ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY
Volume **27**, Number 1, 2024, 37–49

Enhancing Recognition in Multimodal Biometric Systems: Score Normalization and Fusion of Online Signatures and Fingerprints

Toufik HAFS[1,*], Hatem ZEHIR[1], Ali HAFS[2], Hanene BRAHMIA[3], and Amine NAIT-ALI[4]

[1]L.E.R.I.C.A. University of Badji Mokhtar P. Box 12, 23000 Annaba, Algeria
[2]Department of Physics ,University of Chadli Bendjedid, P. Box 73, El Tarf, 36000 Algeria
[3]LRS, Dept. computer science, Badji Mokhtar Annaba University, Algeria
[4]LISSI, University of Paris 12 Val de Marne, 61 avenue du Gnral de Gaulle 94010 Crteil France
E-mails: hafstoufik@gmail.com*, hatemzehir@gmail.com, hafsali2006@yahoo.fr, hanenebrahmia@gmail.com , naitali@u-pec.fr
* Corresponding author

Abstract. Multimodal biometrics employs multiple modalities within a single system to address the limitations of unimodal systems, such as incomplete data acquisition or deliberate fraud, while enhancing recognition accuracy. This study explores score normalization and its impact on system performance. To fuse scores effectively, prior normalization is necessary, followed by a weighted sum fusion technique that aligns impostor and genuine scores within a common range. Experiments conducted on three biometric databases demonstrate the promising efficacy of the proposed approach, particularly when combined with *Empirical Modal Decomposition* (EMD). The fusion system exhibits strong performance, with the best outcome achieved by merging the online signature and fingerprint modalities, resulting in a normalized Min-Max score-based *Equal Error Rate* (EER) of 1.69%.

Key-words: Empirical mode decomposition; fingerprints; image and signal processing; min-max; multibiometrics; online handwritten signatures; scores fusion; weighted sum.

1. Introduction

Determining automatically the identity of individuals is more than a necessity in today's world. For example, it is imperative to recognize 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 can not 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 from thw point of view of physical modalities (Fig. 1) such as fingerprints [1], iris [2] and palm print [3], and behavioral modalities such as signature [4], keystroke [5] and speech [6].

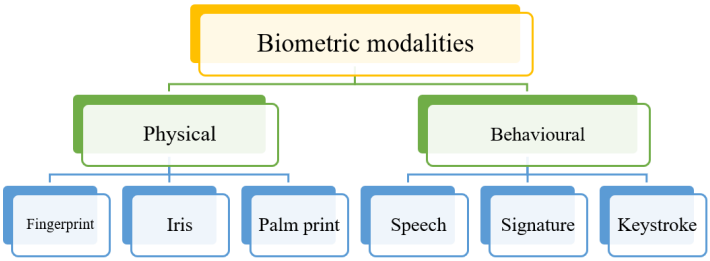

Fig. 1. Biometric modalities.

Biometric modalities are more secure as they verify the following requirements: universality, unique, permanent, measurable, precise and difficult to reproduce.

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 19^{th} century when fingerprints were used by the judicial police to identify people guilty of committing crimes. Since then, this use has never been 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 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. 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 behavioral 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. Our main contribution in this research lies

in the robust and high-performance fusion of two distinct biometric modalities: the behavioral modality of online signatures and the structural modality of fingerprints. By merging these two modalities, we introduce a novel approach that combines the strengths of both behavioral and structural characteristics in biometric recognition. This fusion methodology enhances the overall accuracy and reliability of the biometric system, offering improved performance compared to existing approaches. Our research provides valuable insights into the effective integration of diverse biometric modalities, paving the way for advancements in multimodal biometric systems. The rest of this paper is organized as follows: in Section 2, related works are discussed. Section 3 describes the proposed system. Section 4 discusses the experimental findings, and finally, Section 5 presents the conclusion and the prospects of this paper.

2. 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 that are used in the authentication process that is done using five of the best-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 fingers veins 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 3 different universities and 2 two training centers on three different continents and through more than 50 activities, all the test images collected from the students contain at least 80% of the face area and the *signal-to-noise ratio* (SNR) captured from the microphones is low enough to allow voice recognition. The number of samples used is as follows: 373410 images, 1007 audio clip, and 653 keystrokes. Many successful applications of modeling and classification techniques in various fields have been established . The use of signatures in fuzzy modeling[10], evolving fuzzy models for SMA wire actuators[11], the early detection of mortality in COVID-19 patients through factor analysis and ANNs [12], the implementation of LSTM algorithms for human mobility prediction [13], the improvement of K-means clustering [14] and the use of Bayesian filtering techniques in modeling various systems [15] showcase the potential of these approaches to address complex real-world challenges and provide valuable insights in different domains.

3. 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. 2.

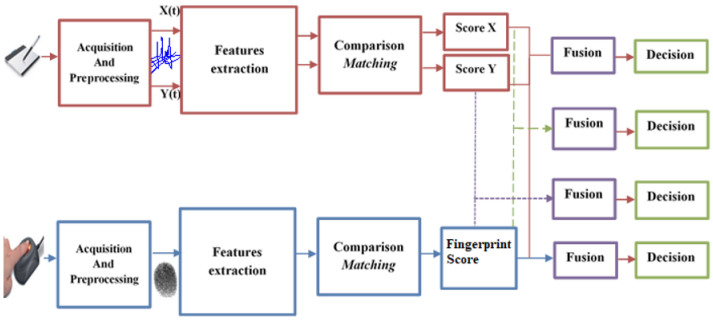

Fig. 2. Architecture of the proposed multimodal biometric authentication system.

3.1. Databases

For the evaluation of our 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 [16], 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 mm^2, 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 and for 5 different groups 5 genuine signatures and 5 skilled forgeries of another participant. Hence, each contributor ends up with 25 genuine signatures and his 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 [17], 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 was 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 forge on a computer screen, the skilled forgery collection was not started until the participant practiced his skilled forgery and become convinced that he completely mastered it. For the fingerprint part, the data was 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. 10 fingerprint samples are collected from each volunteer. To allow the evaluation of the system under different conditions, each sample is 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 [18–19]. For this database, the data was 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 are 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 was collected from participants in three different sessions separated by at least two-week period, four impressions of four different fingers (forefinger and middle finger of both hands) of each user were recorded at each session (Fig. 3). The total number of gathered finger impressions was 1440 from 30 volunteers.

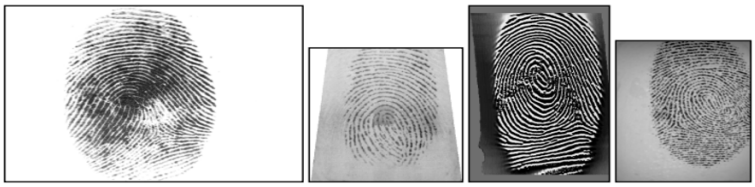

Fig. 3. One fingerprint image from each database, at the same scale factor [19].

3.2. 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. [20] 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.

3.2.1. Pre-processing

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 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 center 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 a better data processing time and less storage usage.

3.2.2. Enrollment

The user's profiles are created during this stage, 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 for testing the system. All of the first five signatures were first pre-processed as described in Section 3.2.1. After that the reference signature is determined by averaging the first five signatures according to the following expression:

$$S_{ref} = \frac{S_1 + S_2 + S_3 + S_4 + S_5}{5}, \tag{1}$$

where $S_1, S_2, \ldots, S_5$ are the first five signatures of each user. Fig. 4 shows the reference signature alongside the first five signatures of the database.

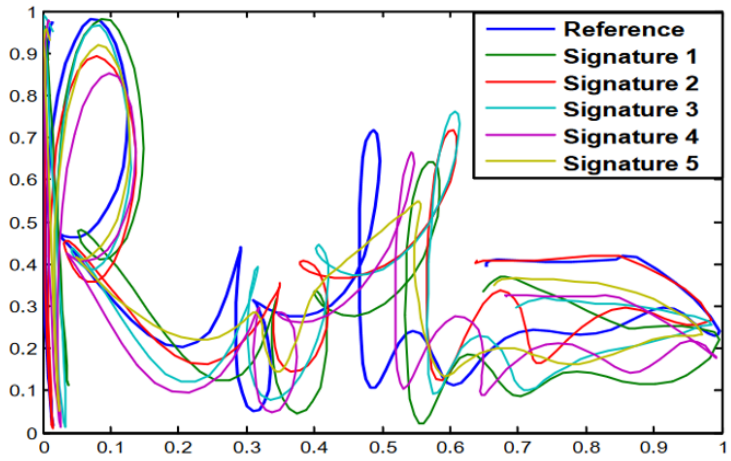

Fig. 4. Reference signature [4].

3.2.3. Test phase

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) [20], 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 can't be larger than one.
- The mean value of an IMF is equal to zero.

This algorithm is implmemented as shown in [21]. 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

$$SD = \sum |E_{j-1}(t)| \leq \varepsilon, \tag{2}$$

where ε is the stop criterion threshold .The value of ε is generally fixed at 0.2 or 0.3 [22], in our experience, we are using an SD of 0.2 [23]. 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 $r(t)$ is the residual component and $\mathrm{IMF_i(t)}$ is the IMF components. 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 $(\mathrm{V_{EMD}} = [\mathrm{IMF_x}, \mathrm{IMF_y}])$. Those parameters will allow us to recreate and decompose the original signature.The recorded IMFs occupy a large volume, which implies that the $\mathrm{V_{EMD}}$ cannot be used for signature characterization. For this reason, we used the same algorithm as Rilling *et al.* [24] to locate the minima and maxima of the IMFs of each signature, those extracted parameters are then used to create a new vector V_{emdN}.

3.2.4. Comparison and decision

This 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 V_{emdN}. Based on a comparison score, in this step we classify the test signatures into one of two categories: genuine or imposter. This decision is made using the Euclidean distance between both rebuilt test and reference signatures.

3.3. 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. The synoptic diagram that gives an overview of the steps in the system proposed in this paper is illustrated in Fig. 5.

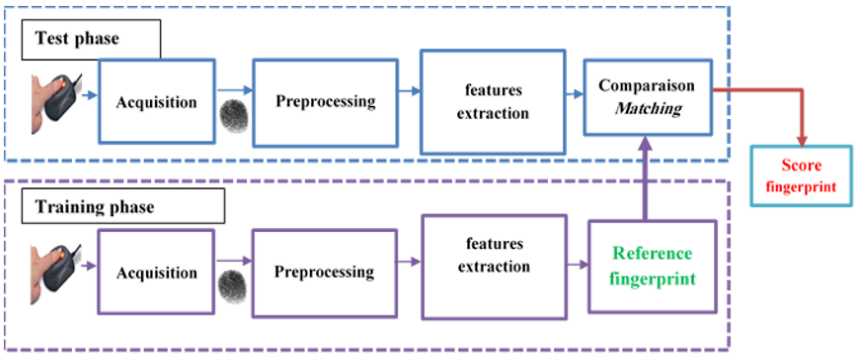

Fig. 5. General architecture of our fingerprint authentication system.

3.3.1. Acquisition

In this paper, use was made of the famous database provided by FVC 2004 (Fingerprint Verification Competition 2002) as well as the bimodal database MCYT (fingerprint and signature) as described in Section 3.1.

3.3.2. Preprocessing

The aim of this 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 equalization occupies the whole range from 0 to 255. The second step is enhancing the fingerprints using the Fourier transform, after that, we binarize 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. And 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 [25], 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.

3.3.3. Feature extraction and enrollment

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 [26]. The second step is the extraction of minutiae.

The enrollment 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 preprocessing 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.

3.3.4. Decision phase

It is done as follows: given S_{ref} (i) the parameter file of the reference fingerprint of the ith user and S_{test} (i) the parameter file of the test fingerprint of the i^{th} user. The S_{emp} fingerprint scores are obtained using the Euclidean distance according to:

$$S_{emp} = \frac{1}{I}\sqrt{\sum_{i=1}^{I}(S_{refi} - S_{testi})^2}. \tag{4}$$

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

3.4. Proposed multimodal biometric system

We have chosen two biometric modalities of different natures: a physical one and a behavioral 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 normalized using three score normalization 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 using he weighted sum approach. The weighted sum has been prominently mentioned in the literature. It has been used to merge biometric modalities such as online handwritten signature [27], iris, and face [28]. The greatest advantage of this method is its simplicity and very low computational cost. Let S_1 , ..., S_k be the scores resulting from comparing the different parameter vectors of our modalities. The fusion score is given by:

$$S = \sum_{i=1}^{K} w_i S_i, \tag{5}$$

where w_i are the weights associated with each modality type. These weights represent the degree of reliability of the modalities. If the weights are all equal, we revert to the case of the majority vote principle. The estimation of weights and hence reliability can be done using several criteria [29]. In this paper, the choice was of the method that calculates them based on the *Equal Error Rates* (EER) of each system as follows [30]:

$$w_i = \frac{EER_i}{\sum_{m=1}^{N} EER_m}. \tag{6}$$

Note that $0 \leq w_i \leq 1$, $\sum w_i = 1$, and that the weights are inversely proportional. Thus, the more discriminative a modality is, the more important its weight, and vice versa. In our case, for each of the four proposed combinations, we will calculate the weights of the weighted sum based on the performance of each subsystem separately. The evaluation and decision algorithm note is as follows:

- Let H_0 be the hypothesis that the score S originates from an imposter.
- Let H_1 be the hypothesis that the score S originates from an authentic user. Therefore, we need to choose the most probable hypothesis. We consider that the score S originates from an authentic user if $P(H_1/S) > P(H_0/S)$. By applying Bayes theorem, we obtain:

$$\frac{P(S/H_1)P(H_1)}{P(S)} > \frac{P(S/H_0)P(H_0)}{P(S)}. \tag{7}$$

And thus:

$$\frac{P(S/H_1)}{P(S/H_0)} > \frac{P(S/H_0)}{P(S/H_1)}. \tag{8}$$

Since the values of $P(H_0)$ and $P(H_1)$, which respectively represent the probability of an imposter or an authentic user attempting to access the system, are difficult to estimate, we compare the likelihood ratio to an experimental threshold θ called the decision threshold.

4. 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 behavioral 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. The decision to accept or reject a user is based on the authentication score. This decision can be improved by normalizing the scores.

The 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 behavioral 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 normalization, with the three normalization methods of our system is illustrated as a DET curve in Fig. 6.

Table 1 summarizes our results obtained after merging the globality of our two biometric modalities (fingerprint and signature) with several normalization types.

It can be seen in Table 1 that the normalization with the Min-Max method improves the decision in all cases. Moreover, an EER of 1.69% was obtained which is a real success for our system. This success is 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 normalization and fusion method adopted by our system. The following table summarizes all our best results obtained on the MCYT-100 database. The improvement is very noticeable. Indeed, we make a significant improvement in the error rates which dropped from 2.91% to 1.69%.

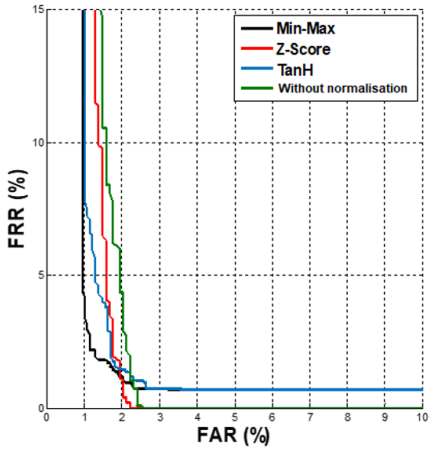

Fig. 6. The DET curves of the fusion between the fingerprint and the handwritten signature.

Table 1. Results obtained after merging the fingerprint and the signature in terms of EER on the MCYT-100 base.

Normalization method / Normalization method	EER %			
	min-max	Z-score	Tanh	No Normalization
Fingerprint and signature	1.69	1.85	1.76	2.16

5. Conclusions

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 started by presenting the performance of our two modalities separately before performing the fusion 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 normalization 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 is capable of handling delicate situations, in particular when unimodal systems do 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 Polytechnica Hungarica **16**(5), 2019, pp. 87–100.

[2] J. K. PILLAI, V. PATEL, R. CHELLAPPA and N. K. RATHA, *Secure and robust iris recognition using random projections and sparse representations*, IEEE Transactions on Pattern Analysis and Machine Intelligence **33**(9), 2011, pp. 1877–1893.

[3] T. CHAI, S. PRASAD, J. YAN and Z. ZHANG, *Contactless palmprint biometrics using DeepNet with dedicated assistant layers*, The Visual Computer, 2022, pp. 1–19.

[4] T. HAFS, L. BENNACER, M. BOUGHAZI and A. NAITALI, *Empirical mode decomposition for online handwritten signature verification*, IET Biometrics **5**(3), 2016, pp. 190–199.

[5] S. PARKINSON, S.KHAN, A.CRAMPTON, Q. XU, W. XIE, N. LIU and K. DAKIN, *Password policy characteristics and keystroke biometric authentication*, IET Biometrics **10**(2), 2021, pp. 163–178.

[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*, Proceedings of 2014 Twentieth National Conference on Communications (NCC), Kanpur, India, 2014, pp. 1–6.

[7] M. LEGHARI, S. MEMON, L. DHOMEJA and D. JALBANI, A. ALI, *Deep feature fusion of fingerprint and online signature for multimodal biometrics*, Computers **10**(2), 2021.

[8] B. EL-RAHIEM, F. ABD EL-SAMIE and M. AMIN, *Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein*, Multimedia Systems **28**, 2022, pp. 1325–1337.

[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 **9**, 2021, pp.72398–72411.

[10] C. POZNA, N. MINCULETE, R.-E. PRECUP, L. T. KÓCZY and Á. BALLAGI, *Signatures: Definitions, operators and applications to fuzzy modelling*, Fuzzy Sets and Systems **201**, 2012, pp. 86–104.

[11] R.-E. PRECUP, C.-A. BOJAN-DRAGOS, E.-L. HEDREA, R.-C. ROMAN and E. M. PETRIU, *Evolving fuzzy models of shape memory alloy wire actuators*, Romanian Journal of Information Science and Technology **24**(4), 2021, pp. 353–365.

[12] S. OGUTCU, M. INAL, C. CELIKHASI, U. YILDIZ, N. O. DOGAN and M. PEKDEMIR, *Early detection of mortality in COVID-19 patients through laboratory findings with factor analysis and artificial neural networks*, Romanian Journal of Information Science and Technology **25**(34), 2022, pp. 290–302.

[13] I. NURHAIDA, H. NOPRISSON, V. AYUMI, H. WEI, E. DWIKA PUTRA, M. UTAMI and H. SETIAWAN, *Implementation of deep learning predictor (LSTM) algorithm for human mobility prediction*, International Journal of Interactive Mobile Technologies **14**(18), 2020, pp. 132–144.

[14] I.-D. BORLEA, R.-E. PRECUP and A.-B. BORLEA, *Improvement of K-means cluster quality by post processing resulted clusters*, Procedia Computer Science **199**, 2022, pp. 63– 70.

[15] C. POZNA, R.-E. PRECUP, J. K. TAR, I. ŠKRJANC and S. PREITL, *New results in modelling derived from Bayesian filtering*, Knowledge-Based Systems **23**(2), 2010, pp. 182–194.

[16] 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 Proceedings Vision, Image and Signal Processing **150**(6), 2003, pp. 395–401.

[17] 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, Springer, Berlin, Heidelberg, 2004, pp. 16–22.

[18] D. MALTONI, D. MAIO, A. K. JAIN and J. FENG, Eds., *Handbook of Fingerprint Recognition*, Springer International Publishing, Cham, 2022.

[19] 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., Lecture Notes in Computer Science, Springer, Berlin, Heidelberg **3072**, 2004.

[20] 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*, Proceedings: Mathematical, Physical and Engineering Sciences 454(1971), 1998, pp. 903–995.

[21] L. GAO, 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*, Applied Sciences **12**(16), 2022, pp. 81–87.

[22] G. RILLING, Décompositions Modales Empiriques. Contributions á la théorie, l'algorithmie et l'analyse de performances, Ph.D. thesis, Ecole Normale suprieure de Lyon, Lyon, France, 2007.

[23] L. LIN, Y. WANG and H. ZHOU, *Iterative filtering as an alternative algorithm for empirical mode decomposition*, Advances in Data Science and Adaptive Analysis **1**(4), 2009, pp. 543–560.

[24] G. RILLING, P. FLANDRIN, P. GONALVES and J. LILLY, *Bivariate empirical mode decomposition*, IEEE Signal Processing Letters **14**(12), 2008, pp. 936–939.

[25] L. HONG, *Automatic personal identification using fingerprints*, Ph.D. thesis, Michigan State University, East Lansing, MI, USA, 1998.

[26] L. C. JAIN, U. HALICI, I. HAYASHI, S. B. LEE and S. TSUTSUI, Eds., *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, CRC Press, USA, 1999.

[27] Y. WANG, T. TAN and A. K. JAIN, *Combining face and iris biometrics for identity verification*, in Audio- and Video-Based Biometric Person Authentication AVBPA 2003, J. Kittler and M. S. Nixon, Eds., Lecture Notes in Computer Science, Springer, Berlin, Heidelberg **2688**, 2003.

[28] T. SCHEIDAT, C. VIELHAUER and J. DITTMANN, *Distance-level fusion strategies for online signature verification*, Proceedings of the IEEE International Conference on Multimedia and Expo, Amsterdam, The Netherlands, 2005, pp. 1294–1297.

[29] R. T. MARLER and J. S. ARORA, *Survey of multi-objective optimization methods for engineering*, Structural and Multidisciplinary Optimization **26**, 2004, pp.369–395.

[30] T.SCHEIDAT, C. VIELHAUER and J. DITTMAN, *Single semantic multi-instance fusion of handwritten based biometric authentication systems*, Proceedings of 2007 IEEE International Conference on Image Processing, San Antonio, TX, USA, 2007, pp. II-393–II-396.