Practical Method for Evaluating the Performance of a Biometric Algorithm

Tahirou Djara[1,2(✉)], Abdou-Aziz Sobabe[1,2], Macaire Bienvenu Agbomahena[1,2], and Antoine Vianou[1,2]

[1] Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC), Cotonou, Benin
csm.djara@gmail.com
[2] Institut d'Innovation Technologique (IITECH), Abomey-Calavi, Benin

Abstract. This paper presents a modality-independent method of evaluating the performance of an algorithm in biometrics. The operation mode is about developing a JAVA application that offers the user a graphical representation of the evaluation results. This application is interacting with a MySQL database containing the extracted signatures as well as the matching values of the modalities present in the evaluated biometric system. The evaluation system is used to generate the Genuine Matching and Impostor Matching score distribution curves, the False Match Rate and False Non Match Rate curves and the ROC curve. 1000 lines of code were used to develop the application. The method proposed is original and practical. Thus, an application of this method has been made in the case of a contactless fingerprint modality. We plan to improve the developed method by adding the representation of 4 main operating points (EER, WER, Fixed FMR, Fixed FNMR).

Keywords: Biometrics · Performance evaluation · Biometric algorithm
Genuine Matching (GM) · Impostor Matching (IM) · False Match Rate (FMR)
False Non Match Rate (FNMR) · Receiver Operating Characteristic (ROC)
Modality-independent

1 Introduction

Biometrics is a global technique aimed at establishing the identity of a person by measuring a morphological (such as face), biological (such as DNA, genetic inheritance) and/or behavioral (such as signature) characteristics. The usual techniques of access control are based on what we know (password, PIN code, etc.) and what we have (identity card, badge, etc.) [1]. But these methods pose problems of reliability such as falsification of document, forgetting one's code and decryption of password. Contrary to "what we know" or "what we have", biometrics is based on "what we are" or "how we behave" and thus avoids duplication, theft, forgetfulness or loss. A biometric system can operate either in authentication mode or in identification mode. Authentication is to answer the question: are you the one you claim to be? On the other hand, identifying comes down to answering the question: who are you? The

R. Zitouni and M. Agueh (Eds.): AFRICATEK 2018, LNICST 260, pp. 125–132, 2019.
https://doi.org/10.1007/978-3-030-05198-3_11

characteristics used must meet 5 modalities. They must be universal, unique, permanent, easy to collect and acceptable [2].

According to [3], two very basic questions often arise when dealing with biometric systems or components: how can the accuracy of a biometric system (or its components) be measured and how to compare different systems with each other? The answer to these two questions lies in the determination of a sixth modality, that of performance. This performance factor has a double advantage for the designer but also for the user of the system. For the designer of a biometric system, he has the obligation to produce information to assess the performance of his product in comparison with existing ones. On the user's side, the performance of a biometric system makes it easy for him to make a decision as to the choice to be made in the large array of existing biometrics. Contrary to what one could imagine, the evaluation of the performance of a biometric system is based on a very varied range of parameters with possibilities of combinations. Some parameters are quantitative (for example the processing time) while others are qualitative (for example the satisfaction of the user). The analysis of the performance of a biometric system takes into account the context of implementation. According to a study presented in [2], DNA and Iris show the best performances in terms of treatment algorithms (EER) but at the same time they are the most hated by users.

In this paper, we show how to obtain the curve of the GM (Genuine Matching) and IM (Impostor Matching) distributions, the False Match Rate (FMR) curve, the False Non-Match Rate (FNMR) curve and the Receiver Operating Characteristics (ROC) curve to evaluate the performance of any biometric identification algorithm. For the display of the characteristic curves, we used a database where the various extracted signatures are saved as well as the values of pairings. The evaluation method developed was tested on a practical example based on contactless fingerprint. In Sect. 2, we present the previous work in biometrics evaluation. The operating principle of the developed method is presented in Sect. 3 while Sect. 4 presents an application of the method to a biometric system using a contactless fingerprint. Section 5 concludes the paper.

2 Related Work

Biometric systems are designed and developed in laboratories with the purpose of being used in everyday life. But before deployment in a real situation, it is necessary to evaluate them in order to know their performances and their limits. Depending on the application, this evaluation can consider several parameters such as: ease of use for users, security, cost, data protection problems, reliability of the system or sensors, maintenance requirements, human control requirements in operational mode and of course recognition error rates [4].

Taking into account the opinion of the user, [5] presented an overview of existing evaluation aspects of biometric systems based on data quality, usability and security. Regarding the biometric systems tested, the robustness of a system against attacks, the computation time required during the verification phase and its ease of use were identified as important factors influencing user's opinion. Several studies have shown that the quality of biometric samples has a significant impact on the accuracy of a

matcher. On the security aspects, [6] present 8 vulnerable points of attacks in a biometric system.

[2] have made a survey on international competitions and platforms that aims to evaluate the performance of biometric systems. All that works have been synthesized in the Table 1.

Table 1. International biometrics competitions and platforms

Category of competition	Name of competition	Year	Performance metrics used
Mono-modal competitions	FVC [7]	2000, 2002, 2004 and 2006	GMS and IMS, average and maximum template size, average enrolment and verification time, FTE and ROC curves
	FpVTE [8]	2003	ROC, DET, FAR and FRR
	SVC [9]	2004	EER
	CBT2006 [10]	2006	FNMR, FMR, Transactional-FNMR, Transactional-FMR, FTA, Transactional-FTA, and FTE
	ITIRT2005 [11]	2005	FNMR, FMR, T-FNMR, T-FMR, FTA, T-FTA, and FTE
Multi-modal competitions	BMEC	2007	ROC curves and their corresponding EERs
Platforms	BioSecure	2007	ROC curves and their corresponding EERs
	GREYC-Keystroke [12]	2009	GMS and IMS, ROC curves and the FTA rate
	FVC-OnGoing [13]	2009	FTE and FTA, FNMR for a fixed FMR and vice-versa, average enrolment and verification time, maximum template size, GMS and IMS, ROC curves and their corresponding EERs

Earlier studies devoted to estimating the performance of biometric systems, have specified three types of rating [14]. These are: technology evaluation, scenario evaluation and operational evaluation. The technology evaluation is responsible for testing only the performance of the algorithmic parts of the system (feature extraction, comparison and decision) using a pre-acquired database. The scenario evaluation covers a broader field of action that also includes the sensors, the environment and the specific population of the tested application. The operational evaluation for its part takes into account a global biometric system under real conditions of use.

We focused in this work on the technological evaluation, which will test only the algorithmic part of the system using a database that we built. The objective is to provide the research community with a detailed protocol that presents the code of the evaluation program in a transparent manner, regardless of the number and types of modalities used.

3 Presentation of the Operating Principle of the Developed Method

To implement our method of evaluating the performance of algorithms in biometrics, we first developed a graphical interface under JAVA using the NetBeans IDE 8.2 for the automatic generation of each of these curves (GM, IM, FMR, FNMR and ROC). The JAVA code structure and the excerpt of the graphical interface developed are available in the appendix document at https://refod.net/iitech/paper/Appendix.pdf. The metadata needed to generate the curves consists of the signatures of the biometric modality selected for the identification. These signatures and the different matching values will be stored in a MySQL database. A connection is established between the JAVA program and the created database.

3.1 Principle of Design of Different Charts

This paragraph provides the technical details of the design of the three evaluation graphs presented. For any given modality (fingerprint, hand geometry, face, iris, gait, DNA, etc.), the protocol used for the matching test is as follows:

Let S_{ij} be the j^{th} signature extracted from the i^{th} modality M_{ij} ($1 \leq i \leq n$; $1 \leq j \leq m$). The S_{ij} signature extracted from M_{ij} is stored in a MySQL database.

For signature matching, we do the following operations:

1. Genuine Matching (GM) study: each S_{ij} signature is compared with the set of S_{ik} signatures ($k \neq j$) from the same i, which provides the corresponding match value gms_{ijk} (Genuine Matching Score) saved in a table of the database.
2. Impostor Matching (IM) study: the first S_{k1} copy of each modality is compared with each copy of the remaining modalities S_{ij} ($i > k$) and provides the corresponding matching value ims_{ik} (Impostor Matching Score) saved in another table of the database.

The number of matches (NGRA: Number of Genuine Recognition Attempts and NIRA: Number of Impostor Recognition Attempts) is defined in each case by the following formula:

$$\text{Case 1 : NGRA} = \left\| \left\{ gms_{ijk},\, i \in [1\ldots n],\, 1 \leq j \neq k \leq m \right\} \right\| = n \times m \times (m-1) \tag{1}$$

$$\begin{aligned} \text{Case 2 : NIRA} &= \left\| \{ ims_{ik},\, i \in [1\ldots n],\, 1 \leq j \neq k \leq m \} \right\| \\ &= m\left[(n-1) + (n-2) + \cdots + 1 \right] \end{aligned} \tag{2}$$

The Genuine Matching-Impostor Matching Chart. The graphical representation of GM and IM distributions shows how the algorithm differentiates the two classes. For each distribution (GM and IM), it is necessary to create a text file (txt format) which saves gradually after comparisons the value of pairing. Once these files are created, it is a question of counting the repetition of each value of pairing and thus the probability of

appearance. The count result at each distribution is also stored in a text file. At the graph level, the match values will be represented on the x-axis while the number of repetitions (count) will be on the y-axis. The code used for this operation is available in the appendix document.

The FMR-FNMR Chart. The GM and IM distributions are used to calculate the FMR (t) and the FNMR (t) as functions of the t threshold that characterizes decision-making in the verification phase.

FMR(t) and FNMR(t) are defined as:

$$\text{FMR}\ (t) = \frac{card\{ims_{ik}/ims_{ik} \geq t\}}{NIRA} \tag{3}$$

$$\text{FNMR}\ (t) = \frac{card\{gms_{ik}/gms_{ijk} < t\}}{NGRA} \tag{4}$$

card denotes the cardinal of the set considered, FMR (t) corresponds to the percentage of users recognized by error ($ims_{ik} \geq t$) and FNMR (t) corresponds to the percentage of users rejected by error ($gms_{ijk} < t$).

The code used to generate the FMR-FNMR chart is available in the appendix document.

The ROC Chart. The ROC curve is the one that gives the FNMR as a function of the FMR. This curve is obtained by using the code available in the appendix document.

The Complementary Code. The complementary code consists of the two remaining code portions for the database connection and the JAVA main project. These codes are available in the appendix document.

3.2 Database Creation Principle

The database to be created will have as many tables as needed. Thus, for each signature sub-modality (for example the sub-signatures of bifurcations on the one hand and endings on the other hand for a fingerprint signature), a table is created for storing the metadata of the signature. This means that there will be as many tables as signature sub-modalities. In addition, the results of each pairing operation are also stored in tables. There will therefore be two tables for the genuine and impostor classes whose codes are available in the appendix document.

4 Application of the Method to a Biometric System Using a Contactless Fingerprint

4.1 Fingerprint Acquisition System

This is an application called Contactless Biometric Fingerprint Software (CBFS) developed by [15]. The launch of the CBFS automatically triggers the activation of the webcam connected to the computer and opens an intuitive graphical interface

(see Fig. 3 in the appendix document) with 4 zones for interaction between the user and the application. The first area at the top left of the interface gives an instant snapshot of the image in the webcam field. This zone 1 is used to adjust the finger which one wants to recover the image of the fingerprint. The bottom left (zone 2) contains the command buttons used to capture the image of the fingerprint once the adjustments are judged satisfactory. As for the upper right (zone 3), it shows the user the image that has just been taken. Finally, the last part (zone 4) is at the lower right position of the interface. It consists of a message display space for the purpose of assisting the user throughout the process of acquisition of fingerprints.

For experimentation, we created a database of 420 fingerprints comprising 28 sets of different fingers (each finger representing an individual), each comprising 15 different acquisitions.

4.2 Protocol Used for the Matching Test

Note S_{ij} the j^{th} signature extracted from the i^{th} fingerprint E_{ij} ($1 \leq i \leq n$; $1 \leq j$ m). The signature S_{ij} extracted from E_{ij} is stored in a MySQL database called ***"fingerprint"***. For each fingerprint, the extracted signature is represented as:

$$\begin{bmatrix} x_1 & y_1 & \theta_{11} & \theta_{21} & \theta_{31} & z_0 & z_1 & \cdots & z_n \\ x_2 & y_2 & \theta_{12} & \theta_{22} & \theta_{32} & z_0 & z_1 & \cdots & z_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_M & y_M & \theta_{1M} & \theta_{2M} & \theta_{3M} & z_0 & z_1 & \cdots & z_n \end{bmatrix} \quad (5)$$

for bifurcation points (first sub-modality for the fingerprint) and

$$\begin{bmatrix} x_1 & y_1 & \theta_1 & z_0 & z_1 & \cdots & z_n \\ x_2 & y_2 & \theta_2 & z_0 & z_1 & \cdots & z_n \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_N & y_N & \theta_N & z_0 & z_1 & \cdots & z_n \end{bmatrix} \quad (6)$$

for endpoints (second sub-modality for fingerprint).

(xi, yi) denotes the position of the minutiae. θ_{ij} denote the relative angles between the branches of bifurcations and θ_i the termination angle as defined in [15]. z_i represent the characteristics extracted at the level of each minutia. Expression (5) represents a table called ***"bifurcations"*** in the fingerprint base while expression (6) represents a table called ***"terminations"*** in the same base. Figures 4 and 5 in the appendix document respectively show an illustration of each table.

For the test, we perform the following operations:

1. Genuine Matching (GM) study: each S_{ij} signature is compared with the set of S_{ik} signatures $(k \neq j))$ from the same finger i, which provides the corresponding match value gms_{ijk} (Genuine Matching Score) recorded in the "intraclasse" table of the "fingerprint" database. Figure 6 in the appendix document gives an illustration of this table.

2. Impostor Matching (IM) study: the first copy S_{k1} of each fingerprint is compared with each copy of the remaining fingerprints $S_{ij}(i > k)$ and provides the corresponding matching value ims_{ik} (Impostor Matching Score) recorded in the "interclasse" table of the "fingerprint" database. Figure 7 in the appendix document gives an illustration of this table.

According to Eqs. (1) and (2), NGRA = 5880 and NIRA = 5670 in our case.

Curves Construction. Let ***msintra.txt*** and ***msinter.txt*** be the files of the GM and IM matching values, then ***countIntra.txt*** and ***countInter.txt*** the corresponding count files. The application allows us to have the GM and IM distributions curve, the FMR and FNMR curve and the ROC curve (respectively Figs. 8, 9 and 10 in the appendix document).

5 Conclusion and Perspectives

In this article, we presented a practical modality-independent method for evaluating the performance of an algorithm in biometrics. This method was tested using a contactless fingerprint system. Our experimental protocol has two main phases: the curves construction and the database creation. At the curves construction phase (GM-IM, FMR-FNMR and ROC), the developed JAVA code was presented. At the database creation phase, we explained the test operations for attempted authenticity and imposture from extracted signatures. In each case, these signatures as well as their match values are stored in tables of a MySQL database. The originality of the approach we propose lies in the detailed presentation of the methodology and the JAVA and SQL codes that have been developed.

Our first perspective will be to represent the major operating points of our application case on a curve of error rates according to the decision threshold as well as on a ROC curve [4]. The 4 operating points that will be the subject of our future work are: EER, WER, Fixed FMR and Fixed FNMR.

We also plan to develop two complementary modules to measure the FTA (Failure To Acquire Rate) and FTE (Failure To Enroll Rate) characteristics [10]. In addition, we will adapt the developed method to a multimodal biometric system.

References

1. AlMahafzah, H., AlRwashdeh, M.Z.: A survey of multibiometric systems. Int. J. Comput. Appl. **43**(15), 36–43 (2012)
2. El-Abed, M., Charrier, C.: Evaluation of biometric systems, chapter 7. In: New Trends and Developments in Biometrics, pp. 149–169 (2012). https://doi.org/10.5772/52084. hal-00990617
3. Precise Biometrics: White-Paper, Understanding biometric performance evaluation. AB – SPA 133 1000 4160/wpbpe RA (2014)

4. Allano, L.: La Biométrie multimodale: stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles. Thèse de doctorat, Institut National des Télécommunications dans le cadre de l'école doctorale SITEVRY en co-accréditation avec l'Université d'Evry-Val d'Essonne (2009)
5. El-Abed, M., Giot, R., Hemery, B., Rosenberger C.: Evaluation of biometric systems: a study of users' acceptance and satisfaction. Inderscience Int. J. Biom. (IJBM), 1–27 (2012). https://doi.org/10.1504/ijbm.2012.047644. hal-00984024
6. Marasco, E., Ross, A.: A survey on anti-spoofing schemes for fingerprint recognition systems. ACM Comput. Surv. **47**(2), 1–36 (2014). Article A
7. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, 2nd edn. Springer Science+Business Media, New York (2003). © Springer-Verlag London Limited 2009
8. FpVTE: Fingerprint vendor technology evaluation 2003 (NISTIR 7123) (2003). http://fpvte.nist.gov/. Accessed 13 Jan 2018
9. Zhang, D., Jain, A.K. (eds.): ICBA 2004. LNCS, vol. 3072. Springer, Heidelberg (2004). https://doi.org/10.1007/b98225
10. IBG: International biometric group, comparative biometric testing. Round 6 Public Report (2006)
11. IBG: International biometric group, independent testing of iris recognition technology. Final report (2005)
12. Giot, R., El Abed, M., Rosenberger, C.: GREYC keystroke: a benchmark for keystroke dynamics biometric systems. In: IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–6 (2009)
13. Dorizzi, B., et al.: Fingerprint and on-line signature verification competitions at ICB 2009. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 725–732. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01793-3_74
14. Phillips, P.J., Martin, A., Wilson, C.L., Przybocki, M.: An introduction to evaluating biometric systems. Computer **33**(2), 56–63 (2000)
15. Djara, T., Assogba, M.K., Vianou, A.: A contactless fingerprint verification method using a minutiae matching technique. Int. J. Comput. Vis. Image Process. **6**(1), 12–27 (2016)