenberger. ”Evaluation de la qualit de donnes biomtriques”. Revue des Nouvelles Technologies de l’Information (RNTI), numro spcial ”Qualit des Donnes et des Connaissances / Evaluation des mthodes d’Extraction de Connaissances dans les Donnes”, p.1-18, 2011.

[6] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K.Kollreider, and J. Bigun. ”A comparative study of fingerprint image-quality estimation methods”. IEEE Transactions on Information Forensics and Security, vol. 2 : p. 734-743, 2007.

[7] E. Tabassi, C. L. Wilson, A novel approach to fingerprint image quality. In IEEE International Conference on Image Processing, (ICIP), volume 2, pp. II-37, 2005.

[8] P. Grother, E. Tabassi, Performance of biometric quality measures. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 4, number 29, p. 531-543, 2007.

[9] S. Lee, C. Lee, and J. Kim. ”Model-based quality estimation of fingerprint images”. In IAPR/IEEE International Conference on Biometrics (ICB’06), p. 229-235, 2006.

[10] N.K. Ratha, J.H. Connell, and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, vol. 40 : p. 614 - 634, 2001.

[11] Mohamad El-Abed, Romain Giot, Baptiste Hemery, and Christophe Rosenberger. A study of users’ acceptance and satisfaction of biometric systems. International Carnahan Conference on Security Technology (ICCST), IEEE, p. 170-178, 2010

[12] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics : A grand challenge. International Conference on Pattern Recognition (ICPR), vol. 2 : p. 935-942,2004.

[13] E. P. Kukula and R. W. Proctor. Human-biometric sensor interaction : Impact of training on biometric system and user performance. In Proceedings of the Symposium on Human Interface 2009 on Human Interface and the Management of Information. Information and Interaction. Part II, vol. 5618, p. 168-177, 2009.

[14] E. P. Kukula, C. R. Blomeke, S. K.Modi, and S. J. Elliott. Effect of human-biometric sensor interaction on fingerprint matching performance, image quality and minutiae count. International Journal of Computer Applications in Technology, 34(4) : p. 270-277, 2009.

[15] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, FVC2002: Second Fingerprint Verification Competition International Conference on Pattern Recognition (ICPR), vol. 3, p. 811-814, 2002.

[16] D. Maio, D. Maltoni, J.L. Wayman, A.K. Jain, FVC2004: Third Fingerprint Verification Competition in Proceedings of the First International Conference on Biometric Authentication, 2004

[17] M. Martinez-Diaz, J. Fierrez-Aguilar , F. Alonso-Fernandez, et al. Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In : Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International. IEEE, 2006. p. 151-159.

[18] J. Lancia, Un framework de fuzzing pour cartes puce : application aux protocoles emv. SSTIC, 2011.

[19] ISO/IEC 7816-1 to 15 : Identification cards - Integrated circuit(s) cards with contacts (Parts 1 to 15), http://www.iso.org.

[20] S. Vernois, ”WSCT a software for smartcard transactions”, 2007.