Optik - International Journal for Light and Electron Optics 258 (2022) 168773

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.com/locate/ijleo

Original research article

A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications

Mai Helmy [a,*], Walid El-Shafai [a,b], El-Sayed M. El-Rabaie [a], Ibrahim M. El-Dokany [a], Fathi E. Abd El-Samie [a,c]

[a] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, 32952 Menouf, Egypt
[b] Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia
[c] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 21974, Saudi Arabia

ARTICLE INFO

Keywords:
Cancelable biometric system
RC6
AES
Chaotic
Rubik's cube
Security applications

ABSTRACT

The need for high-speed and secure multi-biometric systems has grown in the last few decades. The progress in Internet applications and computer networks has prompted new problems with security and privacy. Having a reliable and secure means for storing biometrics is a necessary issue. Hence, data encryption and network security have become significant. Thence, because of the fast progress in network development, humans can easily and arbitrarily distribute or access digital data from networks. Therefore, ownership security has become a significant issue for individuals, and it requires much interest. Thus, there is a significant threat to copyright owners and digital multimedia producers to conserve multimedia from intruder prospection to avert loss in transmitted data. Ten years ago, most modern security systems depended on biometrics. Unfortunately, these systems have suffered for a long time from hacking trials. If the biometric databases have been hacked and stolen, the saved biometrics will be lost forever. Thus, there is a bad need to develop new cancelable biometric systems. In a classical authentication system, a user can easily change a password if it is compromised. However, the user's biometrics are limited and unique, and if a user biometric is compromised, it will be impossible to change it in a particular system or at least difficult. Cancelable biometrics can be generated with intentional, repeatable distortions of biometric signals based on transforms. Hence, biometric templates are compared in the transform domain. Cancelable biometrics depend on transforming data to replace a single biometric template in the same or different systems. This paper presents a cancelable biometric system that depends on a novel hybrid encryption framework based on the Rubik' cube technique. It allows simultaneous encryption of multiple images. The suggested hybrid enrollment stage begins with chaotic Baker map permutation in the Cipher FeedBack (CFB) operation mode, Advanced Encryption Standard (AES) or Ron's Code (RC6) algorithm as a first stage for encrypting the multiple images, separately. After that, the output encrypted images are passed to the second encryption stage via Rubik's cube technique. Chaotic, RC6, or AES encrypted face images are utilized as the Rubik's cube faces. For the RC6 and AES algorithms, they add a degree of diffusion, while the chaotic algorithm adds a degree of permutation. Moreover, the Rubik's cube technique adds more permutations to the encrypted images, simultaneously. The encrypted

* Corresponding author.
E-mail addresses: mai_hil@yahoo.com (M. Helmy), eng.waled.elshafai@gmail.com (W. El-Shafai), elsayedelrabaie@gmail.com (E.-S.M. El-Rabaie), dokany_2006@hotmail.com (I.M. El-Dokany), fathi_sayed@yahoo.com (F.E.A. El-Samie).

https://doi.org/10.1016/j.ijleo.2022.168773
Received 27 June 2021; Received in revised form 14 November 2021; Accepted 25 February 2022
Available online 28 February 2022
0030-4026/

images are used in the cancelable biometric system. The simulation results prove that the hybrid proposed encryption framework is efficient. Moreover, it has strong robustness and security.

1. Introduction

Recent years have seen an exponential growth in the use of various cancelable biometric technologies. Unlike credit cards and passwords, which can be attacked and reissued when compromised, biometrics are permanently associated with a user's unique characteristics and cannot be replaced [1–3]. Biometrics are either signals or images presented from persons for discrimination between them. The most common biometrics are fingerprints, faces, iris, and speech signals. The basic idea of the operation of biometric systems is to collect the biometrics from some authorized persons [4,5]. Generally, face recognition depends on the geometric determination of eyes, nose, and mouth in the face images [6,7]. All traditional biometric systems depend on acquiring a signal or an image from the users or subscribers, and then matching it with those stored in a pre-arranged database [8]. The main disadvantage of this traditional trend is that each person has to provide his original biometrics for access [9,10]. The enrollment data are saved in the database. This means that if the database is stolen, the original biometrics will be lost forever, and hence the system will not be suitable for utilization again.

Moreover, the users whose biometrics have been stolen will not use them again in other systems [11]. A new trend towards more secure biometrics is to use cancelable biometrics for persons. These biometrics can be changed easily in emergency cases without changing the system at all [12,13]. Moreover, encryption techniques can be used with all types of biometrics [14,15] to generate cancelable templates. Different algorithms have been presented in the literature due to the importance and popularity of the recognition systems [16]. Recent cancelable biometric concepts have been adopted for face, fingerprint, and iris recognition by using random kernels to generate cancelable image templates. This approach is called the Minimum Average Correlation Energy (MACE) filter approach. It adopts the correlation coefficient as a tool for verification without automatic classifiers [17].

Encryption is one of the most favorable methods to secure digital multimedia files in the domains of copyright protection and data authentication. Data encryption has more implementations in different fields such as medical imaging, Internet communication, telemedicine, multimedia systems, and military communications. A biometric authentication system automatically identifies or verifies a person using physical, biological, and behavioral characteristics such as the face, iris, fingerprints, hand geometry, or voice [18,19]. Compared to traditional methods of verification and identification (password, card, ID), biometrics are more suitable for users, can reduce attacks, and allow more security. Recently, modern biometric systems have been developed to enhance the security. The basic concept of cancelable biometrics is to use another version of the original biometric template created through a one-way transform or an encryption scheme to keep the original biometric safe and away from utilization in the system [20–22].

In this paper, our proposed cancelable biometric system is based on Rubik's cube technique, which depends on the puzzle concept. A puzzle is a problem that tests the ability of the solver's mind, imagination, skill, and cleverness. Puzzles were and are still classified as games and entertainment tools, but we can also consider them in mathematical problems or logical quizzes in different cases. People with a high attitude may be better than others when they are dealing with those puzzles. Also, those quizzes may be solved easily by computer programs [23]. The proposed cryptosystem is based on Rubik's cube technique mixed with chaotic Baker map, RC6, and AES algorithms. The Initialization Vector (IV) of the chaotic map works as the main key, and the block is a square lattice of $N \times N$ pixels [24–26]. The RC6 and AES algorithms will be used in this paper. The RC6 algorithm has six simple and basic operations, which are addition (+), subtraction (−), left rotation (>>>), right rotation (<<<), XOR ($\oplus$), and multiplication (*). The utilization of the multiplication process increases the diffusion per round greatly, leading to more security, fewer rounds, and finally, large throughput [27,28]. The RC6 algorithm uses a key table consisting of $2r + 4w$-bit words [28,29]. The Rubik's cube technique adopted in this paper is used to achieve further permutation in the encryption process over its faces. It will be used to encrypt a group of images, simultaneously. The images implemented on these nine faces are encrypted with the chaotic, RC6 or AES technique. The proposed hybrid encryption framework will guarantee both diffusion and permutation in the encrypted images. Hence, the proposed biometric cryptosystem based on Rubik's cube principle can achieve good encryption and hiding ability and resist different types of attacks. Several encryption algorithms based on chaotic map, AES, and RC6 algorithms have been proposed to protect digital data against different cryptographic attacks [30].

This paper introduces cancelable face recognition systems. The first and classical cancelable face recognition system consists of random kernel generation, convolution, and authentication stages. The matcher can decide and classify the encrypted faces as accepted or rejected based on a threshold value. The quantitative evaluations of this proposed cancelable face recognition system depends on EER, False Acceptance Rate (FAR), False Rejection Rate (FRR), Area under Receiver Operating Characteristic (ROC) curve (AROC), and decidability. Another cancelable face recognition system based on the Rubik's cube technique is also presented. We present a novel image encryption enrollment stage based on Rubik's cube technique, achieving good encryption and perfect hiding ability and resisting different attacks [31].

The rest of this paper is organized as follows. In Section 2, the review and related studies are introduced. In Section 3, the proposed hybrid encryption framework is presented. In Section 4, the cancelable biometric templates are presented. Section 5 is devoted to system architecture. Section 6 presents the authentication metrics of both schemes. Section 7 gives the simulation results of the paper. Section 8 offers the concluding remarks and future research directions.

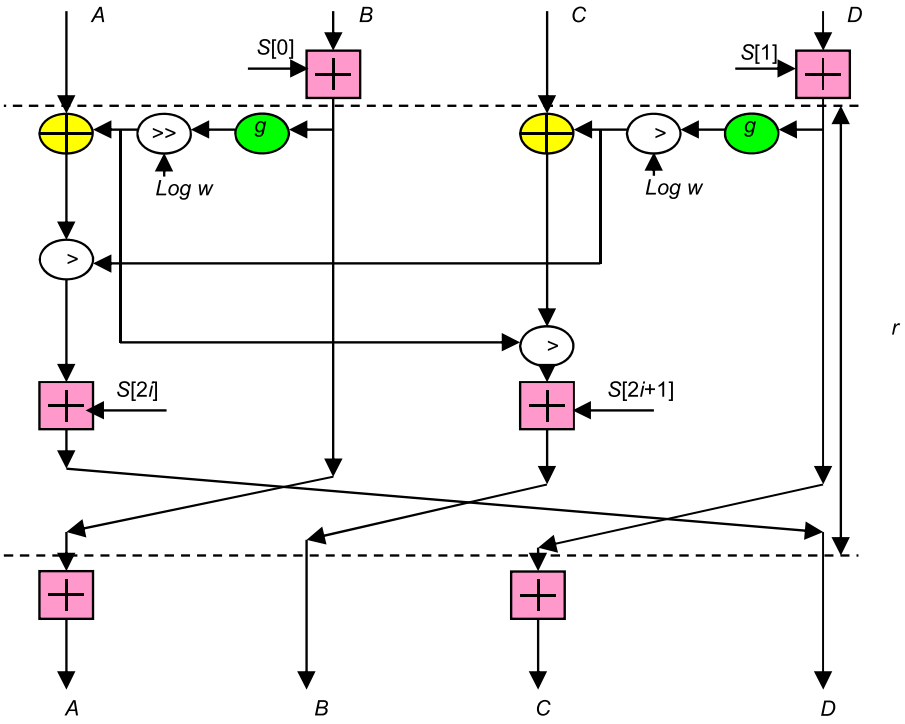


Fig. 1. The RC6 encryption algorithm.

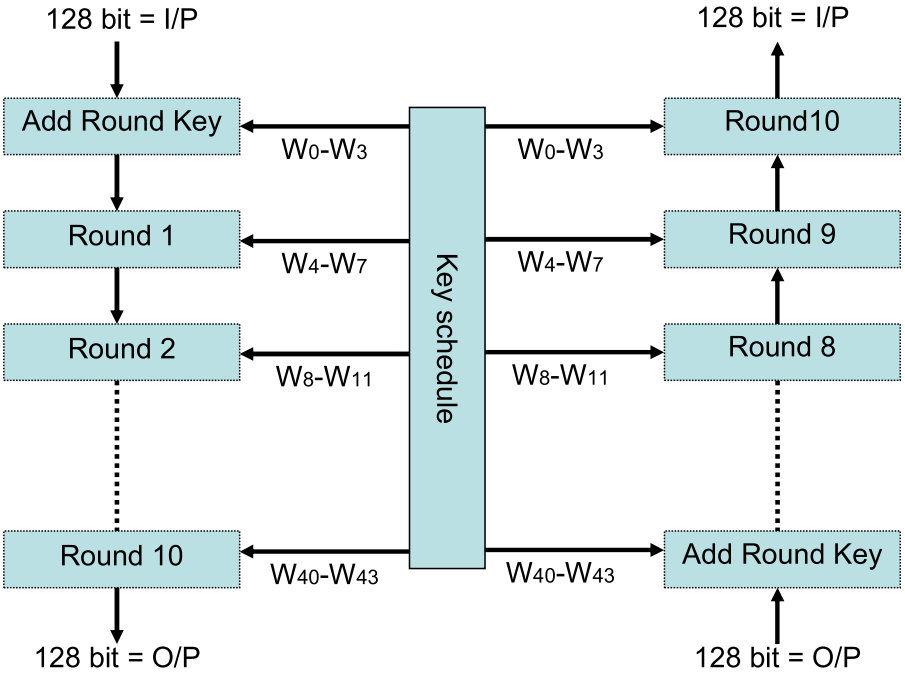


Fig. 2. The AES model of a 128-bit encryption key.

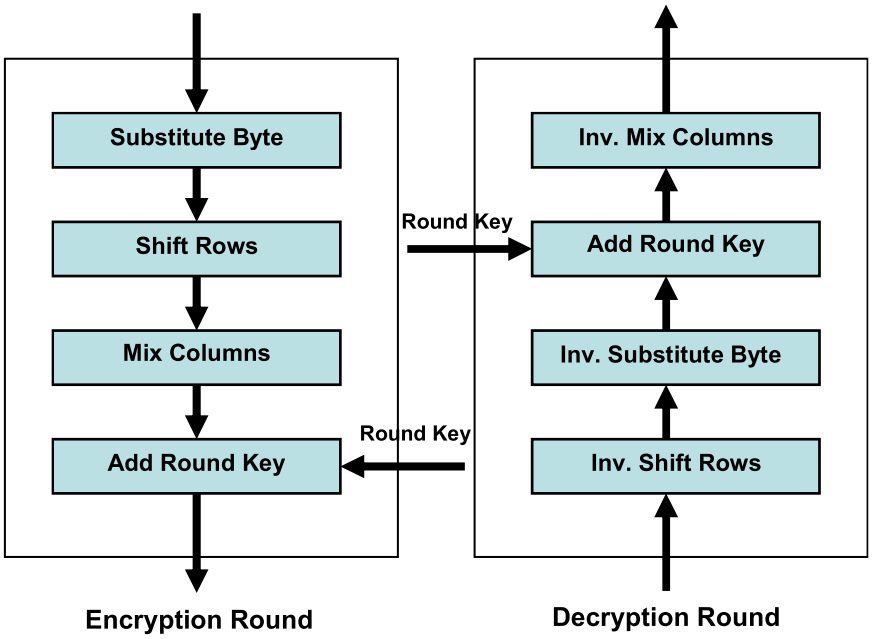


Fig. 3. At left, a single round of encryption, and at right, a single round of decryption.

2. Review and related studies

2.1. RC6 algorithm

The RC6 algorithm depends on four processing registers, and each register works with 32 bits to handle 128 bits as a total size of the input and output blocks. Therefore, the RC6 is parameterized by the word size (w) in bits, the number of rounds (r), and the encryption/decryption key length in bytes (b). Fig. 1 shows the different stages of the RC6 encryption algorithm.

The (f) function, the quantum rotations, and the modular additions give the algorithm its strength, where the number of runs increases the security [32]. The key is extended from a b-byte key into a $2r+4$ word array to produce a secret key $S = (S_0,.,S_{2r+3})$. The RC6 encryption algorithm is performed using four registers A, B, C, and D [33].

2.2. AES algorithm

The AES encryption/decryption algorithm is shown in Fig. 2, where the AES number of rounds is ten rounds, when the encryption key length is 128 bits. The number of rounds will be 12 with 192 key length and 14 with 256 key length. At any round, the system input data is XORed with the first four words of the key array. In the decryption procedure, we XOR the decrypted data array with the last four words of the key array. The last process will be XORing the output data of the four steps described before with four words from the key array [34].

The four steps in each round of processing are shown in Fig. 3, and are described as follows [35,36]:

1. SubBytes. It is defined as a forward substitution process, and it is applied in a byte-by-byte sequence.
2. ShiftRows. It is defined as a forward array shifting of the row states.
3. MixColumns. It is defined as the forward mixing process of each byte, separately, in each column.
4. AddRoundKey. It is defined as the round key adding to the output data of the previous step.

2.3. CBC, CFB, and OFB chaotic encryption modes

The general model of a typical encryption algorithm could be described by Eq. (1), where P is the plaintext image, E is the encryption algorithm, K is the encryption key, and C is the ciphertext image. At the receiver end, the decryption procedure is given by Eq. (2), where D is the decryption algorithm and K' is the decryption key. It may or may not be the same as the encryption key, K. The chaotic multimedia encryption can be done with three modes of operation, the Cipher Block Chaining (CBC) mode, the CFB mode, and the Output FeedBack (OFB) mode [37].

$$E(P,K) = C \tag{1}$$

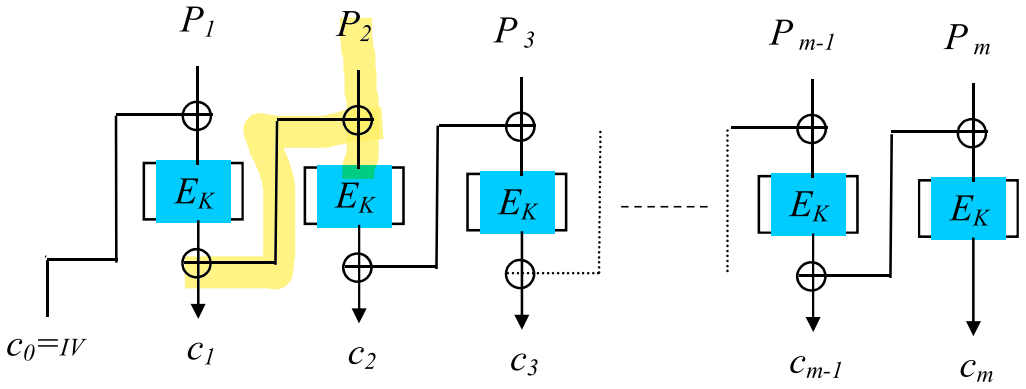


Fig. 4. The encryption process with the CBC mode.

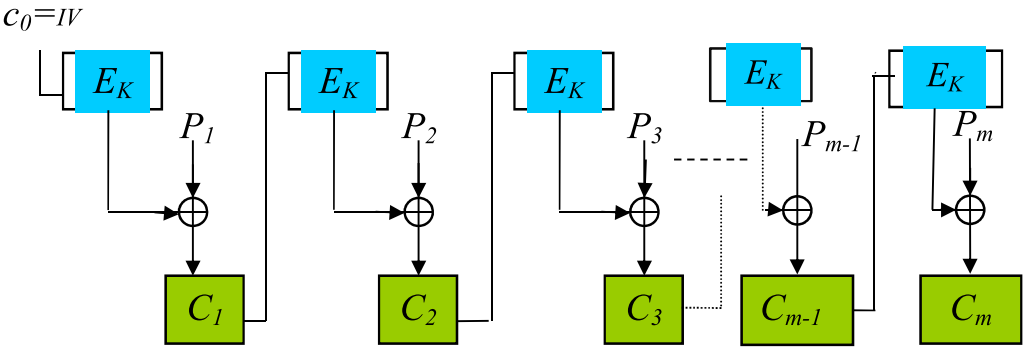


Fig. 5. The encryption process with the CFB mode.

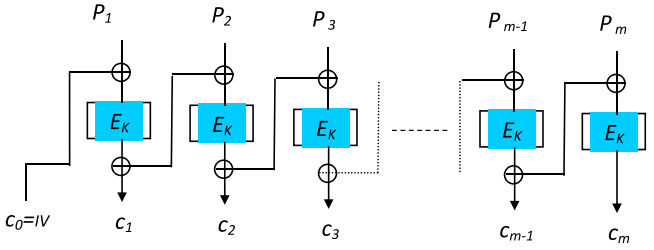


Fig. 6. The encryption process with the OFB mode.

$$D(C, K') = P \tag{2}$$

The CBC is a mode of operation for a block cipher in which a sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block. Cipher block chaining uses an IV of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block cipher of the ciphertext to depend on all preceding ciphertext blocks [38]. In the CBC mode, each plaintext block is XORed with the previous ciphertext block before being encrypted. So, each ciphertext block is dependent on all plaintext blocks up to that point. Then, in decryption, the same XOR operation is repeated, so that its effect is canceled. This mechanism is shown in Fig. 4.

The CFB is an encryption mode in which the plaintext block is XORed with the previous stage output obtained for the preceding block. Like CBC mode, the CFB mode uses an IV [37,38]. The XOR operation conceals the plaintext patterns. The plaintext cannot be directly worked on unless blocks are retrieved from either the beginning or end of the ciphertext. Fig. 5 illustrates the CFB mode.

The OFB mode has some similarities with the CFB mode in that it permits encryption of different block sizes, but has the main difference that each plaintext block is XORed directly with the encryption result of the preceding block. It also uses an IV. Changing the

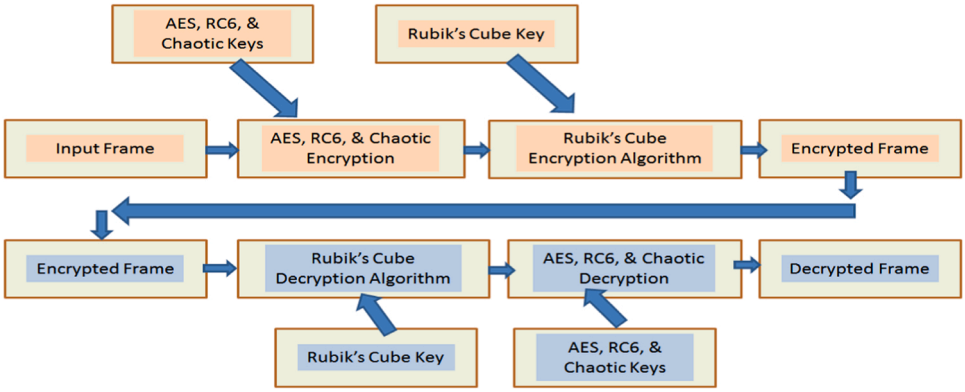


Fig. 7. The proposed framework implementation.

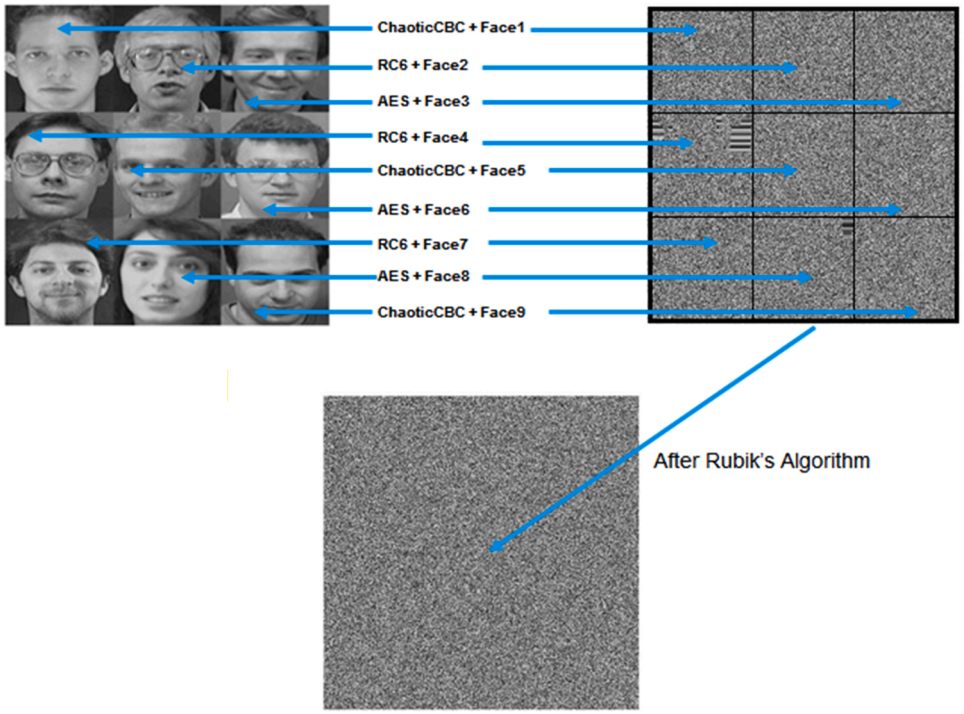


Fig. 8. The different 2D images and the encrypted one using Rubik's cube technique.

IV for the same plaintext block results in different ciphertexts [39]. The OFB mode is illustrated in Fig. 6.

3. Proposed hybrid enrollment framework

We use in this paper the Rubik's cube technique with different random keys to randomize the pixels of the original gray-scale images, by changing the positions of the pixels within the encrypted images via the circular-shift step applied on each of the columns and rows. Then, columns and rows are XOR-ed with the secret keys, and these stages can be repeated to improve the security strength of this algorithm.

The proposed methodology is explained in the diagram shown in Fig. 7. The hybrid encryption framework is described in Fig. 8 and Fig. 9. The proposal is described as a member of the symmetric encryption family. So, the decryption stage is defined as the reverse of

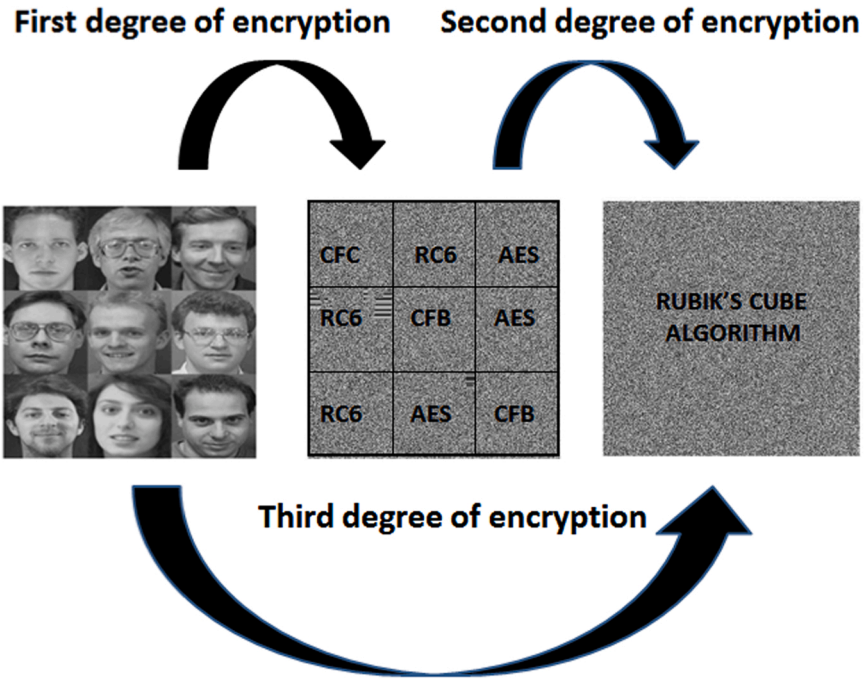


Fig. 9. The security levels of Rubik's cube encryption algorithm.

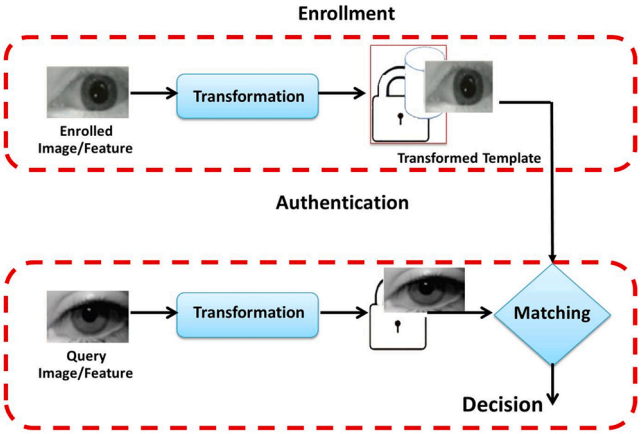


Fig. 10. Block diagram of a cancelable biometric system.

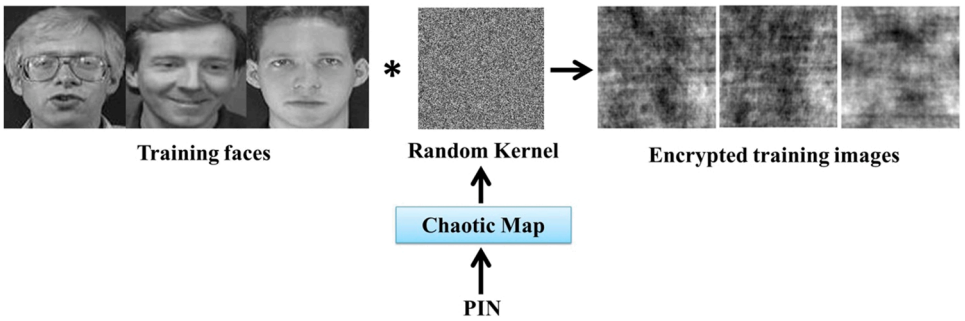


Fig. 11. The enrollment stage for generating cancelable biometric templates.

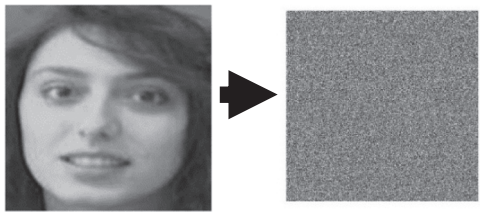


Fig. 12. A face and its encrypted version using Rubik's cube encryption.

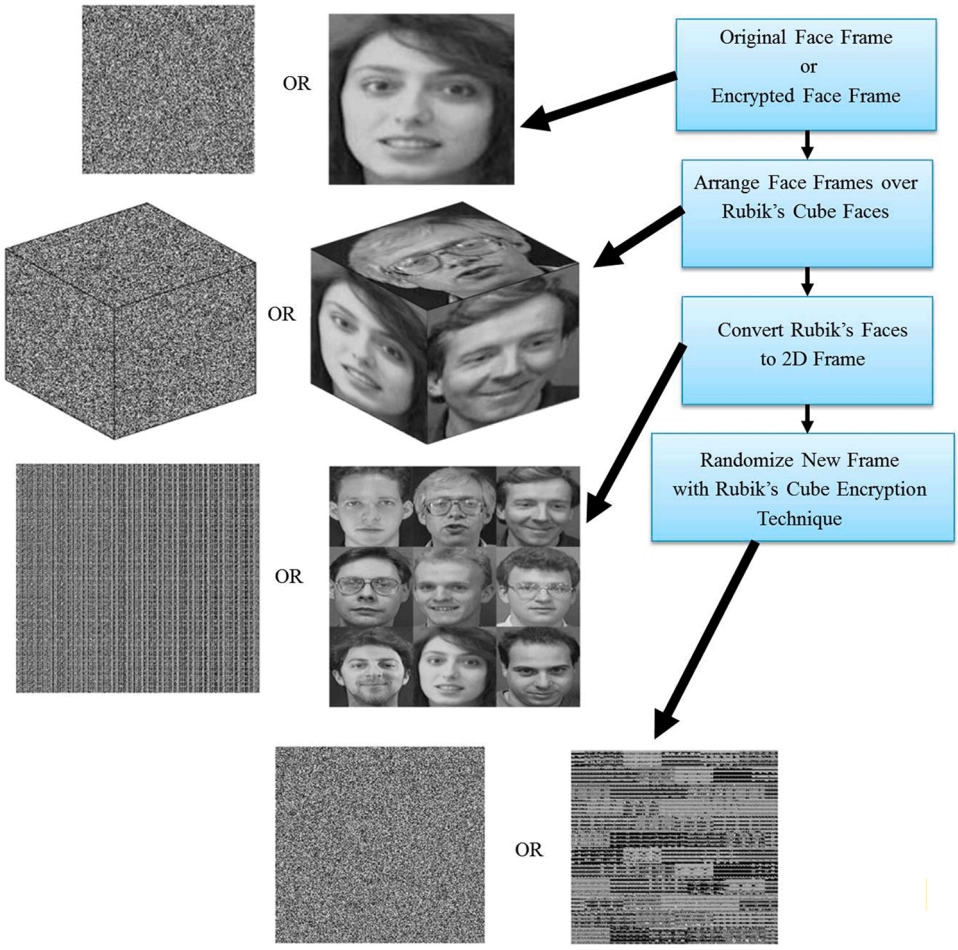


Fig. 13. The proposed hybrid enrollment stage.

the encryption stage, where the same key is used on both sides. Initially, the chaotic AES and RC6 encrypted images are obtained, and then put on the Rubik's cube faces.

We work on a gray-scale image $I_o(x, y)$ of size $M \times N$. The (x, y) coordinates indicate the positions of pixels in the encrypted image. In the proposed hybrid framework, the input images are the chaotic, AES, and RC6 encrypted images to be fed to the Rubik's cube technique. The encryption framework includes the following steps:

(1) One key K_{Rubix} and nine different keys for nine different images $K_{Class.Cipher}$, each of length $M \times N$, are generated in parallel. Each element in $K_{Rubix}(i)$ and $K_{Class.Cipher}$ (j) can take values from 0 to 255.
(2) We initialize a counter of iteration numbers, which is represented by I.R.

Table 1
Correlation values for the multiplexed encrypted faces of sample1 stream.

Multiplexed images of sample1	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode+Rubik's technique	0.2030	0.0023	1.0000	1.0000
[Face2] / encrypted with RC6 +Rubik's technique	0.1322	0.0038	0.8486	0.0013
[Face3] / encrypted with AES+Rubik's technique	0.1904	0.0010	0.7192	-0.0070
[Face4] / encrypted with RC6 +Rubik's technique	0.1976	0.0037	0.8509	0.0023
[Face5] / encrypted with chaotic map in CFB mode+Rubik's technique	0.2030	-0.0033	0.8197	0.0009
[Face6] / encrypted with AES+Rubik's technique	0.1928	0.0050	0.7416	0.0051
[Face7] / encrypted with RC6 +Rubik's technique	0.1858	0.0038	0.8103	-0.0019
[Face8] / encrypted with AES+Rubik's technique	0.1262	0.0072	0.8507	-0.0052
[Face9] / encrypted with chaotic map in CFB mode+Rubik's technique	0.1873	-0.0053	0.8937	0.0010

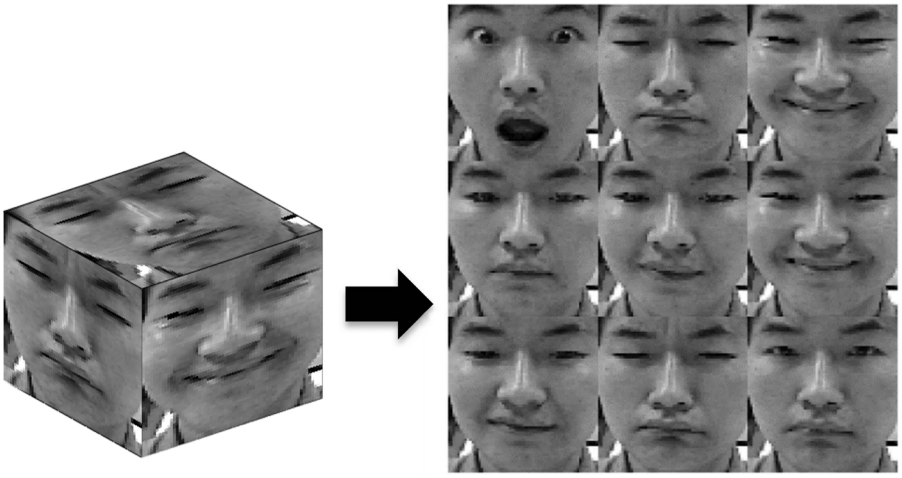


Fig. 14. Conversion of 3D Rubik's cube faces into a 2D image for the tested first nine images of sample1.

(3) We increment I.R by one: I.R = I.R+ 1.
(4) Box operations on the input image include:
(a) For each box *i*, we compute the sum of all elements, and it is denoted as $S_{Rubix}(i)$.

$$S_{Rubix}(i) = \sum_{j=1}^{N} I_o(i,j), i = 1,2,3,.M \tag{3}$$

i = 1... M
1 box = 1 row

(b) We perform modulo 2 operation on $S_{Rubix}(i)$, giving $M_{Rubix}(i)$.
According to $M_{Rubix}(i)$, the box *i* is left or right circular shifted by $K_{Rubix}(i)$ positions as follows:
If $M_{Rubix}(i) = 0$, we perform a right circular shift.
Otherwise, we perform a left circular shift.
(5) Then, each box of a scrambled image $I_{Class.Cipher}$ is bitwise XOR-ed with a random key K_{Rubix}

$$I_{Rubix}(i, 2j-1) = I_{Class.Cipher}(i, 2j-1)\ XOR\ K_{Rubix}(j) \tag{4}$$

Io(x, y) = grayscale image

and

$$I_{Rubix}(i, 2j) = I_{Class.Cipher}(i, 2j)\ XOR\ rot180^{o}(K_{Rubix}(j).)$$

where *rot*180 (K_{Rubix}) represents the flipping of K_{Rubix} from left to right.
(6) We repeat the steps from 3 to 5 until all iterations (I.R = $I.R_{MAX}$) are completed. Then, an encrypted image will be created. We assume $B(n_1,.,n_k)$ as the Rubik's cube algorithm with a secret key S_{key}. The 2D Rubik's cube image is of dimensions $I \times I$. The

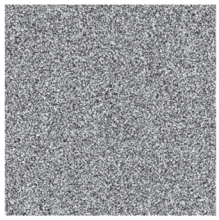
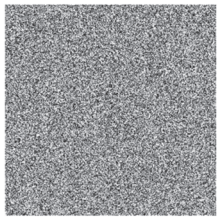
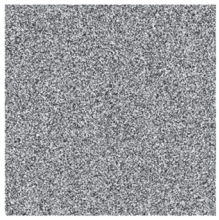
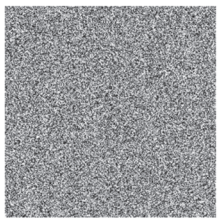
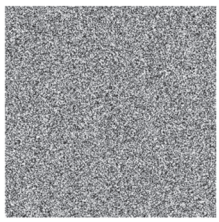
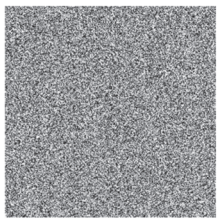
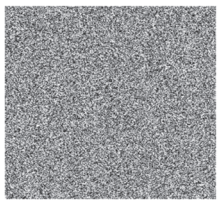
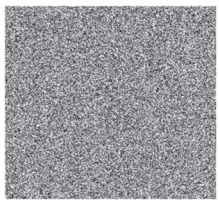
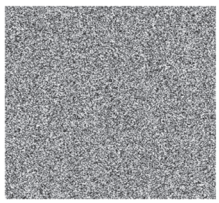
Output of Enrollment stage by the Kernel method			
	Face1	Face2	Face3
Output of Enrollment stage by Rubik's cube method			
	Face1	Face2	Face3
Output of Enrollment stage by the Kernel method			
	Face4	Face5	Face6
Output of Enrollment stage by Rubik's cube method			
	Face4	Face5	Face6
Output of Enrollment stage by the Kernel method			
	Face7	Face8	Face9
Output of Enrollment stage by Rubik's cube method			
	Face7	Face8	Face9

Fig. 15. Enrollment stage output for kernel and Rubik's cube techniques for the nine faces of sample1.

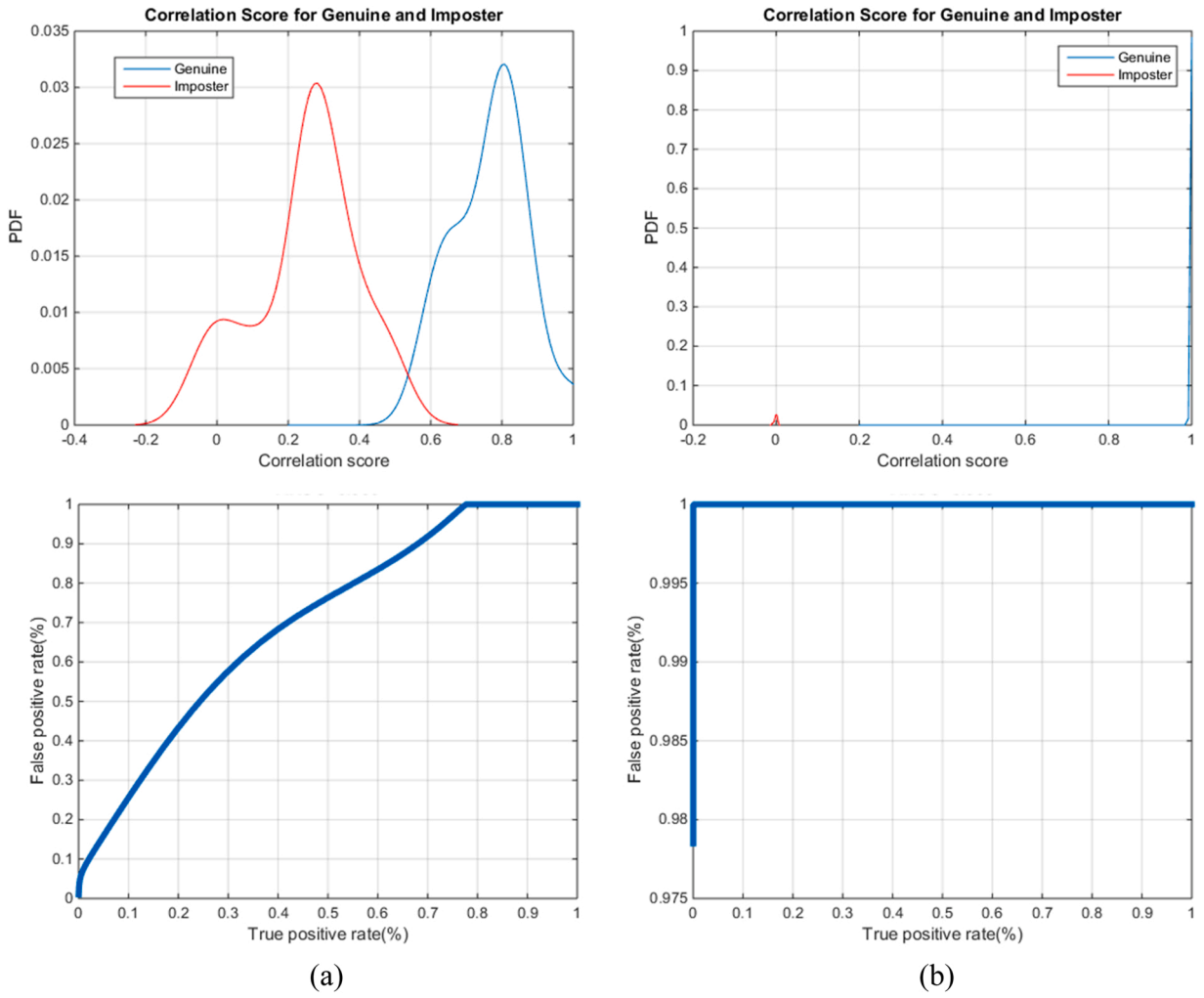


Fig. 16. PTD, PFD, and ROC curve with (a) kernel and (b) Rubik's cube encryption based cancelable biometric systems without noise using sample1 images.

secret key is selected provided that n_i satisfies $n_1 + \ldots + n_k = I$ [40]. The permutation moves the pixel at position (r,s) such that $I_i \le r < I_i + n_i$ and $0 \le s < I$ to another place according to:

$$B_{(n_1,..,n_k)}(r,s) = \left[\frac{I}{n_i}(r - I_i) + s \bmod \frac{I}{n_i}, \frac{n}{I}\left(s - s \bmod \frac{I}{n_i}\right) + I_i\right] \tag{5}$$

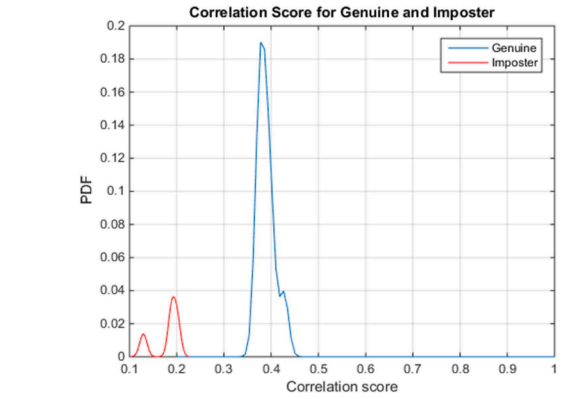
The proposed hybrid encryption algorithm depends on three levels of encryption, as shown in Fig. 9.

1. The first level of encryption is the classical encryption algorithms like chaotic, AES, and RC6.
2. The second level of encryption is Rubik's cube technique.
3. The third level of encryption is considered as combination of two different encryption algorithms. We have different varieties of arrangement on the Rubik's cube faces as follows:

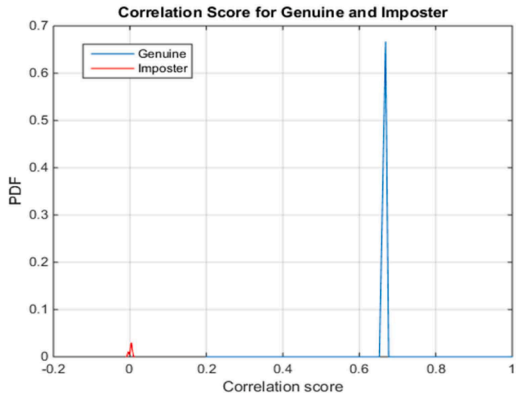
3-a) Chaotic/CFB - AES - RC6 - AES - RC6 - Chaotic/CFB - AES - RC6 - Chaotic/CFB.
3-b) Chaotic/CFC - RC6 - AES - RC6 - Chaotic/CFC - AES - RC6 - AES - Chaotic/CFB.
3-c) Chaotic/CFC - RC6 - AES - RC6 - Chaotic/CFC - AES - RC6 - AES - Chaotic/CFB.
3-d) Other different possibilities based on probability theory.

4. Cancelable biometric templates

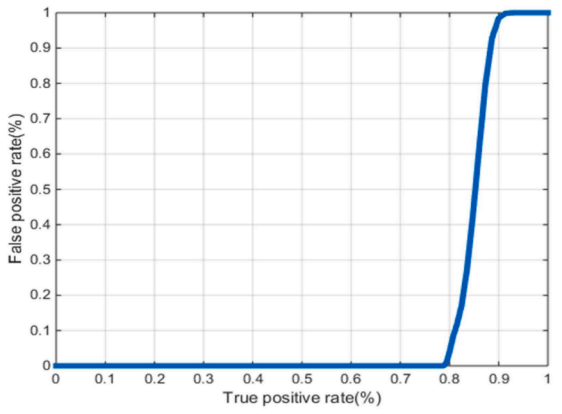
Why do people need several security and privacy concerns with biometrics? The answer of this question can be summarized as



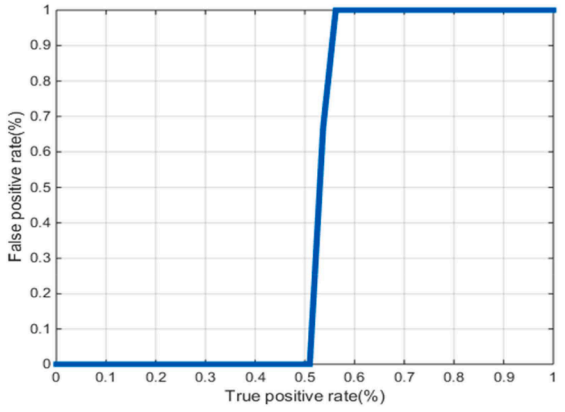
(a) PTD and PFD curves in kernel scheme.



(b) PTD and PFD curves in the case of Rubik's cube scheme.



(c) ROC curve of kernel scheme, AROC= 0.1495.



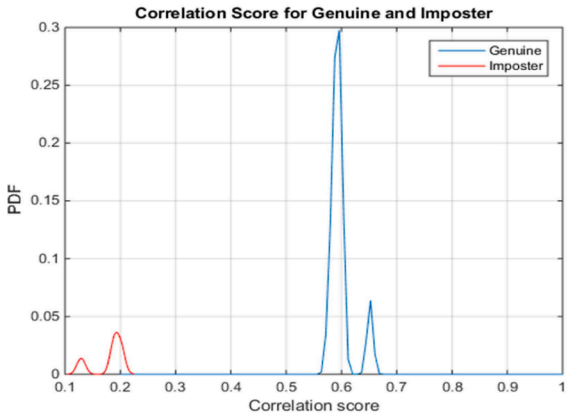
(d) ROC curve of Rubik's cube scheme, AROC= 0.4669.

Fig. 17. Distributions and ROC curves for the authentication stage of kernel, and Rubik's cube encryption based cancelable biometric systems using sample1 images at SNR= 5 dB.

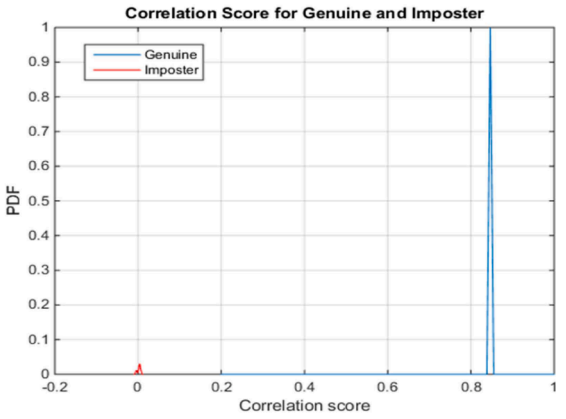
follows:

1. Passwords and cryptographic keys are known only to the user, and hence secrecy can be maintained. In contrast, biometrics such as voice, face, signature, and fingerprints can be easily recorded and misused without the user's knowledge.
2. If a hacker gets access to the biometric samples and has the ability to present them to a system emulating a human presence, there will be no trust associated with the biometrics. In this scenario, biometrics are stolen forever. On the contrary, passwords, crypto-keys and PINs can be changed if stolen.
3. It is highly recommended to use different passwords in different applications. However, biometric-based authentication methods rely on the same biometrics. Therefore, if a biometric template is stolen in an application, then the same method can be used to penetrate all applications, where the biometric is used. This is called cross-matching.

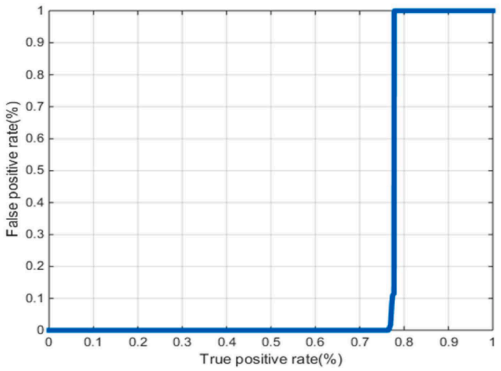
To overcome these problems associated with biometric systems, simple hash functions or encryption methods can be used to enhance privacy. Hash functions are susceptible to minor changes in the input. In practice, all biometric templates change with environmental conditions. For instance, face and iris biometrics are significantly affected by illumination variations. Therefore, these functions cannot be used directly in practice as they are applied only on the exact data. In encryption algorithms, when biometrics are encrypted, they need to be decrypted to carry out matching. This creates a possible attack point if an unauthorized person gets access to the decrypted biometrics. Hence, the research in cancelable biometrics has gained much interest in recent years. In this scenario, instead of storing the original biometrics, they are transformed using a one-way function. It was shown that this way of constructing biometric templates leads to the desired properties of cancelable biometric templates, as shown in Fig. 10. In particular, a stolen biometric can be re-enrolled using another transformation. This preserves privacy, since it is computationally difficult to recover the original biometric from a transformed one. It prevents cross-matching between databases since each application uses a different transformation that does not degrade the accuracy of the matching algorithm as the statistical characteristics of features are approximately maintained after transformation [41].



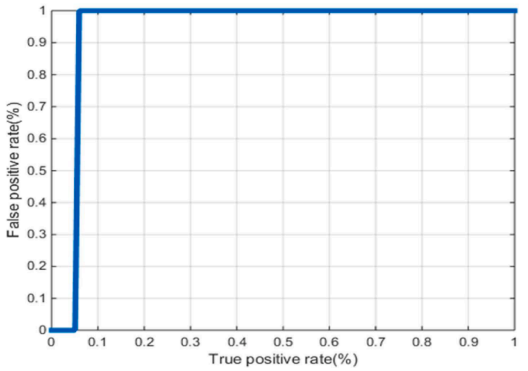
(a) PTD and PFD curves in the case of kernel scheme [35].



(b) PTD and PFD curves in the case of Rubik's cube scheme.



(c) ROC curve of kernel scheme [35], AROC = 0.2231.



(d) ROC curve of Rubik's cube scheme, AROC= 0.9448.

Fig. 18. Distribution and ROC curves for the authentication stage of the kernel, and Rubik's cube based cancelable biometric systems using sample1 images at SNR= 10 dB.

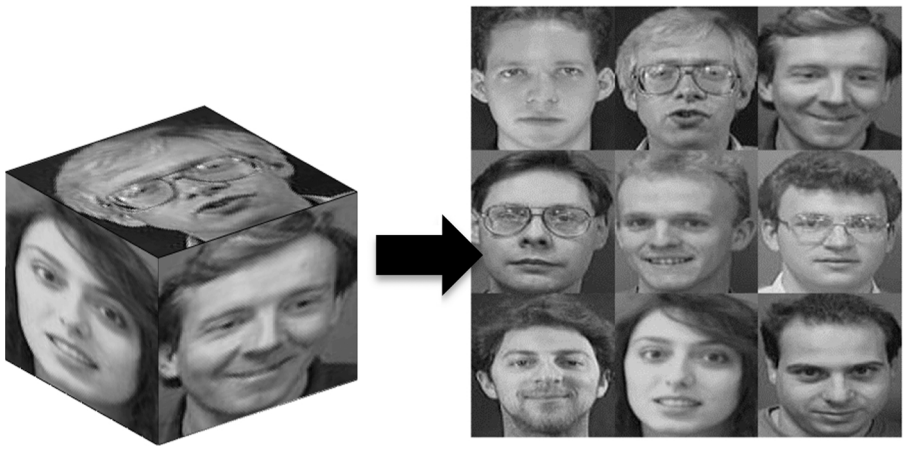


Fig. 19. Conversion of 3D Rubik's cube faces into a 2D image for sample2 images.

5. System architecture

Traditional identity authentication methods are based on what is physically possessed, such as ID cards, and what can be mentally stored in the memory, such as passwords and keys. For instance, the shortfalls of both are that ID cards can easily be lost or forged, while passwords and keys can either be easily guessed or forgotten, respectively. Short passwords are often preferred for memory

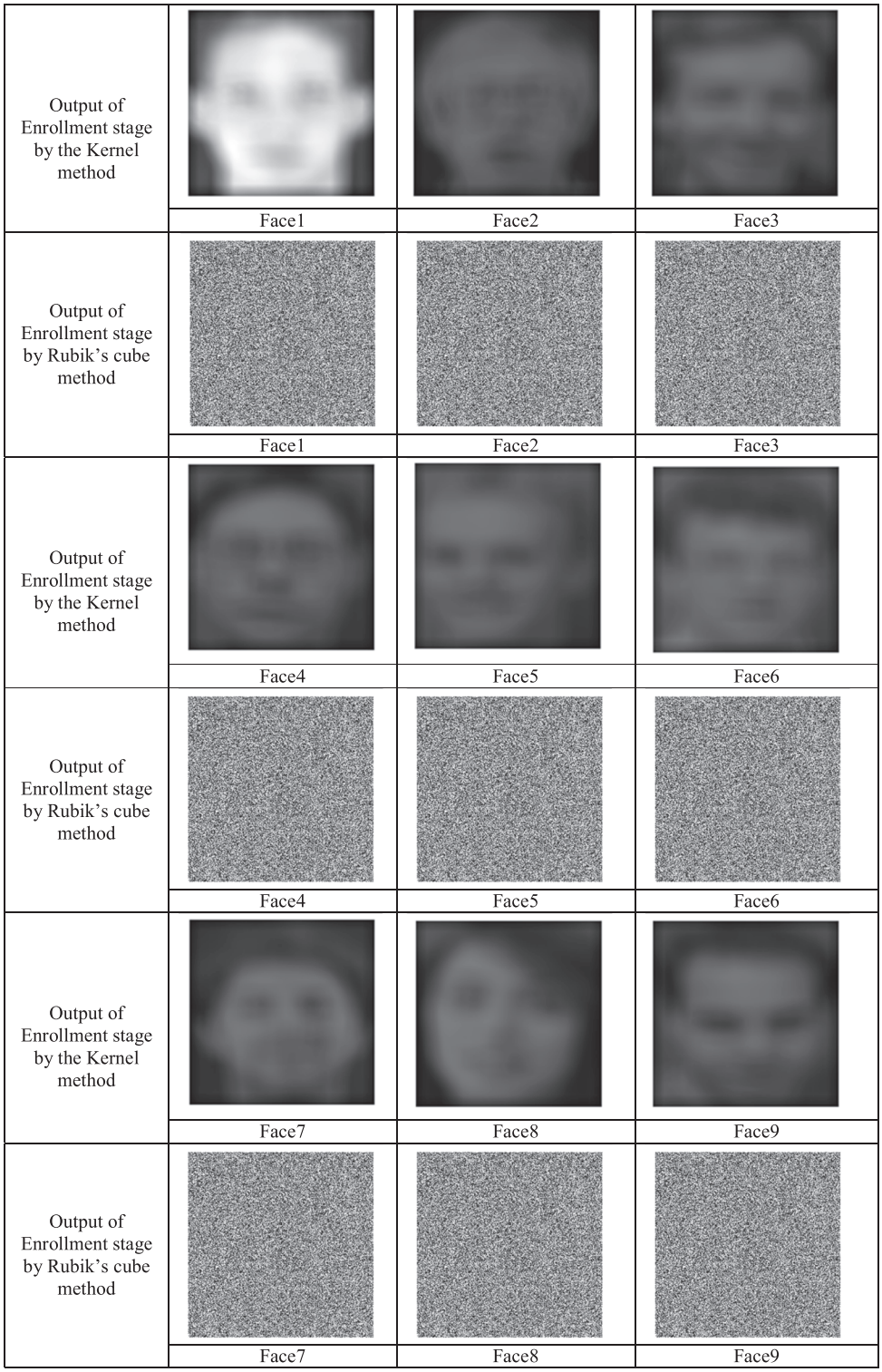


Fig. 20. Enrollment stage output for kernel and Rubik's cube based encryption of sample2 images.

requirements, but easily guessed by others. On the other hand, long passwords (commonly known as keys) that cannot be easily guessed are prone to memory problems. Key storage is, therefore, an issue, and it is recommended that general long keys are stored in key cards and at the same time, short passwords are used to protect the key cards. Eventually, short passwords are still essential to allow authentication. Biometric features inherited by a person include two major categories: physical and behavioral characteristics.

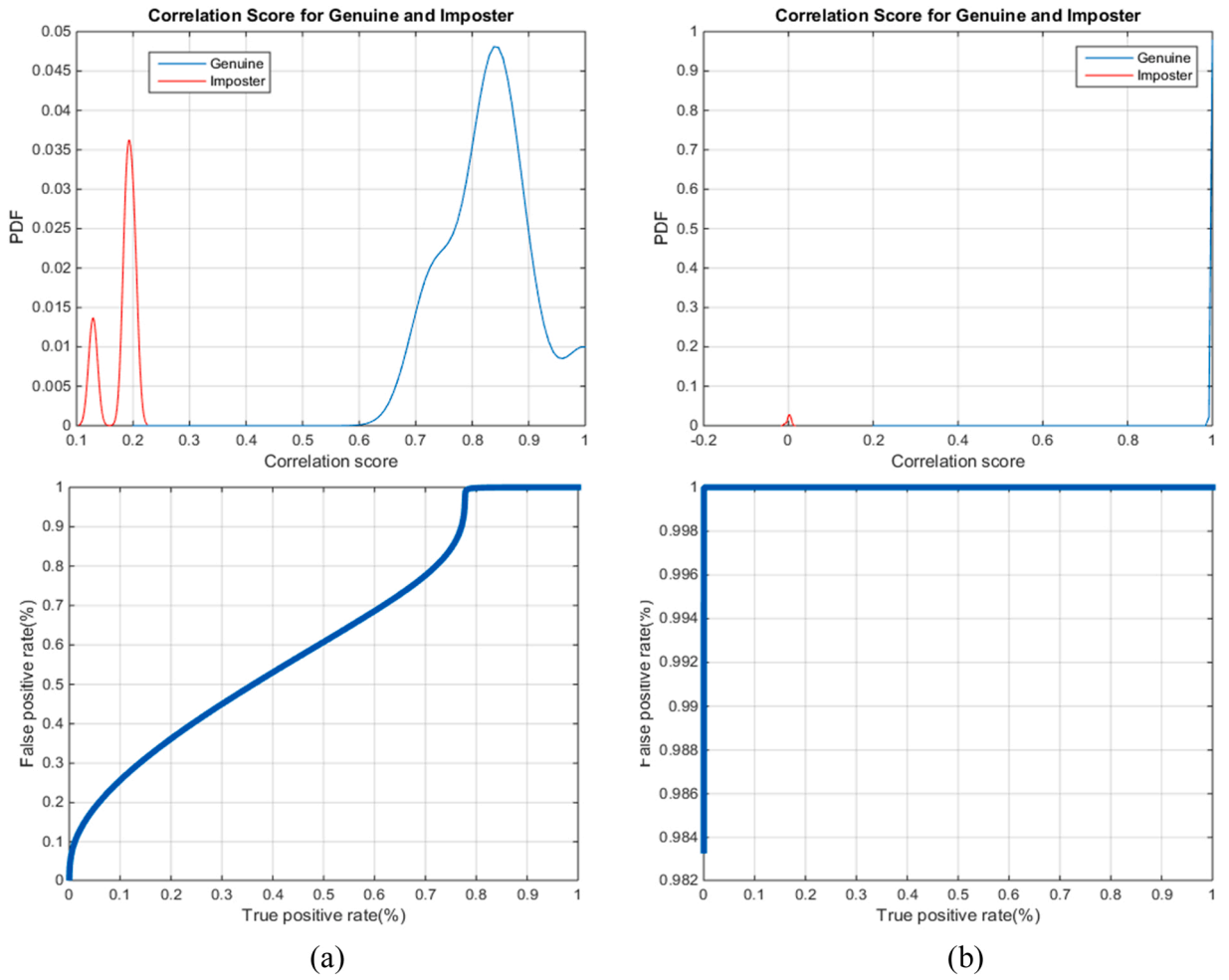
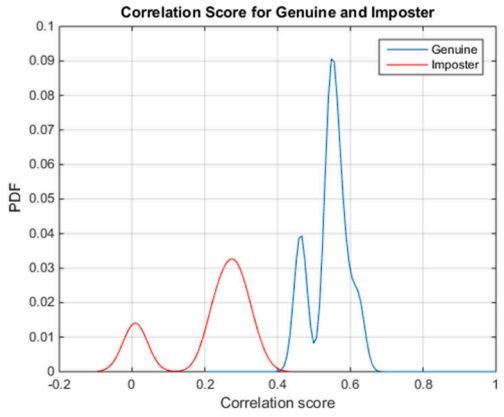


Fig. 21. PTD, PFD, and ROC curve with (a) kernel and (b) Rubik's cube based encryption for the cancelable biometric systems working on sample2 images without noise.

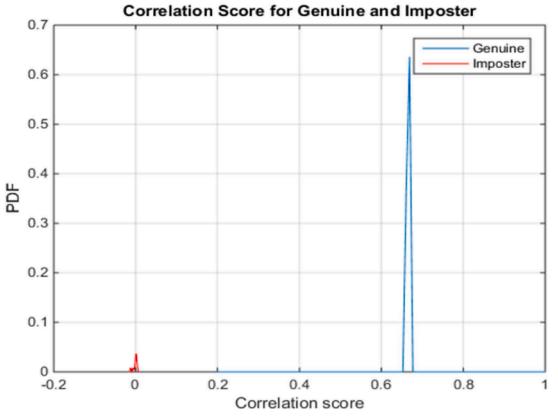
Physiological characteristics are fingerprints, face, iris, palm prints, and voice, to name but a few. Behavioral characteristics include gait, signature, keystrokes, etc. These characteristics have attracted a large number of scholars, who conducted extensive research on them. In order to perform the identification, an automatic technology is adopted to extract these features and have them compared with those stored in a database [37]. This infers that biometric identification technology is the solution to the several authentication problems. Before popularizing and applying computers, biometrics were checked manually, mainly by experts (e.g., the American FBI has several fingerprint experts). The development of information technology today has allowed automation of biometric recognition using computers. The Automatic Fingerprint Identification System (AFIS), for example, is one of the automated systems ever established. The typical AFIS includes an offline register and an online identification process. The offline register includes signal acquisition, template storage, and other necessary steps. The online identification includes signal acquisition, registration, template matching, etc. The biometric identification system has two modes for identity authentication: authentication (1:1) and identification (1: *N*). Authentication mode tests that you are the person you claimed, and identification mode verifies your identity information in the database and who you are. The two methods have a large gap between their algorithm processing times and complexity [15].

A cancelable biometric system, in general, is divided into two stages, the enrollment stage and the authentication stage, as shown in Fig. 10. On the classical enrollment stage shown in Fig. 11, a face capturing device is used to generate images to be convolved with a random convolution kernel. In this system, the kernel is generated by a PIN that is used as an initial condition of the chaotic map to generate the random convolution kernel. This random convolution kernel is convolved with the training images to generate the encrypted training images. The encrypted training images are then stored on a card and used for identity authentication. In our study, in the enrollment stage, we will apply the Rubik's cube technique on the data. Rubik's cube parameters are used for ordering of chaotic Baker map, RC6, and AES encryption results on the cube faces as shown in Fig. 13. Hence, this achieves a high level of security and protection of the biometric templates.

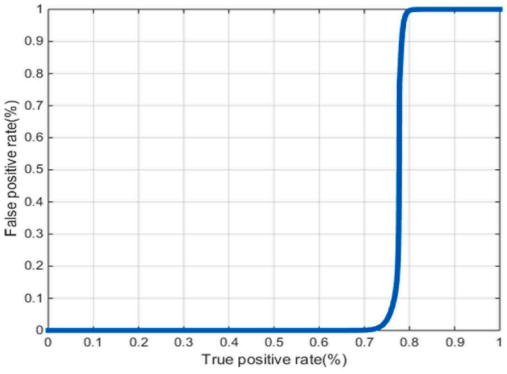
In both classical and Rubik's cube authentication stages, the resulting test images after enrollment are then correlated with the encrypted biometric templates stored in the database, and the correlation outputs are examined to perform authentication.



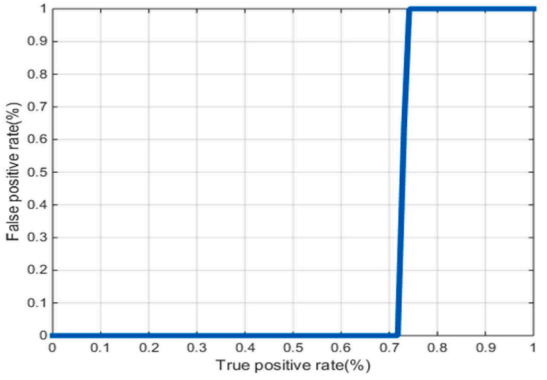
(a) PTD and PFD curves in the case of kernel scheme.



(b) PTD and PFD curves in the case of Rubik's cube scheme.



(c) ROC curve of kernel scheme, AROC= 0.2245.



(d) ROC curve of Rubik's cube scheme, AROC= 0.2715.

Fig. 22. Distribution and ROC curves for the authentication stage of the kernel, and Rubik's cube based encryption for the cancelable biometric systems working on sample2 images at SNR= 5 dB.

In the proposed cancelable biometric system, the face frames are firstly encrypted by the proposed hybrid encryption framework, as illustrated in Figs. 12 and 13. This is the enrollment stage which can be summarized as follows:

1- Encrypt the faces with chaotic, AES, or RC6 algorithm.
2- Set the encrypted faces over the Rubik's cube faces.
3- Convert all faces into a 2D image with a larger size.
4- Randomize the converted 2D image with Rubik's cube technique.

The 2D Rubik's cube encryption is some sort of chaotic encryption. Let $B(n_1, ., n_k)$ denote the map that is implemented in the Rubik's cube encryption with a secret key, S_{key}. The secret key is chosen such that each integer n_i divides I, and $n_1 + . + n_k = I$. The 2D image extracted from the Rubik's cube has dimensions of $I \times I$ [38]. The mapping equation is represented as in Eq. (5), with $I_i \leq r < I_i + n_i$ and $0 \leq s < I$.

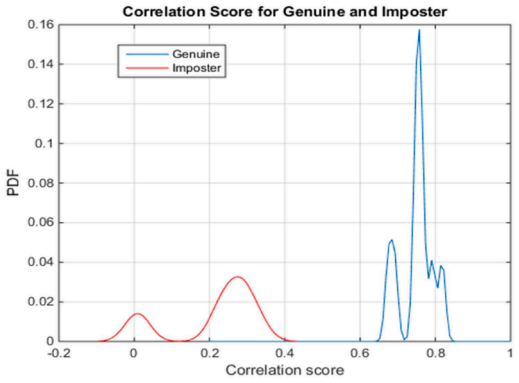
In steps, Rubik's cube randomization is performed in two permutation steps described as follows.

1- The $I \times I$ square matrix is divided into "k^2" boxes, each with height I/k with width I/k and number of elements $(I/k)^2$, and then permutated randomly.

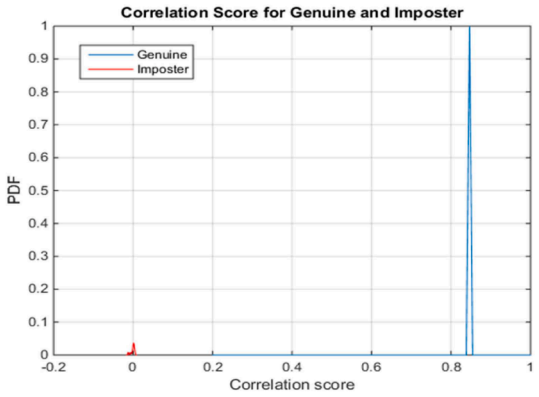
2- Each of these boxes is mapped to a row of pixels by mapping column by column (the left one at the bottom and the right one at the top). For example, Fig. 12 gives a face image and its encrypted version.

6. Authentication metrics

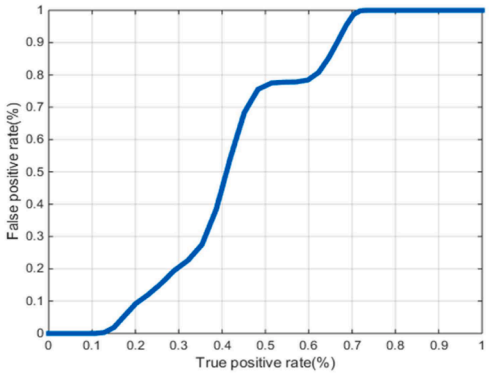
The correlation values are used to measure the similarity between a test pattern and stored biometric templates. The higher the score, the higher the similarity between petterns is. Access to the system is granted only if the score for a test person is higher than a certain threshold [37,38]. ROC analysis is used to quantify how accurately a system can discriminate between two states [39]. The ROC curve shows the trade-off between a true positive fraction (TPF) and a false-positive fraction (FPF) as one changes the threshold value [39].



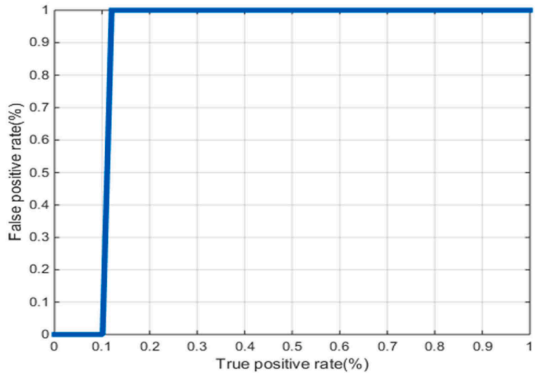
(a) PTD and PFD curves in the case of kernel scheme.



(b) PTD and PFD curves in the case of Rubik's cube scheme.



(c) ROC curve of kernel scheme, AROC = 0.5763.



(d) ROC curve of Rubik's cube scheme, AROC = 0.8893.

Fig. 23. Distribution and ROC curves for the authentication stage of the kernel, and Rubik's cube based encryption for the cancelable biometric system working on sample2 images at SNR= 10 dB.

Table 2
Correlation values for the jointly-encrypted faces of sample1 stream at SNR= 5 dB.

Jointly-encrypted images for sample1	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2030	0.0023	0.4276	0.6629
[Face2] / encrypted with RC6 + Rubik's technique	0.1322	0.0038	0.3728	0.6646
[Face3] / encrypted with AES + Rubik's technique	0.1904	0.0010	0.3787	0.6629
[Face4] / encrypted with RC6 + Rubik's technique	0.1976	0.0037	0.4031	0.6668
[Face5] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2030	0.0033	0.3954	0.6668
[Face6] / encrypted with AES + Rubik's technique	0.1928	0.0050	0.3913	0.6660
[Face7] / encrypted with RC6 + Rubik's technique	0.1858	0.0038	0.3819	0.6636
[Face8] / encrypted with AES + Rubik's technique	0.1262	0.0072	0.3710	0.6697
[Face9] / encrypted with chaotic map in CFB mode + Rubik's technique	0.1873	0.0053	0.3821	0.6650

In our biometric authentication study, the test data consists of both authorized and unauthorized patterns. The scores of all patterns would be somehow distributed around a certain mean score. The mean score of the authorized patterns is higher than that of the unauthorized patterns. A probability density distribution is used in the system test. Hence, the correlation scores resulting in the authentication stage are represented by the Probability of True Distribution (PTD) and the Probability of False Distribution (PFD). Moreover, several metrics may express the quality of encryption, such as deviation and correlation coefficient between original and

Table 3
Correlation values for the jointly-encrypted faces of sample1 stream at SNR= 10 dB.

Jointly-encrypted images of sample1	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2030	0.0023	0.6516	0.8453
[Face2] / encrypted with RC6 + Rubik's technique	0.1322	0.0038	0.5876	0.8460
[Face3] / encrypted with AES + Rubik's technique	0.1904	0.0010	0.5874	0.8461
[Face4] / encrypted with RC6 + Rubik's technique	0.1976	0.0037	0.5957	0.8448
[Face5] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2030	0.0033	0.6000	0.8462
[Face6] / encrypted with AES + Rubik's technique	0.1928	0.0050	0.5946	0.8464
[Face7] / encrypted with RC6 + Rubik's technique	0.1858	0.0038	0.6000	0.8460
[Face8] / encrypted with AES + Rubik's technique	0.1262	0.0072	0.5784	0.8465
[Face9] / encrypted with chaotic map in CFB mode + Rubik's technique	0.1873	0.0053	0.5891	0.8457

Table 4
Correlation values for the multiplexed encrypted faces of sample2 stream.

Multiplexed images of sample2	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique)	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode+Rubik's technique	0.2722	0.0024	1.0000	1.0000
[Face2] / encrypted with RC6 +Rubik's technique	0.2970	0.0020	0.8811	-0.0027
[Face3] / encrypted with AES+Rubik's technique	0.3318	0.0000	0.7763	0.0028
[Face4] / encrypted with RC6 +Rubik's technique	0.2929	0.0022	0.8131	0.0048
[Face5] / encrypted with chaotic map in CFB mode+Rubik's technique	0.2240	-0.0016	0.6404	0.0000
[Face6] / encrypted with AES+Rubik's technique	0.0148	-0.0020	0.6020	-0.0006
[Face7] / encrypted with RC6 +Rubik's technique	0.2322	-0.0080	0.7923	-0.0071
[Face8] / encrypted with AES+Rubik's technique	0.0028	-0.0037	0.7941	-0.0041
[Face9] / encrypted with chaotic map in CFB mode+Rubik's technique	0.2643	0.0001	0.7167	0.0023

Table 5
Correlation values for the jointly-encrypted faces of sample2 stream at SNR= 5 dB.

Jointly-encrypted images of sample2	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2722	0.0061	0.5674	0.6663
[Face2] / encrypted with RC6 + Rubik's technique	0.2970	0.0041	0.5512	0.6677
[Face3] / encrypted with AES + Rubik's technique	0.3318	0.0020	0.5427	0.6658
[Face4] / encrypted with RC6 + Rubik's technique	0.2929	0.0122	0.5420	0.6617
[Face5] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2240	0.0007	0.4624	0.6668
[Face6] / encrypted with AES + Rubik's technique	0.0148	0.0012	0.4639	0.6669
[Face7] / encrypted with RC6 + Rubik's technique	0.2322	0.0021	0.5861	0.6655
[Face8] / encrypted with AES + Rubik's technique	0.0028	0.0014	0.6220	0.6660
[Face9] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2643	0.0000	0.5498	0.6670

encrypted images [42].

6.1. Probability distributions

The PTD is the probability distribution of the correlation between the true faces (authorized patterns) and the encrypted biometric templates, and the PFD is the probability distribution of the correlation between the false faces (unauthorized patterns) and the encrypted biometric templates. The point of the intersection between these two curves is the threshold point. Access to the system is granted only if the score for the test face is higher than the threshold with an error probability, which can be determined as the area

Table 6
Correlation values for the jointly-encrypted faces of sample2 stream at SNR= 10 dB.

Jointly-encrypted images of sample2	Correlation with a false face	Correlation with a false face	Correlation with a true face	Correlation with a true face
	kernel technique	Rubik's technique	kernel technique	Rubik's technique
[Face1] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2722	0.0061	0.7650	0.8458
[Face2] / encrypted with RC6 + Rubik's technique	0.2970	0.0041	0.7562	0.8478
[Face3] / encrypted with AES + Rubik's technique	0.3318	0.0020	0.7489	0.8468
[Face4] / encrypted with RC6 + Rubik's technique	0.2929	0.0122	0.7488	0.8460
[Face5] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2240	0.0007	0.6749	0.8462
[Face6] / encrypted with AES + Rubik's technique	0.0148	0.0012	0.6917	0.8462
[Face7] / encrypted with RC6 + Rubik's technique	0.2322	0.0021	0.7914	0.8466
[Face8] / encrypted with AES + Rubik's technique	0.0028	0.0014	0.8179	0.8467
[Face9] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2643	0.0000	0.7597	0.8473

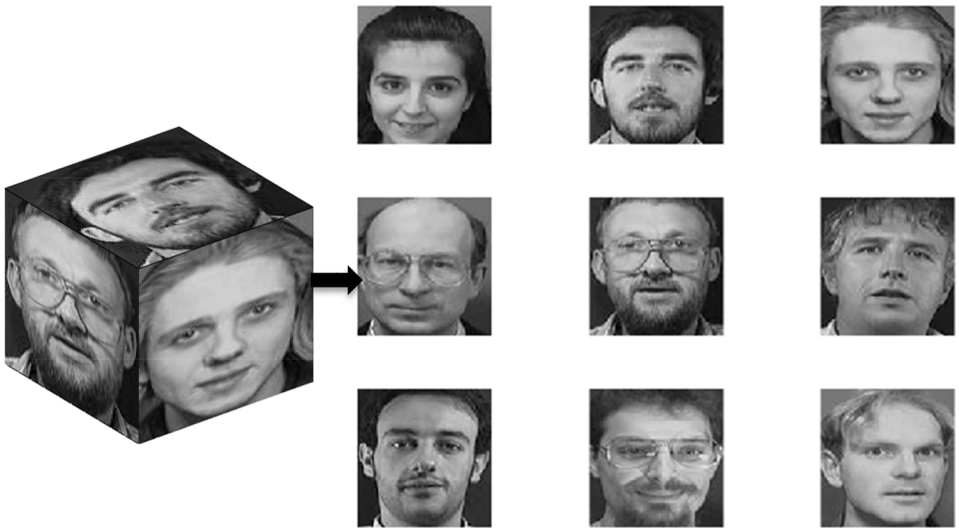


Fig. 24. Conversion of the 3D Rubik's cube faces into a 2D image for the tested images of sample3.

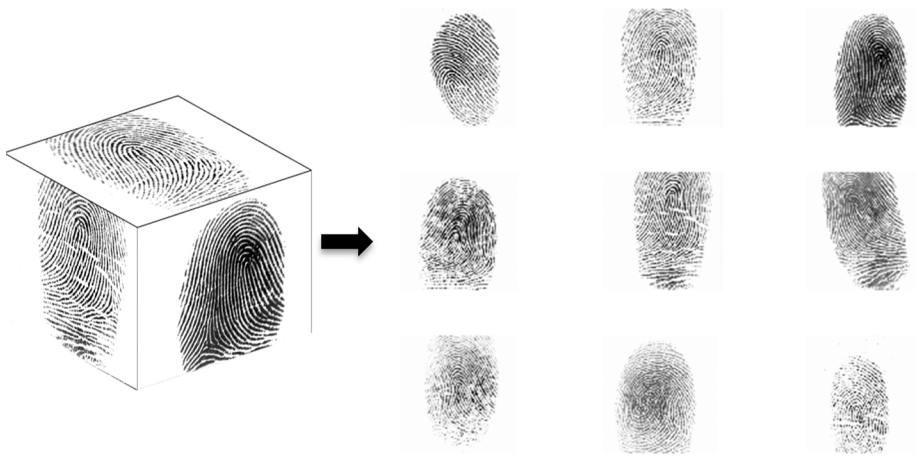


Fig. 25. Conversion of the 3D Rubik's cube faces into a 2D image for images of sample4 images.

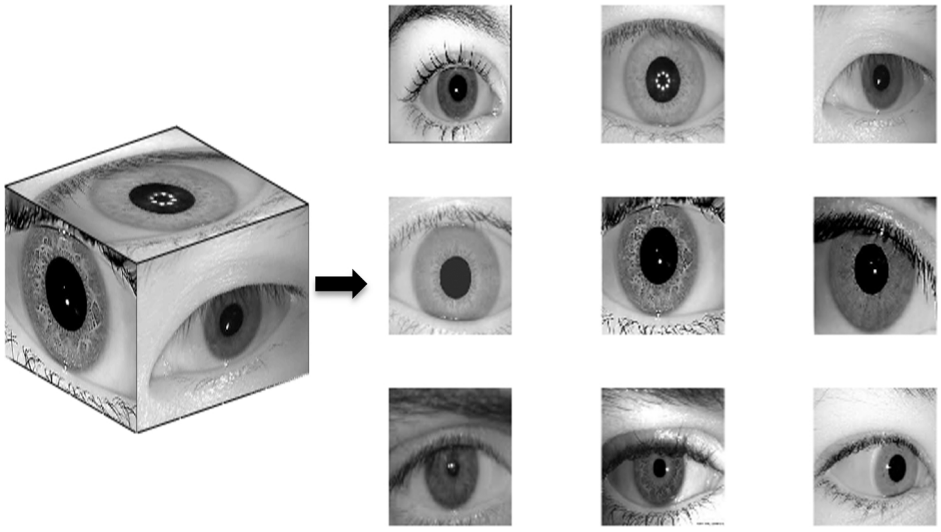


Fig. 26. Conversion of 3D Rubik's cube faces into a 2D image for sample5 images.

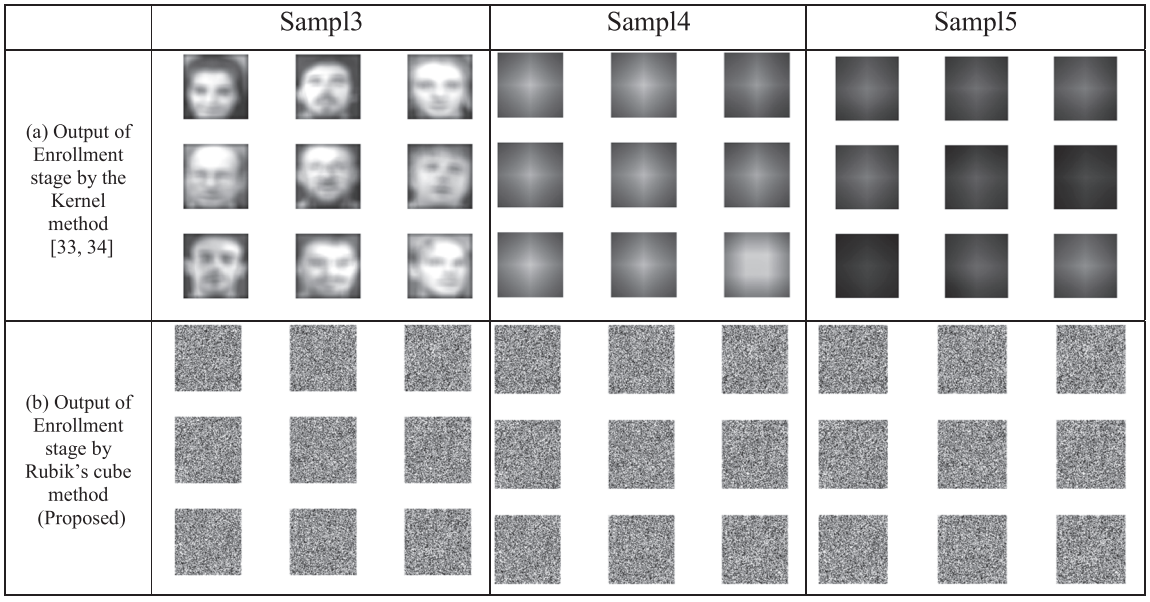


Fig. 27. Enrollment stage output for kernel and Rubik's cube encryption of the nine sample3, sample4 and sample5 images.

under the Probability Density Function (PDF) curve after the threshold value. The probability of correct detection can be easily obtained from the error probability. The lower the error probability, the better the system performance is.

6.2. *Correlation coefficient*

To clarify the influence of employing the suggested hybrid encryption framework, we test two different samples cases. The tested simulation case depends on the selection of the first nine images of sample1 and sample2 streams, separately to be the faces of the proposed Rubik's cube, as shown in Figs. 11 and 12. Then, we encrypt each of these nine images on the Rubik's cube faces for each sample stream individually with different encryption algorithms including chaotic encryption with CFB mode, RC6, and AES. We have carried out several random simulation experiments to check the best encryption algorithm that must be selected for each image on the Rubik's cube faces in oeder to achieve the best encryption performance. Finally, we found that the best encryption results can be achieved in the case of choosing the Rubik's cube faces with chaotic encryption with CFB mode, RC6, AES, RC6, chaotic encryption with CFB mode, AES, RC6, AES, and chaotic encryption with CFB mode, respectively. Finally, we compared the performance of the proposed encryption framework with and without employing the proposed Rubik's cube encryption technique.

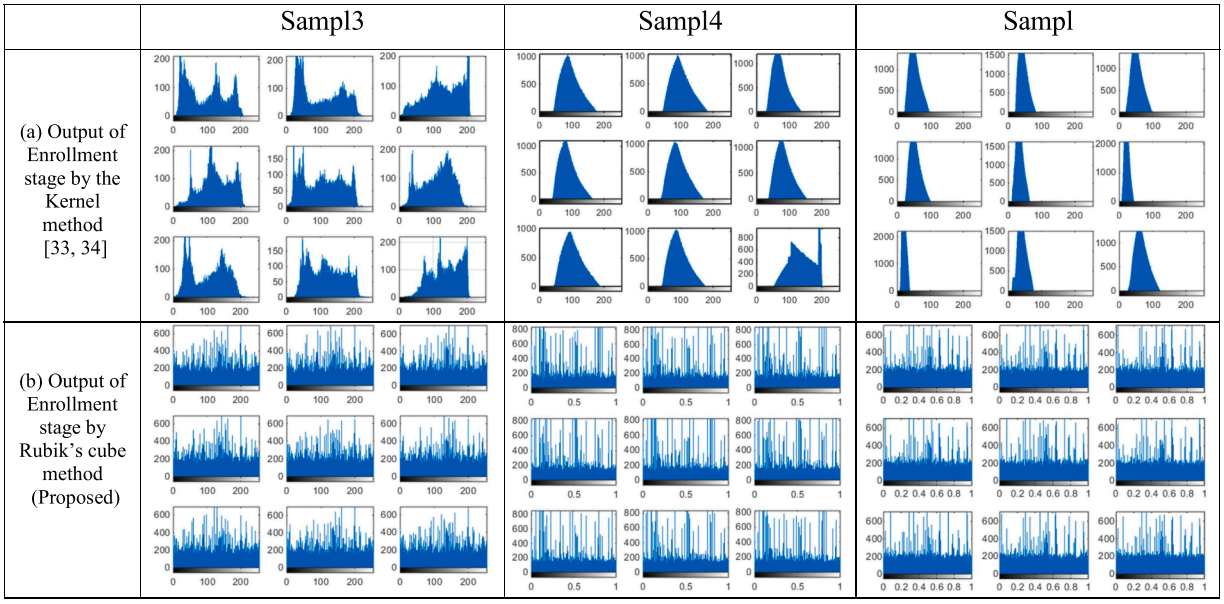


Fig. 28. Enrollment stage output histograms for kernel and Rubik's cube encryption of the nine sample3, sample4 and sample5 images.

6.3. *Receiver operating characteristic (ROC) curve analysis*

In the ROC curve, the true positive rate (Sensitivity) is plotted as function of the false positive rate for different cut-off points. Each point on the ROC curve represents a sensitivity/specificity pair corresponding to a particular decision threshold. For example, a test with perfect discrimination (no overlap in the two distributions) has a ROC curve that passes through the upper left corner (100% sensitivity, and 100% specificity). Therefore, the closer the ROC curve to the upper left corner, the higher the test overall accuracy is.

6.4. *Processing time*

The average times of the different tested cases with and without employing the Rubik's cube encryption have been estimated. It is noticed that the case of using Rubik's cube encryption needs short time in processing, as shown in Table 1 and Table 4. The real time of the Rubik's cube encryption itself is very short. The computational times of the traditional RC6, AES, and chaotic encryption algorithms can be reduced significantly with parallel processing in the case of employing all algorithms, simultaneously.

7. Simulation results

Wrong reference Table 1, 4

7.1. *Simulation results of face samples*

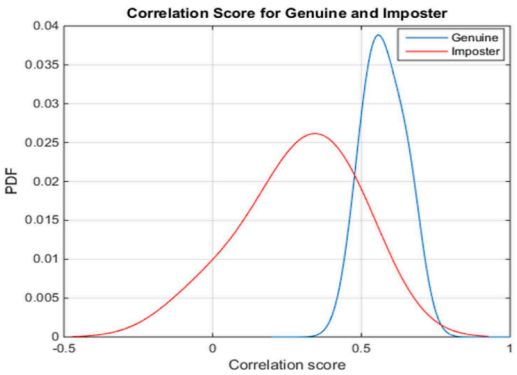
In order to test and evaluate the performance of the proposed cancelable face recognition scheme, we have carried out the proposed framework on images taken from the ORL database of faces, which was built between 1992 and 1994 at the laboratories of Cambridge University [40]. This database comprises ten different images for 40 distinctive subjects taken at different times, illumination conditions, and facial expressions.

To validate the proposed cancelable face recognition system, we have worked on 18 images from the ORL database that were selected randomly. The cancelable templates are extracted from these images with two different scenarios for comparison: the fully proposed cancelable face recognition scenario illustrated in Fig. 11 and the Rubik's cube scenario, which is shown in Fig. 13. In the simulation, the first testing sample is for nine different faces of the same person with nine different emotions, and the second sample is for nine different persons, as shown in Fig. 14 and Fig. 19. Each face is of 256 × 256 pixels. In the authentication stage, two face images have been tested. One belongs to an authorized user, and the other belongs to an unauthorized user. The test users enter the PIN and generate the random convolution kernel or enter the key to generate the Rubik's cube output. It is assumed that the unauthorized user knows the right PIN or key for an authorized user to test the degree of security of the system. Finally, the correlation coefficients are calculated between each of the two encrypted faces and the nine encrypted biometric templates.

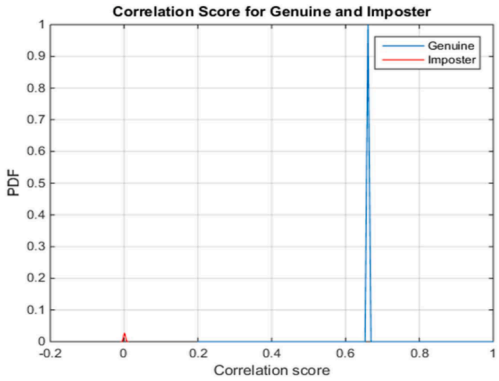
rubik's cube output???

We plot the PTD and PFD curves with different encryption algorithms to determine the threshold and error probability in three different cases of no noise as shown in Fig. 16, of SNR = 5 dB as shown in Fig. 17 and of SNR=10 dB as shown in Fig. 18 for sample1. We repeat the same results in Fig. 21, Fig. 22 and Fig. 23 for sample2. The intersection between the two curves determines the threshold value used to decide whether the user is an authorized user or not. From the obtained PTD, PFD, and AROC results of the two tested simulation cases, we notice the significance of exploiting the proposed Rubik's cube encryption technique for achieving better

Sample3

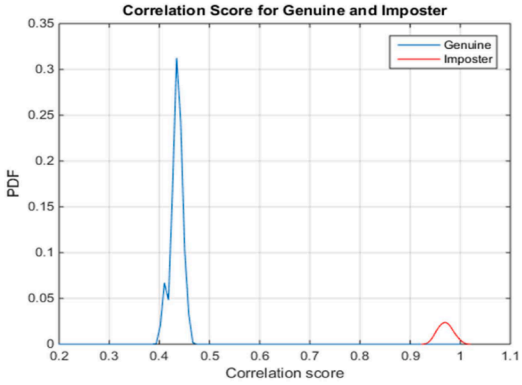


(a) PTD and PFD curves in the case of the Kernel scheme [40].

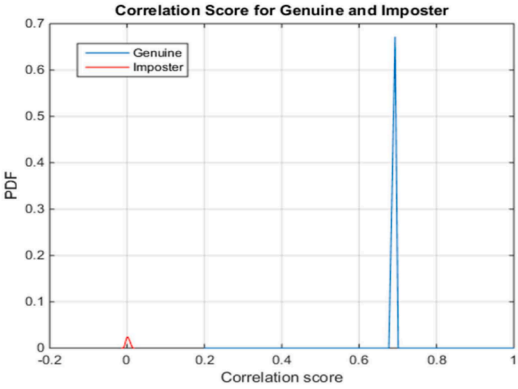


(b) PTD and PFD curves in the case of Rubik's cube scheme.

Sample4

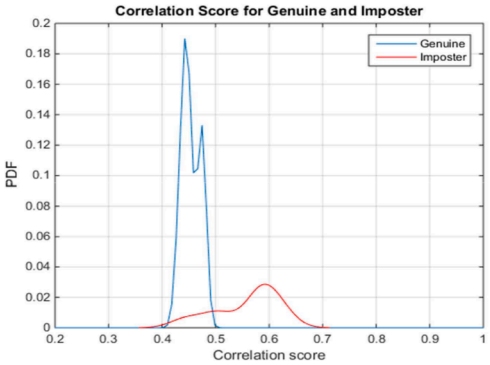


(c) PTD and PFD curves in the case of the Kernel scheme [40].

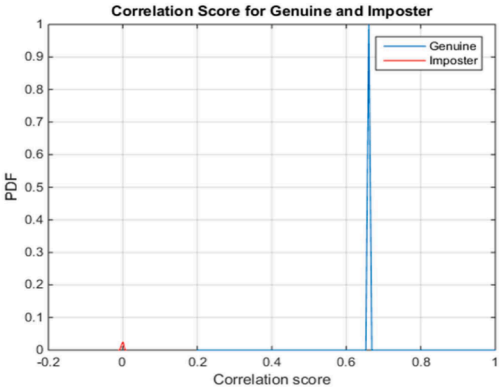


(d) PTD and PFD curves in the case of Rubik's cube scheme.

Sample5



(e) PTD and PFD curves in the case of the Kernel scheme [40].



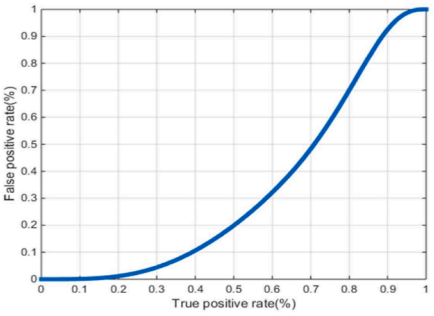
(f) PTD and PFD curves in the case of Rubik's cube scheme.

Fig. 29. The PTD, PFD, and ROC curves of the authentication stage for the proposed cancelable biometric system based on Rubik's cube technique compared to the state-of-the-art kernel based scheme on the nine tested biometric images of sample3, sample4 and sample5 at SNR= 5 dB.

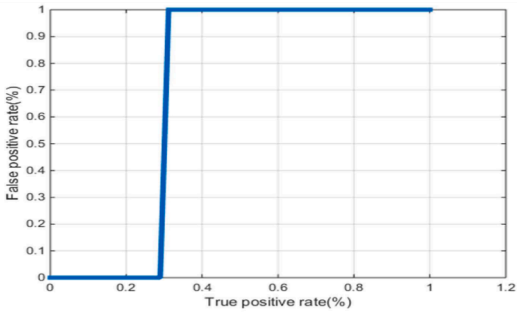
performance in the cancelable biometric systems compared to the utilization of the traditional techniques [36,37,39,41].

Fig. 15 and Fig. 20 show the results of the enrollment stage for the classic and the proposed Rubik's cube encryption for the two tested biometrics samples. It is noticed from the two tested simulation cases that the full proposed hybrid encryption framework based on Rubik's cube encryption is recommended and appreciated for an efficient cancelable biometric system compared to traditional techniques [36,41].

Sample3

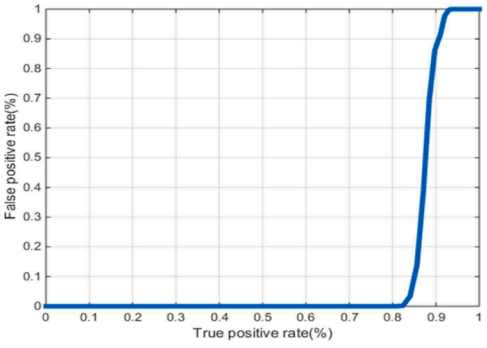


(g) ROC curve in the case of Kernel scheme [40], AROC= 0.33.

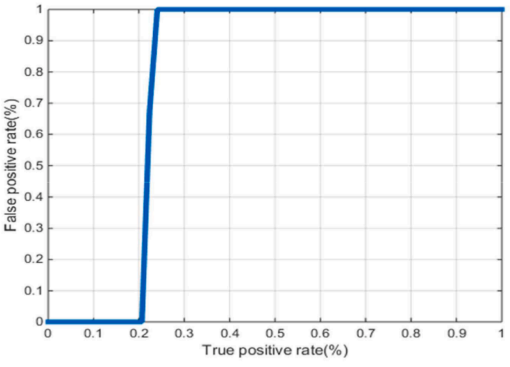


(h) ROC curve in the case of Rubik's cube scheme, AROC= 0.70.

Sample4

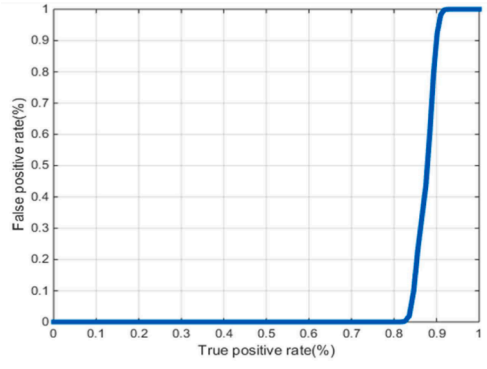


(i) ROC curve in the case of the Kernel scheme [40], AROC= 0.12.

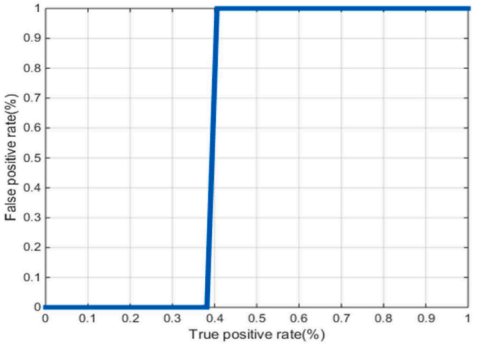


(j) ROC curve in the case of Rubik's cube scheme, AROC=0.77.

Sample5



(k) ROC curve in the case of the Kernel scheme [40], AROC= 0.13.



(l) ROC curve in the case of Rubik's cube scheme, AROC= 0.61.

Fig. 29. (*continued*).

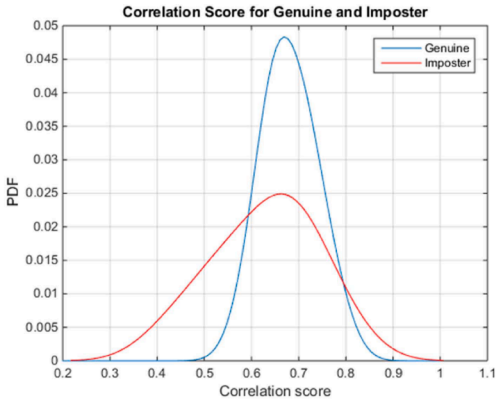
Tables 1–6 show the correlation test results for the nine frames of sample1 and sample2 sequences for the proposed encryption algorithms with and without the Rubik's cube technique. In addition, from the obtained correlation values of the two tested simulation cases, the results prove the significance of exploiting the proposed Rubik's cube encryption technique to achieve good performance for cancelable biometric systems compared to traditional techniques [36,37,41].

7.2. Simulation results of face, fingerprint, and iris samples

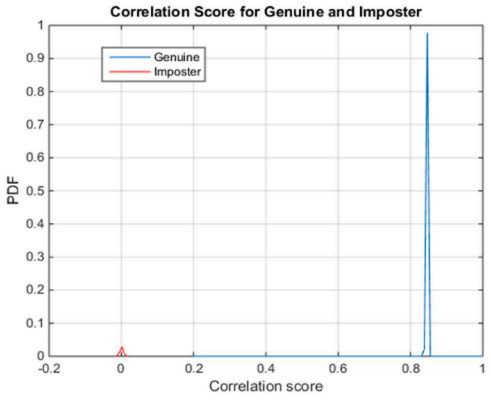
In the second part of the simulation results, we worked on three different samples to make sure that our framework is efficient for a wide variety of samples. The third testing sample comprises nine different faces for nine different persons, the fourth sample is for nine different fingerprints and the fifth sample is for nine different irises as shown in Fig. 24, Fig. 25 and Fig. 26, respectively. Each image has 256 × 256 pixels.

We plot the PTD and PFD curves for the proposed cancelable biometric system to determine the threshold and error probability for

Sample3

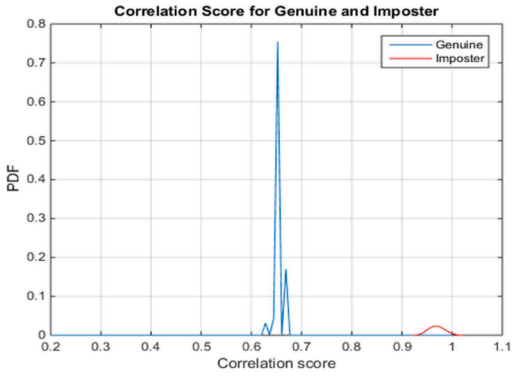


(a) PTD and PFD curves in the case of the Kernel scheme [40].

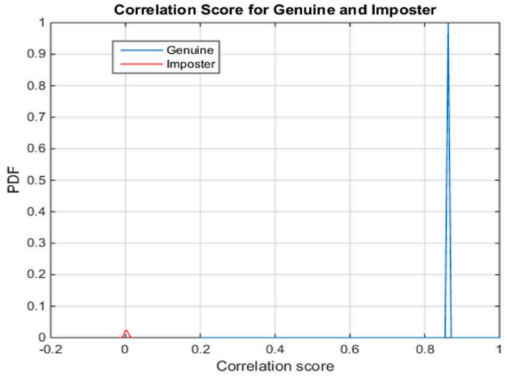


(b) PTD and PFD curves in the case of Rubik's cube scheme.

Sample4

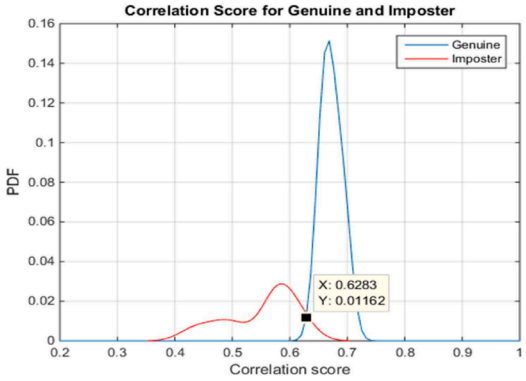


(c) PTD and PFD curves in the case of the Kernel scheme [40].

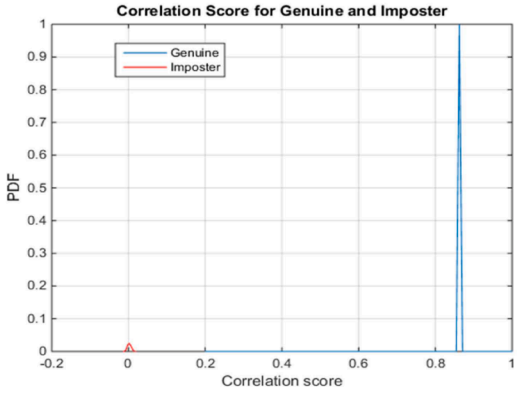


(d) PTD and PFD curves in the case of Rubik's cube scheme.

Sample5



(e) PTD and PFD curves in the case of the Kernel scheme [40].

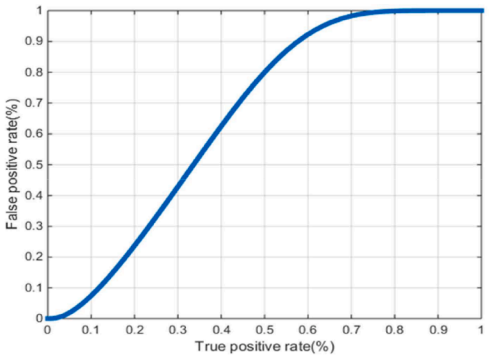


(f) PTD and PFD curves in the case of Rubik's cube scheme.

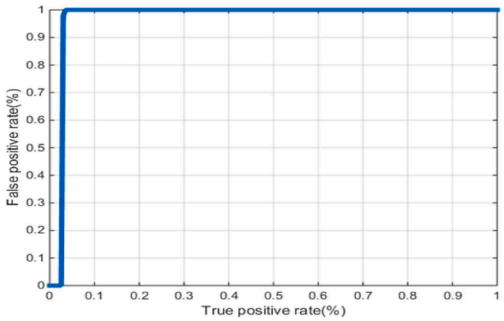
Fig. 30. PTD, PFD, and ROC curves of the authentication stage for the proposed cancelable biometric system based on SIFT+DRPE+ Rubik's cube encryption compared to the state-of-the-art DRPE and SIFT+DRPE scheme on the nine tested biometric images of sample3, sample4, and sample3 at SNR= 10 dB.

three different cases, comprising the ideal case in Fig. 13 and the non-ideal cases with noise at SNR = 5 dB and 10 dB as shown in Fig. 29, and Fig. 30, respectively, for sample3, sample4, and sample5 images. The intersection between the two curves determines the threshold value used to decide, whether this user is authorized or not. From obtained PTD, PFD, and AROC results of the three tested simulation cases, the significance of exploiting the proposed Rubik's cube encryption technique to achieve better performance for the cancelable biometric system is very clear [36,37,39].

Sample3

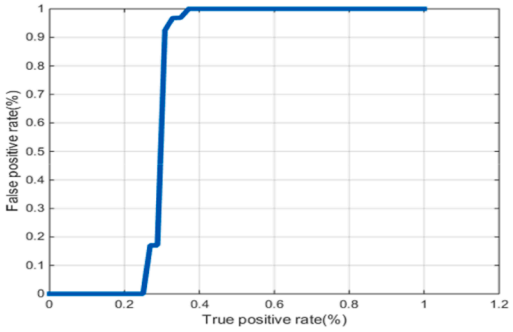


(g) ROC curve in the case of the Kernel scheme [40], AROC=0.66.

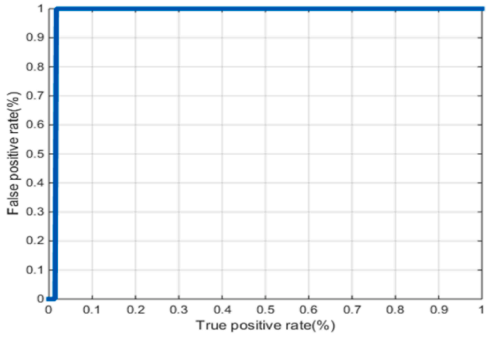


(h) ROC curve in the case of Rubik's cube scheme, AROC= 0.98.

Sample4

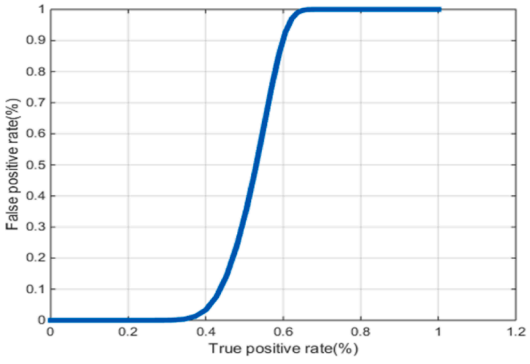


(i) ROC curve in the case of the Kernel scheme [40], AROC=0.71.

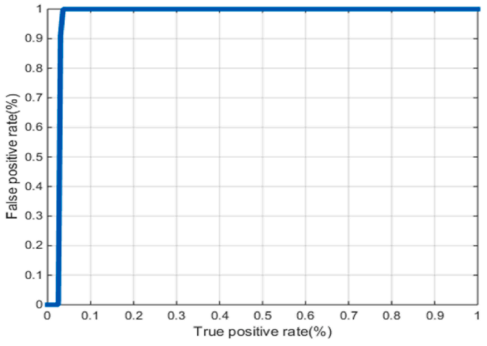


(j) ROC curve in the case of Rubik's cube scheme, AROC= 0.98.

Sample5



(k) ROC curve in the case of the Kernel scheme [40], AROC=0.46.



(l) ROC curve in the case of Rubik's cube scheme, AROC= 0.98.

Fig. 30. (*continued*).

Fig. 27 and Fig. 28 show the output results of the enrollment stage and their histograms for the classic and the proposed Rubik's cube technique for three tested biometric samples. It is noticed from the three tested simulation cases that the full proposed hybrid encryption framework with the proposed Rubik's cube encryption is recommended and appreciated for an efficient cancelable biometric system compared to the traditional techniques [36,37,39].

Tables 7–8 show the correlation values of the nine encrypted images of sample3, sample4, and sample5 for the proposed encryption framework with and without the Rubik's cube encryption. Moreover, from the obtained correlation values for the two tested simulation cases, the results prove the significance of exploiting the Rubik's cube encryption technique to achieve good performance of the cancelable biometric system compared to traditional techniques [36,37,39].

Finally, we discuss the complexity of the proposed framework by adding the processing time in Table 9. The computational times of the proposed framework with Rubik's cube technique and that with the traditional kernel method are compared. It is noticed that the case of using AES+RC6 +Rubik's cube encryption needs more time in processing, when it is compared with the kernel-based method due to the large processing time of the AES and RC6 algorithms. In comparison, the real time of the Rubik's cube technique itself is very

Table 7
Correlation values for the jointly encrypted nine biometrics images at SNR= 5 dB.

	Correlation with a false image of Sample3		Correlation with a true image of sample3		Correlation with a false image of Sample4		Correlation with a true image of sample4		Correlation with a false image of sample5		Correlation with a true image of sample5	
	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)
[Face1] / encrypted with chaotic map in CFB mode + Rubik's technique	0.0459	0.0021	0.4795	0.5694	0.9714	0.0077	0.4425	0.6884	0.6106	0.1854	0.0017	0.4467
[Face2] / encrypted with RC6 +Rubik's technique	0.0989	0.0003	0.5737	0.5657	0.9810	0.0032	0.4267	0.6908	0.5770	0.1723	0.0027	0.4305
[Face3] / encrypted with AES+Rubik's technique	0.4120	0.0003	0.5864	0.4660	0.9561	0.0025	0.4521	0.6870	0.5827	0.1042	0.0045	0.4554
[Face4] / encrypted with RC6 +Rubik's technique	0.3851	0.0018	0.5405	0.4739	0.9799	0.0018	0.4367	0.6894	0.5868	0.1586	0.0009	0.4409
[Face5] / encrypted with chaotic map in CFB mode + Rubik's technique	0.2674	0.0026	0.6266	0.5259	0.9633	0.0004	0.4313	0.6823	0.4425	0.1018	0.0004	0.4764
[Face6] / encrypted with AES+Rubik's technique	0.2787	0.0002	0.5137	0.4285	0.9634	0.0028	0.4317	0.6869	0.4909	0.2027	0.0019	0.4751
[Face7] / encrypted with RC6 +Rubik's technique	0.2622	0.0003	0.5333	0.5058	0.9723	0.0038	0.4393	0.6920	0.5171	0.1338	0.0008	0.4475
[Face8] / encrypted with AES+Rubik's technique	0.5021	0.0045	0.6567	0.4728	0.9937	0.0084	0.4387	0.6868	0.5911	0.2800	0.0038	0.4721
[Face9] / encrypted with chaotic map in CFB mode +Rubik's technique	0.4725	0.0031	0.6554	0.4101	0.9493	0.0007	0.4103	0.6877	0.6277	0.1848	0.0016	0.4413

Table 8
Correlation values for the jointly encrypted nine biometrics images at SNR= 10 dB.

.	Correlation with a false image of sample3		Correlation with a true image of sample3		Correlation with a false face image of sample4		Correlation with a true image of sample4		Correlation with a false image of sample5		Correlation with a true image of sample5	
	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)	Kernel [40]	Rubik's cube (Proposed)
[Face1] / encrypted with + Rubik's technique	0.0464	0.0019	0.8429	0.8430	0.9710	0.0077	0.6530	0.8599	0.6052	0.0017	0.6705	0.8426
[Face2] / encrypted with RC6 +Rubik's technique	0.0949	0.0004	0.8401	0.8457	0.9809	0.0032	0.6489	0.8595	0.5687	0.0027	0.6547	0.8434
[Face3] / encrypted with AES+Rubik's technique	0.4077	0.0089	0.7587	0.8417	0.9538	0.0025	0.6672	0.8591	0.5822	0.0045	0.6701	0.8431
[Face4] / encrypted with RC6 +Rubik's technique	0.3802	0.0018	0.7321	0.8411	0.9793	0.0018	0.6495	0.8596	0.5814	0.0009	0.6527	0.8418
[Face5] / encrypted with + Rubik's technique	0.2629	0.0049	0.8158	0.8429	0.9624	0.0004	0.6508	0.8570	0.43 36	0.0004	0.6979	0.8402
[Face6] / encrypted with AES+Rubik's technique	0.2743	0.0013	0.7374	0.8417	0.9625	0.0028	0.6515	0.8578	0.4761	0.0019	0.6835	0.8408
[Face7] / encrypted with RC6 +Rubik's technique	0.2588	0.0039	0.7890	0.8420	0.9704	0.0038	0.6500	0.8608	0.5072	0.0008	0.6678	0.8420
[Face8] / encrypted with AES+Rubik's technique	0.5035	0.0073	0.7818	0.8435	0.9932	0.0084	0.6473	0.8595	0.5786	0.0038	0.6932	0.8422
[Face9] / encrypted with chaotic map in CFB mode +Rubik's technique	0.4697	0.0021	0.6933	0.8438	0.9496	0.0007	0.6314	0.8594	0.6230	0.0016	0.6597	0.8407

Table 9
Processing times for five different samples with kernel, hybrid proposed, and Rubik's cube techniques.

Algorithm	Sample1	Sample2	Sample3	Sample4	Sample5
Kernel technique	7.41 Sec.	5.26 Sec.	6.99 Sec.	9.10 Sec.	6.72 Sec.
Hybrid proposed technique	7963.77 Sec.	4990.54 Sec.	62,035.54 Sec.	3630.54 Sec.	9943.77 Sec.
Rubik's cube technique	4 Sec.	2.73 Sec.	3.85 Sec.	4.13 Sec.	2.87 Sec.

FAR: False Acceptance Rate, EER: Equal Error Rate, AROC: Area beneath ROC curve, FRR: False Rejection Rate

Table 10
Comparison of the suggested cancelable biometric recognition system with the previous ones.

Cancelable biometric recognition system	FAR	EER	AROC	FRR
Proposed	0.0060	0.0021	0.9996	0.0014
Ref. [10]	0.0296	0.0039	0.9236	0.1139
Ref. [11]	0.0527	0.0086	0.9416	0.0372
Ref. [13]	0.0946	0.0219	0.8920	0.2983
Ref. [14]	0.0741	0.0622	0.9343	0.0667
Ref. [16]	0.0632	0.0436	0.9592	0.0279
Ref. [24]	0.0071	0.0178	0.8967	0.0579
Ref. [25]	0.0359	0.0862	0.9274	0.0129
Ref. [28]	0.0167	0.0195	0.9728	0.0134
Ref. [32]	0.0038	0.0096	0.9372	0.0926
Ref. [41]	0.0497	0.0351	0.9583	0.2836
Ref. [42]	0.0263	0.0096	0.9673	0.0192

short. Therefore, although the computational time of the traditional RC6, AES, and chaotic encryption algorithms can be reduced significantly with parallel processing during the Rubik's cube merging step, the processing time of the proposed framework is more than those of some related works, but it is still suitable for real-time applications and also for offline applications.

Therefore, from all presented objective and subjective results, it is recognized that the proposed hybrid encryption framework with the Rubik's cube technique is appreciated and recommended for building robust cancelable biometric systems compared to the traditional techniques [36,37,39]. Furthermore, the proposed hybrid encryption framework has preferable objective and visual simulation results compared to those of the case without Rubik's cube encryption. Furthermore, it is noticed that the suggested hybrid encryption framework gives adequate experimental results for different biometric templates.

For additional verification of the competence of the suggested framework for consistent cancelable biometric recognition, further studies are carried out for comparing the outcomes of the suggested cancelable biometric system with the recent literature works in [10,11,13,14,16,24,25,28,32,41,42]. We compared the FAR, Equal Error Rate (EER), AROC, and FRR results with the suggested framework with those of the previous recent works as summarized in Table 10. The offered outputs in Table 10 demonstrate that the FAR, EER, AROC, and FRR of the suggested framework-based cancelable biometric recognition system are superior and highly recommended compared to those of traditional cancelable biometric systems.

8. Conclusions and future work

This paper presented an improved hybrid encryption framework for an efficient cancelable biometric system that is more secure against hackers. The major contribution of this work is the inclusion of Rubik's cube encryption in the hybrid framework comprising AES, RC6, and chaotic encryption algorithms. The proposed hybrid encryption framework adds more permutation and diffusion to the encrypted biometric images. Experimental simulation results verified the heartening achievements of the proposed hybrid encryption framework in efficiently encrypting the stored biometric images. So, it is more qualified for securing biometric templates compared to the traditional techniques. Moreover, it provides appreciated PTDs, PFDs, ROC curves, correlation values, and processing times. Hence, the proposed hybrid encryption framework has proved its capability of adequately encrypting various biometric datasets. Moreover, the simulation results expounded the prominence of implementing the proposed Rubik's cube encryption with the traditional encryption algorithms to reinforce the ability to generate cancelable biometric templates likewise acquiring considerable subjective and objective results. In the future work, it will be appropriate to study different cases of biometric Rubik's cube cryptosystems with different key arrangements.

Declaration of Competing Interest

No conflict exists: Authors declare that they have no conflict of interest.

References

[1] M.A. Ben Farah, R. Guesmi, A. Kachouri, M. Samet, A new design of cryptosystem based on S-box and chaotic permutation", Multimed. Tools Appl. (2020).
[2] W. El-Shafai, E.S.M. El-Rabaie, M. El-Halawany, F.E. Abd El-Samie, Efficient multi-level security for robust 3D color-plus-depth HEVC, Multimed. Tools Appl. 77 (23) (2018) 30911–30937.

[3] W. El-Shafai, Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission, 3D Research 6 (1) (2015) 10.
[4] E.M. El-Bakary, W. El-Shafai, S. El-Rabaie, O. Zahran, M. El-Halawany, F.E. Abd El-Samie, Proposed enhanced hybrid framework for efficient 3D-MVC and 3D-HEVC wireless communication, Multimed. Tools Appl. 78 (11) (2019) 14173–14193.
[5] W. El-Shafai, A.K. Mesrega, H.E. Ahmed, N. Abdelwahab, F.E. Abd El-Samie, An efficient multimedia compression-encryption scheme using latin squares for securing internet of things networks, J. Inf. Secur. Appl. 64 (2022), 103039.
[6] O.S. Faragallah, W. El-Shafai, A.I. Sallam, I. Elashry, E.S.M. EL-Rabaie, A. Afifi, H.S. El-sayed, Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication, J. Ambient Intell. Humaniz. Comput. (2021) 1–25.
[7] W. El-Shafai, E.M. El-Bakary, S. El-Rabaie, O. Zahran, M. El-Halawany, F.E. Abd El-Samie, Efficient 3D watermarked video communication with chaotic interleaving, convolution coding, and LMMSE Equalization, 3D Research 8 (2) (2017) 1–24.
[8] N.F. Soliman, M.I. Khalil, A.D. Algarni, S. Ismail, R. Marzouk, W. El-Shafai, Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication, Multimed. Tools Appl. 80 (3) (2021) 4789–4823.
[9] O.S. Faragallah, E.A. Naeem, W. El-Shafai, N. Ramadan, H.E.H. Ahmed, M.M.A. Elnaby, I. Elashry, S.E. El-khamy, F.E.A. El-Samie, Efficient chaotic-Baker-map-based cancelable face recognition, J. Ambient Intell. Humaniz. Comput. (2021) 1–39.
[10] A. Alarifi, M. Amoon, M.H. Aly, W. El-Shafai, Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system, IEEE Access 8 (2020) 221246–221268.
[11] A.D. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F.E.A. El-Samie, N. F Soliman, Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications, Entropy 22 (12) (2020) 1361.
[12] W. El-Shafai, I.M. Almomani, A. Alkhayer, Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication, IEEE Access 9 (2021) 35004–35026.
[13] I.S. Badr, A.G. Radwan, E.R. El-Sayed, L.A. Said, G.M. El Banby, W. El-Shafai, F.E. Abd El-Samie, Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion, Digit. Signal Process. 116 (2021), 103103.
[14] W. El-Shafai, F.A.H.E. Mohamed, H.M. Elkamchouchi, M. Abd-Elnaby, A. ElShafee, Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm, IEEE Access 9 (2021) 77675–77692.
[15] I. Eldokany, E.S.M. El-Rabaie, S.M. Elhalafawy, M.A.Z. Eldin, M.H. Shahieen, N.F. Soliman, F.E.A. El-Samie, "Efficient transmission of encrypted images with OFDM in the presence of carrier frequency offset.", Wirel. Pers. Commun. 84 (2015) 475–521.
[16] H.A.A. El-Hameed, N. Ramadan, W. El-Shafai, A.A. Khalaf, H.E.H. Ahmed, S.E. Elkhamy, F.E.A. El-Samie, Cancelable biometric security system based on advanced chaotic maps, Vis. Comput. (2021) 1–17.
[17] O.S. Faragallah, M.A. Alzain, H.S. El-Sayed, J.F. Al-Amri, W. El-Shafai, A. Afifi, B. Soh, Block-based optical color image encryption based on double random phase encoding, IEEE Access 7 (2018) 4184–4194.
[18] M. Helmy, W. El-Shafai, S. El-Rabaie, I.M. El-Dokany, F.E.A. El-Samie, Efficient security framework for reliable wireless 3D video transmission, Multidimens. Syst. Signal Process. (2021) 1–41.
[19] W. El-Shafai, F. Khallaf, E.S.M. El-Rabaie, F.E. Abd El-Samie, Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications, J. Ambient Intell. Humaniz. Comput. 12 (2021) 1–29.
[20] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, E.A. Naeem, M.A. Alzain, F.E. Abd El-Samie, Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications, IEEE Access 8 (2020) 42491–42503.
[21] W. El-Shafai, E.E.D. Hemdan, Robust and efficient multi-level security framework for color medical images in telehealthcare services, J. Ambient Intell. Humaniz. Comput. (2021) 1–16.
[22] A. Sedik, O.S. Faragallah, H.S. El-sayed, G.M. El-Banby, F.E.A. El-Samie, A.A. Khalaf, W. El-Shafai, An efficient cybersecurity framework for facial video forensics detection based on multimodal deep learning, Neural Comput. Appl. (2021) 1–18.
[23] El-Sayed M. Mai Helmy, Ibrahim El-Rabaie, M. Eldokany, E. Fathi, Abd El-Samie, Chaotic encryption with different modes of operation based on Rubik's cube for efficient wireless communication, Multimed. Tools Appl. (4 2018) 1–25.
[24] F.E. Abd El-Samie, R.M. Nassar, M. Safan, M.A. Abdelhamed, A.A. Khalaf, G.M. El Banby, W. El-Shafai, Efficient implementation of optical scanning holography in cancelable biometrics, Appl. Opt. 60 (13) (2021) 3659–3667.
[25] N.F. Soliman, A.D. Algarni, W. El-Shafai, F.E. Abd El-Samie, G.M. El Banby, An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics, CMC-Comput. Mater. Contin. 69 (2) (2021) 1571–1595.
[26] M. Helmy, E.S.M. El-Rabaie, I.M. Eldokany, F.E.A. El-Samie, 3-D image encryption based on Rubik's cube and RC6 algorithm, 3D Research 8 (2017) 38.
[27] O.S. Faragallah, H.S. El-Sayed, W. El-Shafai, Efficient opto MVC/HEVC cybersecurity framework based on arnold map and discrete cosine transform, J. Ambient Intell. Humaniz. Comput. (2021) 1–16.
[28] Ibrahim, S., Egila, M.G., Shawkey, H., Elsaid, M.K., El-Shafai, W., & Abd El-Samie, F.E. (2020, October). Hardware Implementation of Cancellable Biometric Systems. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 1145–1152). IEEE.
[29] O.S. Faragallah, H.S. El-sayed, A. Afifi, W. El-Shafai, Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional fourier transform, Opt. Lasers Eng. 137 (2021), 106333.
[30] A. Alarifi, S. Sankar, T. Altameem, K.C. Jithin, M. Amoon, W. El-Shafai, A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications, IEEE Access 8 (2020) 128548–128573.
[31] M.A. Ben Farah, A. Farah, T. Farah, An image encryption scheme based on a new hybrid chaotic map and optimized substitution box, Nonlinear Dyn. (2020).
[32] S. Ibrahim, M.G. Egila, H. Shawky, M.K. Elsaid, W. El-Shafai, F.E. Abd El-Samie, Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption, Multimed. Tools Appl. 79 (19) (2020) 14053–14078.
[33] X. Zhang, W. Nie, Y. Ma, Q. Tian, Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box, Multimed. Tools Appl. 76 (2017) 15641–15659.
[34] O.S. Faragallah, A. Afifi, W. El-Shafai, H.S. El-Sayed, M.A. Alzain, J.F. Al-Amri, F.E. Abd El-Samie, Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications, IEEE Access 8 (2020) 103200–103218.
[35] Das S., Mandal S.N., Ghoshal N., "Diffusion and Encryption of Digital Image Using Genetic Algorithm.", the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), 2015.
[36] V.M. Patel, N.K. Ratha, R. Chellappa, Cancelable biometrics: a review, IEEE Signal Process. Mag.: Spec. Issue Biom. Secur. Priv. 32 (5) (2015) 54–65.
[37] M. Savvides, B. Kumar, P. Khosla, Cancelable biometric filters for face recognition, Proc. Int. Conf. Pattern Recognit. 3 (2004) 922–925.
[38] N. Ratha, S. Chikkerur, J. Connell, R. Bolle, Generating cancelable fingerprint templates, IEEE Trans. Pattern Anal. Mach. Intell. 29 (4) (2007) 561–572.
[39] A.Teoh T.Connie, M.Goh, D.Ngo, Palm hashing: a novel approach to cancelable biometrics, Inf. Process. Lett. 93 (1) (2004) 1–5.
[40] ORL Database, accessed September 2018 ⟨https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase⟩. html.
[41] I.F. Elashry, W. El-Shafai, E.S. Hasan, S. El-Rabaie, A.M. Abbas, F.E. Abd El-Samie, O.S. Faragallah, Efficient chaotic-based image cryptosystem with different modes of operation, Multimed. Tools Appl. 79 (29) (2020) 20665–20687.
[42] D. Chang, S. Garg, M. Hasan, S. Mishra, Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3152–3167.