IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 20, 2022, accepted April 9, 2022, date of publication May 11, 2022, date of current version May 31, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3174350

A Cancelable Biometric Security Framework Based on RNA Encryption and Genetic Algorithms

FATMA A. HOSSAM ELDEIN MOHAMED[1], WALID EL-SHAFAI[2], HASSAN M. A. ELKAMCHOUCHI[1], (Life Senior Member, IEEE), ADEL ELFAHAR[1], ABDULAZIZ ALARIFI[3], MOHAMMED AMOON[3], MOUSTAFA H. ALY[4], FATHI E. ABD EL-SAMIE[2], AMAN SINGH[5,7], AND AHMED ELSHAFEE[6]

[1]Department of Electronics and Electrical Communications Engineering, Alexandria University, Alexandria 21544, Egypt
[2]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3]Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[4]Electronics and Communications Engineering Department, College of Engineering and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria 1029, Egypt
[5]Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain
[6]Department of Electrical Engineering, Faculty of Engineering, Ahram Canadian University, 6th October City, Giza 12451, Egypt
[7]Department of Engineering, Universidad Internacional Iberoamericana, Arecibo 00613, Puerto Rico, U.S.

Corresponding authors: Abdulaziz Alarifi (abdulazizalarifi@ksu.edu.sa) and Walid El-Shafai (eng.waled.elshafai@gmail.com)

This work was supported by the Researchers Supporting Project, King Saud University, Riyadh, Saudi Arabia, under Grant RSP-2021/300.

ABSTRACT Cancelable biometric recognition techniques play a vital role in the privacy and security of remote surveillance systems to keep the genuine users' confidential data safe and away from intruders. This research work presents an efficient cancelable biometric recognition framework that exploits an irreversible hybrid encryption algorithm. It incorporates Deoxyribonucleic, Ribonucleic Acid sequence (DNA and RNA) encryption technique, and an evolutionary optimization technique, namely Genetic Algorithms (GAs). These techniques are employed to create completely deformed templates from their original ones. Hence, the main contribution is introducing a novel biometric security framework that achieves unique randomness characteristics using RNA and DNA sequences and the evolutionary GA technique. The proposed framework produces entirely deformed biometric templates by ciphering the main discriminative features of the biometric traits of the authorized clients. It is firstly initialized by creating several encrypted biometric images for the original users with the logistic map. After that, the initially encrypted images are transformed into vectors of a binary array. Then, they are converted to their corresponding introns, and exons, and consequently, their relevant codons are stored in the cloud database. These relevant codons are replaced by new ones after generating encrypted RNA lists. The utilized encryption key for each template is extracted from the original biometric image through excessive permutations between pixels. The GA optimization technique is applied to select the most convenient biometric features. Finally, after employing the GA-based cross-over and mutation operations, the chosen features are used to generate the cancelable biometric traits. To assess the proposed framework, six different biometric databases are considered. These databases are Olivetti Research Laboratory (ORL) Faces (gray), CASIA v.5 Faces (color), UPOL Iris (gray), Indian Institute of Technology Delhi (IIT Delhi) Ear (color and gray), Fingerprint, and CASIA Palmprint (color and gray). The security performance of the proposed encryption algorithm is compared to those of recent studies in this field, such as Optical Scanning Holography (OSH) and Double Random Phase Encoding (DRPE). The simulation results prove the superior performance of the proposed framework in terms of all adopted evaluation metrics. The proposed framework provides high Area under the Receiver Operating Characteristic (AROC) curve that reaches 0.9990, low False Acceptance Rate (FAR) of 0.0015, more uniform histograms, high correlation values for genuine users, and completely hidden biometric features. In addition, from the security perspective, the proposed framework achieves good entropy, Unified Average Changing Intensity (UACI), and Number of Pixels Change Rate (NPCR) values that reach 7.9960, 33.55%, and 99.65%, respectively.

INDEX TERMS Biometric security, DNA, RNA, GA, OSH, cross-over, mutation, AROC, FAR.

I. INTRODUCTION

Biometric recognition techniques have acquired a large attention nowadays in security applications. They are now taking

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

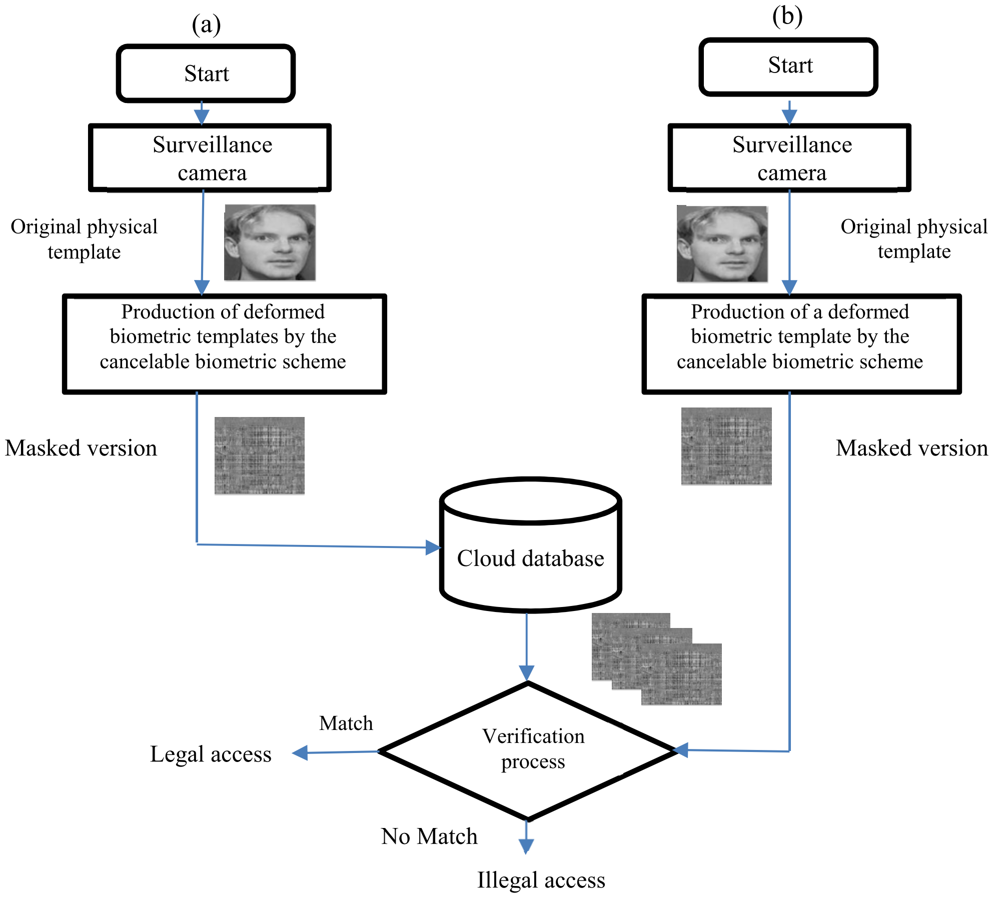


FIGURE 1. General cancelable biometric system, (a) Registration phase and (b) Testing phase.

place of the old scenarios of maintaining privacy and security, such as Personal Identification Numbers (PINs), passwords, and tokens that can be stolen or damaged, easily. Hence, nowadays, biometric features and traits corresponding to genuine users are applied in different aspects of security applications, such as verification, authentication, and recognition systems. The utilization of biometric images in these applications provides a remarkable improvement in preserving the confidentiality and privacy of users because of their uniqueness. Despite the effectiveness of using biometric features, there are a lot of limitations for exploiting their characteristics in various authentication applications. First of all, if the biometric system is hacked, the biometric traits cannot be replaced or altered. In addition, intruders may copy the personal data, if the features are stolen [1]. Hence, several research studies have been introduced to keep biometric data safe and away from unauthorized access. As a result, various generated biometric traits can be extracted from the original ones and used in several security systems and institutions, such as schools, banks, firms, and corporations.

The conventional biometric authentication techniques depend on the extraction of unique features from the registered templates to reduce the amount of collected data. Moreover, these features are kept in a safe data storage. This operation of registration is considered as the enrollment phase. In addition, the authentication phase includes the measurement of similarity between the corresponding biometric features of the enrolled data for authorized users and those of new users trying to access the system. The main disadvantage of these traditional biometric security techniques is obtaining the biometric traits and storing them in the cloud database. If an intruder succeeds in snatching the original biometric data, this will lead to a significant failure of the whole authentication system, as the information about the authorized users is lost. Moreover, the intruder can access the system as an authorized user [2]. In addition, biometric traits that have been stolen or hacked cannot be used again by their owners in any other application. Consequently, traditional biometric recognition techniques that depend on the original traits are not considered reliable [2]. Therefore, recently, cancelable biometric recognition systems have appeared as an alternative solution to keep the original biometrics safe [3]. Fig. 1 illustrates the idea of cancelable biometrics.

The main concept of the cancelable biometric schemes is the transformation of genuine biometric data to transformed or deformed templates [2], [3]. Several templates can be generated for the same original template to be used in different applications. One-way arithmetic transformations and encryption algorithms are possible solutions to generate cancelable biometric templates. The generated templates need to satisfy reusability, revocability, and randomness criteria. A major advantage of this trend in biometric recognition is privacy preservation [5], [6]. Different transformations can be designed to achieve the requirements of cancelable biometric systems [7]–[10].

Generally, the cancelable biometric systems that depend on feature encryption are preferred to those depending on non-invertible transformations. This is reflected in the evaluation metrics including correlation scores, AROC, FAR, and histogram uniformity [4]. Hence, the trend of feature encryption has been widely adopted in cancelable biometric systems. In addition, the matching process of encrypted templates is easy with correlation metrics. Unfortunately, traditional image encryption algorithms, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are not recommended for cancelable biometric recognition applications due to several implementation difficulties like key management and implementation complexity [5]. The main challenge for most encryption techniques is how to keep immunity to hacking and intrusion attempts [6].

The essential merits of the proposed cancelable biometric recognition framework are summarized as follows:

1. The suggested framework is composed of a hybrid structure of deformation tools, based mainly on encryption technique. This structure leads to more security of the cancelable biometric system and confidentiality of users.
2. The secret key of encryption is kept away from intruders, because it is not registered or stored. Alternatively, RNA encryption lists are adopted in generating the initial populated cipher images with GA.
3. The features of the evolutionary GA technique are exploited. They include:
   a) Selecting the best initial cipher image, which leads to more randomness.
   b) Implementing the cross-over step, which leads to more confusion.
   c) Implementation of mutation operation, which leads to more diffusion and diversity.
4. The proposed cancelable biometric recognition framework is superior to the related studies in terms of reliability and efficiency, when examined over a large variety of biometric datasets.
5. The proposed cancelable biometric recognition framework is immune to different levels of noise according to the adopted evaluation metrics.
6. The proposed framework is superior to other cancelable biometric system as revealed by the introduced comparison study.

The rest of the sections of this research work are arranged as follows. Section II presents the recent related works. Section III describes the basic concepts of the logistic map, DNA, RNA, and GA technique. Section IV gives an explanation of the proposed cancelable biometric recognition framework. Moreover, it illustrates the methodology of generating the chromosomes and off-spring cipher templates using the logistic map and RNA codons. Section V presents the experimental results with discussions and comparisons. Moreover, it illustrates the security analysis of the hybrid RNA-GA encryption-based cancelable biometric recognition framework. It also gives a discussion of the definitions of the examined evaluation metrics. Section VI demonstrates the importance of converting the biometric image to RNA symbols before applying the GA technique. Finally, the conclusion and future work are introduced in Section VII.

II. RELATED WORK

Biometric traits can be divided into two main categories, according to the dependence on either behavioral or physical features. The physical features are more reliable than behavioral features because of their uniqueness. In addition, they have more robustness to noise than behavioral features [4]. That is why most researchers presented their research studies on faces, fingerprints, palmprints, ECG pulses, or EEG signals. Different studies are now directed to making the original biometric traits safe and more protected [7]–[30], as summarized in Table 1.

In [1], the authors introduced a key generation algorithm that employs a fuzzy commitment scheme to hide the secret keys for generating cancelable iris patterns. This algorithm provided an EER equal to zero. In [2], the authors presented an asymmetric encryption algorithm to produce a couple of public keys to be exploited in the encryption stage to enhance the level of security. In [7], the authors reviewed the conventional encryption schemes used in cancelable biometric applications in order to produce the cipher key that can be used for making the original data hard to access. In [8], [9], the researchers introduced different encryption methods that depend on chaotic algorithms. The chaotic theory provides remarkable, distributive, and statistical characteristics that can be employed in image encryption, while keeping a good level of entropy. Moreover, these features make the relation between the original templates, key, and encrypted templates hard to be recognized.

In [10], the authors suggested a biometric security algorithm that is dependent on various discrete transformations such as Discrete Fourier Transform (DFT), Fractional Fourier Transform (FrFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Furthermore, a matrix rotation process is used to obtain cancelable biometric traits that satisfy the revocability and confusion characteristics. This algorithm achieved good experimental results, namely an AROC of 0.998, an EER of 0.0023, an FAR of 0.08, and an FRR of 0.003.

The authors of [11] introduced cancelable face and fingerprint recognition systems depending on the 3D Jigsaw transformation and an optical ciphering technique. The FrFT is used in the optical ciphering process with a single random

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

Work	Purpose	Biometric traits	Approach	Merits	Demerits
[13]	Obtaining ciphered traits using Gabor filters, convolution kernels, and chaotic maps	Iris traits (CASIA v.3)	Bilateral modified chaotic logistic maps	Achieving an accuracy of up to 99.07%	Vulnerable to brute-force attacks and replay attacks
[15]	Producing cancelable biometric traits based on merging various patterns	Iris templates (CASIA v.3 & v.4)	DRPE and FrFT	Accuracy reaches 99.75%	Vulnerable to reversible brute-force attacks, more expensive, and more complex
[16]	Adopting the fuzzy commitment scheme to encrypt biometric traits	Fingerprint traits	Several spiral curves using the fuzzy concepts	Achieving blind authentication	The system suffers from the instability that leads to high FRR
[17]	Employing non-invertible transformations to conceal the genuine iris features	Iris features (CASIA v.3)	Encryption and one-way transformations	Providing a recognition rate of up to 99.9%	Low variety of tested biometric traits
[22]	Constructing cancelable EEG feature vectors using different matrix operations	EEG signals (MIT-BIH arrhythmia, PTB, and CYBHi datasets)	Modified Bio-Hashing and matrix operations	Providing a solution for the low accuracy, which is the essential obstacle in Bio-Hashing	The biometric details can be discovered if a hacker has preceding knowledge about the key and the biometric features
[23]	Employing 2D Gabor filter to generate cancelable palmprint templates	Palmprint features (poly U version 2 dataset)	A matrix of palm Hash code	Concealing vertical similarities	Low robustness to statistical analysis attack for different biometric traits
[24]	Implementing ECG cancelable biometric analysis using the diffusion of pulse levels	ECG signal database	Traditional neural-network and Q-Gaussian multi-SVM	Presenting high recognition accuracy and robustness to spoof attacks	Need to increase the speed of operations
[25]	Producing cancelable biometric traits based on the GA ciphering technique	Face and fingerprint templates (FERET, LFW, ORL, and FVC 2004 datasets)	GA-based permutations and encryption algorithms	Achieving more randomization, lower processing time, and AROC = 0.9998	Vulnerable to masquerade attacks
[26]	Generating cancelable fingerprint features using the fuzzy vault scheme	Fingerprint features	Fuzzy vault-based encryption technique	Efficient performance during the verification process	Vulnerable to blended substitution attacks and possibility of hacking on error-correcting codes.
[27]	Using fingerprint features to generate cryptographic keys	Fingerprint features	Data-dependent cipher technique	High privacy for the storage of client data	Vulnerable to masquerade attacks
[28]	Employing random projection and discrete Fourier transform	Fingerprint features	Hybrid transformations	Robustness of the authorized features	More complexity to integrate and implement the algorithm
[29]	Applying random salting to generate cancelable templates	Fingerprint features	K-nearest neighbor scheme	Hard to be hacked by most attacks	Vulnerable to record multiplicity attacks
[30]	Exploiting hash coding as an irreversible transformation scheme	Fingerprint features	Hash coding	Useful for the revocability and linkability	Less performance, because it suffers from accuracy loss
Proposed work	Implementing a cancelable biometric security framework based on the hybrid RNA-GA encryption algorithm	Six different biometric datasets (ORL and CASIA v.5 for faces, UPOL iris, IIT Delhi ears, CASIA palmprints, and fingerprints)	Logistic map, RNA encryption, and GA optimization	1) No glimpses of the genuine biometric features in the cancelable traits 2) No storage of the original genuine biometric traits during the enrollment 3) Working on gray and color biometric templates 4) No need for image registration 5) Robustness to noise effect	Need for high storage area in the cloud system to store the codon tables

phase mask. The experimental results revealed an average EER, an AROC, an FAR, and an FRR of 9.3997×10^{-15}, 0.9997, 2.6288×10^{-17}, and 1.8969×10^{-13}, respectively. In [12], the authors presented a cancelable biometric authentication system based on multimodal databases. First, cancelable templates are generated by projecting the pattern points on a random surface obtained with the help of a private user key. Then, the cartesian coordinates are transformed into cylindrical coordinates. This system achieved an EER of 0.004. In [13], the authors presented an iris image deformation technique that merges a one-way transformation with a ciphering scheme to generate cancelable iris templates. This technique revealed an accuracy of 99.9%. In addition, Soliman *et al.* in [14] generated cancelable face patterns using optimized versions of logistic map. This scheme achieved an AROC of 0.9908 and an EER of 0.01175. In [15], the same authors introduced a cancelable biometric scheme based on DRPE face traits. A convolution operation is also involved in the generation of cancelable templates. This scheme provided an EER of 0.0017 and an accuracy of 0.993.

In [16], the authors presented a coordinate transformation of pixel positions in the fingerprint traits. This algorithm achieved a moderate EER and a high accuracy level. The authors of [17] produced a cancelable fingerprint recognition system based on a fuzzy vault scheme to generate the ciphered pattern. This system achieved an EER of 0.0117. In [18], the authors presented a cancelable biometric system based on random projection for generating cancelable iris patterns. It achieved an accuracy of 0.9967 and an EER of 0.0058. In [19], the authors presented a rotational convolution scheme to generate masked versions of fingerprints. This scheme depends on a non-invertible transformation that provides high confidentiality and authentication performance. It offered good results compared with other state-of-the-art techniques. In [20], a hybrid recognition scheme was presented based on Rivest, Shamir, Adleman (RSA) asymmetric encryption combined with OSH to transfer the biological patterns to cipher hologram vectors. These vectors are encrypted by RSA encryption scheme. In [21], a deep learning algorithm was introduced to build a biometric verification system for Internet-of-Things (IoT) applications. This system provided high accuracy of recognition.

In [22], the authors presented a cancelable EEG biometric recognition algorithm based bilateral schemes. Firstly, an improved bio-hashing scheme is applied. After that, different mathematical operations are utilized to convert the genuine features to cancelable traits using an irreversible conversion. In [23], the authors exploited a two-dimensional Gabor filter to obtain the cancelable versions of palmprint templates. A two-dimensional palm hash code is used to hide the main biometric details to construct the deformed palmprint templates. In [24], an ECG cancelable biometric system was introduced for authentication purposes using different fusion levels.

There are weak points in the presented conventional biometric security schemes. These points are summarized as follows:

1. The conventional encryption schemes could not achieve the required trade-off between the verification phase sensitivity and the cancelable pattern randomization.
2. The evaluation metrics such as AROC and EER are not fair enough to assess efficiency and privacy.
3. The presented schemes have been tested only on limited-size databases.
4. The performance assessment has not been implemented on all presented schemes.
5. The noise effect has not been investigated in all cancelable biometric recognition schemes.
6. Computational time has not been considered in all cancelable biometric recognition schemes.

These limitations encouraged us to propose an efficient encryption-based cancelable biometric recognition framework that can withstand various types of attacks, such as brute-force attacks, statistical attacks, and differential attacks.

TABLE 2. Conditions of pairing rules of DNA.

Introns of DNA	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

AGG-TAG-CTC-TCC-AAG

TCC-ATC-CAG-AGG-TTC

FIGURE 2. Codons of DNA.

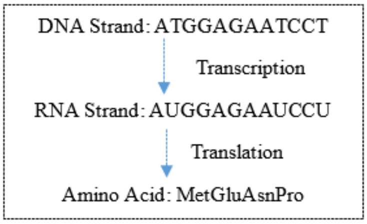


FIGURE 3. Translation operations from DNA to RNA and then to protein.

Hence, the proposed framework depends on the GA technique to choose the best cipher image from the initial population frames after generating them by the logistic map and RNA techniques. The GA-based encryption stage increases the diversity and unlinkability of patterns [31]–[34]. The GA implementation depends on three main stages: cross-over, mutation, and selection of the best initial populated cipher images. Hence, it adds more randomization to the obtained cancelable templates.

Therefore, the main contribution of the proposed framework is the integration of GA and DNA encryption in the so-called RNA-GA encryption algorithm for generating cancelable biometric templates that can be used for authentication. The utilization of the RNA codons with the GA technique for the encryption of color and gray-scale biometric images improves the histogram results and provides cancelable biometric templates with much deformation, when compared to the original biometric templates.

The main steps of the proposed encryption algorithm are summarized as follows:

Step 1: The initially populated cipher templates (chromosomes) of the GA technique are generated by employing chaos theory represented in the logistic map.

Step 2: The initial output cipher templates are then transformed to a DNA sequence, and consequently to the corresponding RNA codons using the truth-table of DNA and RNA representations.

Step 3: The secret key in its binary format is used to obtain the newly encrypted lists of RNA symbols.

Step 4: Finally, the GA technique is applied. It starts by choosing the best initial cipher templates from the initially

TABLE 3. RNA triplet codons and their corresponding amino acids.

No. of pixels	RNA code	Binary code	Amino acid	No. of pixels	RNA code	Binary code	Amino acid	No. of pixels	RNA code	Binary code	Amino acid	No. of pixels	RNA code	Binary code	Amino acid
0	AAA	000000	Lys	16	CAA	010000	Gin	32	GAA	100000	Glu	48	UAA	110000	Stop
1	AAC	000001	Asn	17	CAC	010001	His	33	GAC	100001	Asp	49	UAC	110001	Tyr
2	AAG	000010	Lys	18	CAG	010010	Gin	34	GAG	100010	Glu	50	UAG	110010	Stop
3	AAU	000011	Asn	19	CAU	010011	His	35	GAU	100011	Asp	51	UAU	110011	Tyr
4	ACA	000100	Thr	20	CCA	010100	Pro	36	GCA	100100	Ala	52	UCA	110100	Ser
5	ACC	000101	Thr	21	CCC	010101	Pro	37	GCC	100101	Ala	53	UCC	110101	Ser
6	ACG	000110	Thr	22	CCG	010110	Pro	38	GCG	100110	Ala	54	UCG	110110	Ser
7	ACU	000111	Thr	23	CCU	010111	Pro	39	GCU	100111	Ala	55	UCU	110111	Ser
8	AGA	001000	Arg	24	CGA	011000	Arg	40	GGA	101000	Gly	56	UGA	111000	Stop
9	AGC	001001	Ser	25	CGC	011001	Arg	41	GGC	101001	Gly	57	UGC	111001	Cys
10	AGG	001010	Arg	26	CGG	011010	Arg	42	GGG	101010	Gly	58	UGG	111010	Trp
11	AGU	001011	Ser	27	CGU	011011	Arg	43	GGU	101011	Gly	59	UGU	111011	Cys
12	AUA	001100	Ile	28	CUA	011100	Leu	44	GUA	101100	Val	60	UUA	111100	Leu
13	AUC	001101	Ile	29	CUC	011101	Leu	45	GUC	101101	Val	61	UUC	111101	Phe
14	AUG	001110	Start	30	CUG	011110	Leu	46	GUG	101110	Val	62	UUG	111110	Leu
15	AUU	001111	Ile	31	CUU	011111	Leu	47	GUU	101111	Val	63	UUU	111111	Phe

populated templates. Then, cross-over and mutation operations are employed to generate the final unique cancelable biometric templates.

III. BASIC CONCEPTS

This section introduces the concepts of the logistic map, the DNA sequences, and the evolutionary GA technique.

A. LOGISTIC MAP

The logistic map varies over time based on its recent state. When the current state suffers from a small change, it profoundly affects the final result. The logistic map is defined with the following equation [35]:

$$X_{n+1} = KX_n(1 - X_n) \tag{1}$$

where K ranges from 0 to 4, and the initial value of X_n ranges from 0 to 1. When $K \in [3.5, 4]$, the bifurcation is obtained [36]. When K is almost equal to 4, a high degree of randomization is achieved. Hence, in our work, we take $K = 3.99$ [35, 36].

B. BIOMOLECULAR COMPUTATIONS

Deoxyribose Nucleic Acid, abbreviated as DNA, is defined as a genetic component in human bodies. DNA encoding system consists of four chemical bases: A for Adenine, C for Cytosine, G for Guanine, and T for Thymine. A and T are considered the complements of G and C [37]. The art of encryption provided by DNA sequences is called DNA computing [38]. Table 2 introduces the cases of the binary representation of a two-bit encoding system for DNA [37].

The encryption process is implemented on biometric pixel values. For instance, if the pixel value equals 231, the encoded value in binary is [11100111]. Hence, the resultant DNA sequence is [T C G T], as indicated in Table 2. In addition, the opposite form of DNA provides the information to be replaced, independently [38]. The DNA chains and their opposites are formed of triple nucleotides called codons, as shown in Fig. 2 [38].

Another macromolecule can be extracted from the DNA nucleic acids, namely Ribonucleic acid (RNA) sequence. Two DNA chains suffer from a separation process resulting in RNA nucleotides, which are the complementary components of a single chain of DNA. For example, if the DNA strand consists of A, T, C, G nucleotides, the RNA chain consists of A, U, C, and G nucleotides. The transcription process includes the conversion operation from non-coding symbols defined as introns according to DNA sequences to encoding data defined as exons corresponding to m RNA text. Hence, we obtain exons of mRNA after a separation and splicing operation applied on introns of DNA to get one strand of RNA, which consists of data about amino-acid formation, and consequently the protein mixture [38]. The translation process includes transformation of the mRNA code into amino acids and proteins, as shown in Fig. 3 [38].

There are common codons between RNA and DNA because of the similarity between nucleotides of both of them, except T for DNA and U for RNA. These two different nucleotides are arranged in protein formation. As shown in Fig. 3, an example shows how the transcription process is implemented by replacing each T in DNA sequence by U in RNA text in both triplet codons. The RNA nucleotides can be assembled in the binary system, as shown in Table 2. According to one amino acid, every three nucleotides can generate 64 resultant codons, as illustrated in Table 3. For illustration, we assume a pixel value of 43. After converting it to a binary format, we get (101011). Then, we transform it to RNA text or codon according to Tables 2 and 3. Subsequently, we get the text (GGU) of RNA.

C. GENETIC ALGORITHM

The Genetic Algorithm (GA) is a progressive solution for encrypting plain-text images to produce a good cipher image. It depends on two general steps called cross-over and mutation [25]. The GA operation can be summarized as follows:

1. Firstly, the population of generated attempted solutions is considered.

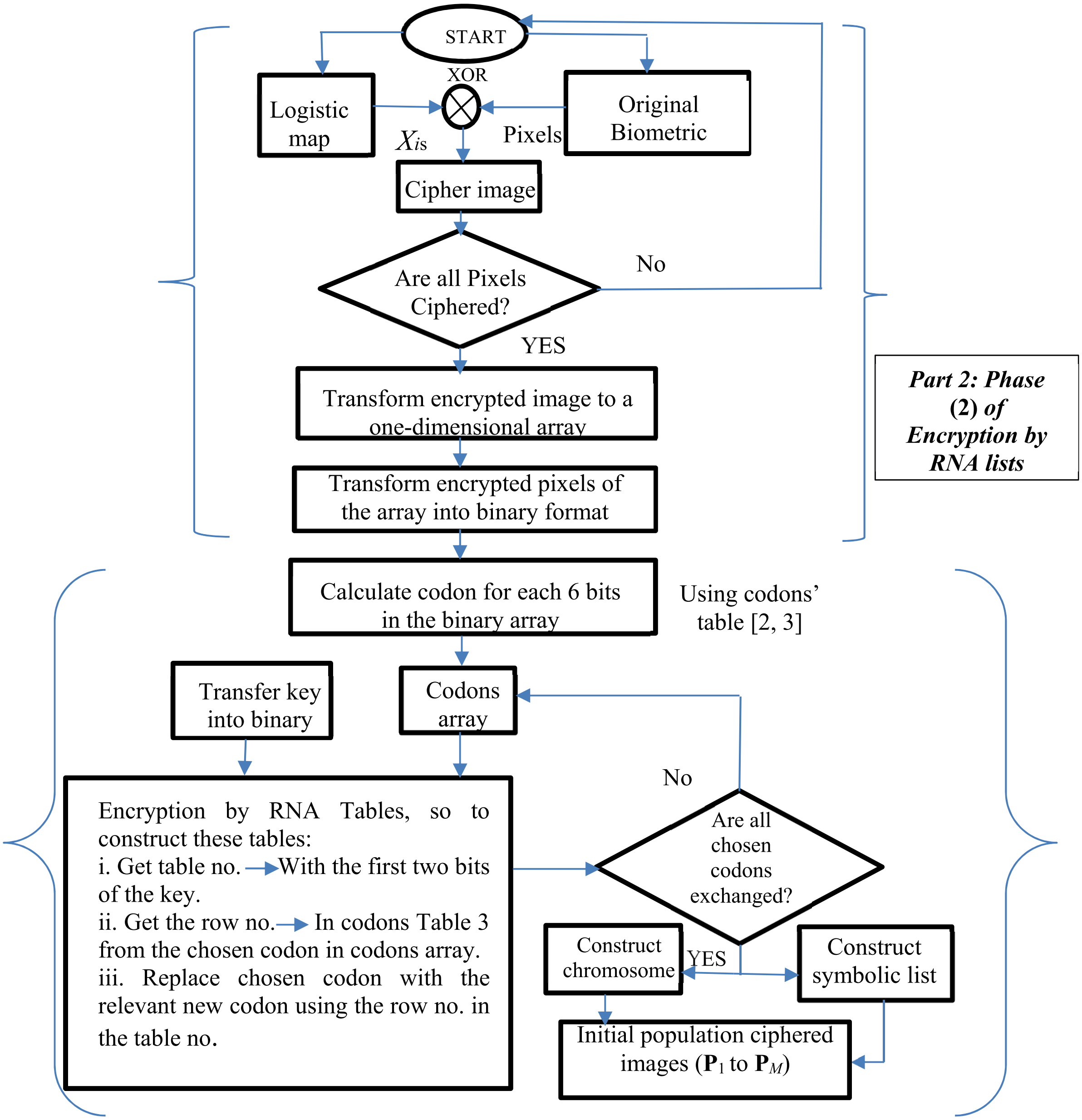


FIGURE 4. **Flowchart of the proposed encryption algorithm.**

2. Repeatedly, the subsequent procedure is performed: (a) each generated solution is evaluated, (b) the best solution is chosen, and (c) a new population is generated using the best solution.
3. The algorithm terminates, when satisfactory results are produced.
4. When applying the algorithm, new images are produced due to the recombination process of the parent strings in the cross-over step. This step provides more randomness to the cipher image.
5. The mutation operation is performed, and it is defined as a change in the pixel values of an image as the child chromosomes have to be different from their parent.

IV. PROPOSED CANCELABLE BIOMETRIC RECOGNITION SYSTEM

The main steps of the proposed encryption algorithm are offered in Fig. 4. The process begins by forming the initial population images (chromosomes) using the logistic map and bio-molecular computation as *m*RNA. Then, the GA technique is applied to these chromosomes (initial populated images) to get the final cancelable images or templates. So, we have four subsequent phase, as shown in Fig. 4. They are explained in detail as follows:

Phase 1:

1. Generation of initial population images by encrypting the original biometric traits using the logistic map with

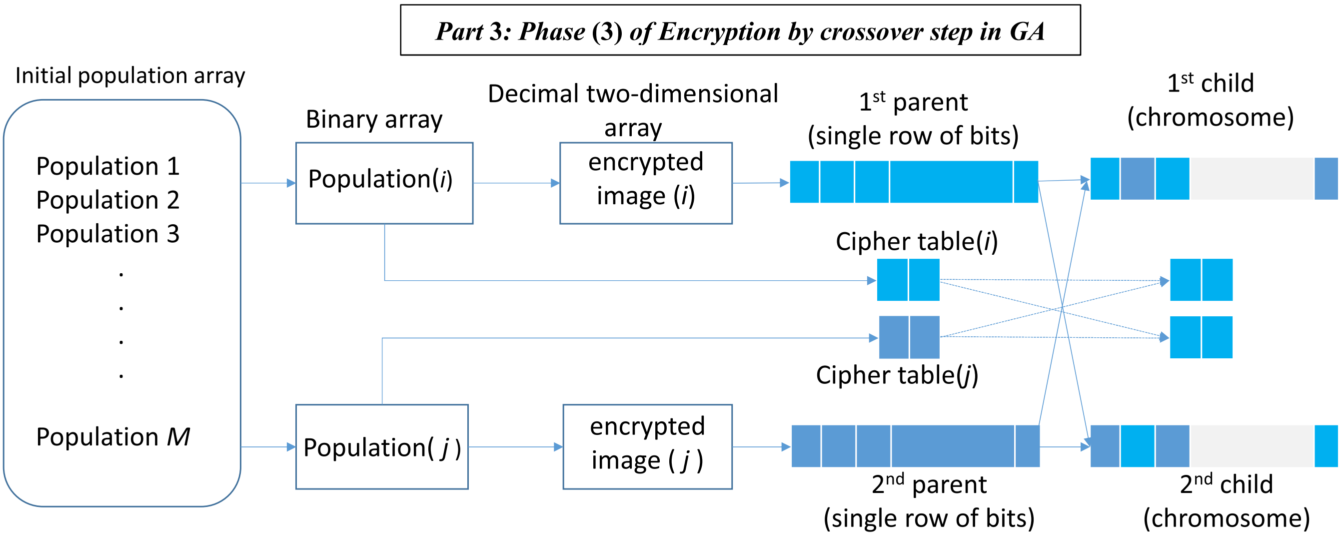


FIGURE 5. Cross-over step of the suggested biometric encryption algorithm.

FIGURE 6. Patterns of nine faces from the 1st examined database.

FIGURE 7. Patterns of nine faces from the 2nd examined database.

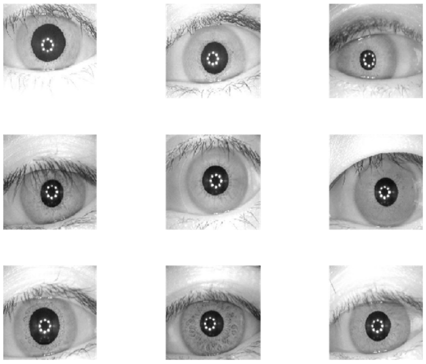


FIGURE 8. Patterns of nine irises from the 3rd examined database.

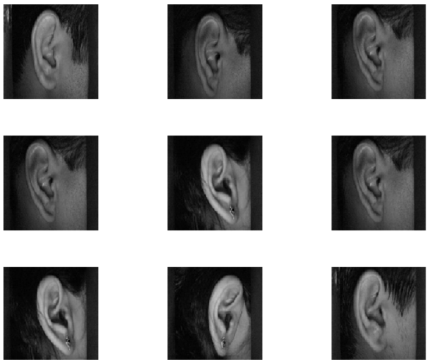


FIGURE 9. Patterns of nine ears from the 4th examined database.

Eq. (1). Assume X_0 is the initial value calculated by Eq. (2) using a 256-bit secret key that is written in an amino acid formulation, which is then converted to RNA codons, and consequently to the corresponding binary format:

$$X_0 = \frac{S^{255}_{31,0} + S^{254}_{31,1} + \ldots\ldots. + S^{127}_{16,0} + \ldots.. + S^{1}_{0,6} + S^{0}_{0,7}}{2^{256}} \tag{2}$$

To guarantee high security of biometric templates, the value of X_0 in Eq. (1) is taken from a 256-bit key as explained

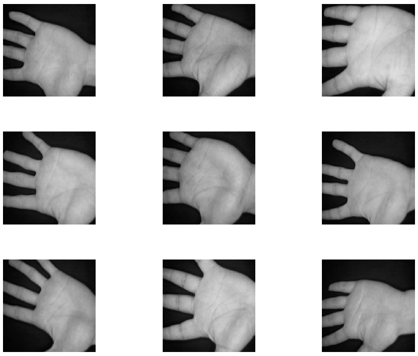


FIGURE 10. Patterns of nine palmprints from the 5th examined database.

FIGURE 11. Patterns of nine fingerprints from the 6th examined database.

Algorithm 1 Steps for Composing **L**00 and **L**01

```
Input: RNA codons truth-table.
Outlet: Ciphered RNA Lists.
$N$ ◄— (size of the initial population × size of the original biometric image).
for $r = 1$ to 64, do
    Address: chaos_ value ◄— composes $X_n + 1$ using equation.1.
    Row_ level ◄— round (chaos value × 63) +1.
    If Row_ level is repetitive, Then
        $N$ ◄— $N + 1$.
        Jump to Address.
    end if
    L[$r$] ◄— Row value.
end for
```

TABLE 4. Entropy values of the encrypted templates of the palmprint database with different encryption algorithms.

Traits	Entropy			
	Original	DRPE	OSH	Proposed RNA-GA
Palmprint 1	6.8078	7.7305	7.7527	7.9952
Palmprint 2	6.9742	7.7455	7.6742	7.9960
Palmprint 3	7.1029	7.7572	7.3867	7.9963
Palmprint 4	6.9681	7.7897	7.7849	7.9956
Palmprint 5	7.0165	7.7700	7.7190	7.9955
Palmprint 6	6.7422	7.7344	7.7478	7.9959
Palmprint 7	6.8888	7.7028	7.8152	7.9956
Palmprint 8	6.9785	7.8235	7.7179	7.9958
Palmprint 9	6.8166	7.6815	7.7887	7.9958
Average	**6.8218**	**7.7295**	**7.7612**	**7.9956**

TABLE 5. NPCR and UACI values of the encrypted templates of the palmprint database with different encryption algorithms.

Traits	DRPE		OSH		Proposed RNA-GA	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Palmprint 1	99.487	24.699	99.111	13.644	99.580	33.436
Palmprint 2	99.537	30.175	99.266	18.360	99.580	33.550
Palm print 3	99.525	30.019	99.002	15.832	99.592	33.557
Palmprint 4	99.453	25.968	98.876	13.395	99.656	33.644
Palmprint 5	99.464	25.125	98.786	16.050	99.656	33.616
Palmprint 6	99.453	24.310	98.860	16.357	99.629	33.418
Palmprint 7	99.501	27.692	98.701	15.685	99.581	33.402
Palmprint 8	99.554	27.771	99.101	18.179	99.575	33.563
Palmprint 9	99.507	24.080	98.477	10.589	99.610	33.561
Average	**99.41**	**26.41**	**98.16**	**15.54**	**99.61**	**33.45**

by Eq. (2), where $S_{m,n}$ represents the character digit, and n represents the bit digit in S_m. The secret key $= \{S_1, S_2, \ldots, S_{31}\}$ is converted to $S_m = \{S_{m,0}, S_{m,1}, \ldots.., S_{m,7}\}$. Consequently, X_0 is calculated with Eq. (1) to generate the related logistic chain. The logistic element, X_m, is transferred to the range of 0 to 255 through Eq. (3) as:

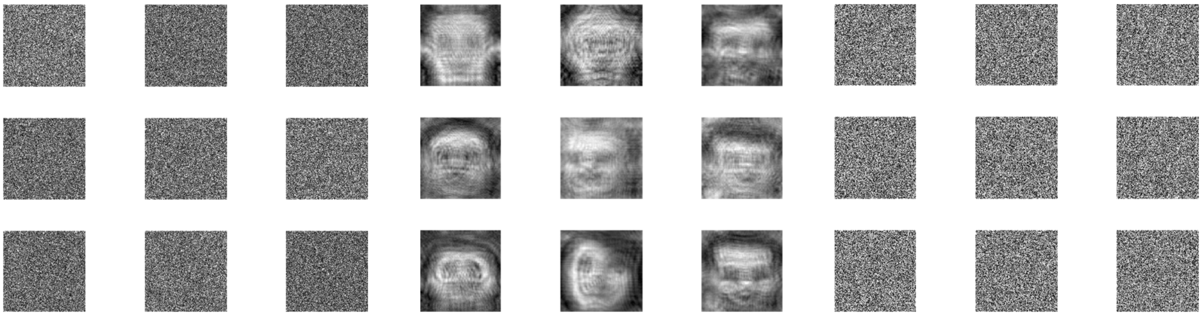
$$X(Digit) = round(x_i \times 255) \tag{3}$$

2. The chromosome image of the initial population is composed first by adding the original biometric image and X_{ms} using the XOR operation. Hence, some cipher images are generated as initial GA population. They are selected according to the degree of randomness estimated through calculating entropy and output histogram.
3. The pixels of these initial encrypted images are ordered in one-dimensional arrays. Then, these arrays are converted to their corresponding ASCII codes and binary values.

Phase 2:

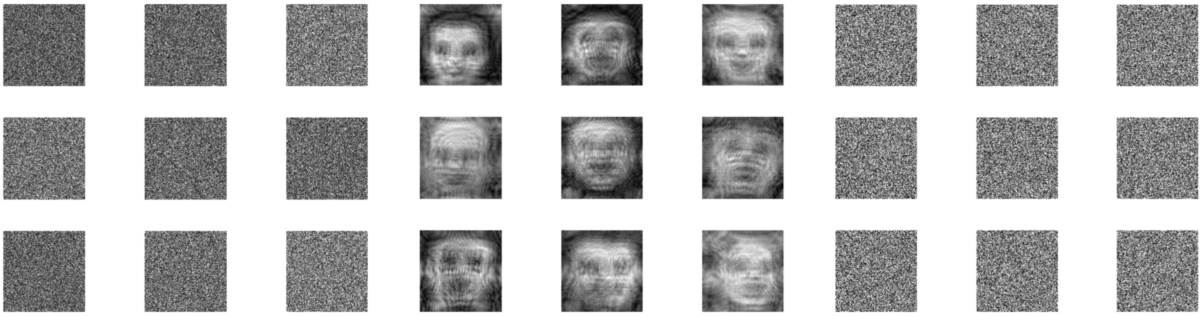
1. The binary values are transformed to their related codons using DNA sequences, and then transformed to their RNA codons using Table 3 [38].

Therefore, the preceding binary conversion is applied on the encryption key. The encryption key is chosen to determine a specified table of ciphered RNA tables using its first two bits. The ciphered lists of RNA are four lists **L** = {**L**00, **L**01, **L**10, **L**11}, which are composed of codon mixture of Table 3. **L**00 and **L**01 are directly extracted from Table 3. Due to the complementary law of RNA between its nucleotides, **L**10 is the complement of **L**01, and **L**11 is the complement of **L**00. Each RNA list has 16 rows. Algorithm 1 illustrates how **L**00 and **L**01 are constructed.



(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 12. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 1st examined biometric database.



(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 13. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 2nd examined biometric database.

TABLE 6. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 1st examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Face 1	0.9246	0.9009	0.9485	0.0019	-0.0033	-0.0035
Face 2	0.9120	0.8913	0.9492	0.0040	-0.0061	0.0026
Face 3	0.9093	0.8538	0.9497	-0.0009	-0.0026	-0.0009
Face 4	0.9128	0.8543	0.9491	0.0018	-0.0031	0.002710
Face 5	0.9200	0.8419	0.9480	-0.0009	-0.0087	-0.0006
Face 6	0.9225	0.8465	0.9490	0.0005	-0.0037	0.0043
Face 7	0.9113	0.8858	0.9481	-0.0003	-0.0026	0.0013
Face 8	0.9182	0.9082	0.9486	-0.0040	-0.0072	0.0001
Face 9	0.9073	0.8685	0.9483	0.0015	-0.0032	-0.0042
Average	**0.9153**	**0.8724**	**0.9487**	**0.0004**	**-0.0045**	**0.0002**

Moreover, the new codon of the initial population image is formed from the corresponding two bits of the encryption key and the chosen codon from the codons array. The chosen codon is utilized to get the related row level in the specified list number, which is dedicated by the first two bits of the encryption key. This row level is utilized to get the new codon in Table 3.

2. The new codon is later exchanged with the chosen codon. We must satisfy that all codons in the codon array are replaced with the related new codons, generating the new off-springs. Each constructed off-spring has a table that consists of a single row and two columns. This is the symbolic table. It is a one-dimensional array with two different pointers containing similar values (key1).
3. Afterwards, the transformation to binary representation from RNA sequences is implemented using Table 3 [38]. Finally, the conversion of the initialized cipher images (chromosomes) from the binary system to the decimal system is carried out to recombine the deformed pixels of each image.

Phase 3:

1. The randomness of each initial population of the generated images is calculated using a fitness function

TABLE 7. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 2nd examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Face 1	0.8983	0.9081	0.9484	0.0008	-0.0073	-0.0008
Face 2	0.9064	0.8893	0.9481	0.0012	-0.00218	0.0043
Face 3	0.9250	0.8832	0.9484	0.0064	-0.0040	-0.00567
Face 4	0.9212	0.8526	0.9489	0.0078	-0.0030	0.00005
Face 5	0.9106	0.8926	0.9490	0.0023	-0.0002	-0.00157
Face 6	0.9083	0.8375	0.9484	0.0017	-0.0011	0.0008
Face 7	0.9038	0.8720	0.9487	0.0006	0.0009	-0.0045
Face 8	0.9163	0.8894	0.9486	0.0001	0.0060	0.0047
Face 9	0.9282	0.8499	0.9486	0.0033	0.0028	0.0027
Average	**0.9131**	**0.8747**	**0.9486**	**0.0027**	**-0.0009**	**0.00001**

TABLE 8. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 3th examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Iris 1	0.9464	0.8701	0.9481	-0.0039	0.0023	-0.0038
Iris 2	0.9449	0.8150	0.9488	0.0067	-0.0012	-0.0082
Iris 3	0.9405	0.8207	0.9489	0.0014	0.0023	0.0003
Iris 4	0.9397	0.8706	0.9487	0.0007	-0.0027	0.0002
Iris 5	0.9421	0.8144	0.9485	0.0016	0.0011	0.0001
Iris 6	0.9408	0.8527	0.9486	0.0001	-0.0036	-0.0093
Iris 7	0.9431	0.8667	0.9494	0.0101	-0.0010	-0.0005
Iris 8	0.9378	0.8648	0.9494	0.0062	-0.0010	0.0030
Iris 9	0.9452	0.8705	0.9488	0.0034	-0.0001	0.0050
Average	**0.9429**	**0.8495**	**0.9488**	**0.0029**	**-0.0004**	**-0.0014**

TABLE 9. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 4th examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Ear 1	0.8115	0.8875	0.9484	0.004	-0.0066	-0.0031
Ear 2	0.7389	0.9125	0.9491	-0.0014	-0.0054	-0.0010
Ear 3	0.7769	0.9127	0.9482	-0.0042	-0.0032	-0.0013
Ear 4	0.7776	0.9126	0.9482	0.0002	-0.0032	-0.0013
Ear 5	0.8087	0.9183	0.9486	0.0020	-0.0041	0.0049
Ear 6	0.7786	0.9132	0.9483	-0.0029	-0.0032	-0.0013
Ear 7	0.8133	0.9184	0.9489	-0.0005	-0.0041	0.0049
Ear 8	0.8139	0.9150	0.9483	0.0036	-0.0036	0.0035
Ear 9	0.8287	0.8895	0.9482	0.0021	-0.0049	-0.0002
Average	**0.7942**	**0.9089**	**0.9485**	**0.0003**	**-0.0043**	**0.0005**

comprising entropy. Finally, the Roulette wheel algorithm is applied to choose the best initial populated image.

2. In the cross-over step, a symbol list is reconstructed (key2) to dedicate the swapping point position for each couple of parent images with an incremented value calculated by key2 (both parent images are chosen as they are the highest-entropy images from the initial population) as shown in Fig. 5.
3. During the last step in generating the chromosomes with GA, each symbolic cipher list (key1) is considered a parent of the mentioned off-spring swapping key (key2).
4. Each cipher image is considered a parent transferred to a binary array with one dimension, as shown in Fig. 5. The binary arrays suffer from swapping by a uniform cross-over rate of 0.7 [25]. Moreover, the symbolic table (keys) of off-springs must be reconstructed for each turn in the GA technique. Therefore, the value of the first index in the resultant off-spring is the same value corresponding to the first index of the *first* parent, and the value of the second index of the *same* off-spring

TABLE 10. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 5th examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Palmprint 1	0.9104	0.9394	0.9487	-0.0046	-0.0006	-0.0036
Palmprint 2	0.9123	0.9197	0.9481	-0.0021	-0.0021	-0.0058
Palmprint 3	0.9381	0.8928	0.9484	0.0004	0.0004	0.0055
Palmprint 4	0.9194	0.9360	0.9487	-0.0023	0.0017	0.0032
Palmprint 5	0.9149	0.9322	0.9486	-0.0053	-0.0020	0.0022
Palmprint 6	0.909156	0.9387	0.9491	-0.0039	0.0006	0.0009
Palmprint 7	0.9056	0.9364	0.9480	-0.0028	-0.0037	0.002323
Palmprint 8	0.9318	0.9307	0.9484	-0.0031	0.0036	-0.0001
Palmprint 9	0.9021	0.9483	0.9477	0.0072	-0.0003	0.0037
Average	**0.9160**	**0.9305**	**0.9485**	**-0.0018**	-0.0002	**0.0009**

TABLE 11. Correlation scores of the proposed cancelable biometric recognition system and the systems based on DRPE and OSH for the 6th examined database in the presence of noise with variance = 0.01 (non-ideal environment).

Traits	Geniune test			Imposter test		
	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm	System based on the DRPE algorithm	System based on the OSH algorithm	System based on the proposed RNA-GA algorithm
Fingerprint 1	0.9476	0.7463	0.9486	0.0025	0.0027	-0.0022
Fingerprint 2	0.9482	0.7022	0.9483	-0.0002	0.0023	-0.0061
Fingerprint 3	0.9466	0.8639	0.9490	0.0027	0.0075	0.0042
Fingerprint 4	0.9474	0.8131	0.9485	0.0020	0.0049	0.0003
Fingerprint 5	0.9477	0.7031	0.9485	0.0055	0.0065	0.0053
Fingerprint 6	0.9473	0.7947	0.9487	0.0027	0.0089	0.0055
Fingerprint 7	0.9480	0.7124	0.9487	0.0002	0.0042	-0.0050
Fingerprint 8	0.9468	0.7616	0.9495	-0.0054	-0.0004	-0.0015
Fingerprint 9	0.9484	0.6707	0.9488	0.0005	0.003836	-0.0047
Average	**0.9476**	**0.7520**	**0.9487**	**0.0012**	**0.0045**	**-0.0004**

TABLE 12. Approximate template encryption time in (seconds) for the six examined biometric databases.

Biometric database	Processing time		
	DRPE	OSH	Proposed RNA-GA
Face database 1	1.0698	0.5038	0.9213
Face database 2	1.0128	0.40508	0.7914
Iris database	1.1457	0.31115	0.8028
Ear database	0.98411	0.3646	0.8897
Palmprint database	0.93629	0.3279	0.5928
Fingerprint database	1.01647	0.31438	0.7369

is the value pointed by the *second* index according to the *second* parent as shown in Fig. 5.

5. Finally, in the mutation step, almost 5% of pixel values of the entire population (with distinguished modification in intensity) are exchanged with the new cancelable encrypted templates constructed by step1 in every GA turn.

V. EXPERIMENTAL RESULTS AND COMPARISONS

In this section, different simulation experiments are performed to verify the validity of the proposed cancelable biometric system. We work on various biometric databases that have specifications, such as high and low brightness, white and black backgrounds, and animated objects [39]–[44]. Two different types of face databases are considered [39], [40]. One sample for each biometric database is examined, involving ear [41], palmprint [42], fingerprint [43], and iris [44]. For simplicity, only nine biometric templates of each examined database are presented in the experimental results, as shown in Figs. 6-11.

TABLE 13. AROC and FAR values of the cancelable biometric recognition systems on the 1st examined biometric database in the presence of noise with different levels.

Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9953	0.0102	0.9888	0.0204	0.9998	0.0008
0.01	0.9922	0.0158	0.9859	0.0482	0.9993	0.0009
0.02	0.9729	0.0547	0.9481	0.1298	0.9967	0.0048
0.03	0.9672	0.0622	0.8664	0.2794	0.9824	0.0199
0.04	0.9372	0.0989	0.8353	0.3147	0.9682	0.0349
0.05	0.7592	0.3323	0.8024	0.3499	0.9639	0.0390

TABLE 14. AROC and FAR values of the cancelable biometric recognition systems on the 2nd examined biometric database in the presence of noise with different levels.

Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9987	0.0025	0.9974	0.0103	0.9996	0.0005
0.01	0.9972	0.0071	0.9926	0.0237	0.9990	0.0011
0.02	0.9903	0.0244	0.9513	0.1255	0.9972	0.0031
0.03	0.9660	0.0630	0.8551	0.3037	0.9958	0.0047
0.04	0.9242	0.1501	0.8848	0.2307	0.9790	0.0230
0.05	0.8417	0.2529	0.7460	0.4430	0.9441	0.0609

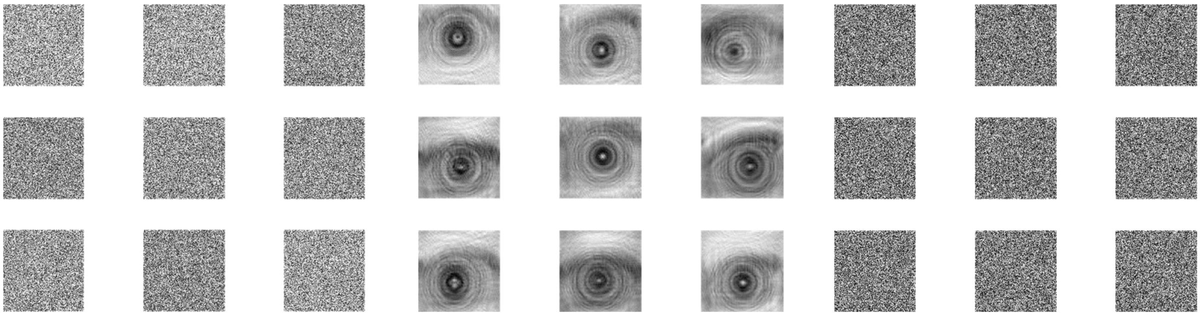

(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 14. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 3rd examined biometric database.

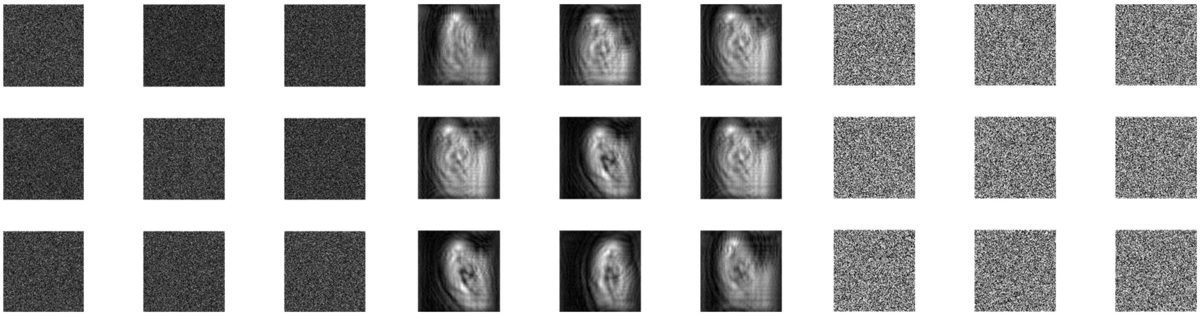

(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 15. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 4th examined biometric database.

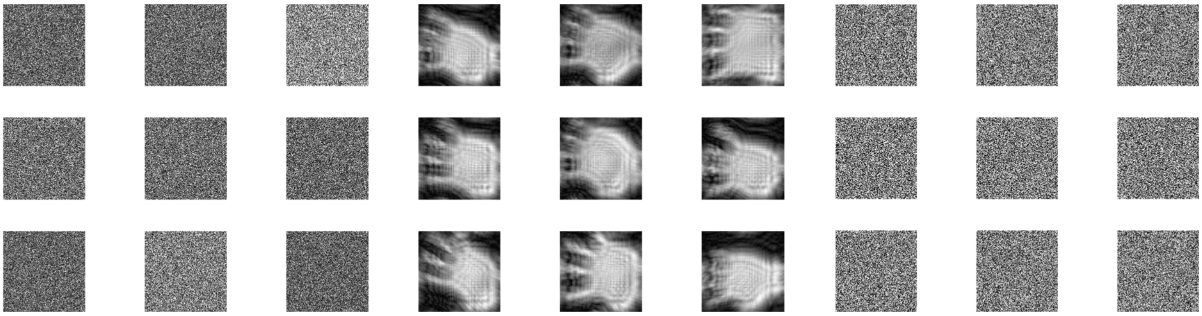

(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 16. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 5th examined biometric database.

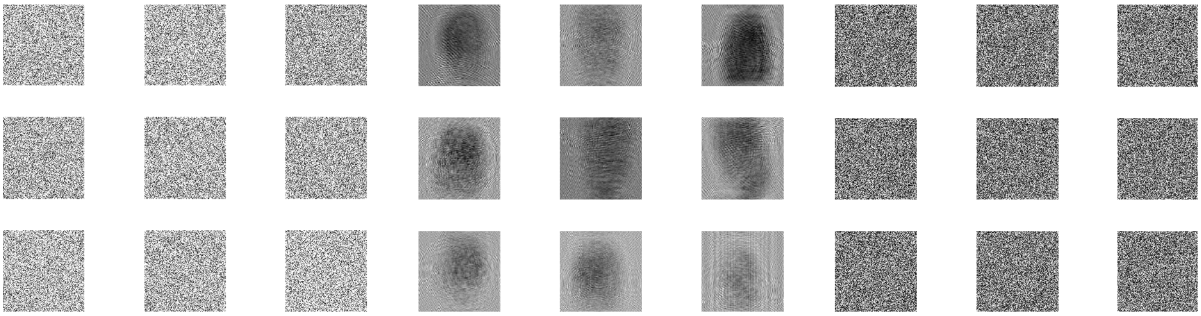
TABLE 15. AROC and FAR values of the cancelable biometric recognition systems on the 3rd examined biometric database in the presence of noise with different levels.

Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9862	0.0004	0.9961	0.0125	0.9993	0.0016
0.01	0.9990	0.0012	0.9857	0.0376	0.9980	0.0025
0.02	0.9929	0.0114	0.8264	0.2371	0.9981	0.0022
0.03	0.9870	0.0219	0.8700	0.2320	0.9914	0.0096
0.04	0.8984	0.1376	0.7808	0.3288	0.9642	0.0390
0.05	0.9517	0.0707	0.8141	0.2928	0.9641	0.0390

TABLE 16. AROC and FAR values of the cancelable biometric recognition systems on the 4th examined biometric database in the presence of noise with different levels.

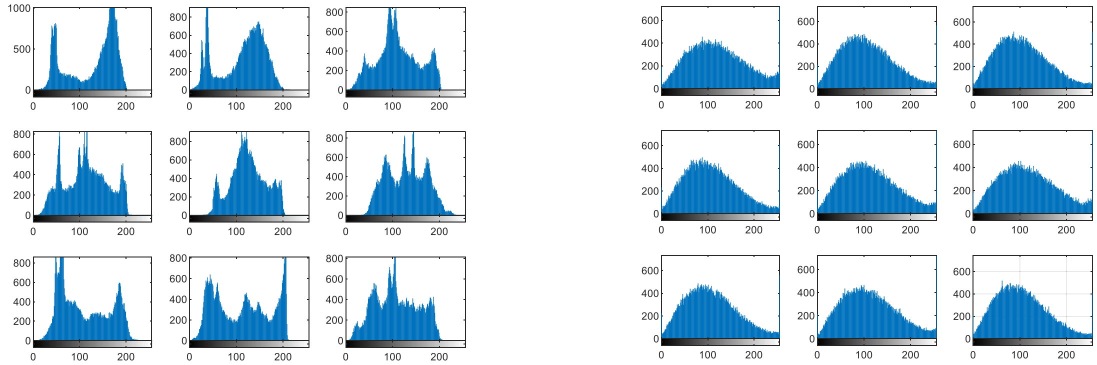
Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9644	0.0691	0.9916	0.8669	0.9906	0.8594
0.01	0.9379	0.1394	0.9967	0.0059	0.9990	0.0011
0.02	0.8993	0.1976	0.9731	0.0515	0.9725	0.0322
0.03	0.7255	0.4398	0.8853	0.1460	0.9886	0.0128
0.04	0.3077	0.8667	0.7975	0.3435	0.9636	0.0397
0.05	0.3340	0.8448	0.7798	0.3446	0.9488	0.0553

The used biometric traits are ciphered by the proposed hybrid RNA-GA encryption algorithm and compared to the results of the DRPE and OSH encryption algorithms. In addition, some security evaluations in terms of NPCR, UACI, and entropy metrics are presented for the proposed hybrid encryption framework. The simulation outcomes of only one sample of the examined biometric databases are introduced to validate the suggested hybrid encryption-based cancelable biometric system. Different performance metrics are evaluated to validate the proposed RNA-GA-based cancelable biometric system. Both visual inspection, processing time,

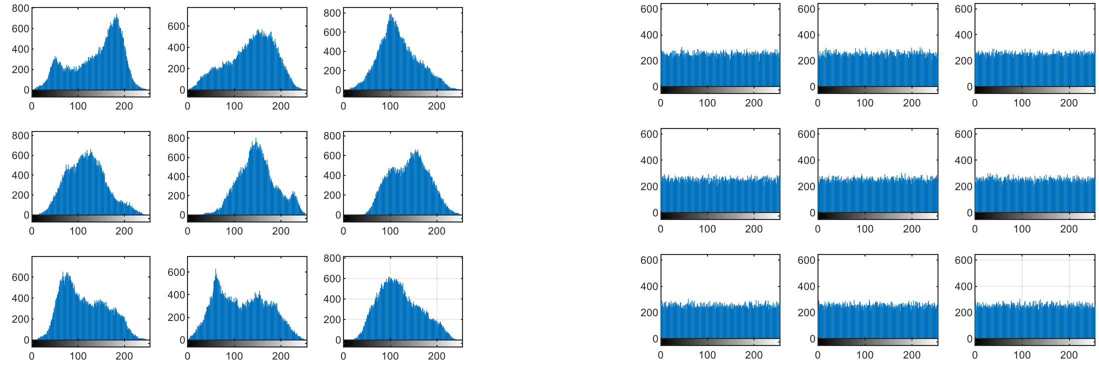


(a) DRPE. (b) OSH. (c) Proposed RNA-GA.

FIGURE 17. Resultant cancelable templates with the proposed RNA-GA, DRPE and OSH algorithms for the 6th examined biometric database.



(a) Original traits. (b) DRPE.



(c) OSH (d) Proposed RNA-GA.

FIGURE 18. Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 1st examined biometric database.

TABLE 17. AROC and FAR values of the cancelable biometric recognition systems on the 5th examined biometric database in the presence of noise with different levels.

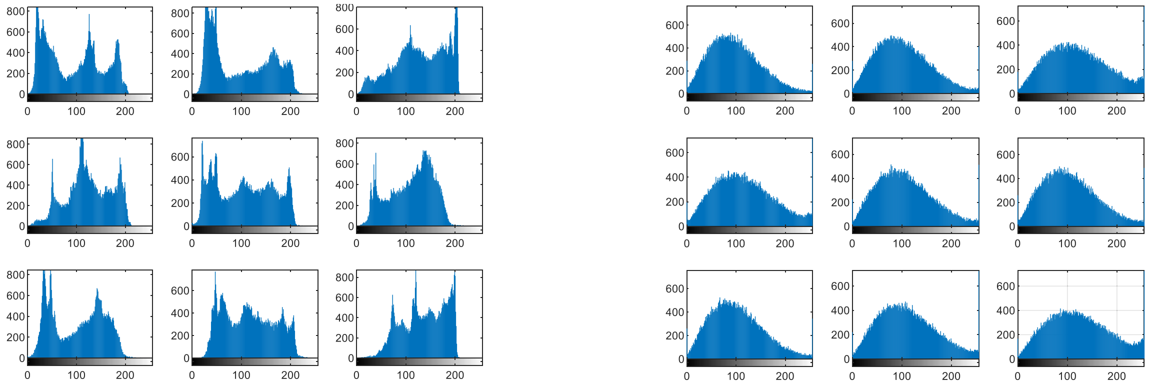
Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9803	0.0078	0.9602	0.0655	0.9930	0.0024
0.01	0.9979	0.0047	0.9983	0.0052	0.9986	0.0015
0.02	0.9826	0.0427	0.9877	0.0476	0.9978	0.0014
0.03	0.9345	0.1139	0.9566	0.15403	0.9903	0.0107
0.04	0.9507	0.07705	0.9562	0.1494	0.9716	0.0311
0.05	0.9221	0.1321	0.9581	0.1327	0.9269	0.1197

TABLE 18. AROC and FAR values of the cancelable biometric recognition systems on the 6th examined biometric database in the presence of noise with different levels.

Noise Variance	DRPE		OSH		Proposed (RNA-GA)	
	AROC	FAR	AROC	FAR	AROC	FAR
0.0	0.9976	0.00116	0.96124	0.11037	0.9988	0.00268
0.01	0.9989	0.00124	0.93842	0.16562	0.99909	0.00107
0.02	0.9869	0.01502	0.83056	0.3365	0.9964	0.00409
0.03	0.9792	0.02304	0.57507	0.7057	0.9897	0.01147
0.04	0.9838	0.01960	0.5564	0.68332	0.97615	0.02601
0.05	0.9592	0.04506	0.39875	0.851196	0.97381	0.02824

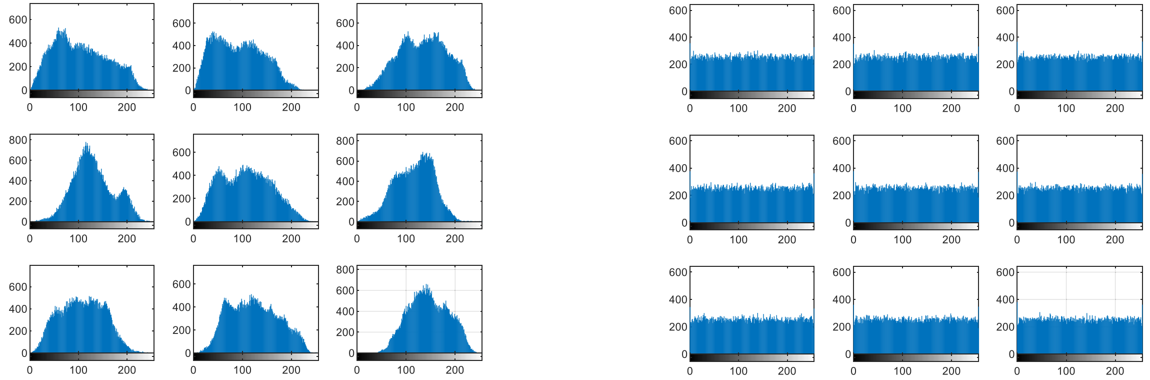
PFD, PTD, FAR, FRR, EER, AROC, correlation coefficients, and histogram analysis are considered.

To simplify the presentation of the simulation outcomes, the resultant values for only nine ciphered biometric templates of each of the six examined biometric databases are introduced. Finally, the improvement of the proposed cancelable biometric security system based on the hybrid RNA-GA symmetric encryption algorithm is discussed versus other



(a) Original traits.

(b) DRPE.



(c) OSH.

(d) Proposed RNA-GA.

FIGURE 19. **Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 2nd examined biometric database.**

TABLE 19. **Average AROC and FAR values of the proposed cancelable biometric recognition system and the state-of-the-art systems.**

System	AROC	FAR
Proposed	0.9990	0.0011
[25]	0.9943	0.02180
[26]	0.8271	0.0781
[27]	0.9414	0.0315
[28]	0.8812	0.0865
[29]	0.9822	0.0067
[30]	0.9591	0.0307
[48]	0.9236	0.0296
[49]	0.8920	0.0946
[50]	0.9416	0.0527
[51]	0.8967	0.0071
[52]	0.9673	0.0263

related studies that depend on the DRPE and OSH symmetric encryption algorithms [20], [32], [36], [45].

In the following sub-sections, the simulation outcomes of different authentication evaluation metrics are obtained to measure the efficiency of the proposed biometric security system. The security analysis for the proposed system is presented in terms of different eight categories, (a) Visual inspection, (b) PTD and PFD, (c) Correlation score, (d) Histogram analysis, (e) FAR, and AROC analysis, (f) Speed analysis (g) Noise interruption, and (h) Comparative analysis.

All experimentation results are obtained using MATLAB software on 256 × 256 gray-scale biometric images.

A. SECURITY ANALYSIS OF RNA-GA ENCRYPTION-BASED CANCELABLE BIOMETRIC SYSTEM

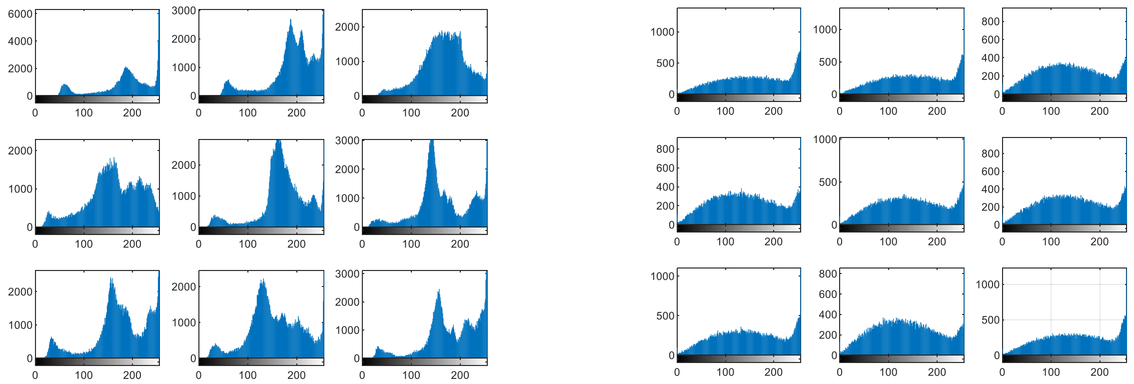
1) ENTROPY ANALYSIS

The degree of randomness of encrypted templates is estimated with entropy. The smallest entropy value is zero, while the optimum value is 8. Thus, the higher the entropy, the more uniform the image distribution is. Therefore, an efficient cryptosystem must offer an information entropy up or close to 8 [46].

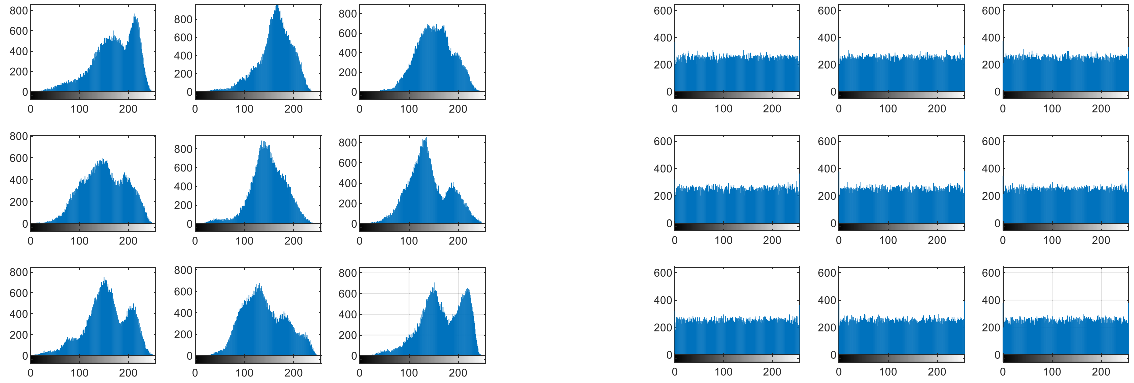
Table 4 gives a comparison of entropy values of the encrypted biometric images generated with the proposed encryption algorithm and those obtained with DRPE and OSH. It is noticed that the entropy values of the cancelable palmprint templates encrypted with the proposed algorithm are close to 8 (the optimum value). This proves the high randomness of cancelable templates obtained with the proposed encryption algorithm.

2) NPCR AND UACI ANALYSIS

Two other security metrics, namely NPCR and UACI [47], are employed to prove the effect of one-bit modification in the plain image on the encrypted one. Table 5 illustrates the NPCR and UACI values, which are both near the



(a) Original traits. (b) DRPE.



(c) OSH. (d) Proposed RNA-GA.

FIGURE 20. **Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 3rd examined biometric database.**

optimum values. We reach an average value of 99.6564% for NPCR, and 33.5535% for UACI. This proves that the cancelable biometric security system has high sensitivity to any modifications in the original traits, even if these modifications are so slight. This assures that the proposed RNA-GA algorithm has the ability to resist differential attacks.

B. ASSESSMENT OF THE CANCELABLE BIOMETRIC RECOGNITION SYSTEM

1) VISUAL INSPECTION

Figures 12-17 illustrate the ciphered templates of the examined biometric database samples with the proposed, DRPE and OSH algorithms [20], [32], [36], [45]. For the six used databases, it is noticed that the proposed algorithm is superior to both DRPE and OSH algorithms [20], [32], [36], [45]. Hence, the proposed encryption algorithm can be used to achieve high immunity to intrusion attempts.

2) HISTOGRAM ANALYSIS

The histogram reflects the distribution of pixel levels in the image. It should be as uniform as possible for high quality of encryption. Histograms of encrypted images with the proposed as well as traditional encryption algorithms are shown in Figs. 18-23. It is observed that the templates obtained with the proposed encryption algorithm have more uniform histograms.

3) CORRELATION ANALYSIS

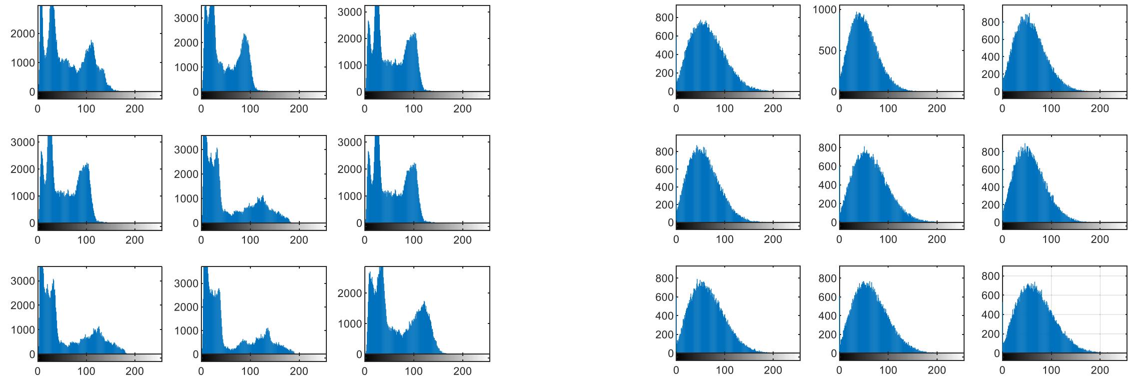
The correlation coefficient (C_c) is estimated between original and encrypted templates. We have two cases for C_c:

1. The value of C_c is close or equal to zero. This case ensures high quality of encryption.
2. The value of C_c is close or equal to ±1. This case reveals poor quality of encryption.

Moreover, the correlation coefficient value is important for genuine and imposter tests between encrypted templates. Low correlation values are required in imposter tests, while high correlation values are required in genuine tests. Tables 6 to 11 introduce the correlation scores obtained for genuine and imposter tests in the cancelable biometric systems that depend on the proposed as well as traditional encryption algorithms. The obtained results ensure higher correlation scores with the proposed encryption algorithm in genuine tests and lower scores in imposter tests compared to other algorithms.

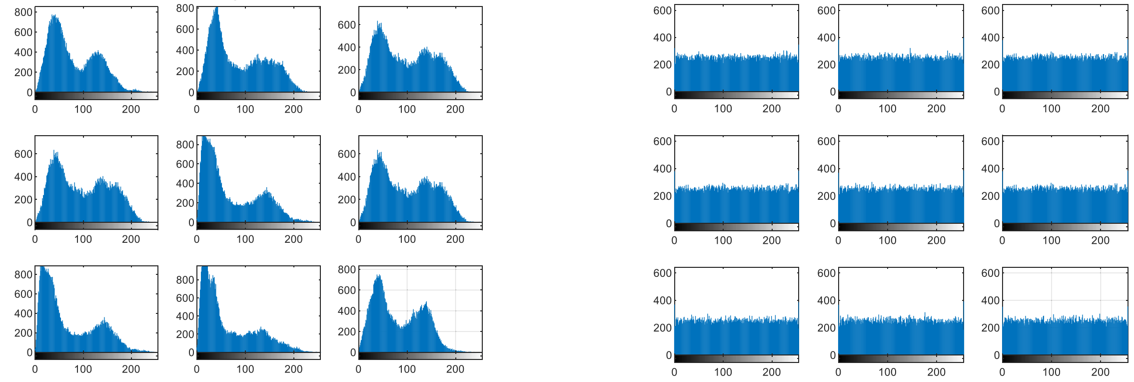
4) CORRELATION DISTRIBUTIONS

The PTD and PFD are the probability distributions of the correlation coefficient for genuine and imposter tests, respectively. Figures 24 to 29 show these distributions in the cancelable biometric systems based on the proposed, DRPE and OSH algorithms on all tested biometric databases.



(a) Original traits.

(b) DRPE.



(c) OSH.

(d) Proposed RNA-GA.

FIGURE 21. Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 4th examined biometric database.

TABLE 20. Correlation scores of the proposed cancelable biometric recognition systems based on the proposed RNA-GA algorithm and the GA algorithm for the 1st examined database.

Traits	Genuine test		Imposter test	
	System based on GA algorithm [25]	System based on the proposed RNA-GA algorithm	GA scheme [25]	System based on GA algorithm [25]
Face 1	0.9037	0.9485	0.0034	-0.0035
Face 2	0.8952	0.9492	0.0013	0.0026
Face 3	0.8827	0.9497	-0.0019	-0.0009
Face 4	0.8881	0.9491	-0.0044	0.0027
Face 5	0.8293	0.9480	-0.0018	-0.0006
Face 6	0.8533	0.9490	-0.0058	0.0043
Face 7	0.9110	0.9481	-0.0014	0.0013
Face 8	0.9234	0.9486	0.0011	0.0001
Face 9	0.8918	0.9483	-0.0029	-0.0042
Average	**0.8865**	**0.9487**	**-0.0013**	**0.0002**

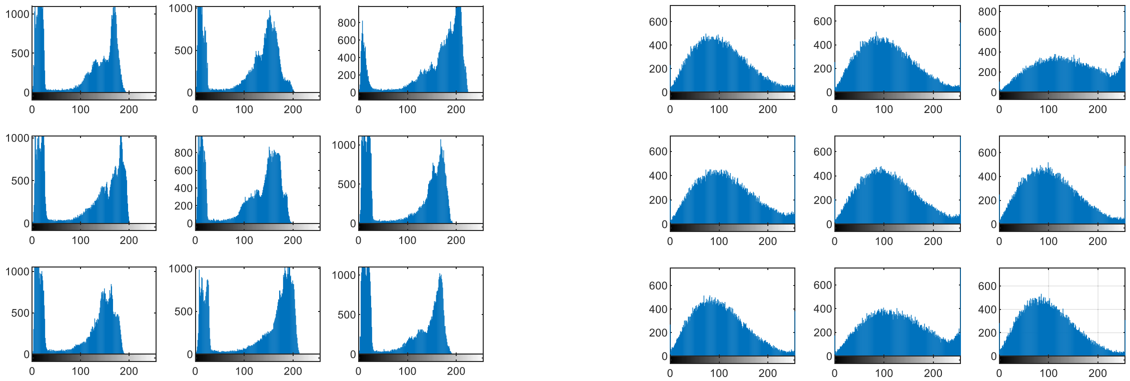
These obtained curves illustrate that the two distributions are farther with the proposed encryption algorithm, which reflects the high ability of the proposed cancelable biometric framework to distinguish between genuine and imposter users on all databases.

5) ROC CURVE ANALYSIS

The ROC curve is adopted for performance assessment of biometric systems. In addition, the AROC is an indicator of the accuracy level of the biometric recognition system. Figures. 24-29 give the ROC curves for the cancelable biometric recognition systems based on the proposed, DRPE, and OSH algorithms. The results reveal higher AROC values with the proposed encryption algorithm. Hence, the cancelable biometric system based on the proposed encryption algorithm is superior to the other systems.

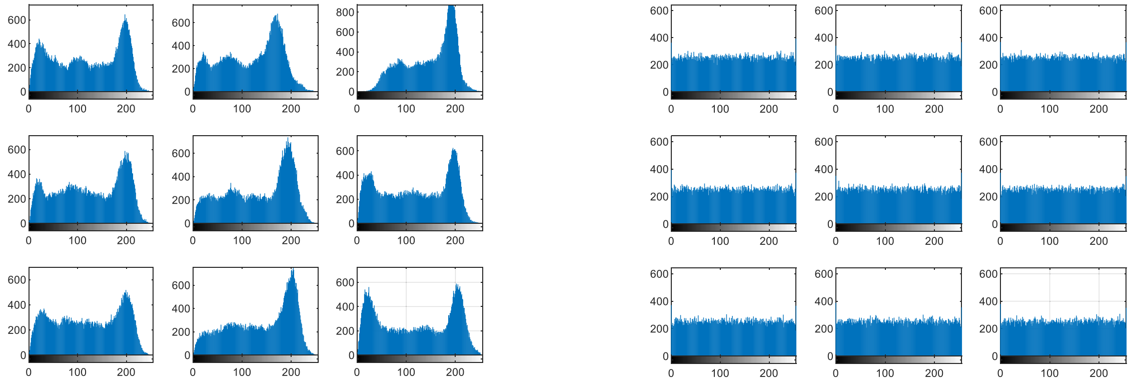
6) COMPUTATIONAL TIME

The computational times for all algorithms, implemented with MATLAB R2019b software on a platform of Windows 8



(a) Original traits.

(b DRPE.



(c) OSH.

(d) Proposed RNA-GA.

FIGURE 22. Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 5th examined biometric database.

TABLE 21. Correlation scores of the proposed cancelable biometric recognition systems based on the proposed RNA-GA algorithm and the GA algorithm for the 6th examined database.

Traits	Genuine test		Imposter test	
	System based on GA algorithm [25]	System based on the proposed RNA-GA algorithm	System based on GA algorithm [25]	System based on the proposed RNA-GA algorithm
Fingerprint 1	0.9855	0.9486	-0.0039	-0.0022
Fingerprint 2	0.9837	0.9483	-0.0012	-0.0061
Fingerprint 3	0.9808	0.9490	-0.0039	0.0042
Fingerprint 4	0.9815	0.9485	-0.0032	0.0003
Fingerprint 5	0.9821	0.9485	-0.0021	0.0053
Fingerprint 6	0.9753	0.9487	-0.0038	0.0055
Fingerprint 7	0.9837	0.9487	-0.0013	-0.0050
Fingerprint 8	0.9804	0.9495	-0.0016	-0.0015
Fingerprint 9	0.9879	0.9488	-0.0033	-0.0047
Average	**0.9823**	**0.9487**	**-0.0027**	**-0.0004**

with Intel (R) CPU @ 1.80 GHz/2.40 GHz core (TM) i5-4300 and 4 GB RAM, are estimated for the comparison purpose.

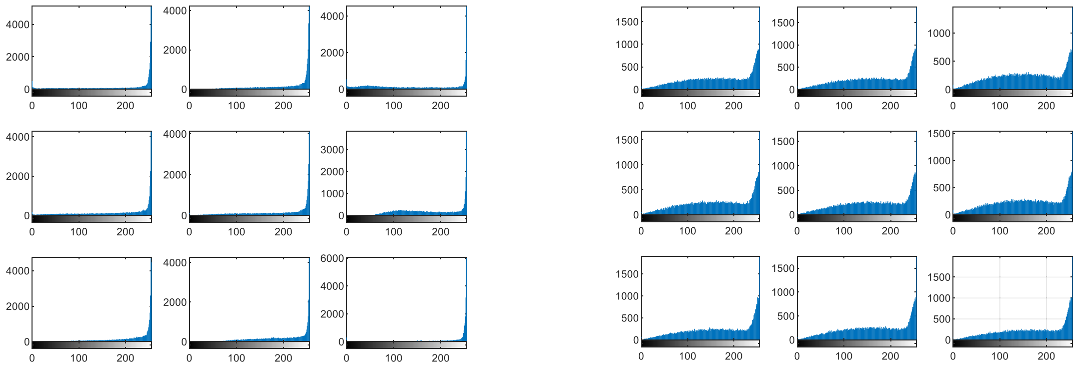
Table 12 illustrates the average processing times for all encryption algorithms. It is clear that the proposed encryption algorithm records the least computational times.

7) NOISE ANALYSIS

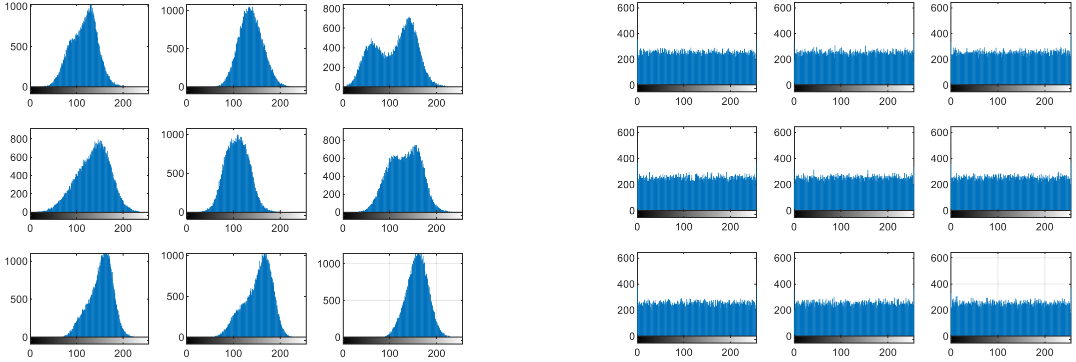
The effect of noise is investigated for the cancelable biometric recognition systems based on different encryption algorithms. Tables 13 to 18 illustrate the obtained values of FAR and AROC metrics in the presence of noise with different levels. It is demonstrated that the proposed cancelable biometric system has a robust performance in the presence of noise, which is reflected in the more convenient FAR and AROC values compared to the results of the conventional algorithms.

8) COMPARISON WITH RECENT STUDIES

The proposed cancelable biometric system has been compared with the related studies in [25]–[30], [48]–[52]. Both AROC and FAR have been considered in this comparison. Table 19 gives the results or this comparison revealing higher

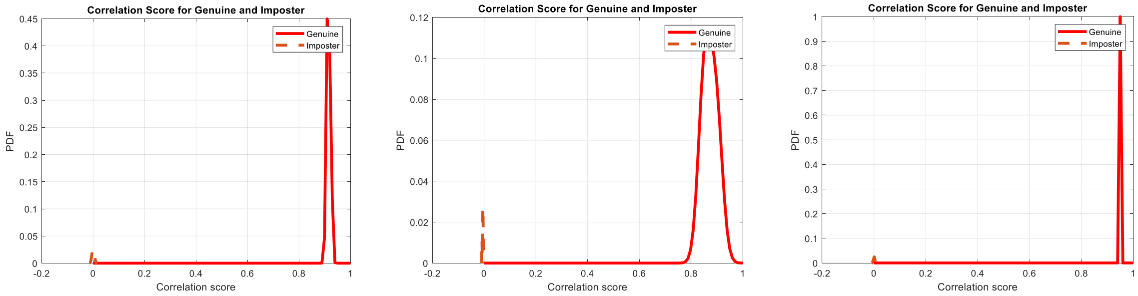


(a) Original traits.   (b) DRPE.

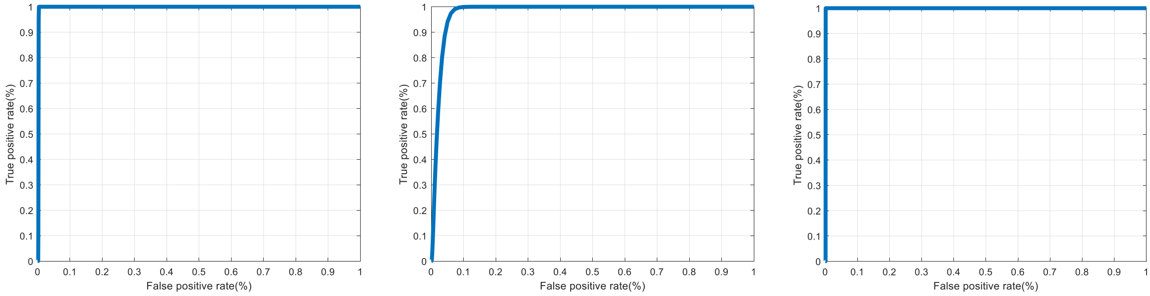


(c) OSH.   (d) Proposed RNA-GA.

FIGURE 23. **Histograms of original and cancelable templates generated with the proposed RNA-GA, DRPE and OSH algorithms for the 6th examined biometric database.**



(a) TD and FD with DRPE.   (b) TD and FD with OSH.   (c) TD and FD with RNA-GA.

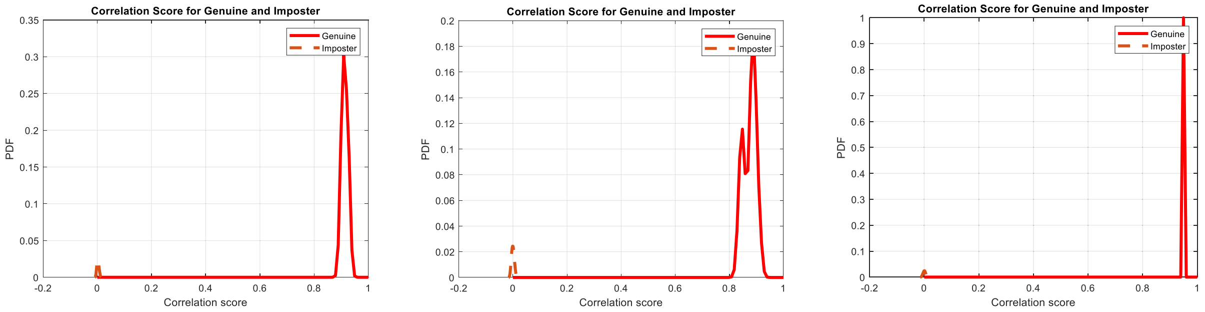


(d) ROC with DRPE.   (e) ROC with OSH.   (f) ROC with RNA-GA.

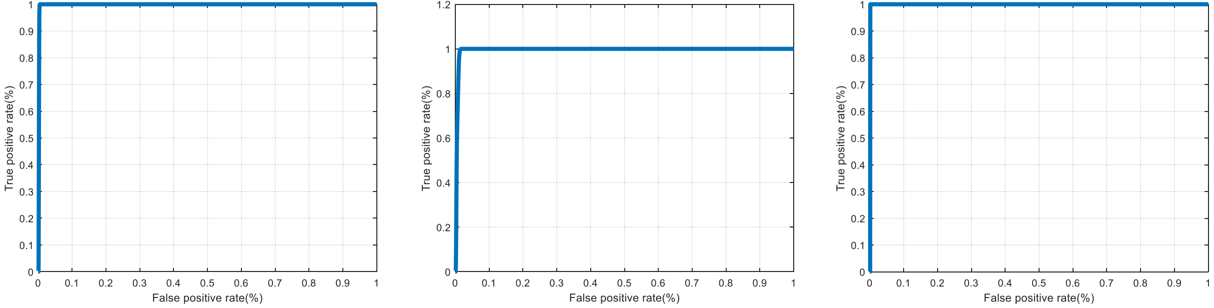
FIGURE 24. **TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 1st examined biometric database.**

AROC values and lower EER values for the proposed cancelable biometric recognition system.

We can come to the conclusion that the proposed hybrid RNA-GA symmetric encryption algorithm succeeds in hiding all details of biometric templates of different databases. This leads to better performance of the proposed cancelable biometric recognition system based on this encryption algorithm.

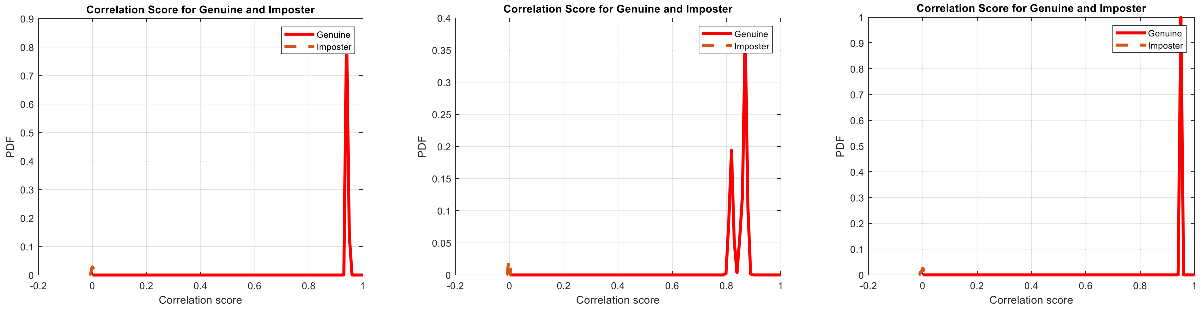


(a) TD and FD with DRPE. (b) TD and FD with OSH. (c) TD and FD with RNA-GA.

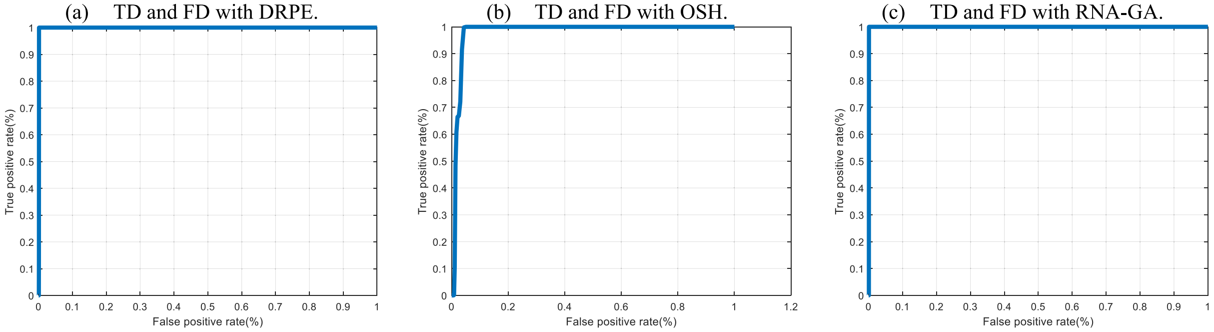


(d) ROC with DRPE. (e) ROC with OSH. (f) ROC with RNA-GA.

FIGURE 25. **TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 2nd examined biometric database.**



(a) TD and FD with DRPE. (b) TD and FD with OSH. (c) TD and FD with RNA-GA.

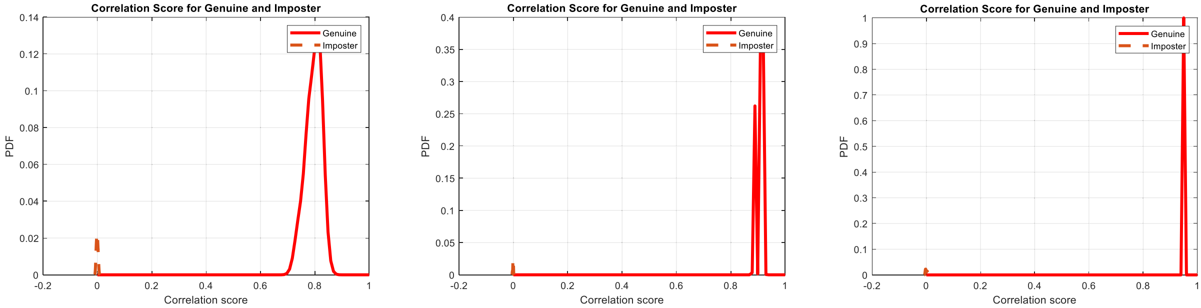


(d) ROC with DRPE. (e) ROC with OSH. (f) ROC with RNA-GA.

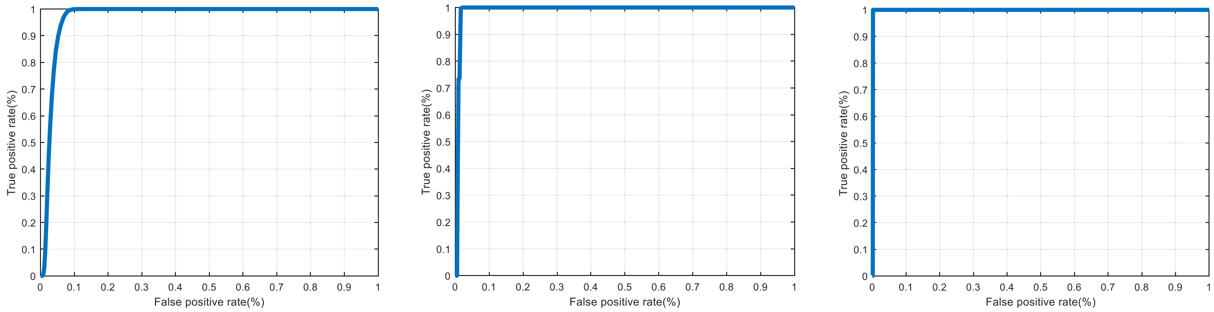
FIGURE 26. **TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 3rd examined biometric database.**

VI. THE EFFECT OF EXPLOITING RNA SYMBOLS BEFORE THE GA TECHNIQUE

Converting the pixel values of the biometric templates to RNA codons before employing the GA technique provides more randomization of the generated templates. The large degree of randomization of generated templates contributes to enhancing the privacy of users, as it becomes difficult for intruders to recover the original biometric templates again. The obtained templates with the proposed encryption algorithm have approximately uniform histograms. High quality of encryption leads to better performance of the cancelable biometric recognition system. Two scenarios in the encryp-

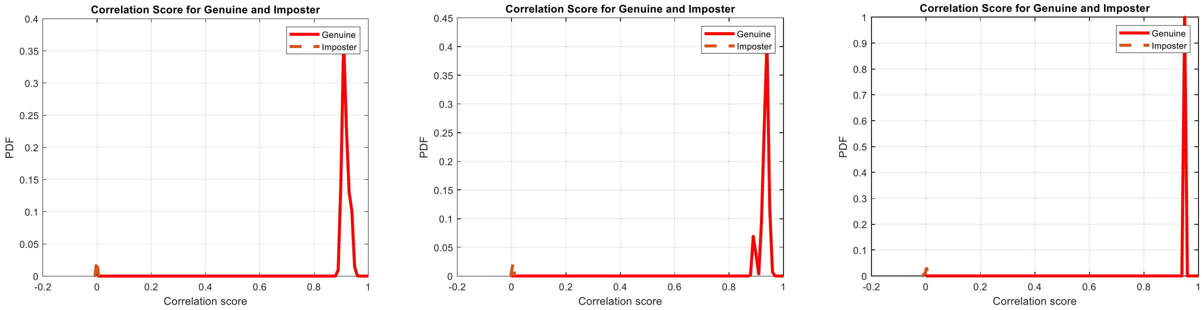


(a) TD and FD with DRPE. (b) TD and FD with OSH. (c) TD and FD with RNA-GA.

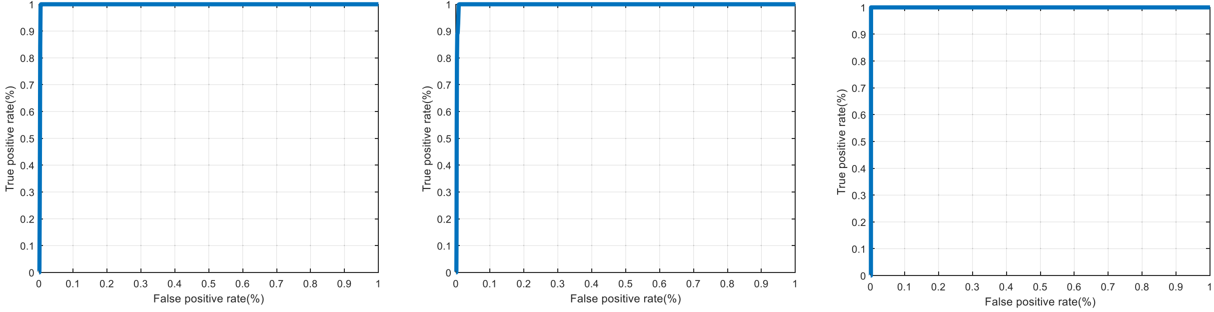


(d) ROC with DRPE. (e) ROC with OSH. (f) ROC with RNA-GA.

FIGURE 27. TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 4th examined biometric database.



(a) TD and FD with DRPE. (b) TD and FD with OSH. (c) TD and FD with RNA-GA.

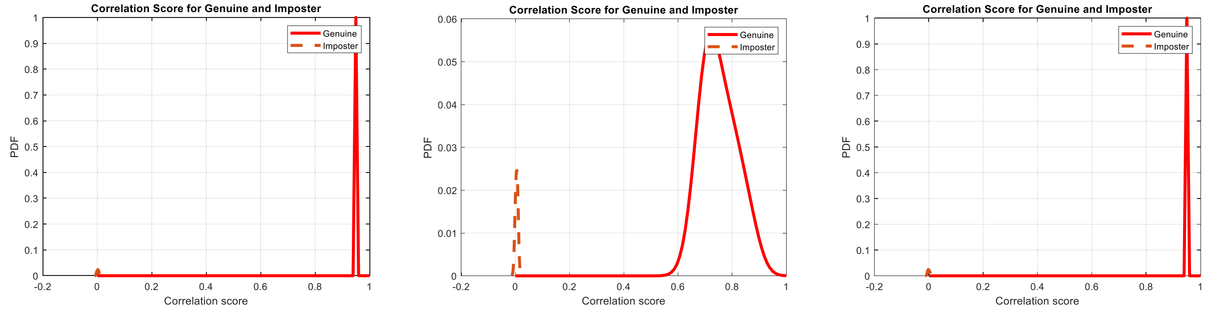


(d) ROC with DRPE. (e) ROC with OSH. (f) ROC with RNA-GA.

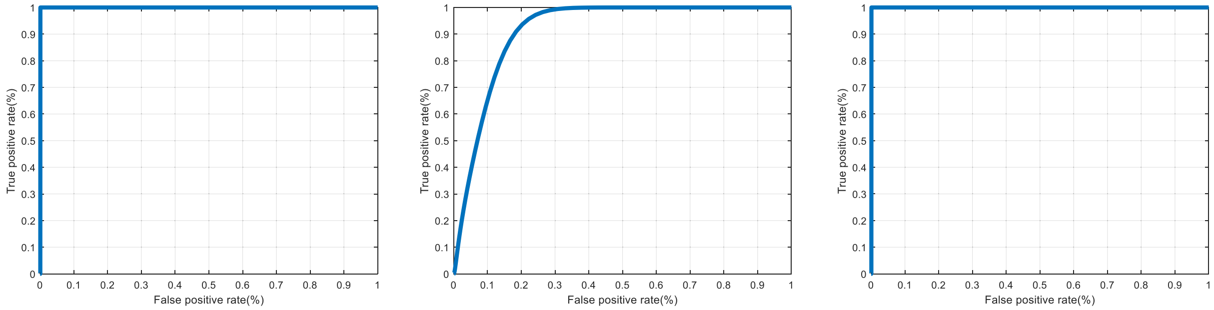
FIGURE 28. TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 5th examined biometric database.

tion process are investigated in this paper. The first one is converting pixels to RNA symbols through RNA cipher lists, and the second one is employing only the GA technique directly on the examined biometric traits [25]. The results of these scenarios are shown in Figs. 30 and 31 for the 1st examined [39], and 6th examined [43] databases for both faces and fingerprints, respectively.

Moreover, Tables 20 and 21 show the correlation values for genuine and imposter tests. The results confirm the importance of using RNA cipher lists to encode the examined

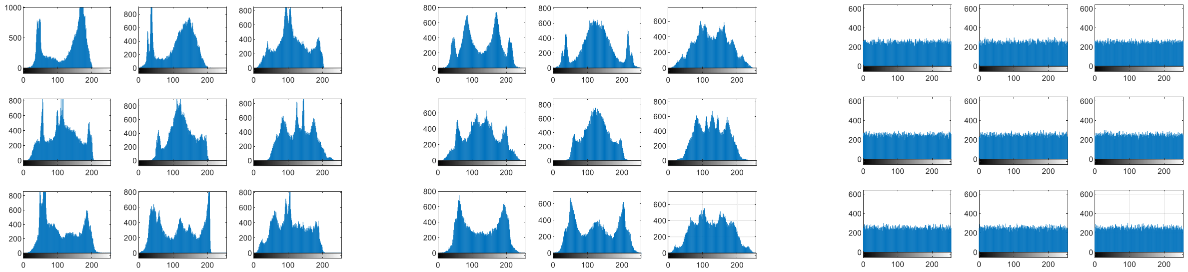


(a) TD and FD with DRPE. (b) TD and FD with OSH. (c) TD and FD with RNA-GA.



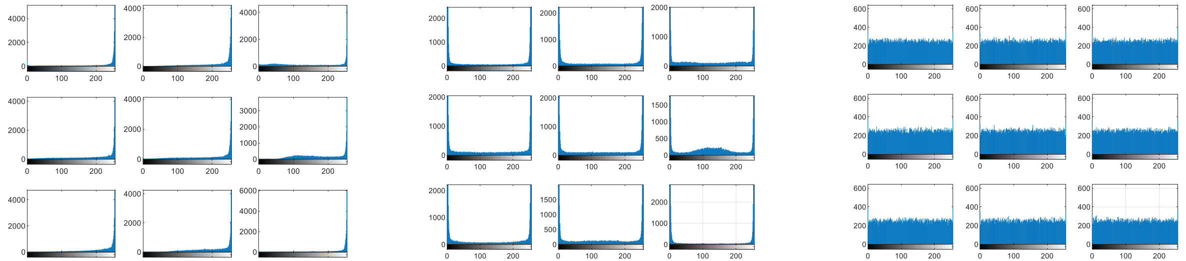
(d) ROC with DRPE. (e) ROC with OSH. (f) ROC with RNA-GA.

FIGURE 29. **TD, FD, and ROC curves for the proposed cancelable biometric recognition system based on the RNA-GA algorithm and the systems based on DRPE and OSH algorithms for the 6th examined biometric database.**



(a) Original template histograms. (b) Histograms of templates obtained with the GA-based algorithm [25]. (c) Histograms of templates obtained with the proposed RNA-GA algorithm.

FIGURE 30. **Histograms of original and cancelable templates generated with the proposed RNA-GA algorithm and the GA-based algorithm for the 1st examined biometric database.**



(a) Original template histograms. (b) Histograms of templates obtained with the GA-based algorithm [25]. (c) Histograms of templates obtained with the proposed RNA-GA algorithm.

FIGURE 31. **Histograms of original and cancelable templates generated with the proposed RNA-GA algorithm and the GA-based algorithm for the 6th examined biometric database.**

biometric templates before applying the GA technique. The proposed hybrid RNA-GA encryption algorithm achieves more uniform histograms for the cancelable templates. It also achieves high correlation scores in genuine tests and low correlation scores in imposter tests.

VII. CONCLUSION AND FUTURE WORK

An efficient and improved symmetric ciphering algorithm has been introduced for robust and reliable cancelable biometric recognition. The novelty of the proposed algorithm lies in the utilization of the GA technique with bio-molecular computations and RNA representations to generate secure cancelable biometric templates. The proposed algorithm provides high degrees of confusion and diffusion in the encrypted biometric templates. Several experimental tests have been performed to illustrate the efficacy of the proposed algorithm in generating completely-deformed biometric traits. The utilized assessment metrics prove that the proposed algorithm outperforms the related works from the encryption assessment perspective on different types of biometrics. Furthermore, the proposed cancelable biometric recognition system based on the hybrid encryption algorithm provides high performance with FAR, and AROC values of 0.0015, and 0.9990, respectively. For the future work, we intend to build cancelable biometric recognition systems based on deep feature extraction and feature encryption to allow more robustness in performance.

ACKNOWLEDGMENT

This work was funded by the Researchers Supporting Project Number (RSP-2021/300), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

[1] L. A. Abou Elazm, S. Ibrahim, M. G. Egila, H. Shawkey, M. K. H. Elsaid, W. El-Shafai, and F. E. Abd El-Samie, ''Hardware implementation of cancellable biometric systems,'' in *Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Oct. 2020, pp. 1145–1152.

[2] 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.

[3] F. E. Abd El-Samie, R. M. Nassar, M. Safan, M. A. Abdelhamed, A. A. Khalaf, G. M. El Banby, and W. El-Shafai, ''Efficient implementation of optical scanning holography in cancelable biometrics,'' *Appl. Opt.*, vol. 60, no. 13, pp. 3659–3667, 2021.

[4] O. S. Faragallah, E. A. Naeem, W. El-Shafai, N. Ramadan, H. E. D. H. Ahmed, M. M. A. Elnaby, and F. E. A. El-Samie, ''Efficient chaotic-Baker-map-based cancelable face recognition,'' *J. Ambient Intell. Humanized Comput.*, pp. 1–39, 2022, doi: 10.1007/s12652-021-03398-0.

[5] 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.

[6] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. A. El-Samie, and W. El-Shafai, ''Efficient HEVC integrity verification scheme for multimedia cybersecurity applications,'' *IEEE Access*, vol. 8, pp. 167069–167089, 2020.

[7] 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.

[8] I. S. Badr, A. G. Radwan, E.-S.-M. El-Rabaie, L. A. Said, G. M. El Banby, W. El-Shafai, and F. E. Abd El-Samie, ''Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion,'' *Digit. Signal Process.*, vol. 116, Sep. 2021, Art. no. 103103.

[9] H. A. A. El-Hameed, N. Ramadan, W. El-Shafai, A. A. Khalaf, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, ''Cancelable biometric security system based on advanced chaotic maps,'' *Vis. Comput.*, vol. 38, pp. 2171–2187, Sep. 2021.

[10] 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.

[11] W. El-Shafai, F. Khallaf, E.-S.-M. El-Rabaie, and F. E. A. El-Samie, ''Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications,'' *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 10, pp. 9007–9035, Oct. 2021.

[12] K. Gupta, G. S. Walia, and K. Sharma, ''Novel approach for multimodal feature fusion to generate cancelable biometric,'' *Vis. Comput.*, vol. 37, no. 6, pp. 1401–1413, Jun. 2021.

[13] R. F. Soliman, N. Ramadan, M. Amin, H. H. Ahmed, S. El-Khamy, and F. E. Abd El-Samie, ''Efficient cancelable Iris recognition scheme based on modified logistic map,'' *Proc. Nat. Acad. Sci., India A, Phys. Sci.*, vol. 90, no. 1, pp. 101–107, Mar. 2020.

[14] 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, 2018.

[15] R. F. Soliman, M. Amin, and F. E. Abd El-Samie, ''A double random phase encoding approach for cancelable iris recognition,'' *Opt. Quantum Electron.*, vol. 50, no. 8, pp. 1–12, Aug. 2018.

[16] 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.

[17] 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.

[18] R. F. Soliman, M. Amin, and F. E. Abd El-Samie, ''A modified cancelable biometrics scheme using random projection,'' *Ann. Data Sci.*, vol. 6, no. 2, pp. 223–236, Jun. 2019.

[19] S. Wang and J. Hu, ''Design of alignment-free cancelable fingerprint templates via curtailed circular convolution,'' *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, Mar. 2014.

[20] P. W. M. Tsang, A. Yan, T.-C. Poon, and H. Lam, ''Asymmetrical and biometric encrypted optical scanning holography (ABE-OSH),'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1094–1101, Feb. 2020.

[21] T. Sudhakar and M. Gavrilova, ''Cancelable biometrics using deep learning as a cloud service,'' *IEEE Access*, vol. 8, pp. 112932–112943, 2020.

[22] G. N. Rajendra and B. R. Kaur, ''A new approach for data encryption using genetic algorithms and brain μ waves,'' *Int. J. Sci. Eng. Res.*, vol. 2, no. 5, May 2011.

[23] L. Leng, A. B. Jin 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.

[24] 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.

[25] W. El-Shafai, F. A. H. E. Mohamed, H. M. A. 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.

[26] 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.

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

[28] 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.

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

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

[31] P. Refregier and B. Javidi, ''Optical image encryption based on input plane and Fourier plane random encoding,'' *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.

[32] G. Unnikrishnan, J. Joseph, and K. Singh, ''Optical encryption by double-random phase encoding in the fractional Fourier domain,'' *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.

[33] X. Peng, Z. Cui, and T. Tan, ''Information encryption with virtual-optics imaging system,'' *Opt. Commun.*, vol. 212, nos. 4–6, pp. 235–245, Nov. 2002.

[34] G. Situ and J. Zhang, ''Double random-phase encoding in the Fresnel domain,'' *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.

[35] W. El-Shafai, I. M. Almomani, and A. Alkhayer, ''Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication,'' *IEEE Access*, vol. 9, pp. 35004–35026, 2021.

[36] 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.

[37] P. Liu, T. Zhang, and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 14823–14835, Jun. 2019.

[38] W. P. Klein, S. A. Díaz, M. Chiriboga, S. A. Walper, and I. L. Medintz, "Dendrimeric DNA-based nanoscaffolded BRET-FRET optical encryption keys," *ACS Appl. Nano Mater.*, vol. 2, no. 12, pp. 7459–7465, Dec. 2019.

[39] AT&T. (1994). *ORL Database of Faces*. Accessed: Jun. 15, 2020. [Online]. Available: http://www.cl.cam.ac.U.K./

[40] B. I. Test. (2005). *CASIA-Facev5*. Accessed: Jun. 15, 2020. [Online]. Available: http://www.biometrics.idealtest.org

[41] (2002). *IIT Delhi Ear Database Version 1*. Accessed: Jun. 15, 2020. [Online]. Available: http://webold.iitd.ac.in/biometrics/Database_Ear.htm

[42] B. I. Test. (2005). *CASIA Palmprint*. [Online]. Available: http://www.biometrics.idealtest.org

[43] (2004). *Fingerprint Veri_cation Competition*. Accessed: Jun. 15, 2020. [Online]. Available: http://bias.csr.unibo.it/fvc2004

[44] M. Dobes and L. Machala. (2004). *Upol Iris Image Database*. Accessed: Jun. 15, 2020. [Online]. Available: http://phoenix.inf.upol.cz/iris/

[45] O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, and B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2018.

[46] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7279–7297, 2019.

[47] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[48] H. Kaur and P. Khanna, "Random slope method for generation of cancelable biometric features," *Pattern Recognit. Lett.*, vol. 126, pp. 31–40, Sep. 2019.

[49] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Gener. Comput. Syst.*, vol. 102, pp. 30–41, Jan. 2020.

[50] H. Kaur and P. Khanna, "PolyCodes: Generating cancelable biometric features using polynomial transformation," *Multimedia Tools Appl.*, vol. 79, pp. 20729–20752, Aug. 2020.

[51] 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 Appl.*, vol. 79, no. 19, pp. 14053–14078, Feb. 2020.

[52] D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3152–3167, 2020.

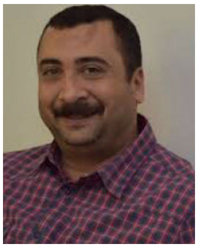
FATMA A. HOSSAM ELDEIN MOHAMED was born in Alexandria, Egypt. She received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Alexandria Higher Institute of Engineering and Technology, Alexandria, in 2010, and the M.Sc. degree from the Faculty of Engineering, Alexandria University, in 2016. She had worked as a Teaching Assistant at the Alexandria Higher Institute of Engineering and Technology. She is currently a Ph.D. Researcher with the Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Alexandria University, Egypt. Her research interests include information security, optical signal processing, big data, 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.

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 multiview video coding, multiview video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filter design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codec standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software-defined networks, Internet of Things (IoT), medical diagnosis applications, FPGA implementations for signal processing algorithms and communication systems, cancelable 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 system applications. He also serves as a reviewer for several international journals.

HASSAN M. A. ELKAMCHOUCHI (Life Senior Member, IEEE) is currently a Professor Emeritus of wireless communications, antennas and wave propagation with the Electronics and Electrical Communications Department. He was given the Encouragement State Award in 2002 from the 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.

ADEL ELFAHAR is currently an Assistant Professor with the Department of Electrical Engineering, Alexandria University, Alexandria. Egypt. His research interests include code division multiple access, computational complexity, multiuser detection, and optimization.

ABDULAZIZ ALARIFI received the Ph.D. degree in information security from the University of Wollongong, Australia. He is currently an Assistant Professor with the Department of Computer Science, Community College, King Saud University (KSU), Saudi Arabia. He is also the Head of the Research Unit, Community College, KSU. His main research interests include information security, information technology management, cloud computing, big data, information privacy, risk assessment and management, e-governance, and mobile applications.



MOHAMMED AMOON received the B.Sc. degree in electronic engineering and the M.Sc. and Ph.D. degrees in computer science and engineering from Menoufia University, in 1996, 2001, and 2006, respectively. He is currently a Professor of computer science and engineering with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. He is also a Professor of computer science with the Department of Computer Science, King Saud University. His research interests include agent-based systems, fault tolerance techniques, scheduling algorithms, green computing, distributed computing, grid computing, cloud computing, fog computing, and the Internet of Things (IoT).

MOUSTAFA H. ALY was born in Alexandria, Egypt, in 1953. He received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Engineering, Alexandria University, Alexandria, in 1976, 1983, and 1987, respectively. He is currently a Professor of optical communications with the Electronics and Communications Engineering Department, College of Engineering and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria. He was a co-supervisor of 135 M.Sc. and Ph.D. students and he published 290 journals and conference papers. His research interests include optical communications, optical amplifiers, and optical networks.

FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He worked as a Researcher at the KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICs), from 2013 to 2015. His current research interests include image processing, multimedia communications, medical signal and image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the *Digital Signal Processing* journal in 2008.

AMAN SINGH received the Ph.D. degree in computer science and engineering from Lovely Professional University, India. He is currently working with the Universidad Europea del Atlántico, Spain. He is also the Scientific Advisor to a multinational research-based industry, Velmenni, situated in Estonia and India. Most of his papers appeared in very selective and reputable conferences and journals, such as *IEEE Wireless Communications Magazine* and the IEEE INTERNET OF THINGS JOURNAL. He has been invited to give keynote talks, lectures and tutorials on artificial intelligence and mathematical modeling in international conferences and summer schools. He also has strong collaboration with industry, including projects, consultancy, and corporate social work. He has published more than 60 refereed papers, including journals and international conferences. His main research interests include education 4.0, artificial intelligence, deep learning, machine learning, and mathematical modeling. He is a member of the editorial board of numerous international journals. He has been a guest editor of several special issues for reputable international journals. He is also a Regular Reviewer for prominent journals, including IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, *ACM Transactions on Sensors*, IEEE INTERNET OF THINGS JOURNAL, *AI*, *CMPB*, and *CBM*.

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 an Acting Vice-Dean of the Faculty of Engineering, Ahram Canadian University. He published 27 research papers in international conferences, and journals in electrical engineering and computer engineering related fields. His research works were cited by 427 other research works, and his H-index is nine, till January 2021. He was given 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)."

• • •