The Visual Computer (2022) 38:2171–2187
https://doi.org/10.1007/s00371-021-02276-2

ORIGINAL ARTICLE

# Cancelable biometric security system based on advanced chaotic maps

Hayam A. Abd El-Hameed[1] · Noha Ramadan[2,4] · Walid El-Shafai[3,4] · Ashraf A. M. Khalaf[1] · Hossam Eldin H. Ahmed[4] · Said E. Elkhamy[5] · Fathi E. Abd El-Samie[4,6]

Accepted: 1 August 2021 / Published online: 27 September 2021

## Abstract

In recent years, the protection of human biometrics has witnessed an exponential growth. Fingerprint recognition has been utilized for cell phone authentication, biometric passports, and airport security. To improve the fingerprint recognition process, different approaches have been proposed. To keep biometrics away from hacking attempts, non-invertible transformations or encryption algorithms have been proposed to provide cancelable biometric templates for biometric protection. This paper presents a scheme that depends on chaos-based image encryption with different chaotic maps. The chaotic maps are used instead of the simple random number generator to overcome the loss of randomness in the case of a large number of images. To preserve the authentication performance, we should convolve the training images with random kernels to build the encrypted biometric templates. We can obtain different templates from the same biometrics by varying the chaotic map used to generate the convolution kernels. A comparative study is introduced between the used chaotic maps to determine the one, which gives the best performance. The simulation experiments reveal that the enhanced quadratic map 3 achieves the lowest error probability of 3.861% in the cancelable fingerprint recognition system. The cancelable fingerprint recognition system based on this chaotic map achieves the largest probability of detection of 96.139%, with an Equal Error Rate (EER) of 0.593.

**Keywords** Cancelable biometric security · Authentication · Chaotic maps · Fingerprint recognition

## 1 Introduction

Due to the quick development of advanced information, cloud computing, and Internet of Things (IoT) applications, protection, and individual data security have got extraordinary mindfulness. The main difficulties within the validation frameworks include codes, individual recognizable Proof Identification Numbers (PINs), and passwords. Refined frameworks of individual security can be used for better confirmation and identification. In this way, biometric traits are utilized in different validation, check, and recognizable proof applications. The essential capacity of these

✉ Hayam A. Abd El-Hameed
hayamabdalmordy@yahoo.com

Noha Ramadan
eng_noharamadan@yahoo.com

Walid El-Shafai
walid.elshafai@al-eng-menofia.edu.eg

Ashraf A. M. Khalaf
ashkhalaf@yahoo.com

Hossam Eldin H. Ahmed
hhossamkh@yahoo.com

Said E. Elkhamy
elkhamy@ieee.org

Fathi E. Abd El-Samie
fathi_sayed@yahoo.com

[1] Department of Electronics and Electrical Communications, Faculty of Engineering, Minia University, Minya, Egypt

[2] Department of Electrical Engineering, Ahram Canadian University, 6th of October, Egypt

[3] Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia

[4] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[5] Department of Communication Engineering, Alexandria University, Alexandria, Egypt

[6] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 21974, Saudi Arabia

biometric frameworks incorporates selecting biometrics for certain people. After that, features are extracted and stored in datasets. Biometric schemes for the security of physiological traits of people, like face, iris, and fingerprint traits, are turning into a broad reality. The issue is that the clients use biometrics forever and cannot change them. It is recommended that irreversible transforms are applied to prevent biometrics from being stolen. To improve the security of fingerprint recognition, different features and algorithms have been proposed.

Generally, passwords and encryption keys are simply known to the client, yet can be utilized without the client's allowance. Accordingly, secrecy can not be achieved. In addition, biometrics like face, voice, and fingerprint can be recorded and abused without the client’s allowance. Therefore, these biometrics can be stolen, forever. Moreover, the stolen biometrics can be used in a cross-coordinating scenario [1].

To overcome the above-mentioned issues, the cancelable biometrics can be used. In a cancelable biometric framework, basic hashing functions or encryption schemes can be used to strengthen the protection and security of the framework. However, the hash functions are susceptible to minor changes in the information interaction. Practically, all biometric changes as indicated by environmental conditions may affect the obtained hash functions. For example, face and iris biometrics are exceptionally affected by light contrast. So, in practice, these functions cannot be used, directly.

In simple biometric encryption schemes, biometric traits are encrypted at the transmitter and decrypted at the receiver to allow authentication or verification using decrypted biometrics. Unfortunately, this strategy allows hacking scenarios as the decrypted biometrics may be stolen. On the other hand, the concept of cancelable biometrics depends on verification or authentication with encrypted or deformed biometrics. This trend of cancelable biometrics prevents cross-matching as a cancelable template can be generated for each application. In addition, it is infeasible for the attackers to try to get the original biometrics from the cancelable templates [2].

The main contributions of this paper can be summarized as follows:

1. Different types of chaotic maps are investigated and compared for biometric encryption.
2. A bio-convolving scheme is investigated, and new biometric encryption schemes are proposed.
3. The suggested encryption schemes are implemented in a cancelable biometric framework.

The contents of this paper are organized as follows. Section 2 gives the related work. Section 3 gives the chaotic map description. Section 4 introduces a scheme for biometric encryption based on convolution kernels. Section 5 introduces the description of the chaos-based cancelable biometric recognition system, its architecture and the authentication metrics. Section 6 gives the simulation results and discussion. Finally, Sect. 7 gives the concluding remarks.

## 2 Related work

Several strategies for producing cancelable biometric templates were produced in [3] to overcome the problem of cross-matching between biometric databases. These strategies work on fingerprint images to generate multiple cancelable templates. In essence, a user can use biometric identifiers as needed by issuing a new transformation key. The identifiers can be cancelled and replaced, when attacked. These strategies were applied on face and fingerprint biometrics. The biometric templates can be changed in the signal or feature domain. In [4], an alignment-free scheme to produce cancelable fingerprint biometrics was presented. This scheme is based on a circular curtailed convolution algorithm, which is one-way in nature. It can protect the biometric templates without the possibility to retrieve them from the convolution outcomes. This scheme achieves improvement in the ability to generate cancelable templates and the diversity of these templates.

In [5], the authors tried to overcome the problems of security, and trustiness of biometric templates generated from their scheme. This scheme is dependent on Double Random Phase Encoding (DRPE) and cepstral analysis. In the merged biometric template for each person, four biometrics are combined through Discrete Cosine Transform (DCT) compression. To guarantee security, the authors encrypt the unified biometric templates with the DRPE algorithm. The ability to generate cancelable templates is warranted by changing the random phase sequences of the DRPE algorithm. The compression is performed for all four biometrics by maintaining the most significant coefficients in the DCT domain. In the biometric recognition phase, the unified biometric templates are decrypted, and then a cepstral analysis scheme is applied for biometric verification.

In [6], the authors proposed a fingerprint- and finger-vein-based cancelable multi-biometric scheme. This scheme provides template authentication and verification. It merges the minutia-based feature set of fingerprints and the image-based feature set of finger-veins. In [7], the authors studied biometric recognition based on a pore feature-based scheme. This scheme discovers pores in the input fingerprint images with a Convolutional Neural Network (CNN) model. Then, a patch CNN-based descriptor is estimated for each uncovered pore. This high-resolution fingerprint recognition scheme achieves EERs of 2.91% and 0.57% on partial DBI and complete DBII fingerprints for the standard Poly UHRF dataset.

In [8], the authors presented a scheme for fingerprint recognition via deep learning using CNNs. In this scheme, fingerprint recognition was conducted on few available samples.

In [9], the authors provided a comprehensive review and insightful analysis of different types of biometric recognition schemes using deep learning. A comprehensive review of all schemes was presented, including network architectures, training data, and strategies. Both face, fingerprint, iris, palm print, ear, voice, signature, and gait recognition were considered in this paper. In [10], a cancelable fingerprint recognition scheme that depends on multiple spiral curves and fuzzy principles was presented. The fuzzy commitment scheme was used to perform encryption of minutiae features. This scheme achieved an EER of 1.17%. The authors of [11] stated that one of the advantages of cancelable biometrics is to save privacy. In order to save privacy, cancelable biometric transformations should be non-invertible. No information about the original biometric templates should be revealed from the cancelable templates. Also, the authors of [11] presented new cancelable biometric schemes based on bio-hashing. Those schemes depend on non-invertible transforms to protect privacy of users.

In [12], the authors presented a feature-based method for generating cancelable templates from 2D face images. The authors have used five public databases in their proposed scheme and used Speeded-Up Robust Features (SURF) and Scale-Invariant Feature Transform (SIFT) for feature extraction. The authors of [13] presented a merging scheme for aligning fingerprint images in the training set, followed by a learning descriptor for all pore patches using a patch matching model based on a CNN. The scheme in [14] presented a new feature descriptor for fake iris detection. This descriptor exploits the relationship between the center pixel and its hexa neighbor. A hexagonal shape using the six-neighbor approach is preferable to the rectangular structure due to its higher symmetry, consistent connectivity, and efficient use of space. The authors of [15] proposed some ideas to improve the bio-hashing scheme. This improved bio-hashing scheme was used to maintain a very low error rate, when nobody steals the hash key, and to reach a good performance when an attacker steals the hash key. The authors in [16] introduced a cancelable biometric recognition scheme based on producing secret keys for cryptographic methods. The authors of [17] proposed a scheme that encrypts the biometric templates, or training images, by convolving them with random convolution kernels. The authors used the seed to generate the random convolution kernels, which are utilized as the Personal Identification Numbers (PINs). The random kernels are saved and used in the authentication process.

In [18], a new architecture for template generation in the context of situation awareness systems in real and virtual applications was presented. The authors of this paper presented a cancelable biometric template generation algorithm using random biometric fusion, and random projection. This random cross-folding scheme generates cancelable biometric templates from multiple biometric traits.

In this paper, we investigate the efficiency of chaotic maps for the generation of cancelable biometric templates. In addition, the effect of chaotic map parameters on the cancelable biometric system is investigated. First, we investigate different types of chaotic maps to be used for the encryption of the biometric templates. Then, we discuss the effect of the kernel size.

## 3 Chaotic maps

Implementation of chaos-based cryptography depends on chaotic maps. A function whose domain (input) space and range (output) space are chaotic is called a chaotic map. Chaotic maps represent a class of dynamic systems in which time is discrete rather than being continuous. They exhibit a chaotic behavior for specific parameter values. In the next subsections, we present a brief description of some chaotic maps used in this paper.

### 3.1 Logistic map

Logistic map is a nonlinear dynamic map. It is one of the simple and popular chaotic maps [19]. The logistic map equation is as follows:

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

where $X_n$ is a value between 0 and 1, $n$ is the iteration index, and $r$ is a positive number between 0 and 4.

- **Bifurcation**

This property is referenced as qualitative bifurcation transition from regular behavior to chaotic behavior. It is achieved by changing the control parameter. The bifurcation diagram of the logistic map is shown in Fig. 1. This diagram contains three regions. The convergence region is at $r \in [0, 3]$. The bifurcation region is at $r \in [3, 3.57]$, where the phenomenon of period-doubling bifurcation occurs. The chaos region is at $r \in [3.57, 4]$, where there is a chaotic behavior.

- **Lyapunov Exponent**

Lyapunov exponent $\lambda$ reveals the nature of a chaotic system. It is used as a quantitative metric for the sensitivity to initial conditions. For example, for a discrete system

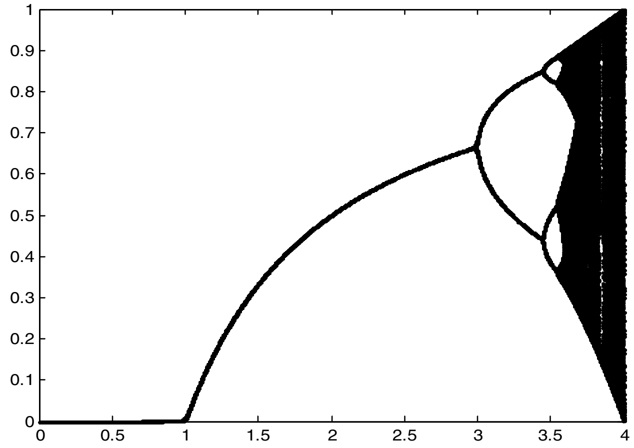


**Fig. 1** Logistic map bifurcation diagram for $r \in [0, 4]$, $X_0 = 0.02$

represented as $X_{n+1} = f(X_n)$ with an orbit beginning with $X_0$, the Lyapunov exponent can be characterized as follows [20–22]:

$$\lambda(X_0) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{\infty} \ln \left| f'(X_i) \right| \tag{2}$$

where $f'$ is the derivative of $f$. If $\lambda$ is above 0, the system is chaotic as the evolution is sensitive to initial conditions. If $\lambda$ is under 0, the system is not chaotic. If $\lambda$ is 0, the system is stable, and this represents a steady-state mode. The largest $\lambda$ defined by Eq. (2) is the Maximal Lyapunov Exponent (MLE). It defines the concept of predictability for a chaotic system.

When $r$ is between 0 and 4, we can plot the Lyapunov exponent of the logistic map with Eq. (2), as shown in Fig. 2. From Fig. 2, we observe that all Lyapunov exponents are equal to 0 or less. The orbit is attracted to a fixed or stable point. When $r \in [3.57, 4]$, the Lyapunov exponents are larger than zero, leading to a chaotic behavior. The MLE of the logistic map is 0.6785 at $r = 4$.

### 3.2 Modified logistic map

The modified logistic chaotic map is a development of the classical logistic map given by Eq. (1), where two polynomial terms $(1 - X_{n-1})$, and $(1.2 - 2 \times X_{n-1})^2$ are added to the logistic map equation to enlarge the range of the parameter $r$. The modified logistic map is defined as follows [23]:

$$\begin{aligned} X_n = {} & r \times X_{n-1} \times (1 - X_{n-1}) \times (1 - X_{n-1}) \\ & \times (1.2 - 2 \times X_{n-1}) \times (1.2 - 2 \times X_{n-1}) \end{aligned} \tag{3}$$

where $X_n$ is a value between zero and one, $n$ is the iteration index, and $r$ is a number between 0 and 13.8.

- **Bifurcation**

Figure 3 illustrates the bifurcation diagram of the modified logistic map. This chart contains three regions. When $r \in [0, 3.4]$, this refers to the convergence region. When $r \in [3.4, 5.2]$, this refers to the bifurcation region. Finally, for the chaos region, $r \in [5.2, 13.8]$.

- **Lyapunov exponent**

We can plot the Lyapunov exponent of the modified logistic map as shown in Fig. 4. It is clear that when $r \in [0, 5.2]$, Lyapunov exponent is less than or equal to 0.

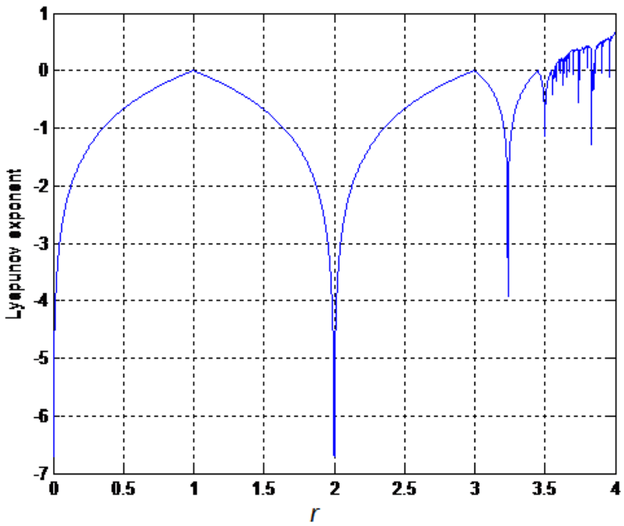


**Fig. 2** Logistic map Lyapunov exponent

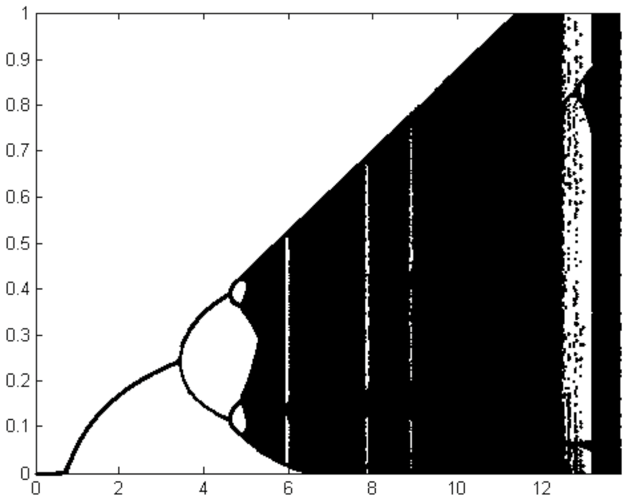


**Fig. 3** Modified logistic map bifurcation diagram at $r \in [0,13.8]$, and $X_0 = 0.02$

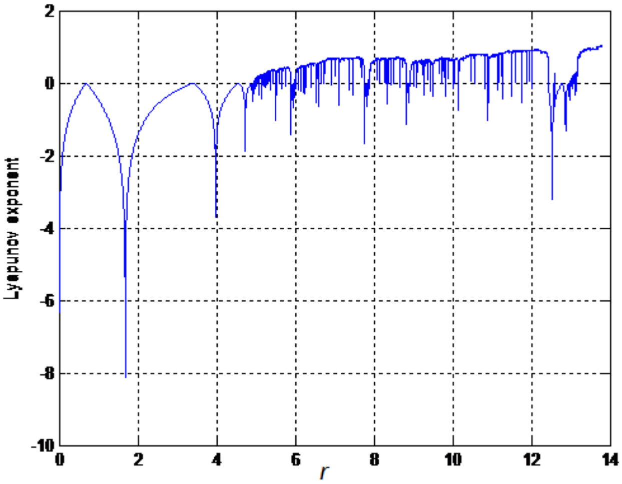


**Fig. 4** Lyapunov exponent of the modified logistic map

When $r \in [5.2, 13.8]$, the Lyapunov exponents are positive, and the dynamic behavior is chaotic. The MLE of the modified logistic map is 1.0317 at $r = 13.8$. It is higher than the MLE of the classical logistic map.

## 3.3 Classical quadratic map

An essential example of a chaotic system is the quadratic map. The classical quadratic map equation is given by [23]:

$$X_{n+1} = r - aX_n^2 \tag{4}$$

where $r$ is a parameter of the chaotic map, $a$ is constant and $n$ is the iteration index.

- **Bifurcation**

Figure 5 shows the bifurcation diagram of the quadratic map. This diagram has three regions. The convergence region is at $r \in [0, 0.74]$. The bifurcation region is at $r \in [0.74, 1.5]$. The chaos region is at $r \in [1.5, 2]$.

- **Lyapunov exponent**

Figure 6 shows the Lyapunov exponent of the quadratic map. It is clear that when $r \in [0, 1.5]$, all Lyapunov exponents are equal to or less than 0. When $r \in [1.5, 2]$, the Lyapunov exponents are above 0, and hence the behavior is chaotic. The MLE of the quadratic map is 0.6720.

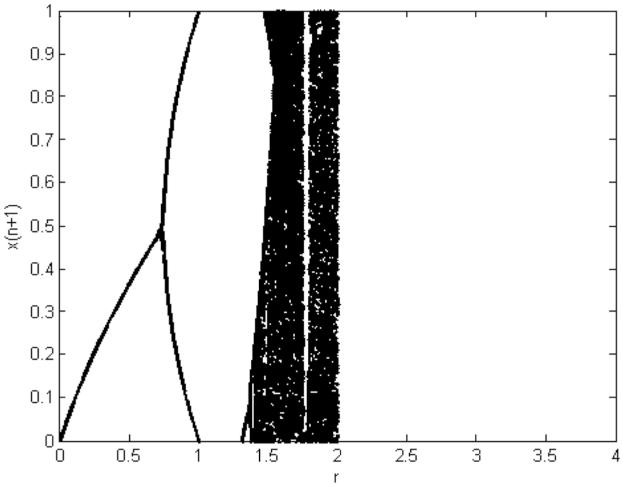


**Fig. 5** Classical quadratic map bifurcation diagram

## 3.4 Proposed quadratic maps

The proposed quadratic maps general equation is:

$$X_{n+1} = \left(r + \left(1 - aX_n\right)^2\right) \bmod 1 \tag{5}$$

We supplant $-(X_n)^2$ in Eq. (4) with the term $(1 - aX_n)^2$ and take the modulo 1 division. For three unique values of $a = 2$, 4, and 8, we analyze the proposed quadratic maps to illustrate the cycle state, bifurcation region, and Lyapunov exponent. Table 1 summarizes the characteristics of all chaotic maps. It reveals the values of both chaotic parameter $r$ and MLE.

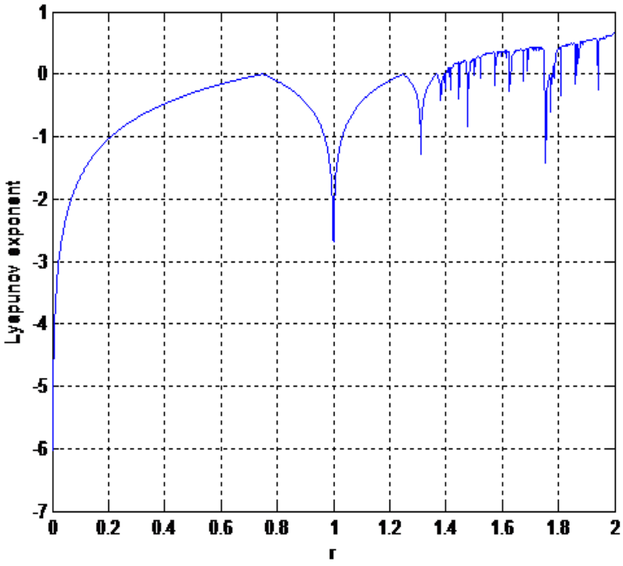


**Fig. 6** Classical quadratic map Lyapunov exponent

**Table 1** Comparison between classical and proposed quadratic maps

| Chaotic map | Equation | Chaotic parameter range | MLE |
|---|---|---|---|
| Classical quadratic map | $X_{n+1} = r - X_n^2$ | $r \in [1.5, 2]$ | 0.6720 |
| Proposed quadratic map 1 | $X_{n+1} = \left(r + \left(1 - 2X_n\right)^2\right) mod1$ | $r \in [0, 0.14]$, $r \in [1.56, 2.14]$, $r \in [2.56, 3.14]$ periodically to $\infty$ | 0.6732 |
| Proposed quadratic map 2 | $X_{n+1} = \left(r + \left(1 - 4X_n\right)^2\right) mod1$ | $r \in [0, 0.137]$, $r \in [0.14, 2.14]$, $r \in [1.14, 3.14]$ periodically to $\infty$ | 2.0257 |
| Proposed quadratic map 3 | $X_{n+1} = \left(r + \left(1 - 8X_n\right)^2\right) mod1$ | All values except $r$=0.11, 1.11 periodically to $\infty$ | 3.4709 |

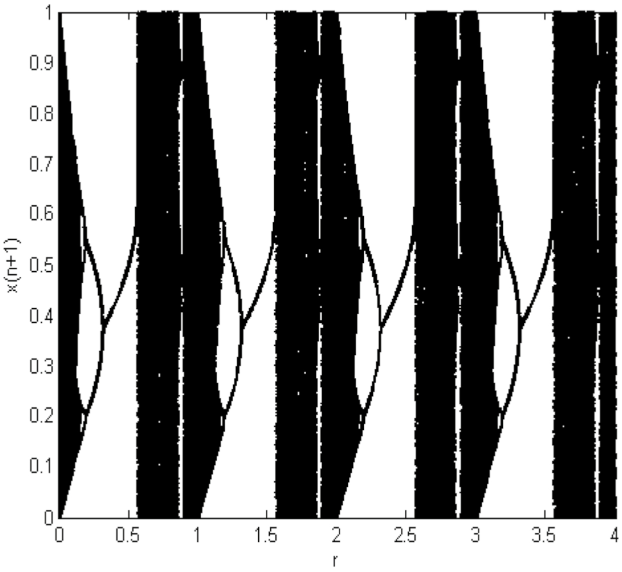


**Fig. 7** Bifurcation diagram of the quadratic map 1

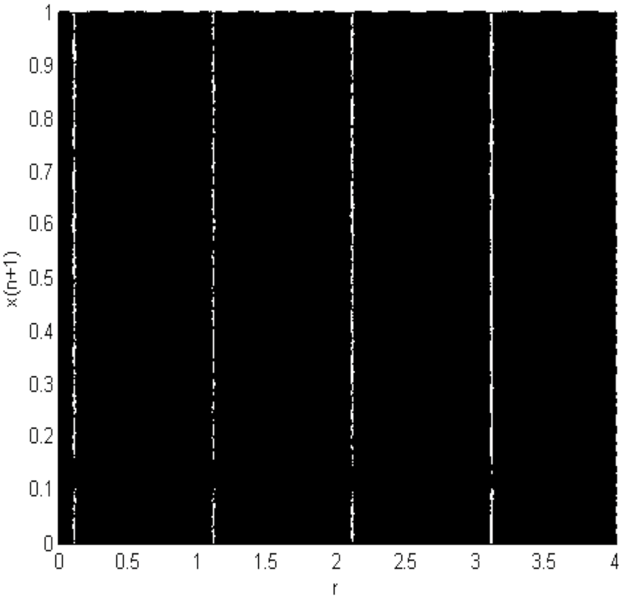


**Fig. 9** Bifurcation diagram of the quadratic map 3

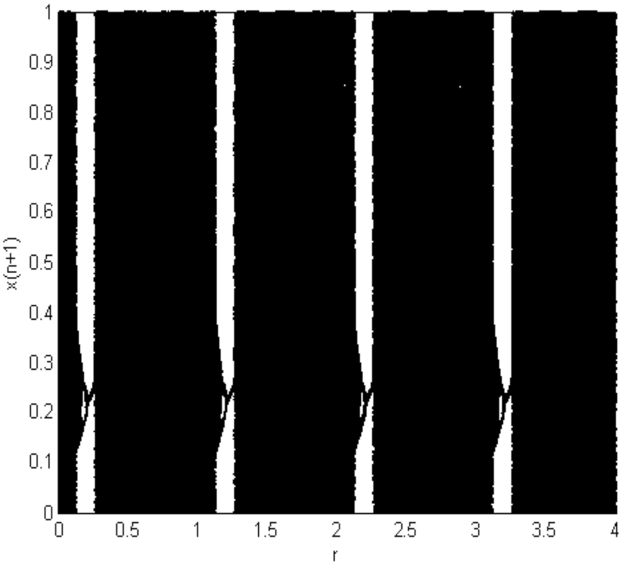


**Fig. 8** Bifurcation diagram of the quadratic map 2

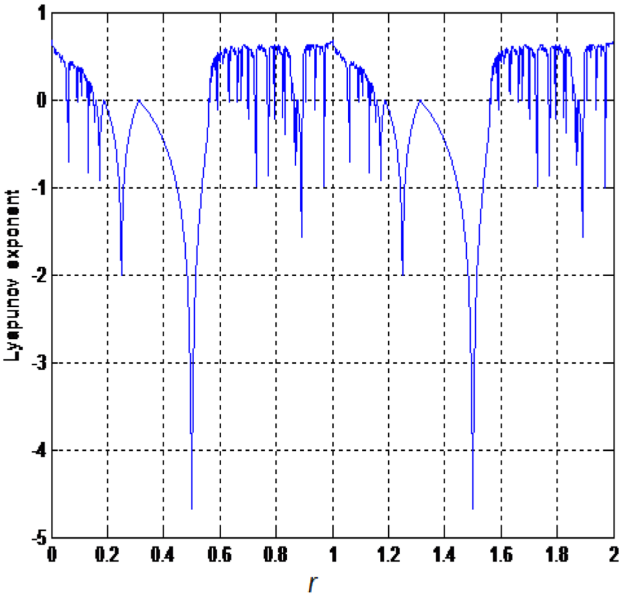


**Fig. 10** Lyapunov exponent of the quadratic map 1

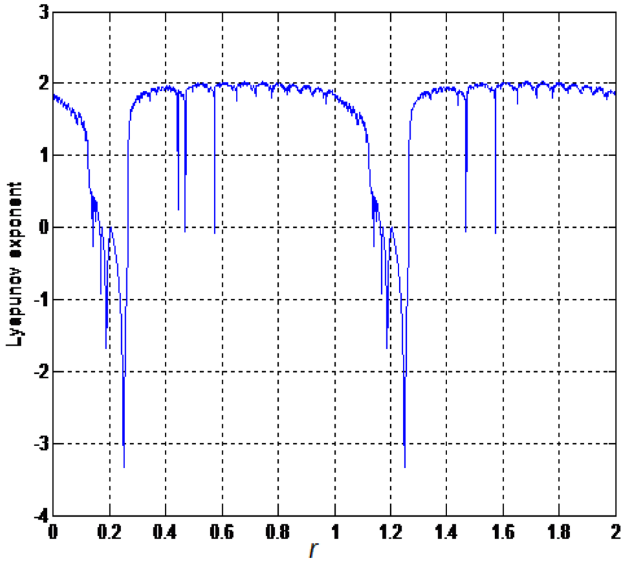


**Fig. 11** Lyapunov exponent of the quadratic map 2

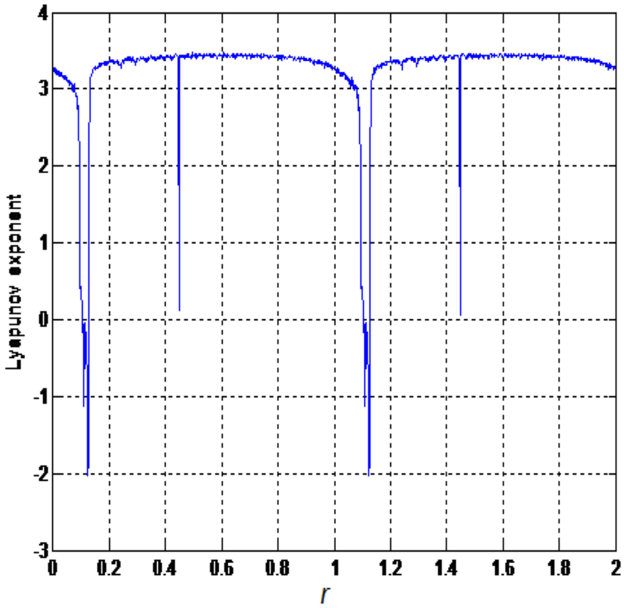


**Fig. 12** Lyapunov exponent of the quadratic map 3

Figures 7, 8, and 9 show the bifurcation diagrams of the proposed quadratic maps 1, 2, and 3. It is shown that the proposed chaotic quadratic map 3 has a wider range of *r* that can be used for encryption. Figures 10, 11, and 12 reveal the Lyapunov exponent for quadratic maps 1, 2, and 3. The Lyapunov exponent for quadratic map 3 has positive values for all values of *r* except for $r = \{0.11, 1.11, \ldots.\}$. Hence, the MLE of the proposed quadratic map 3 is 3.4709, which is larger than those of the chaotic maps 1 and 2.

## 4 Encryption based on convolution kernels

The proposed encryption scheme is implemented through convolution with a random kernel generated using a key related to the plain image [24]. First, the convolution kernel is generated with one of the chaotic maps discussed above. The encryption process is performed through convolution operation between the random kernel and the fingerprint image.

## 5 Chaos-based cancelable biometric system

To maintain the users' biometrics from hackers and to guarantee the ability to generate cancelable templates, the biometrics need to be encrypted. So, in the case of theft or loss, we can obtain a different encrypted biometric template from the same original biometric pattern. Chaos-based image encryption is very proper for biometric template encryption, as the chaotic maps are very sensitive to initial conditions. By making a small change in the initial conditions of the chaotic map, this radically changes the obtained encrypted biometric that can be reused in the same application. If the cancelable biometrics are stolen, they can be re-issued. In the following subsection, we explain, in detail, the architecture of the cancelable biometric system.

### 5.1 Architecture

The cancelable biometric system is divided into two phases: the enrollment phase and the authentication phase, as shown in Figs. 13 and 14. In the enrollment phase shown in Fig. 13, a fingerprint capturing device is used to generate the fingerprint images [25]. These images are then convolved with a random convolution kernel. In our scheme, the kernel is generated by a PIN generated by the user. To generate the random convolution kernel, the PIN is used as the initial condition. This random convolution kernel is convolved with the training images to generate the encrypted training templates.

The resulting encrypted training templates can be put away on a card and used afterwards to verify the users' IDs. If the card is lost or stolen, it is possible to create an alternate wrapping kernel to generate different encoded biometric templates. If the attacker attempts to use the stolen card to reconstruct the users' biometrics, he or she needs to know the circumvention kernel used in the recording stage. In order for the hackers to retrieve the original model, image decoding must be performed, which is incredibly hard to perform without knowing the client's PIN and the encryption

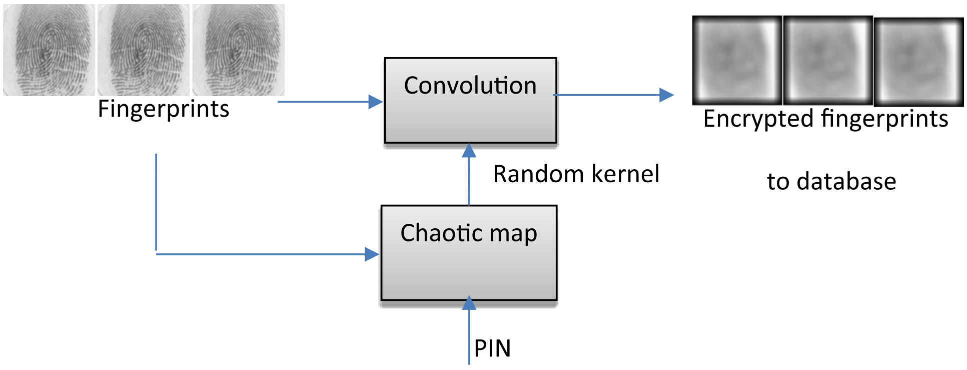


**Fig. 13** Enrollment stage for cancelable biometric templates

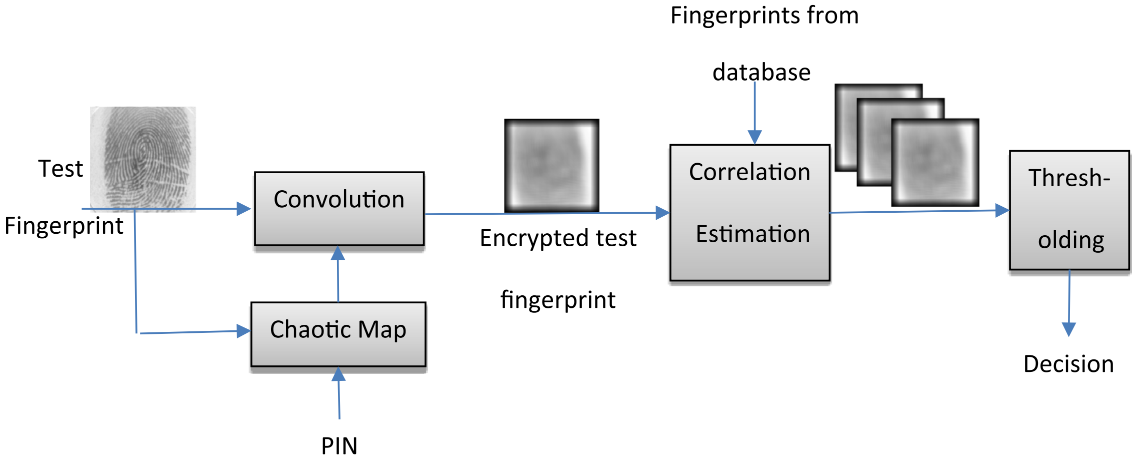


**Fig. 14** Authentication stage for cancelable biometric templates

scheme [17]. Consequently, this is viewed as a significant degree of safety for biometric templates.

In the authentication phase shown in Fig. 14, the user presents an encrypted fingerprint in the same way as in the enrollment phase. The test images are correlated with stored templates. Distributions are generated for the correlation scores in genuine and imposter tests. Hence, a threshold is determined for the approval process for users.

### 5.2 Authentication metrics

To ensure the similarity between a test encrypted fingerprint and an encrypted biometric template in the dataset, the correlation score is used. The higher the correlation value is, the higher the similarity between patterns. If the individual correlation score is higher than a specific threshold, admittance to the system is confirmed. The scores of unapproved users ought to be consistently lower than those of approved users [26].

Because of various reasons in biometric frameworks, some arrangement mistakes may happen. For example, unapproved templates may create scores higher than those of some approved ones.

The threshold can be chosen to ensure that all unapproved scores do not exceed a predetermined threshold. Hence, the system does not acknowledge any templates, wrongly. In addition, approved templates with scores lower than the predetermined threshold are mistakenly rejected. Hence, we can choose the threshold, so that no authorized pattern is rejected, wrongly. In this case, some unapproved subjects are wrongly recognized. Generally, in a biometric verification system, test information contains approved and unapproved patterns. Scores for each of the approved and unapproved examples will be circulated somehow or another around a mean of the distribution. The mean score of approved templates is higher than that of unapproved templates.

Hence, the tools that can be utilized to check the obtained scores are the Probability of True Distribution (PTD) and the Probability of False Distribution (PFD) of correlation scores obtained in the validation stage. The PTD is the probability of correlation between authorized fingerprints and the encoded biometric templates in the database, while the PFD (unapproved designs) is the probability of correlation between an unauthorized fingerprint and those stored in the database. We allow admittance to the system if the new fingerprint score is higher than the predetermined threshold with a certain probability of error. The probability of correct detection can be easily obtained from the probability of error, and we can obtain a better system performance at lower error probabilities.

## 6 Simulation results

Our simulations experiments have been implemented on 20 different fingerprints for 20 persons as shown in Fig. 15 [27]. Each fingerprint is of size 300 × 300 pixels. We use the quadratic and logistic chaotic maps with keys related to the plain images. These keys are used to generate the random convolution kernels (see Fig. 16). The initial conditions of these chaotic maps are changed according to the PIN each user presents. Finally, we compare all chaotic maps.

In the enrollment phase, the user inserts his or her own PIN, and this produces equivalent kernels that are convolved with the training images. The resulting 20 encrypted biometric templates are stored in the database, see Fig. 17.

- **Probability of True Distribution (PTD) and Probability of False Distribution (PFD)**

In the authentication phase, we use two fingerprints for testing. One of them belongs to authorized users, and the other belongs to unauthorized users. In both cases, the test user gives a PIN and produces a random wrap kernel. Hence, we obtain two encoded fingerprints for the test. We assume that the unauthorized person knows the correct PIN for an authorized user to test the system security.

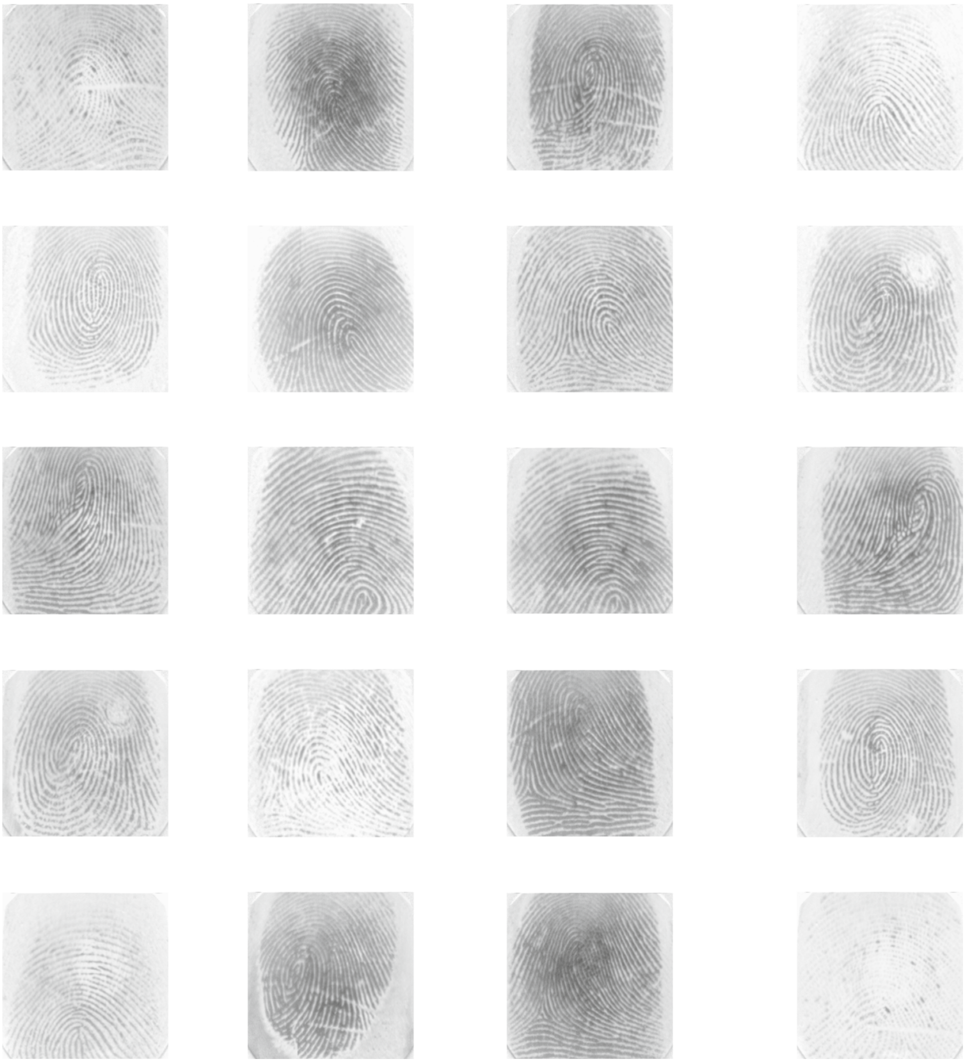


**Fig. 15** Training fingerprints [27]

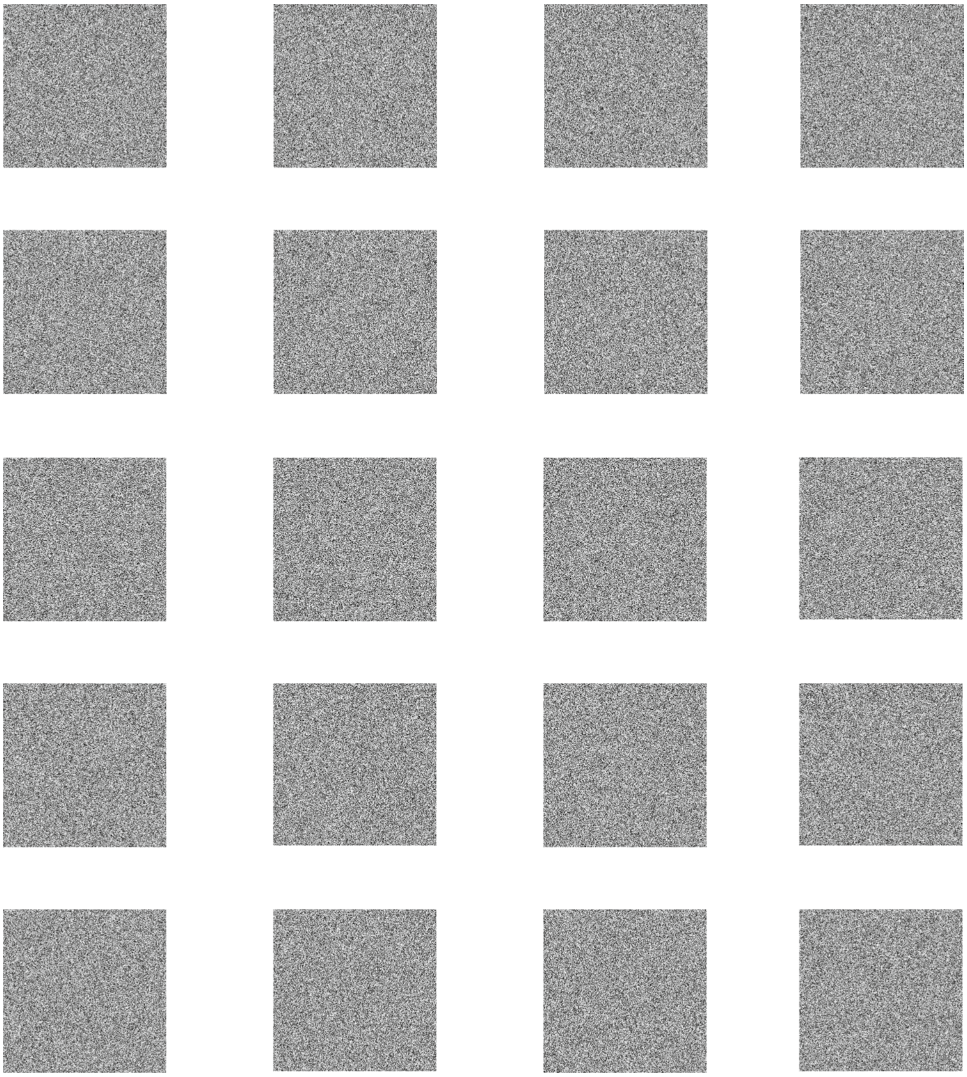


**Fig. 16** Corresponding kernel for each fingerprint

We obtain correlation values between the two encrypted fingerprints and the 20 stored encrypted biometric templates. The PTD and PFD are ploted for the cancelable biometric systems for all chaotic maps to determine the error threshold and probability (see Figs. 18, 19, 20, 21, 22, 23). The intersection of the two curves determines the threshold value according to which we can define whether the user is authorized or not.

We examine the proposed quadratic chaotic map 3, because it has a wide range of the parameter *r*, extended to infinity. Hence, there is no restriction on the PIN chosen by the user. Finally, we compare all chaotic maps. The different sizes of the kernels are illustrated in Table 2.

In the enrollment phase, the user inserts his or her own PIN, and this creates the corresponding kernel, which is convolved with the fingerprint. In the authentication phase, we use two fingerprints for evaluation. One is for an approved person, and the other is for an unapproved person. In the two cases, the test person embeds the PIN and produces the random convolution kernel. Hence, two encoded test fingerprints can be obtained. The unapproved user is assumed to know the correct PIN for one of the approved users to test the level of security of our system. We get the correlation between the two encrypted fingerprints and the 20 stored encrypted biometric templates for each kernel size.

- **True Acceptance Distribution (TAD) and False Acceptance Distribution (FAD)**

We plot the TAD and the FAD as shown in Figs. 24, 25, 26, 27, 28, and 29. The intersection between the two curves determines the threshold value to approve user access.

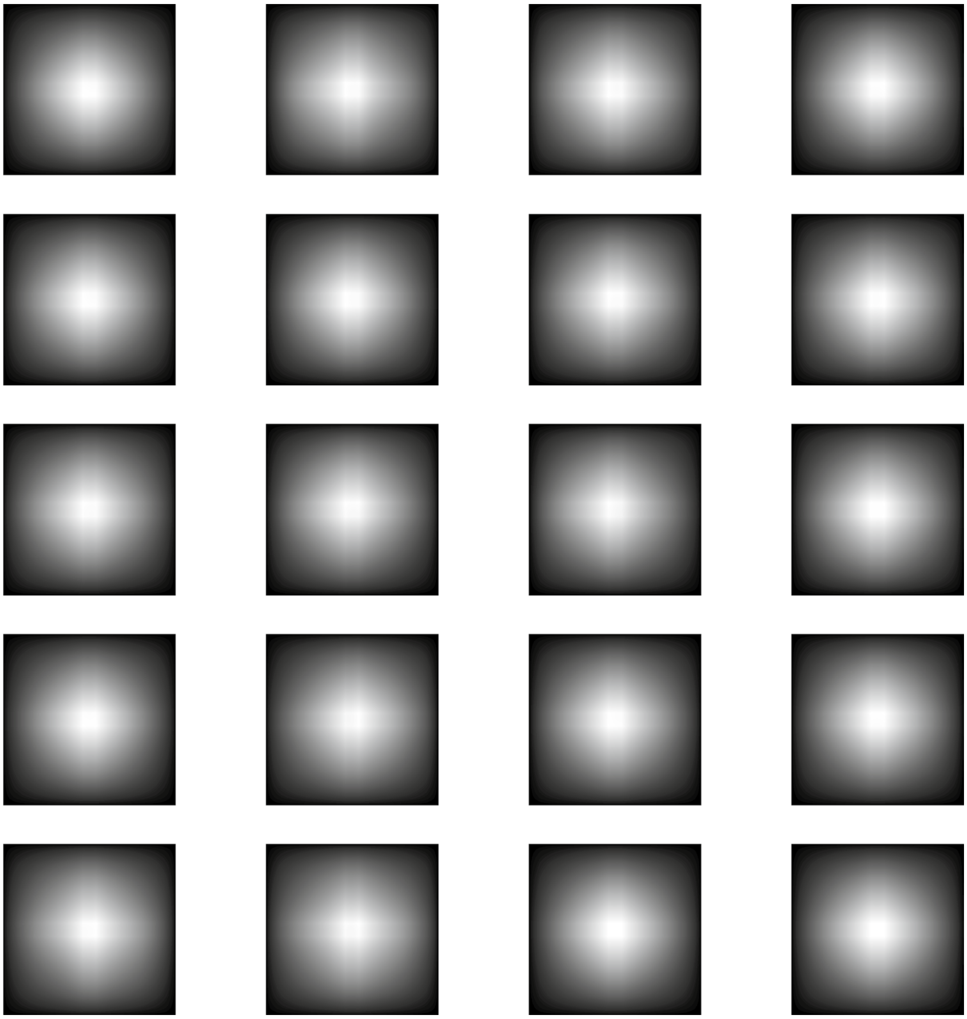
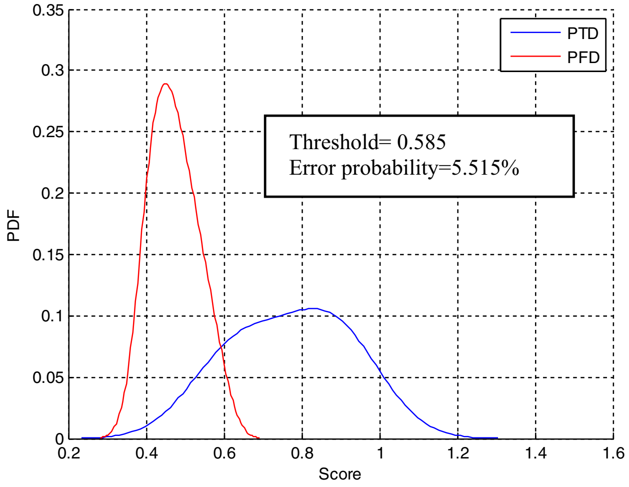
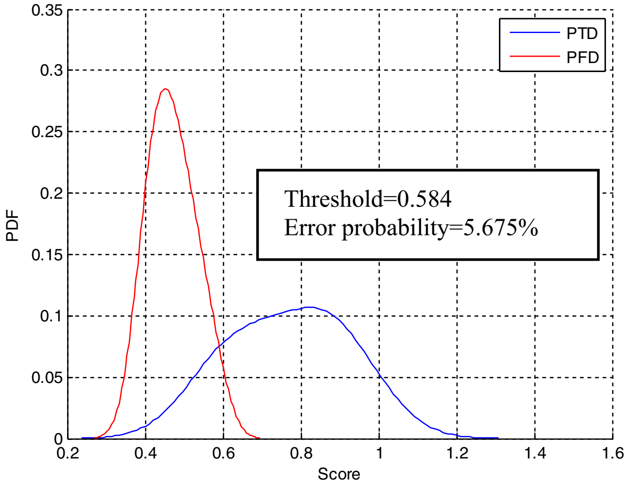


**Fig. 17** Encrypted training fingerprints with corresponding convolution kernels



Threshold= 0.585
Error probability=5.515%

**Fig. 18** PTD and PFD using logistic map for convolution kernel generation



Threshold=0.584
Error probability=5.675%

**Fig. 19** PTD and PFD using modified logistic map for convolution kernel generation

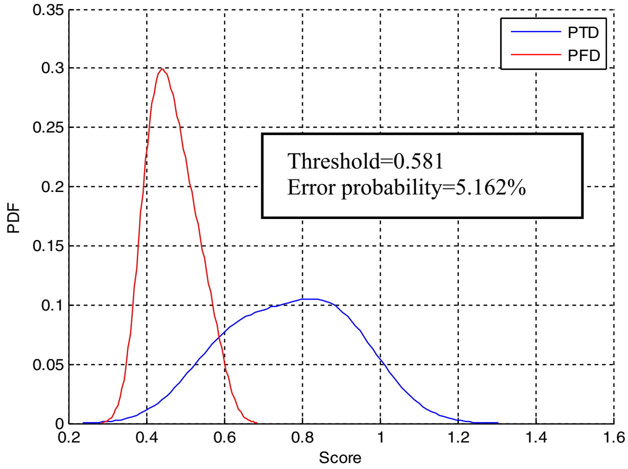


**Fig. 20** PTD and PFD using classical quadratic map for convolution kernel generation

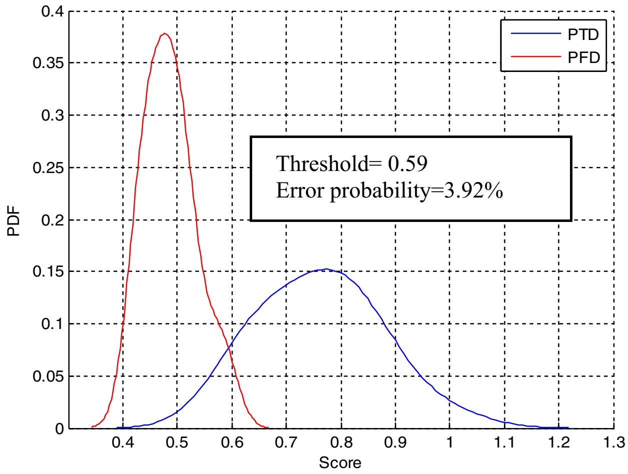


**Fig. 21** PTD and PFD using quadratic map 1 for convolution kernel generation

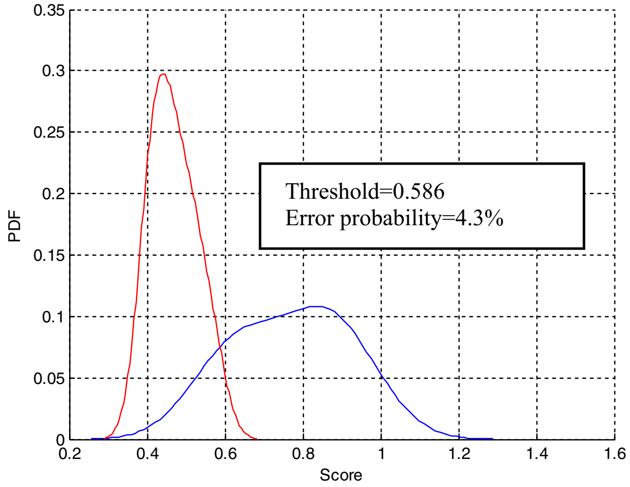


**Fig. 22** PTD and PFD using quadratic map 2 for convolution kernel generation

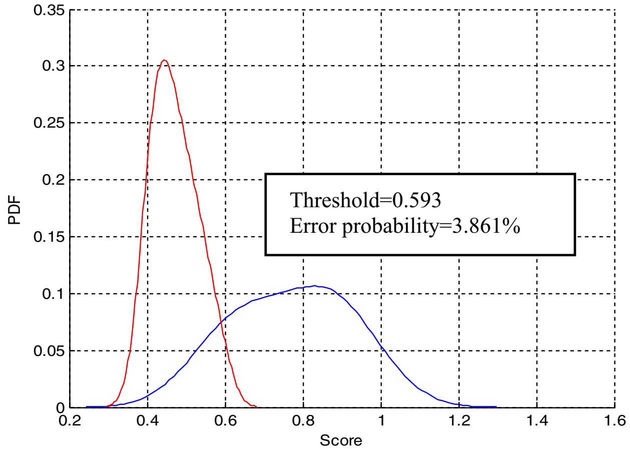


**Fig. 23** PTD and PFD using quadratic map 3 for convolution kernel generation

**Table 2** Kernel size

| Symbol | Kernel size |
|---|---|
| $Z_1$ | 256 × 256 |
| $Z_2$ | 128 × 128 |
| $Z_3$ | 64 × 64 |
| $Z_4$ | 32 × 32 |
| $Z_5$ | 16 × 16 |
| $Z_6$ | 8 × 8 |

- **Kernel size effect**

We study the effect of the kernel size in the enrollment phase, the authentication time, and the threshold value, as shown in Table 3.

As we see from Table 3, for a large kernel size, the threshold value becomes large or close to 1. This case is not preferred since the difference between the correlation distributions of the authorized, and unauthorized scores is very small. As the kernel size is decreased, the threshold value is also decreased until reaching 0.59 for the smallest kernel size of 8 × 8. This means that the distance between the distributions of the correlation for authorized and unauthorized fingerprints is large enough for the system to decide and reject the unauthorized users. The enrollment time, which is used to store the cancelable biometric fingerprints, is decreased as the kernel size is decreased, because the convolution is performed by sliding the kernel over the fingerprint image. As the kernel size is increased,

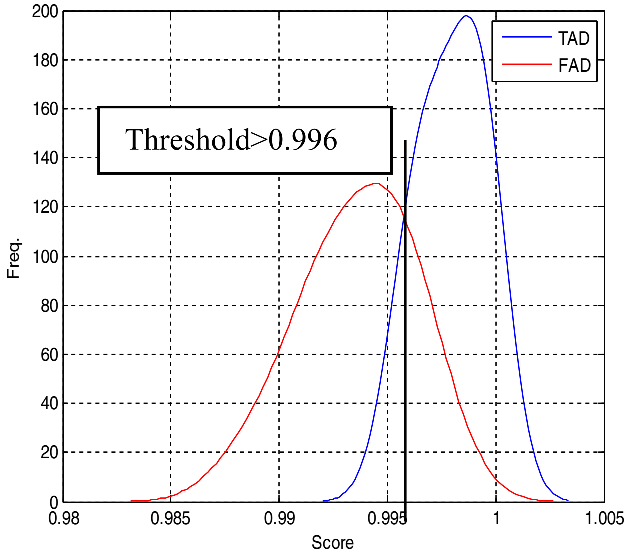


**Fig. 24** TAD and FAD using $Z_1$ kernel

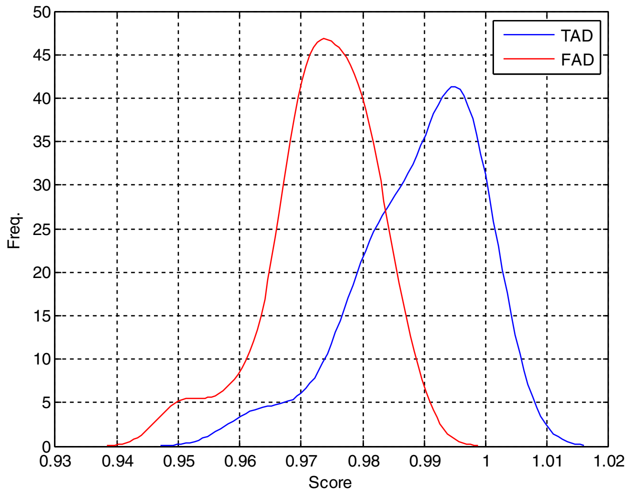


**Fig. 25** TAD FAD using $Z_2$ kernel

the number of multiplication and addition operations is increased, and then the enrollment time is increased.

- Chaotic map effect

Now, we study the effect of all chaotic maps we developed in this paper on the threshold value. The EER is used to predetermine the threshold value for the acceptance or rejection of users. The lower the EER value is, the higher the accuracy of the biometric system. As shown in Table 4, the threshold value with all chaotic maps decreased as the kernel size is decreased. However, the difference in the threshold values between all chaotic maps is very small. The reason is that convolving the training fingerprints with any random convolution kernel generated from any chaotic map does not modify the correlation output, significantly. As a result, the authentication reliability is preserved. In addition, different cancelable biometric templates can be created from the same biometric by altering the convolution kernels simply.

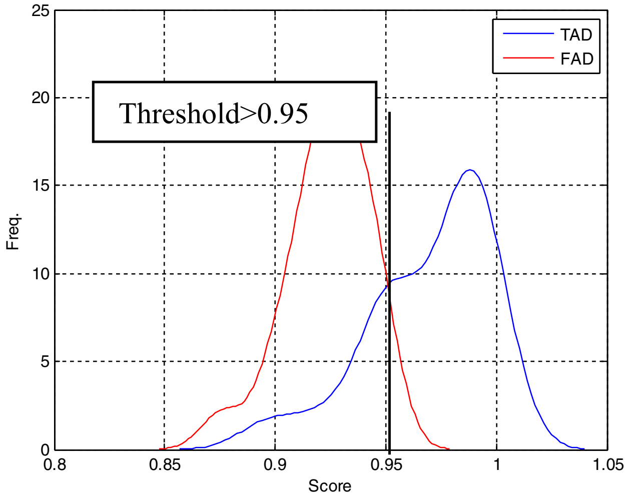


**Fig. 26** TAD and FAD using $Z_3$ kernel

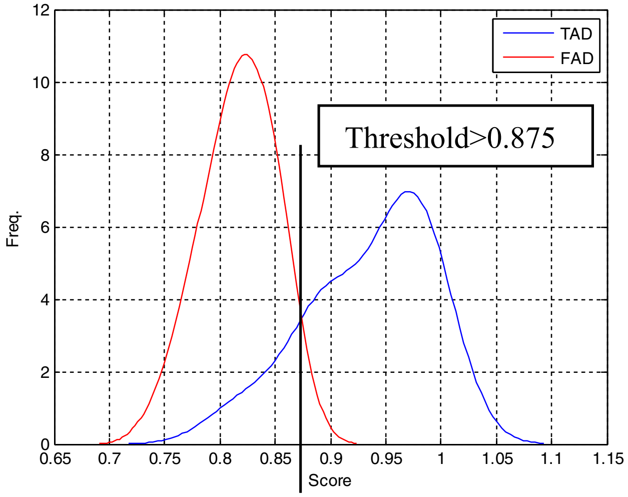


**Fig. 27** TAD and FAD using $Z_4$ kernel

- Performance comparison of different chaotic maps

We study the effect of the different chaotic maps according to the mean value of the authorized patterns, the mean value of the unauthorized patterns, the value of the threshold, the probability of error, and the authentication time as shown in Table 5. The probability of error is changed

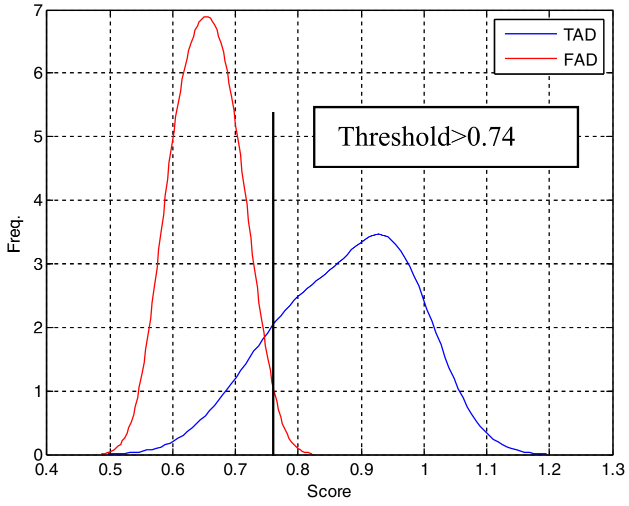


**Fig. 28** TAD and FAD using $Z_5$ kernel

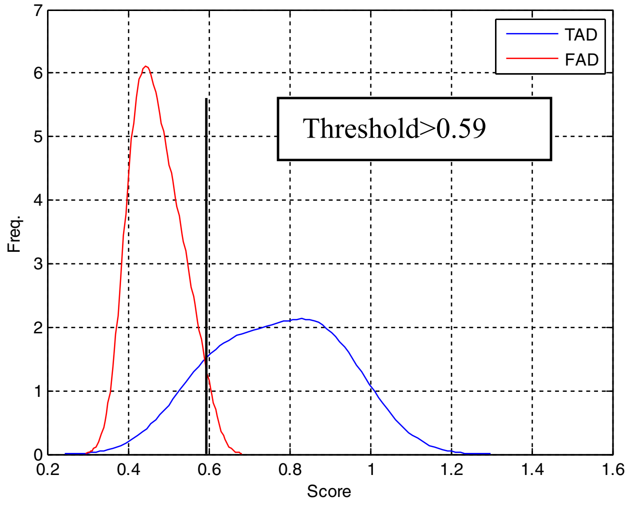


**Fig. 29** TAD and FAD using $Z_6$ kernel

**Table 3** Kernel size effect

| Symbol | Kernel size | Threshold | Enrollment time per user (s) | Authentication time per user (s) |
|---|---|---|---|---|
| $Z_1$ | 256×256 | 0.996 | 15.92 | 8.41 |
| $Z_2$ | 128×128 | 0.984 | 3.20 | 2.36 |
| $Z_3$ | 64×64 | 0.95 | 0.776 | 1.27 |
| $Z_4$ | 32×32 | 0.875 | 0.173 | 0.434 |
| $Z_5$ | 16×16 | 0.74 | 0.071 | 0.338 |
| $Z_6$ | 8×8 | 0.59 | 0.04 | 0.313 |

according to the chaotic map. The proposed quadratic map 3 achieves the smallest value of error probability among all chaotic maps, with 3.861%. The mean values of the authorized/unauthorized patterns and the authentication times per user are nearly the same for all chaotic maps. The difference in the threshold values between all chaotic maps is very small, since convolving the training images with arbitrary convolution kernels produced from different maps does not modify the subsequent correlation output, significantly. Accordingly, the authentication accuracy is kept high. In addition, by altering the PIN for every user, different cancelable biometric templates can be produced from similar biometrics. This is guaranteed through altering the underlying state of the chaotic map and henceforth altering the convolution kernel.

- Comparison with Recent Related Studies

Table 6 provides a comparison between the proposed system that depends on enhanced quadratic map 3 and some other cancelable biometric systems (Sandhya et al. [15], Dahia and Segundo [17], Xu et al. [19], Anand et al. [7]). The results in Table 6 show superior performance with the enhanced quadratic map 3 with good EER values and a small processing burden.

## 7 Conclusion

Encryption and hashing schemes are regularly used to secure biometric templates. There are two issues with these strategies. First, the encoded biometrics need to be decoded for recognition. If the biometrics are decoded, this gives a chance for hacking attempts. Another problem is that minor changes in biometrics affect hash functions, severely. Hence, these functions, in practice, could not be used, directly. The concept of cancelable biometrics is introduced in this paper as a solution for these two problems. We presented a method to produce encrypted biometric templates that can be altered using different convolution kernels generated by different chaotic maps. The utilization of scrambled data in biometric systems allows the implementation of the verification process straightforwardly through a correlation test. Even if the attacker succeeds in stealing the encrypted biometric templates, he needs a deconvolution process with a random kernel generated through a certain key. The effect of the chaotic map on the threshold value, error probability, authentication time, and other parameters has been studied. Finally, a comparison between all the chaotic maps used in this paper show that the utilization of the proposed quadratic map 3 in the cancelable biometric system leads to the smallest error

**Table 4** Chaotic map effect

| Kernel size | Threshold with quadratic map 3 | Threshold with quadratic map 2 | Threshold with quadratic map 1 | Threshold with original quadratic map | Threshold with modified logistic map | Threshold with logistic map |
|---|---|---|---|---|---|---|
| 256×256 | 0.996 | 0.9966 | 0.9823 | 0.997 | 0.9966 | 0.9972 |
| 128×128 | 0.984 | 0.985 | 0.9428 | 0.9827 | 0.9851 | 0.9853 |
| 64×64 | 0.95 | 0.95 | 0.9255 | 0.95 | 0.95 | 0.951 |
| 32×32 | 0.875 | 0.875 | 0.8391 | 0.875 | 0.8776 | 0.875 |
| 16×16 | 0.74 | 0.75 | 0.74 | 0.75 | 0.75 | 0.75 |
| 8×8 | 0.59 | 0.5532 | 0.5886 | 0.5436 | 0.5886 | 0.59 |

**Table 5** Chaotic map effect

| Chaotic map | Mean of authorized patterns | Mean of unauthorized patterns | Threshold | Error probability (%) | Probability of correct detection (%) | Authentication time/user (s) |
|---|---|---|---|---|---|---|
| Logistic map | 0.771 | 0.472 | 0.585 | 5.515 | 94.485 | 0.328 |
| Modified logistic map | 0.769 | 0.471 | 0.584 | 5.675 | 94.325 | 0.317 |
| Classical quadratic map | 0.769 | 0.467 | 0.581 | 5.162 | 94.838 | 0.322 |
| Quadratic map 1 | 0.761 | 0.487 | 0.592 | 3.921 | 96.081 | 0.325 |
| Quadratic map 2 | 0.769 | 0.469 | 0.586 | 4.302 | 95.724 | 0.327 |
| Quadratic map 3 | 0.770 | 0.472 | 0.593 | 3.861 | 96.139 | 0.324 |

**Table 6** Comparison of the EER values for the proposed system with enhanced quadratic map 3 and some other related works

| Method | Year | EER% |
|---|---|---|
| Sandhya et al. [15] | 2017 | 1.17 |
| Dahia and Segundo [17] | 2018 | 1.14 |
| Xu et al. [19] | 2018 | 0.51 |
| Anand et al. [7] | 2020 | 0.57 |
| Proposed enhanced quadratic map 3 | 2021 | 0.59 |

probability among all systems with different chaotic maps. Hence, the cancelable biometric system using the proposed quadratic map 3 has the best performance.

## Declarations

**Conflict of interest** We declare that we have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

1. Ibrahim, S., Egila, M.G., Shawky, H., Elsaid, M.K., El-Shafai, W., Abd El-Samie, F.E.: Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimed. Tools Appl. **79**(19), 14053–14078 (2020)
2. Alarifi, A., Amoon, M., Aly, M.H., El-Shafai, W.: Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. IEEE Access **8**, 221246–221268 (2020)
3. Algarni, A.D., El Banby, G., Ismail, S., El-Shafai, W., El-Samie, F.E.A., Soliman, F.: Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy **22**(12), 1361 (2020)
4. Wang, S., Hu, J.: Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn. **47**(3), 1321–1329 (2014)
5. Zakaria, Y., Nassar, R.M., Zahran, O., Hussein, G.A., El-Rabaie, E.S.M., El-Khamy, S.E., et al.: Cancelable multi-biometric security system based on double random phase encoding and cepstral analysis. Multimed. Tools Appl. **78**(22), 32333–32355 (2019)
6. Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C.: A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recogn. **78**, 242–251 (2018)
7. Anand, V., Kanhangad, V.: Porenet: Cnn-based pore descriptor for high-resolution fingerprint recognition. IEEE Sens. J. **20**(16), 9305–9313 (2020)
8. Minaee, S., Azimi, E., Abdolrashidi, A.: Fingernet: Pushing the limits of fingerprint recognition using convolutional neural network. (2019). arXiv preprint arXiv: 1907.12956
9. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., Zhang, D.: Biometrics recognition using deep learning: a survey. arXiv preprint arXiv: 1912.00271 (2019)
10. Rosenstein, M.T., Collins, J.J., De Luca, C.J.: A practical method for calculating largest Lyapunov exponents from small data sets. Phys. D **65**(1–2), 117–134 (1993)
11. Kantz, H.: A robust method to estimate the maximal Lyapunov exponent of a time series. Phys. Lett. A **185**(1), 77–87 (1994)
12. Gupta, S., Thakur, K., Kumar, M.: 2D-human face recognition using SIFT and SURF descriptors of face's feature regions. Vis. Comput., pp. 1–10. (2020)

13. Ramadan, N., Ahmed, E.H., Elkhamy, E.S.: Hybrid ciphering system of images based on fractional Fourier transform and two chaotic maps. Int. J. Comput. Appl. **119**(11), 12–17 (2015)
14. Agarwal, R., Jalal, A.S., Arya, K.V.: Local binary hexagonal extrema pattern (LBH X EP): a new feature descriptor for fake iris detection. Vis. Comput. **37**, 1357–1368 (2021)
15. Sandhya, M., Prasad, M.V.: Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme. Int. J. Pattern Recognit Artif Intell. **31**(04), 1756004 (2017)
16. Cheung, K.H., Kong, A.W.K., You, J., Zhang, D.: An Analysis on Invertibility of Cancelable Biometrics based on BioHashing. In CISST (Vol. 2005, pp. 40–45) (2005)
17. Dahia, G., Segundo, M.P.: Automatic dataset annotation to learn CNN pore description for fingerprint recognition. arXiv preprint arXiv: 1809.10229 (2018)
18. Paul, P.P., Gavrilova, M., Klimenko, S.: Situation awareness of cancelable biometric system. Vis. Comput. **30**(9), 1059–1067 (2014)
19. Xu, Y., Lu, G., Lu, Y., Liu, F., Zhang, D.: Fingerprint pore comparison using local features and spatial relations. IEEE Trans. Circuits Syst. Video Technol. **29**(10), 2927–2940 (2018)
20. El-Shafai, W., Almomani, I.M., Alkhayer, A.: Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. IEEE Access **9**, 35004–35026 (2021)
21. Ibrahim, S., Egila, M.G., Shawkey, H., Elsaid, M.K., El-Shafai, W., Abd El-Samie, F.E.: 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. (2020)
22. Abd El-Samie, F.E., Nassar, R.M., Safan, M., Abdelhamed, M.A., Khalaf, A.A., El Banby, G.M., et al.: Efficient implementation of optical scanning holography in cancelable biometrics. Appl. Opt. **60**(13), 3659–3667 (2021)
23. Badr, I.S., Radwan, A.G., El-Sayed, E.R., Said, L.A., El Banby, G.M., El-Shafai, W., Abd El-Samie, F.E.: Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. Dig. Signal Process. 103103. (2021 ).
24. El-Shafai, W., Mohamed, F.A.H E., Elkamchouchi, H.M., Abd-Elnaby, M., ElShafee, A.: Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. IEEE Acces (2021).
25. Faragallah, O.S., El-sayed, H.S., Afifi, A., El-Shafai, W.: Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform. Optics and Lasers in Engineering, 137, 106333 (2021).
26. Faragallah, O.S., Afifi, A., El-Sayed, H.S., Alzain, M.A., Al-Amri, J.F., Abd El-Samie, F.E., El-Shafai, W.: Efficient HEVC integrity verification scheme for multimedia cybersecurity applications. IEEE Access **8**, 167069–167089 (2020)
27. FVC2002 (DB1) database. Available online: https://www.biometricsinstitute.org/resources/fingerprint-verification-competition-fvc. Accessed 1 July 2021.

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

**Hayam A. Abd El-Hameed** received the B.Sc. (Honors) in Electronics and Electrical Communications Department from the Faculty of Electronic Engineering, Menoufia University, Egypt, in 2009. She received her M.Sc. degree in Electronics and Electrical Communications from the Faculty of Electronic Engineering, Menoufia University, Egypt, in 2018. She worked as a lecturer in Obour High Institute for Engineering and Technology in 2019. Her current research areas of interest include image processing, digital communications, and signal processing.

**Noha Ramadan** received a B.Sc. (Honors) in Electronic Engineering in May 2000 (Faculty of Electronic Engineering, Menoufia University, Egypt). In 2007, she received her M.Sc. degree in "Multimedia Implementation over General Packet Radio Service". She is now an assistant professor at the Faculty of Engineering (Ahram Canadian University, Egypt). Her research interests are multimedia over mobile networks, security over wireless networks, and image processing.

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

**Ashraf A.M. Khalaf** (PhD) received his B.Sc. and M.Sc. degrees in Electrical Engineering from Minia University, Egypt, in 1989 and 1994, respectively. He received his Ph.D. in Electrical Engineering from Graduate School of Natural Science and Technology, Kanazawa University, Japan, in March 2000. He is currently the head of the Department of Electronics and Communications Engineering, Minia University.

**Hossam Eldin H. Ahmed** received the B.Sc. degree (Hons) in Nuclear Engineering in June 1969, the M.Sc. degree in Microelectronic Electron Diffraction from the Nuclear Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 1977, and the Ph.D. degree from the High Institute of Electronics and Optics, Paul Sabatier University, Toulouse, France, in 1983. From 1970 to 1977, he was in the Egyptian Marine Force. He was a demonstrator until 1977. In 1977, he was a Teaching Lecturer and a Staff Member. In 1993, he was a Professor with the Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt. From 1993 to 1999, he was a Vice-dean for Educations and Students Affairs. In 2001, he became the Head of the Electrical Communications Department. From 2001 to 2004, he was the Dean of the Faculty of Electronic Engineering. He is a member of the Menoufia Periodic Electronic Journal, and since 1995, he has been the Director, Designer, and Constructor of the Menoufia University wide-area network (WAN) (21-LANs). He is the developer of the Menoufia University libraries and FRCU universities libraries in Egypt. His current research interests are electron and scan microscopy, transmission and backscattering of electrons and ion beams into amorphous or polycrystalline targets, optical fibers, VLSI design, nanotechnology, lithography, optical, and multimedia communications, digital image processing, computer security (crypto-analysis), telemetry microcomputer applications in satellites, and satellite communications.

**Said E. Elkhamy** received the B.Sc. (Honors) and M.Sc. degrees from Alexandria University, Alexandria, Egypt, in 1965 and 1967, respectively, and the Ph.D. degree from the University of Massachusetts, Amherst, USA, in 1971. He joined the teaching staff of the Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 1972 and was appointed as a Full-time Professor in 1982 and as the Chairman of the Electrical Engineering Department from September 2000 to September 2003. He is currently an Emeritus Professor. Prof. El-Khamy has published more than three hundred scientific papers in national and international conferences and journals and took part in the organization of many local and international conferences. His current research areas of interest include spread-spectrum techniques, mobile and personal communications, wave propagation in different media, smart antenna arrays, space–time coding, modern signal processing techniques and their applications in image processing, communication systems, antenna design and wave propagation problems. Prof. El-Khamy is a Fellow member of the IEEE since 1999. He received many prestigious national and international prizes and awards including the State Appreciation Award 34394 Multimedia Tools and Applications (2019) 78:34373–34395 (Al-Takderia) of Engineering Sciences for 2004, the most cited paper award from Digital Signal Processing journal for 2008, the IEEE R.W.P. King best paper award of the Antennas and Propagation Society of IEEE, in 1980, the A. Schuman's-Jordan's award for Engineering Research in 1982. He is also a Fellow of the Electromagnetics Academy and a member of Tau Beta Pi, Eta Kappa Nu, and Sigma Xi.

**Fathi E. Abd El-Samie** received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.