Journal of Advanced Engineering Trends
ISSN : 2682 - 2091

Vol. 44, No. 2, July 2025

Multimodal Cancelable Biometric based on EEG signal

Gerges M. Salama[1,*], Basma Omar[1], Safaa El-Gazar[1], Ahmed A. Hassan[1]
[1]*Electrical Engineering Dep., Faculty of Engineering, Minia University, Minia, Egypt*

* *Corresponding author(s) E-mail:* gerges.salama@mu.edu.eg

ARTICLE INFO

Article history:
Received: 22 October 2023
Accepted: 24 February 2024
Online: 23 May 2025

Keywords:
Cancelable biometrics,
EEG,
Double Random Phase Encoding

ABSTRACT

Due to the rapid development of fake programs and hacking, it has become necessary to rely on more reliable access methods. Biometric authentication is an effective trend for more secure access. This biometric should be saved as a cancelable template. Cancelability can be obtained using encryption. In this paper, Double Random Phase Encoding (DRPE) is utilized to generate the cancelable template from the electroencephalogram (EEG) signal spectrogram. For more reliable access, multibiometrics can be used. Biometric images can be fused using the Discrete Wavelet Transform (DWT) and used as masks, aiding in the DRPE encryption process. System performance is evaluated by the Equal Error Rate (EER) and the Area under the Receiver Operating Curve (AROC). Simulation results indicate the good performance of the proposed system, where ERR is close to zero and AROC is close to one. The proposed system is tested in the presence of different types of noise and attacks.

1. Introduction

New technologies such as the Internet of Things (IoT) and telemedicine are critical applications that depend on transmitting or receiving sensitive data. These technologies need a reliable authentication system, where traditional authentication systems have become easily faked [1, 2]. Traditional methods such as password-based authentication and token-based authentication have many problems. It can be forgotten, lost, or tampered with. Biometrics-based authentication is an effective trend in these new technologies, as biometrics are permanent and difficult to tamper with. Biometrics can be classified into physical, such as a face image, behavioral, such as a gait, and both physical and behavioral, such as biometric signals [3]. Biometric signals are the biometrics that depend on the internal body shape and the way a person carries out actions, such as an Electroencephalogram (EEG). Identifying people through their EEG signals is a new and promising topic for research [4].

EEG is a recording of human brain electrical activity. EEG contains different sub-band frequency ranges in 0.5−4 Hz, 4-8 Hz, 8-12 Hz, 12-30 Hz, and over 30 Hz, which are delta, theta, alpha, beta, and gamma, respectively. The EEG signal is superior to the other biometric signals for many reasons, such as [5]:

- EEG signal changes from one activity to another for the same person.
- The human brain cannot be forced to produce the EEG signal. Forcing a person to do an activity produces an EEG signal different from the one produced by doing the same activity, but willingly.
- EEG signal cannot be produced by a non-living brain, it can be considered a sign of a person life.

For these reasons, most of the recent research has focused on the EEG signal and its use in the areas of authentication and identification systems [5].

Therefore, the EEG signal should be saved in a cancelable template to keep the original signal away from hackers. A biometric authentication system consists of two phases: the registration phase and the authentication phase. The registration phase contains biometric acquisition, feature extraction, and cancelable template generation. The verification phase comprises the matching process and the decision-making process [6].

A cancelable biometric template is an intentionally distorted template that is generated from the biometric. This intended distortion is applied through a non-invertible function. Matching is performed on the transformed templates, not the original ones. Cancelable biometric templates should be irreversible and maintain the distinct features of biometrics. Cancellability should not affect individual identification [6].

Biometric authentication systems can be classified into unimodal and multimodal according to the number of biometrics utilized for individual authentication. Although unimodal systems are simple and lower-cost, multimodal systems are more reliable [7].

This paper proposes a multimodal Cancelable Biometric System (CBS). The system depends on encrypting the EEG spectrogram using Double Random Phase Encoding (DRPE) to generate the cancelable template. In addition, fused biometric images are used as masks for the DRPE. Image fusion is applied by the Discrete Wavelet Transform (DWT). The aim of image fusion is to obtain distinctive DRPE masks from the biometric image features. The proposed system can be summarized as follows:

1. Five biometrics should be acquired: face image, fingerprint, iris image, palmprint, and the EEG signal.
2. The face image and fingerprint are fused using DWT to obtain the first DRPE mask. In the same way, the iris image and palmprint are fused to obtain the second DRPE mask.
3. DRPE is used as a deformation tool to generate the cancelable template.

The reset of this paper is organized as follows: Section 2 presents different related CBSs based on the EEG signal. Section 3 presents a background study related to the proposed system. Section 4 presents the proposed CBS. Section 5 presents the simulation results, and Section 6 presents the conclusion, followed by the references.

2. Related Works

EEG can be recorded during different activities, such as eyes opening and closing in relaxation mode, different mental tasks, and auditory or visual stimulation. Different CBSs depended on the EEG signals generated from different activities. Kumari and Vaish presented an identification system based on Empirical Mode Decomposition (EMD) to extract features from the EEG signal and Canonical Correlation Analysis (CCA) to generate the feature vector at the fusion level [8]. Then, the Linear Vector Quantization (LVQ) neural network is implemented for the classification process. The paper achieved accuracy of up to 90%. Likewise, in [9], Thomas et al. presented an algorithm based on power features extracted from different frequency bands, including alpha, beta, and gamma, of the EEG signal selected by the Butterworth band-pass filter. The average recognition rate was about 88.33%. Another algorithm based on the EEG signal was presented by Dai et al. for web applications [10]. Power Spectral Density (PSD) is used to extract features from the EEG signal, and Support Vector Machine (SVM) is used for the classification process. The algorithm achieved an EER of 0.0196. Flower pollination is an algorithm that has been utilized to select the optimum features of the EEG signal to achieve the highest accuracy of classification [11]. EEG channel selection is an issue that should be considered. Increasing the number of channels increases the complexity of the system and makes it inconvenient for the person to be authenticated. Alyasseri [12] employed a binary version of the Grey Wolf Optimizer (BGWO), which is a powerful meta-heuristic swarm-based algorithm, together with an SVM classifier. The system reduced the total number of channels from 64 to 23 and achieved a classification accuracy of 94.13%. In these studies, one of the most significant issues is the low identification accuracy as a result of the inherent low precision of EEG signals, which is not sufficient for practical deployments, particularly in high security environments. In addition, depending on deep learning in feature extraction and classification where deep learning is very time consuming and needs large datasets. In addition, these introduced systems are unimodal systems that cannot achieve reliable authentication. In this paper, the above issues are solved because it depends on a simple correlation coefficient for the verification process, which does not require a large amount of data. Furthermore, this paper presents a multimodal system that is more reliable.

3. Background Study

This section presents the basic algorithms that are relied upon to generate the cancelable template. Image fusion is the first step in the proposed system. Image fusion is utilized using the Discrete Wavelet Transform (DWT). The second step is the DRPE that is applied to the EEG spectrogram. A brief explanation of the DWT and DRPE will be introduced in this section

3.1. Image Fusion using Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) decomposes the image into approximate information and details by applying a combination of filter bank. The filter bank consists of a pair of low pass filter for the low frequencies that represent the approximation coefficients and a high pass filter to extract the high frequencies that represent the detail coefficients. After DWT, the image can be represented by four sub-bands: both horizontal and vertical low frequency components (LL), the horizontal low frequency components and the vertical high frequency components (LH), the horizontal high frequency components and the vertical low frequency components (HL) and both horizontal and vertical high frequency components (HH) [13].

As shown in Fig. 1, the DWT is applied to extract the discriminating features of each image, and then these features are collected in the synthesized image. Finally, an inverse DWT is applied to obtain the fused image. The fused image contains detailed information from each image. Image fusion can be summarized as follows [13]:

1. DWT decomposition is performed to extract the discriminating features from the images.
2. The discriminated features are represented by the detailed information obtained by the high pass filter.
3. Fusion is performed by taking the minimum for approximations and the maximum for the details to obtain the synthesized image.
4. Finally, the inverse DWT is applied to obtain the fused image.

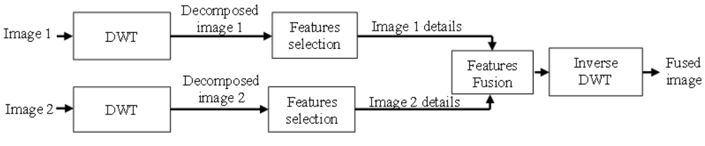


Figure 1 Image fusion using DWT

Image fusion is the process of gathering all the important information from multiple images to reduce the amount of data and produce more constructed images that are appropriate and understandable for human and machine perception. Image fusion is used in this paper to merge the different images and produce one image that carries the important information from each one [13].

3.2. Double Random Phase Encoding (DRPE)

DRPE is one of the optical encryptions that can be simulated through a mathematical model. It is an efficient and simple encryption algorithm that depends on Random Phase Mask (RPM). The mathematical model is performed by applying the Fourier Transform (FT) which represents the optical lens nonlinearity. The mathematical model of the DRPE is shown in Fig. 2 [14].

DRPE depends on two RPMs that are applied to the original image, as indicated by the following equation [14]:

$$e(x,y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{i(x,y)\delta_n(x,y)\} \times \gamma_m(\upsilon,\eta)\} \quad (1)$$

where FT is the Fourier transform, × is the convolution, $i(x,y)$ and $e(x,y)$ are the original and encrypted images in the spatial domain respectively, x and y are the spatial domain coordinates, $\delta_n(x,y)$ is the first spatial domain PRM and $\gamma_m(\upsilon,\eta)$ is the second frequency domain PRM. Both random phase masks are 2D matrices of the same size as $i(x,y)$ having values uniformly distributed between 0 and 2π.

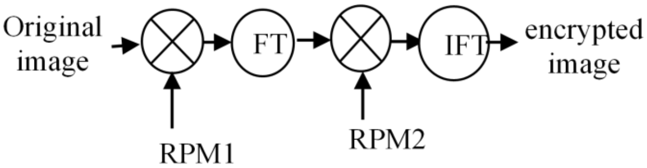


Figure 2 Block diagram of DRPE simulation model [14]

4. The Proposed Cancelable Biometrics System

The authorized system in any application consists of two modes, the first mode is registration. It includes the biometric acquisition and the cancelable template generation. The cancelable template for each user is saved in the application database. The second mode is authentication, where the cancelable template is regenerated for the query user and matched with the corresponding saved one. The result of the matching process helps in making a decision [4].

The proposed system is a multimodal CBS. To generate the cancelable template, it is required to acquire five biometrics from the registered user. Face image, fingerprint, iris image, palm print, and the EEG signal are considered biometrics for the proposed system.

Recording EEG signals is non-invasive with a portable device therefore, EEG is widely used in the Brain Computer Interface (BCI), which can provide a link between the human subject and the computer without physical contact.

The human may control an electronic device not only by sending explicit commands but also by brainwaves. Integrating BCI and EEG-based authentication makes these applications not only execute the user commands but also recognize identity before executing. Since BCI is based on brainwaves, EEG biometrics are the best candidate as an authentication factor in this application [15]. This paper presents an EEG-based authentication system. In addition, traditional biometrics are used to aid in cancelable biometric template generation.

Cancelable biometric template generation can be summarized as follows:

1. Four biometric images are fused using DWT in two stages.
2. As shown in Fig. 3, the face image and the fingerprint are merged together by the DWT fusion, where the detail features from each image are selected and merged to get the first fused image.
3. Likewise, as shown in Fig. 4, the iris image and the palm print are fused to get the second fused image.
4. The two fused images contain the discriminated information from each image.
5. The fused image is multiplied by the RPM where each pixel is multiplied by the corresponding random value in the RPM.
6. Finally, the EEG spectrogram is encrypted by the DRPE with the modified RPMs to obtain the cancelable biometric template as shown in Fig. 5.
7. The cancelable template is saved in the application database.
8. In the authentication mode, the cancelable biometric template of the query user is generated using the same steps as in the registration mode.
9. Then, the query template is compared to the template that have already been saved in the database. The correlation value between the saved and query templates is then calculated using the following equation [16]:

$$c_r = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (2)$$

   where c_r is the correlation value, x_i and y_i are intensity values of the *i*th pixel in saved and query templates, respectively. $E(x)$ and $E(y)$ are mean intensity values of saved and query template. The correlation value is compared with a threshold value to determine the authorized users. If the correlated value is greater than the threshold value, the query user is authorized. The threshold value is determined based on several tests for genuine and imposter users [4].
10. The threshold value is determined as follows:
   Several genuine tests are performed, and the obtained correlation scores are treated as the values of a random variable. The genuine score Probability Distribution Function (PDF) is estimated. Similarly, for imposter users, several tests are performed, and correlation scores are obtained. The PDF of the imposter test correlation scores is estimated. The intersection point of the correlation distribution curves for genuine and impostor tests determines the threshold value [16].

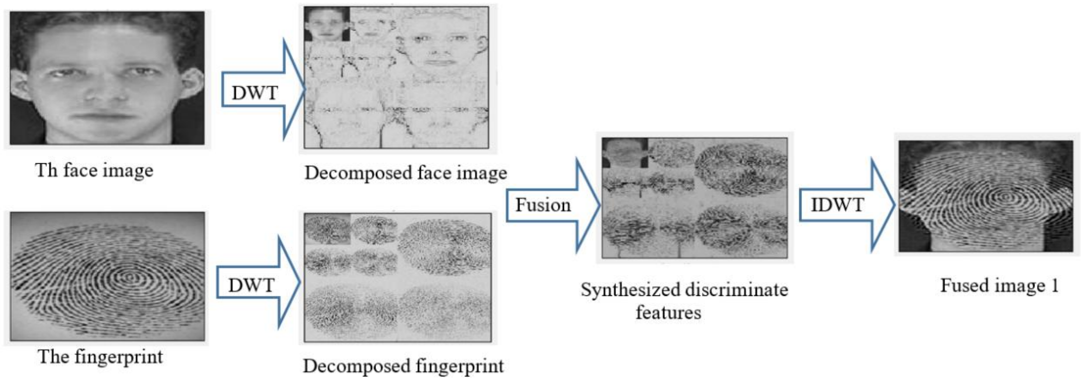


Figure 3 Steps of the fused image 1 generation

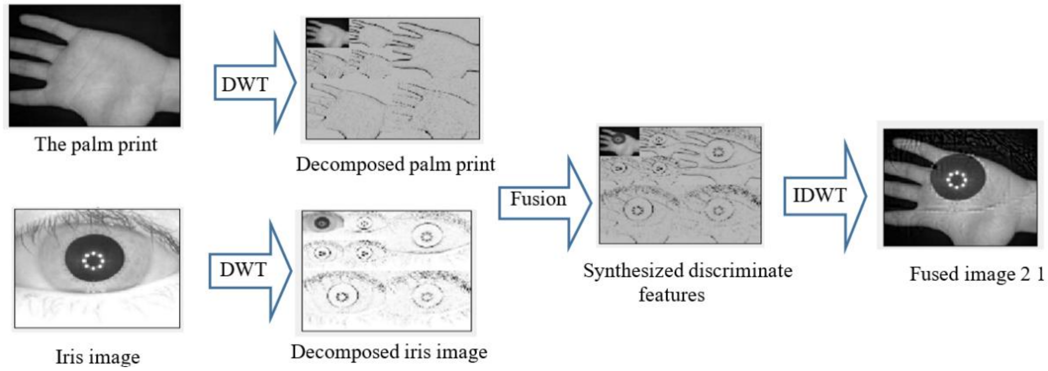


Figure 4 Steps of the fused image 2 generation

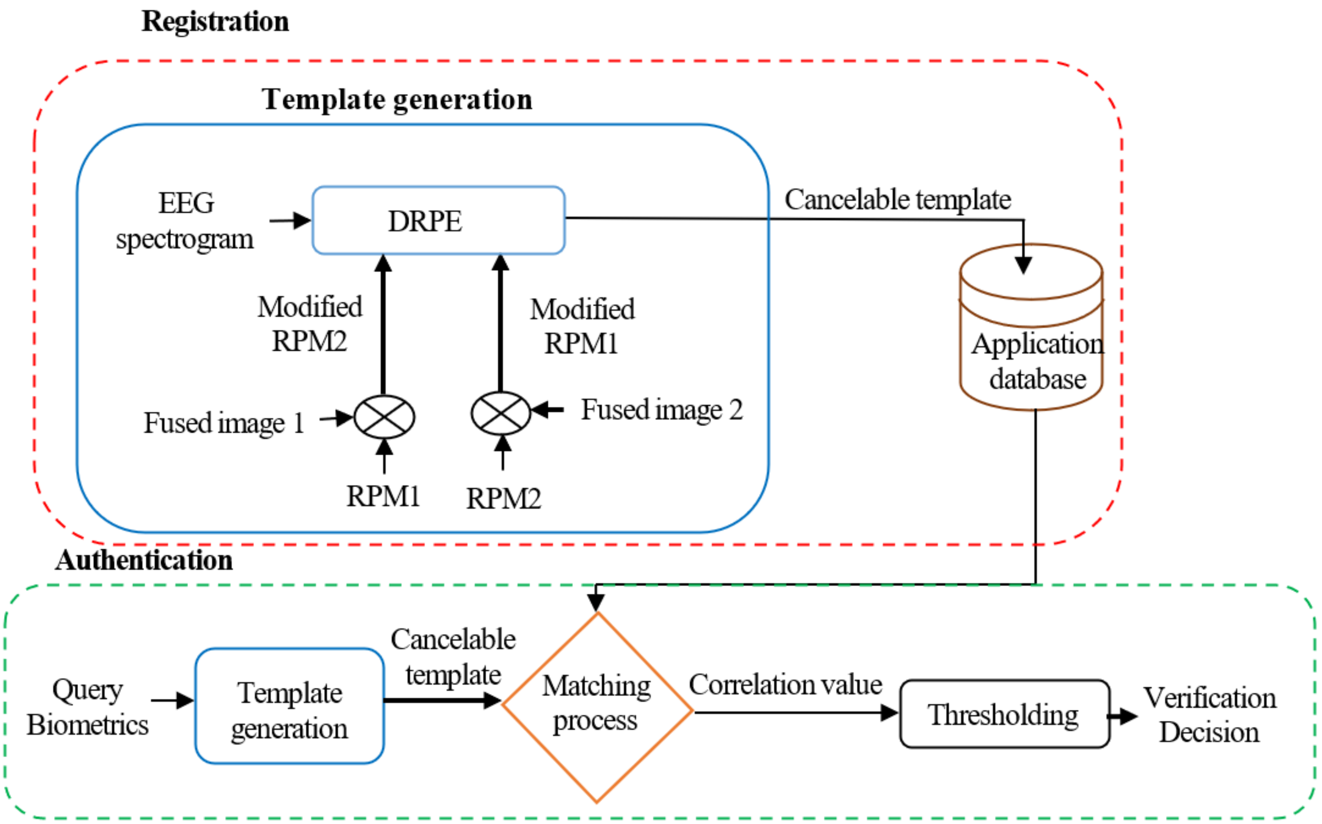


Figure 5 The proposed system block diagram

5. Simulation Results

A personal computer with an Intel 2.5 GHz processor and 6.00 GB of RAM runs the simulations. Simulations are performed using MATLAB R2016b. Simulated biometrics are selected from the EEGMAT database, ORL database, FNC2002 fingerprint dataset, CASIA-IrisV3 dataset, and CASIA palm print image dataset for the EEG signals, face images, fingerprints, iris images, and palm prints, respectively [17–21]. Figure 6 shows nine random samples from each dataset.

As shown in Fig. 7, the first step in the proposed registration mode is image fusion. Every two biometric images are fused to give one image that carries the discriminate data of the original images. The second step is the EEG spectrogram encryption by the DRPE with the RPMs modified by the fused images. Figure 8 shows the EEG spectrograms and the encrypted spectrograms that represent the cancelable templates. The figure shows the histograms of the original EEG spectrograms and the histograms of the obtained cancelable templates. The figure indicates the difference between the original and cancelable histograms, which indicates a change in the grayscale distribution for the obtained templates.

The authentication mode includes the matching process and the decision making. Matching is performed between the saved and query cancelable templates and gives a correlation value [16]. The calculated correlation is compared with a threshold value to make a decision. Figure 9 shows the distribution curves of the genuine and imposter correlations in the presence of different attacks, Additive White Gaussian Noise (AWGN), salt and pepper noise, and blurring with a low Butterworth filter. The figure indicates that the proposed system performance is slightly affected by the attacks. The Receiver Operating Curve (ROC) curves emphasize the same results as shown in the figure. It is indicated that the blurring attack has a great effect on the authentication process.

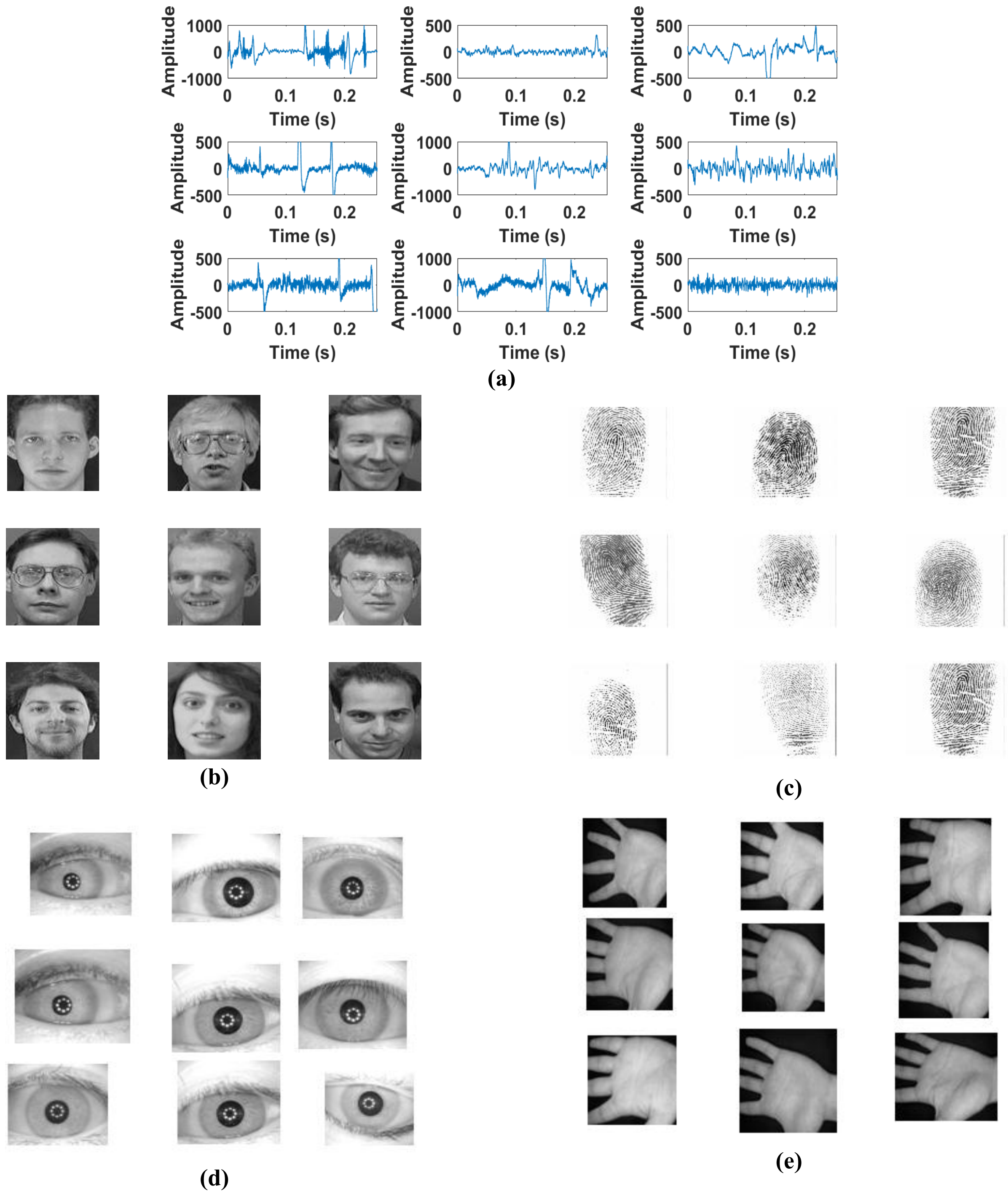
The system performance is evaluated by numerical values represented by the Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR) [16]. These values express the error rates of the system performance, where the closer they are to zero, the better the system performance. Finally, the Area under ROC (AROC) expresses the system performance as a classifier. The closer the AROC to one, the better the system performance as a classifier [16].

Table 1 gives the numerical evaluation values in the presence of AWGN for different noise variances. AWGN may appear as an irregular variation in pixel values, giving the image a grainy or spotted look. The slight variations in the numerical values given in the table indicate the performance stability of the proposed system with the different levels of AWGN. EER values vary from 2.35×10-13 to 2.0242× 10-10, and AROC values vary from 1 to 0.9998 for noise variance from 0.01 to 0.15. The given values indicate that AWGN has a slight or negligible effect on the system performance.

Table 2 indicates the system performance in the presence of salt and pepper noise with different noise densities. It presents sparsely occurring white and black pixels, which can significantly deteriorate the quality of an image. The values show that there is a slight drop in the system performance as the salt and pepper noise density increases, but the system still maintains an acceptable level of performance. The EER values vary from 5.6062× 10-6 to 0.007, and AROC values vary from 1 to 0.9998 as the noise density varies from 0.1 to 0.4.

6. Conclusion

User authentication is an important issue in application access security. Biometric authentication is a security procedure that relies on individual biometric characteristics. EEG signals are a new trend in biometric authentication. Cancelable biometric template generation is an important step in the authentication system. The paper presents a CBS that depends on the EEG signal. The cancelable template is generated by encrypting the EEG signal spectrogram using DRPE. For better system reliability, fused biometric images are used to modify the RPMs of the DRPE. The proposed system achieves high performance, with EER values close to zero and AROC values close to one. However, the proposed system is tested in the presence of different noises and proves its efficiency. Although the proposed system is efficient, it has some limitations, including complexity and high cost. Acquiring five individual biometrics consumes time and requires different devices. This limits the implementation of the proposal to applications that have sufficient funding and are not concerned with the cost factor, such as military applications. There are some recommendations for future work, including the investigation of signal fusion techniques for multimodal CBS comprising different signal modalities, such as ECG and PPG.



(a)

(b)

(c)

(d)

(e)

Figure 6 Random samples of tested datasets (a) EEGMAT EEG waveforms, (b) ORL face images, (c) FVC 2002 DB1 fingerprint images, (c) CASIA-V3 iris images, and (d) CASIA-V1 palm print images [21-25]

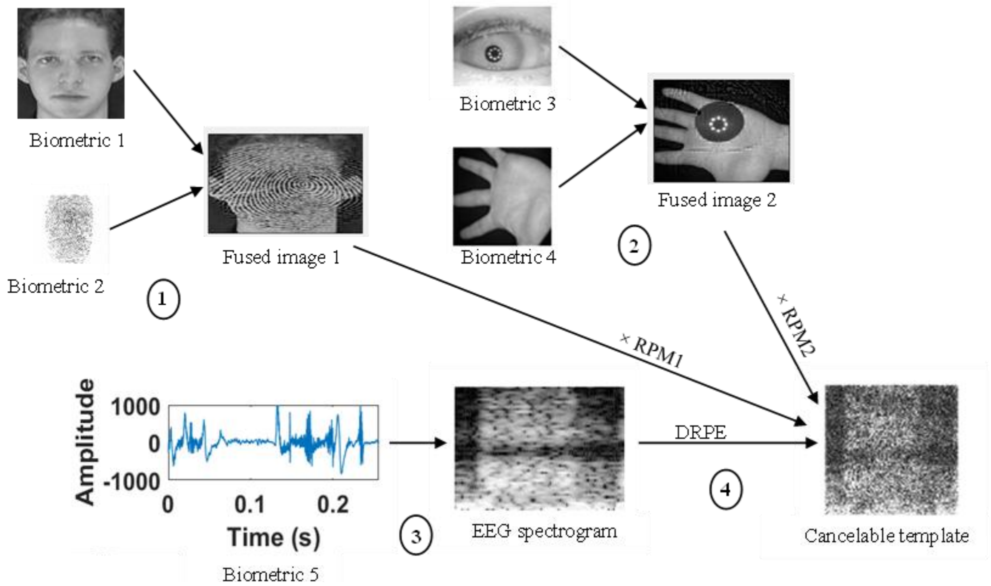
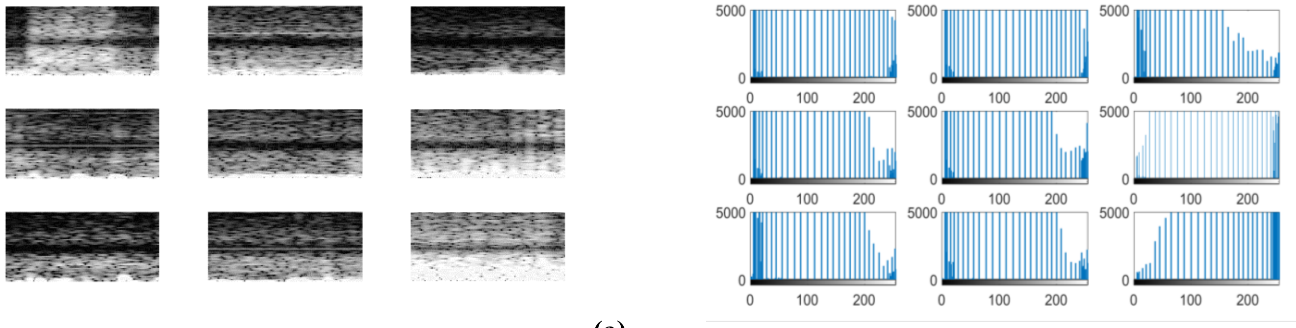
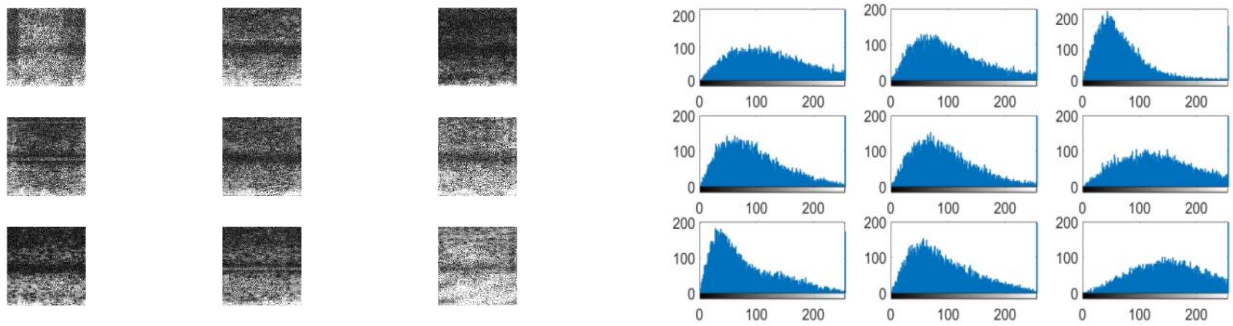


Figure 8 Steps to obtain the cancelable template



(a)



(b)

Figure 7 Nine random samples of (a) Original EEG spectrograms and their histograms, and (b) Cancelable templates and their histograms

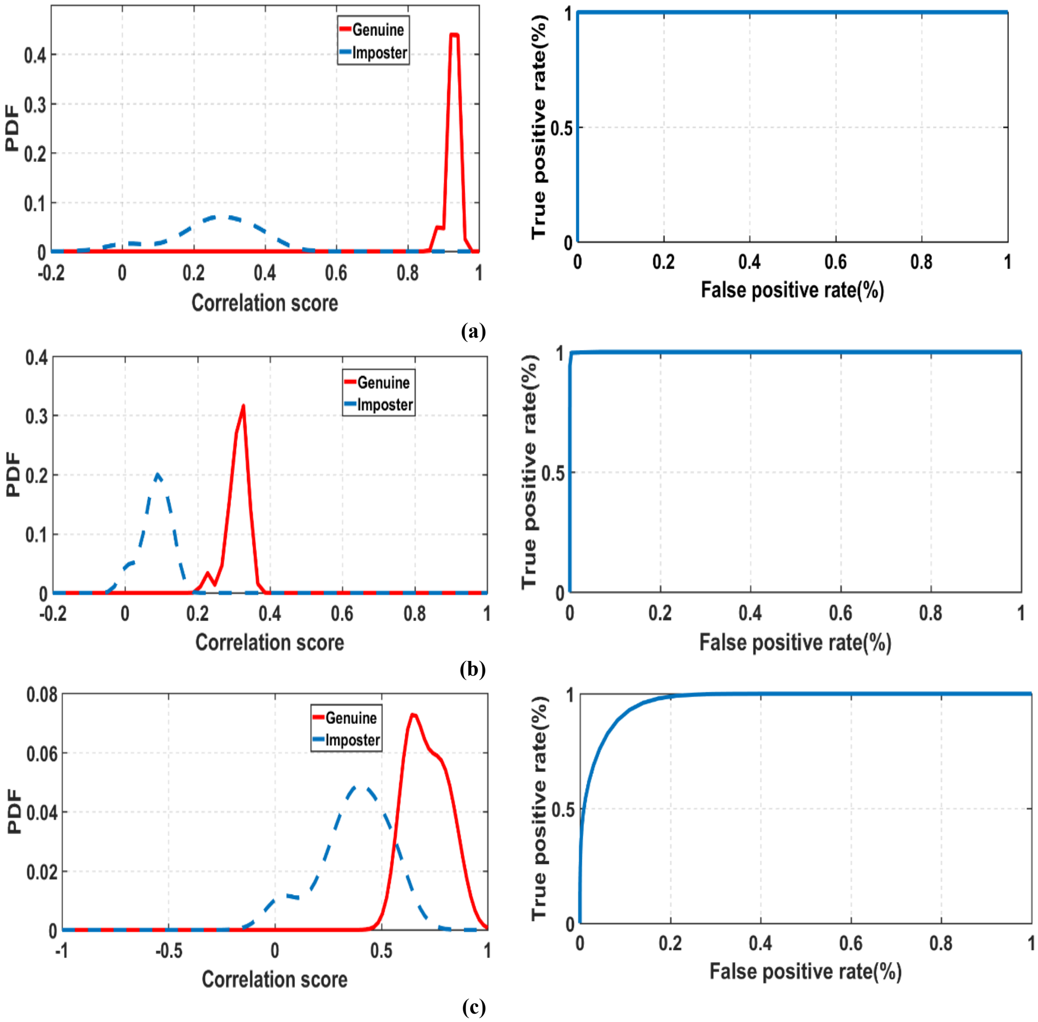


Figure 9 Genuine and impostor distribution curves, and ROC curves for the proposed system in the presence of different attacks (a) AWGN, (b) salt and pepper noise, and (c) blurring with a low Butterworth filter

Table 1 Evaluation metrics values for the different cases of the proposed CBS in the presence of AWGN with different variances

Evaluation Metrics	0.01	0.05	0.1	0.15
EER	2.35×10^{-13}	1.0132× 10^{-12}	5.6173× 10^{-12}	2.0242× 10^{-10}
AROC	1	0.9999	0.9998	0.9998
FAR	1.1125× 10^{-16}	3.3166× 10^{-14}	1.9291× 10^{-15}	1.0143× 10^{-16}
FRR	3.6820× 10^{-13}	2.0264× 10^{-11}	1.1217× 10^{-12}	4.0484× 10^{-10}

Table 3 evaluation metrics values for the different cases of the proposed CBS in the presence of a blurring attack with different window sizes

Evaluation Metrics	2×2	3×3	4×4	5×5
EER	0.0125	0.0307	0.0385	0.0417
AROC	0.9974	0.9697	0.9402	0.9116
FAR	0.0306	0.1400	0.1882	0.2271
FRR	0.0220	0.0705	0.1277	0.1664

Table 4 evaluation metrics values for the different EEG dataset (EEG Signals from an RSVP Task)

Evaluation Metrics	AWGN (0.15 variance)	Salt and pepper noise (0.4 density)	Blurring (window size 4×4)
EER	3.1074×10^{-11}	0.0067	0.0423
AROC	0.9998	0.9997	0.9548
FAR	2.0015×10^{-15}	0.0031	0.1882
FRR	3.9248×10^{-11}	0.0089	0.1277

Table 5 comparison study with the state-of-the-art

Reference number	Implemented algorithm	Performance metrics
Ref [8]	EMD, CCA and LVQ	Accuracy = 90%
Ref [9]	band power features extracted from alpha, beta and gamma bands	average recognition rate = 88.33%
Ref [10]	PSD and SVM	EER = 0.0196.
Ref [11]	Flower pollination	Accuracy = 87.79%
Ref [12]	BGWO and SVM	Accuracy = 94.13%

Proposed system	DWT and DRPE	EER= 2.35×10^{-13}
		AROC=1

Conflict of Interest

The authors declare no conflict of interest.

References

[1] M. I. Gaber, A. A. M. Khalaf, I. Mahmoud, and M. El-Tokhy, “Detection and recognition of moving objects for physical systems protection in nuclear facilities”, Journal of Advanced Engineering Trends, Vol. 40,20121, pp. 85-98.

[2] M. Alaa, G. M. Salama, A. I. Galal, and H. F. A. Hamed, “A robust lane detection method for urban roads”, Journal of Advanced Engineering Trends, Vol. 41,2022, pp 13-26.

[3] A. Kumar, S. Jain, and M. Kumar, “Face and gait biometrics authentication system based on simplified deep neural networks”, International Journal of Information Technology, Vol. 15, 2023, pp.1005-1014.

[4] G. M. Salama, B. Omar, W. El-Shafai, G.M. El-Banby, H. F. Hamed, S. El-Gazar, N. F. Soliman, and F. E. Abd El-Samie, “Secure biometric systems based on bio-signals and DNA encryption of optical spectrograms”, Optics Express, Vol. 31, 2023, pp.3927-3944.

[5] C. A. Fidas, and D. Lyras, “A Review of EEG-based user authentication: trends and future research directions”, IEEE Access, 2023.

[6] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, “A survey on methods and challenges in EEG based authentication”, Computers & Security, Vol. 93, 2020, pp.101788.

[7] N. Bala, R. Gupta, and A. Kumar, “Multimodal biometric system based on fusion techniques: a review”, Information Security Journal: A Global Perspective, Vol. 31, 2022, pp.289-337.

[8] K. Thomas, A. Vinod, “Utilizing individual alpha frequency and delta band power in EEG based biometric recognition”, in 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 4787-4791.

[9] K. Thomas, A. Vinod, N. Robinson, “Online biometric authentication using subject-specific band power features of EEG”, in International Conference on Cryptography, Security and Privacy (ICCSP), 2017, pp. 136-141.

[10] K. Thomas, A. Vinod, “EEG-based biometric authentication using gamma band power during rest state”, Circuits, Systems, and Signal Processing, Vol. 37, 2018, pp. 277–289.

[11] Z. Alyasseri, A. Khader, M. Al-Betar, J. Papa, O. Alomari, S. Makhadme, “An efficient optimization technique of EEG decomposition for user authentication system”, in 2nd International Conference on BioSignal Analysis, Processing and Systems (ICBAPS), 2018, pp. 1-6.

[12] Z. Alyasseri, O. A. Alomari, S. N. Makhadmeh, S. Mirjalili, M. A. Al-Betar, S. Abdullah, and A. K. Abasi, “EEG channel selection for person identification using Binary Grey Wolf Optimizer”, IEEE Access, Vol. 10, 2022, pp. 10500–10513.

[13] R. B. Naik, and P. N. Kunchur, “Image fusion based on wavelet transformation”, International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, 2020, pp. 2249 – 8958.

[14] H. Huang, “Novel scheme for image encryption combining 2d logistic-sine-cosine map and double random-phase encoding”, IEEE Access, Vol. 7, 2019, pp. 177988-177996.

[15] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, “A Survey on Methods and Challenges in EEG Based Authentication”, Computers & Security, Vol. 93, 2020, pp. 101788.

[16] G. M. Salama, S. El-Gazar, B. Omar, R. M. Nassar, A. A. Khalaf, G. M. El-Banby, F. E. Abd El-Samie, “Cancelable biometric system for IoT applications based on optical double random phase encoding”, Optics Express, Vol. 30, 2022, pp. 37816-37832.

[17] https://physionet.org/content/eegmat/1.0.0/

[18] https://www.cl.cam.ac.uk/research/dtg/attarchive/ facedatabase.html.

[19] http://bias.csr.unibo.it/fvc2004/Downloads/DB1_B.zip

[20] CASIA-IrisV3 database, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

[21] CASIA Palm Print Database, http://biometrics.idealtest.org