Applied Computer Systems
ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
June 2023, vol. 28, no. 1, pp. 58–65
https://doi.org/10.2478/acss-2023-0006
https://content.sciendo.com

Multimodal Biometric System Based on the Fusion in Score of Fingerprint and Online Handwritten Signature

Toufik Hafs[1*], Hatem Zehir[1], Ali Hafs[2], Amine Nait-Ali[3]
[1] *LERICA, Dept. Electronics, Badji Mokhtar Annaba University, Annaba, Algeria*
[2] *Department of Physics, University of Chadli Bendjedid, El Tarf, Algeria*
[3] *LISSI, University of Paris, Créteil, France*

***Abstract* – Multimodal biometrics is the technique of using multiple modalities on a single system. This allows us to overcome the limitations of unimodal systems, such as the inability to acquire data from certain individuals or intentional fraud, while improving recognition performance. In this paper, a study of score normalization and its impact on the performance of the system is performed. The fusion of scores requires prior normalisation before applying a weighted sum fusion that separates impostor and genuine scores into a common interval with close ranges. The experiments were carried out on three biometric databases. The results show that the proposed strategy performs very encouragingly, especially in combination with Empirical Modal Decomposition (EMD). The proposed fusion system shows good performance. The best result is obtained by merging the globality online signature and fingerprint where an EER of 1.69 % is obtained by normalizing the scores according to the Min-Max method.**

***Keywords* – Empirical mode decomposition (EMD), fingerprint, image and signal processing, Min-Max, multibiometrics, online handwritten signature, scores fusion, weighted sum.**

I. Introduction

Determining automatically the identity of individuals is more than a necessity in today's world. For example, it is imperative to recognise a person to give him access to a building or sensitive information. That is why researchers today are developing robust security systems that are invulnerable to fraud and spoofing.

The technique used today such as Postal Index Number (PIN) code and passwords does not meet the minimum security threshold by today's standards. For these reasons a more robust mechanism for identification and identification based on something that cannot be stolen, reproduced, forgotten, falsified, and copied namely biometrics, is more than necessary. Biometrics is defined as the science of identifying an individual based on one or more of their characteristics, these characteristics are unique to each individual and can be classified as physical modalities such as fingerprint [1], iris [2], and palm print [3]; and behavioural modalities such as signature [4], keystroke [5], and speech [6]. Figure 1 shows the classification of biometric modalities.

Biometric modalities are more secure as they verify the following requirements:

- Universal: they can be recorded on each individual;
- Unique: different between two individuals;
- Permanent: does not change over time;
- Measurable: inexpensive and non-intrusive;
- Precise: little confusion between individuals;
- Difficult to reproduce.

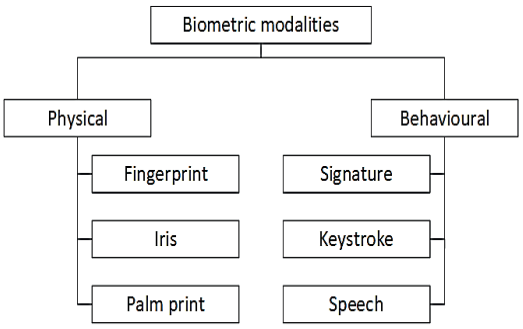

Fig. 1. Biometric modalities.

Unfortunately, in real-life use cases, no modality satisfies all of these requirements at once. Due to the limitations of unimodal systems, multimodality is gaining popularity, especially in high-security applications. That is why multimodal biometric systems are considered superior to any other security system.

There are four main techniques used for biometric modalities fusion and they are classified according to their level on the system: sensor level, feature level, decision level, and score level.

However, biometrics is not as recent as one might think. Its appearance dates back to the 19th century when fingerprints were used by the judicial police to identify people guilty of committing crimes. Since then, this use has never been

* Corresponding author's e-mail: hafstoufik@gmail.com

abandoned, and this identification technique is still being used in a more automated way. In the face of the many limitations imposed by the use of unimodal biometric systems, multimodal biometrics is undeniably emerging as a future alternative in the field of personal and property security. Although biometric systems can be linked at different levels as discussed earlier and as shown in Fig. 2, score-level fusion is the most common, as it has been generally proven to be more effective than the rest of the fusion levels.

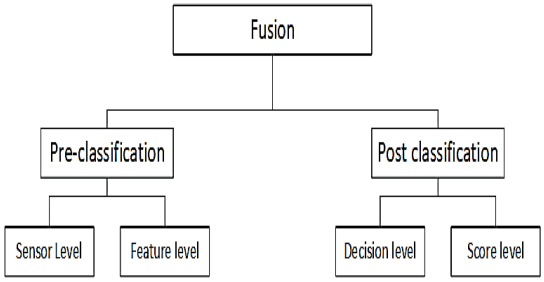

Fig. 2. The different fusion Levels.

In this research paper, we will develop a multimodal biometric system based on two modalities of two different types, the first one is the signature which is a physical modality, and the second one is the fingerprint which is a behavioural one. These two systems will be studied and processed separately and then will be fused in the score level. In this paper, we are going to be particularly interested in the score-level fusion of biometric data. The major contribution of this paper is the development of a new approach based on empirical modal decomposition for handwritten signatures and a structural approach based on minutiae extraction for fingerprints. These approaches allow us to take into account the possible interactions between unimodal biometric systems. The rest of this paper is organised as follows: in Section II, related studies are discussed. Section III describes the proposed system. Section IV discusses the experimental findings, and finally, Section V presents the conclusion and the prospects of this paper.

II. Related Work

Many researchers have studied and implemented two or more modalities in the same biometric system. Leghari et al. [7] introduced a novel method for the fusion of fingerprints and online signatures, they used 1400 samples for online signatures and the same number of samples for fingerprints collected from 280 different individuals. In their research paper, they developed a convolutional neural network (CNN) that can classify the features of the modalities. Two types of fusion were used. The first one is early fusion which achieved an accuracy of 99.10 %, and the second one is late fusion and it achieved a performance of 98.35 %. In the early fusion, the features of the online signature and fingerprint are combined before the fully connected layer, while in the late fusion the features of the two modalities are combined after the fully connected layers. Similarly, Abd El-Rahiem et al. [8] combined the features of the electrocardiogram signal (ECG) and finger vein; they applied filters and pre-processing techniques adapted to each modality, proposed a convolutional neural network for extracting the features used in the authentication process by means of five of the most known classifiers: Support Vector Machine (SVM), K-Nearest Neighbors (KNNs), Random Forest (RF), Naive Bayes (NB), and Artificial Neural Network (ANN). The researchers used two different databases for each modality: TW finger vein and VeinPolyU finger vein databases for the finger vein, and for the ECG, MWM-HIT and ECG-ID databases were used. The system achieved an Equal Error Rate (EER) of 0.12 % using feature fusion and an EER of 1.40 % using score fusion.

Labayen et al. [9] proposed a multimodal system for online student authentication based on facial recognition, voice recognition, and keystroke dynamics. The researchers tested their system in three different universities and two training centres on three different continents and through more than 50 activities, all the test images collected from the students contained at least 80 % of the face area and the signal-to-noise ratio (SNR) captured from the microphones was low enough to allow voice recognition. The number of samples used was as follows: 373 410 images, 1007 audio clips, and 653 keystrokes. The results achieved are described in Table I.

TABLE I
System Performance [9]

	Image processing		Audio processing	
	Precision	Recall	Precision	Recall
Authentication	0.998	0.865	0.964	0.667

As the researchers calculated the recall and the precision only on the fully labelled database, the keystroke performances of the system were not presented in the above table as the features of this modality could not be labelled manually.

III. Proposed System

This section is dedicated to the presentation of our proposed multimodal authentication system. The different stages of our system will be discussed in depth: the applied pre-processing, the extracted features, and the comparison method. The diagram block of the proposed system is illustrated in Fig. 3.

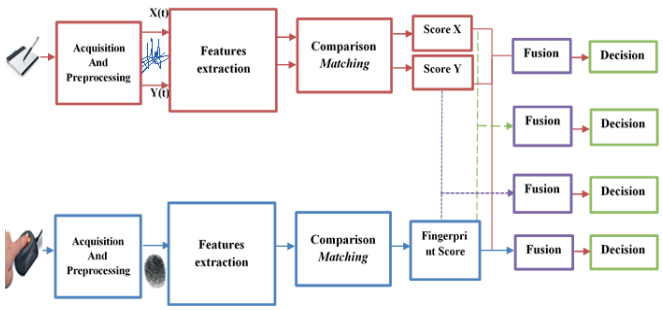

Fig. 3. Architecture of the proposed multimodal biometric authentication system.

A. Databases Used for the Evaluation

For the evaluation of the proposed system, we have used three different databases: one online signature database, one fingerprint database, and one bimodal database for both fingerprint and signature. The use of multiple databases allows us to have more data and also test if the proposed method has a good generalization.

The first used database is the publicly available MYCT-100 [10], the creators of this database have used a WACOM pen tablet to collect, model INTUOS A6 USB to collect the signatures data at a sampling rate of 100 Hz. The tablet has a capture area of 127×97 mm², and a resolution of 2540 lines per inch, which is equivalent to 5080 dots per inch (dpi). The device has a precision of ±0.25 mm. While collecting the signatures each participant was asked to give for 5 different groups 5 genuine signatures and 5 skilled forgeries of another participant. Hence, each contributor ends up with 25 genuine signatures and their signature is forged 25 times. The total number of signers is 330 but only the online signatures of 100 individuals are freely available to download. As a result, our method was tested by using 2500 genuine online signatures and 2500 skilled forgeries.

The second used database is the SVC2004 [11]; it consists of a total of 100 sets, each set contains 20 genuine signatures collected from a single user and 20 skilled forgeries collected from at least 4 other participants. From the 100 collected sets, only 40 are released to the public. The data were collected from two sessions using the WACOM Intuos tablet; in each session the participant was asked to contribute 10 genuine signatures, and the second session was held one week after the first one. As mentioned earlier, the skilled forgeries are collected from at least 4 different contributors and are collected using the following method: each signature forger can see the signature to forge on a computer screen, the skilled forgeries collection was not started until the participant practised his skilled forgery and became convinced that they completely mastered it. For the fingerprint part, the data were acquired using two sensors. The first is the 100SC capacitive sensor with a resolution of 500 dpi. The second is the UareU optical sensor, which also has a resolution of 500 dpi. The output size is 300×300 pixels and 256×400 pixels for both sensors, respectively. Ten fingerprint samples were collected from each volunteer.

To allow the evaluation of the system under different conditions, each sample was acquired 12 times: 3 times in low resolution, 3 times in medium resolution, and 6 times in high resolution. Each user provided a total number of 240 fingerprint images to the database.

The third used database is the FVC 2004 [12], [13]. For this database, the data were collected using a CrossMatch V300 optical sensor, which has a resolution of 500 dpi, a Digital Persona U.are.U 4000 optical sensor, which also has a resolution of 500 dpi, an Atmel FingerChip thermal sweeping sensor, which has a resolution of 512 dpi, and a SFinGe v3.0, which has a resolution of about 500 dpi. The fingerprints were recorded from 90 volunteer students partitioned randomly into 3 groups of 30 participants each. A different sensor was used to acquire fingerprint data from each group. The data were collected from participants in three different sessions separated by at least a two-week period, four impressions of four different fingers (forefinger and middle finger of both hands) of each user were recorded at each session. The total number of gathered finger impressions was 1440 from 30 volunteers. Examples of fingerprint images from this database are illustrated in Fig. 4.

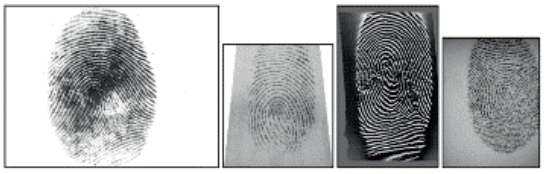

Fig. 4. Architecture of the proposed multimodal biometric authentication system.

B. Online Signature Authentication System

In the proposed signature authentication system, we used the same method as the one proposed by [4]. First, the $x(t)$ and $y(t)$, which represent the position coordinates of the signature are extracted to be pre-processed and prepared for the features extraction stage. The feature extraction is done using an algorithm developed by Huang et al. [14] called empirical modal decomposition. Then comes the comparison step between the parameters extracted from these coordinates and those of the reference signature coordinates where two similarity scores are obtained.

• *Pre-processing and Enrolment Phases*

The main goal of the pre-processing stage is to eliminate the noise and clean the data. This can be done in two steps, the first one is removing the noise due to the pen shaking and this is done by applying a one-dimensional Gaussian low-pass filter with 10 Hz as the cut-off frequency and a distance filter, which is used for sampling the data while maintaining its original shape. The second step consists of normalizing the data in position, this is done by aligning signatures according to their centre of gravity, in size. After this process, all the signatures will have the same fixed size and length, the main goal of this process is to reduce the signature file size which allows for a better data processing time and less storage usage. The user's profiles are created during the enrolment phase. We took the first five signatures of the two used databases: SVC2004 and MYCT-100 and used them to define reference signatures while the remaining signatures were used for testing the system. All of the first five signatures were first pre-processed as described before. After that, the reference signature was determined by averaging the first five signatures according to the following expression:

$$S_{\text{ref}} = \frac{S_1 + S_2 + S_3 + S_4 + S_5}{5}. \quad (1)$$

Figure 5 shows the reference signature alongside the first five signatures of the database.

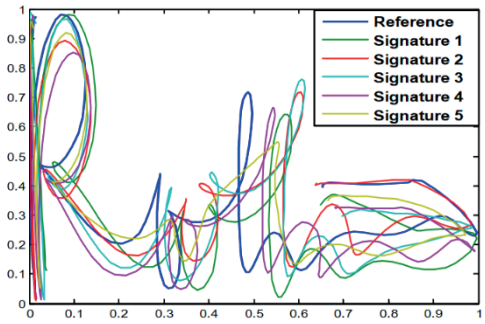

Fig. 5. Reference signature [4].

• *Test and Decision Phases*

The main goal of this stage is to successfully identify users, but before going through the process of identification we need first to extract the most significant features from the data using the empirical mode decomposition (EMD) [14], which is a time-frequency analysis tool that decomposes a time-series signal into multiple intrinsic mode function (IMF) using a sifting process.

Each IMF must obey two rules:

– The difference between maxima and minima cannot be larger than one;
– The mean value of an IMF is equal to zero.

This algorithm is calculated as showed in Fig. 6.

A stop criterion (SD) is set at a certain point to make sure that the iterative algorithm converges.

The threshold between two consecutive siftings is defined by this equation:

$$SD = \sum \left| E_{j-1} \quad (t) \right| \leq \varepsilon . \tag{2}$$

The value of ε is generally fixed at 0.2 or 0.3 [16], in our experience, we are using an *SD* of 0.2 [17].

When the EMD algorithm finishes the execution, we obtain a set of IMFs and a residue, this residue represents the DC components of the signal. The output signal is described mathematically as follows:

$$S(t) = r(t) + \sum_{i=1}^{n} IMF_i(t) , \tag{3}$$

where $x(t)$ and $y(t)$ are the position coordinates that represent the used online signature signals.

The EMD is applied to both of these components and the result is used to create a new vector (*VEMD* = [*IMFx*, *IMFy*]).

Those parameters will allow us to recreate and decompose the original signature. The recorded *IMF*s occupy a large volume, which implies that the *VEMD* cannot be used for signature characterization.

For this reason, we used the same algorithm as Rilling et al. [18] to locate the minima and maxima of the *IMF*s of each signature, those extracted parameters are then used to create a new vector *VemdN*.

The decision stage aims to obtain a comparison score between a candidate signature for authentication and the reference signature of a user.

The comparison is made by calculating the Euclidean distance between the test and reference signature reconstructed from *VemdN*.

Based on a comparison score, in this step we classify the test signatures into one of two categories: genuine or imposter.

This decision is done using the Euclidean distance between both rebuilt test and reference signatures.

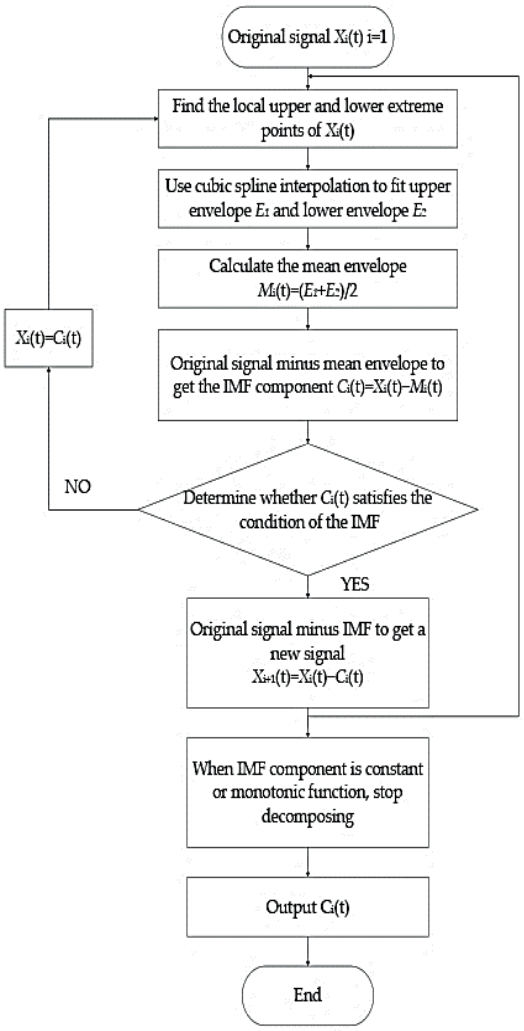

Fig. 6. EMD algorithm [15].

C. Fingerprint Authentication System

Our fingerprint authentication system is essentially composed of five basic steps, which are: acquisition, pre-processing, feature analysis or extraction, learning and comparison or matching. Here is a synoptic diagram that gives an overview of the steps in our system.

Now we will develop the steps of this system as well as the sub-operations performed in each step.

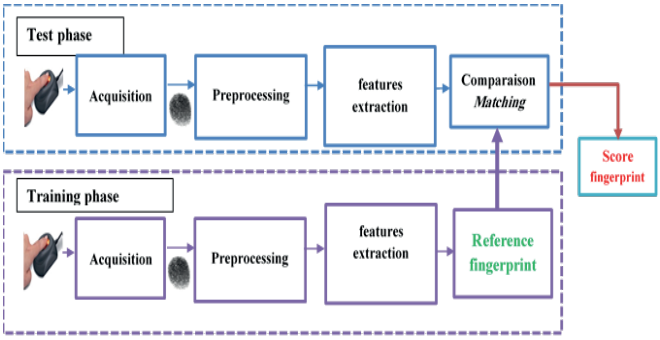

Fig. 7. General architecture of our fingerprint authentication system.

• *Acquisition and Pre-processing Phases*

In our work, we used the famous database provided by FVC 2004 (Fingerprint Verification Competition 2002) [13], as well as the bimodal database MCYT (fingerprint and signature) [10].

The aim of the pre-processing phase is to make the image clearer to facilitate further operations. These preliminary pre-processing methods aim to connect the broken points. The first step in this stage is histogram equalization, which consists of widening the distribution of pixel values in an image in order to increase the perceptual information. The histogram after equalisation occupies the whole range from 0 to 255. The second step is enhancing the fingerprints using the Fourier transform, after that, we binarise the fingerprint image, which is naturally 8-bit and grayscale, to a single-bit image with the assignment of the value "0" for striations and the value "1" for valleys. The last step of this stage is segmentation and extraction of the region of interest (ROI), the ROI is useful for the authentication process because it contains the discriminating information. To extract this region, two steps are necessary. The first one is the estimation of the direction block [19], while the second one is performed using some morphological methods called "opening" and "closing". The opening operation expands the image and removes the peaks introduced by the background noise. The closing operation reduces the image and removes small cavities. The region of interest is obtained after subtracting the closed area from the open area.

• *Feature Extraction, Enrolment and Decision Phases*

The feature extraction process is done in two steps, the first step is the slimming and elimination of peaks and pauses; it consists of eliminating redundant pixels from streak to streak. It uses an iterative and parallel algorithm [20]. The second step is the extraction of minutiae.

The enrolment phase consists of defining the reference fingerprint. In our case, the first fingerprint of each user is considered the reference fingerprint. The latter will undergo all the pre-processing and analysis steps described above and we save its parameter file, which corresponds to the useful information contained in the image which is necessary for authentication. In our case, it is the list of detected and validated minutiae associated with their characteristics. For each detected and validated minutia, three characteristics are extracted:

– Type of minutia: branching or termination;
– Position of the minutia in the image: coordinates (x, y);
– The direction of the local block associated with the streak θ.

The decision phase is done as follows: given $S_{\text{ref}}(i)$ the parameter file of the reference fingerprint of the ith user and $S_{\text{test}}(i)$ the parameter file of the test fingerprint of the ith user. The Semp fingerprint scores are obtained using the Euclidean distance according to:

$$S_{\text{ref}} = \frac{1}{l}\sqrt{\sum_{i=1}^{l}(S_{\text{ref}i} - S_{\text{test}i})^2}\ . \tag{4}$$

This difference seeks to determine a score that represents the number of pairs of identical minutiae in relation to the total number of minutiae.

D. Proposed Multimodal Biometric System

We have chosen two biometric modalities of different nature: a physical one and a behavioural one, namely, the fingerprint and the online handwritten signature, respectively. The two systems are treated separately before merging them at the score level.

As described earlier, in the signature authentication system, the position coordinates ($x(t)$ and $y(t)$) of the signature are extracted and undergo the necessary pre-processing before extracting the discriminating parameters using an original algorithm called empirical modal decomposition. Then comes the comparison step between the parameters extracted from these coordinates and those of the reference signature coordinates where two similarity scores are obtained.

Furthermore, in the fingerprint authentication system, a series of pre-processing operations are applied to the raw fingerprint image in order to facilitate the extraction of the features. Then, the minutiae of the test fingerprint are compared with those of the reference fingerprint to define a similarity score.

Before entering the fusion phase, the scores from each system were normalised using three score normalisation methods: the Min-Max, Z-scores and TanH.

Several combinations of scores were implemented, firstly, we adopted an intermodal fusion between the two signature scores, and then we fused the fingerprint score with each of the signature scores. Finally, the fingerprint score was merged with the combined score between the two signature scores.

IV. Results and Discussion

Multimodal authentication systems, which merge information from several biometric sources at the score level, have gained more popularity in the field of security and specifically in the field of personal identity recognition and verification.

This is due to their ability to overcome the limitations of unimodal biometrics such as the non-universality of biometric traits, noise in biometric sensors and high intra-user variation.

In our case, we have designed a system based on two modalities of different natures, one behavioural and the other physical, in order to distinguish the impact of this choice on the performance of the system in the first place. Several fusion

combinations have been tried by our system in order to define the best possible combination in terms of performance of course.

The first two fusion experiments consist in combining the score from the fingerprint authentication system with each of the scores from the online handwritten signature authentication system ($x(t)$ score and $y(t)$ score), respectively.

We tested our system using three normalization methods (Min-Max, Z-score, TanH) and applied the weighted sum as a fusion method. Figures 8 and 9 show the results obtained after merging the fingerprint score with that of $x(t)$ and $y(t)$ respectively through the DET graph. The tests were conducted on the bimodal MCYT-100 database with three normalisation methods (Min-Max, Z-score, TanH) and without normalisation.

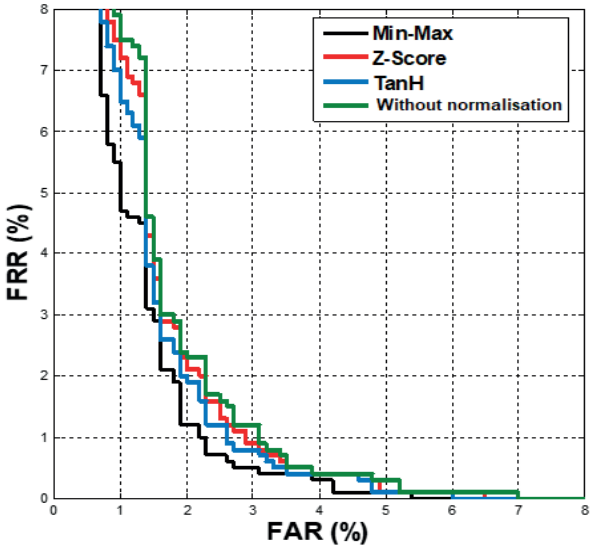

Fig. 8. The detection error tradeoff (DET) curves of the fusion between the fingerprint score and the $x(t)$ score of the online handwritten signature for the MCYT-100 databases.

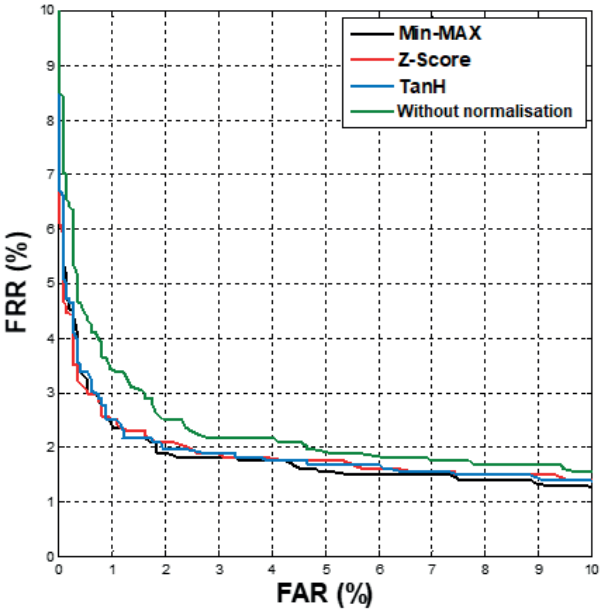

Fig. 9. The detection error tradeoff (DET) curves of the fusion between the fingerprint score and the $y(t)$ score of the online handwritten signature for the MCYT-100 databases.

Table II summarises our results after performing the two fusion combinations mentioned above and with several types of equal error rate (EER) normalisation.

The decision to accept or reject a user is based on the authentication score. This decision can be improved by normalizing the scores. The impact of normalization on performance is confirmed by our results.

TABLE II
SYSTEM PERFORMANCE

Normalization / Fusion method	EER (%)			
	min-max	Z-score	Tanh	Without Normalization
Fingerprint Score and $x(t)$ Score	1.90	2.10	2.00	2.30
Fingerprint Score and $y(t)$ Score	1.89	2.09	1.96	2.36

As can be seen in Table II, the error rates are very close to each other with a step ahead for the Min-Max method which confirms its reputation for biometric scores due to its simplicity and robustness. The error rates obtained are very encouraging compared to those obtained with unimodal systems. The last fusion combination of our system consists in combining the score from the fingerprint authentication system with that from the online handwritten signature authentication system. In fact, in this case, we are going to merge the totality of our two biometric modalities contrary to the previous case where we took only a part of our behavioural modality.

As for the two previous fusion operations, our tests were conducted on the MCYT-100 bimodal database with three normalization methods (Min-Max, Z-score, TanH) and without normalization. The comparison between the results obtained without normalisation, with the three normalisation methods of our system is illustrated as a DET curve in Fig. 10.

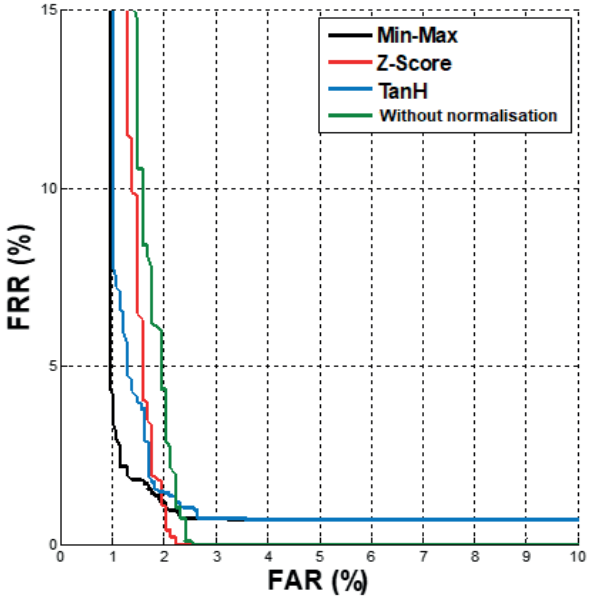

Fig. 10. The detection error tradeoff (DET) curves of the fusion.

Table III summarises our results obtained after merging the globality of our two biometric modalities (fingerprint and signature) with several normalisation types.

TABLE III
RESULTS OBTAINED AFTER MERGING THE FINGERPRINT AND THE SIGNATURE IN TERMS OF EER ON THE MCYT-100 BASE

Normalization / Fusion method	EER (%)			
	min-max	Z-score	Tanh	Without Normalization
Fingerprint and signature	1.69	1.85	1.76	2.16

We can see from Table III that the normalisation with the Min-Max method improves the decision in all cases. Moreover, an EER of 1.69 % was obtained which was a real success for our system. This success was achieved through the contribution of several factors: firstly, the efficiency of the two feature extraction algorithms (the structural approach for fingerprints and the EMD empirical modal decomposition for the online handwritten signature) as well as the choice of the normalisation and fusion method adopted by our system. Table IV summarises all our best results obtained on the MCYT-100 database. The improvement is very noticeable. We were able to make a significant improvement in the error rates, which dropped from 2.91 % to 1.69 %.

TABLE IV
SUMMARY OF THE RESULTS OBTAINED IN TERMS OF EER ON THE MCYT-100 DATABASE

Systems	EER (%)
Online handwritten signature authentication systems	2.23
Fingerprint authentication systems	2.91
Fusion of the fingerprint and $x(t)$ of the signature	1.90
Fusion of the fingerprint and $y(t)$ of the signature	1.89
Fusion of fingerprint and signature	1.69

V. CONCLUSION

In this research paper, we have proposed the tests performed and the results obtained by our novel multimodal biometric authentication system based on the fusion of fingerprint scores and online handwritten signatures. We have started by presenting the performance of our two modalities separately before performing several fusion combinations between our two considered modalities. We also performed a study of score normalization and its impact on the performance of our system. Our fusion system shows good performance. The best result is obtained by merging the globality of our two biometric modalities where we obtained an EER of 1.69% by normalizing the scores according to the Min-Max method. Thus, our fusion system performs much better compared to the unimodal systems illustrated in our work.

This study allowed us to validate the feasibility of a multimodal biometric system through the fusion of two biometric modalities: the fingerprint and the online cursive handwritten signature. By following an evaluation test protocol based on normalisation and score fusion methods (weighted sum of the two biometric modalities), we demonstrated that the adopted approach provided excellent results in terms of equal error rate (EER), and that it was capable of handling delicate situations, in particular when unimodal systems did not allow for good recognition, thus justifying the need to fuse several biometric modalities.

As a perspective, we intend to implement this bimodal system on an FPGA in order to respect the constraints of space and real-time processing and to add a module designed to secure the biometric data.

REFERENCES

[1] K. Lalović, I. Tot, A. Arsić, and M. Škarić, "Security information system, based on fingerprint biometrics," *Acta Polytech. Hung*., vol. 16, no. 5, pp. 87–100, Jul. 2019. https://doi.org/10.12700/APH.16.5.2019.5.6

[2] J. Pillai, V. Patel, R. Chellappa, and N. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell*., vol. 33, no. 9, pp. 1877–1893, Feb. 2011. https://doi.org/10.1109/TPAMI.2011.34

[3] T. Chai, S. Prasad, J. Yan, and Z. Zhang, "Contactless palmprint biometrics using DeepNet with dedicated assistant layers," *Vis. Comput*., pp. 1–19, Jul. 2022. https://doi.org/10.1007/s00371-022-02571-6

[4] T. Hafs, L. Bennacer, M. Boughazi, and A. Nait-Ali, "Empirical mode decomposition for online handwritten signature verification," *IET Biom*., vol. 5, no. 3, pp. 190–199, Sep. 2016. https://doi.org/10.1049/iet-bmt.2014.0041

[5] S. Parkinson, S. Khan, A. Crampton, Q. Xu, W. Xie, N. Liu, and K. Dakin, "Password policy characteristics and keystroke biometric authentication," *IET Biom*., vol. 10, no. 2, pp. 163–178, Mar. 2021. https://doi.org/10.1049/bme2.12017

[6] S. Dey, S. Barman, R. K. Bhukya, R. K. Das, B C Haris, S. R. M. Prasanna, and R. Sinha, "Speech biometric based attendance system," in *2014 Twentieth National Conference on Communications (NCC)*, Kanpur, India, Feb. 2014, pp. 1–6. https://doi.org/10.1109/NCC.2014.6811345

[7] M. Leghari, S. Memon, L. Dhomeja, D. Jalbani, and A. Ali, "Deep feature fusion of fingerprint and online signature for multimodal biometrics," *Computers*, vol. 10, no. 2, Feb. 2021, Art. no. 21. https://doi.org/10.3390/computers10020021

[8] B. El-Rahiem, F. Abd El-Samie, and M. Amin, "Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein," *Multimed. Syst*., vol. 28, pp. 1325–1337, Aug. 2022. https://doi.org/10.1007/s00530-021-00810-9

[9] M. Labayen, R. Vea, J. Florez, N. Aginako, and B. Sierra, "Online student authentication and proctoring system based on multimodal biometrics technology," *IEEE Access*, vol. 9, pp. 72398–72411, May 2021. https://doi.org/10.1109/ACCESS.2021.3079375

[10] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, "MCYT baseline corpus: a bimodal biometric database," *IEE Proc. – Vis. Image Signal Process*., vol. 150, no. 6, pp. 395–401, Dec. 2003. https://doi.org/10.1049/ip-vis:20031078

[11] D.-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First international signature verification competition," in *Biometric Authentication,* D. Zhang and A.K. Jain, Eds. Springer, Berlin, Heidelberg, 2004, pp. 16–22. https://doi.org/10.1007/978-3-540-25948-0_3

[12] D. Maltoni, D. Maio, A. K. Jain, and J. Feng, *Handbook of Fingerprint Recognition*. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-83624-5

[13] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition," in *Biometric Authentication*, D. Zhang and A.K. Jain, Eds. Springer, Berlin, Heidelberg, 2004, pp. 1–7. https://doi.org/10.1007/978-3-540-25948-0_1

[14] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N. Yen, C. C. Tung, and H. H. Liu., "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," *Proc. Math. Phys. Eng. Sci*., vol. 454, no. 1971, pp. 903–995, Mar. 1998. https://doi.org/10.1098/rspa.1998.0193

[15] L. Gao, X. Li, Y. Yao, Y. Wang, X. Y., X. Zhao, D. Geng, Y. Li, and L. Liu, "A modal frequency estimation method of non-stationary signal under mass time-varying condition based on EMD algorithm," *Appl. Sci*., vol. 12, no. 16, Aug. 2022, Art no. 8187. https://doi.org/10.3390/app12168187
[16] G. Rilling, "Décompositions modales empiriques. Contributions à la théorie, l'algorithmie et l'analyse de performances," Ph.D. dissertation, Ecole normale supérieure de lyon – ENS LYON, 2007. [Online]. Available: https://tel.archives-ouvertes.fr/tel-00442634. Accessed on: Oct. 23, 2022.
[17] L. Lin, Y. Wang, and H. Zhou, "Iterative filtering as an alternative algorithm for empirical mode decomposition," *Adv. Adapt. Data Anal*., vol. 1, no. 4, pp. 543–560, 2009. https://doi.org/10.1142/S179353690900028X
[18] G. Rilling, P. Flandrin, P. Gonçalves, and J. Lilly, "Bivariate empirical mode decomposition," *IEEE Signal Process. Lett*., vol. 14, no. 12, pp. 936–939, Dec. 2008. https://doi.org/10.1109/LSP.2007.904710
[19] L. Hong, "Automatic personal identification using fingerprints," Ph.D. dissertation, Michigan State University, USA, 1998.
[20] L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, and S. Tsutsui, *Intelligent Biometric Techniques in Fingerprint and Face Recognition*. USA: CRC Press, Inc., 1999.

Toufik Hafs is currently an Associate Professor at the Faculty of Technology, University of Badji Mokhtar Annaba, Algeria. He obtained his PhD in Electronics from the University of Badji Mokhtar Annaba, Algeria, in 2016. His research interests include signal processing, biometrics and transportation systems.
E-mail: hafstoufik@gmail.com
ORCID iD: https://orcid.org/0000-0003-4950-1562

Hatem Zehir is currently a PhD student in Electronics at the Faculty of Technology, University of Badji Mokhtar Annaba, Algeria. His research interests include biometrics and signal processing.
E-mail: hatemzehir@gmail.com
ORCID iD: https://orcid.org/0000-0002-3578-2634

Ali Hafs is a Full Professor at the Department of Physics, University of Chadli Bendjedid El Tarf, Algeria. His research interests include materials science and biometrics.
E-mail: hafsali2006@yahoo.fr
ORCID iD: https://orcid.org/0000-0003-4950-1562

Amine Nait-Ali was born in 1972. He received the *M.sc.* degree in Electrical Engineering "Ingénieur d'état en électronique" at the University USTO (Oran) in 1994, then the DEA degree "Diplôme des Etudes Approfondies" in Signal Processing and Automatic from the University Paris XI (1995). In 1998, he received the PhD degree in Biosignal Processing and "Habilitation à Diriger des Recherches" (HDR) from the University Paris XII, in 2007. He has been an Associate Professor and currently is a Professor at the same university. His research interests are focused on biosignal processing, biometrics, optimization, modelling and medical signal and image compression. He has co-authored a number of international peer-reviewed papers and edited and co-edited five books in the biomedical and biometrics field (Springer, ISTE-Wiley and Hermes).
E-mail: naitali@u-pec.fr
ORCID iD: https://orcid.org/0000-0002-5490-9215