International Journal of Industrial Engineering & Production Research March 2022 Vol. 33, No. 1: 1-12
DOI: 10.22068/ijiepr.33.1.6

RESEARCH PAPER

Evaluation and Comparison of the Performance of Biometric Recognition

Fatima Zohra Allam[1*], Latifa Hamami-Mitiche[2] & Hicham Bousbia-Salah[3]

Received 11 December 2021; Revised 18 December 2021; Accepted 28December 2021;

ABSTRACT
For several years, considerable efforts have been made in the field of biometric research. The major interest of this line of research is linked, among other things, to the recognition of the individual because the security needs are becoming increasingly important, and the economic stakes are colossal. There are many and diverse biometric applications that provide a substantial level of security. Unimodal biometric systems allow a person to be recognized using a single biometric modality, but cannot guarantee correct identification with certainty. While multimodal biometric systems, using several biometric modalities, guarantee better recognition. In this article, we are interested in the study of evaluation tools for biometric systems. For this, we will first calculate three essential parameters, namely: False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER). Second, we will determine the performance curves, in this case, the ROC curve (Receiver Operating Characteristic) and the DET curve (Detection Error Tradeoff). The calculation of these metrics allows the evaluation of unimodal and bimodal biometric systems to compare the benefit of merging the biometric modalities.

KEYWORDS: *Unimodal and bimodal recognition systems; Authentication mode; FRR; FER; EER; ROC Curve; DET curve.*

1. Introduction

The need for secure, automated access to physical or virtual environments is growing. This need requires reliable means to verify the identity of a person who reports to the access system. However, conventional means relying on passwords or magnetic cards associated with a personal code often have a number of drawbacks. Indeed, a password can be forgotten or stolen by another individual, or even given to someone else and access cards can also be lost or stolen [1-4].
The ability to identify individuals seems to have become an obsession with governments who have adopted a new paradigm under which our security is ensured through widespread surveillance of populations. It is therefore crucial to develop automatic authentication systems capable of combating fraud and ensuring security in various fields [5-8].
To meet these needs, biometrics seems to be a practical, reliable and efficient solution whose cost in terms of effort and money is constantly decreasing. Biometrics refers to all the processes aimed at identifying an individual from the measurement of one or more of their physical, physiological or behavioral characteristics [1], [9] and [10]. There can be several types of physical characteristics, some more reliable than others, but all must be tamper-proof and unique in order to be representative of one and only one individual.
Unimodal biometric systems allow a person to be recognized using a single biometric modality, but cannot guarantee correct identification with certainty. In addition, these systems are sensitive to the noise introduced by the single sensor, to the non-universality and lack of individuality of the chosen biometric modality, as well as to intrusion attempts [11]. Most of these problems can be reduced by setting up multimodal biometric systems using multiple biometric signatures from the same person [1] and [10].

* **Corresponding author:** ***Fatima Zohra Allam***
fatima_zohra.allam@g.enp.edu.dz

1. *Department of Electronics, National Polytechnic School, 10, Avenue des Frères Oudek El Harrach 16200 Alger Algeria.*
2. *Department of Electronics, National Polytechnic School, 10, Avenue des Frères Oudek El Harrach 16200 Alger Algeria.*
3. *Department of Electronics, National Polytechnic School, 10, Avenue des Frères Oudek El Harrach 16200 Alger Algeria.*

In this paper, we are interested in the performance measurement of unimodal and bimodal biometric systems. The concepts relating to unimodal and multimodal biometrics are well developed in the literature, particularly [1], [6], [10] and [12].

We are going to build, first, a biometric recognition system based on the iris, then another based on the face. Then, we will merge the two previous systems (modalities) to achieve a bimodal biometric recognition system in order to improve performance and eliminate certain constraints related to the first two systems. We will present a comparative study corresponding to the three systems produced.

2. Performance Measurement of A Biometric System

A biometric system makes it possible to verify the identity of a person using one or more specific methods (voice, iris, face, fingerprints, etc.). It is an automatic biometric measurement control system based on the recognition of individual characteristics.

In biometrics, we define two types of populations: Genuine, who have authorization to access the protected area, and imposters, who have no authorization but will still try to enter [13-15].

Any biometric system has a similarity score in the range [0,1]. Indeed, the closer the score is to "1", the more the system is sure of the claimed identity. The closer the score is to "0", the less confident the system is in the claimed identity.

Decision making in each biometric recognition system is calculated using a parameter called "threshold τ", such that biometric samples that generate scores above the threshold τ are considered “Genuine”. On the other hand, the samples which generate scores lower than the threshold τ are considered as “impostors”.

In this article, we are interested in the study of assessment and development tools for a biometric system operating in authentication mode (verification) to confirm whether or not an individual belongs to an access system. predefined. For this, three essential parameters are defined, namely: FRR, FER and EER.

In order to assess the performance of a biometric system operating in authentication (verification) mode, a large number of comparisons must be made from an already existing "Tests" database. We assume that the different samples of the same individual are independent. Each biometric sample from each individual in the database is then compared to all the other samples in the database. In the case where the compared samples come from the same individual, the comparison is called "genuine comparison". In the event that the two samples come from different individuals, the comparison is called an "impostor comparison" [16].

The score densities for the "genuine" and "impostor" comparisons are generated from the entire database. The precision of the biometric system is then evaluated by the ability to separate these two densities. The separation is done thanks to the threshold τ, from which the decision of acceptance or rejection of identity will be taken.

We can then distinguish two cases:

- If the score is above the threshold, the decision is considered positive and the identity of the individual is accepted.
- If the score is below the threshold, the decision is considered negative and the identity of the individual is rejected.

It should be noted that in the case of an ideal biometric system, the two score densities do not overlap. On the other hand, in the case of a real biometric system, these two densities overlap and no threshold value makes it possible to separate them completely. This overlap is mainly due to errors in decision-making by the system, in particular, false acceptances (in the case where an "Impostor" comparison returns a high similarity score) and false rejections (in the case where a comparison "genuine" returns a very low score).

In the literature, especially in [1], there are several metrics and several types of curves to define the performance of a biometric system. In what follows, we will define the most used.

2.1. False rejection rate (FRR)

This rate determines the likelihood that a system will not recognize a person who normally should have been recognized. It is a ratio of the number of legitimate people denied access to the total number of legitimate people being authenticated.

$$FRR = \frac{Number\ of\ Rejected\ "Client"}{Total\ Number\ of\ "Client"Access} \tag{1}$$

2.2. False acceptance rate (FAR)

This rate determines the likelihood that a system will recognize a person who normally should not have been recognized. It is a ratio of the number of people who got accepted when they shouldn't have been and the total number of unauthorized people who tried to get accepted.

$$FAR = \frac{Number\ of\ Impostors\ Accepted}{Total\ Number\ of\ Impostors\ Access} \tag{2}$$

2.3. Equal error rate (EER)

This rate is calculated from the first two criteria and constitutes a point of current performance measurement. This point corresponds to the place where FRR = FAR, that is to say the best compromise between false rejections and false acceptances [1].

$$EER = FRR = FAR \tag{3}$$

2.4. Half total error rate (HTER)

It is a metric which corresponds to the average between the FAR and FRR for a fixed threshold τ [17]:

$$HTER = \frac{FAR(\tau)+FRR(\tau)}{2} \tag{4}$$

Theoretically, the HTER is used to approximate the EER in the case where the two error rates FAR and FRR are of the same order of magnitude. Generally speaking, the HTER is used to quantify system performance in the event that the distribution of scores from legitimate users and imposters is not available. It is estimated using the operational decision threshold τ of the system [15] and [16].

The following figure shows the performance metrics. Figure 1 shows a distribution of the likelihood rates that legitimate users and impostors would obtain from a given verification system.

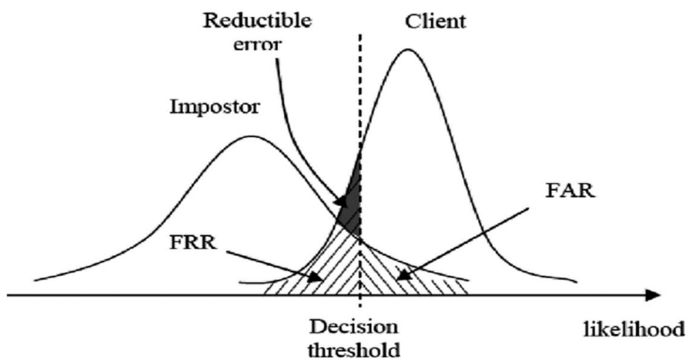

Fig. 1. Distributions of the likelihood rates of legitimate users and impostors of a Biometric System [16]

Ideally, the system should have FAR and FRR equal to zero. However, in practice, it is impossible to have these two parameters zero. So, we have to find a compromise between FAR and FRR.

It should be noted that the lower the decision threshold, the more the system will accept legitimate users and therefore it will also accept more impostors.

Conversely, the higher the decision threshold, the more the system will reject impostors and therefore it will reject more legitimate users.

It is therefore impossible to reduce both types of errors simultaneously. This is one of the reasons behind the introduction of multimodality. Indeed, if several modalities are correctly combined, it becomes possible to reduce both types of errors at the same time [18].

3. Performance Curves

There are other criteria that can be used to assess the performance of biometric systems. Now we will define two types of performance curves:

3.1. ROC Curve (Receiver Operating Characteristic)

This curve represents on the y-axis the proportion of positive tests among the authentic users (the sensitivity) as a function of the proportion of positive tests among the impostors (complement of specificity or 1–specificity, on the x-axis) for all the values of the test thresholds possible [19] and [20]. To be able to determine the validity of a test through this curve, it is necessary to calculate the area under the ROC curve called AUC (Area Under the Curve). Several methods have been proposed in [20-23]_to estimate the AUC. Thus, when the test is perfectly discriminating, the area under the curve (AUC) is equal to 1 but this is never possible. In fact, the larger the AUC, the better the algorithm performs [24] and [25].

The following figures show performance metrics. Figure 2 shows the Percentage of Times a False Reject (FFR) and False Accept (FAR) curve as a function of Sensitivity (Security Level).

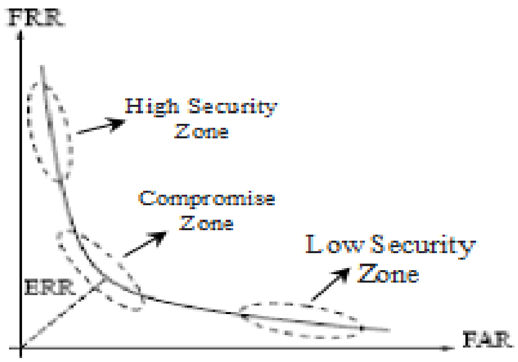

Fig. 2. ROC Curve [18]

This curve plots the false rejection rate as a function of the false acceptance rate [18]. The more this curve tends to follow the shape of the benchmark, the more efficient the system, i.e. having a high overall recognition rate.

3.2. DET curve (detection error tradeoff)

An alternative to the ROC curve is the Detection Error Compromise (DET) graph, which plots the rate of false negatives (missed detections) versus the rate of false positives (false alarms) on the x and y axes non-linearly transformed. This curve illustrates the relationship between the FRR and the FAR. It is obtained by varying the decision threshold and by calculating each time the two values FRR and FAR [24] and [26].

The transformation function is the quantile function of the normal distribution, that is, the inverse of the cumulative normal distribution. This alternative spends more graphics area on the region of interest. Most of the ROC area is of little interest; the main concern is the region tight against the y-axis and the upper left corner - which, due to the use of the failure rate instead of its complement, the success rate, is the lower left corner of a DET route.

In addition, DET graphs have the useful property of linearity and linear threshold behavior for normal distributions. The DET trace is widely used in the automatic recognition community of individuals [26].

In what follows, we will discuss the processing steps of each modality with the algorithms corresponding to each module. We then illustrate the simulation results of each system before and after the merger of the two modalities. We then assess the performance of each system produced.

4. Steps in the Realization of the Three Biometric Recognition Systems

The database used is CASIA-Iris-Distance, a subset of CASIA-IrisV4. It contains iris images, in JPEG format and 8-bit grayscale, captured using a long-range, high-resolution system, collected under near infrared lighting [27] and [28]. The different characteristics shown in the iris images make it possible to study research questions specific to iris recognition, such as the robustness of iris recognition against changes in lighting, the recognition of iris, iris of twins, …

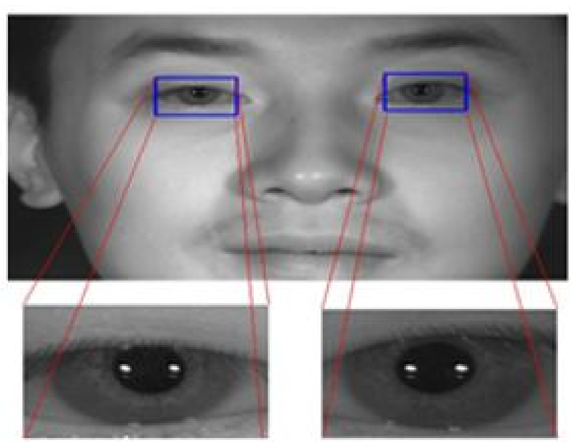

Fig. 3. Example images in the CASIA-Iris-Distance database.

In the following, we will develop the steps for processing and extracting iris and facial features.

5. Extraction of Local Characteristics

Local feature extraction involves extracting local features from face and iris images, including features of the Gabor Filter, features of Zernike Moments, and features of the Local Binary Pattern (LBP).

The steps for extracting facial features are the same as those applied to the iris [29-34]. The normalized iris image is of size [20x245], this image will be divided into twelve blocks of size [20x20]. We will apply to each block the three algorithms, in this case LBP, Zernike Moment and Gabor Filter.

5.1. LBP algorithm

We used a new method of extracting iris features based on local binary type images (LBP) and on the chunk coding method [35]. First, we apply the LBP to the normalized iris image and we get the LBP iris image, then we extract the iris characteristic via the information-based chunk coding method iris statistics.

To speed up the processing and keep a high recognition rate, the LBP model is used in the recognition algorithm, and is introduced as a complementary measure for the contrast of the local image. Compared to Gabor wavelets, LBP features can be extracted faster in a single scan through the raw image and are in a lower dimensional space, while retaining the iris texture information. To implement efficient and more precise recognition, we have modified the method of extracting LBP features [36]. We have developed a chunk coding method based on statistical information to obtain the characteristic code of both irises and the face.

The original LBP operator is a powerful means of texture description. The first incarnation of the operator worked with the eight neighbors of a pixel, using the value of the central pixel as a threshold. The pixels of neighborhood $g_0 - g_7$ are converted to 0 if their gray levels are lower than those of the center g_c, or to 1 in the other cases. Then, an LBP code for the center pixel g_c is produced by multiplying the converted neighborhood pixel values by the weights 2^n given to the corresponding pixels (n is the index of the eight neighbors, respectively), then we add the result [35] and [36].

5.2. Zernike moment algorithm

In object / image recognition, a region (part of an image) can be described using a scalar or a set of scalars based on the geometric properties of the object. Such scalars are called descriptors because they describe objects recognized by an artificial vision system [37].

In this section, we will calculate the Zernike Moment (ZM), moments based on the region. Using the ZM and geometric features, we extracted twelve features [38].

The ZM are orthogonal moments based on Zernike polynomials. Orthogonality here means that there is no redundancy or overlap of information between the moments. Thus, the moments are uniquely quantified according to their orders. The distinguishing feature of ZM is the invariance of its magnitude with respect to rotation [39] and [40].

We will calculate Zernike moments for the sub-blocks of the iris and face images**:**

Let (m; n) be the ordered pair which represents the order of the Zernike polynomial and the multiplicity of its phase angle, the Zernike moment, Z_{nm} for a sub-block of an image (of the iris or of the face) $\{f(x_i, y_i)/1 \leq i \leq 20 \; and \; 1 \leq j \leq 20\}$ can be calculated using:

(a) Cartesian coordinate system

$$Z_{nm} = \frac{n+1}{\pi} \iint f(x,y)\, V_{nm}(x,y) \partial x \partial y \qquad (5)$$

$$Z_{nm} = \frac{n+1}{\pi} \sum_x^M \sum_y^N V_{nm}(x,y) f(x,y)$$

(b) Polar coordinate system

$$Z_{nm} = \frac{n+1}{\pi} \iint f(\rho,\theta)\, R_{nm}(\rho,\theta) \partial \rho \partial \theta \qquad (6)$$

Where:

$$V_{nm}(\rho,\theta) = R_{nm}(\rho) e^{i\theta} \qquad (7)$$

With: $\rho = \sqrt{x^2 + y^2}$ and $\theta = \arctan\left(\frac{y}{x}\right)$

m defines the order of the Zernike polynomial

n represents the multiplicity of phase angles in ZM. It is negative or positive.

5.3. Gabor filter algorithm

Entity encoding was implemented by convolving the normalized iris model with 1D Log-Gabor wavelets [41]. The 2D normalized model is decomposed into a number of 1D signals, then these 1D signals are convoluted with 1D Gabor wavelets. The lines of the normalized 2D model are taken as the 1D signal, each line corresponds to a circular ring on the iris region [42] and [43]. The angular direction is taken rather than the radial direction, which corresponds to the columns of the normalized model, since the maximum independence occurs in the angular direction.

The intensity values at the known noise areas in the normalized pattern are set to the average intensity of the surrounding pixels to prevent the influence of noise in the filter output. The output of the filtering is then quantized in phase to four levels using the Daugman method [14] and [44], each filter produces two data bits for each phasor. The output of the phase quantization is chosen to be a gray code, so that when moving from one quadrant to another, only one-bit changes. This will minimize the number of bits in disagreement, considering that two intra-class models are slightly offset and thus provide more accurate recognition.

The encoding process produces a bit pattern containing a number of information bits and a noise mask corresponding to corrupted areas in the iris pattern, and marks the bits in the pattern as corrupt. Since the phase information will be meaningless in the regions where the amplitude is zero, these regions are also marked in the noise mask [42].

The total number of bits in the model will be the angular resolution multiplied by the radial resolution, multiplied by 2, multiplied by the number of filters used. The number of filters, their central frequencies and the parameters of the modulating Gaussian function will be chosen in order to obtain the best recognition rate.

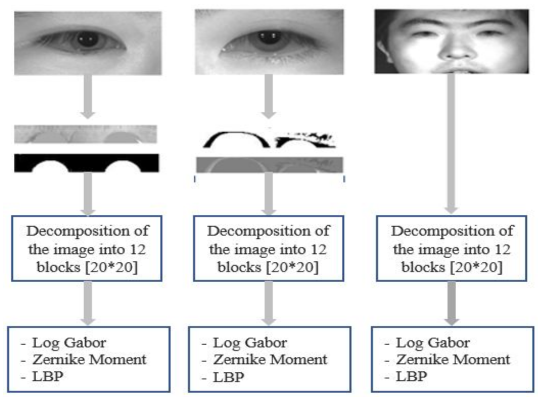

Fig. 4. Different steps and methods necessary for the construction of the recognition system

6. Modeling of the Local Fusion of the Characteristics

We are designing a multimodal fusion framework for face and iris images. Concretely, we first extract three types of local visual characteristics, in particular the function of the Gabor Filter, the Zernike Moment function and the function of the LBP [45] and [46]. Next, we build a block based on a feature-image matrix to collect all the local features of the image.

Finally, we extract compact blending functions based on the 2D image matrix directly using 2D-PCA method, which can extract more efficient image features than traditional PCA.

(a) The vector $F_B^i = [FG_i, FH_i, FL_i]^T$ designates the local characteristic vector of the i^{th} face image block.

(b) The vector $Ft_B^i = [FtG_i, FtH_i, FtL_i]^T$ designates the local characteristics of the i^{th} block of images of the iris.

Where: $i \in \{1, \dots, K\}$

K denotes the block number of the face image and the iris image.

The extraction of the visual characteristics of the local fusion of the multimodal biometric image is shown below:

$$X = \left[F_B^1, F_B^2, \dots, F_B^k, Ft_B^1, Ft_B^2, \dots, Ft_B^k\right]_{K*2K} \quad (8)$$

This matrix is constructed by all the local characteristics of the image blocks of K faces and 2K irises.

7. Matching and Decision Module

Hamming distance gives a measure of the number of bits that are identical between two binary data strings. Using the Hamming distance, a decision can be made as to whether the two strings were generated from different irises or from the same model [47].

Since an individual iris region contains features with high degrees of freedom, each iris region will produce a binary data string which is independent of that produced by another iris. On the other hand, two iris codes produced by the same iris will be strongly correlated.

The Hamming distance will be calculated using only the bits generated from the true region of the iris. The modified Hamming distance formula is given by:

$$HD = \frac{\sum_{j=1}^{N} X_j (xor) Y_j (and) X'_{nj} (and) Y'_{nj}}{N - \sum_{k=1}^{N} X_{nk} (or) Y_{nk}} \quad (9)$$

Where:
X_j and Y_j are the two-bit patterns to compare
X_{nj} and Y_{nj} are the corresponding noise masks for X_j and Y_j
N is the number of bits represented by each pattern.
Although, theoretically, two iris models generated from the same iris have zero Hamming distance. In the practical case, this will not happen. Normalization is not perfect, and there will also be some noise that will not be detected, so variation will be present when comparing two intra-class iris models.

8. Simulation and Discussion of the Results of Multimodal Fusion

8.1. Iris recognition system

The simulation results of the iris recognition algorithm were satisfactory. We obtained a recognition rate equal to 83%.

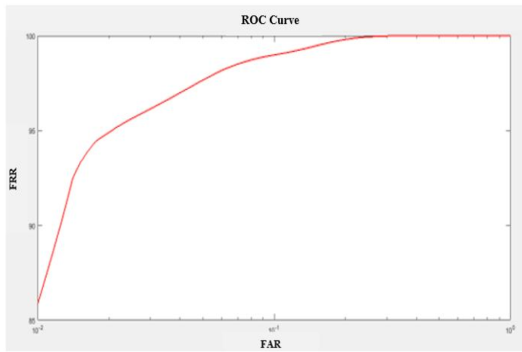

Fig. 5. Iris recognition system ROC curve

8.2. Face recognition system

The simulation results of the facial recognition algorithm were satisfactory with a recognition rate equal to 75%.

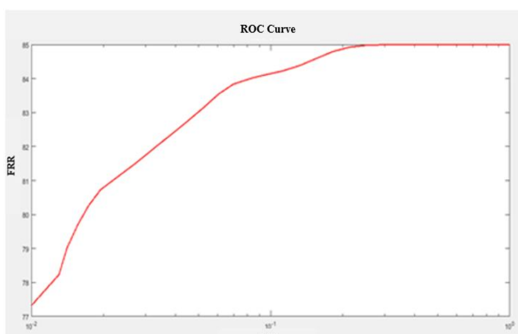

Fig. 6. Facial recognition system ROC curve

8.3. Merger of the two modalities

To achieve a powerful and robust bimodal biometric system, with a low EER value, we chose for the iris segmentation the method based on the Hough transform and for the normalization, we applied the Rubber Sheet model.
These steps have been the subject of a study developed in [48]. For the extraction of face features and Iris, we chose three algorithms in order to retain as much useful information as possible to increase the recognition rate. Next, we applied the merge at the feature level. The resulting matrix was processed by the PCA algorithm to compress the features and reduce the size of the feature matrix.
In order to provide accurate recognition of individuals, the most discriminating information present in a model must be extracted. Only the significant characteristics will be coded in order to be able to perform comparisons between the models.
The model generated in the feature encoding process will also need a correspondence metric, which performs a similarity measurement between two iris models. As mentioned in section 7, this metric gives a range of values when comparing models generated from the same

individual, in this case we speak of an intra-class comparison, and another range of values when comparing models created from different samples, in this case, they are comparisons between classes. These two cases give distinct and separate values, so that one can make a decision with great confidence whether the two models are from the same person or not.

The simulation results on MATLAB of the recognition system after fusion of the two modalities, iris and face, gave the results illustrated by the following figures.

We obtained a recognition rate equal to 88%.

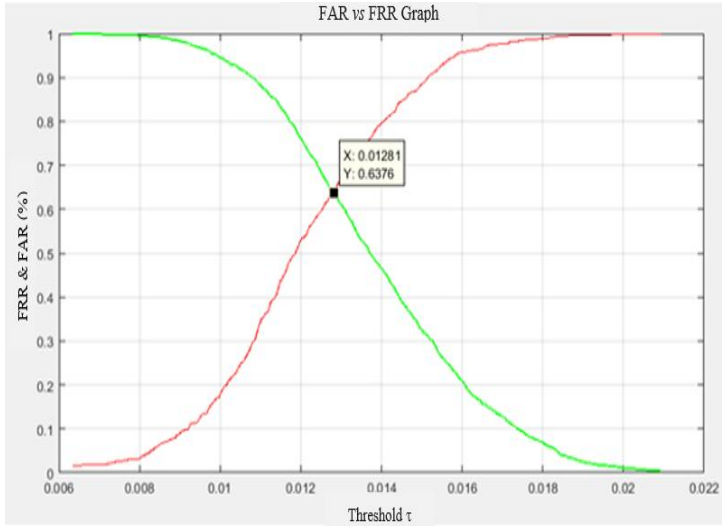

Fig. 7. Illustration of FRR and FAR as a function of the threshold value

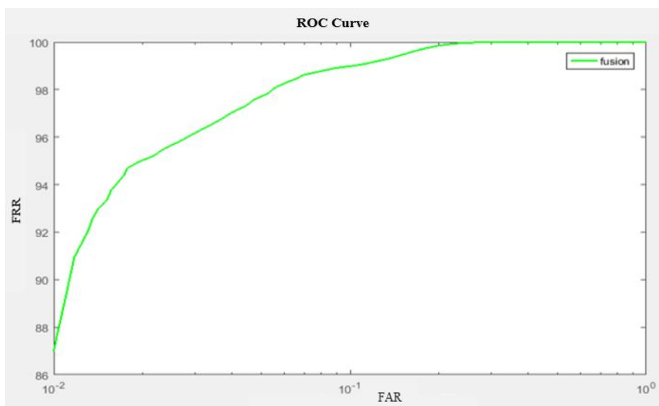

Fig. 8. ROC curve after merger of the two modalities: face and iris

9. Evaluation of the Multimodal Face and Iris Authentication System

From the figure **7** and **8**, we notice that the verification method based on the bimodal fusion of the iris and the face where we used new feature extraction algorithms (presented previously), gave a result with an EER = 0.6% for a threshold "τ = 0.6376" and the evaluation by the ROC curve shows that for a FAR = 12% we have 100-FRR = 88%. This method offers both speed, simplicity and also better performance.

Finally, at the end of this comparison between the performance of unimodal and multimodal systems, we will formulate managerial recommendations in the light of the findings which show that multimodal systems guarantee better individual recognition. This observation is in line with many works developed in the literature.

10. Conclusion

Bimodal recognition systems are characterized by their high recognition performance. However, errors of the type false acceptances or must reject are due to the consequences of errors coming from the sub-processes which govern the progress of the identification system.

In this work, we are interested in the measurement of performance metrics of unimodal and bimodal biometric systems. We performed a comparative study of three biometric systems. The first is an iris-based single-mode biometric recognition system. We obtained in simulation a recognition rate of 83%. For the second system which uses the face as a modality, we obtained a recognition rate of 75%. Then, we merged the two in order to achieve a robust recognition system with better performance. We confirmed the reliability of the bimodal recognition system based on the two modalities. By comparing the performance of each of the previous systems, we noticed an increase in the recognition rate to 88%.

These results are very encouraging and show the efficiency of the descriptors used for feature extraction, namely, LBP, Zernike Moment and Gabor Filter.

The main constraints encountered are related to the calculation time to develop certain algorithms. In everyday life, the computing time for such identification systems is a parameter that is very important for practical and commercial reasons. Hence the major interest of researchers in developing these systems and automating them to achieve reliable recognition systems operating in real time.

As a perspective, it is possible to realize this bimodal system on FPGA type electronic components to overcome the constraints of space and real-time processing.

References

[1] Morizet, N, "*Biometric Recognition by Multimodal Fusion of the Face and the Iris*", PhD Thesis in Signal and Images, National Higher School of Telecommunications, Doctoral School of Computer Science, Telecommunications and Electronics, Paris, France, (2009).

[2] Allano, L, "*Multimodal biometrics: score fusion strategies and dependency measures applied to databases of virtual people*", PhD Thesis in Image and Signal Processing, National Institute of Telecommunications, Sitevery Doctoral School, France, (2009).

[3] Mellakh, A, "*Recognition of faces in degraded conditions*", PhD Thesis in Image and Signal Processing. Department of Electronics and Physics. National Institute of Telecommunications, Sitevery Doctoral School, France, (2009).

[4] Ly Van, B, "*Realization of an on-line Handwritten Signature Verification System Independent of the Acquisition Platform*", PhD Thesis in Optimization and Safety of Systems. National Institute of Telecommunications, Doctoral School of Technological and Organizational Systems Sciences, France, (2005).

[5] Gauthier, JM, "*Legal framework for the use of Biometrics in Quebec: Security and Privacy*", Master's Thesis (LLM), Information Technology Law, Public Law Research Center, Faculty of Law, University of Montreal, Canada, (2014).
Available from: http://hdl.handle.net/1866/11879

[6] Belguechi, RO, "*Security of Biometric Systems: Revocability and Protection of Privacy*", PhD Thesis in Computer Science, National School of Computer Science, Algeria, (2015).

[7] Belguechi, RO, Cherrier, E, and Rosenberger, C, "*How to Evaluate Transformation Based Cancelable Biometric Systems?*" in NIST International Biometric Performance Testing Conference (IBPC), Gaithersburg, United States, Computer, Image and Instrumentation Research Group of Caen, (2014).
Available from: https://hal.archives-ouvertes.fr/hal-00993469.

[8] Belguechi, RO, Lacharme, P, and Rosenberger, C, "*Enhancing the privacy of electronic passports*", in International Journal of Information Technology and Management (IJITM), Special Issue on Advances and Trends in Biometrics, Inderscience, Vol. 11, Nos. 1-2, (2011), pp. 122-137.

[9] Ratha, NK, Connell, JH, and Bolle, RM, "*Enhancing security and privacy in biometrics-based authentication systems*", IBM Systems Journal, Print ISSN: 0018-8670, Vol. 40, No. 3, (2001), pp. 614-634.
Doi:10.1147/sj.403.0614.

[10] Perronnin, F, and Dugelay, JL, "*Introduction to biometrics - Authentication of individuals by audio-video processing*", Institute of Eurecom Multimedia Communications Department, Signal Processing Review, Vol. 19, No. 4,

(2002).

[11] Buhan, L, Kelkboom, E, and Simoens, K, "*A survey of the security and privacy measures for anonymous biometric authentication systems*", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), (2010). Doi:10.1109/IIHMSP.2010.91.

[12] Wang, Y, Tan, T, and Jain, AK, "*Combining Face and Iris Biometrics for Identity Verification*", in Proceedings of Fourth International Conference on Audio and Video Based Biometric Person Authentication (AVBPA), Vol. 2688, (2003), pp. 805-813. Doi:10.1007/3-540-44887-X 93.

[13] Gurban, M, and Thiran, JP, "*Basic Concepts of Multimodal Analysis*", Federal Institute of Technology in Lausanne, Switzerland, Multimodal Signal Processing, Theory and Applications for Human – Computer Interaction, Elsevier Ltd, Handbook Part II, Chapter 7, (2010), pp. 145-152.

[14] Daugman, JG, "*Combining Multiple Biometrics*", The Computer Laboratory, Cambridge University, (1998). Available from: http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html

[15] Hong, L, Jain, A, and Pankanti, S, "*Can multibiometrics improve performance?*" Proceedings of the IEEE Workshop on Automatic Identification Advanced Technologies, (1999), pp. 59-64.

[16] Hernández-Orallo, J, *Flach, PA, and Ferri* Ramirez, C, "*A unified view of performance metrics: translating threshold choice into expected classification loss*", Journal of Machine Learning Research, Vol. 13, (2012), pp. 2813-2869.

[17] El Abed, M, "*Evaluation of Biometric Systems*", PhD Thesis in Computer Science and Applications, University of Caen Basse-Normandie, France, (2011). HAL Id: tel-01007679.

[18] Perronnin, F, and Dugelay, JL, "*Introduction to biometrics - Authentication of individuals by audio-video processing*", Signal Processing, Vol. 19, No. 4, (2002).

[19] Powers, DMW, *"Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedeness & Correlation",* International Journal of Machine Learning Technology, Vol. 2, No. 1, (2011), pp. 37-63.

[20] Powers, DMW, *"ROC-ConCert: ROC-Based Measurement of Consistency and Certainty*", *Spring Congress on Engineering and Technology (SCET), IEEE,* Published in Spring Congress on Engineering and Technology, (2012), pp. 238-241. Doi:10.1109/SCET.2012.6342144.

[21] *Fawcett, T, "An Introduction to ROC Analysis*", Pattern Recognition Letters, Vol. 27, No. 8, (2006), pp. 861-874. Doi:10.1016/j.patrec.2005.10.010.

[22] *Powers, DMW, "The Problem of Area Under the Curve",* International Conference on Information Science and Technology, Published in: IEEE International Conference on Information Science and Technology, (2012). Doi:10.1109/ICIST.2012.6221710.

[23] Fogarty, J, Baker, SR, and Hudson, SE, *"Case Studies in the use of ROC Curve Analysis for Sensor-Based Estimates in Human Computer Interaction*", ACM International Conference Proceeding Series, Proceedings of the Graphics Interface , (2005). Doi:10.1145/1089508.1089530.

[24] Hand, DJ, *"Measuring classifier performance: A coherent alternative to the area under the ROC Curve*", Machine Learning, Springer Science & Business Media, LLC , Vol. 77, (2009), pp. 103-123. Doi:10.1007/s10994-009-5119-5.

[25] Flach, PA, Hernández-Orallo, J, and Ferri Ramirez, C, "*A coherent interpretation of AUC as a measure of aggregated classification performance*", in Proceedings of the 28th International Conference on Machine Learning, Bellevue, WA, USA (ICML-11), (2011), pp. 657-664.

[26] Navratil, J, and Klusacek, D, *"On Linear DETs",* IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07. Vol. 4, (2007), pp. IV.229-IV.232.

[27] *Chakraborty, DP, "Observer Performance Methods for Diagnostic Imaging: Foundations, Modeling, and Applications with R-Based Examples*", CRC Press, 2019, 1st Edition, (2021) by CRC Press, 590 Pages, Available on Taylor & Francis eBooks.

[28] Tan, T, He, Z, and Sun, Z, "*Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition*", Image and Vision Computing, Vol. 28, No. 2, (2010), pp. 223-230. Doi:10.1016/j.imavis.2009.05.008.

[29] Sun, Z, and Tan, T, "*Ordinal measures for iris recognition*", in IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 31, No. 2, (2009), pp. 2211-2226.

[30] Ma, L, Wang, Y and Tan, T, "*Iris recognition using circular symmetric filters*", in Proceedings of the 16th International Conference on Pattern Recognition ICPR, (2002), pp. 414-417.

[31] Zhu, Y, Tan, T, and Wang, Y "*Biometric personal identification based on iris patterns*", in Proceedings of the 15th International Conference on Pattern Recognition ICPR-2000, (2002), pp. 801-804. Doi:10.1109/ICPR.2000.906197.

[32] Wildes, RP, "*Iris recognition: an emerging biometric technology*", in Proceedings of the IEEE, Vol. 85, No. 9, (1997), pp. 1348-1363.

[33] Kienzle, W, Bakir, GH, Franz, MO, and Schölkopf, B, "*Face Detection – Efficient and Rank Deficient*", Conference Advances in Neural Information Processing Systems 17 (NIPS), (2004).

[34] Tisse, CL, Martin, L, Torres, L, and Robert, M, "*Person identification technique using human iris recognition*", in Proceedings of Vision Interface, (2016), pp. 294-299. Available from: https://hal-lirmm.ccsd.cnrs.fr/lirmm-00269539

[35] Hou, Y, He, Y, and Evangelia, MT, "*Iris feature extraction method based on LBP and chunked encoding*", Seventh International Conference on Natural Computation, (2011). Doi:10.1109/ICNC.2011.6022302.

[36] Julsing, BK, "*Face Recognition with Local Binary Patterns*", Bachelor Assignment, University of Twente, Department of Electrical Engineering, Mathematics & Computer Science (EEMCS), Signals & Systems Group (SAS), Report Number: SAS008-07, (2007).

[37] Rao, B, Vara, D, and Pavan, C, "*Feature Extraction Using Zernike Moments*", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2, No. 2, (2013), pp. 228-234, e-ISSN: 2278-621X.

[38] Khotanzad, A, and Hong, YH, "*Invariant image recognition by Zernike moments*", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 12, No. 5, (1990), pp. 489-498.

[39] Hero, AO, O'Neill, J, and Williams, WJ, "*Moment matrices for recognition of spatial patter in noise images*", in Proceedings of International Conference on Image Processing, (2002).

[40] Armastrong, L, Leng, J, and Diepeveen, D, "*Zernike Moments and Genetic Algorithm: Tutorial and Application*". British Journal of Mathematics and Computer Science, Vol. 4, No. 15, (2014), pp. 2217-2236. Doi:10.9734/BJMCS/2014/10931.

[41] Perlibakas, V, "*Face Recognition using Principal Component Analysis and Log-Gabor Filters*", Computer Science, Computer Vision and Pattern Recognition, (2006).

[42] Jones, JP, and Palmer, LA, "*An evaluation of the two-dimensional Gabor filter model of simple receptive fields in cat striate cortex*", JNP Journal of Neuro Physiology, Vol. 58, No. 6, (1987), pp. 1233-1258. Doi:10.1152/jn.1987.58.6.1233.

[43] Kovesi, P, "*What are Log-Gabor Filters and why are they good?*" School of Computer Science & Software Engineering, The University of Western Australia, (2000). Available from: http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/PhaseCongruency/Docs/convexpl.html

[44] Daugman, JG, "*High confidence recognition of persons by rapid video analysis of iris texture*", European Convention on Security and Detection, (1995), pp. 244-251. Doi:10.1049/cp:19950506.

[45] Sanderson, C, and Paliwal, KK, "*Identity verification using speech and face information*", Digital Signal Processing, Vol. 14, No. 5, (2004), pp. 449-480. Doi:10.1016/j.dsp.2004.05.001

[46] Nandakumar, K, "*Multibiometric Systems: Fusion Strategies and Template Security*", PhD Thesis, Computer Systems Management and Standards Anatomy and Physiology, Michigan State University East Lansing Department of Computer Science and Engineering, (2008).

[47] Libor, M, "*Recognition of Human Iris Patterns for Biometric Identification*", Computer Science and Software Engineering Report. The University of Western Australia, Australia, (2003).

[48] Allam, FZ, Bousbia-Salah, H, & Hamami, L, "*Modeling of Biometric Recognition Based on Human Visual System*". International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, Nos. 1-2, (2020), pp. 198-204.

Follow This Article at The Following Site:

Allam F Z, Hamami -Mitiche L, Bousbia-Salah H. Evaluation and Comparison of the performance of Biometric Recognition. IJIEPR. 2022; 33 (1) :1-12
URL: http://ijiepr.iust.ac.ir/article-1-1385-en.html