IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 17, 2021, accepted May 14, 2021, date of publication May 24, 2021, date of current version June 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3082940

Efficient and Secure Cancelable Biometric Authentication Framework Based on Genetic Encryption Algorithm

WALID EL-SHAFAI[1,2], FATMA A. HOSSAM ELDEIN MOHAMED[3], HASSAN M. A. ELKAMCHOUCHI[3], (Life Senior Member, IEEE), MOHAMMED ABD-ELNABY[4], AND AHMED ELSHAFEE[5]

[1]Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[2]Security Engineering Laboratory, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Alexandria University, Alexandria 21527, Egypt
[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[5]Department of Electrical Engineering, Faculty of Engineering, Ahram Canadian University, 6th October City 12451, Egypt

Corresponding author: Walid El-Shafai (eng.waled.elshafai@gmail.com)

This work was supported by Taif University Researchers Supporting Project Number (TURSP-2020/147), Taif university, Taif, Saudi Arabia.

ABSTRACT Various cancelable biometric techniques have been proposed to maintain user data security. In this work, a cancelable biometric framework is introduced to satisfy user data security and keeping the original biometric template safe away from intruders. Thus, our main contribution is presenting a novel authentication framework based on the evolutionary Genetic Algorithm (GA)-based encryption technique. The suggested framework produces an entirely unrecognized biometric template by hiding the whole discriminative features of biometric templates; this is with exploiting the outstanding characteristics of the employed Genetic operations of the utilized encryption technique. Firstly, the GA initiates its search from a population of templates, not a single template. Secondly, some statistical operators are used to exploit the resulting initial population to generate successive populations. Finally, the crossover and mutation operations are performed to produce the ultimate cancelable biometric templates. Different biometric databases of the face and fingerprint templates are tested and analyzed. The proposed cancelable biometric framework achieves appreciated sensitivity and specificity results compared to the conventional OSH (Optical Scanning Holography) algorithm. It accomplishes recommended outcomes in terms of the AROC (Area under the Receiver Operating Characteristic) and the probability correlation distribution between the original biometrics and the encrypted biometrics stored in the database. The experimental results prove that the proposed framework achieves excellent results even if the biometric system suffers from different noise ratios. The proposed framework achieves an average AROC value of 0.9998, an EER (Equal Error Rate) of 2.0243×10^{-4}, FAR (False Acceptance Rate) of 4.8843×10^{-4}, and FRR (False Rejection Rate) of 2.2693×10^{-4}.

INDEX TERMS Cancelable biometrics, GA, OSH, crossover, mutation, AROC, EER, FAR, FRR.

I. INTRODUCTION

Biometric recognition has been improved speedily and is almost used in our life daily. The biometric techniques recognize and verify the unique features accurately, rapidly, and appropriately to control the entry process in dedicated systems or applications [1]–[3]. It is essential to control the access process and prevent intruders from compromising or recognizing the original templates.

User Biometrics are divided into physical features and logical features [4], [5]. The unique physical features are defined as the face, iris, retina, palm print, and fingerprint, but the features which are called logical or behavioural features are measured by the behaviour of the body and its reaction against the different circumstances such as voice, signature, keystrokes pattern, and walking style.

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenhua Guo.

All of these biometric techniques measured traits or characteristics of our human body, which are employed to verify that no intruders can access or control the access to the services rendered [6]–[8]. Traditionally, tokens and passwords are applied to prevent the cryptographic key from being stolen or compromised for an adequate system or application. Same passwords have been used across various applications by most persons and never vary these tokens to make it easy when applying different long passwords for various applications. If an intruder tries to access the system and a piece of the private password is compromised, it may violate privacy for many services [9]. Institutions look forward to keeping their documents safe and improve a service network to dedicate illegal access to them. Verification and identification are used to confirm that the authorized entry can only get into the correct and secure position. Authentication by traditional techniques, specifically personal identification numbers (PINs) and passwords, has been applied over the years. Nowadays, we have been used magnetic cards and PINs for more safety [10]–[12].

Some disadvantages associated with the traditional ways come up because they identify some characters possessed by the owner rather than recognizing the owner itself, who indeed owned them. These tokens can be exposed by stolen or lost, so any intruder can easily be entered or controlled by the system. There is a new approach in authentication systems that exploit biometrics in various fields as governmental services, commercial applications, knowledge-based systems, tokens-based systems, and applications related to forensic evidence that depend on human-being supervision recognize biometric [13], [14].

When an application needs a high level of privacy, system security is not reliable, so biometric features must be secured. It improves the confidentiality and accuracy in recognizing individuals [7], [8]. The biometric system is represented by four main stages of the input device (sensors), image signal processing, dataset storage, and output device [15], as shown in Fig. 1. In the identification process based on conventional biometric techniques, datasets of dedicated features are obtained, and distinctive characteristics are excluded and stored immediately in the cloud during the enrollment stage.

Valuable security properties have been achieved by biometric-based authentication techniques, specifically in telemedicine services, to secure user information of offline password attacks [15]. In conventional biometric identification and authentication techniques, cross-matching (diversity) and cross-application invariance are the major challenges that make an obstacle towards these systems because all services and applications involved in user biometrics can be easily hacked, so the information of the users will be easily tracked [16], [17]. Therefore, biometric encryption techniques achieve high privacy with security and uniqueness for authorized individuals. Encryption keys provide increased protection to the biometric cryptosystems. In these cryptosystems, the genuine biometric features are not kept directly in the cloud, but they are initially processed and converted into deformed templates called noise templates (encrypted images) [18], [19].

Biometric template techniques are divided into helper-data-based schemes and cancelable biometric schemes. Biometric protection algorithms should achieve three main concepts for privacy, which are: (1) unlinkability, where various secured templates must be applied for various services to prevent cross-matching attacks, (2) irreversibility, to provide high protection against the recovery of the original biometric templates, and (3) confidentiality, which means that the authorized biometric feature must be secured against intruder access. In the helper-data-based method, user information is dependent on the authorized template. In addition to that, helper data provides the recovery and makes the secret key is accessible during the authentication operation. The most famous techniques for cancelable biometric templates are fuzzy schemes, especially the fuzzy vault scheme involved in the helper-data methodology.

In [20], the descriptors of the fingerprint are connected to provide high performance during the matching process and the privacy of a fuzzy fingerprint vault. The obstacles and restrictions that face the key binding scheme during the generation of the converted form of templates and the matches are obtained by exchanging the fuzzy commitment scheme with an error correction code (ECC). In cases of unauthorized attacks, renewability and revocability are the most widespread problems facing the biometric cryptosystems that effectively enter the system and identify the stored template features. Besides, biometric cryptosystems suffer from various attacks [21]. Transformations can be identified as repetitive alterations applied to the original biometric template to convert it to the unrecognized image before being stored. These transformations are one-way functions used for the extracted features that enhance the diversity and unlinkability properties. The same biometric template can be suffered from different transformations for various services to forbidden cross-matching between stored biometrics in various cloud datasets [13], [22]–[26].

Another type of cancelable biometric system is called a hybrid approach. It combines two or more template protection techniques [27]–[30]. One of the most advanced alternatives to produce a deformed biometric template is to apply data-dependent cryptography. In [31], user fingerprint templates can generate cryptographic keys of an encryption scheme for fingerprints. Therefore, it is sophisticated or impossible for the intruder to impose the secret keys without prior user features. Random projection and discrete Fourier transform have been applied on the genuine templates as a cancelable method to cover all features of the original biometric templates [32]. This kind of deformation makes the reach to the authorized templates very hard and complex, increasing the security against violating the biometric system. In [33], a biometric security technique was employed to the original feature vectors to generate secured templates utilizing the K-nearest neighbour approach. PIN and random salting are applied to the original templates to produce cancelable ones.

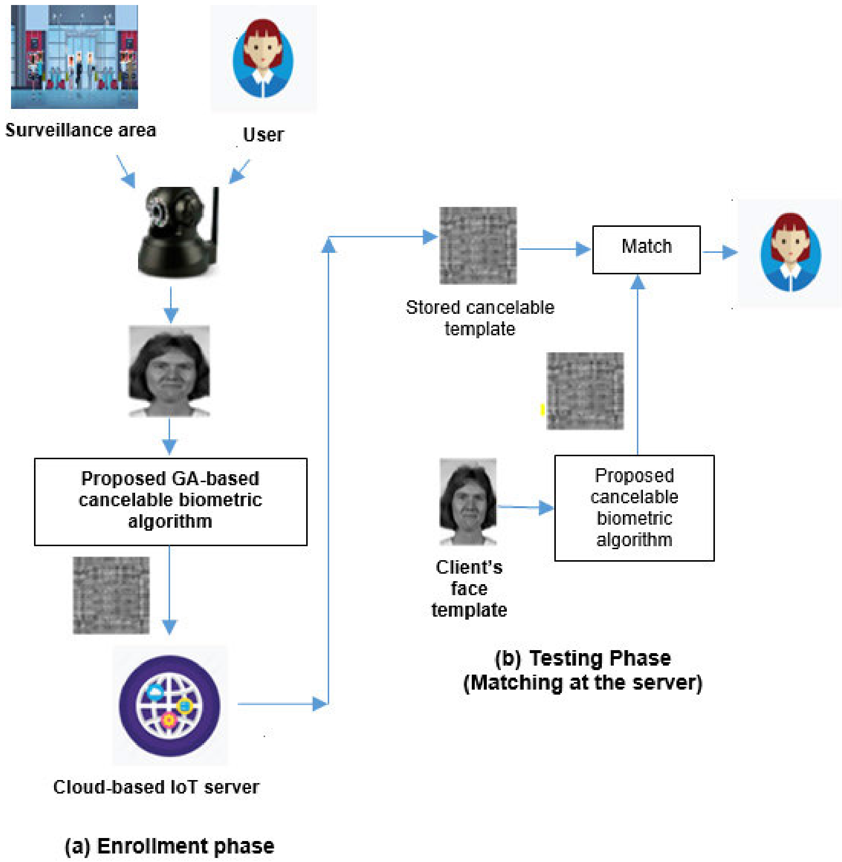


FIGURE 1. Cloud-based biometric authentication IoT system.

In [34], hash coding was employed as a one-way transformation technique, which serves the revocability and linkability to achieve an acceptable degree of the performance of the biometric system.

In remote surveillance systems, authentication techniques involved on the internet of things (IoT) devices is essential to IoT security because it participates in preventing unauthorized person entry to IoT networks, as shown in Fig. 1. Biometric data is an interested authentication manner due to its merits over old-way password-based authentication techniques. Although the protection of biometric data itself is essential, the original biometric data cannot be substituted or altered if compromised. Examples of the standard physical features used in IoT biometric authentication systems are the face, fingerprint, iris, palmprint, and RNA (Ribonucleic acid) biometrics. The choice of a specific trait has developed according to the need of the applied authentication system. For instance, voice traits are convenient in Android devices because the mobile phones' built-in set is sensitive to vocal characteristics.

The essential principle of the IoT biometric recognition system is its ability to recognize the authorized users and the unauthorized users who are not assigned to the system, as shown in Fig. 2. Fingerprint and face modalities-based authentication systems are the most powerful and common traits for user authentication in IoT systems. Fingerprint modality consists of specific details called minutiae. So, minutiae provide unique spatial distribution for each user. Several enterprises have been applied automated fingerprint identification systems for guarantying security and privacy. Besides, many commercial and civil applications exploit fingerprints for authentication. Face authentication systems use the physical relation between the spatial distribution of involved traits such as nose and eyes because the face traits have a high level of specificity at various circumstances [35].

In the proposed work, the crossover and mutation operations of the utilized GA encryption scheme are employed to generate a cancelable biometric template. The proposed cancelable biometric authentication framework has two distinct steps, which are called substitution and mutation. They are performed to scramble the pixel values of the biometric image to decrease the correlation amongst adjacent pixels. Thence, the proposed authentication framework is mandatory in biometric-based IoT systems to provide privacy and confidentiality to the biometric system.

Figure 3 illustrates the steps of the Genetic algorithm. Figure 4 presents the flowchart of the proposed cancelable biometric system used in this paper. First, the biometric

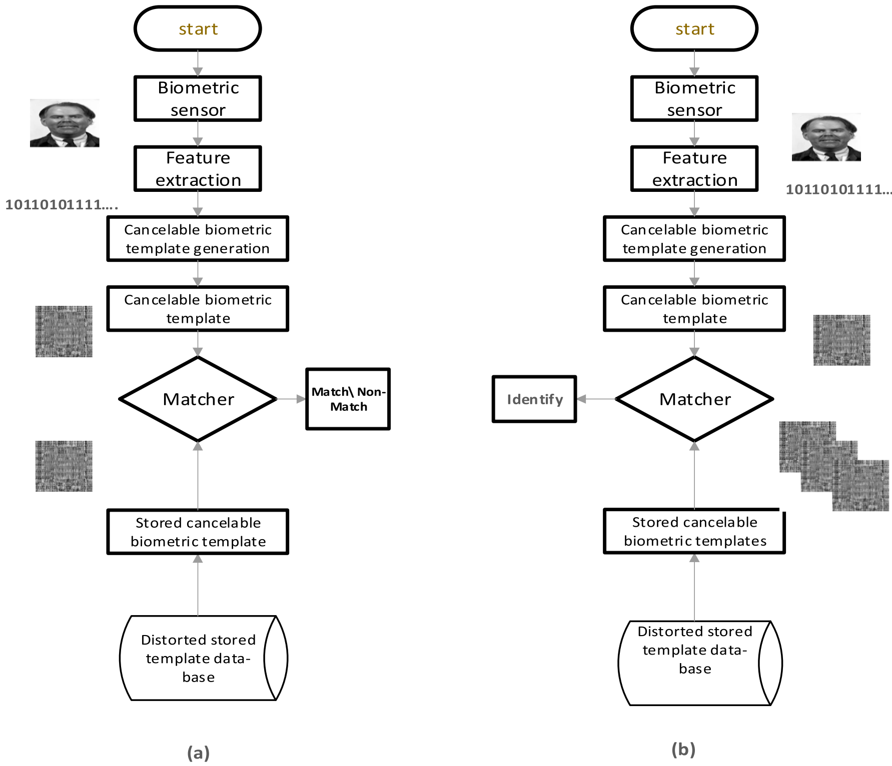


FIGURE 2. **Biometric recognition process: (a) Verification (b) Identification.**

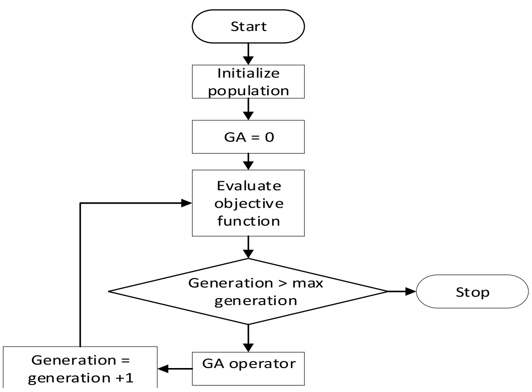


FIGURE 3. **Main steps of the Genetic algorithm.**

image is converted to its RGB components after employing permutation to its rows and columns. After that, each sub-section is considered an image with ($W \times H$), where H and W are the height and width of an image. This image is splitted into a group of N vectors of length L ($L = 32$ bytes is utilized). Subsequently, the crossover and mutation operations are applied to these vectors (rows\columns). If the histogram of the cancelable image becomes uniform, these offsprings are accepted, and another sub-image is selected from another image component with the least distributive histogram. Otherwise, another sub-image from the current image component, with less distributive histogram, is picked up, and the above process (from the second step) is applied until the cancelable biometric image has resulted from the GA-based encryption stage. The algorithm proceeds very fast, and the cancelable biometric image has a higher distribution probability of pixel values.

The remainder of this research is planned as follows. Section II presents some previous works. Section III offers the proposed cancelable biometric authentication framework. Section IV gives the descriptions of the utilized authentication and quality evaluation metrics. Section V introduces the performance comparative analysis and simulation results. The concluding remarks are summarized in Section VI.

II. RELATED WORK

The cancelable biometric techniques are employed for providing deformed copies of the biometrics in the verification operation [36], [37]. In hacking scenarios, it is possible to eliminate or alternate the authorized features if necessary. The cancelable biometric concept is committed to maintaining the high accuracy level of the stored biometrics to increase users' privacy.

Ali and Tahir [38] introduced an authentication system for iris recognition. It is based on the combination of non-invertible transformations and encryption for concealing the iris template. They accomplished a detection rate of 99.9%. In [39], different security tools are presented for face identification. They have used various operations for the extraction of geometric features. Another algorithm is presented

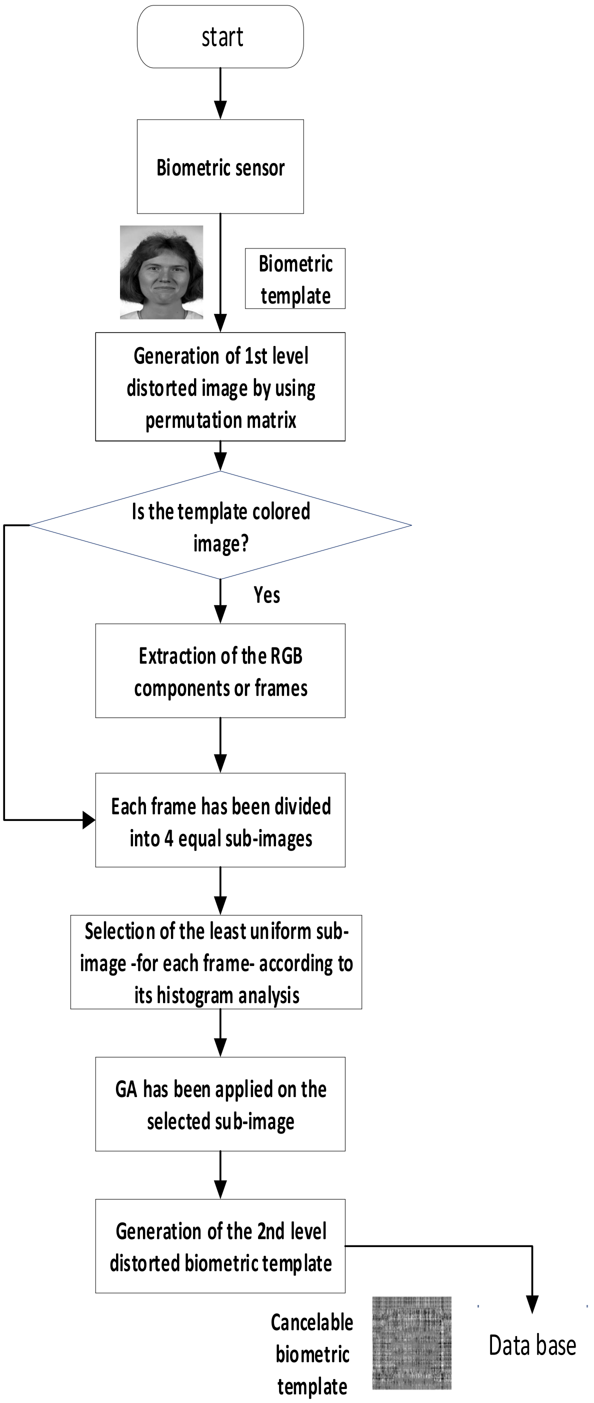


FIGURE 4. Flow chart of the GA-based cancelable biometric authentication proposed framework.

dependent on producing encrypted templates after applying Gabor filters. In this algorithm, two types of chaos maps were introduced that are logistic and modified logistic maps. This algorithm accomplished 99.08% accuracy and 1.175% EER with the chaotic logistic map. In [40], the authors presented a DRPE-based authentication system for face biometrics. The bio-convolving algorithm was employed to accomplish both security and privacy for the users' faces. Furthermore, the same authors in [41] introduced an authentication framework for multi-biometrics. It is based on merging various features of the biometric patterns. The FRFT-based algorithm is used to produce a one-way iris template. The encryption keys, RPM 1 and RPM 2 are used in the presented cancelable biometric scheme. One of these keys, RPM 1, is the first phase mask for the left iris feature vector, and the second one is for the right iris feature template of the person itself. Simulation results showed that the introduced scheme improves privacy. In addition to that, it accomplished an EER of 0.63% and an accuracy of 99.75%.

Cancelable fingerprint recognition techniques apply a feature extraction operation in a repeated way. Ratha *et al.* [36] introduced a cancelable geometric approach for fingerprint identification. It is based on the deduction of feature pixels and the deployment of polar and Cartesian coordinate systems to produce cancelable features of the fingerprints. This algorithm achieves a high accuracy level of privacy and security while preserving cancelability. In [37], the authors introduced a security algorithm for fingerprint detection that depends on several spiral curves using fuzzy concepts. The fuzzy commitment algorithm was adopted for ciphering the detailed characteristics. This algorithm provides an equal error rate (EER) of 1.17%.

The OSH technique was introduced by Korpel and Poon in [42], which exploited a one-pixel sensor to register the hologram of a three-dimensional object through a sequential scanning operation that was applied in a row-by-row order. The optical scanning holography is deduced from the concept of heterodyne optical scanning. So, it is capable of converting a 3D structure into a 2D structure. The electrical signal is introduced by a transformer, as a photodetector, from the incident light beam. This electrical signal interprets the applied data of the scanned biometric template [26]. A 2D digital image of the scanned input object is extracted from the scanned electrical data by storing it in a digital form on a computer. This technique is variant from standard digital hologram acquisition methods proposed by two-dimensional cameras with specified capturing areas and highly restricted spatial resolution; OSH can acquire holograms of wide-field objects with superior resolution. In [42], the authors explained compressive optical scanning holography to solve this problem. They succeeded in achieving a correlation score of 0.93 as maximum.

It is possible to conclude that deformation of the original data can be achieved by using one of two methods: mathematical transformations-based cancelable algorithms or encryption-based cancelable algorithms. The GA encryption algorithm can be used to attain biometric image cancelability. In [43], GA is also adopted as an encryption algorithm in the frequency domain. In [44], the authors introduced an image cryptosystem to generate ransom patterns for biometrics. In the crossover stage, frequency components of the imaginary parts were dislocated, while their real parts were subtracted from the input key in the mutation stage. In [45], [46], because the randomness of the ciphered image depends greatly on the ciphering key, GA is also employed to adjust the secret key. A secret key with n bits can be readjusted by $n!$ states. The GA algorithm selects the ideal secret key with optimal length to achieve higher encryption [47], [48].

Another type of cancelable biometric technique is the conventional method that starts with a feature extraction process and ends with a cancelable feature vector. For instance, in [49], the authors presented a cancelable biometric scheme based on ECG signals using two techniques. Firstly, an improved Bio-Hash algorithm has been applied. Then, a matrix operation has been exploited to transform the original feature vector to a cancelable template by one-directional transformation. In [50], the authors employed a two-dimensional Gabor filter to accomplish the feature extraction operation from a palmprint, and then they applied a two-dimensional palm Hash code to hide these features and generate the cancelable palmprint vector. In [51], an algorithm is employed for multi-biometric traits to generate cancelable biometrics to achieve more privacy and confidentiality based on various feature fusion levels.

Therefore, several cancellable biometric algorithms based on symmetric encryption or transformations are introduced in the literature, as summarized in Table 1. They did not provide cancelable biometric templates with a high level of security. They did not achieve better confidentiality and biometric authentication for specific sensitive systems such as military and telemedicine applications. The main disadvantages of the conventional algorithms are summarized as follows:

1. The security analysis of the traditional algorithms does not reveal outstanding outcomes in terms of the AROC and EER metrics that are considered the most important evaluation metrics for biometric authentication systems.
2. Only two or three biometric datasets are utilized for testing the authentication performance of the traditional algorithms.
3. Many security and quality evaluation metrics that can be employed to evaluate the biometric system quality and security levels have not been used and investigated in most traditional algorithms.
4. The traditional algorithms are not tested in the presence of noise.
5. The computational processing time of the traditional algorithms is not explored and evaluated as a vital evaluation metric in online authentication applications.

Considering these shortcomings of the traditional algorithms, we propose a secure and efficient cancelable biometric framework based on the evolutionary genetic encryption operation to generate encrypted biometric templates with a high level of specificity and sensitivity. The Genetic Algorithm is an iterative procedure shown in Fig. 3. The concept meaning of GA is natural selection, where the fittest images are chosen for reproduction to produce offspring of the upcoming generation. The main contributions of the proposed cancelable biometric authentication framework based on the GA encryption scheme can be summarized as follows:

1. Because GA operation depends on three main stages, which are crossover, mutation, and selection of the best initial populated cipher image, thus, the proposed GA-based cancelable biometric authentication framework can allow multi-encrypted cancelable images, which adds strength and more randomization to the cancelable template as getting its histogram more uniform.
2. In each round of the employed GA scheme, 20% of the entire population is altered with new cancelable templates.
3. The performance analysis of the proposed framework is studied in the presence of noise disturbance on the biometric authentication system.
4. Processing time has been considered for evaluating the performance of the proposed framework compared to the traditional OSH algorithm.
5. Various security and quality assessment metrics are examined on five different biometric datasets.

III. PROPOSED CANCELABLE BIOMETRIC AUTHENTICATION FRAMEWORK

The flowchart of the proposed cancelable biometric authentication framework is introduced in Fig. 4. The main steps of the proposed framework are demonstrated in Algorithm 1 and can be summarized as follows:

1. Permute the rows and columns of the original template in a dedicated sequence with the help of a permutation matrix.
2. Extract RGB components from the input image. If the biometric template is a grayscale image, we can skip this step.
3. Divide each extracted component image into four same-sized parts (sub-images).
4. Select one sub-image according to its histogram uniformity, where the least uniform histogram will be the best sub-image choice (repeated for each RGB component).
5. Consider the sub-image I $(W \times H)$, where W and H are the width and height of image I (here $W = 128$ and $H = 128$). Merge the image I into a group of N vectors of length L ($L = 32$ bytes).
6. Obtain $R1$ and $R2$ from the equations:

$$R_1 = \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} (-1)^{(i+j)} \times \frac{I\,(i,j)}{128 \times L} \tag{1}$$

$$R_2 = \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} (-1)^{(i+j+1)} \times \frac{I\,(i,j)}{128 \times L} \tag{2}$$

   where the value of $(R_1 + R_2)/2$ is the initial value of the employed random number generator scheme (*e.g.*, we applied a linear random number generator proposed in [47] after changing control values according to sub-image dimension).
7. Suppose $x = R_1$ and $y = R_2$. For $I = 0, \ldots\ldots, N$-1, initiate the next information for each vector $\mathbf{V}i$ from the group of N vectors:
   - ➢ Crossover index $= x$.
   - ➢ Crossover iteration $= \mathbf{V}_i(x)$.
   - ➢ Mutation index $= y$.

TABLE 1. Comparative study between the related studies and the proposed work.

Work	Methodology and goal	Biometric modality	Approach	Utilized evaluation metrics	Advantages	Disadvantages
[20]	Fingerprint descriptors are connected before applying fuzzy vault scheme for generating cancelable image	Fingerprint templates	Fuzzy vault-based encryption scheme	FRR=3.251×10^{-3} FAR=0.7814 EER=0.0214	High performance during the matching process	Vulnerable to blended substitution attacks, and the attacks on error-correcting codes.
[32]	Uses fingerprint templates to generate cryptographic keys of an encryption scheme	Fingerprint templates	Data-dependent cryptography	FRR=1.751×10-4 FAR=0.0314 EER=4.589×10^{-9}	High privacy for the storage of user information	Complicated and vulnerable to masquerade attacks
[33]	Random projection and discrete Fourier transform	Fingerprint templates	Hybrid transformation	FRR=2.369×10^{-3} FAR=0.0864 EER=2.67×10^{-11}	Robustness of the authorized templates	More complex to analyze the system
[34]	PIN and random salting are applied to generate the cancelable biometrics	Fingerprint templates	K-nearest neighbour approach	FRR=1.925×10^{-5} FAR=0.00678 EER=1.827×10^{-3}	Unbreakable by intruders	Vulnerable to record multiplicity attacks
[35]	Hash coding was employed as a one-way transformation technique	Fingerprint templates	Hash coding	FRR=0.2731 FAR=0.0308 EER=0.00186	Serves the revocability and linkability	Less performance due to suffering from accuracy loss
[38]	The fuzzy commitment algorithm was adopted for ciphering the detailed features	Fingerprint templates	Several spiral curves using fuzzy concepts	FRR=0.492 FAR=0.0627 EER=0.0117	Achieves blind authentication	The system suffers from the instability that leads to high FRR
[39]	Non-invertible transformations to mask the genuine iris template	Iris templates (CASIA v.3)	Encryption and non-invertible transformations	FRR=1.114 FAR=0.0046 EER=0.00017	Produced recognition rate up to 99.9%	Low variety of applied biometrics
[40]	Producing encrypted templates after applying Gabor filters for feature extraction from iris images with convolution kernels achieved by chaotic maps	Iris templates (CASIA v.3)	Two types of chaotic maps: logistic maps and modified logistic maps	FRR=1.185 FAR=0.0086 EER=0.00117	Accuracy leads to 99.08%	Vulnerable to brute force attack and replay attacks
[42]	Introducing a cancelable iris recognition algorithm based on merging various patterns of biometric features	Iris templates (CASIA v.3 & v.4)	DRPE and FrFT	FRR=0.274×10^{-3} FAR=0.00029 EER=0.0063	Accuracy leads to 99.75%	Vulnerable to reversible brute force attack, expensive, and complex implemented system
[50]	The protected feature vector is created from the inner product between the ECG feature matrix while the matrix operation is applied to the ECG feature matrix	ECG signals (MIT-BIH arrhythmia, PTB, and CYBHi datasets)	An improved Bio-Hashing and matrix operation technique	FRR=0.0 FAR=0.38 EER=0.26	Get solution for accuracy loss which is the main obstacle in Bio-Hashing	The genuine information can be recognized if an intruder has previous knowledge about the key and the biometric data
[51]	2D Gabor filter was proposed as a cancelable palmprint coding scheme for secure palmprint verification	Palmprint templates (poly U version 2 dataset)	Two-dimensional (2D) palm Hash code	Conventional statistical analysis	Suppress vertical correlation	Still vulnerable to statistical analysis attack for various biometric modalities
[52]	A multi-modal biometric system integrates information from more than one biometric modality	ECG (PTB database and CYBHi database) Fingerprint templates (livedet 2015 and FVC 2004 databases)	Conventional neural-network and Q-Gaussian multi-support vector machine based on different level fusion	FRR=0.0 FAR=0.004 EER=0.0014	Overcome authentication accuracy loss and spoof attacks	Need to speed up the authentication task
Proposed work	Develop a cancelable biometric framework based on the GA encryption method	Face and fingerprint templates (FERET, LFW, ORL, and FVC 2004 datasets)	Initial permutation followed by encryption operation based on GA to generate cancelable biometric traits	FRR=2.269×10^{-4} FAR=4.8×10^{-4} EER=2.02×10^{-4}	1) Satisfies more randomization with appreciated histogram results and lower processing time. 2) Better results have been achieved than related works. 3) AROC= 0.9998	Vulnerable to masquerade attacks

➢ Mutation iteration = $\mathbf{V}_i(y)$.

$$x = x + 1$$
$$y = y + 1$$
$$\text{if } (x \text{ or } y) = L, \text{ then set } x = 0 \text{ and } y = 0.$$

8. For $I = 0, \ldots, N$-1, apply step (9) and step (10) for each vector $\mathbf{V}_i$ from the group of N vectors of the dedicated sub-images with histogram more uniform than others. Remind that both values in $\mathbf{V}_i(x)$ (crossover index) and $\mathbf{V}_i(y)$ (mutation index) are not involved in the crossover and mutation operations.
9. Employ crossover operation.
 - Initiate crossover index of vector $\mathbf{V}_i$ as a new initial value of the adopted random number generation scheme.
 - For j from 0 to crossover iteration of vector $\mathbf{V}_i$, produce two random values N_1 and N_2 with values between (0, ..., L-1), then apply to swap $\mathbf{V}_i(N_1) \leftrightarrow \mathbf{V}_i(N_2)$.
10. Employ mutation operation.
 - Initiate mutation index of vector $\mathbf{V}_i$ as a new initial value of the adopted random number generation scheme.
 - For j from 0 to mutation iteration of vector $\mathbf{V}_i$, initialize one random number N_1 with values between (0, ..., L-1), then apply $\mathbf{V}_i(N_1) = 127$-$\mathbf{V}_i(N_1)$.
11. Produce the cancelable biometric template from the encrypted sub-images of each colored component produced from N encrypted vectors. Then, conceal the values R_1 and R_2 in the encrypted sub-images.

Algorithm 1 Steps of the Proposed Model

Input: Biometric image I ($W \times H$), where $W = 128$ and $H = 128$ with No. of iterations = 5.
Output: Cancelable biometric image.
01: Initialize $W = 0$ to 128.
Initialize $H = 0$ to 128, L (max. length of each block) = 32.
02: Calculate $N = 4$ (vectors).
03: Merge I into N vectors with a length L.
04: Generate the initial value of the random number generator (using Eqs. (1) and (2)).
05: Apply a random number generator scheme.
06: Apply GA steps:
(a) Crossover: for best initial populated image (with less uniform histogram).
(b) Mutation: initialize mutation index mui = 0, apply muiter = $(5 \times x + 73 \times y)$, where $x = 0$, $y = 0$, $x = x + 1$, and $y = y + 1$.
07: After average iterations = 5, produce acceptable cancelable images with uniform histogram.

IV. AUTHENTICATION EVALUATION METRICS

The essential parameter in testing the encrypted or cancellable biometrics is the visual inspection, where good encryption and high cancelability result from highly hidden features for the proposed cancelable biometric cryptosystem.

FIGURE 5. The tested twenty biometric images of the ORL database.

FIGURE 6. The tested twenty biometric images of the FERET database.

FIGURE 7. The tested twenty biometric images of the LFW database.

Quality evaluation does not depend only on visual inspection. So, various metrics are involved in measuring the improvement of the cancelable biometric framework. Correlation factors measure the similarity between a stored biometric pattern and a biometric input pattern. The higher the value of factors, the higher will be the similarity amongst templates. If the correlation coefficient for a tested user is above a dedicated threshold, access to the system is allowed. Theoretically, the score of correlation for an authorized person must be higher than the correlation score for an intruder trying to access the system. A single threshold would be sufficient to separate the two groups of scores divided into authorized persons and intruder persons.

The achievement of the proposed cancelable biometric authentication framework can be evaluated by the receiver operating characteristic (ROC) curve. The ROC curve illustrates the difference between the true positive factor (TPF) and the false-positive factor (FPF) [52], [53]. The concept of the ROC curve is based on a decision variable. The tested information consists of genuine and fake templates in any

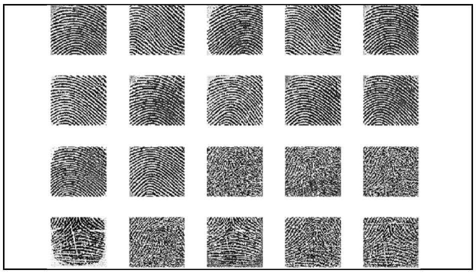


FIGURE 8. The tested twenty biometric images of the first FVC2002 database.

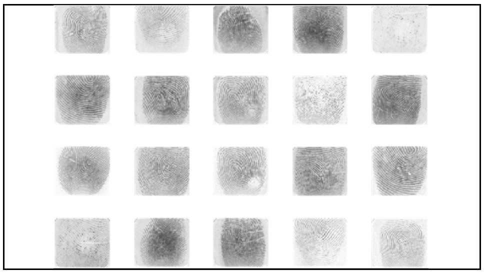


FIGURE 9. The tested twenty biometric images of the second FVC2002 database.

biometric authentication system so that each pattern value could be distributed around a specific mean value. Therefore, the mean value of the genuine template is higher than the mean value of the fake templates. For that purpose, we need to use the estimated distribution of the probability density in our proposed work. Furthermore, the correlation coefficients obtained from the authentication phase are tested by the PFD (probability of the false distribution) and the PTD (probability of true distribution).

Various variations are affected in pixel levels comparing with their intensities before biometric template encryption using GA. This demonstrates that the more the difference in pixel level and permutations are applied, the more influential the biometric encryption scheme will perform, and consequently, a higher encryption performance will be achieved.

The encryption performance is examined by measuring correlation coefficients, histogram deviation, and histogram uniformity between encrypted and original biometrics. The authentication metrics applied to evaluate the quality of the proposed cancelable biometric authentication framework will be discussed in detail as follows:

A. HISTOGRAM ANALYSIS

The histogram illustrates the distribution degree for each pixel intensity in a biometric image. The histogram must possess both characteristics for the encrypted biometric template in case of cancelable biometric systems, which is dependent on encryption schemes [54]:

1. The histogram of the encrypted biometric image is different from the histogram of the original biometric image.

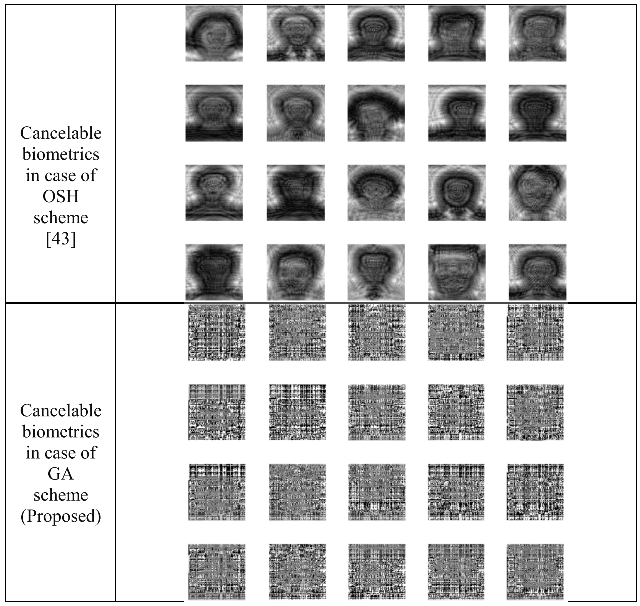


FIGURE 10. The cancelable biometrics for the GA cryptosystem compared to the OSH cryptosystem for the ORL database.

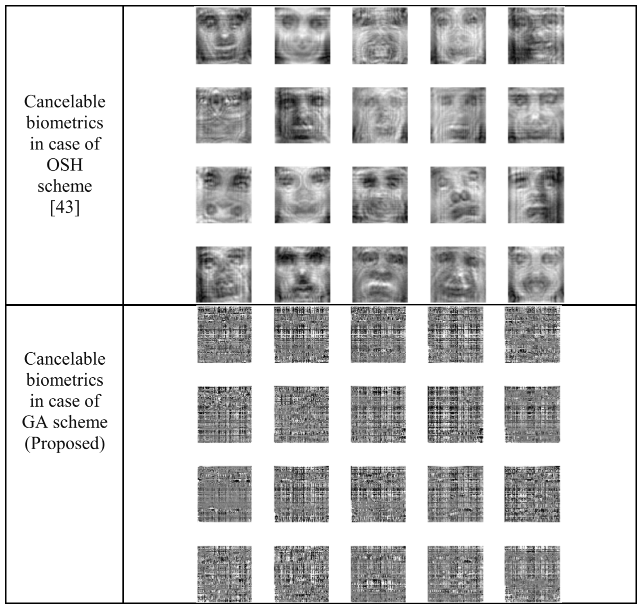


FIGURE 11. The cancelable biometrics for the GA cryptosystem compared to the OSH cryptosystem for the FERET database.

2. It must have an equal distribution, which means uniform distribution of all grey-intensities or pixel values.

B. CORRELATION SCORE

The correlation is an examination performed on the biometric template and its deformed copy. Two situations in the correlation examination are explained below:

1. When the correlation coefficient (C_r) is equal or close to ± 1, it investigates the maximum score, which happens only if two biometric images are similar or highly

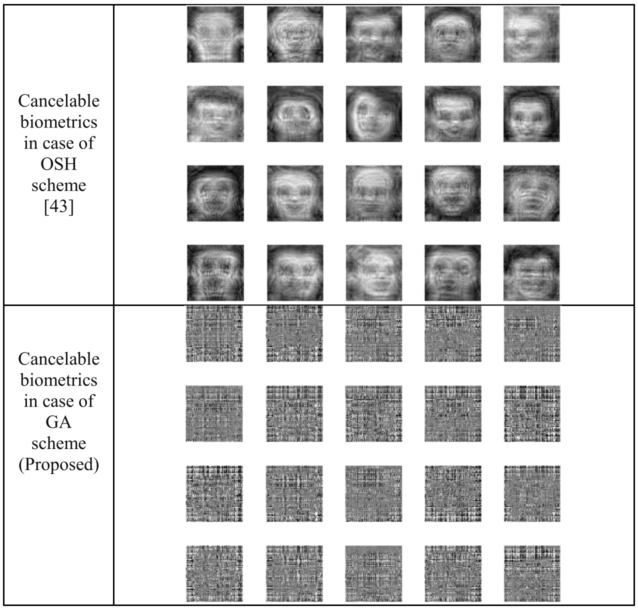


FIGURE 12. The cancelable biometrics for the GA cryptosystem compared to the OSH cryptosystem for the LFW database.

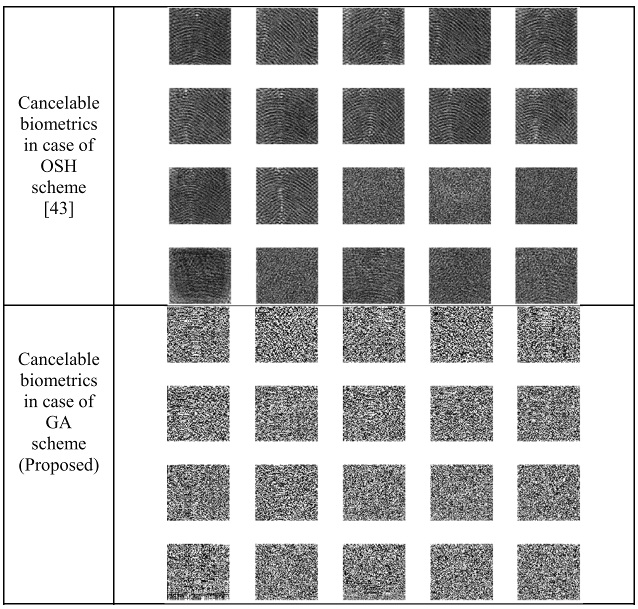


FIGURE 13. The cancellable biometrics for the GA cryptosystem compared to the OSH cryptosystem for the first FVC2002 database.

dependent. That case will be achieved at the verification phase for authorized access scenarios according to the encrypted biometric image stored in the cloud and the encrypted test image for the same authorized user.

2. The C_r value is close or equal to 0, which proposes a significant change between the authorized biometric image and its encrypted version at the enrollment phase, where the ciphered biometric template is extremely independent of the primary one, on the other hand, that case also appears at the verification phase in unauthorized access scenarios.

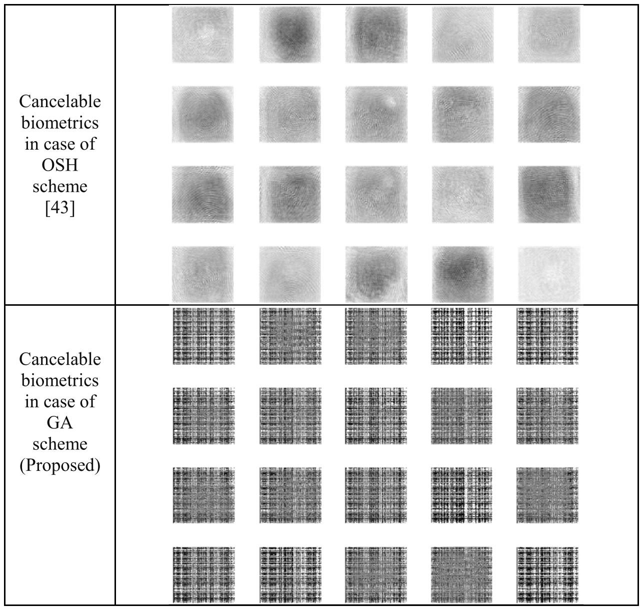


FIGURE 14. The cancelable biometrics for the GA cryptosystem compared to the OSH cryptosystem for the second FVC2002 database.

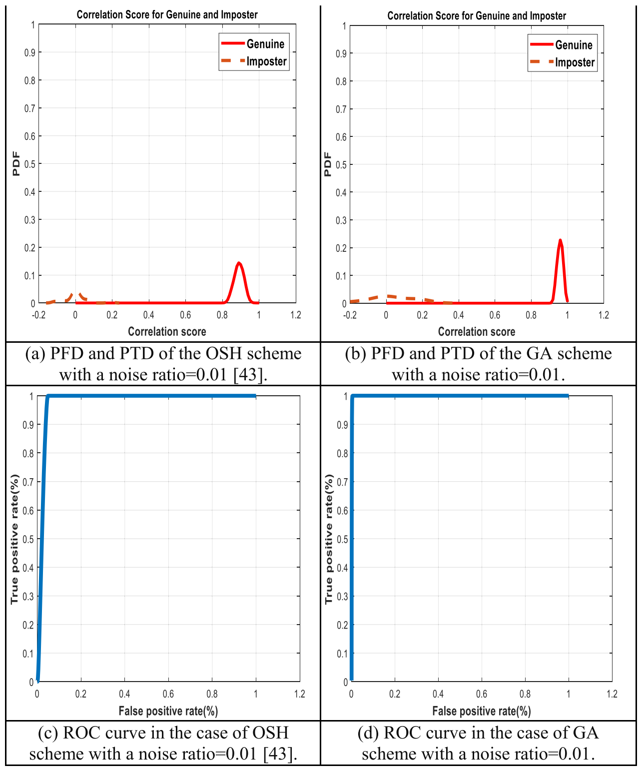
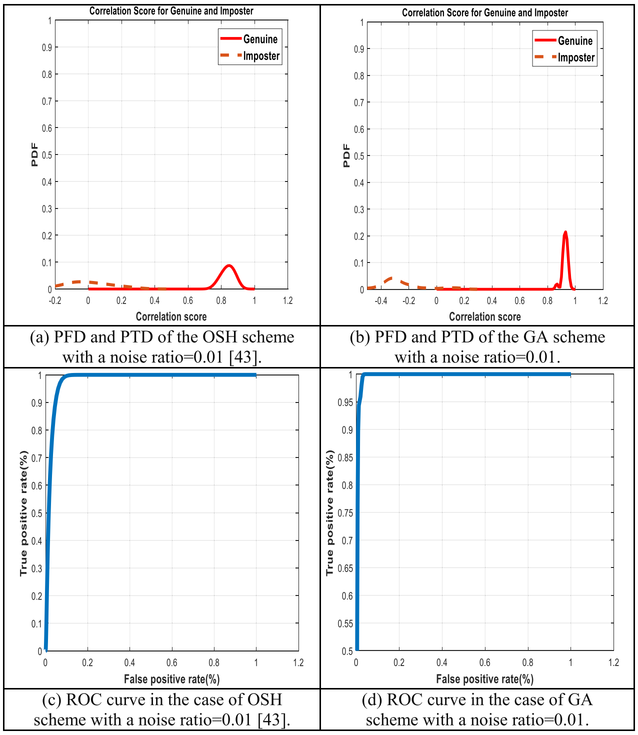


FIGURE 15. The authentication outcomes of the GA and OSH cryptosystems using the ORL database.

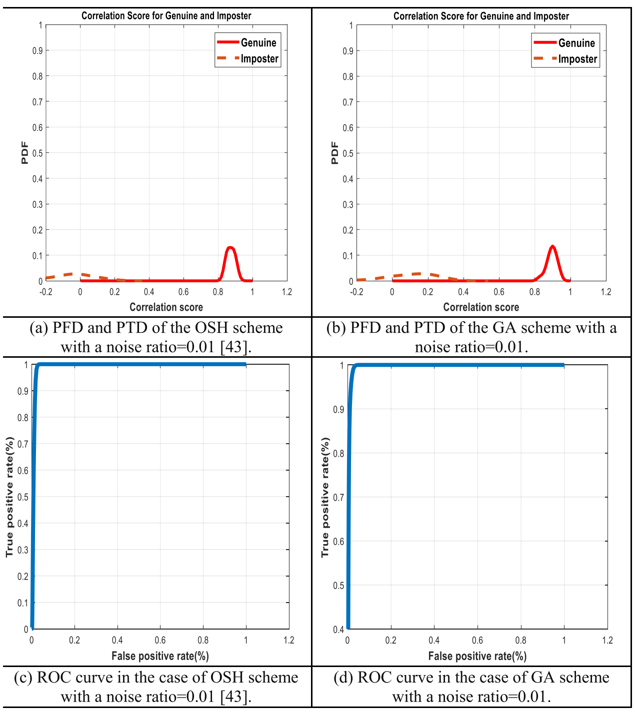
C. THE PROBABILITY OF TRUE DISTRIBUTION (PTD) AND FALSE DISTRIBUTION (PFD)

The PTD is the likelihood correlation distribution among the authorized patterns (true biometrics) with the ciphered patterns stored in the database. The PFD is the likelihood correlation distribution among the unauthorized patterns (fake biometrics) with the cipher biometrics. The point resulting from the crossing between the PFD and PTD distributions



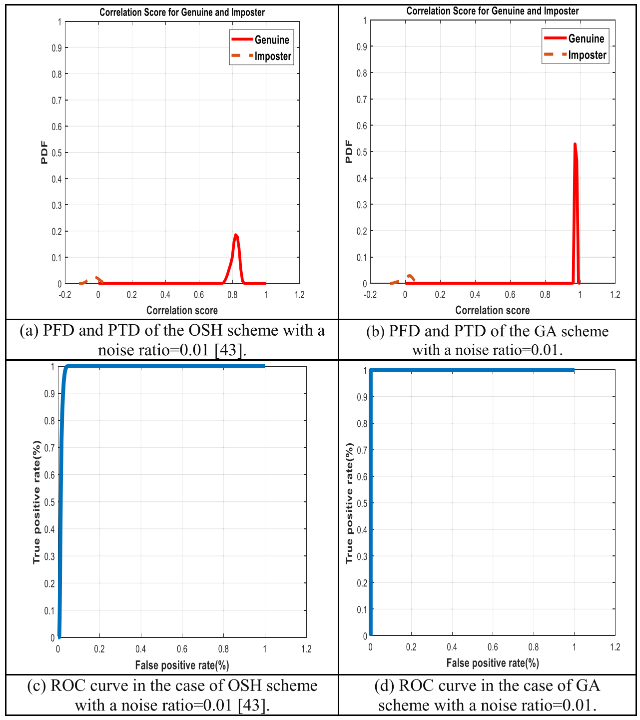
(a) PFD and PTD of the OSH scheme with a noise ratio=0.01 [43].
(b) PFD and PTD of the GA scheme with a noise ratio=0.01.
(c) ROC curve in the case of OSH scheme with a noise ratio=0.01 [43].
(d) ROC curve in the case of GA scheme with a noise ratio=0.01.

FIGURE 16. The authentication outcomes of the GA and OSH cryptosystems using the FERET database.



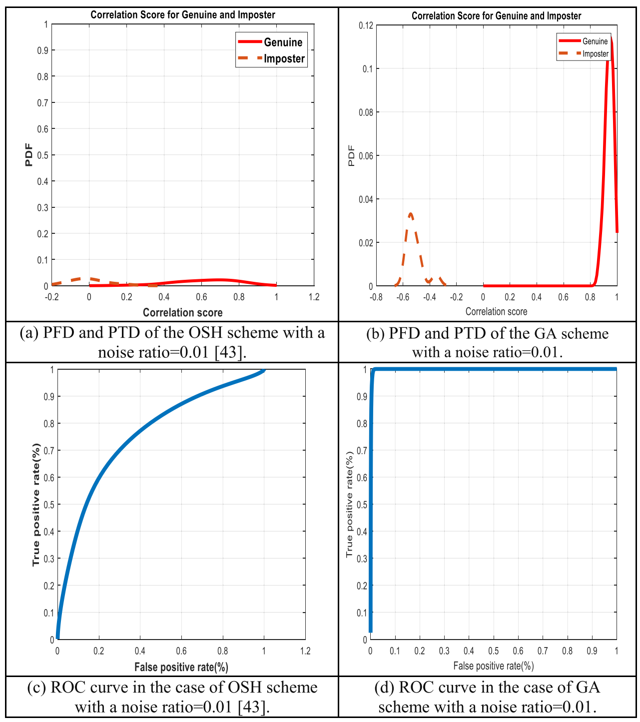
(a) PFD and PTD of the OSH scheme with a noise ratio=0.01 [43].
(b) PFD and PTD of the GA scheme with a noise ratio=0.01.
(c) ROC curve in the case of OSH scheme with a noise ratio=0.01 [43].
(d) ROC curve in the case of GA scheme with a noise ratio=0.01.

FIGURE 17. The authentication outcomes of the GA and OSH cryptosystems using the LFW database.



(a) PFD and PTD of the OSH scheme with a noise ratio=0.01 [43].
(b) PFD and PTD of the GA scheme with a noise ratio=0.01.
(c) ROC curve in the case of OSH scheme with a noise ratio=0.01 [43].
(d) ROC curve in the case of GA scheme with a noise ratio=0.01.

FIGURE 18. The authentication outcomes of the GA and OSH cryptosystems using the first FVC2002 database.



(a) PFD and PTD of the OSH scheme with a noise ratio=0.01 [43].
(b) PFD and PTD of the GA scheme with a noise ratio=0.01.
(c) ROC curve in the case of OSH scheme with a noise ratio=0.01 [43].
(d) ROC curve in the case of GA scheme with a noise ratio=0.01.

FIGURE 19. The authentication outcomes of the GA and OSH cryptosystems using the second FVC2002 dataset.

is the threshold intersection point which can be differed based on the employed ciphering scenario. Entry or controlling the system is forbidden if the coefficient for the test trait is lower than a specific threshold [55].

D. THE RECEIVER OPERATING CHARACTERISTIC (ROC) CURVE ANALYSIS

In a ROC curve, the sensitivity (true positive rate) is represented as a mathematical function of the specificity (false

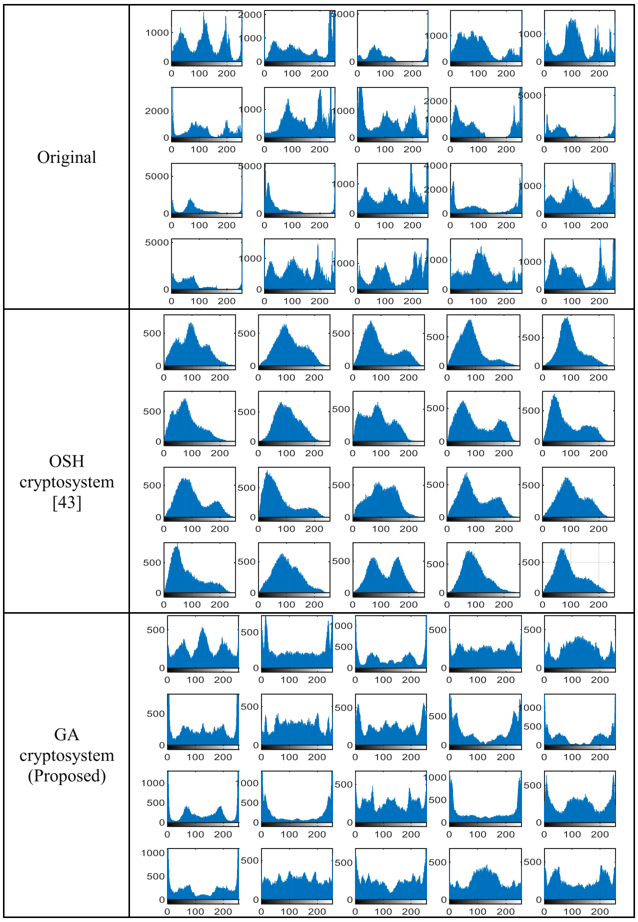


FIGURE 20. Histogram results of the GA and OSH cryptosystems using the ORL database.

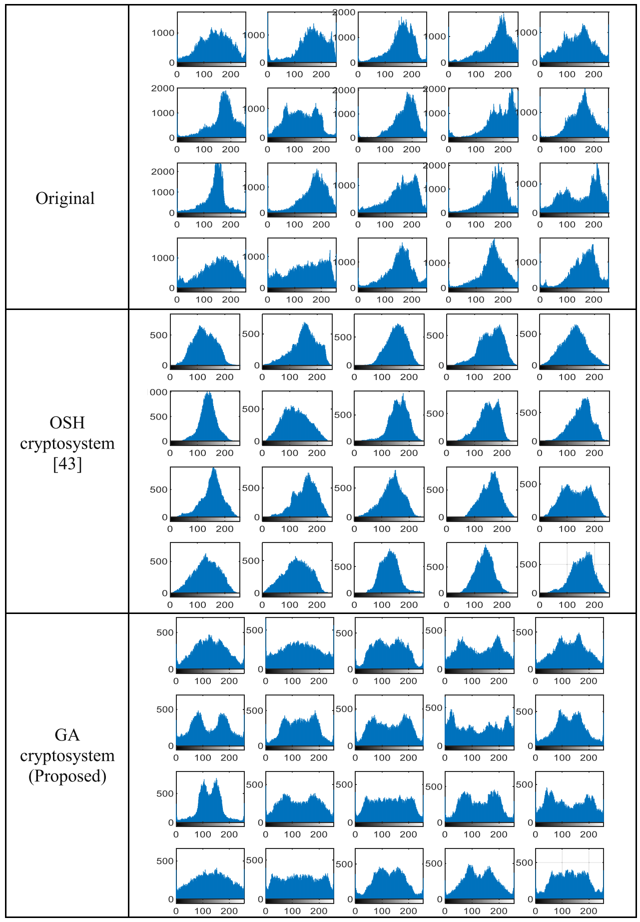


FIGURE 21. Histogram results of the GA and OSH cryptosystems using the FERET database.

positive rate) for various intersection positions. So, every point on the ROC signifies a specificity/sensitivity pair corresponding to a particular determination threshold [55].

V. SIMULATION RESULTS AND DISCUSSIONS

To validate our proposed method, we test the proposed framework on five different biometric databases that compose two types of biometric modalities of face and fingerprint templates. The tested face biometrics used in the simulations are obtained from the Research Laboratory for Olivetti and Oracle (ORL) database [56], the NIST Face Recognition Technology (FERET) database [57], and the Mass Labelled Faces in the Wild (LFW) database of the University of Massachusetts' Computer Vision laboratory [58]. The two versions of the fingerprint FVC2002 databases [59], [60] are also utilized in the simulation studies. For further details, descriptions and explanations of the examined biometric datasets can be found in [56]–[60]. More security and authentication evaluation measurements are analyzed and discussed, such as FRR, FAR, PTD, PFD, AROC, histogram analysis, visual analysis, noise analysis, and processing time analysis.

Thus, we examine three various sample datasets of faces [56]–[58] and two distinct fingerprint datasets [59], [60]; to assess the proposed cancelable biometric authentication framework. In simulation results, the tested twenty various biometric faces and fingerprints of different users are shown in Figs. 5 to 9. Therefore, five simulation cases for the tested sample datasets are analyzed. The simulation results are accomplished with MATLAB environment (2019b), set-upped on Windows 8 with Intel®CPU @ 1.80GHZ /2.40GHZ Core i5-4300 and 4GB RAM. We compare the accomplishment of the suggested GA-based cancelable biometric framework with the OSH-based cancelable biometric framework [42].

Figures 10 to 14 illustrate the ciphering results of the suggested GA cryptosystem contrasted to the OSH cryptosystem [42] for all tested biometric samples. We noticed that the suggested GA encryption scheme results are recommended and appreciated for the efficient cancellable biometric system compared to the traditional technique [42]. From the visual encryption analysis point of view, the proposed cancelable biometric framework achieves a complete distortion and encryption for the original biometrics to be stored safely in the secured cloud server. In the authentication stage, for all tested simulation tests, there are two biometrics images have been tested. One belongs to a genuine user, and the other

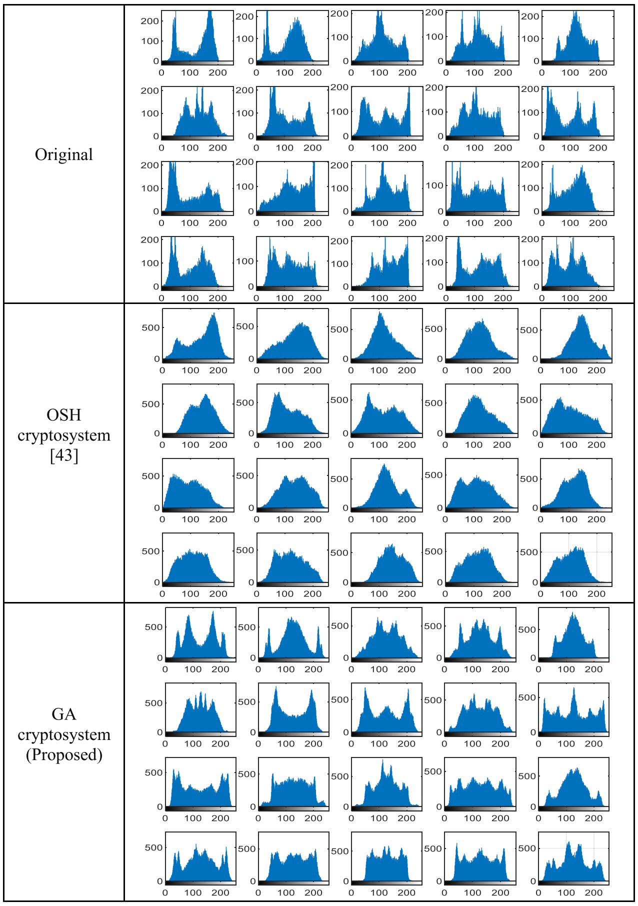


FIGURE 22. Histogram results of the GA and OSH cryptosystems using the LFW database.

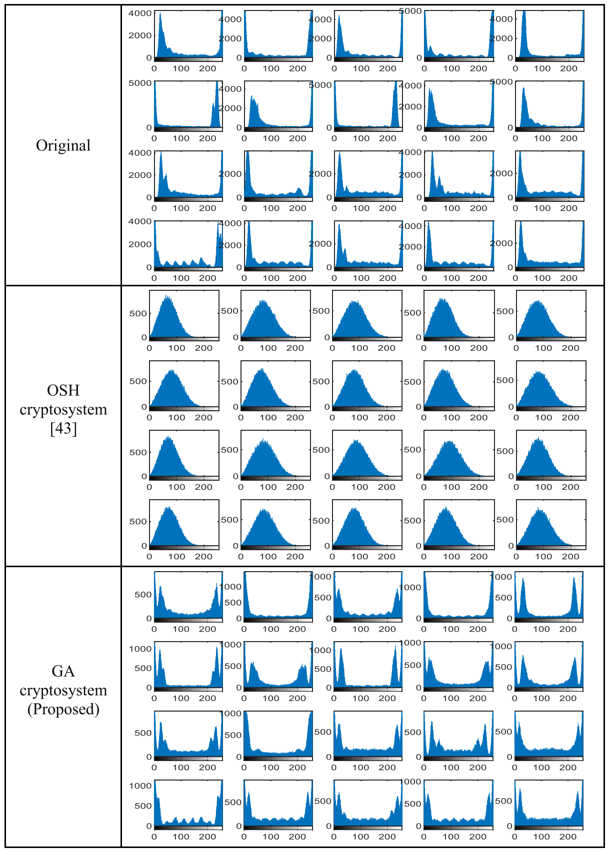


FIGURE 23. Histogram results of the GA and OSH cryptosystems using the first FVC2002 database.

belongs to the imposter one. In the two cases, it is imposed that the fake user has previous knowledge with the correct key for any genuine user to examine the level of privacy and the degree of accuracy of the system. The correlation coefficients are calculated between the two tested encrypted images and the twenty encrypted biometric templates. Our study considers that the actual environment has a degree of noise that may affect the tested or stored biometric templates. So, all experimental results are carried out in the presence of noise.

Figures 15 to 19 illustrate the ROC, PFD, and PTD curves of the verification phase for the suggested GA encryption scheme compared to the state-of-the-art OSH technique for all examined biometric samples. The crossing point of the PFD and PTD determines the threshold crossing rate, which is exploited to investigate, according to it, whether this person is a genuine user or not.

Figures 20 to 24 illustrate the histogram results for the GA and OSH cryptosystems for the whole examined biometric samples. It is noticed that the suggested GA cryptosystem affords roughly uniform and flat histogram outcomes compared to the OSH cryptosystem which prove its superior finidings.

TABLE 2. Correlation values for the twenty biometrics traits of the ORL database.

The twenty biometrics images of the ORL database	Correlation with the false face		Correlation with the true face	
	OSH [43]	GA scheme (Proposed)	OSH [43]	GA scheme (Proposed)
Face1	-0.1128	0.0123	0.8884	0.9415
Face2	0.0659	-0.0702	0.8841	0.9638
Face3	0.0081	0.0050	0.9168	0.9676
Face4	0.0319	0.1919	0.8718	0.9518
Face5	0.0121	0.0571	0.8551	0.9353
Face6	0.0618	0.1836	0.8780	0.9606
Face7	-0.0050	-0.1537	0.8502	0.9415
Face8	-0.0063	0.1411	0.8939	0.9567
Face9	-0.0828	-0.0181	0.9305	0.9735
Face10	-0.0042	0.0378	0.9177	0.9763
Face11	0.0011	-0.0347	0.9057	0.9676
Face12	-0.0009	0.1882	0.9131	0.9807
Face13	-0.0274	-0.0689	0.8810	0.9520
Face14	0.0121	-0.0244	0.9093	0.9758
Face15	-0.0044	-0.0144	0.8858	0.9538
Face16	0.0399	0.1593	0.9100	0.9705
Face17	0.0242	0.0474	0.8769	0.9459
Face18	-0.0591	-0.2013	0.8935	0.9603
Face19	0.1939	0.2010	0.8504	0.9352
Face20	-0.0197	0.0383	0.8878	0.9566
Average	0.0043	0.0341	0.8901	0.9584

Tables 2 to 6 illustrate the correlation comparison values of the twenty biometric traits for all experimental biometric

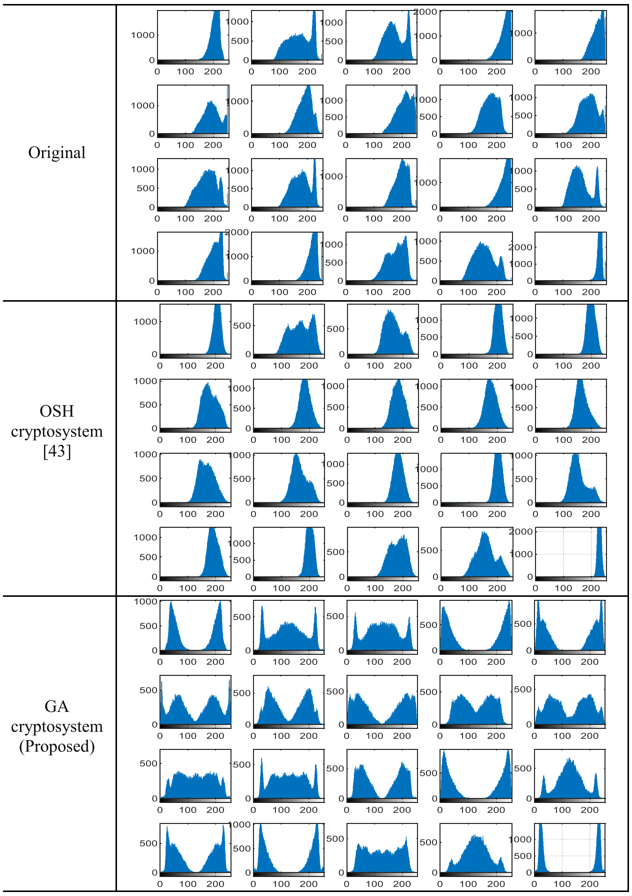


FIGURE 24. Histogram results of the GA and OSH cryptosystems using the second FVC2002 dataset.

databases for the suggested GA encryption scheme contrasted to the state-of-the-art OSH technique. From all correlation results of the five examined simulation cases, the results ensure the importance of exploiting the proposed GA encryption scheme for achieving better performance for cancelable biometric systems, as it presents the higher AROC values and the lower EER, FRR, and FAR values compared to the utilization of the traditional OSH technique [42]. Tables 7 to 11 illustrate the existing effect of different Gaussian noise variances on the tested biometrics for the proposed cancelable technique and the OSH technique with presenting the average EER and AROC values. The obtained average EER and AROC results prove the minimal noise sensitivity for the proposed framework with acceptable EER and AROC compared to the traditional OSH algorithm.

The computational processing time is estimated for the proposed framework compared to the traditional OSH algorithm for the examined biometric datasets, as revealed in Table 12. It is remarked that the proposed framework achieved lower processing time compared to the conventional algorithm. Therefore, the proposed cancelable biometric authentication framework is highly recommended in online and real-time biometric authentication applications.

TABLE 3. Correlation values for the twenty biometrics traits of the FERET database.

The twenty biometrics images of the FERET database	Correlation with the false face		Correlation with the true face	
	OSH [43]	GA scheme (Proposed)	OSH [43]	GA scheme (Proposed)
Face1	-0.1209	-0.1963	0.8418	0.9174
Face2	-0.1216	-0.3495	0.8801	0.9383
Face3	-0.0417	-0.3226	0.8088	0.9133
Face4	0.0540	-0.3548	0.8514	0.9428
Face5	0.2603	0.0672	0.8681	0.9213
Face6	-0.0532	-0.3764	0.7661	0.9321
Face7	0.2030	0.1523	0.8798	0.9143
Face8	-0.0442	-0.4360	0.8088	0.9318
Face9	-0.3149	-0.5503	0.8223	0.9567
Face10	0.0279	-0.2639	0.8388	0.9090
Face11	-0.1057	-0.2020	0.8370	0.8663
Face12	0.0526	-0.3194	0.8514	0.9355
Face13	-0.0420	-0.3058	0.8453	0.9350
Face14	0.1016	-0.3348	0.8076	0.9240
Face15	-0.2582	-0.3185	0.8906	0.9440
Face16	0.1781	-0.0641	0.8738	0.9333
Face17	-0.0949	-0.1716	0.8827	0.9432
Face18	-0.0968	-0.2739	0.7936	0.9109
Face19	0.1069	-0.2868	0.7825	0.9167
Face20	0.0554	-0.2930	0.8396	0.9218
Average	-0.0119	-0.2584	0.8383	0.9256

TABLE 4. Correlation values for the twenty biometrics traits of the LFW database.

The twenty biometrics images of the LFW database	Correlation with the false face		Correlation with the true face	
	OSH [43]	GA scheme (Proposed)	OSH [43]	GA scheme (Proposed)
Face1	-0.0217	-0.0079	0.9013	0.9032
Face2	-0.0339	0.1418	0.8915	0.8923
Face3	0.0570	0.2285	0.8548	0.8809
Face4	-0.0157	0.1797	0.8553	0.8846
Face5	-0.1120	-0.0248	0.8418	0.8258
Face6	-0.2642	-0.1980	0.8448	0.8498
Face7	-0.0821	0.1240	0.8810	0.9087
Face8	-0.2792	-0.0281	0.9084	0.9230
Face9	-0.0065	0.2406	0.8691	0.8884
Face10	-0.2202	0.1770	0.9059	0.9353
Face11	-0.1411	0.1605	0.8889	0.9362
Face12	0.0818	0.0423	0.8841	0.8970
Face13	0.0509	0.0762	0.8511	0.8722
Face14	-0.0286	0.1844	0.8953	0.9229
Face15	-0.1260	0.1344	0.8437	0.8775
Face16	-0.0266	0.2286	0.8739	0.9172
Face17	0.1365	0.2144	0.8878	0.8991
Face18	0.1439	-0.0130	0.8503	0.8682
Face19	-0.0426	0.0482	0.8698	0.9042
Face20	-0.0756	0.2963	0.8619	0.9094
Average	-0.0496	0.1099	0.8729	0.8950

From the illustrated objective/subjective outcomes, it is emphasized that the suggested GA cryptosystem is excellent for accomplishing a robust cancelable biometric framework associated with the traditional OSH technique [42]. The suggested GA cryptosystem has remarkable objective and

TABLE 5. Correlation values for the twenty biometrics traits of the first FVC2002 database.

The twenty biometrics images of the first FVC2002 database	Correlation with the false fingerprint		Correlation with the true fingerprint	
	OSH [43]	GA scheme (Proposed)	OSH [43]	GA scheme (Proposed)
Fingerprint 1	-0.0267	0.0350	0.7670	0.9738
Fingerprint 2	-0.0338	-0.0097	0.8267	0.9823
Fingerprint 3	-0.0074	0.0353	0.8258	0.9777
Fingerprint 4	-0.0511	-0.0163	0.7856	0.9825
Fingerprint 5	-0.01689	0.0383	0.8189	0.9746
Fingerprint 6	-0.05738	-0.0408	0.8168	0.9790
Fingerprint 7	-0.0443	0.0399	0.8124	0.9727
Fingerprint 8	-0.0295	-0.0452	0.8129	0.9781
Fingerprint 9	-0.0460	0.0293	0.8057	0.9755
Fingerprint 10	-0.0505	0.0520	0.8400	0.9729
Fingerprint 11	-0.0580	0.0376	0.7834	0.9714
Fingerprint 12	-0.0455	0.0081	0.8363	0.9778
Fingerprint 13	-0.0122	0.0161	0.8356	0.9717
Fingerprint 14	0.0043	0.0253	0.8410	0.9665
Fingerprint 15	-0.0171	0.0066	0.8104	0.9716
Fingerprint 16	0.0136	-0.0114	0.7912	0.9777
Fingerprint 17	0.0020	0.0212	0.8275	0.9726
Fingerprint 18	-0.0122	0.0243	0.8051	0.9721
Fingerprint 19	-0.0244	0.0196	0.8124	0.9743
Fingerprint 20	-0.0200	-0.0001	0.8308	0.9711
Average	-0.0268	0.0129	0.8145	0.9749

TABLE 6. Correlation values for the twenty biometrics traits of the second FVC2002 database.

The twenty biometrics images of the second FVC2002 database	Correlation with the false fingerprint		Correlation with the true fingerprint	
	OSH [43]	GA scheme (Proposed)	OSH [43]	GA scheme (Proposed)
Fingerprint 1	-0.1174	-0.5707	0.4452	0.9551
Fingerprint 2	-0.1307	-0.4811	0.8405	0.9262
Fingerprint 3	-0.0232	-0.4767	0.7696	0.9191
Fingerprint 4	0.2058	-0.5384	0.4721	0.97637
Fingerprint 5	-0.0907	-0.5700	0.5009	0.9724
Fingerprint 6	-0.0378	-0.5298	0.7246	0.9528
Fingerprint 7	-0.0285	-0.5320	0.6117	0.9360
Fingerprint 8	0.0482	-0.5283	0.6393	0.9616
Fingerprint 9	0.0389	-0.4921	0.6477	0.9118
Fingerprint 10	-0.0606	-0.5288	0.6552	0.9425
Fingerprint 11	-0.0294	-0.4881	0.7366	0.9225
Fingerprint 12	-0.1656	-0.5350	0.7420	0.9222
Fingerprint 13	0.0289	-0.5392	0.5694	0.9469
Fingerprint 14	-0.0455	-0.5608	0.4688	0.9755
Fingerprint 15	0.1142	-0.3600	0.7637	0.8914
Fingerprint 16	-0.0863	-0.5603	0.5894	0.9557
Fingerprint 17	0.1623	-0.5422	0.4628	0.9678
Fingerprint 18	0.0662	-0.4667	0.7564	0.9223
Fingerprint 19	0.0247	-0.3378	0.8048	0.8731
Fingerprint 20	-0.0126	-0.5684	0.2285	0.9772
Average	-0.0073	-0.5123	0.6223	0.9404

TABLE 7. EER and AROC of the ORL database in the existence of noise.

Noise variance	OSH [43]		GA scheme (Proposed)	
	EER	AROC	EER	AROC
0.0	0.0021	0.9803	0.0025	0.9990
0.01	0.0023	0.9814	0.0026	0.9990
0.02	0.0027	0.9816	0.0025	0.9992
0.03	0.0023	0.9803	0.0021	0.9990
0.04	0.0018	0.9782	0.0023	0.9991
0.05	0.0073	0.9859	0.0024	0.9991

TABLE 8. EER and AROC of the FERET database in the existence of noise.

Noise variance	OSH [43]		GA scheme (Proposed)	
	EER	AROC	EER	AROC
0.0	0.0116	0.9792	0.0096	0.9951
0.01	0.0109	0.9791	0.0101	0.9951
0.02	0.0113	0.9787	0.0094	0.9953
0.03	0.0115	0.9792	0.0094	0.9951
0.04	0.0111	0.9794	0.0102	0.9946
0.05	0.0114	0.9787	0.0106	0.9951

TABLE 9. EER and AROC of the LFW database in the existence of noise.

Noise variance	OSH [43]		GA scheme (Proposed)	
	EER	AROC	EER	AROC
0.0	0.0095	0.9917	0.0064	0.9953
0.01	0.0094	0.9920	0.0067	0.9952
0.02	0.0097	0.9922	0.0067	0.9953
0.03	0.0093	0.9919	0.0062	0.9953
0.04	0.0095	0.9913	0.0063	0.9954
0.05	0.0095	0.9922	0.0071	0.9951

TABLE 10. EER and AROC of the first FVC2002 database in the existence of noise.

Noise variance	OSH [43]		GA scheme (Proposed)	
	EER	AROC	EER	AROC
0.0	0.0093	0.9829	0.0005	0.9998
0.01	0.0101	0.9842	0.0002	0.9998
0.02	0.0102	0.9824	0.0004	0.9998
0.03	0.0098	0.9817	0.0003	0.9998
0.04	0.0109	0.9863	0.0007	0.9998
0.05	0.0092	0.9828	0.0006	0.9998

TABLE 11. EER and AROC of the second FVC2002 database in the existence of noise.

Noise variance	OSH [43]		GA scheme (Proposed)	
	EER	AROC	EER	AROC
0.0	0.0186	0.7534	0.0128	0.9985
0.01	0.0185	0.7551	0.0131	0.9985
0.02	0.0184	0.7603	0.0122	0.9985
0.03	0.0187	0.7543	0.0130	0.9985
0.04	0.0186	0.7494	0.0125	0.9984
0.05	0.0185	0.7499	0.0126	0.9984

subjective outcomes for different fingerprints and faces with various features.

To further investigate the efficiency of the presented GA cryptosystem for developing an efficient cancelable biometric authentication system, further experiments are performed for testing the performance accomplishment of the suggested authentication framework with the conventional authentication frameworks [8], [14], [21], [23], [29], [33], [42], [45]. We compared the statistical evaluation security analysis of the False Accept Rate (FAR), EER, False Reject Rate (FRR), and AROC results of the proposed GA-based cancelable biometric authentication system with the recent literature cancelable biometric authentication systems in [42, 34, 24, 21, 14, 8,

TABLE 12. Processing time (sec) of the proposed framework and the traditional OSH algorithm.

Biometric database	OSH [43]	GA (Proposed)
FERET database	0.5616	33.77×10^{-3}
LFW database	0.4273	76.65×10^{-3}
ORL database	0.5038	37.04×10^{-3}
1st Fingerprint database	0.4973	12.65×10^{-3}
2nd Fingerprint database	0.3291	16.94×10^{-3}

TABLE 13. The statistical security analysis for the suggested biometric authentication framework and the related biometric authentication frameworks.

Cancelable biometric system	EER	FAR	FRR	AROC
Proposed (GA)	2.0243×10^{-4}	4.8843×10^{-4}	2.2693×10^{-4}	0.9998
OSH [43, 27]	0.0102	0.0541	0.0155	0.9791
[8]	0.0178	0.0017	0.8769	0.8967
[14]	8.7546×10^{-09}	0.0435	6.1101×10^{-03}	0.7187
[21]	0.0016	0.1955	4.5354×10^{-04}	0.8737
[24]	5.6942×10^{-10}	3.0414×10^{-07}	0.9671	0.9076
[30]	3.1524×10^{-12}	0.0985	1.6822×10^{-04}	0.8630
[34]	0.0046	2.3550×10^{-04}	0.9292	0.8837
[46]	9.5647×10^{-05}	0.0056	2.5216×10^{-03}	0.8684

30, 46] as shown in Table 13. From the illustrated comparative outcomes in Table 13, we observed that the obtained values of the whole examined metrics of the suggested authentication framework are more appreciated and recommended compared to other literature cancelable biometric systems. This is due to the earlier discussed outstanding merits and features of the employed GA encryption algorithm.

VI. CONCLUSION AND FUTURE WORK

This paper investigated an improved encryption algorithm for developing and building an efficient cancelable biometric authentication framework, which is more robust against hackers. The significant contribution of this proposal is the application of a Genetic encryption algorithm for achieving a powerful cancelable biometric authentication system. The presented GA encryption scheme performs diffusion and scrambling to the ciphered biometric traits instantaneously. The tested simulation outcomes emphasized improving the proposed GA cryptosystem for inexpensively enciphering the stored biometric templates. So, it is convenient for protecting biometric patterns contrasted to conventional algorithms. It delivers pleasing PFD, PTD, ROC, histogram, correlation, processing time, and graphical findings. The suggested GA encryption scheme has verified its ability to deform or cipher different biometric patterns efficiently. So, the proposed cancelable biometric system strengthens the cancellability of the stored biometric templates compared to the state-of-the-art methods. Also, simulation and comparison findings acquired for the suggested biometric authentication framework accomplish an average EER, FAR, and FRR of 2.0243×10^{-4}, 4.8843×10^{-4}, and 2.2693×10^{-4}, correspondingly, and an average AROC of 0.9998. In the future, a detailed study of multi-level cancelable biometric privacy systems may be tested with the application of various encryption, watermarking, and steganography algorithms for attaining robust and reliable storage of biometrics. Furthermore, we are interested in involving security-based deep learning methods to secure biometrics storage and transmission.

ACKNOWLEDGMENT

The authors would like to acknowledge the support received from Taif University Researchers Supporting Project Number (TURSP-2020/147), Taif university, Taif, Saudi Arabia.

REFERENCES

[1] N. F. Soliman, M. I. A. D. K. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 1–35, 2020.
[2] A. D. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. E. A. El-Samie, and N. F. Soliman, "Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications," *Entropy*, vol. 22, no. 12, p. 1361, Nov. 2020.
[3] L. A. A. Elazm, S. Ibrahim, M. G. Egila, H. Shawkey, M. K. H. Elsaid, W. El-Shafai, and F. E. A. El-Samie, "Hardware implementation of cancellable biometric systems," in *Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Oct. 2020, pp. 1145–1152.
[4] A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, "A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.
[5] S. Ibrahim, M. G. Egila, H. Shawky, M. K. Elsaid, W. El-Shafai, and F. E. A. El-Samie, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, vol. 79, pp. 1–26, Feb. 2020.
[6] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101690.
[7] M. Joshi, B. Mazumdar, and S. Dey, "A comprehensive security analysis of match-in-database fingerprint biometric system," *Pattern Recognit. Lett.*, vol. 138, pp. 247–266, Oct. 2020.
[8] A. Sinha, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes," *Opt. Eng.*, vol. 44, no. 5, May 2005, Art. no. 057001.
[9] W. El-Shafai, I. M. Almomani, and A. Alkhayer, "Optical bit-pane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication," *IEEE Access*, vol. 9, pp. 35004–35026, 2021.
[10] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
[11] O. Enerstvedt, "Analysis of privacy and data protection principles," in *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, O. M. Enerstvedt, Ed. Cham, Switzerland: Springer, 2017, pp. 307–394.
[12] X. Zheng, "The application of information security encryption technology in military data system management," in *Proc. Int. Conf. Man-Mach.-Environ. Syst. Eng.* Singapore: Springer, Oct. 2017, pp. 423–428.
[13] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102704.
[14] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.
[15] R. Jaichandran, "Biometric based user authentication and privacy preserving in cloud environment," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 347–350, Apr. 2021.
[16] V. R. Falmari and M. Brindha, "Privacy preserving biometric authentication using chaos on remote untrusted server," *Measurement*, vol. 177, Jun. 2021, Art. no. 109257.
[17] N. D. Sarier, "Efficient biometric-based identity management on the blockchain for smart industrial applications," *Pervas. Mobile Comput.*, vol. 71, Feb. 2021, Art. no. 101322.

[18] Z. Xu, Z. Shao, Y. Shang, B. Li, H. Ding, and T. Liu, ''Fusing structure and color features for cancelable face recognition,'' *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 1–18, 2021.

[19] M. Shahzad, S. Wang, G. Deng, and W. Yang, ''Alignment-free cancelable fingerprint templates with dual protection,'' *Pattern Recognit.*, vol. 111, Mar. 2021, Art. no. 107735.

[20] A. Nagar, K. Nandakumar, and A. K. Jain, ''A hybrid biometric cryptosystem for securing fingerprint minutiae templates,'' *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 733–741, Jun. 2010.

[21] C. Rathgeb and A. Uhl, ''A survey on biometric cryptosystems and cancelable biometrics,'' *Eurasip J. Inf. Secur.*, vol. 2011, no. 1, p. 3, Dec. 2011.

[22] V. M. Patel, N. K. Ratha, and R. Chellappa, ''Cancelable biometrics: A review,'' *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[23] C. Moujahdi, S. Ghouzali, M. Mikram, M. Rziza, and G. Bebis, ''Spiral cube for biometric template protection,'' in *Proc. Int. Conf. Image Signal Process.* Berlin, Germany: Springer, 2012, pp. 235–244.

[24] L. Zhang, H. Wang, and L. Tao, ''One-factor cancelable fingerprint template protection based on feature enhanced hashing,'' in *Proc. 12th Int. Conf. Graph. Image Process. (ICGIP)*, Jan. 2021, Art. no. 1172017.

[25] H. Mandalapu, A. Reddy P N, R. Ramachandra, K. S. Rao, P. Mitra, S. R. M. Prasanna, and C. Busch, ''Audio-visual biometric recognition and presentation attack detection: A comprehensive survey,'' *IEEE Access*, vol. 9, pp. 37431–37455, 2021.

[26] A. Alarifi, M. Amoon, M. H. 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.

[27] O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, ''Secure color image cryptosystem based on chaotic logistic in the FrFT domain,'' *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2495–2519, Jan. 2020.

[28] I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas, F. E. A. El-Samie, H. S. El-sayed, and O. S. Faragallah, ''Efficient chaotic-based image cryptosystem with different modes of operation,'' *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 20665–20687, Aug. 2020.

[29] O. S. Faragallah, H. S. El-sayed, A. Afifi, and W. El-Shafai, ''Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform,'' *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106333.

[30] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E.-S.-M. El-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. A. El-Samie, and H. S. El-sayed, ''Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication,'' *J. Ambient Intell. Humanized Comput.*, vol. 710, pp. 1–25, Feb. 2021.

[31] A. Sarkar, B. Singh, and U. Bhaumik, ''Cryptographic key generation scheme from cancelable biometrics,'' in *Progress in Computing, Analytics and Networking*. Singapore: Springer, 2018, pp. 265–272.

[32] B. Alam, Z. Jin, W.-S. Yap, and B.-M. Goi, ''An alignment-free cancelable fingerprint template for bio-cryptosystems,'' *J. Netw. Comput. Appl.*, vol. 115, pp. 20–32, Aug. 2018.

[33] Q. Gao and C. Zhang, ''Constructing cancellable template with synthetic minutiae,'' *IET Biometrics*, vol. 6, no. 6, pp. 448–456, Nov. 2017.

[34] Z. Jin, J. Hwang, S. Kim, S. Cho, Y. Lai, and A. Teoh, ''A cancelable ranking based hashing method for fingerprint template protection,'' in *Proc. Int. Conf. Mobile Netw. Manage.* Cham, Switzerland: Springer, 2017, pp. 378–389.

[35] M. S. Obaidat, S. P. Rana, T. Maitra, D. Giri, and S. Dutta, ''Biometric security and Internet of Things (IoT),'' in *Biometric-Based Physical and Cybersecurity Systems*. Cham, Switzerland: Springer, 2019, pp. 477–509.

[36] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, ''Generating cancelable fingerprint templates,'' *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[37] M. Sandhya and M. V. N. K. Prasad, ''Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme,'' *Int. J. Pattern Recognit. Artif. Intell.*, vol. 31, no. 4, Apr. 2017, Art. no. 1756004.

[38] M. A. M. Ali and N. M. Tahir, ''Cancelable biometrics technique for iris recognition,'' in *Proc. IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2018, pp. 434–437.

[39] R. Soliman, N. Ramadan, M. Amin, H. Ahmed, S. El-Khamy, and F. El-Samie, ''Efficient cancelable Iris recognition scheme based on modified logistic map,'' in *Proc. Nat. Acad. Sci., India A, Phys. Sci.*, 2018, pp. 1–7.

[40] R. F. Soliman, G. M. El Banby, A. D. Algarni, M. Elsheikh, N. F. Soliman, M. Amin, and F. E. A. El-Samie, ''Double random phase encoding for cancelable face and iris recognition,'' *Appl. Opt.*, vol. 57, no. 35, pp. 10305–10316, Dec. 2018.

[41] R. F. Soliman, M. Amin, and F. E. A. El-Samie, ''A double random phase encoding approach for cancelable iris recognition,'' *Opt. Quantum Electron.*, vol. 50, no. 8, p. 326, Aug. 2018.

[42] T. C. Poon and J. P. Liu, *Introduction to Modern Digital Holography: With MATLAB*. Cambridge, UK.: Cambridge Univ. Press, 2014.

[43] P. W. M. Tsang, J.-P. Liu, and T.-C. Poon, ''Compressive optical scanning holography,'' *Opt. Soc. Amer.*, vol. 2, no. 5, pp. 476–483, 2015.

[44] V. Srikanth, U. Asati, V. Natarajan, T. P. Kumar, T. Mullapudi, and N. C. H. S. N. Iyengar, ''Bit-level encryption of images using genetic algorithm,'' *Int. J. Comput. Sci. Commun. Technol.*, vol. 3, no. 1, pp. 546–550, 2010.

[45] I. S. I. Abuhaiba and M. A. S. Hassan, ''Image encryption using differential evolution approach in frequency domain,'' *Signal Image Process., Int. J.*, vol. 2, no. 1, pp. 51–69, Mar. 2011.

[46] A. Gorodilov and V. Morozenko, ''Genetic algorithm for finding the key's length and cryptanalysis of the permutation cipher,'' *Int. J. Inf. Theories Appl.*, vol. 15, no. 4, pp. 94–99, 2008.

[47] S. Bhowmik and A. Acharyya, ''Image cryptography: The genetic algorithm approach,'' in *Proc. IEEE Int. Conf. Comput. Sci. Automat. Eng.*, vol. 3, Jun. 2011, pp. 223–227.

[48] A. F. M. Al-Husainy, ''Image encryption using genetic algorithm,'' *Inf. Technol. J.*, vol. 3, pp. 516–519, Jan. 2006.

[49] G. N. Rajendra and R. K. Kaur, ''A new approach for data encryption using genetic algorithms and brain mu waves,'' *Int. J. Sci. Eng. Res.*, vol. 2, no. 5, pp. 1–4, 2011.

[50] M. Hammad, G. Luo, and K. Wang, ''Cancelable biometric authentication system based on ECG,'' *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1857–1887, Jan. 2019.

[51] L. Leng, A. B. J. Teoh, M. Li, and M. K. Khan, ''Analysis of correlation of 2DPalmHash Code and orientation range suitable for transposition,'' *Neurocomputing*, vol. 131, pp. 377–387, May 2014.

[52] M. Hammad, Y. Liu, and K. Wang, ''Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint,'' *IEEE Access*, vol. 7, pp. 26527–26542, 2019.

[53] V. G. Machado and K. B. Sudeepa, ''Genetic algorithm based image cryptography,'' *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 5, no. 5, pp. 226–232, 2016.

[54] E. Volte, J. Patarin, and V. Nachef, ''Zero knowledge with Rubik's cubes and non-abelian groups,'' in *Proc. Int. Conf. Cryptol. Netw. Secur.* Cham, Switzerland: Springer, 2013, pp. 74–91.

[55] J. Wu, Z. Zhu, and S. Guo, ''A quality model for evaluating encryption-as-a-service,'' in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, 2017, pp. 557–569.

[56] M. Tarek, O. Ouda, and H. T. Hamza, ''Pre-image resistant cancelable biometrics scheme using bidirectional memory model,'' *IJ Netw. Secur.*, vol. 19, no. 4, pp. 498–506, 2017.

[57] (Accessed: Dec. 12, 2020). *ORL Database*. [Online]. Available: https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[58] (Accessed: Dec. 12, 2020). *FERET Database*. [Online]. Available: https://www.nist.gov/itl/products-and-services/color-feret-database

[59] (Accessed: Dec. 12, 2020). *LFW Database*. [Online]. Available: http://vis-www.cs.umass.edu/lfw/

[60] (Accessed: Dec. 12, 2020). *FVC2002 (DB1) Database*. [Online]. Available: https://www.biometricsinstitute.org/resources/fingerprintverification-competition-fvc

[61] (Accessed: Dec. 12, 2020). *FVC2002 (DB2) Database*. [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. Since January 2021, he has been a Postdoctoral Research Fellow with the Security Engineering Laboratory (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently working as a Lecturer and an Assistant Professor with the Department of Electronics and Communication Engineering (ECE), FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software-defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He also serves as a reviewer for several international journals.

FATMA A. HOSSAM ELDEIN MOHAMED was born in Alexandria, Egypt. She received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Alexandria Higher Institute of Engineering and Technology, Alexandria, in 2010, and the M.Sc. degree from the Faculty of Engineering, Alexandria University, in 2016. She has been a Teaching Assistant with the Alexandria Higher Institute of Engineering and Technology. Her research interests include information security, optical signal processing, big data, and cloud computing, image and video signal processing, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, encryption, and steganography.

HASSAN M. A. ELKAMCHOUCHI (Life Senior Member, IEEE) is currently a Professor of wireless communications, antennas and wave propagation with the Electronics and Electrical Communications Department, Faculty of Engineering, Alexandria University. He has a demonstrated history of working in antennas and wave propagation, data security in computer and communication networks, cryptography and steganography, electrical and electronic manufacturing industry, and biomedical engineering skilled in mathematica. He received the Encouragement State Award 2002 from the Faculty of Engineering, Alexandria University.

MOHAMMED ABD-ELNABY received the B.S., M.S., and Ph.D. degrees in electronic engineering from Menoufia University, Menouf, Egypt, in 2000, 2004, and 2010, respectively. Since 2010, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. Since 2015, he has also been working as an Associate Professor with the Department of Electronics and Electrical Communication, Faculty of Electronic Engineering, Menoufia University. He has coauthored about 69 articles in international journals and conference proceedings. His research interests include wireless resource management, MAC protocols, cognitive radio, cooperative communication, the IoT, 5G communication, NOMA, and D2D communication.

AHMED ELSHAFEE received the Ph.D. degree in electrical engineering from the Faculty of Engineering, Alexandria University. He currently works as an Associate Professor and the Acting Vice-Dean of the Faculty of Engineering, Ahram Canadian University. He published 27 research articles, international conferences, and journals in electrical engineering and computer engineering related fields. His researches were cited by 427 other research, and his H-index is nine, till January 2021. He received the Best Young Scientist Award as per the conference council recommendation (National Radio Science Conference 2001), Alexandria, Egypt, for his paper entitled Rotor Enhanced Block Cipher (REBC).