ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/377206031

Cancelable biometric authentication system based on hyperchaotic technique and fibonacci Q-Matrix

Article *in* Multimedia Tools and Applications · January 2024

DOI: 10.1007/s11042-023-17855-9

CITATION
1

READS
218

2 authors:

Fatma Hossam
Alexandria University
5 PUBLICATIONS **55** CITATIONS

SEE PROFILE

Walid El-Shafai
Menoufia University
355 PUBLICATIONS **4,241** CITATIONS

SEE PROFILE

All content following this page was uploaded by Walid El-Shafai on 06 January 2024.

The user has requested enhancement of the downloaded file.

Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-17855-9

Cancelable biometric authentication system based on hyperchaotic technique and fibonacci Q-Matrix

Fatma A. Hossam Eldein Mohamed[1] · **Walid El-Shafai**[2,3]

Received: 7 April 2023 / Revised: 9 September 2023 / Accepted: 12 December 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract
Due to the rapid growth in the field of information transmission techniques, billions of data are transmitted through variant authentication applications between clients. Providing protection to store and transmit these details has the priority in most services. Cancelable biometric techniques have the ability to store and employ these biometric signatures safe away any intruders. These template protection techniques are derived into transformation and cipher based cancelable biometric methodologies. The cipher approaches that are dependent on chaotic schemes quite achieve the two requirements of successful cancelable systems known by confusion and diffusion. This is prompted us to propose a novel cancelable research combines between Hyperchaotic technique and Fibonacci Q-matrix. The hyperchaotic system employs six initial conditions, equations, to construct the initial deformed patterns. Afterwards, the stage of diffusion is accomplished by employing Fibonacci Q-matrix for the resultant dislocated patterns to obtain the final protected template. The proposed cancelable authentication technique is validated by the two evaluation perspectives of authentication and security measurements, respectively. Furthermore, the proposed cancelable system is compared with the most recent studies in the same state-of-art which are utilized by GA and RNA-GA. Five tested biometrics are exploited to prove the validation of our work through any gray or colored biometric patterns with different sizes under different capturing environments even in the presence of noise level. The proposed work achieves high authentication performance by large values of AROC (Area under Receiver Operating Characteristic) Curve leads to 0.999, and similarity coefficients of licensed clients. As well as, the least values of FAR, and FRR (False Acceptance, and False Rejection Ratios) in addition the more uniform resultant histogram shapes due to the cancelable patterns. From the security perspective, the proposed cancelable methodology achieves high entropy of 7.99, NPCR (Number of Pixels Change Rate), and UACI (Unified Average Changing Intensity) values lead to almost optimum results of 99.0271%, and 31.2058%, respectively. This validates its immunity against probable differential attacks.

Keywords Cancelable Biometrics · Six-dimensional hyperchaotic · Fibonacci Q-matrix · Confusion · Diffusion

Extended author information available on the last page of the article

Published online: 06 January 2024

1 Introduction

The internet of things (IoT) is providing new ways to gain access to systems and data. Each IoT device is an end point appliance, therefore it considered as a potential back door for hackers. These devices may be involved in routers, security cameras, DVRs to medical devices, or cars, and others. So, all these appliances can be controlled remotely which lead them to face high degree of infection with malware, and purposed cyber-attacks searching for directing their power towards specific targets that is previously chosen.

In remote surveillance systems, authentication and recognition techniques involved in the internet of things (IoT) devices, are essential to maintain privacy and confidentiality to the genuine users in these systems. Because of its participation in preventing the unauthorized entry to IoT networks [1]. Verification and identification are used to confirm that the authorized entry only can access his, or her account. Authentication by traditional techniques, specifically personal identification numbers (PINs) and passwords, has been applied over the past years. Nowadays, we have been used magnetic cards and PINs for more safety [2].

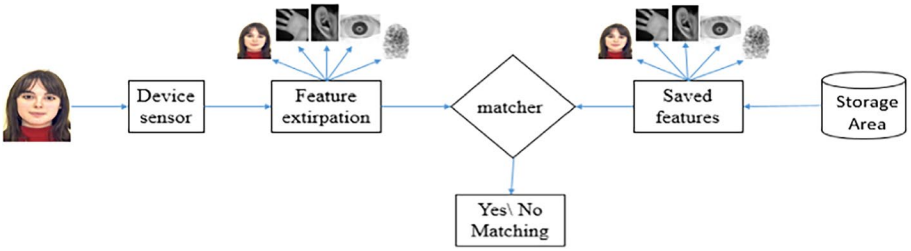
Some disadvantages associated with the previous ways come up because they identify some characters possessed by the owner rather than recognizing the owner itself, who indeed owned them. These tokens can be exposed by stolen or lost, so any intruder can easily be entered or controlled by the system. There is a new approach in authentication systems that exploit biometrics in various fields as governmental services, commercial applications, knowledge-based systems, tokens-based systems, and the applications are related to forensic evidence that depend on human-being supervision [2].

Recently, the biometric data has much concern over the traditional password based authentication techniques because of its uniqueness. Biometric is a merged word resultant from Bio which means life and metric which means measuring [2]. There are many biometric characteristics as Face, Ear, Fingerprints, Iris, and Palm prints, which are the mandatory tested templates in this state-of-art.

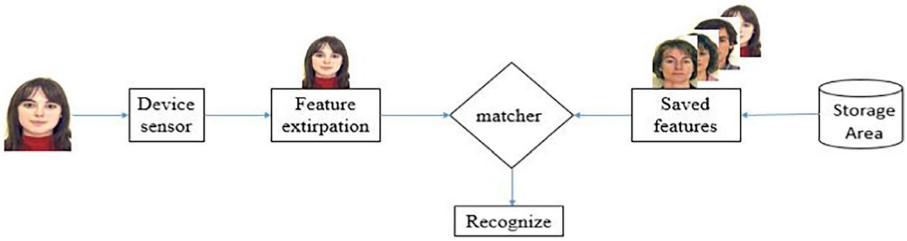
Biometric techniques have been applied in many applications on a wide scale as access permission systems, classification and identification, surveillance, and behavioral analysis studies [2]. Thus, biometric traits are classified into physical, and behavioral samples. Behavioral traits are dependent on analysis due to the person act in several circumstances, but it is still not reliable compared with the physical characteristics. That is due to their instability of the reactions towards the same situations leading to make them impractical.

Biometric identification defines as the act of recognition or verification for the identity of the user. Biometric identification is involved in two categories, (a) Recognition (b) Verification. In recognition, person's biometric trait is captured by the sensors of the security systems. Then, it is passed over all stored genuine traits until finding the matched one, as well as recognizing it. For verification, the unique feature of the client is checked with each feature that was already stored in the database. The result of this check shows if the match happens or not. Figure 1 shows simple examples for the two operations of pattern identification. It is obvious that the recognition process is considered as 1 to N matching process, but the verification process has 1 to 1 matching criteria [2].

Thus, the biometric data is better than the old-passwords and tokens that may be stolen or forgotten. But, it still faces some challenges to be more secure and unrecognizable. So, the idiom of Cancelable Biometric is appeared and taken a big consideration by the researchers.



(a) Biometric verification



(b) Biometric recognition

Fig. 1 Biometric identification process

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 measure of similarity between the corresponding biometric features of the enrolled data belonging to 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. 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. Therefore, recently, cancelable biometric recognition systems have appeared as an alternative solution to keep the original biometrics safe [3].

Cancelable Biometrics are defined as the genuine features suffer from some pattern deformations to attain unrecognized user's pattern without any effect on the recognition or verification processes. The researchers seek to increase the privacy protection, in addition enhancing the accuracy of recognition and verification. There are specific characteristics must be achieved in any cancelable biometric system. These five characteristics are as follows: Diffusion, confusion, revocability, non-invertible result, and high recognition degree.

Each property is discussed as following, Diffusion hides the statistical relationship between the cancelable template and the original feature, Confusion means that there is a big effect on the cancelable template if one bit in the original trait has changed, Revocability means regeneration of the cancelable template if the system is hacked, noninvertible transformations are summarized as the genuine templates cannot be fetched or obtained

if any intruder hacks the security system. The performance efficiency is involved in the examination of the tested trait and the cancelable stored one from the view of two perspectives, the first perspective is corresponding to the authentication metrics and the second perspective is involved in the security analysis.

There are two stages in any cancelable biometric authentication system as shown in Fig. 2 i.e. (a) Registration which is defined by the enrollment process, and (b) Verification. In the registration stage, a surveillance device captures the biometric patterns of the authorized users and analyzes them to get the required biometric features. After applying some of the variant techniques as Encryption, Mapping or Hybrid Transformations, the cancelable biometric traits are obtained. Then, these cancelable traits are stored in the cloud device or system. The previously mentioned steps are applied firstly in the verification stage. Finally, the matching is verified between the stored cancelable features and the cancelable tested images.

Generally, the cancelable biometric systems that depend on feature encryption are preferred to those depending on non-invertible transformations. This is reflected in the resultant evaluation metrics including correlation scores, Area under the Received Operating Curve (AROC), False Acceptance Rate (FAR), and histogram uniformity. 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 DEA, AES, and RSA are not recommended for cancelable biometric authentication applications due to several implementation difficulties like key management and implementation complexity. The main challenge for most encryption techniques is just how to keep immunity against hacking or intrusion attempts [3].

In addition, biometric encryption techniques based cancelable schemes with multiple features achieve high degree of privacy as well as a high degree of recognition level for the authorized individuals. In these cryptosystems, the genuine biometric features are not kept directly in the cloud, but they are initially processed and converted into deformed templates called noise templates (encrypted images) [4, 5].

A lot of chaos-based cipher schemes of biometric features have been introduced recently. Some of them is introduced in this research. In [6], the authors employed dual

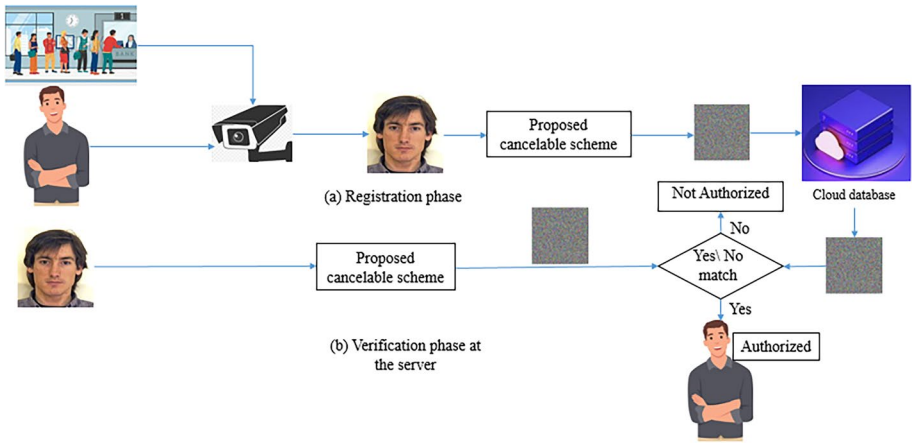


Fig. 2 The authentication stages in the cancelable biometrics

of hyper chaotic schemes to implement deformed samples of body tissue for diagnostic or forensic purposes. In [7], Chen's hyper-chaotic technique accompanied with fractional Fourier transform were introduced to conceal the discriminative details. Hyper-chaotic is utilized as an alternate method instead the one and two dimensional simple chaotic techniques to avoid their weakness towards cracking or deceiving. The methodology of hyper-chaotic is initialized by more than one dimensional condition in terms of non-linearity, unpredictability, randomness, and initial state values. So, these hyperchaotic techniques-based cipher schemes developed by a large key length. It is considered as a merit to progress the privacy level. However, template cipher schemes which are dependent on hyper-chaotic methodology possess some of system failure towards various types of hacking. In addition, the resultant histograms of deformed templates were not stable enough due to relevant techniques [8].

The progressive performance due to the proposed work show great improvements in the simulation assessments which are either based on cancelable metrics or security evaluation. The contributions achieved by our proposal are summarized as follows:

1. The 1st exploitation of Fabonacci Q-matrix in producing different cancelable biometric frames.
2. The employment of six-dimensional hyperchaotic technique in performing such state-of-art.
3. The increase in key length due to our proposed approach compared with the ordinary key space obtained by low dimensional chaotic approaches contributes to more protection against brute force attacks.
4. The proposed technique has more validation in generating cancelable biometric features over the two comparable techniques.
5. The implementation of cancelable algorithm by six-dimensional hyperchaotic technique, to confirm the confusion property, accompanied by Fibonacci Q-matrix, to achieve complete diffusion, for the whole deformed pixels raises the privacy indices.
6. The implementation process is more feasible compared with the other two comparative cancelable techniques based on GA, and RNA-GA. Thus, it consequently implies to a remarkable increase in the processing speed during the simulation run.

The rest of the sections of this research work are arranged as follows. Section 2 presents the recent related works. Section 3 describes the basic concepts of the 6D-hyperchaotic, and Fibonacci Q-matrix techniques. Section 4 gives an explanation of the proposed cancelable biometric authentication framework. Section 5 presents the experimental results with discussions and comparisons. Moreover, it illustrates the security analysis of the hybrid 6D hyperchaotic and Fibonacci Q-matrix cipher-based cancelable biometric authentication approach. As well as it gives a discussion for the examined evaluation assessments. Finally, the conclusion and future work are exposed in Sect. 6.

2 Relevant work

In remote monitoring systems, authentication algorithms involved in the internet-of-things appliances are essential for IoT security systems because they participate in preventing the hackers to enter the IoT networks. Biometric details are a concerned authentication pattern due to its unique characteristics over ancient password-based

authentication schemes. Biometric template methods are categorized by helper-data-based algorithms and cancelable biometric schemes. Biometric defense schemes should provide triple conceptual criteria of secrecy, that are: (a) in-connectivity, where variant of secret features must be employed for various applications to forbidden cross-matching attacks, (b) single-way transformation, to obtain rising level of security against the reveal of the genuine biometric traits, and (c) integrity, which is defined by the licensed biometric trait must be protected against foreign access.

In [9], the descriptors of the fingerprint are linked to obtain high interpretation during the matching phase and the authentication phase of a fuzzy fingerprint vault. The difficulties and restrictions that open out over the key binding algorithm through the formation of the transferred array of templates and the recognitions are achieved by alternating the fuzzy commitment scheme with an error correction code (ECC). In cases of unlicensed access, renewability and revocability are the most repetitive problems appearing in front of the biometric cancelable techniques. These problems give the intruder a chance to inlet the system and identify the stored template traits. Besides, biometric cryptosystems suffer from various attacks [10]. Transformations can be defined as repetitive permutations employed to the authenticated biometric trait to transfer it into unrecognized feature in advance. Then, it will be stored in the system database. These transformations are irreversible functions applied for the tested traits that improve the diversity and unlink ability criteria. The same biometric features can be suffered from different transformations for various applications to inhibit cross-matching between saved features in various cloud databases [11–16].

One more model of cancelable biometric system is called a hybrid algorithm. It gathers two or more cancelable biometric techniques [17]. One of the most novel options to obtain a distorted biometric feature is to employ data-dependent cryptography. In [18], client fingerprint features can formulate secret keys of a cipher scheme for fingerprints. Therefore, it is unfeasible for the foreigner to expect the secret keys without preceding client's features. Random projection and discrete Fourier transform have been employed on the authorized features as a cancelable scheme to veil all traits of the licensed biometric templates [19]. This pattern of distortion leads the reaching to the genuine features very intractable, increasing the protection against hacking the biometric stored datasets. In [20], a biometric template protection scheme was applied to the licensed trait arrays to reconstruct protected templates exploiting the K-nearest neighbor scheme. PIN and random salting are utilized on the genuine templates to obtain cancelable features. In [21], hash coding was applied as a single-way transformation approach, which satisfies the revocability and unlink ability or in-connectivity to obtain an appropriate level of the fulfillment of the biometric application.

In [63], the researchers integrated a zigzag technique to obtain the diffused template. After that, EL- Gamal cipher scheme was employed to deform the diffused pattern. At last, Lorenz and Rossler chaotic formula are employed to dislocate the position of pixels. Visual and numerical assessments were applied to validate the pattern crypto-system to secure templates against many kinds of familiar attacks. The presented approach achieved obvious improvements towards visual inspection and security evaluation measurements.

In [64], a recent study on image cryptography was introduced based on bit alternation criteria, chaotic systems, and DNA symbols transformation. Initially, each pixel was transformed to its binary representation. After that the zero bit was alternated to the sequence of (1 0) and the one bit was changed to sequence of (0 1). Moreover, the resultant constructed patterns are ciphered by employing high dimensional chaotic systems. Furthermore, the obtained cipher templates are encoded by the introns and exons of DNA sequences. Finally,

these DNA resultant patterns were combined together by the usage of DNA addition rules. The introduced approach investigated high NPCR lead to 99.61% and UACI of 34.61%.

In [65], a low complexity circular queue data structure cryptography was introduced by the usage of complicated alternative factors. These adaptive factors were represented in the size of the circular queue, the start bits of the elected key-word letter and the multiple representations of a number in the Fibonacci matrix. Then, all letters were alternated to ASCII binary representations to be exploited in the logical and shift operations during the processing of security algorithm. The results achieved by the presented security scheme had the ability to decrease the complexity into half compared with other studies based on multible circular queues scheme (MCQA). Moreover, the Fibonacci matrix and its variables improved the flexibility in alternating the privacy of the technique according to the application requirements.

Researchers in [22] presented a verification system for iris identification. It is dependent on the integration of one-way transformations and cipher scheme for veiling the iris trait. They achieved an effective authentication of 99.9%. In [23], variant of protection tools are introduced for face recognition. They have employed many processes for the extraction of geometric traits. Another algorithm is introduced based on developing ciphered features after using gabor filters. In this scheme, two kinds of chaos maps were presented which are logistic and modified logistic maps. This algorithm achieved 99.08% efficiency and 1.175% EER by the chaotic logistic maps. In [24], the authors exposed, a double random phase encoding, DRPE-based authentication system for iris features. The bio-convolving scheme was applied to satisfy both confidentiality and privacy for the clients' iris. Moreover, the same researchers in [25] presented an authentication framework for multiple sorts of physical features resembled in iris and faces traits. It is dependent on gathering different traits of the biometric templates. The Fractional Fourier Transform, FRFT-based algorithm, is used to achieve a one-way iris template. The secret keys, RPM 1 and RPM 2 are used in the introduced cancelable biometric algorithm. One of these keys, RPM 1, is the initial step mask of the left iris trait array, and the second one is for the right iris trait pattern of the specified user himself. Experimental results illustrated that the presented scheme improves confidentiality. In addition to that, it satisfied an EER of 0.63% and an efficiency of 99.75%. Cancelable fingerprint authentication frameworks employ a feature extirpation process in a repetitive way. Ratha et al. [26] presented a cancelable geometric scheme of fingerprint verification. It is dependent on the derivation of feature pixels and the usage of transfer coordinates from polar to Cartesian coordinate to achieve cancelable features of the fingerprints. This algorithm satisfies a high accuracy degree of privacy and confidentiality while maintaining the fingerprint frames are distorted. In [27], the researchers investigated a protection algorithm of fingerprint detection that is based on multiple spiral curves employing fuzzy commitment scheme. The fuzzy commitment framework was employed for encrypting the fingerprint minutiae. This algorithm satisfies an equal error rate (EER) of 1.17%.

The optical scanning holography, OSH approach was presented by Korpel and Poon in [28], which applied a one-pixel sensor to enroll the hologram of a three-dimensional object through a successive scanner that was employed in a row-by-row order. The optical scanning holography is concluded from the idiom of heterodyne optical scanning. So, it has the ability to transform a three-dimensional image into a two dimensional array. The electrical signal is the resultant output from a transformer, as a photodetector, where the incident light beam is the input signal. This electrical signal implements the introduced details of the scanned biometric feature [16]. A two-dimensional digital image of the scanned input feature is deduced from the scanned electrical output, then it is kept in a digital form on a

computer. This approach differs from the ordinary digital hologram acquisition schemes exposed by two-dimensional snapping sensors with dedicated capturing areas and efficient restricted spatial resolution; OSH can produce holograms of wide-field images with high resolution. In [28, 29], the researchers illustrated compressive optical scanning holography, and it is succeeded in satisfying a correlation score of 0.93 as maximum.

Therefore, we can deduce that distortion of the licensed details can be developed by employing single or couple of two schemes, as well as it is allowed to be performed by a combination between more than bilateral approaches resembled in mathematical transformations-based cancelable algorithms or encryption-based cancelable algorithms.

Thus, Genetic Algorithm, GA cipher scheme can be employed to develop a distorted biometric feature. GA is also provided a cryptographic technique in the frequency domain. In [30], the researchers exposed GA as an image cipher approach to construct alternative patterns of dedicated scenes. In the crossover phase, frequency coefficients of the imaginary parts were replaced, while their real coefficients were subtracted from the input key in the mutation phase. In [31, 32], because the randomness of the cryptographic image is based on the cipher key, GA is also applied to adjust the secured key. A secured key with n bits can be alternated by $n!$ components. The GA scheme chooses the ideal confidential key with optimal length to produce efficient encryption [33, 34].

The exploitation of the RNA codons accompanied with GA to conceal the color and gray-scale biometric patterns as it increases the stability of histogram to become more uniform. Thus, this technique satisfies protected biometric templates with more deformation than other achieved patterns by GA only. So, the security assessments are obviously improved with no significant decrease during the evaluation of the authentication metrics. This technique provides an average EER, FAR, and FRR of 0.03087, 0.00749, and 0.03379, respectively, and the result for AROC leads to 0.9998.

Another kind of the template protection schemes were resembled in the old-way techniques that initialized with a feature deduction and terminated with the resultant protected template. In [35], the researchers introduced a template protection scheme based on ECG signals using two feature protection approaches. Initially, a developed Bio-Hash scheme has been utilized. Then, an array transformation is employed to transfer the genuine template into a cancelable trait by a single direction transformation. In [36, 37], the authors applied a bidirectional Gabor filter to achieve the feature deduction from palmprint features, after that they applied two-dimensional palm Hash code to conceal these traits and construct the cancelable palmprint features array. In [37], a cancelable technique is employed over palm-biometric traits to generate cancelable biometrics as well as achieve more privacy and confidentiality that are dependent on various feature fusion levels.

Fortunately, the template protection techniques which are based on template cryptosystem have the superior achievements in the authentication and recognition purposes over those depending on non-invertible transformations. This makes an obvious progress in the evaluation criteria including correlation factors, AROC, FAR, FRR and the shape of the output histogram [38]. Thus, the tendency of template cryptosystem has been widely developed in biometric template protection techniques. Furthermore, the recognition phases of cipher features are much easier with correlation measurements. However, conventional template cipher schemes, such as DEA, AES, and RSA have not the priority to be utilized in the biometric template protection services because of the multiple implementation difficulties as key management and programming run complexity [39]. However, the mandatory requirement of different cipher schemes is how to keep immunity against hacking and intrusion attempts [40] without reducing the accuracy of recognition or authentication performances.

In [41], the researchers presented a key creation scheme that utilized a fuzzy commitment approach to conceal the secured key in the deformed iris traits. This template protection scheme developed an EER reached to zero. In [42, 43], the authors imposed variant of cipher schemes for face traits that are based on chaotic maps. The chaotic theory achieves remarkable as well as distributive statistical characteristics that can be utilized in template protection study with satisfying a moderate entropy value. In addition, these properties increase the mystery between the genuine features, key, and resultant ciphered traits which make these traits unfeasible to be recognized.

In [44], the researchers illustrated a biometric multi-template protection technique that depends on variant of discrete transformations like Discrete Fourier Transform (DFT), Fractional Fourier Transform (FrFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Furthermore, a matrix rotation is employed to develop cancelable fingers and faces templates that achieve the revocability and confusion criteria. This algorithm provided well evaluation metrics, resembled in AROC of 0.998, EER of 0.0023, FAR of 0.08, and FRR of 0.003.

In [61], the researchers investigated many template protection techniques with different biometric criteria. Bio-Hashing, Multi-Layer Perceptron (MLP) Hashing Bloom Filters, and two techniques were dependent on Index of Maximum Hashing (IoM). Moreover, the researchers studied a template protection technique was dependent on binary translation successive to client –specific random conversions. FAR, FRR, and AROC were estimated on deep learning based traits exploited from various biometric features and behavioral attitudes including face, voice, fingers, and iris.

In [62], multi-template protection based recognition technique was employed by several convolutional nural networks (CNNs) to pick up the deep traits from various facial sections. Batch normalization, depth concatenation, and a residual learning framework were employed to form a new CNN architecture. Several CNNs were employed to extract deep traits from each face section, followed by a fusion network gathered these traits together to form one feature descriptor. Furthermore, to add more protection to the secured templates, bio-convolving encryption was applied on the final facial descriptor. This technique achieved competitive results but it still suffered from time consumption issue during its processing.

Thus, many cancellable biometric approaches are based on different traditional cipher schemes or\and irreversible transformations are exposed in this study and summarized in Table 1. There are multiple weak points in the presented traditional template protection schemes. These points are summarized as following [3]:

1. Low key space leads to a reduction in sensitivity for initial condition.
2. When the deformed patterns are disturbed by noise or data fading, some of the cancelable algorithms lead to failure in recognizing or authentication-based systems.
3. The ordinary presented cipher schemes could not achieve the mandatory trade-off between the identification stage sensitivity and the cancelable pattern randomization.
4. The quality measurements as AROC and EER are not sufficient good to prove efficiency and privacy.
5. The previously mentioned approaches are examined only on limited sizes and types of datasets.
6. The assessment of the encryption perspective has not been implemented in the introduced cancelable biometric schemes.

Table 1 Comparison of the performance of previously related studies and our proposed cancelable schemes [3]

Work	Illustration and Purposes	Biometric Patterns	Algorithm	Performance Measurements	Merits	Demerits
[9]	Fingerprint descriptors are linked together before utilizing fuzzy vault approach to construct cancelable template	Fingerprint patterns	Fuzzy vault-based cipher scheme	FRR = 3.251×10^{-3} FAR = 0.7814 EER = 0.0214	Good performance through recognition	Vulnerable to blended substitution attacks, and the attacks on error-correcting codes Only one physical modality is examined to prove reliability
[18]	Employs fingerprint patterns to deduce secret keys of the cipher technique	Fingerprint patterns	Modal- based crypto-system	FRR = 1.751×10^{-4} FAR = 0.0314 EER = 4.589×10^{-9}	High confidential stored genuine traits	Sophisticated implementation and vulnerable to masquerade attacks
[19]	Random projection and discrete Fourier transform	Fingerprint patterns	Hybrid deformation	FRR = 2.369×10^{-3} FAR = 0.0864 EER = 2.67×10^{-11}	Robustness for the licensed patterns	Unfeasible to analyze the system
[20]	PIN and stray salting are employed to construct the cancelable templates	Fingerprint patterns	K-nearest neighbor approach	FRR = 1.925×10^{-5} FAR = 0.00678 EER = 1.827×10^{-3}	Unbreakable by foreigners	Vulnerable to record multiplicity attacks
[21]	Hash coding was utilized as a single direction transfer scheme	Fingerprint patterns	Hash coding	FRR = 0.2731 FAR = 0.0308 EER = 0.00186	Serves the revocability and link ability	Low efficiency therefore it suffers from severe degradation of accuracy due to noise existence
[27]	The fuzzy commitment scheme was developed to encrypt the discriminant features	Fingerprint patterns	Employing multiple spiral curves by means of fuzzy concepts	FRR = 0.492 FAR = 0.0627 EER = 0.0117	satisfies blind authentication	The approach faces the run instability leading to high FRR
[22]	Irreversible feature deformation to conceal the licensed iris traits	Iris patterns (CASIA v.3)	Encryption combined with irreversible transformations	FRR = 1.114 FAR = 0.0046 EER = 0.00017	Obtained authentication rate up to 99.9%	Uni-modal biometric features

Table 1 (continued)

Work	Illustration and Purposes	Biometric Patterns	Algorithm	Performance Measurements	Merits	Demerits
[23]	Developing cipher traits after the utilization of Gabor filters to extract features from iris templates by means of convolution kernels obtained by chaotic maps	Iris patterns (CASIA v.3)	Two kinds of chaotic approaches: logistic maps and modified logistic maps	FRR = 1.185 FAR = 0.0086 EER = 0.00117	Efficiency leads to 99.08%	Vulnerable to brute force attack and replay attacks One physical modal was implemented
[25]	adopted cancelable iris identification scheme based on multiple biometric features fusion	Iris patterns (CASIA v.3 & v.4)	Fractional Fourier Transform (FrFT)	FRR = 0.274×10^{-3} FAR = 0.00029 EER = 0.0063	efficiency leads to 99.75%	Vulnerable to reversible brute force attack, sophisticated code implementation with high processing time
[35]	The protected templates are generated by the inner product operation between the ECG traits after converting the ECG pulses to features arrays	ECG impulses (MIT-BIH arrhythmia, PTB, and CYBHi databases)	A modified Bio-Hashing and matrix operation scheme	FRR = 0.0 FAR = 0.38 EER = 0.26	Satisfying more validation and reliability against accuracy loss due to noise presence which is the main obstacle in Bio-Hashing	The licensed details can be identified if a foreigner has previously knowledge of the generated key which is easily extracted from the biometric information
[36]	Bi-directional coordinates Gabor filters were suggested as template protection technique to provide palmprint authentication	Palmprint patterns (poly U version 2 dataset)	Bi-direction in (x, y) implementation of palm Hash code	Traditional statistical analysis	Conceal vertical correlation	Still low performance over different biometric patterns

Table 1 (continued)

Work	Illustration and Purposes	Biometric Patterns	Algorithm	Performance Measurements	Merits	Demerits
[37]	A multi-modal biometric technique merges details from more than one biometric pattern	ECG (PTB dataset and CYBHi dataset) Fingerprint patterns (livedet 2015 and FVC 2004 datasets)	Traditional neural-network and Q-Gaussian multiple support array machine which integrated on various level fusion	FRR = 0.0 FAR = 0.004 EER = 0.0014	Faces verification accuracy reduction and spoof attacks	Need to accelerate the verification process
[41]	A key creation scheme that utilized a fuzzy commitment approach to conceal the secured key in the deformed iris traits	Iris patterns (CASIA v.3)	A fuzzy commitment approach	EER reached to zero	Faces the increase in false recognition or authentication rate	Any attacker who has access to the target machine would be able to disassemble the code to find the private key
[42]	The authors imposed variant of cipher schemes of faces traits that are based on chaotic maps	Faces patterns (ORL dataset)	Chaotic maps	High correlation ratios between licensed features and very low correlation ratios between the genuine trait and the fake ones	Remarkable distributive statistical characteristic that satisfies a moderate entropy values	Vulnerable to the increase of noise disturbances One physical modality was tested (gray level only)
[44]	A biometric multi-template protection system based on variant discrete transformations as DFT, FrFT, DCT, and DWT plus a matrix rotation is employed to develop cancelable fingers and faces templates	Fingerprint patterns (CASIA v.2) Faces patterns (FERET, LFW)	DFT, FrFT, DCT, and DWT plus a matrix transformation	FRR = 0.003 FAR = 0.08 EER = 0.0023	Achieve the revocability and confusion criteria	Need to speed up the algorithm Sophisticated code implementation

Table 1 (continued)

Work	Illustration and Purposes	Biometric Patterns	Algorithm	Performance Measurements	Merits	Demerits
[61]	Different cancellable biometric schemes are employed on deep-learning extracted features	Various Biometric patterns	Bio-Hashing, Multi-Layer Perceptron (MLP) Hashing Bloom Filters, and two techniques were dependent on Index of Maximum Hashing (IoM)	FRR = 0.01 FAR = 0.001 EER = 2×10^{-3}	Resilience to spoof attacks	Time consumption was not considered during each method process There was no discussion on results in the presence of any kind of noise
[62]	multi-template protection based recognition technique was employed by several convolutional neural networks (CNNs)	Different regions of faces	Several CNNs were employed to extract deep traits from each face section, followed by a fusion network gathered these traits together	Average AROC = 97.14%	Likability and Irreversibility were satisfied	Suffers from processing time delay due to CNNs

Table 1 (continued)

Work	Illustration and Purposes	Biometric Patterns	Algorithm	Performance Measurements	Merits	Demerits
The Proposed Work	Provide a hybrid template protection scheme based on a hyperchaotic system and Fibonacci Q-matrix	Faces databases (ORL, FERET, LFW, and ICA) Ears databases (AMI, and IITD) Palmprints databases (CASIA, and IITD) Fingerprints databases (FVC, and CASIA) Iris databases (CASIA, and UPOL)	Dislocation of pixels' positions by hyperchaotic equations, then a change in the pixels' intensity by Fibonacci Q-matrix	$FRR = 1.202 \times 10^{-3}$ $FAR = 1.5 \times 10^{-4}$ $EER = 1.02 \times 10^{-4}$	1) Satisfies more randomization with appreciated histogram results and lower processing time 2) Better results have been achieved than related works 3) AROC = 0.9999 4) No glimpses of the licensed biometric features in the cancelable traits 5) Working on gray and color biometric templates 6) No need for image registration 7) Robustness to noise effect and data cut attacks	Large key space management

7. The disturbance influence as noise existence is not mentioned in almost whole relative studies.
8. Run duration is not calculated over almost whole cancelable biometric authentication systems.

These demerits enforced us to propose efficient hybrid cancelable biometric authentication techniques that face variant kinds of attacks. The uniqueness of our proposed work is summarized as follows:

1. The first exploitation of Fibonacci Q-matrix in the cancelable biometric research.
2. Employing six-dimensional hyperchaotic technique to obtain unrecognizable features to the deceived persons as well as keep the original traits safe away any intruder.
3. The implementation of both six-dimensional hyperchaotic approach and Fibonacci Q-matrix adds more secure to the authentication-based system.
4. The large key space of the proposed technique satisfies well immune against the brute force attacks.
5. The ease implementation accompanied by obtaining good cancelable based recognition results as well as remarkable security evaluation assessments.
6. The proposed cancelable biometric algorithm achieves flat histograms for the protected templates gaining more resistance against statistical attacks contrary with other mentioned cancelable techniques.

3 Preliminary concepts

This part illustrates the principles of the usage of 6D hyperchaotic technique, and the definition of Fibonnaci Q-matrix.

3.1 6D Hyperchaotic technique

The statistical distribution exposes that the behavior of chaotic equations suffers from nonlinearity characterization. Thus, the response analysis is random. The previously related works of hyperchaotic techniques are emphasized that the random statistical response of hyperchaotic functions is more sophisticated compared with the response of ordinary chaotic functions. Therefore, the hyperchaotic approach must possess an equal or more than 4-dimensional system. Furthermore, the ordinary chaotic systems of low dimensional mathematical implementation are derived by a lone positive Lyapunov exponent, however the hyperchaotic approaches possess two or more positive Lyapunov exponents [8]. The authors in [45], identified the six-dimensional hyperchaotic approach by the group of the following equations:

$$\begin{aligned} y_1 &= k(y_2 - y_1) + y_4 - y_5 - y_6 \\ y_2 &= my_1 - y_2 - y_1y_3 \\ y_3 &= -ly_3 + y_1y_2 \\ y_4 &= ny_4 - y_2y_3 \\ y_5 &= py_6 + y_3y_2 \\ y_6 &= qy_1 \end{aligned} \tag{1}$$

where k,l,m,n,p, and q are constant values whereas y_1, y_2, y_3, y_4, y_5, and y_6 define the six phases values of the six dimensional hyperchaotic approach. In this chapter, the involved constants are estimated by $k=10$, $l=8/3$, $m=28$, $n=-1$, $p=8$, and $q=3$. These elected constant values to guarantee the existence of two positive Lyapunov exponents over the system, where the condition of the sum of whole obtained exponents is negative has been satisfied.

3.2 Fibonacci Q-matrix

The components of Fibonacci array, $F_{n,}$ are [46]:

$$F_n = F_{n-1} + F_{n-2}, n > 1 \tag{2}$$

where $F_0 = F_{1=}$ 1. The Fibonacci Q-matrix is defined by:

$$\boldsymbol{Q} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{3}$$

The nth power of Fibonacci Q-matrix is estimated by the next matrix:

$$\boldsymbol{Q}^n = \begin{bmatrix} Fn+1 & Fn \\ Fn & Fn-1 \end{bmatrix} \tag{4}$$

where as F_n is the Fibonnaci value, and the determinant of the Fibonnaci Q-matrix is evaluated by:

$$Det(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n \tag{5}$$

4 The proposed hyperchaotic technique and fibonacci q-matrix based cancelable biometric approach

The novel scheme is employed a six-dimensional hyperchaotic technique and Fibonacci Q-matrix to deform the genuine trait. Because of the high level of randomness which is achieved by the hyperchaotic system due to the bilateral positive Lyapunov exponents. Thus, it increases the privacy level without affecting the cancelable assessments. Furthermore, the implementation of Fibonacci Q-matrix is very feasible, quick run, and has the ability to diffuse the deformed pixels. Figure 3 exposes the methodology stages during its run.

The cipher scheme is based on two phases that are confusion then diffusion. The pixel location and intensity are altered due to both properties, respectively. First of all, six dimensional hyperchaotic scheme is responsible for satisfying the confusion phase by initially progress the estimation of preliminary condition according to the applied system is achieved by means of the original pattern details. After that a novel vector is acquired after two iterations of processing the hyperchaotic equations, and then the election of three sequences is proceeded by y_1, $y_{3,}$ and y_5. The resultant vector is considered as the altered locations values for current pixels locations of the genuine pattern. So this vector is kept away in any cloud database. Second, the phase of diffusion comes up to spread

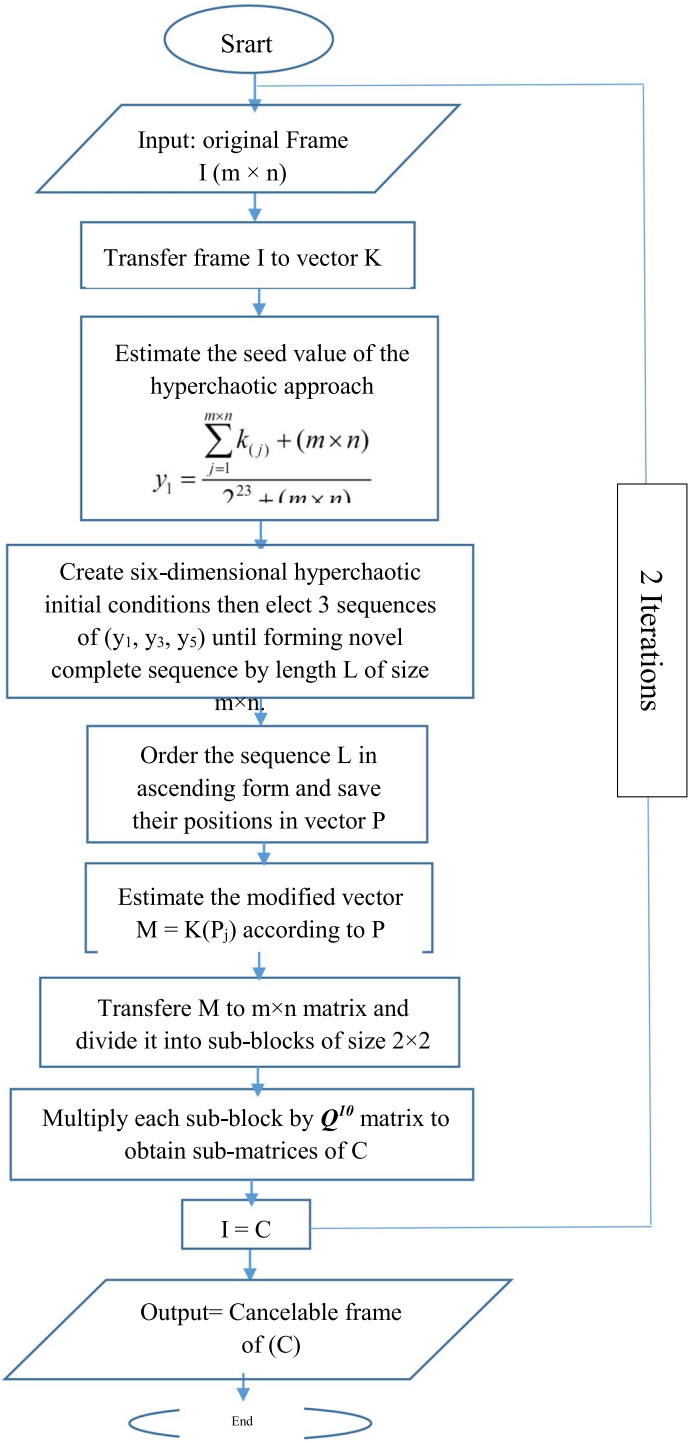


Fig. 3 The flow chart of the proposed cancelable biometric technique

Input: Original frame (I) of size (m×n).

Output: Cancelable frame (C).

01: ***for*** *r*= 1 to 2, ***do***

02: Convert the pattern's frame to vector ***K*** by estimating initially the seeds of hyperchaotic approach as following:

03: $y_1 = \dfrac{\sum_{j=1}^{m\times n} k_{(j)} + (m\times n)}{2^{23} + (m\times n)}$, y_j = mod (y_{j-1} ×10^6, 1) j=2, 3, ….,6. To obtain the initial conditions of y_2, y_3, y_4, y_5, y_6 then repeat the step 3 almost m×n/3 rounds to obtain a novel sequence of chaotic variables of length L= m×n because we choose three sequences of y_1, y_3, y_5 to be proceeded.

04: Arrange the resultant L in the form of ascending then store their positions in the position vector P.

05: Recreate the frame vector K by utilizing the position vector of P to obtain a novel permuted vector of M by Mj = K (Pj), j= 1 to (m×n).

06: Transfer the permuted sequence M to a 2-dimensional array M', then derived the sub-blocks of size 2×2.

07: Multiply each sub-block by nth power Fibonacci Q-matrix of Q10 to get the sub-blocks of C as following:

$$\begin{bmatrix} C_{i,j} & C_{i,j+1} \\ C_{i+1,j} & C_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} M'_{i,j} & M'_{i,j+1} \\ M'_{i+1,j} & M'_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix} mod\ 256.$$

Where i=1, 3,……., m, j=1, 3,……, n.

08: Construct the final cancelable frame of C.

09: Let *r*=*r*+*1*.

10: ***end for***

Algorithm 1 The proposed pattern cancelable approach.

the replacement effect or confused pixels over the whole pattern. This diffusion process is accomplished here through the employment of Fibonacci Q-matrix by dividing the confused pattern into 2×2 sub-blocks. Each sub-block is suffered from a diffusion for its pixels levels by using the equations through 2 to 5. As well as, two iterations of diffusion is progressed to produce the cancelable biometric pattern. The cipher based cancelable scheme is illustrated in Algorithm 1 showing its two phases' procedures.

5 The applied evaluation metrics

5.1 Authentication evaluation metrics

The vital quality factor of examining the cancellable features is the visual inspection, where good cancelable templates are due to highly hidden features for the proposed cancelable biometric cryptosystem. Cancelable traits efficiency is not based only on visual evaluation. So, different measurements are involved in detecting the progress of the cancelable biometric framework. Correlation ratios evaluate the symmetry of the registered biometric

feature with the input biometric trait. The higher the value of coefficient, the higher will be the resemblance between the both groups of features. If the resemblance ratio of the examined client is above a specific threshold, the entrance into the system is acceptable. Thus, the resultant value of symmetry for a licensed user must be greatly more than the value of symmetry due to a foreigner seeking to get into the system. A one threshold value would be efficient to differentiate between the two classes of the tested data classified into licensed users and unlicensed clients [1].

The accomplishments of the proposed cancelable biometric authentication frameworks can be estimated by the receiver operating characteristic (ROC) curve. The ROC curve demonstrates the divergence between the true positive ratio (TPR) and the false-positive ratio (FPR) [47, 48]. The analysis of the ROC curve is dependent on a decision variable. The examined data consists of licensed and unlicensed patterns in any biometric authentication system so that each protected template has pixels intensities would be spread around a dedicated mean value. Therefore, the probability distribution of the licensed patterns due to symmetry coefficients is higher than the probability distribution of the fake patterns. Thus, we are obligated to employ the distribution evaluation of the probability density in our proposed work. Furthermore, the symmetry factors obtained from the verification test are involved in the PFD (probability of the fake distribution) and the PTD (probability of the true distribution) [1].

Variant of alternatives are affected in pixel intensities evaluation comparing with their initial values before applying the proposed template protection scheme. This illustrates that the more the divergence in pixel intensity and dislocations are applied, the more influence the biometric template protection scheme will gain, and consequently, more privacy and confidentiality will be obtained [1].

Besides, the template protection progress is tested by evaluating the symmetry ratios, and the shape of data randomness using histogram analysis of the protected and genuine patterns. In the following sub-sections, these estimated criteria of various verification measurements are achieved to evaluate the efficiency of the proposed biometric template protection schemes. The authentication analysis for the suggested cancelable schemes is introduced in terms of variant of seven criteria, (A) Visual assessment, (B) Histogram analysis, (C) PTD and PFD, (D) Symmetry coefficients, (E) FAR, FRR, EER, and AROC analysis, (F)The effect of noise existence (G) Estimated processing time.

All simulations are progressed on various biometric features with different sizes, gray and colored Faces [49–51], Ears [52, 53], Iris [54, 55], Fingers [56, 57], and Palmprints [58, 59] are tested on MATLAB platform (R2019b) with a computer specified by Core i5-2430 M 2.4 GHz CPU and 4 GB RAM, on different sizes of gray, and colored scale biometric patterns. The verification metrics are employed in estimating the reliability of the proposed cancelable biometric authentication frameworks will be exposed in detail as following:

5.1.1 Visual assessment

A visual assessment is a kind of traditional evaluations to prove the results quality of the cancelable algorithm by the naked eye. This type of evaluation does not need any calculations or special formulations. So, the efficient output of deformed patterns can be detected easily as a first step of evaluation. In principle, if the protected template is fully deformed, then its template protection algorithm has the superiority over the other cancelable schemes.

Figures from 4, 5, 6 7 and 8 show the visual effect on the protected patterns of the tested biometric samples with the proposed algorithm, GA and RNA-GA cancelable schemes. Due to the five physical features; Faces, Ears, Fingerprints, Iris, and Palmprints, respectively, it is obvious that the proposed model has the superiority over both GA [1], and RNA-GA [3] comparative studies. Therefore, the proposed template protection technique can be used to achieve an ultimate defense against cracking attempts. The proposed biometric template protection framework satisfies full deformation for the genuine physicals to be then kept remotely away hackers.

5.1.2 Histogram analysis

The histogram is considered as the visual representation of pattern pixels' intensities in the biometric template. The histogram must own two vital specifications for the protected biometric features that is essentially based on applied cipher, transformation or both schemes [3]:

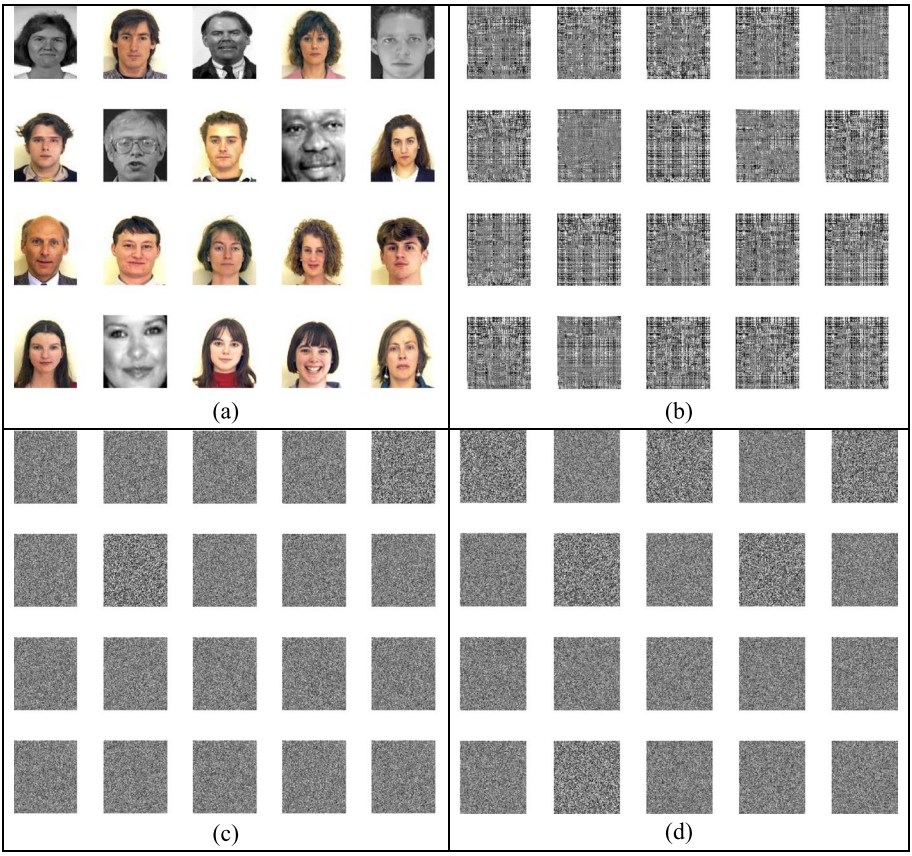


Fig. 4 Visual results of the Faces samples: (**a**) Original Faces features, (**b**) Cancelable Faces due to GA [1], (**c**) Cancelable faces due to RNA-GA [3], and (**d**) Cancelable faces due to the proposed model

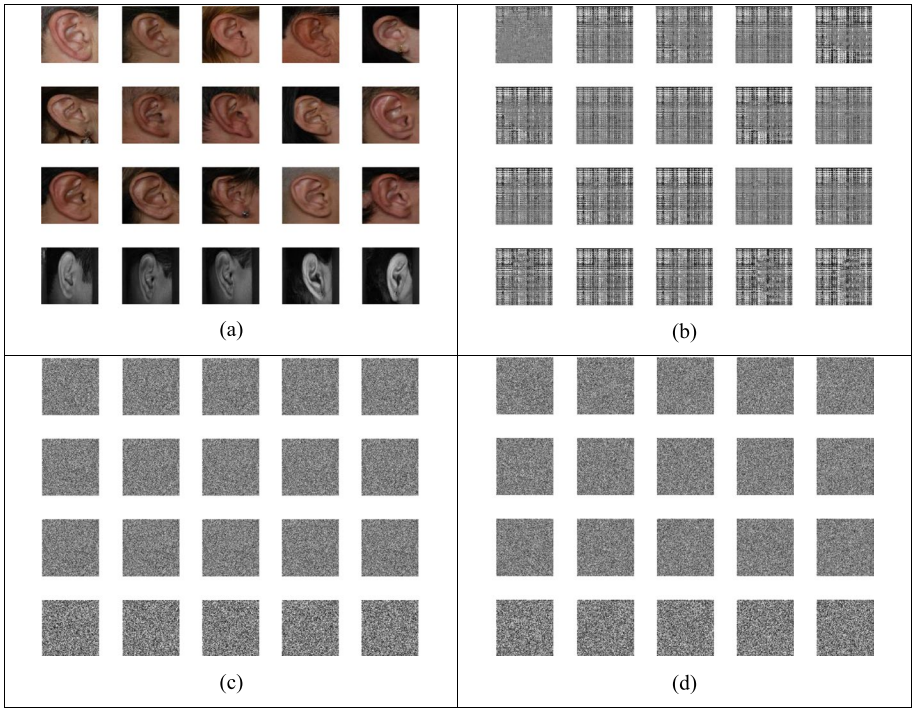


Fig. 5 Visual results of the Ears samples: (**a**) Original Ears features, (**b**) Cancelable Ears due to GA [1], (**c**) Cancelable Ears due to RNA-GA [3], and (**d**) Cancelable Ears due to the proposed model

1. The histogram of the cancelable biometric pattern is completely different from the histogram of the original biometric trait.
2. It is preferred to possess more flat distribution, which increases the degree of randomness of the whole pixels' intensities.

Histograms of the genuine, and their related protected patterns by the suggested and the compared algorithms are shown in Figs. 9, 10, 11, 12 and 13. It is concluded that the patterns resultant from the proposed template protection algorithm have uniform histogram shapes.

5.1.3 Correlation coefficients

Correlation practically defines as the ratio of the similar details between the two patterns. In template protection techniques, we may create various deformed patterns for the same feature by choosing different cipher scheme or another transfer matrix or both together to be employed as a hybrid scheme. Resultant cancelable features for the same pattern must not be similar to each other of the various applied cancelable schemes, but they must have high correlation ratio between the deformed versions of the stored genuine trait and its tested feature resultant after employing the same cancelable technique. As well as, they would have low correlation ratio between the deformed versions of the stored genuine trait and the unlicensed tested feature resultant from the same template protection technique [2].

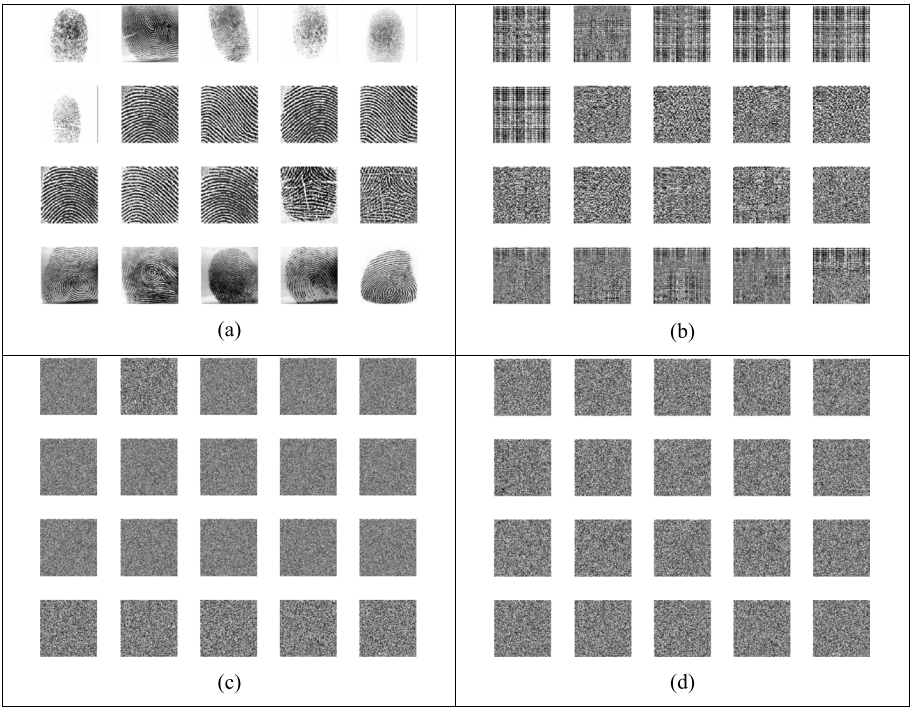


Fig. 6 Visual results of the Fingerprints samples: (**a**) Original Fingerprints features, (**b**) Cancelable Fingerprints due to GA [1], (**c**) Cancelable Fingerprints due to RNA-GA [3], and (**d**) Cancelable Fingerprints due to the proposed model

$$C_c(P1, P2) = \frac{M((P1 - M(P1))(P2 - M(P2)))}{\sqrt{D(P1)D(P2)}} \tag{6}$$

where,

$$M(P) = \frac{1}{k}\sum_{i=1}^{k} p_i \tag{7}$$

$$D(P) = \frac{1}{k}\sum_{i=1}^{k} (p_i - M(P))^2 \tag{8}$$

As shown in Eqs. (6), and (7), and (8), C_c is the correlation coefficient between the two cancelable patterns **P1**, and **P2**. M (**P**) estimates the mean value of **P1**, and **P2** while k is the total no. of pixels in each **P1**, or **P2** [2]. D (**P**) evaluates the variance for each **P1**, and **P2**, respectively. Two resultant statuses in the similarity examination will be obtained as below:

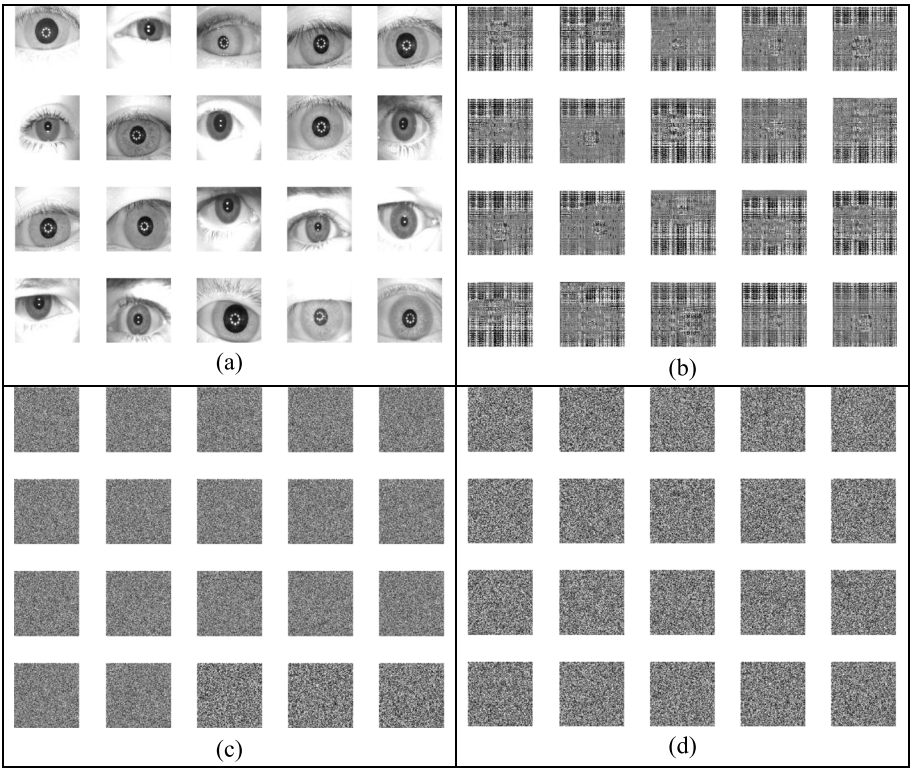


Fig. 7 Visual results of the Iris samples: (**a**) Original Iris features, (**b**) Cancelable Iris due to GA [1], (**c**) Cancelable Iris due to RNA-GA [3], and (**d**) Cancelable Iris due to the proposed model

1. When the correlation ratio (C_c) is equal or near ± 1, it demonstrates the optimum ratio, which occurs only if two biometric patterns are symmetric or highly dependent. This expected result will be obtained at the verification step for licensed access scenarios.
2. The C_c value is near or equal to 0, while there is a significant change between the licensed biometric pattern and its deformed version through the enrollment phase, where the deformed biometric template is extremely independent of the genuine one, on the other hand, this expected result is also presented through the verification step due to the unlicensed access scenarios [1].

Table 2 validates the average of similarity ratios resulted by the genuine and imposter tests. The resultant similarity ratios provide significant increase in their values due to the proposed protected model in the case of genuine test and a severe decrease in the coefficient values for the case of imposter test compared with their results due to the relative studies. This proposed model provide the best authentication results corresponding to the similarity test of the overall tested physical features even over the both related studies of GA, and RNA-GA.

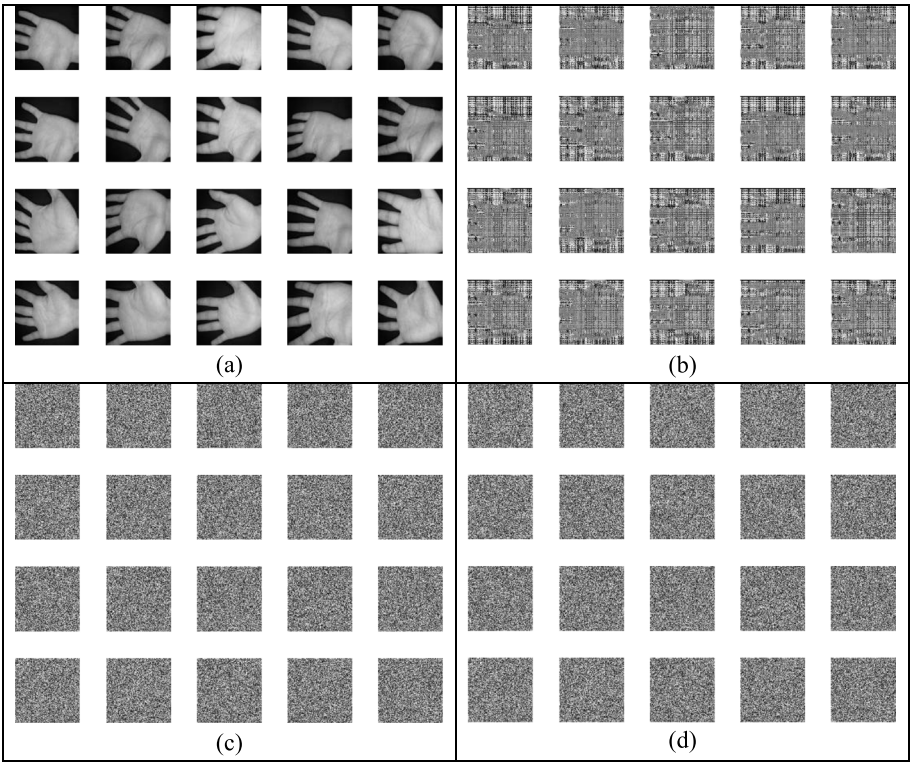


Fig. 8 Visual results of the Palmprints samples: (**a**) Original Palmprint features, (**b**) Cancelable Palmprint due to GA [1], (**c**) Cancelable Palmprint due to RNA-GA [3], and (**d**) Cancelable Palmprint due to the proposed model

5.1.4 The true and the fake probabilities distribution

The TPD is the prospect similarity distribution of the deformed licensed patterns (true features) through the registered veiled patterns in the database. The FPD is the prospect similarity ratios' distribution of the unlicensed patterns (foreigners' features) through the registered veiled traits in the database. Thus, the decision of two biometric patterns are owned by the same client or not is dedicated by the correlation coefficients, when the identification is achieved between two cancelable patterns for the same client, this is called a true\ positive identification. On contrary, when the identification is proved between two various clients, this is defined by a false \fake identification process. Probability distribution analysis (PDF) is employed to classify the symmetry over intruders and authorized patterns according to their correlation coefficients. Therefore, the authorized patterns have significant increase in similarity ratios. The verification phase is processed according to PDF classification. A point is chosen precisely to differentiate accurately between the false distribution (FD), and the true distribution (TD). This threshold is resultant from the graph combining the FPD, and TPD curves which are dependent on the proposed deformation algorithm. Access to the protected data is inhibited, if the symmetry ratio of the tested feature decreases under the threshold level [3].

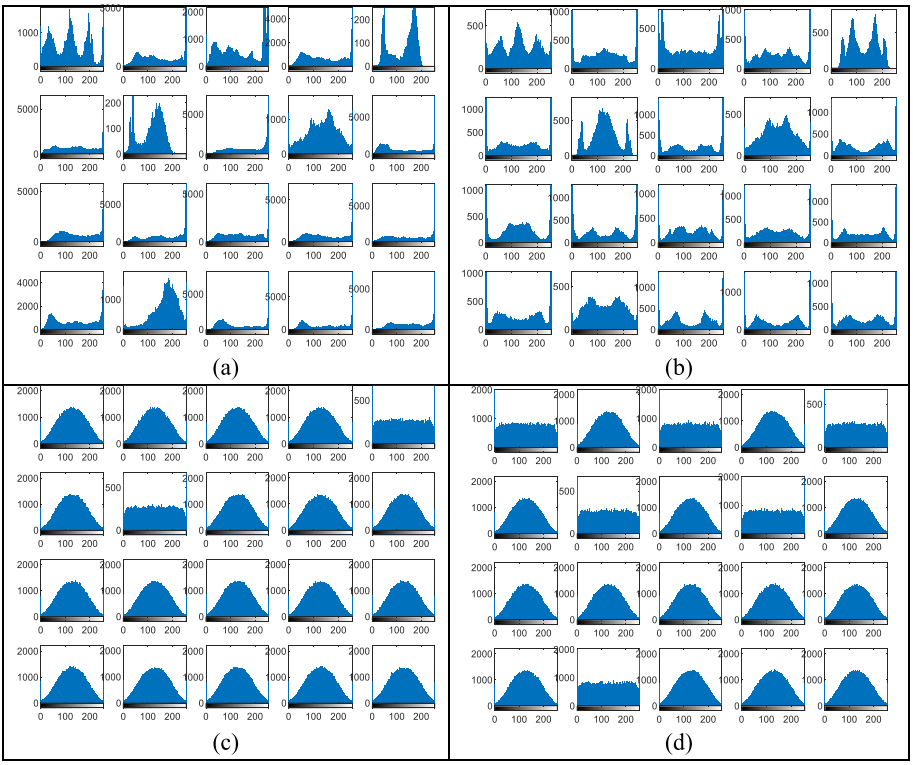


Fig. 9 Histograms of the Faces samples: (**a**) Original histogram, (**b**) Histogram of the protected Faces due to GA [1], (**c**) Histogram of the protected Faces due to RNA-GA [3], and (**d**) Histogram of the protected Faces due to the proposed model

If the imposter ratio is obtained higher than the threshold value, then it is called a False Acceptance (FA), as well as when the licensed ratio is achieved lower than the threshold coefficient, this is defined as False Rejection (FR) as shown in relations 9, and 10. Whereas *FP, FN, TP,* and *TN* are the False Positive, False Negative, True Positive, and True Negative clients, respectively. When the separation distance between the FD curve and the TD curve is very narrow or their curves intersect, it is sophisticated to estimate the threshold point accurately. Consequently, the False Acceptance Rate (FAR), and the False Rejection Rate (FRR) will be highly increased which lead to lower efficiency and sometimes a whole authentication system failure [2].

$$FAR = \frac{FP}{FP + TN} \tag{9}$$

$$FRR = \frac{FN}{TP + FN} \tag{10}$$

Figure 14 exposes the distribution of the genuine and fake correlation ratios for the proposed template protection model, as well as the cancelable models based on GA and RNA-GA algorithms over the whole tested biometric modalities. The obtained plots investigate that the distance between both distributions is away enough due to our proposed template

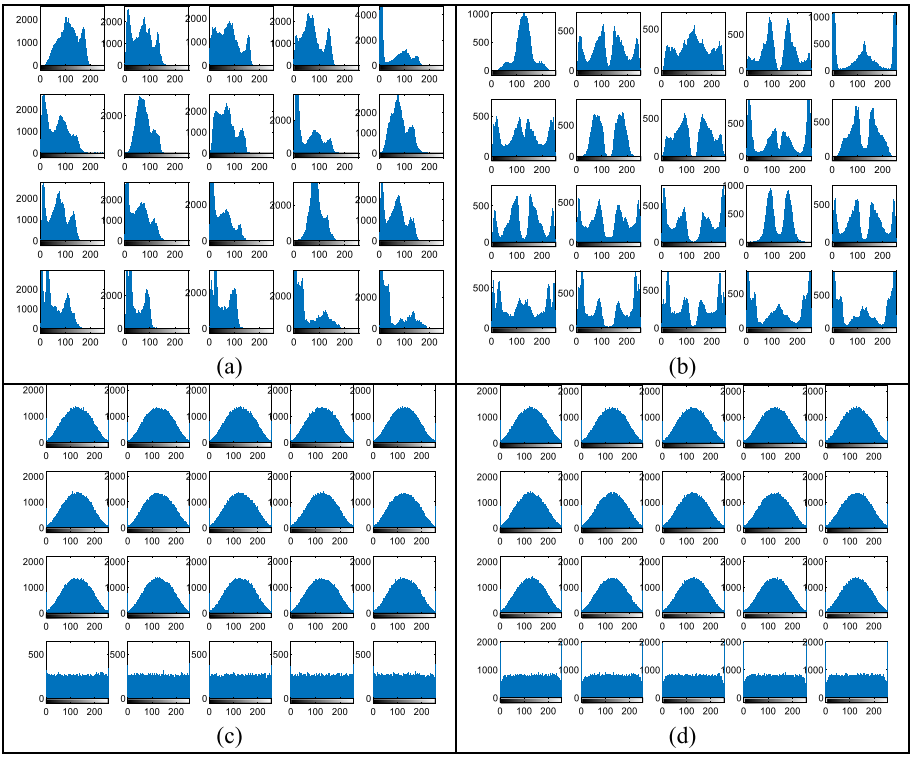


Fig. 10 Histograms of the Ears samples: (**a**) Original histogram, (**b**) Histogram of the protected Ears due to GA [1], (**c**) Histogram of the protected Ears due to RNA-GA [3], and (**d**) Histogram of the protected Ears due to the proposed model

protection algorithm than the other two comparative studies. It is obvious in the elongation provided by the eccentricity of the two curves (PDF of TD, and FD). That validates the powerful capability of our template protection framework based on hyperchaotic and Fibonacci Q-matrix methodology to differentiate between the licensed and unlicensed clients through any acquired authentication test.

Moreover, In Table 3, a summary for the various FAR, and FRR of the whole tested physical templates for the processed cancelable methods applied in this research. These assessments validate our proposed work by the minimum obtained rates for false approved/unapproved users. Thus, some resultant fake rates are decreased which is considered a remarkable merit acquired by the proposed scheme compared with the resultant FAR, and FRR due to the proposed GA, and RNA-GA based cancelable approaches.

5.1.5 The analysis of receiver operating characteristic curve (ROC)

It is a plot between the sensitivity, (true positive ratio) along y-coordinate, which is introduced by a mathematical relation of the specificity, (false positive ratio) along x-coordinate, over variant intersection points. So, every point on the ROC signifies a specificity/sensitivity pair corresponding to an estimated threshold [3]. The accuracy is then calculated from the Area under the ROC curve, in other words, it is the relative

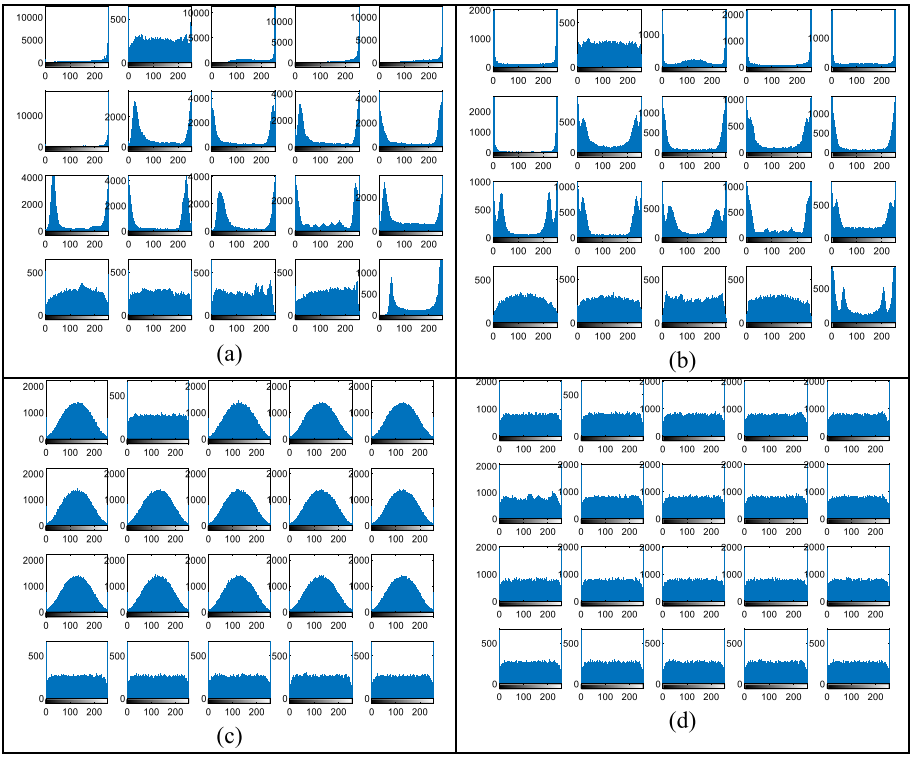


Fig. 11 Histograms of the Fingerprints samples: (**a**) Original histogram, (**b**) Histogram of the protected Fingerprints due to GA [1], (**c**) Histogram of the protected Fingerprints due to RNA-GA [3], and (**d**) Histogram of the protected Fingerprints due to the proposed model

relation of true verification results w.r.to all output possibilities as shown in the relation 11. The intersection points in which the balance between false acceptance rate (FAR), and false rejection rate (FRR) is achieved [2]. This balance is defined by the Equal Error Rate (EER) respective to the applied cancelable scheme.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

Figure 15 exposes also the received operating characteristic plots of the tested protected templates according to the template protection approaches which are applied by the proposed scheme, GA, and RNA-GA. The results reveal higher recognition accuracy based on the proposed approach.

Tables 4, 5, 6, 7 and 8 conclude the resultant values of EER, and AROC respectively over different levels of noise disturbances to validate the reliability of the proposed method. As well as Table 9 illustrates the average time consumed through the run of the proposed algorithm and its comparative studies of GA, and RNA-GA. The results register the superiority of our proposed algorithm.

These results prove that the suggested template protection approach has a significant robustness against various degrees of noise disturbance, from 0.01 Gaussian distributive

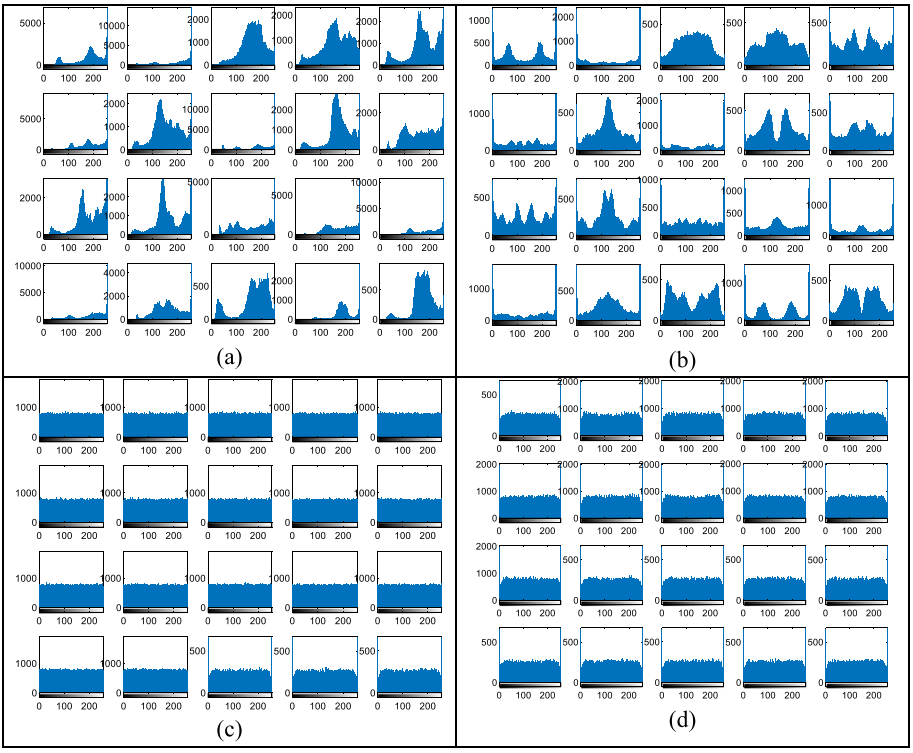


Fig. 12 Histograms of Iris samples: (**a**) Original histogram, (**b**) Histogram of the protected Iris due to GA [1], (**c**) Histogram of the protected Iris due to RNA-GA [3], and (**d**) Histogram of the protected Iris due to the proposed model

noise to level of 0.05, which is investigated by the least resultant EER and the largest AROC over different noise levels compared with the results due to comparative algorithms.

From the previous measurements, our proposed scheme achieves good authentication results with least time consumed through its run.

5.2 5.2. Security evaluation metrics

5.2.1 5.2.1. Entropy Assessment

The alignment degree of histogram lead to a desired diversity of pixels intensities for the protected features. This diversity is estimated by entropy value. The entropy values range through the interval [0, 8]. The minimum value is zero which means no random data would be obtained in the resultant cancelable pattern, and so it degrades until reaches the optimum value of 8. Thus, the higher the entropy, the more distinction the template distribution suffers from. Therefore, the reliable cipher scheme should satisfy a pattern entropy up or near 8 [60].

The pattern randomness estimated by the entropy is investigated in the following Eq. 12:

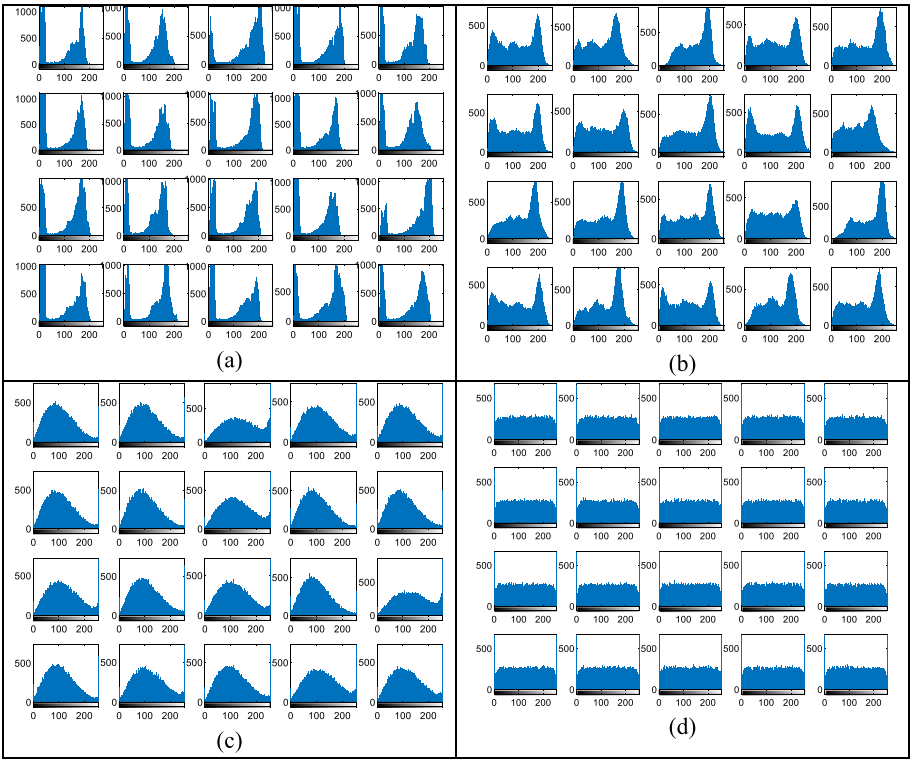


Fig. 13 Histograms of Palmprints: (**a**) Original histogram, (**b**) Histogram of the protected Palmprints due to GA [1], (**c**) Histogram of the protected Palmprints due to RNA-GA [3], and (**d**) Histogram of the protected Palmprints due to the proposed model

Table 2 Average Correlation coefficients by the three cancelable biometric techniques

Biometric Modalities	Unlicensed Users			Licensed Users		
	GA [1]	RNA-GA [3]	Hyperchaotic and Fibonacci Q-matrix	GA [1]	RNA-GA [3]	Hyperchaotic and Fibonacci Q-matrix
Faces	-0.17319	0.01395	-5.75×10^{-04}	0.95248	0.89678	0.93691
Ears	1.64×10^{-04}	0.00294	5.97×10^{-04}	0.81730	0.90263	0.90672
Fingerprints	-0.14464	-0.02579	-0.00138	0.96871	0.90719	0.94908
Iris	0.08284	-0.06476	-0.00108	0.95262	0.89809	0.94918
Palm prints	0.10011	1.33×10^{-04}	-0.00214	0.94435	0.95885	0.96886

$$E(p) = \sum_{n=1}^{2^k-1} P(p_n) log_2 \frac{1}{P(p_n)} \tag{12}$$

where p_n is the pattern pixel, $P\ (p_n)$ is the probability of pixel existence, and the whole number of pixels are defined by k. whereas 2^k is the total possibilities of p_n.

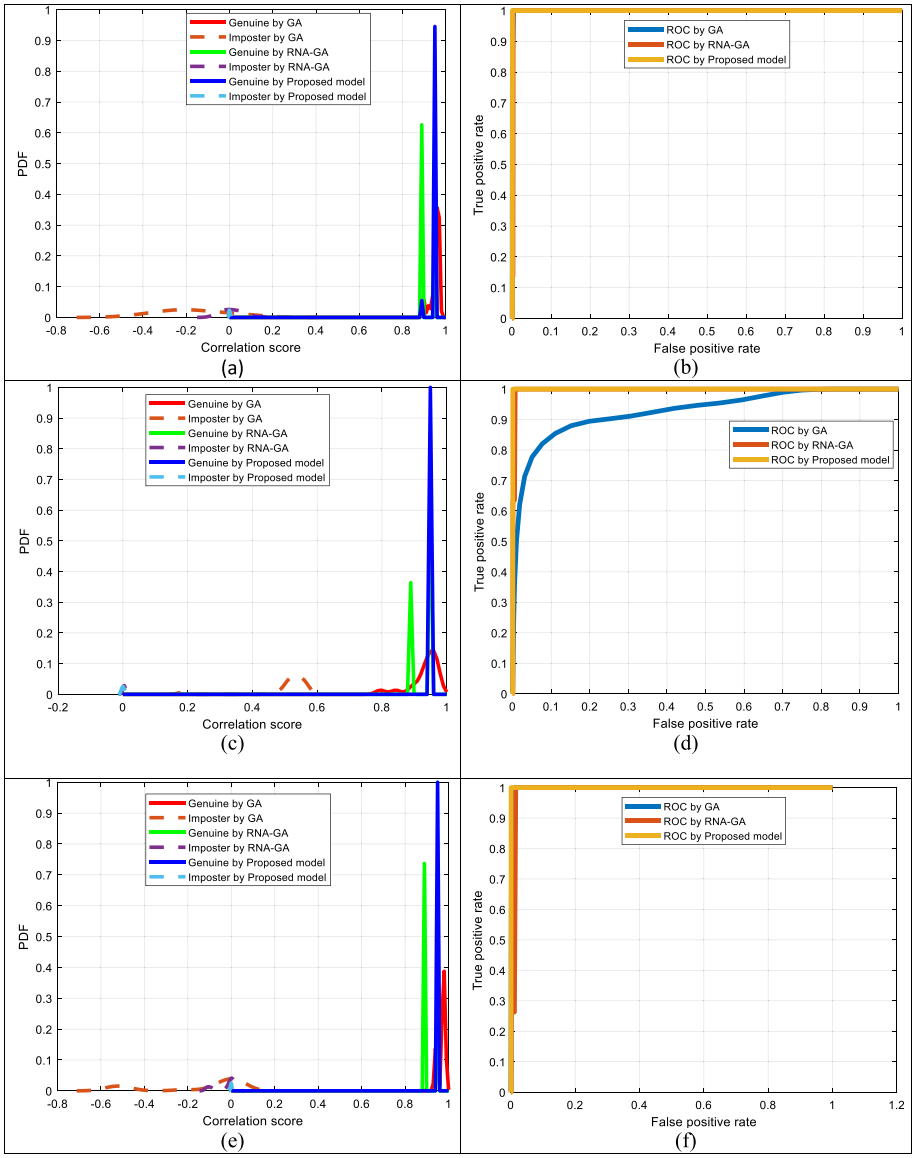


Fig. 14 PDF and ROC curves of cancellable five features due to proposed GA, RNA-GA, and Hyperchaotic and Fibonacci Q-matrix algorithms respectively. (**a**) and (**b**) for cancellable faces. (**c**) and (**d**) for cancellable ears. (**e**) and (**f**) for cancellable fingerprints. (**g**) and (**h**) for cancellable iris. (**i**) and (**j**) for cancellable palmprints

Table 10 exposes the average resultant entropy of the resultant biometric patterns generated in the proposed template protection approach and the other approaches based on GA and RNA-GA. It is remarked that the entropy values of the generated biometric patterns by the proposed scheme based on hyperchaotic, and Fibonacci Q-matrix are

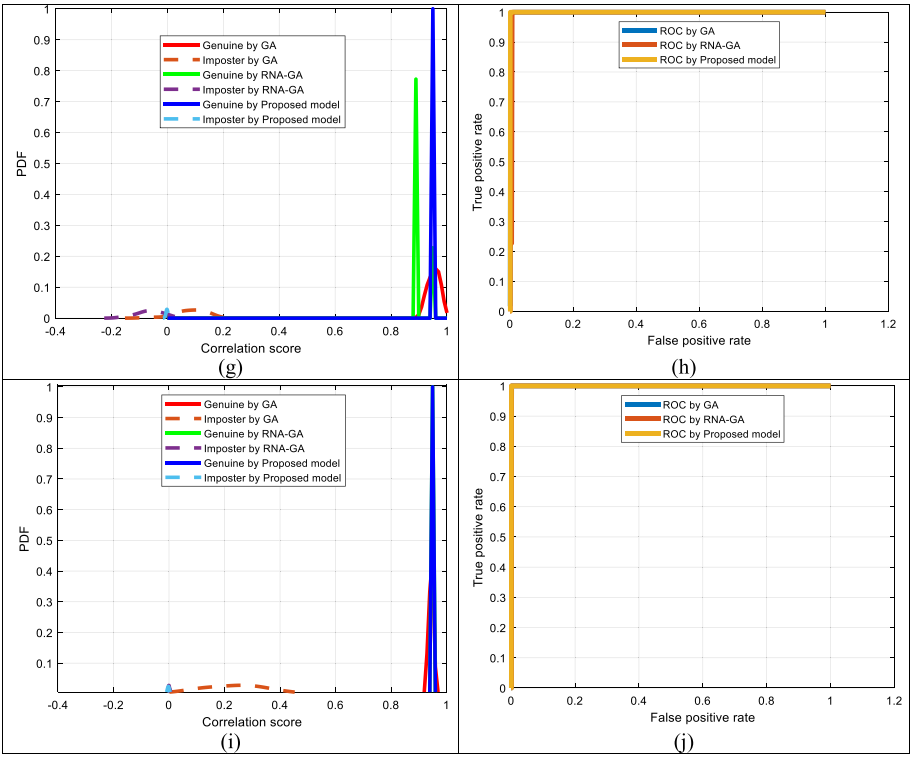


Fig. 14 (continued)

Table 3 Comparison of FAR and FRR between the triplet cancelable studies

Physical Modalities	FAR			FRR		
	GA [1]	RNA-GA [3]	Hyperchaotic and Fibonacci Q-matrix	GA [1]	RNA-GA [3]	Hyperchaotic and Fibonacci Q-matrix
Faces	0.00034	0.0024	0.00313	0.00028	0.0663	0.00241
Ears	0.10975	0.00677	0.00101	0.01805	0.03379	0.2510
Fingerprints	0.00113	0.01544	7.9663×10^{-04}	0.00254	0.27306	0.3103
Iris	0.00791	0.00749	8.329×10^{-04}	0.00246	0.07655	0.19618
Palmprints	0.00205	$6.14 \times 10–^{04}$	0.00116	8.84×10^{-04}	0.03027	0.00273

most near to 8 (the optimum value). This investigates highly random cancelable pixels which adds more unfeasibility to be optimized.

5.2.2 NPCR and UACI Assessments

The intruders seek to recognize and get the authority to access the cancelable data in the stored database without knowing the cipher matrix (key) or scheme. Thus, they can

Table 4 The resultant accuracy and EER of the three cancelable systems over different levels of noise disturbance due to tested faces

	EER			AROC		
Noise Variance	GA [1]	RNA-GA [3]	**Proposed model**	GA [1]	RNA-GA [3]	**Proposed model**
0.0	0.0011	0.01047	**0.0012**	0.9995	0.99953	**0.9998**
0.01	0.0139	0.03087	**0.0016**	0.9994	0.99940	**0.9996**
0.02	0.0054	0.03115	**0.0099**	0.9971	0.99776	**0.9841**
0.03	0.0109	0.03698	**0.1060**	0.9920	0.99276	**0.9563**
0.04	0.0119	0.03924	**0.1073**	0.9842	0.99022	**0.8880**
0.05	0.0131	0.04039	**0.1284**	0.9727	0.98242	**0.8957**

Table 5 The resultant accuracy and EER of the three cancelable systems over different levels of noise disturbance due to tested ears

	EER			AROC		
Noise Variance	GA [1]	RNA-GA [3]	**Proposed model**	GA [1]	RNA-GA [3]	**Proposed model**
0.0	0.0051	0.0051	**0.0113**	0.9505	0.9998	**0.9995**
0.01	0.0323	0.0747	**0.0439**	0.9332	0.9991	**0.9994**
0.02	0.1590	0.1399	**0.0881**	0.8841	0.9688	**0.9778**
0.03	0.2478	0.2132	**0.1043**	0.8505	0.9463	**0.8835**
0.04	0.2811	0.2954	**0.2004**	0.8203	0.8382	**0.7992**
0.05	0.3269	0.3138	**0.2862**	0.7907	0.8235	**0.7475**

Table 6 EER and AROC of the employed cancelable studies corresponding to Fingerprint samples

	EER			AROC		
Noise Variance	GA [1]	RNA-GA [3]	**Proposed model**	GA [1]	RNA-GA [3]	**Proposed model**
0.0	0.0063	0.0053	**0.0083**	0.9995	0.9998	**0.9999**
0.01	0.0135	0.3260	**0.0668**	0.9992	0.9996	**0.9998**
0.02	0.0270	0.4521	**0.3001**	0.9887	0.9991	**0.9997**
0.03	0.0365	0.4669	**0.3211**	0.9669	0.9293	**0.9996**
0.04	0.0444	0.5650	**0.3999**	0.9314	0.8924	**0.9889**
0.05	0.0494	0.5848	**0.4730**	0.8924	0.8378	**0.9726**

try to discover the connection between the genuine data, if they could succeed to obtain a one sample of genuine user, and the ciphered details. So, when the minimum pixels change their value in the genuine pattern, this will affect severely the pixels distribution intensity in the ciphered trait, and consequently the hacking process against the whole stored data will be sufficiently unfeasible. Efficient cancelable techniques must have the ability to face this attack. The robustness assessments against this kind of attacks

Table 7 EER and AROC of the employed cancelable studies corresponding to Iris samples

	EER			AROC		
Noise Variance	GA [1]	RNA-GA [3]	**Proposed model**	GA [1]	RNA-GA [3]	**Proposed model**
0.0	0.0111	0.0113	**0.0113**	0.9999	0.9999	**0.9999**
0.01	0.0020	0.0201	**0.1735**	0.9999	0.9998	**0.9999**
0.02	0.0100	0.0387	**0.2005**	0.9990	0.9728	**0.9950**
0.03	0.0152	0.0642	**0.2008**	0.9818	0.9220	**0.9950**
0.04	0.0211	0.0929	**0.2071**	0.9614	0.8498	**0.9811**
0.05	0.0248	0.1788	**0.3611**	0.9279	0.7765	**0.8767**

Table 8 EER and AROC of the employed cancelable studies corresponding to Palmprints samples

	EER			AROC		
Noise Variance	GA [1]	RNA-GA [3]	**Proposed model**	GA [1]	RNA-GA [3]	**Proposed model**
0.0	1.1359×10^{-04}	0.01096	**0.00110**	0.9998	0.9999	**0.9999**
0.01	8.4285×10^{-04}	0.05119	**0.00511**	0.9993	0.9995	**0.9997**
0.02	0.00413	0.05602	**0.00730**	0.9958	0.9980	**0.9990**
0.03	0.00765	0.06143	**0.01342**	0.9866	0.9889	**0.9885**
0.04	0.01466	0.07248	**0.02658**	0.9691	0.9764	**0.9739**
0.05	0.03211	0.10015	**0.02937**	0.9441	0.9630	**0.9597**

Table 9 The processing time due to the implemented cancelable systems

Applied Approaches	Run Durations (in sec.)				
	Faces	Ears	Fingerprints	Iris	Palmprints
GA [1]	75.6220×10^{-2}	33.1037×10^{-2}	35.8245×10^{-2}	65.2867×10^{-02}	8.4296×10^{-02}
RNA-GA [3]	805.218×10^{-2}	91.2810×10^{-2}	88.8245×10^{-2}	122.28×10^{-02}	20.014×10^{-02}
Hyperchaotic and Fibonacci Q-matrix	66.361×10^{-3}	52.910×10^{-3}	50.193×10^{-3}	52.814×10^{-03}	42.01×10^{-03}

are demonstrated by the Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) as shown [8]:

$$NPCR = \frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M} DIF(i,j)\times 100(\%) \tag{13}$$

Table 10 Resultant entropy of the original, and various deformed biometric patterns due to the applied approach and the comparative studies

Entropy				
Physical Modality	Original Patterns	Deformed Patterns due to GA	Deformed Patterns due to RNA-GA	Deformed Patterns due to proposed model
Faces	7.02198	7.86077	7.8876	7.74862
Ears	6.92670	7.74040	7.8379	7.73300
Fingerprints	6.67250	7.54260	7.7310	7.73100
Iris	5.46150	7.82230	7.8695	7.95480
Palmprints	6.96390	7.88690	7.9741	7.95630

$$UACI = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{\left| I_2(i,j) - I_1(i,j) \right|}{N-1} \times 100\% \tag{14}$$

while,

$$DIF(i,j) = \begin{cases} 0, I_2(i,j) = I_1(i,j) \\ 1, I_2(i,j) \neq I_1(i,j) \end{cases} \tag{15}$$

$\mathbf{I_1}$ resembles to the cipher pattern which is encrypted from the same genuine feature. Whereas $\mathbf{I_2}$ resembles to the cipher pattern of the genuine template after alternating one pixel only [8]. Thus, the stored cancelable patterns can withstand this popular kind of hacking, if these security measurements reach the optimum values [8]. For NPCR, it reaches 99.5693%, while UACI ranges from 30.2824% to 33.6447% for efficient image cryptography of pattern size 256×256.

Tables 11 demonstrates the average values of NPCR and UACI results that are satisfied almost the optimum values. Their values provide an average of 99.0271% for NPCR, and 31.8058% for UACI. These are admitted that the implemented cancelable biometric scheme can discover any alternation processed through the original features, even if the licensed templates are affected by rare change in their original pixels value. Thus, our implemented scheme becomes more reliable because it has a remarkable capability to overcome the differential attacks.

Table 11 Average NPCR, and UACI assessments of tested cancelable modalities

Physical Modality	GA based deformed patterns		RNA-GA based deformed patterns		Hyperchaotic and Fibonacci Q-matrix based deformed patterns	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Faces	96.8120	26.7205	98.5746	28.0053	98.7261	28.0671
Ears	97.2736	26.6924	98.2750	27.6924	97.5550	27.5138
Fingerprints	97.5928	27.5102	98.6175	28.9480	99.3053	30.2058
Iris	98.3112	27.7294	98.4786	27.9922	96.6915	27.4035
Palmprints	98.3825	30.4011	99.4102	33.4480	99.7461	33.2245

5.3 Comparisons with recent studies

The proposed cancelable biometric system has been compared with the related studied in [16, 17, 21–23, 25, 28]. EER, FAR, FRR, and AROC have been considered in this comparison. Table 12 exposes the results and revealing higher AROC values and lower EER values for the proposed cancelable biometric system.

To further verify the efficiency of the proposed six- dimensional hyperchaotic cryptosystem and Fibonacci Q-matrix technique for the reliable cancelable biometric system, tested simulations are employed for comparing results of the proposed cancelable system with the recent state-of-the-art schemes [16, 17, 21–23, 25, 28]. A comparison is accomplished for the statistical evaluation assessments of the EER, False Accept Rate (FAR), False Reject Rate (FRR), and AROC results of the proposed hyperchaotic cryptosystem and Fibonacci Q-matrix based cancelable biometric system with the recent literature encryption-based cancelable biometric schemes in [16, 17, 21–23, 25, 28] as given in Table 12. Form the presented comparative assessments in Table 12, it is observed that the FAR, FRR, EER, AROC results of the proposed cancelable templates for the proposed cancelable system are more appreciated and recommended compared to other literature cancelable biometric systems.

6 Conclusions and future work

The valuable results of this proposed methodology are achieved due to the exploitation of Fibonacci Q-matrix to produce the diffused pixels of deformed patterns by hyperchaotic system with six initial conditions. The implementation to construct an efficient biometric template protection based authentication system by the presented cancelable approach provides high diffusion to be employed on frame's pixels with different sizes and consequently obtaining the scrambled biometric features consequently. The resultant cancelable frames succeed in improving the privacy by enhancing the cancelable evaluation measurements and confidentiality by providing the better security performance metrics. So, the proposed scheme has the superiority over the recent template protection techniques as GA, and RNA-GA. Furthermore, the introduced biometric protection technique, based on hyperchaotic and Fibonacci Q-matrix approach, investigates the more protection for biometric patterns

Table 12 The statistical evaluation analysis results for cancelable templates of the proposed cancelable system and the literature cancelable systems in [16, 17, 21–23, 25, 28]

Cancelable biometric system	EER	FAR	FRR	AROC
Proposed scheme	0.00511	0.00116	0.00273	0.9999
OSH [28]	0.0102	0.0541	0.0155	0.9791
FRFT only [17]	0.0046	2.3550×10^{-03}	0.9292	0.8837
Ref. [25]	5.6942×10^{-3}	3.0414×10^{-03}	0.9671	0.9076
Ref. [16]	0.0016	0.1955	4.5354×10^{-03}	0.8737
Ref. [21]	8.7546×10^{-03}	0.0435	6.1101×10^{-03}	0.7187
Ref. [22]	3.1524×10^{-03}	0.0985	1.6822×10^{-04}	0.8630
Ref. [23]	9.5647×10^{-03}	0.0056	2.5216×10^{-03}	0.8684

even over the two previously proposed cancelable algorithms because the proposed methodology adds more confusion due to the utilization of six hyperchaotic initial conditions instead of the usage of ordinary chaotic systems that have only one initial condition. Thus, it satisfies convenient PFD, PTD, ROC, histogram, correlation, run duration, and visual assessments, the more confusion is achieved, and the higher values are obtained for FAR, FRR, and EER compared with their related cancelable techniques. The proposed cancelable scheme has the validity to conceal the details of different biometric patterns efficiently. In addition, the experimental reviews and comparisons are obtained for the proposed biometric authentication framework providing an average EER, FAR, and FRR of 0.00511, 0.00116, and 0.00273, respectively, and the result for AROC leads to 0.9999.

From the security measurements perspective, the cancelable approach due to hyperchaotic system and Fibonacci Q-matrix achieves high level of randomness for each small change in the original trait's pixel that improves the immunity against differential attacks as well, moreover our security system provides privacy measurements almost equal to the optimum results through the various tested biometrics with different pattern sizes that reach to 7.99 for entropy, 99.0271% for NPCR, and 31.2058% for UACI.

Acknowledgements The authors are very grateful to all the institutions given in the affiliation list for performing this research work successfully. The authors would like to thank Prince Sultan University for their support.

Authors' contributions All authors are equally contributed.

Funding The authors did not receive support from any organization for the submitted work.

Data availability All data are available upon request from the corresponding author.

Declarations

Ethics approval and consent to participate All authors are contributing and accepting to submit the current work.

Consent for publication All authors are accepting to submit and publish the submitted work.

Competing interests The authors have no relevant financial or non-financial interests to disclose.

References

1. El-Shafai W et al (2021) Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Access 9:77675–77692
2. Kumar N (2020) Cancelable biometrics: a comprehensive survey. Artif Intell Rev 53(5):3403–3446
3. Mohamed FA, Eldein H et al (2022) A Cancelable Biometric Security Framework Based on RNA Encryption and Genetic Algorithms. IEEE Access 10:55933–55957
4. Xu Z et al (2021) Fusing structure and color features for cancelable face recognition. Multimed Tools App 80:14477–14494
5. Shahzad M et al (2021) Alignment-free cancelable fingerprint templates with dual protection. Pattern Recog 111:107735
6. Liu H, Kadir A, Liu J (2019) Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system. Opt Lasers Eng 122:123–133
7. Yu S-S et al (2020) Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Optics and Lasers Eng 124:105816
8. Hosny KM et al (2021) New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. Electronics 10.9:1066

9. Nagar A, Nandakumar K, Jain AK (2010) A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recogn Lett 31(8):733–741
10. Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011(1):1–25
11. Patel VM, Ratha NK, Chellappa R (2015) Cancelable biometrics: A review. IEEE Signal Process Mag 32(5):54–65
12. Yang W et al (2021) A cancelable biometric authentication system based on feature-adaptive random projection. J Inf Secur App 58:102704
13. Moujahdi C et al. (2012) Spiral cube for biometric template protection. Image and Signal Processing: 5th International Conference, ICISP 2012, Agadir, Morocco, June 28–30, 2012. Proceedings 5. Springer Berlin Heidelberg
14. Zhang L, Wang H, Tao L (2021) One-factor cancelable fingerprint template protection based on feature enhanced hashing. Twelfth International Conference on Graphics and Image Processing (ICGIP 2020). 11720. SPIE
15 Mandalapu H et al (2021) Audio-visual biometric recognition and presentation attack detection: A comprehensive survey. IEEE Access 9:37431–37455
16 Alarifi A et al (2020) Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. IEEE Access 8:221246–221268
17 Faragallah OS et al (2020) Secure color image cryptosystem based on chaotic logistic in the FrFT domain. Multimed Tools App 79:2495–2519
18. Sarkar A, B Kr Singh, Bhaumik U (2018) Cryptographic key generation scheme from cancellable biometrics. Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2017. Springer Singapore
19 Alam B et al (2018) An alignment-free cancelable fingerprint template for bio-cryptosystems. J Netw Comput App 115:20–32
20. Gao Q, Zhang C (2017) Constructing cancellable template with synthetic minutiae. IET Biometrics 6(6):448–456
21. Jin Z et al. (2018) A cancellable ranking based hashing method for fingerprint template protection. Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13–15, 2017, Proceedings 9. Springer International Publishing
22. Ali MAM, Md Tahir N (2018) Cancelable biometrics technique for iris recognition. 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE
23. Soliman RF et al (2020) Efficient cancelable Iris recognition scheme based on modified logistic map. Proc Nat Acad Sci India Section a: Phys Sci 90:101–107
24 Soliman RF, Amin M, Abd El-Samie FE (2018) A double random phase encoding approach for cancelable iris recognition. Opt Quantum Electron 50:1–12
25. Soliman RF et al (2018) Double random phase encoding for cancelable face and iris recognition. App Optics 57.35:10305–10316
26 Ratha NK et al (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Machine Intell 294:561–572
27. Sandhya M, Prasad MVNK (2017) Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme. Int J Pattern Recognit Artif Intell 3104:1756004
28 Poon T-C, Liu J-P (2017) Introduction to modern digital holography: with MATLAB. Cambridge University Press
29 Tsang PWM, Liu J-P, Poon T-C (2015) Compressive optical scanning holography. Optica 2.5:476–483
30. Srikanth V et al. (2010) Bit-level encryption of images using genetic algorithm. Int J Comput Sci Commun Technol 3.1
31. Hassan MAS, Abuhaiba ISI (2011) Image encryption using differential evolution approach in frequency domain. Signal & Image Process 2:51–69
32. Gorodilov A, Morozenko V (2008) Genetic algorithm for finding the key's length and cryptanalysis of the permutation cipher
33. Bhowmik S, Acharyya S (2011) Image cryptography: The genetic algorithm approach. 2011 IEEE Int Conference Comput Sci Automation Eng 2. IEEE
34 Al-Husainy MAF (2006) Image encryption using genetic algorithm. Inf Technol J 53:516–519
35. Hammad M, Luo G, Wang K (2019) Cancelable biometric authentication system based on ECG. Multimed Tools App 78:1857–1887
36. Nasereddin HHO, Darwesh AJ (2020) An Encryption and Decryption Technique using Genetic algorithm. Talent Dev Excell 12
37 Leng L et al (2014) Analysis of correlation of 2DPalmHash Code and orientation range suitable for transposition. Neurocomputing 131:377–387
38. Faragallah OS et al. (2022) Efficient chaotic-Baker-map-based cancelable face recognition. J Ambient Intell Humanized Comput 1–39

39. Faragallah OS et al (2021) Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform. Optics and Lasers Eng 137:106333
40. Faragallah OS et al (2020) Efficient HEVC integrity verification scheme for multimedia cybersecurity applications. IEEE Access 8:167069–167089
41. Ibrahim S et al. (2020) Hardware implementation of cancellable biometric systems. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE
42. Badr IS et al (2021) Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. Digital Signal Process 116:103103
43. El-Hameed, Abd HA et al. (2021) Cancelable biometric security system based on advanced chaotic maps. The Visual Comput 1–17
44. Algarni AD et al (2020) Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy 22.12:1361
45 Wang J et al (2019) A new six-dimensional hyperchaotic system and its secure communication circuit implementation. Int J Circuit Theory App 47.5:702–717
46 Zhou T et al (2020) Logarithmic encryption scheme for cyber–physical systems employing Fibonacci Q-matrix. Future Gener Comput Syst 108:1307–1313
47. Hammad M, Liu Y, Wang K (2018) Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. IEEE Access 7:26527–26542
48. Liang Z, Qin Q, Zhou C (2022) An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. Neural Comput Appl 34(21):19313–19341
49. ORLDatabase. Availableonline:https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html (last accessed on 12 December 2020).
50. FERET Database. Available online: https://www.nist.gov/itl/products-and-services/color-feret-database (last accessed on 12 December 2020)
51. LFW Database. Available online: http://vis-www.cs.umass.edu/lfw/ (last accessed on 12 December 2020).
52. (2002) IIT Delhi Ear Database Version 1. Accessed: Jun. 15, 2020. [Online]. Available: http://webold.iitd.ac.in/biometrics/Database_Ear.htm
53. AMIEarDatabase (2015) [Online] Available:http://www.ctim.es/research_works/ami_ear_database
54. Dobes M, Machala L (2004) Upol Iris Image Database. Accessed: Jun. 15, 2020. [Online]. Available: http://phoenix.inf.upol.cz/iris/
55. CASIAIRISDatabase [Online] Available:http://www.cbsr.ia.ac.cn/english/IrisDatabase. sp
56. FVC2002(DB1)Database.Availableonline:https://www.biometricsinstitute.org/resources/fingerprintverification-competition-fvc (last accessed on 12 December 2020).
57. FVC2002(DB2)Database. Available online: http://bias.csr.unibo.it/fvc2002/databases.asp (last accessed on 12 December 2020)
58. BI Test (2005)CASIAPalmprint.[Online]. Available:http://www.biometrics.idealtest.org
59. IITDPalmprintDatabase,[Online],Available:http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm.
60. Hasanzadeh E, Yaghoobi M (2020) A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys. Multimed Tools App 79:7279–7297
61. Shahreza HO, Melzi P, Osorio-Roig D, Rathgeb C, Busch C, Marcel S,... Vera-Rodriguez R (2023) Benchmarking of cancelable biometrics for deep templates. arXiv preprint arXiv:2302.13286
62. Abdellatef E, Ismail NA, Abd Elrahman SES, Ismail KN, Rihan M, Abd El-Samie FE (2020) Cancelable multi-biometric recognition system based on deep learning. Vis Comput 36:1097–1109
63. Yousif SF, Abboud AJ, Radhi HY (2020) Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory. IEEE Access 8:155184–155209
64. Yousif SF, Abboud AJ, Alhumaima RS (2022) A new image encryption based on bit replacing, chaos and DNA coding techniques. Multimed Tools App 81(19):27453–27493
65. Albu-Rghaif AN, Jassim AK, Abboud AJ (2018). A data structure encryption algorithm based on circular queue to enhance data security. In 2018 1st International Scientific Conference of Engineering Sciences-3rd Scientific Conference of Engineering Science (ISCES) (24–29). IEEE

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Fatma A. Hossam Eldein Mohamed[1] · **Walid El-Shafai**[2,3]

✉ Fatma A. Hossam Eldein Mohamed
fatma.hossam51@gmail.com

Walid El-Shafai
eng.waled.elshafai@gmail.com; walid.elshafai@el-eng.menofia.edu.eg; welshafai@psu.edu.sa

1 Department of Electronics and Electrical Communications Engineering, Alexandria University, Alexandria, Egypt

2 Security Engineering Lab, Computer Science Department, Prince Sultan University, 11586 Riyadh, Saudi Arabia

3 Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

View publication stats