Computers, Materials & Continua
DOI: 10.32604/cmc.2023.033765
Article

Proposed Biometric Security System Based on Deep Learning and Chaos Algorithms

Iman Almomani[1,2], Walid El-Shafai[1,3,*], Aala AlKhayer[1], Albandari Alsumayt[4], Sumayh S. Aljameel[5] and Khalid Alissa[6]

[1]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[2]Computer Science Department, King Abdullah II School of Information Technology, The University of Jordan, 11942, Jordan
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[4]Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, 31441, Saudi Arabia
[5]Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, 31441, Saudi Arabia
[6]SAUDI ARAMCO Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, 31441, Saudi Arabia
*Corresponding Author: Walid El-Shafai. Email: welshafai@psu.edu.sa
Received: 27 June 2022; Accepted: 16 August 2022

Abstract: Nowadays, there is tremendous growth in biometric authentication and cybersecurity applications. Thus, the efficient way of storing and securing personal biometric patterns is mandatory in most governmental and private sectors. Therefore, designing and implementing robust security algorithms for users' biometrics is still a hot research area to be investigated. This work presents a powerful biometric security system (BSS) to protect different biometric modalities such as faces, iris, and fingerprints. The proposed BSS model is based on hybridizing auto-encoder (AE) network and a chaos-based ciphering algorithm to cipher the details of the stored biometric patterns and ensures their secrecy. The employed AE network is unsupervised deep learning (DL) structure used in the proposed BSS model to extract main biometric features. These obtained features are utilized to generate two random chaos matrices. The first random chaos matrix is used to permute the pixels of biometric images. In contrast, the second random matrix is used to further cipher and confuse the resulting permuted biometric pixels using a two-dimensional (2D) chaotic logistic map (CLM) algorithm. To assess the efficiency of the proposed BSS, (1) different standardized color and grayscale images of the examined fingerprint, faces, and iris biometrics were used (2) comprehensive security and recognition evaluation metrics were measured. The assessment results have proven the authentication and robustness superiority of the proposed BSS model compared to other existing BSS models. For example, the proposed BSS succeeds in getting a high area under the receiver operating characteristic (AROC) value that reached 99.97% and low rates of 0.00137, 0.00148, and

0.00157 for equal error rate (EER), false reject rate (FRR), and a false accept rate (FAR), respectively.

Keywords: Biometric security; deep learning; AE network; 2D CLM; cybersecurity and authentication applications; feature extraction; unsupervised learning

1 Introduction

Cancelable biometrics schemes are being significantly used nowadays. In general, a cancelable biometric scheme depends on extracting various facial, iris, and fingerprint features in order to authenticate individuals in a real-time manner [1]. These extracted features of the obtained biometrics structure the cancelable biometric templates. A cancelable biometric scheme mainly consists of two core stages, enrolment and authentication. In the enrolment stage, the obtained biometrics from the sensors for specific users are stored in a database. However, during the authentication stage, a query template is generated to be compared with the biometrics that is stored in the database [2]. The user is authenticated if both the stored biometrics and the provided query templates match. A cancelable biometric scheme can be either uni-biometric-based or multi-biometric-based [3]. The uni-biometric-based schemes deploy a single input such as the face, iris, or fingerprint to authenticate the individuals. Whereas, the multi-biometric-based scheme exploits two or more inputs. However, multi-biometric-based schemes are considered more secure since it is hard to hack a set of biometrics simultaneously.

Usually, the obtained biometrics are stored in the database during the enrollment stage. Even in the case of deploying encryption techniques on the stored biometrics, this requires implementing decryption during the authentication stage. Thus, the original biometrics might be exposed. Consequently, an ideal cancelable biometric scheme should take into consideration preventing unauthorized access to the original biometric templates while maintaining the biometric scheme's high performance. Furthermore, the cancelable biometric scheme should guarantee that authorized users can easily access the system with high recognition performance. Besides assuring high recognition, the cancelable biometric scheme should attain the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24745:2022 requirements [4]. The first requirement is to assure preventing the cross-matching of the biometric templates whether the templates have been obtained from the same or different biometrics. In other words, the correlation of various templates across different databases should be infeasible. The second requirement is to assure irreversibility in which infeasible to retrieve the original biometrics given the cancelable biometric template. A further condition restricts generating new cancelable templates before abolishing the old versions in order to protect the database if it has been compromised.

The aforementioned conditions arose the need to develop a cancelable biometric scheme to protect the original biometric by applying some encryption or transformation techniques. For instance, feature domain transformation can be deployed utilizing non-invertible transformation techniques such as polar and Cartesian transformations [5]. A further non-invertible transformation is the random projection technique [6], in which the extracted biometric feature is transformed by projecting it to a random space. Deep learning (DL) algorithms have recently proven noticeable results in supervised learning [7–9]. Since the cancelable biometrics scheme authorizes individuals based on their biometric features, it mainly includes supervised learning. Thus, deep learning techniques can achieve great success in this domain. Furthermore, deep learning uses multiple layers to abstract features the deeper the network gets. Its core use is Convolutional Neural Networks (CNN), in which features are extracted

by applying a series of filters to the biometric input [10]. Subsequently, the resulted images are reduced in size by utilizing a pooling layer.

A further protection level can be applied by implementing encryption methods before storing the cancelable biometrics in the database. One of the most efficient techniques is the utilization of chaotic encryption techniques [11]. Chaotic encryption has various characteristics such as non-periodicity, independency on initial conditions, and divergence. Thus, a small deviation in the biometric input results in a huge change in the whole generated cancelable template. These characteristics match the standards of securing the cancelable biometric sensors. In this work, both deep learning algorithms and chaos encryption techniques have been adopted.

The significant contributions of the proposed work are:

- Summarizing the recent related BSS frameworks utilized in biometric authentication and cybersecurity applications.
- Hybridizing of DL and chaos algorithms for implementing an efficient and robust cancelable BSS model to secure private user biometric information.
- Generating highly robust permutation and confusion matrices that are used as sensitive secret keys to produce the cancelable and ciphered biometric patterns.
- Testing different standardized color and grayscale biometric images for evaluating the proposed cancelable BSS model.
- Examining different security and recognition evaluation metrics to comprehensively assess the performance of the proposed cancelable BSS model.
- Performing deep comparisons to prove the superiority of the proposed cancelable BSS model compared to other related cancelable BSS models.

The remainder of this paper is organized as follows. Section 2 summarizes the recent security algorithms used in cancelable biometric applications. Section 3 introduces the proposed biometric security system. Section 4 discusses the security analysis and obtained results of the proposed BSS model. Finally, Section 5 presents the concluding remarks and some suggestions for future work.

2 Literature Review

Various approaches have been proposed in the literature for implementing biometric recognition schemes, as shown in Tab. 1. The authors of [12] deploy Discrete Cosine Transform (DCT) compression on four biometric images of the same person. Subsequently, the resulting image is encrypted using the Double Random Phase Encoding (DRPE) algorithm. At the receiver, the counter approach is implemented to decrypt the biometric. However, for the identity verification, the recognition method deploys a cepstral approach. Other research works deployed only one biometric sensor, such as the face or iris features, for implementing the security solution. For example, Sudhakar et al. extracted the iris features by combining random projection and deep learning algorithms to generate revocable biometrics [13].

Table 1: Summary of recent biometric security systems

Work	Goal and purpose	Biometric dataset	Technique	Tested parameters
[12]	To deploy cosine transformation and encryption techniques to assure the security of biometrics and storage savings.	ORL, CASIA-V3, CASIA-V1	DRPE, cepstral analysis, DCT	Fingerprint, palm, face recognition rate
[13]	To combine random projection and deep learning algorithms to generate revocable biometrics	IITD, MMU	Random projection, support vector machine	Accuracy and loss of CNN, confusion matrices
[14]	To provide the biometric system as a cloud service enabling fast response, intensive computing, and high accuracy.	IITD, MMU, FV-USM	Deep learning, random projection	10-fold cross validation, stratified 5-fold cross-validation, repeated random train test splits
[15]	To adopt a region-based technique in order to construct the cancelable biometric by extracting facial features using the CNN approach.	FERET, PaSC, LFW	Deep learning, bio-convolving encryption	Precision, recall, F-score
[16]	To apply several discrete transformations with multiple rotations to generate the cancelable face and fingerprint templates.	ORL, FERET, LFW	DFT, FrFT, DCT, DWT,	FAR, FRR, EER, histograms, probability distribution functions (PDF), ROC
[17]	To develop a cancelable face and iris system by extracting features using scale-invariant feature transform.	CASIA-IrisV3, ORL	Double random phase encoding, scale-invariant feature transform	Histograms, genuine and imposter distributions, AROC, EER, decidability metrics

(Continued)

Table 1: Continued

Work	Goal and purpose	Biometric dataset	Technique	Tested parameters
[18]	To generate non-invertible cancellable face templates by applying encryption and transformation techniques.	ORL, FERET, LFW	Random projection, intuitionistic fuzzy logic	Histograms, correlation scores, structural similarity index metric (SSIM)AROC
[19]	To develop a cancelable biometric recognition cryptosystem based on an asymmetric encryption algorithm.	ORL, FERET, LFW, FVC2002	Phase truncated Fourier transform	AROC, FRR, EER, FAR, PDF, histogram, execution time, correlation
[20]	To build cancelable biometrics using a hybrid optical encryption algorithm by implementing more permutation and diffusion	ORL, LFW, FVC2002	3D jigsaw transform, fractional fourier transform	PDF, AROC, histogram, correlation
[21]	To alter the biometrics using convolution kernels produced by various chaotic maps.	FVC2002	Chaos-based image encryption	PDF, FRR, and FAR
[22]	To hide all discriminative features of biometrics by employing genetic techniques	ORL, FERET, LFW, FVC2002	Genetic algorithm, crossover and mutation operations	Histogram, FRR, FAR, AROC, noise, processing time
[23]	To blur the biometric with two prime operators and retrieve it by calculating the GCD of the two blurred biometrics.	ORL, FVC2000, CASIA-IrisV3, CASIA palm	Greatest common divisor	visual analysis, entropy analysis, correlation analysis, differential attack analysis

(Continued)

Table 1: Continued

Work	Goal and purpose	Biometric dataset	Technique	Tested parameters
Proposed work	Design a secure and efficient cancelable biometric authentication system based on deep learning and cryptography techniques	Different biometric modalities (Faces, iris, and Fingerprints)	AE-based DL network and 2D chaotic logistic algorithm	Histograms, AROC distribution, correlation scores, visual inspection, SSIM scores, FAR, FRR, EER, mean and variance scores, processing time, noise analysis

On the other side, some existing solutions utilized the cloud as a platform to provide the biometric system as a cloud service enabling fast response, intensive computing, and high accuracy. In [14], the authors developed a CNN-based biometric system on the Amazon Web Services (AWS) cloud platform. By implementing cross folding algorithms and quick response (QR) code steganography technique, the CNN-based system on the cloud outperformed the standalone systems. Another CNN-based solution was proposed by [15] in which the facial features were extracted from different face regions to create the cancelable biometric.

In general, different transformation algorithms can be applied to biometrics such as DCT, Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and Fractional Fourier Transform (FrFT) to generate cancelable biometric templates. In [16], several discrete transformations such as DFT, FrFT, DCT, and DWT have been employed to generate the cancelable face and fingerprint templates. Furthermore, multiple rotations have been applied to ensure the irreversibility of the process. The authors of [17] developed a cancelable face and iris system by extracting features using scale-invariant feature transform. Subsequently, the extracted features were encrypted using the optical DRPE method.

In [18], the authors have applied sequential steps to generate non-invertible cancelable face templates. Initially, the grayscale pixels were transformed from the spatial domain into the fuzzy domain. As a pre-processing phase, the Intuitionistic Fuzzy Logic (IFL) was applied. Then, a further distortion was implemented via the Random Projection (RP). The authors of [19] developed a cancelable biometric recognition cryptosystem based on the optical Phase Truncated Fourier Transform (PTFT) asymmetric encryption by employing public keys. Consequently, the user can retrieve the original biometric by using two different private truncated keys. Ibrahim et al. applied more permutation and diffusion to create robust cancelable biometrics using a hybrid optical encryption algorithm resulting in more secure templates against attacks [20]. Mainly, the proposed hybrid system deployed the 3D jigsaw transform and FrFT to generate cancelable face and fingerprint templates.

Another implemented technique along with encryption is chaos-based ciphering to achieve better the loss of randomness. In [21], several cancelable templates were generated from the same biometric by applying different chaotic maps. El-Shafai et al. proposed a cancelable biometric scheme that hides all discriminative features of biometrics by employing a Genetic algorithm (GA) [22]. Initially, the GA

scans a set of biometric templates. Subsequently, successive sample sets were generated by applying some statistical operators to the original set of biometric templates. The final cancelable biometric templates were generated by performing crossover and mutation techniques.

An efficient solution proposed by [23] utilized the greatest common divisor (GCD) algorithm. To blur the biometric with two prime operators and retrieve it by calculating the GCD of the two generated cancelable biometrics. Thus, eliminating the need for extra data or images to generate the cancelable biometric. Due to some of the limitations in the related biometric security systems concerning lower robustness and security accomplishments, in this work, we proposed an efficient BSS model. This model is based on hybridizing AE-based DL and 2D CLM-based ciphering algorithms to secure and cipher the stored biometric patterns. The foremost merit of integrating DL and chaotic-based security algorithms for biometric authentication is accomplishing better-ciphering efficiency. The first step in the proposed BSS model is the generation of two chaotically and random security keys using an AE network with only three layers. Then, these two random security keys are used together for permutation and confusion purposes to completely cipher the user's biometric details. The first chaotic key is the utilized shuffling matrix used to permutate and shuffle the biometric image pixels. The second chaotic key is the employed confusion matrix used to distort the correlation between the permuted biometric pixels. The examined security and biometric recognition analyses prove the authentication and robustness superiority of the proposed BSS compared to other related BSS models.

3 Proposed Biometric Security System (BSS)

This section discusses the proposed BSS model based on the hybridization of deep learning and chaotic map algorithms in detail. Fig. 1 presents the primary steps of the proposed BSS model. It consists of two separate stages: the enrollment and authentication stages.

Although the chaos-based ciphering algorithms introduced high security & efficiency for encrypting the color & grayscale visual images, they still have some demerits regarding the ciphering key sensitivity. So, the hybridization of deep learning algorithms with chaos-based ciphering algorithms can improve image security performance. Thus, this inspired us to exploit both DL and chaos algorithms for securing the biometric images for implementing a more secure cancelable BSS model. Therefore, the proposed hybrid DL-chaos map ciphering technique is introduced to achieve better optimization performance towards improving the ciphering efficiency of biometric templates. Furthermore, the hybrid ciphering approach in the proposed BSS model performs extensive optimization and learning processes to generate sensitive and robust secret keys against various multimedia assaults and attacks.

The employed deep learning algorithm in the proposed BSS model uses an Auto-Encoder (AE) network as a pre-processing step prior to the chaos-based ciphering step to enhance and optimize the security efficiency by obtaining the main features and details in biometric images. These extracted features from the biometric templates are exploited to generate two different security keys (random chaos matrices). The first security key is exploited to produce a permutation matrix that is applied to scramble the pixels of biometric images. The second security key is used to generate a non-correlated random sequence (confusion matrix) that is exploited to further encrypt the permuted biometric images. Therefore, both permutation and confusion processes are utilized to cipher the biometric images sufficiently to hide all visual biometric details. The confusion process is performed using the 2D CLM algorithm [24].

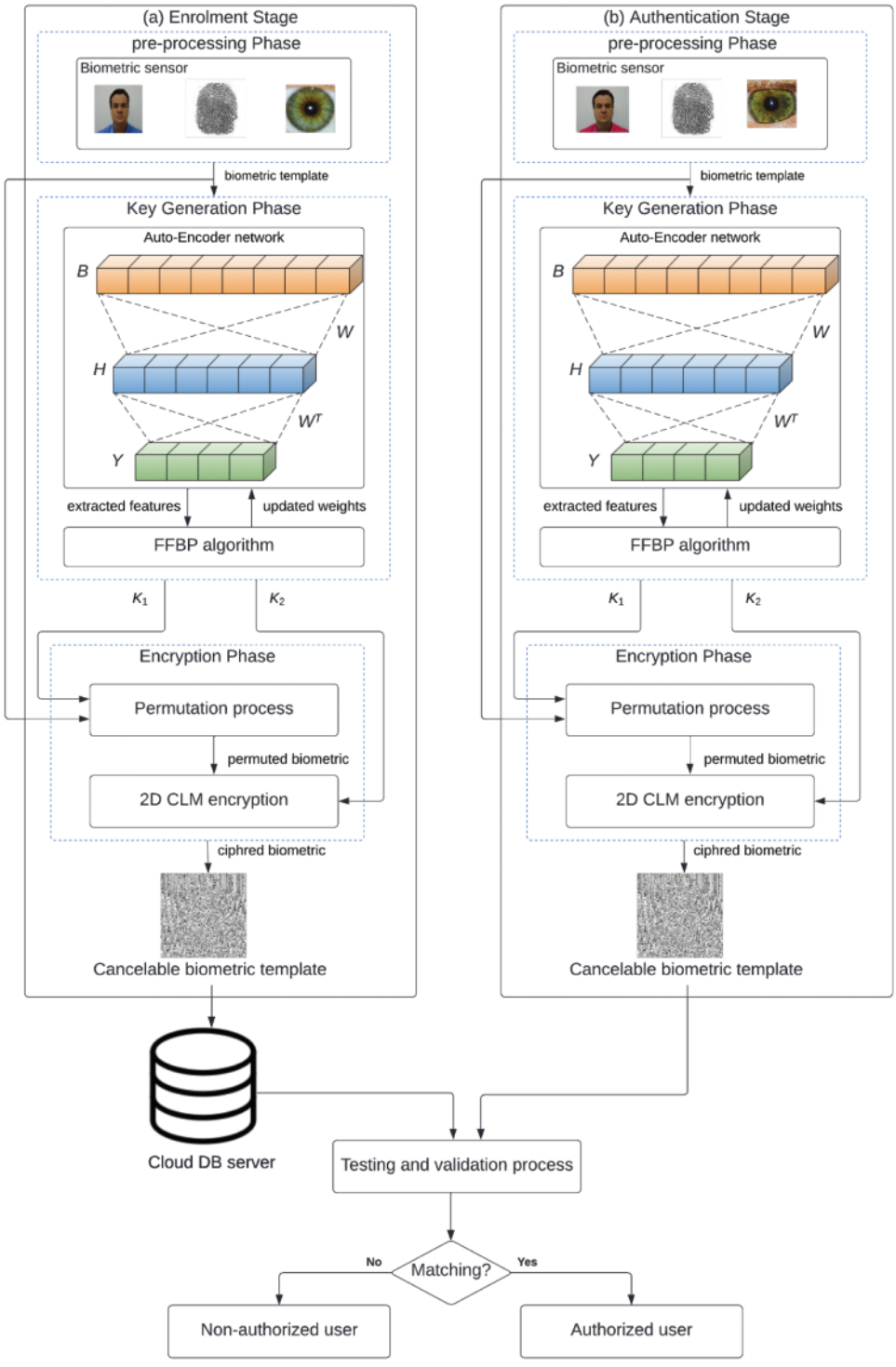


Figure 1: Proposed DL-chaos-based biometric security system

The utilized AE network in the proposed BSS model is an unsupervised network used for biometric feature extraction. So, the employed deep neural AE network is working based on the Feed-Forward Back-Propagation (FFBP) algorithm [25] in the generation process of the secret keys. Thus, the proposed BSS model can efficiently resist the possible attacks on the encrypted biometric templates. Besides, the main benefit of using the AE network in the proposed BSS model is its parallelization in processing and computation, thus decreasing the complexity and runtime of the proposed BSS model. In addition, because the utilized AE network is an unsupervised algorithm, there is no mandatory prerequisite for labeled and identified biometric data in the learning process.

As shown in Fig. 1, firstly, the user biometric images are captured using the biometric sensors, and then they are forwarded to the proposed structure of the AE network for training purposes. This is to generate new random matrices with similar dimensions to those of the input biometric images. Then, the FFBP algorithm is employed to efficiently generate the best possible randomness keys (K_1 and K_2).

The first key (K_1) is the random permutation key, while the second key (K2) is the random confusion key. Therefore, the key, K_1, is used to permutate the pixels' positions of biometric images. After that, the resulting permutated biometric images are further ciphered using the second key, K_2, by applying the 2D CLM algorithm. This algorithm performs the bit eXclusive OR (XOR) process between the permuted biometric image and the key, K_2, to produce the final ciphered biometric image that is stored in the cloud server instead of keeping the original biometric templates. Thus, the 2D CLM algorithm exploits the generated keys to further improve biometric image security and ciphering quality.

So, as shown in Fig. 1, the utilized hybrid DL-chaos-based ciphering algorithm in the proposed BSS model incorporates two sequential stages, which are (1) key generation stage and (2) encryption stage. The stacked AE network with only two stacks based on utilizing the FFBP algorithm is used in the key generation stage. In the encryption stage, both permutation and confusion mechanisms are performed using the generated secret keys from the first stage and the 2D CLM algorithm.

The stacked AE network used in the generation process of secret keys is considered the backbone stage of the biometric ciphering operation. It is an unsupervised deep neural structure with three consecutive layers stages (input, hidden, and output). First, the input layer collects the input biometric images and transfers their representation to another vector representation. Then, the single hidden layer takes a weighted version of the output vectors resulting from the preceding input layer. Finally, the hidden layer forwards the weighted decoding reconstruction vectors to the output layer. So, the input layer represents the encoder part of the utilized stacked AE network, while the output layer represents the decoder part. The values of weights and biases are initiated arbitrarily, and after that, they are updated iteratively during the back-propagation mechanism in the training process. The input and output parameters of the utilized stacked AE network are (1) encoder input (biometric vectors) $B_i = (B_1, B_2, \ldots., B_n)$, (2) hidden layer ($H$), (3) weighted matrix ($W$), (4) tied weighted matrix (W^T), (5) decoder output (reconstructed biometric vectors) $Y_o = (Y_1, Y_2, \ldots., Y_n)$, and (6) generated random keys (K_1 and K_2)

Through the operation of the FFBP algorithm, deep fine-tuning and optimization processes are performed to achieve better backward and forward secrecy during the key generation stage. In addition, the main benefit of using the FFBP algorithm in the training process of the proposed stacked AE structure is minimizing or removing the noise that can reduce the performance of the training efficiency of the AE network. This is to produce and generate the most effective randomization and robust secret keys. Therefore, integrating the DL-based AE network with the 2D CLM-based ciphering

algorithm reduces the number of iterations and achieves better ciphering and security of biometric images.

To generate efficient random and robust secret keys from the employed stacked AE network, different cost (error) and activation functions are utilized during the training process. So, in the operation of the FFBP algorithm, the softmax activation function [26] and cross-entropy error function [27] are used. This softmax activation function is based on a sigmoid function [28]. In addition, the stochastic gradient optimization algorithm [29] is applied in the training process of the utilized stacked AE network to minimize the training loss.

The best-generated secret keys are the ones that achieve the best uniform pixels distribution of the ciphered biometric images. So, in the training process of the stacked AE network, the minimization of the uniform distribution error is one of our main targets in the key generation process to produce the best efficient random secret keys. Thus, to obtain ciphered biometric images with a uniform pixels distribution, an error function is incorporated in the training stages of the stacked AE structure. This error function is calculated based on estimating the minimal value of the mean square error (MSE) between the ciphered biometric image and an image with pixel values of l (that has uniform distribution). The expression of the MSE function [30] utilized in the training process is given as follows:

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} (B_c(i,j) - l)^2 \tag{1}$$

where $B_c(i,j)$ is the ciphered biometric image and M & N are the dimension of the input image.

The authentication step in the proposed BSS model is the testing and evaluation process between the stored ciphered biometric templates and new input ciphered biometric images. This validation step is a mandatory process to check if the input user biometric image is a licensed template or an unlicensed template.

4 Results and Security Analysis

This section discusses and explains the obtained results and security analysis of the proposed BSS model. To comprehensively assess the proposed cancelable BSS model's efficiency, different security and recognition evaluation metrics [20–23] are examined. The objective evaluation parameters that are used to evaluate the proposed BSS model are (1) correlation scores, (2) SSIM, (3) EER, (4) false positive rate (FPR), (5) true positive rate (TPR), (6) AROC, (7) FRR, (8) FAR, (9) mean and variance of authorized and unauthorized patterns, and (10) computational time.

The ciphering process for biometric patterns was developed using Python programming and run on a Windows 10 machine with an Intel Core i7 processor and 8 Giga-Byte memory. Also, different standardized color and grayscale images from six various datasets [31–36] of faces, fingerprint, and iris biometrics were also tested in the evaluation analysis of the proposed cancelable BSS model. Fig. 2 shows the original image samples from the examined biometric datasets.

As shown in the following subsections, the security efficiency assessment of the proposed BSS model is investigated in terms of (1) visual ciphering analysis, (2) histogram analysis, (3) ROC and PDF analysis, (4) correlation and SSIM analysis, (5) recognition, security, and computational analysis, (6) noise analysis, (6) comparative analysis with other related and recent BSS models. For a simple presentation of all obtained simulation outcomes, we selected the objective and subjective results of only 15 sample images from each tested biometric dataset to be presented.

Figure 2: Original image samples from the examined biometric datasets

4.1 Visual Ciphering Analysis

This section presents the visual ciphering results of the proposed hybrid AE-based DL and chaos-based encryption algorithms used in the proposed BSS model. Fig. 3 introduces the encrypted biometrics of the examined users' samples for the six analyzed datasets. These ciphered biometric images prove the cancelability efficiency and security capability of the proposed BSS model in encrypting all details of recognized data within the biometric patterns. Also, the obtained results confirm that the proposed BSS model performed well for different modalities of user biometrics. Thus,

the proposed BSS model can be implemented and utilized efficiently in biometric authentication and cybersecurity applications.

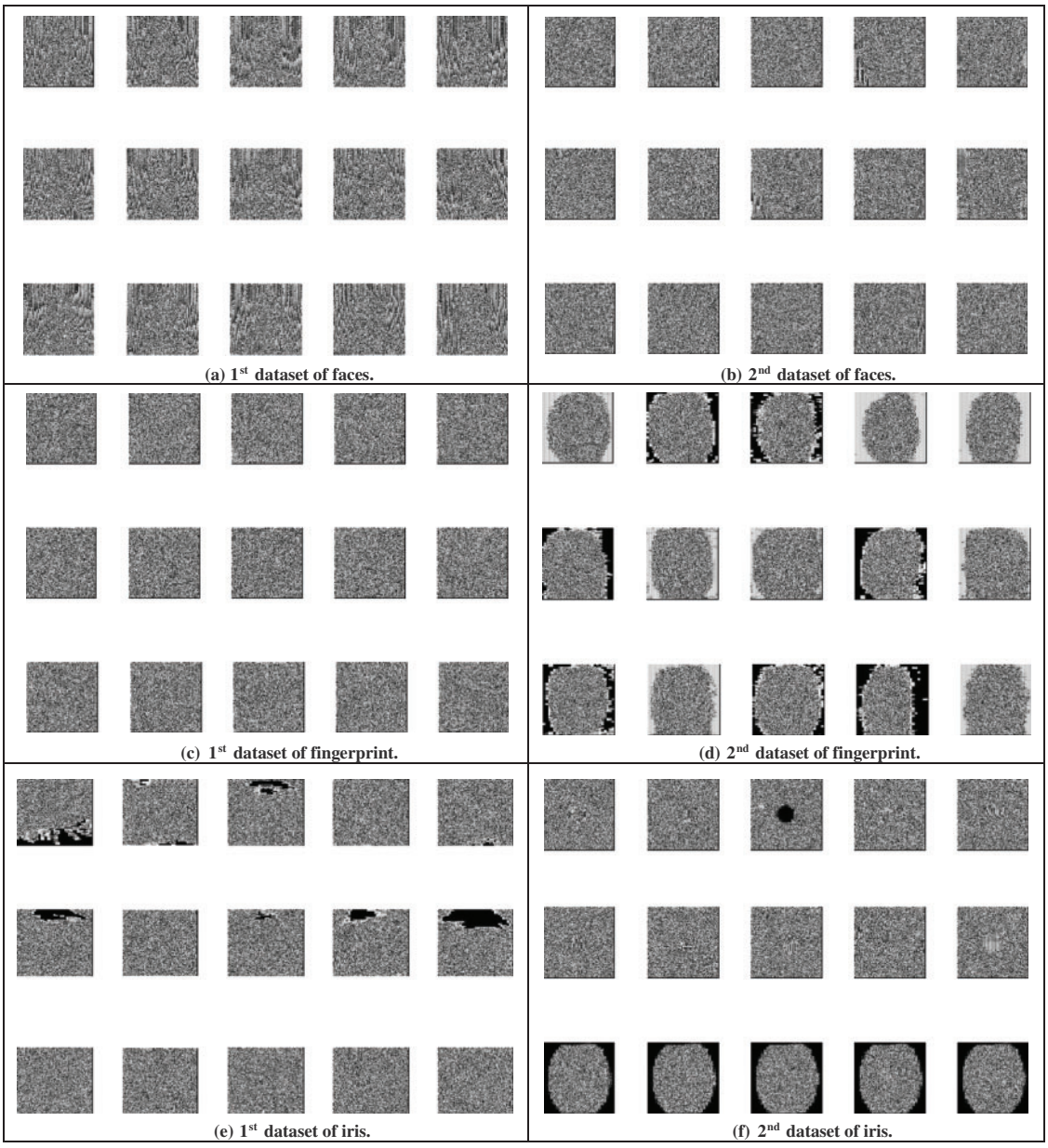


Figure 3: Encrypted biometrics of the examined user samples

4.2 Histogram Analysis

This section presents the visual histogram analysis of the proposed BSS model for the examined biometric samples. The histogram distribution is considered a subjective evaluation metric that is used to clarify the power density of the distributed pixels within biometric images. It is well known that the most efficient and secure ciphering algorithm in terms of mitigating statistical and intrusion attacks

is the one that can generate uniform histogram representation for the ciphered biometrics [37]. Also, it is the one that can produce entirely different histograms for the ciphered biometrics compared to those of their original biometrics.

Fig. 4 demonstrates the visual representation of the histograms of the original image samples from the analyzed biometric datasets presented in Fig. 2, while Fig. 5 offers the obtained visual histograms of the examined users' encrypted biometrics samples. It is observed that the histogram representations of the obtained ciphered biometric samples are totally different from those of the original ones. In addition, all histograms of encrypted biometrics have uniform distributions compared to those of the original ones. Thus, this proves the high security & efficiency of the proposed hybrid cryptography algorithm used in the proposed BSS model.

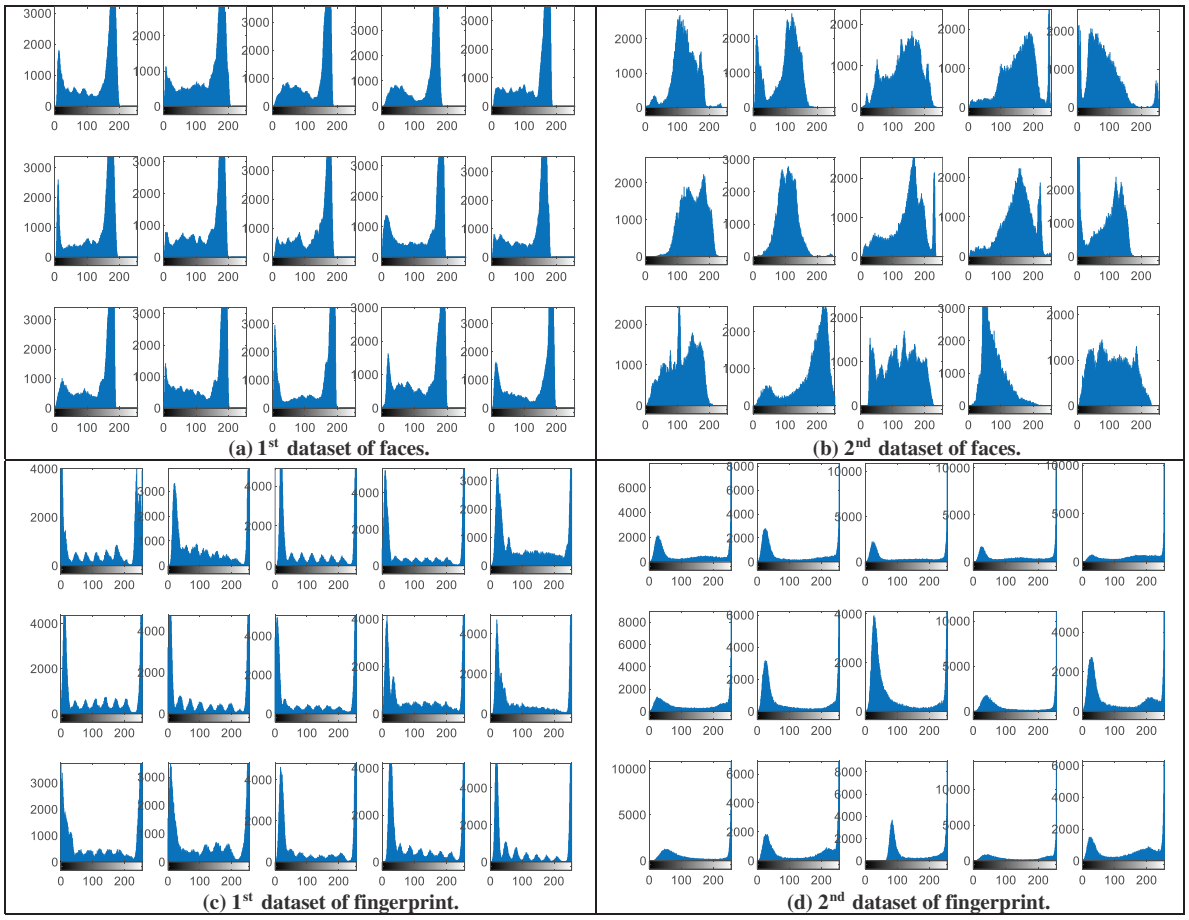
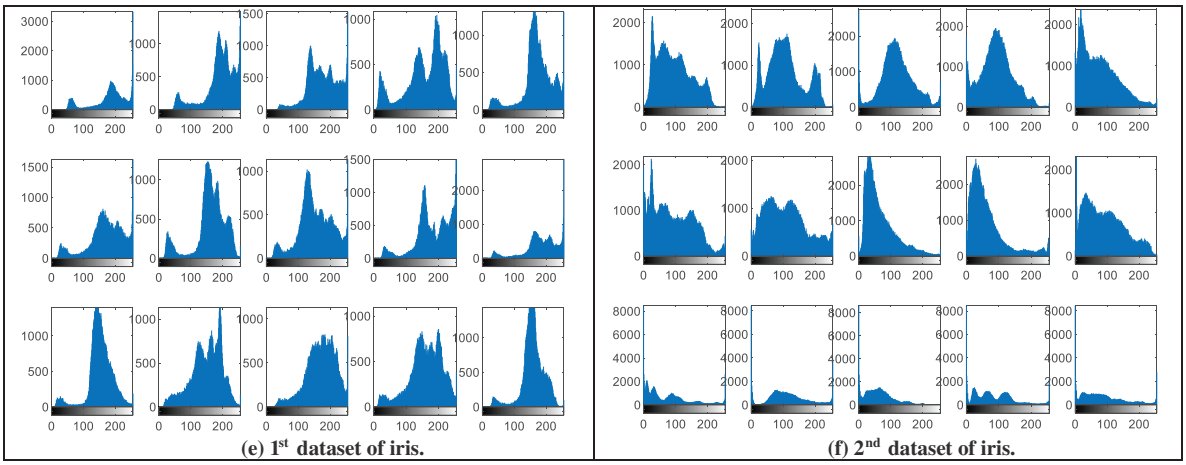
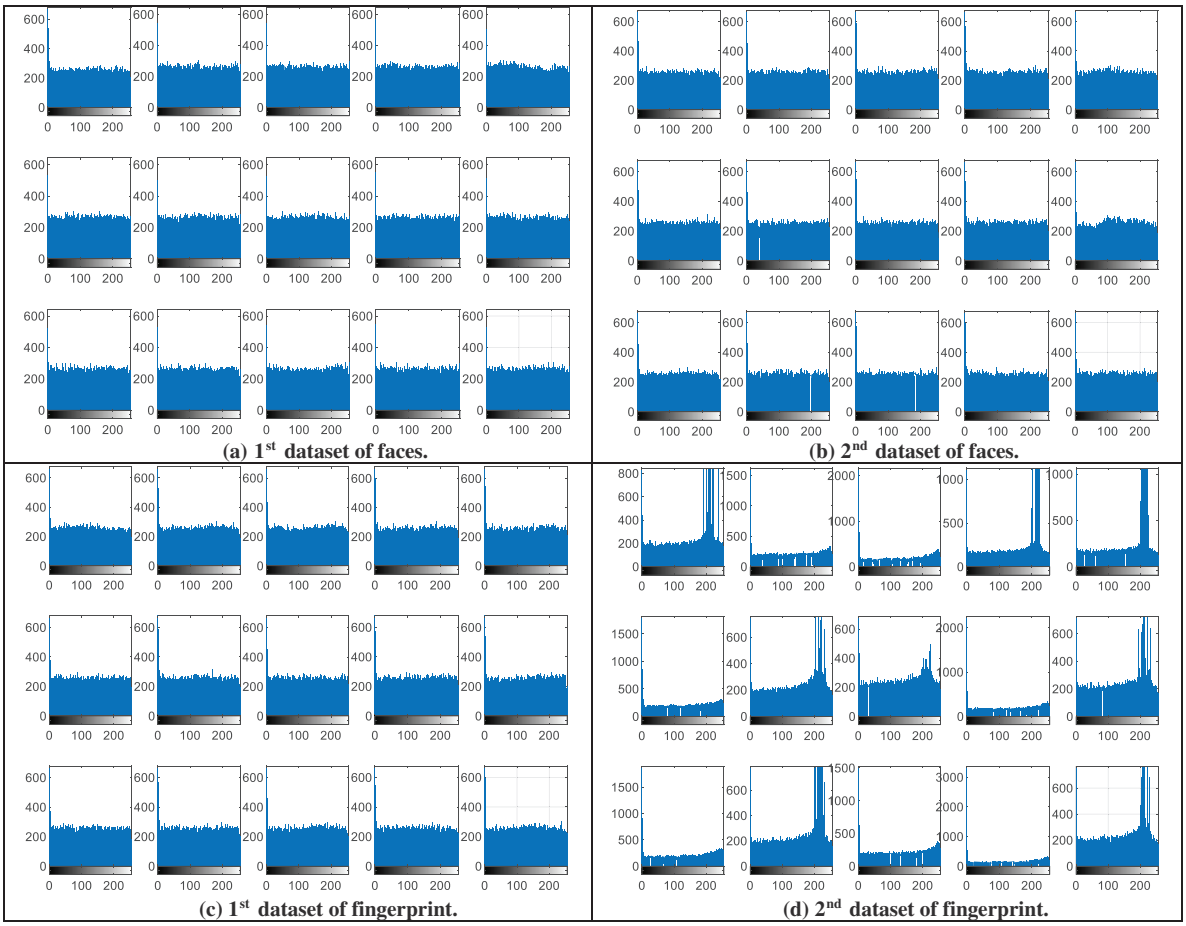


Figure 4: (Continued)



(e) 1st dataset of iris. (f) 2nd dataset of iris.

Figure 4: Histograms of the original image samples from the examined biometric datasets



(a) 1st dataset of faces. (b) 2nd dataset of faces.

(c) 1st dataset of fingerprint. (d) 2nd dataset of fingerprint.

Figure 5: (Continued)

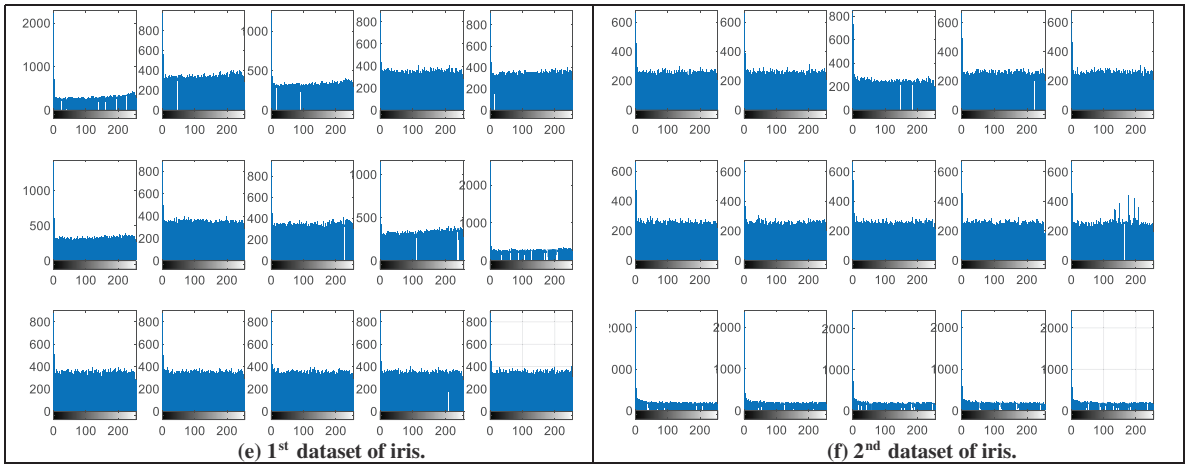


Figure 5: Histograms of encrypted biometrics of the examined users samples

4.3 ROC and PDF Analysis

This section discusses the ROC and PDF analysis of the proposed BSS model. The ROC distribution shows the percentage and relation between FPR and TPR values of the biometric authentication system. The PDF distribution offers the representation of the density function of the correlation scores for license and unlicensed patterns. Fig. 6 displays the ROC and correlation score distributions of the stored encrypted biometrics of the examined user samples for the six analyzed datasets. The obtained ROC distributions confirm that the proposed BSS model achieves high TPR values that near to be ideal for all analyzed biometric samples. In addition, the attained PDF distributions prove that they achieved high correlation scores for the biometric patterns of the licensed users and low correlation scores for the biometric patterns of the unlicensed users. Moreover, it is demonstrated that there are no intersections between the PDF of the licensed patterns and unlicensed patterns; thus, the proposed BSS model achieves low ERR percentages. Therefore, all these ROC and PDF results verify the high performance of the proposed biometric security system's authentication, robustness, and recognition.

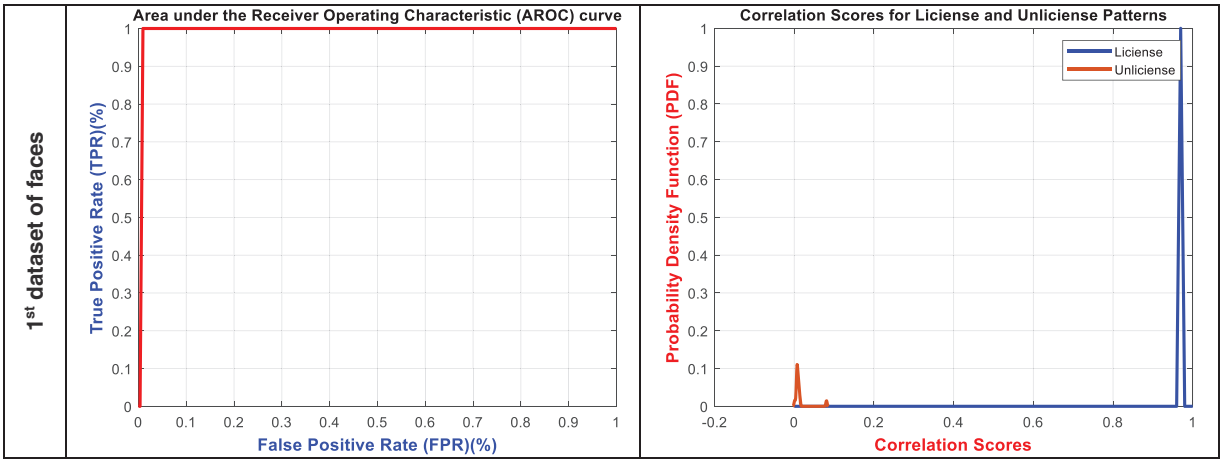


Figure 6: (Continued)

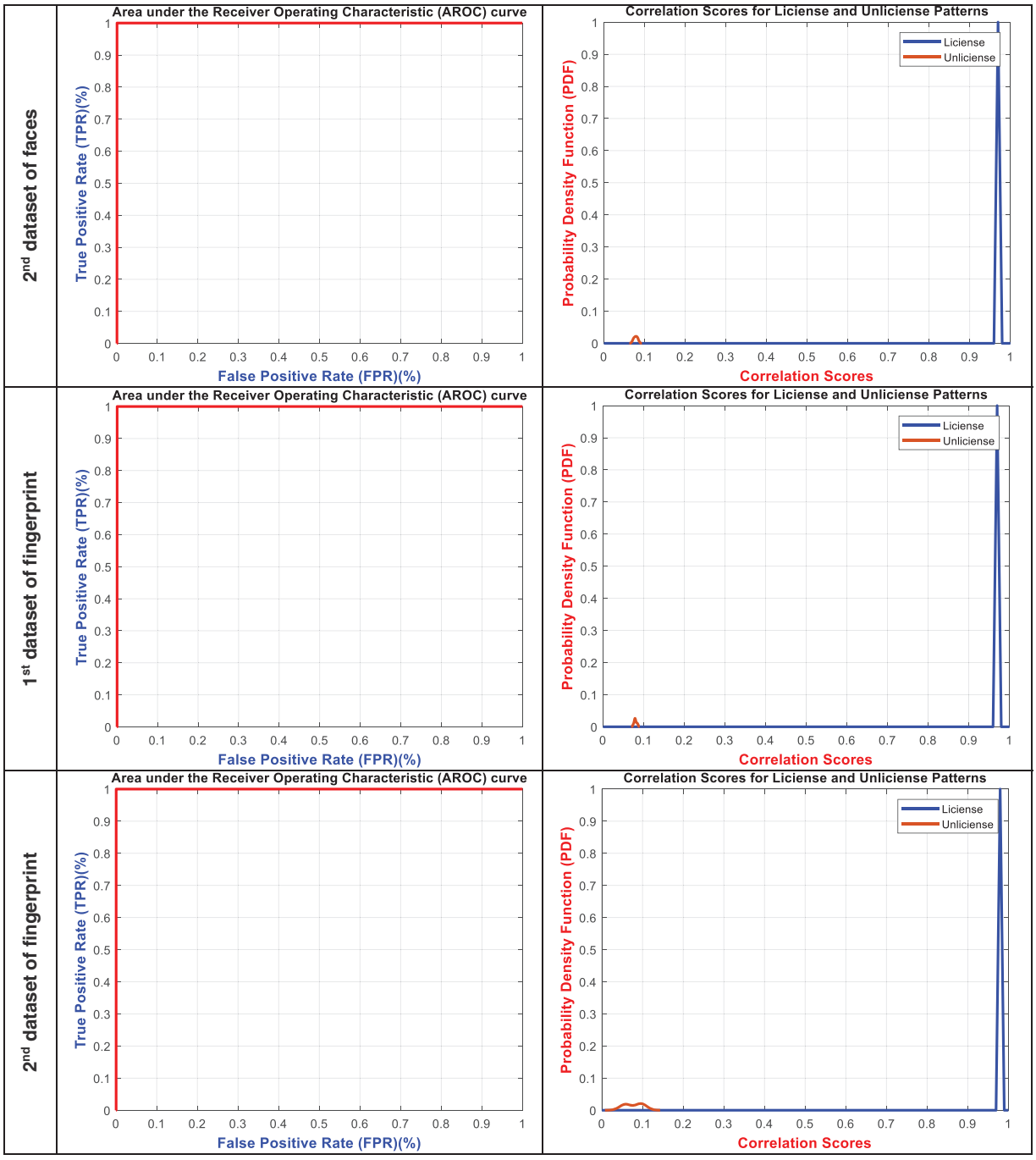


Figure 6: (Continued)

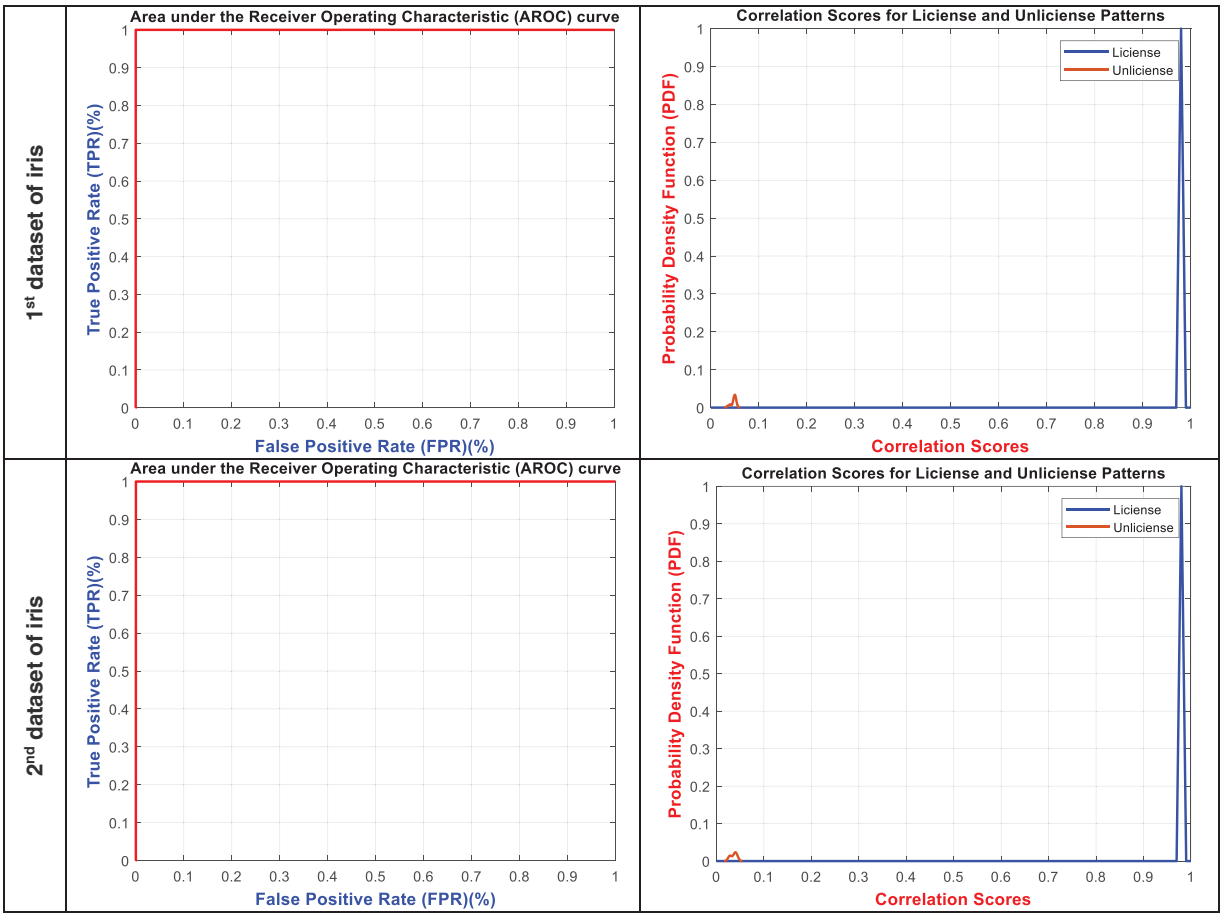


Figure 6: ROC and correlation score distributions of the stored encrypted biometrics

4.4 SSIM and Correlation Analysis

To further confirm the achieved security and recognition results in Section 4.3, the numerical analysis of the SSIM and correlation scores for the proposed BSS model is presented in this section. In the experimental study, we investigated the authentication performance of two recognition cases. The first case compares the encrypted biometrics of licensed users with the stored encrypted biometrics, while the second case compares the encrypted biometrics of unlicensed users with the stored encrypted biometrics. These recognition comparisons and authentication tests are examined using two standard statistical objective evaluation metrics: SSIM and correlation coefficients [37].

Tabs. 2 and 3 offer the numerical SSIM and correlation scores of the stored encrypted biometrics with licensed and unlicensed encrypted biometrics. These numerical results show that the proposed BSS model attains high SSIM and correlation scores for the encrypted biometrics of licensed users. On the other hand, it achieves low SSIM and correlation scores for the encrypted biometrics of unlicensed users for all tested biometric datasets. Thus, the proposed BSS model can efficiently differentiate between licensed and unlicensed patterns when they are compared to the stored encrypted patterns, and therefore, it can mitigate the possible trials of intrusion attacks.

Table 2: Numerical SSIM scores of the stored encrypted biometrics with licensed and unlicensed encrypted biometrics

Sample no.	SSIM score with a licensed biometric/SSIM score with an unlicensed biometric					
	1st dataset of faces	2nd dataset of faces	1st dataset of fingerprint	2nd dataset of fingerprint	1st dataset of iris	2nd dataset of iris
#1	0.9624/0.0325	0.9638/0.0234	0.9634/0.0311	0.8935/0.0374	0.8719/0.0150	0.9643/0.0195
#2	0.9699/0.0036	0.9640/0.0285	0.9642/0.0352	0.8795/0.0124	0.9532/0.0205	0.9642/0.0141
#3	0.9686/0.0044	0.9637/0.0224	0.9642/0.0284	0.8569/0.0176	0.9389/0.0221	0.9630/0.0200
#4	0.9691/0.0003	0.9648/0.0246	0.9647/0.0282	0.8005/0.0352	0.9663/0.0262	0.9643/0.0177
#5	0.9676/0.0086	0.9605/0.0315	0.9644/0.0262	0.8035/0.0370	0.9615/0.0183	0.9641/0.0160
#6	0.9696/0.0022	0.9641/0.0259	0.9648/0.0255	0.8580/0.0204	0.9184/0.0156	0.9647/0.0150
#7	0.9695/0.0072	0.9644/0.0289	0.9634/0.0269	0.9120/0.0339	0.9647/0.0227	0.9652/0.0219
#8	0.9686/0.0062	0.9631/0.0278	0.9642/0.0247	0.9456/0.0340	0.9616/0.0192	0.9650/0.0196
#9	0.9699/0.0028	0.9639/0.0384	0.9640/0.0294	0.8212/0.0200	0.9317/0.0221	0.9623/0.0146
#10	0.9694/0.0080	0.9552/0.0325	0.9643/0.0329	0.9249/0.0321	0.8317/0.0209	0.9585/0.0165
#11	0.9685/0.0088	0.9638/0.0320	0.9643/0.0320	0.8702/0.0187	0.9665/0.0170	0.7719/0.0040
#12	0.9689/0.0088	0.9635/0.0313	0.9648/0.0275	0.8956/0.0412	0.9663/0.0214	0.7742/0.0026
#13	0.9683/0.0041	0.9634/0.0248	0.9638/0.0262	0.8938/0.0180	0.9659/0.0207	0.7677/0.0052
#14	0.9683/0.0049	0.9641/0.0243	0.9640/0.0289	0.7274/0.0125	0.9664/0.0234	0.7708/0.0022
#15	0.9698/0.0086	0.9640/0.0275	0.9632/0.0258	0.9021/0.0373	0.9656/0.0221	0.7722/0.0030
Average	**0.9686/0.0070**	**0.9631/0.0289**	**0.9641/0.0286**	**0.8656/0.0272**	**0.9420/0.0205**	**0.8975/0.0128**

Table 3: Numerical correlation scores of the stored encrypted biometrics with license and unlicensed encrypted biometrics

Sample no.	Correlation score with a licensed biometric/Correlation score with an unlicensed biometric					
	1st dataset of faces	2nd dataset of faces	1st dataset of fingerprint	2nd dataset of fingerprint	1st dataset of iris	2nd dataset of iris
#1	0.9740/0.0808	0.9742/0.0721	0.9738/0.0826	0.9748/0.0963	0.9809/0.0395	0.9745/0.0426
#2	0.9735/0.0077	0.9744/0.0765	0.9741/0.0861	0.9811/0.0547	0.9752/0.0495	0.9745/0.0351
#3	0.9735/0.0059	0.9746/0.0823	0.9746/0.0781	0.9833/0.0558	0.9770/0.0476	0.9761/0.0392
#4	0.9734/0.0073	0.9751/0.0729	0.9747/0.0763	0.9741/0.1001	0.9741/0.0545	0.9745/0.0406
#5	0.9731/0.0018	0.9743/0.0823	0.9746/0.0759	0.9739/0.0994	0.9743/0.0481	0.9744/0.0386
#6	0.9728/0.0077	0.9745/0.0761	0.9747/0.0752	0.9814/0.0624	0.9775/0.0389	0.9745/0.0391
#7	0.9729/0.0101	0.9745/0.0795	0.9742/0.0780	0.9747/0.0893	0.9734/0.0508	0.9749/0.0438
#8	0.9727/0.0120	0.9744/0.0778	0.9746/0.0751	0.9743/0.0879	0.9748/0.0474	0.97480.0430
#9	0.9730/0.0006	0.9746/0.0859	0.9744/0.0800	0.9830/0.0581	0.9761/0.0496	0.9742/0.0382
#10	0.9731/0.0091	0.9733/0.0833	0.9747/0.0846	0.9748/0.0887	0.9807/0.0341	0.9738/0.0400
#11	0.9734/0.0137	0.9744/0.0814	0.9744/0.0811	0.9823/0.0601	0.9738/0.0462	0.9811/0.0293
#12	0.9727/0.0120	0.9742/0.0802	0.9744/0.0779	0.9747/0.1026	0.9740/0.0500	0.9813/0.0278
#13	0.97350.0059	0.9744/0.0756	0.9743/0.0770	0.9812/0.0589	0.9739/0.0497	0.9811/0.0270
#14	0.9730/0.0069	0. 9744/0.0727	0.9741/0.0801	0.9851/0.0459	0.9737/0.0526	0.9808/0.0295
#15	0.9728/0.0084	0. 9744/0.0763	0.9740/0.0776	0.9746/0.0961	0.9739/0.0520	0.9814/0.0276
Average	**0.9732/0.0133**	**0.9744/0.0783**	**0.9744/0.0790**	**0.9782/0.0771**	**0.97550.0474**	**0.9768/0.0361**

4.5 Recognition, Security, and Computational Analysis

The recognition and authentication efficiency of the proposed BSS model can be evaluated by different quantitative assessment recognition, security, and computational parameters such as AROC, FAR, the mean & variance of licensed and unlicensed patterns, FRR, EER, and computational processing time. Tab. 4 presents the obtained numerical values of the average recognition, security, and computational metrics of the examined biometric datasets. These results confirm the authentication and recognition efficacy of the proposed BSS model in identifying and recognizing the biometric input patterns. Furthermore, it is demonstrated that the proposed biometric security system achieves high values for AROC and mean of licensed patterns, which indicates higher recognition efficiency for the proposed system. On the other hand, the proposed security system achieves low values for EER, FRR, FAR, mean of unlicensed patterns, and variance of licensed and unlicensed patterns, proving that the proposed BSS model has a low false detection rate.

Table 4: Average recognition, security, and computational metrics of the examined biometric datasets

Metric	1st dataset of faces	2nd dataset of faces	1st dataset of fingerprint	2nd dataset of fingerprint	1st dataset of iris	2nd dataset of iris
AROC	0.9996	0.9997	0.9996	0.9997	0.9998	0.9998
EER	0.0023	0.0018	0.0024	0.0005	0.0005	0.0007
FRR	0.0048	0.0019	0.0003	0.0007	0.0006	0.0006
FAR	0.0027	0.0023	0.0009	0.0011	0.0012	0.0012
Mean of licensed patterns	0.9732	0.9744	0.9743	0.9782	0.9756	0.9768
Mean of unlicensed patterns	0.0131	0.0781	0.0798	0.0780	0.0474	0.0361
Variance of licensed patterns	1.5638×10^{-07}	1.7183×10^{-07}	6.5185×10^{-08}	1.8203×10^{-05}	5.6643×10^{-06}	1.0366×10^{-05}
Variance of unlicensed patterns	3.6095×10^{-04}	1.7202×10^{-05}	1.1003×10^{-05}	4.3293×10^{-04}	2.9570×10^{-05}	3.7827×10^{-05}
Computational time (s)	1.6253	1.6985	1.7523	1.8694	1.8069	1.5273

In addition, it is clarified that the proposed hybrid ciphering algorithm used in the proposed security model introduces low computational time in encrypting the biometric patterns before storing in cloud servers. Thus, the proposed BSS model is recommended to be implemented efficiently in real-time biometric authentication and cybersecurity applications.

4.6 Noise Analysis

To further approve the authentication efficacy of the proposed BSS model, it is important to study its sensitivity and recognition performance in the case of existing possible noise attacks on the collected biometric patterns. For testing the sensitivity efficiency of the proposed security model against noise attacks, we examined the recognition performance in terms of AROC and EER parameters at different

values of Gaussian noise variances. Tab. 5 demonstrates the noise analysis results of the AROC and EER security metrics of all examined biometric datasets. It is observed that the proposed BSS model has low sensitivity against noise attacks as it still achieves high AROC and low ERR values at high noise variance. Thus, the proposed BSS model can recognize the input biometrics proficiently with and without noise.

Table 5: Noise analysis results in terms of AROC and EER security metrics of the examined biometric datasets

Variance of noise	AROC/EER					
	1st dataset of faces	2nd dataset of faces	1st dataset of fingerprint	2nd dataset of fingerprint	1st dataset of iris	2nd dataset of iris
0.0	0.9996/0.0023	0.9997/0.0018	0.9996/0.0024	0.9997/0.0005	0.9998/0.0005	0.9998/0.0007
0.01	0.9991/0.0069	0.9991/0.0019	0.9992/0.0038	0.9992/0.0014	0.9991/0.0032	0.9994/0.0024
0.02	0.9985/0.0074	0.9987/0.0026	0.9984/0.0049	0.9987/0.0029	0.9983/0.0047	0.9989/0.0039
0.03	0.9980/0.0079	0.9986/0.0038	0.9978/0.0063	0.9982/0.0037	0.9972/0.0063	0.9982/0.0052
0.04	0.9974/0.0082	0.9981/0.0050	0.9971/0.0082	0.9973/0.0069	0.9963/0.0072	0.9976/0.0074
0.05	0.9965/0.0084	0.9978/0.0076	0.9965/0.0120	0.9964/0.0125	0.9951/0.0104	0.9970/0.0086

4.7 Comparative Analysis

To ensure that the proposed BSS model is highly efficient in differentiating between the licensed and unlicensed patterns, we carried out further experiments to compare the proposed model's efficiency with the authentication performance of the preceding and recent BSS models [16–23] in terms of calculating the AROC, FAR, ERR, and FRR recognition parameters. Tab. 6 offers the comparative analysis results for the proposed biometric security system and recent related systems. The obtained values of all examined security parameters for the proposed BSS model confirm its authentication and recognition superiority compared to other related BSS models.

Table 6: Comparative analysis for the proposed biometric security system and recent related systems

System	AROC	EER	FRR	FAR
Proposed	0.9997	0.00137	0.00148	0.00157
[16]	0.998	0.0023	0.003	0.008
[17]	0.868	0.0924	0.0257	0.0562
[18]	0.952	0.0098	0.018	0.0104
[19]	0.9996	0.0019	0.0012	0.0030
[20]	0.9867	0.0178	0.0579	0.0071
[21]	0.9614	0.0059	–	–
[22]	0.9998	0.00202	0.0023	0.00488
[23]	0.9680	0.0023	0.0024	0.0182

5 Conclusion and Future Works

Authenticating users to control their access to different buildings, systems or services has become essential these days. Biometric-based authentication approaches, including faces, iris, and fingerprints, are heavily used in such contexts. However, ensuring the confidentiality of these biometrics is important to guarantee the efficiency of the provided authentication services. Many existing systems try to store these biometrics encrypted to avoid any unattended disclosure that might cause misuse of these biometrics and allow intruders to gain illegal access to systems and resources. However, the existing approaches vary in their efficiency in terms of security and complexity. Therefore, this paper competes with related work by integrating the unsupervised auto-encoder (AE) network and chaos-based ciphering algorithm to secure and cipher the details of the stored biometric patterns to build an efficient biometric security system (BSS). The proposed BSS was heavily assessed through different evaluation metrics and compared with recent related work. The experiments' results revealed the outperformance of the proposed BSS from security and recognition capabilities compared to exiting biometric-based authentication systems.

In future work, we plan to fuse different biometrics to authenticate the users. Moreover, different deep learning would be investigated with the aim of enhancing the biometrics-based authentication system. Additionally, other biometrics datasets could be collected and tested. Furthermore, we target to study other security parameters to test the recognition and security accomplishment of the proposed biometric system.

Acknowledgement: We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. In addition, the authors would like to acknowledge the support of Prince Sultan University, especially the Security Engineering Lab (SEL).

Funding Statement: We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Singh, C. Vashist, P. Gaurav and A. Nigam, "A generic framework for deep incremental cancelable template generation," *Neurocomputing*, vol. 4, no. 6, pp. 83–98, 2022.

[2] N. Kumar, "CBRW: A novel approach for cancelable biometric template generation based on 1-D random walk," *Applied Intelligence*, vol. 6, pp. 1–19, 2022.

[3] I. Badr, A. Radwan, E. EL-Rabaie, L. Said, G. El Banby *et al.,* "Cancellable face recognition based on fractional-order lorenz chaotic system and haar wavelet fusion," *Digital Signal Processing*, vol. 11, 3, no. 6, pp. 1–25, 2021.

[4] A. Sarkar and B. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 27721–27776, 2020.

[5] N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artificial Intelligence Review*, vol. 53, no. 5, pp. 3403–3446, 2020.

[6] J. Peng, B. Yang, B. Gupta, A. El-Latif and A. Ahmed, "A biometric cryptosystem scheme based on random projection and neural network," *Soft Computing*, vol. 25, no. 11, pp. 7657–7670, 2021.

[7] K. Sundararajan and D. Woodard, "Deep learning for biometrics: A survey," *ACM Computing Surveys*, vol. 51, no. 3, pp. 1–34, 2018.

[8] H. Sun and R. Grishman, "Lexicalized dependency paths based supervised learning for relation extraction," *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 861–870, 2022.
[9] H. Sun and R. Grishman, "Employing lexicalized dependency paths for active learning of relation extraction," *Intelligent Automation & Soft Computing*, vol. 34, no. 3, pp. 1415–1423, 2022.
[10] A. AlDuwaile and M. Islam, "Using convolutional neural network and a single heartbeat for ECG biometric recognition," *Entropy*, vol. 23, no. 6, pp. 73–83, 2021.
[11] R. Sujarani, D. Manivannan, R. Manikandan and B. Vidhyacharan, "Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications," *Wireless Personal Communications*, vol. 9, no. 3, pp. 2517–2537, 2021.
[12] Y. Zakaria, R. Nassar, O. Zahran, G. Hussein, E. El-Rabaie *et al.,* "Cancelable multi-biometric security system based on double random phase encoding and cepstral analysis," *Multimedia Tools and Applications*, vol. 78, no. 22, pp. 32333–32355, 2021.
[13] T. Sudhakar and M. Gavrilova, "Multi-instance cancelable biometric system using convolutional neural network," in *Proc. of IEEE Int. Conf. on Cyberworlds (CW)*, Kyoto, Japan, pp. 287–294, 2019.
[14] T. Sudhakar and M. Gavrilova, "Cancelable biometrics using deep learning as a cloud service," *IEEE Access*, vol. 8, pp. 112932–112943, 2020.
[15] E. Abdellatef, N. Ismail, S. Abd Elrahman, K. Ismail, M. Rihan *et al.,* "Cancelable multi-biometric recognition system based on deep learning," *The Visual Computer*, vol. 36, no. 6, pp. 1097–1109, 2020.
[16] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.,* "Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications," *Entropy*, vol. 22, no. 12, pp. 13–27, 2020.
[17] R. Soliman, G. El Banby, A. Algarni, M. Elsheikh, N. Soliman *et al.,* "Double random phase encoding for cancelable face and iris recognition," *Applied Optics*, vol. 57, no. 35, pp. 10305–10316, 2018.
[18] A. Algarni, G. El Banby, N. Soliman, F. El-Samie and A. Iliyasu, "Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition," *Electronics*, vol. 9, no. 6, pp. 10–36, 2020.
[19] A. Alarifi, M. Amoon, M. Aly and W. El-Shafai, "Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system," *IEEE Access*, vol. 8, pp. 221246–221268, 2020.
[20] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafai *et al.,* "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 14053–14078, 2020.
[21] I. Bendib, A. Meraoumia, M. Haouam and L. Laimeche, "A new cancelable deep biometric feature using chaotic maps," *Pattern Recognition and Image Analysis*, vol. 32, no. 1, pp. 109–128, 2022.
[22] W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby and A. Elshafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access*, vol. 9, pp. 77675–77692, 2021.
[23] N. Soliman, A. Algarni, W. El-Shafai, F. Abd El-Samie and G. El Banby, "An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics," *CMC-Computers Materials & Continua*, vol. 69, no. 2, pp. 1571–1595, 2021.
[24] N. Pareek, V. Patidar and K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.
[25] S. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors and Microsystems*, vol. 77, no. 10, pp. 31–54, 2020.
[26] S. Sharma and A. Athaiya, "Activation functions in neural networks," *Towards Data Science*, vol. 6, no. 12, pp. 310–316, 2017.
[27] Y. Aurelio, G. Almeida, C. Castro and A. Braga, "Learning from imbalanced data sets with weighted cross-entropy function," *Neural Processing Letters*, vol. 50, no. 2, pp. 1937–1949, 2019.
[28] J. Han and C. Moraga, "The influence of the sigmoid function parameters on the speed of backpropagation learning," in *Proc. of Int. Workshop on Artificial Neural Networks (IWANN)*, Berlin, Heidelberg, Springer, pp. 195–201, 1995.

[29] R. Sweke, W. Frederik, M. Johannes, S. Maria, K. Paul *et al.,* "Stochastic gradient descent for hybrid quantum-classical optimization," *Quantum Computing*, vol. 4, no. 3, pp. 1–22, 2020.
[30] D. Allen, "Mean square error of prediction as a criterion for selecting variables," *Technometrics*, vol. 13, no. 3, pp. 469–475, 1971.
[31] FEI Faces Dataset, [Online]. Available: https://fei.edu.br/~cet/facedatabase.html (Last Access on 23-3-2022).
[32] UFI Faces Dataset, [Online]. Available: http://ufi.kiv.zcu.cz/ (Last Access on 23-3-2022).
[33] FVC DB-A Fingerprint Dataset, [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp (Last Access on 23-3-2022).
[34] CASIA Fingerprint Dataset, [Online]. Available: Http://www.biometrics.idealtest.org (Last Access on 23-3-2022).
[35] CASIA-IntervalV3 Iris Dataset, [Online]. Available: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp (Last Access on 23-3-2022).
[36] Libor Machala Iris Database, [Online]. Available: http://phoenix.inf.upol.cz/iris/ (Last Access on 23-3-2022).
[37] K. Byeong-Ho, "A review on image and video processing," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 2, no. 2, pp. 25–49, 2007.