Efficient implementation of cancelable face recognition based on elliptic curve cryptography

Article *in* Optical and Quantum Electronics · July 2023

DOI: 10.1007/s11082-023-04641-y

Rania A. Eltaieb
Menoufia University
8 PUBLICATIONS **49** CITATIONS
SEE PROFILE

Ghada El Banby
Menoufia University
105 PUBLICATIONS **1,025** CITATIONS
SEE PROFILE

Walid El-Shafai
Menoufia University
353 PUBLICATIONS **4,196** CITATIONS
SEE PROFILE

Fathi E. Abd El-Samie
Menoufia University
1,029 PUBLICATIONS **11,304** CITATIONS
SEE PROFILE

Optical and Quantum Electronics (2023) 55:841
https://doi.org/10.1007/s11082-023-04641-y

Efficient implementation of cancelable face recognition based on elliptic curve cryptography

Rania A. Eltaieb[1] · Ghada M. El-Banby[2] · Walid El-Shafai[1,3] · Fathi E. Abd El-Samie[1,4] · Alaa M. Abbas[5]

Received: 30 April 2022 / Accepted: 2 February 2023

Abstract

Most modern authentication systems adopt human biometrics to avoid the shortcomings that result from forgetting passwords and security codes utilized in traditional systems. To increase the security level of the original biometric traits against offensive attacks, cancelable biometric patterns are generated from the original ones to control the system access. This paper presents a new approach for cancelable face recognition based on the concept of Elliptic Curve Cryptography (ECC). The ECC has been classified as a public-key (asymmetric) encryption technique. In public-key encryption, each user (transmitter and receiver) has two keys: a public key and a private key. The proposed framework guarantees full distortion and encryption of the original biometric traits to be saved in the database to completely hide them for intruders. To validate the proposed approach, three sets of face biometric databases have been used. The Receiver Operating Characteristic (ROC) curve and correlation scores are estimated to test the performance. The simulation results prove that the proposed approach is efficient, robust and it achieves promising results.

Keywords Cancelable biometrics · Face recognition · ECC · ROC · Authentication systems

1 Introduction

Traditional authentication systems have their limitations for system access. These systems may fail to guarantee the exact and right password or personal identification number for each authentication process. The most general scheme of biometric authentication involves a sensor module for image acquisition, a pre-processing module to provide alignment and perform noise removal, a segmentation module for region extraction, a feature extraction module and a feature matching module. Biometric traits are classified into two categories: physical and behavioral. The category of physical biometrics includes fingerprints, hand engineering, retinal images, iris scans, and faces. On the other hand, the category of behavioral biometrics includes voice, signature, keystroke pattern, and walking style. These characteristics of the human body can be used to ensure that only the authorized individual has the permission to access the system (Jain et al. 2004; Alarifi et al. 2020a; Algarni et al. 2020a; Abd El-Samie et al. 2021; El-Shafai et al. 2021a; Rathgeb and Busch 2012).

Extended author information available on the last page of the article

Published online: 15 July 2023

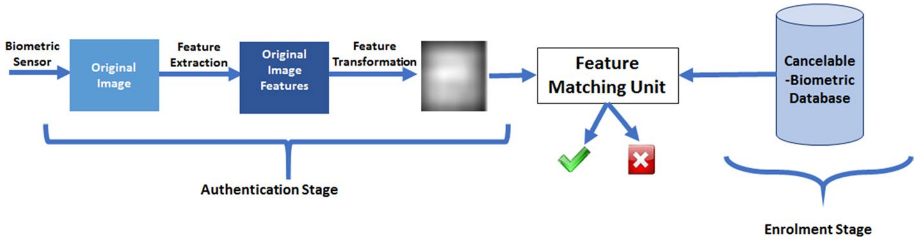

Fig. 1 Cancelable biometric recognition system

To increase the security level of stored biometric traits, a biometric cryptosystem can be used to build a cancelable biometric system. In traditional biometric cryptosystems, the original biometric templates can be encrypted and stored in the database. During the authentication phase, a decryption process is required. On the other hand, in cancelable biometric systems, the encrypted biometric templates are used in a statistical framework for identity verification. So, there is no need to decrypt the stored templates as in the traditional biometric cryptosystems (Rathgeb and Busch 2012; Soliman et al. 2021a; El-Hameed et al. 2022; Ibrahim et al. 2020; Faragallah et al. 2020). Biometric authentication systems work based on two stages. The first stages is the enrolment of the biometrics of the users, and the second stage is the authentication or verification (Helmy et al. 2022; Kaur and Verma 2014). The main idea of cancelable biometrics is to perform distortion of the original templates by certain transformation methods or encryption schemes to store the distorted templates in the database in the enrollment phase. In the authentication phase, the biometric trait of the corresponding user is transformed or distorted in the same manner and matched to the database. According to a matching criterion, the verification of the user for access is performed. So, cancelable biometrics can be classified as a means of privacy preservation to control the system access. The basic concept of cancelable biometrics was introduced by Ratha et al. (2007). Figure 1 displays the main framework of the cancelable biometric recognition system.

As shown in Fig. 1, a cancelable biometric system has two main stages: enrollment and authentication. In the enrollment stage, the users' cancelable biometric templates are obtained and stored in the database. In the authentication stage, the identification of the user is performed by measuring the similarity between the new cancelable biometric templates and the stored ones (Punithavathi and Subbiah 2017; Patel et al. 2015; Kaur and Khanna 2016). Several researchers have developed and presented different techniques to implement user authentication systems based on biometrics (Alarifi et al. 2020b).

Elliptic Curve Cryptography (ECC) was firstly used in encryption in Koblitz (1987) and Miller (1985). The ECC offers a better level of security than those of classical image encryption techniques, because it is hard to solve the discrete logarithmic problem. Moreover, the ECC has a much lower key size than that of the Rivest–Shamir–Adleman (RSA) algorithm that achieves the same level of security. After that, several researchers focused on the ECC due to its strength (Zhang and Wang 2018; Laiphrakpam and Khumanthem 2018; Toughi et al. 2017). The main problem faced with ECC implementation is the computational cost. The ECC multiplication operation is time-consuming, which makes it challenging to implement ECC for real-time applications. Some researchers use the ECC to encrypt images by generating Pseudo-Random Noise (PRN) to map pixel values, according to the generated points, in order to achieve a large degree of permutation (Hayat and Azam 2019). Another important problem encountered with ECC is the increase in the size of the encrypted data compared to that of the plaintext data. The increase in data size is due to mapping of each pixel value in the plaintext image to a point on the elliptic curve that has two coordinates i.e., $p_{x,y}$. In (Abdelwahab et al. 2020; Laiphrakpam and Khumanthem 2017), the authors proposed methods to reduce the encrypted data size by grouping multiple pixel values to a single point. Their methods succeeded to decrease the size of the encrypted data, but it was still larger than that of the plaintext image.

Cancelable biometric methodologies depend on the utilization of transformed or deformed versions of the biometrics in the verification stage (El-Shafai et al. 2021b). The main goal of cancelable biometrics is to increase the privacy of users. So, several studies have been introduced to generate cancelable biometric templates. Soliman el al. (Soliman et al. 2018) presented a cancelable biometric system based on Double Random Phase Encoding (DRPE) for both face and iris recognition. This system depends on the extraction of features from either face or iris images to generate a matrix of features to be encrypted with the DRPE algorithm. Simulation results revealed an Equal Error Rate (EER) of 0.17% and an Area under Receiver Operating Characteristic curve (AROC) of 99.3%. Gowthamim et al. (Gowthami and Mamatha 2015) discussed fingerprint recognition using zone-based linear binary patterns. Their technique depends on feature extraction from fingerprint images using linear binary patterns. Each fingerprint image is divided into equal-size zones, and in each zone, linear patterns are extracted for recognition. They achieved an average recognition accuracy of 94.28%. Buriro et al. (2019) presented an authentication system based on fusion of behavioral biometrics. Their work involved extracting features by different types of sensors built in the smartphone, followed by a Random Forest (RF) classifier to verify the identity of users. Their system achieved a 99.3% True Acceptance Rate (TAR).

Soliman et al. (2021b) proposed an automatic ear recognition system based on the fusion of different color space representations of the ear. Their system has five steps. The first step is for the extraction of the person's ear from the background of the whole image, followed by the conversion of each image of the ear to 13 color space models, which produce 39 images. In the next step, pre-processing is performed on the 39 images through gamma correction, intensity transformation, difference of Gaussian filtering, and histogram equalization. Gabor features are used as discriminative features from all color space models. After that, feature selection and classification are performed based on Sequential Forward Floating Selection (SFFS) followed by a matching step with a nearest neighbor classifier. This system achieved an AROC of 98.5%.

El-Shafai (2015) introduced personal identification and verification techniques based on the Discrete Wavelet Transform (DWT). Patterns of fingerprints, iris, and palm print have been used. The DWT is applied on a certain cropped area of each pattern. Then, secrete information is hidden in the vertical and horizontal high-frequency sub-band (HH). The Inverse Discrete Wavelet Transform (IDWT) is performed to reconstruct the 4 sub-bands. The RC4 is applied for encryption and decryption of the user information. A minutiae mapping technique is used to extract fingerprint, iris, and palm print features to compare with the patterns stored in the database. This authentication system achieved good results.

This paper introduces a new ECC scheme to generate cancelable biometric templates that can guarantee a high security level. The proposed approach guarantees full distortion and encryption of the original biometric traits to be stored in the database. The quantitative evaluations are performed through the computing the EER, and AROC as performance metrics. The rest of this work is arranged as follows. Section 2 briefly describes the mathematical foundations of the elliptic curve, and the ECC-based cancelable biometric recognition approach is explained. Simulation results and comparative analysis are given in Sect. 3. Section 4 gives the concluding remarks.

2 Proposed ECC-based cancelable biometric recognition approach

Cryptography is a data or image protection process that can be implemented in cancelable biometric systems. The biometric traits are encrypted firstly and stored in the database. For the verification process, a distance metric such as the correlation score is calculated. Different attempts for cancelable biometric systems have been presented based on encryption strategy. This paper follows the same trend, but with a new encryption technique, which is based on ECC.

2.1 Elliptic Curve (EC) mathematics

A finite Elliptic Curve (EC) $\in \mathbb{Z}_P$(integers mod P) can be defined with a cubic equation as follows:

$$y^2 = x^3 + ax + b\,(\text{mod } P) \tag{1}$$

where a, b and P are the EC parameters. a and b are integer numbers $\in \mathbb{Z}_p$ and P is a prime number. The parameters must satisfy the condition:

$$4a^3 + 27b^2 \neq 0\,(mod\ P) \tag{2}$$

Figure 2 shows an EC satisfying Eq. (1) and Eq. (2).

We briefly state some of the mathematical operations of EC mathematics. For more details, see Harkanson and Kim (2017) and Menezes et al. (1993).

Point addition: If the point $q_1\left(x_{q_1}, y_{q_1}\right)$ is added to the point $q_2\left(x_{q_2}, y_{q_2}\right)$, the result $q_3\left(x_{q_3}, y_{q_3}\right)$ is calculated as follows:

$$q_1 + q_2 = q_3 \tag{3}$$

where $x_{q_3} = \eta^2 - x_{q_1} - x_{q_2}(\text{mod } P)$

$$y_{q_3} = \eta\left(x_{q_1} - x_{q_3}\right) - y_{q_1}(\text{mod } P)$$

$$\eta = \frac{y_{q_2} - y_{q_1}}{x_{q_2} - x_{q_1}}$$

Figure 3 illustrates the addition operation of two points (Xu 2018).

Point inverse: The inverse of point $q_1\left(x_{q_1}, y_{q_1}\right)$ is $q_2\left(x_{q_2}, y_{q_2}\right)$. It is calculated as follows:

$$q_2\left(x_{q_2}, y_{q_2}\right) = q_1\left(x_{q_1}, P - y_{q_1}\right) \tag{4}$$

Point multiplication: The product of an integer number n by a point $q_1\left(x_{q_1}, y_{q_1}\right)$ is calculated as follows;

$$q_2\left(x_{q_2}, y_{q_2}\right) = n \bullet q_1\left(x_{q_1}, y_{q_1}\right) \tag{5}$$

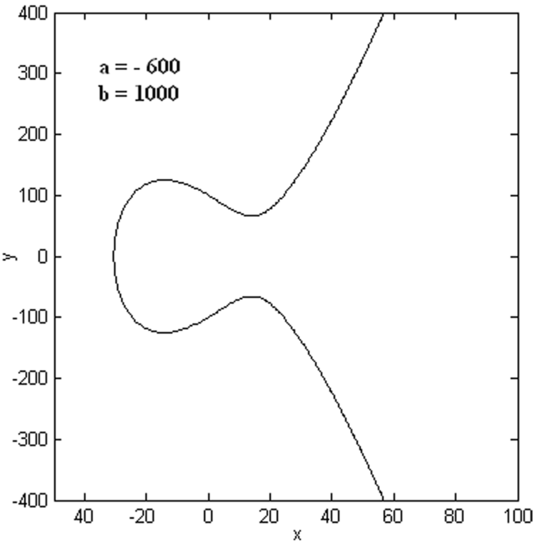

Fig. 2 An elliptic curve

Practically, the multiplication operation is performed by additive operations n times as follows:

$$q_2\left(x_{q_2}, y_{q_2}\right) = \sum_n q_1\left(x_{q_1}, y_{q_1}\right) \tag{6}$$

Discrete logarithm problem: In EC public key encryption, each user randomly chooses his private key, i.e., k_p and shares $\gamma = k_pG$, where G is a generating point, which is shared through the channel. An intruder tries to gather information about the used key. It is very easy to calculate γ as k_pG, but it is infeasible to calculate k_p from γ, and G. This is known as the discrete logarithm problem.

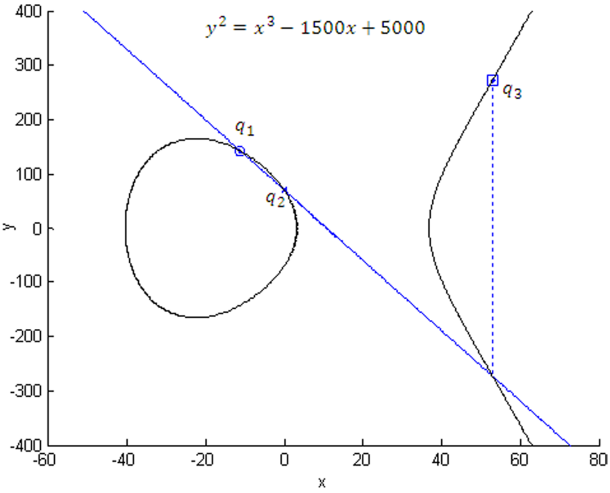

Fig. 3 Addition operation

2.2 Image encryption using ECC

Different from symmetric–key encryption, the ECC is a public-key encryption. In public-key encryption, each user has two keys: public and private. The private key is secret, and no one can decrypt an encrypted message without knowing the private key. Diffie and Hellman in 1976 proposed a solution to securely share the key between users. They introduced a public-key protocol to exchange keys with EC, securely (Washington 2008).

For message encryption, El Gamal cryptosystem with EC was firstly introduced in 1984 (Washington 2008). El Gamal is a public key encryption algorithm, which uses two keys. The two users, denoted as α and β, agree on predetermined curve parameters (a, b, and P), and pick a point on the curve G. A pixel value of the plaintext image represents information mapped to a point M on the curve and encoded for transmission over the channel. The protocol of encryption and decryption is as follows:

1. Users randomly choose their private keys, k_α and k_β, and keep them secret.
2. Users calculate their public keys, $Q_\alpha = k_\alpha G$ and $Q_\beta = k_\beta G$, and share them over the channel.
3. If user α wants to send a message M to user β, it calculates:

$$S = M + k_\alpha Q_\beta \tag{7}$$

4. User α sends S to user β.
5. User β decrypts the message by calculating:

$$S + \left(-k_\beta\right) Q_\alpha = M + k_\alpha Q_\beta - k_\beta Q_\alpha = M + k_\alpha k_\beta G - k_\beta k_\alpha G = M \tag{8}$$

Any intruder aiming to calculate k_α or k_β form Q_α or Q_β will face the discrete logarithm problem, which is computationally infeasible to solve.

To encrypt an image using ECC, each pixel value is mapped to a point on a predefined EC. The EC parameters play an important role in the pixel scrambling process to satisfy the required confusion level. The number of points of the selected EC parameters should be greater than the size of the plaintext image to achieve a high security level. In this paper, we select the technique that is implemented in Soleymani et al. (2013) to encrypt the images. In Soleymani et al. (2013), the authors proposed a mapping method to distribute the pixel values on the points of a selected EC. For example, they selected an EC with 123,456 points, and the image pixel value 0 is mapped to 482 points specified according to repetitions of the pixel value 0 in the image. For more details, see Algarni et al. (2020b) and Nishchal (2019). We have chosen this method, because it is simple and suitable for our application. Figure 4 shows the results of ECC encryption of three different images. Figure 5 shows the block diagram of the proposed ECC-based cancelable biometric approach. The correlation coefficient score is considered as the metric of matching.

Figure 5 describes the authentication process of the current user or entity in two cases. When the person is authorized, his/her encrypted distorted template is highly correlated with a one stored in the database. The other case is for the imposter with low correlation score. The proposed cancelable biometric recognition approach is tested with several noise

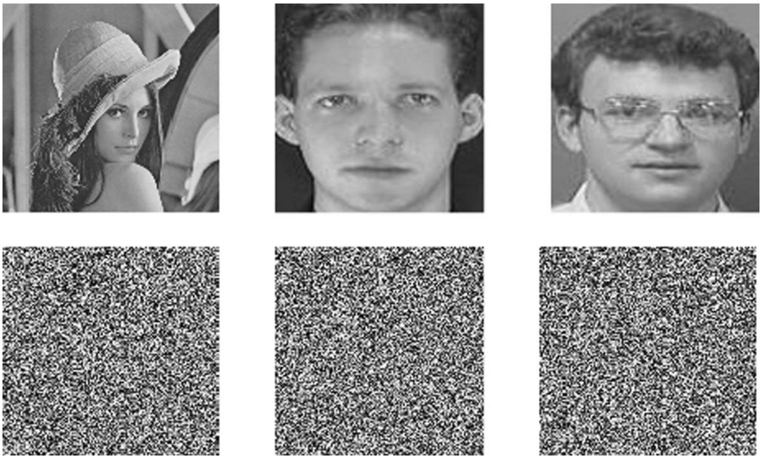

Fig. 4 Encryption results

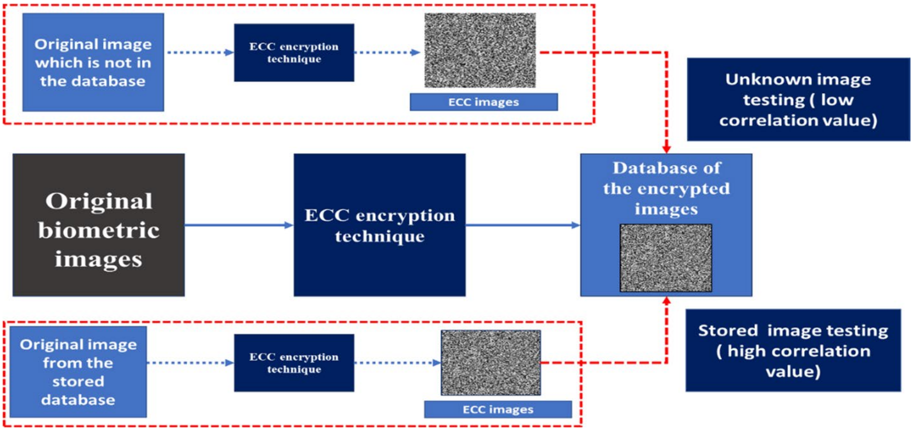
Original image which is not in the database
ECC encryption technique
ECC images
Unknown image testing (low correlation value)
Original biometric images
ECC encryption technique
Database of the encrypted images
Original image from the stored database
ECC encryption technique
ECC images
Stored image testing (high correlation value)

Fig. 5 Block diagram of the proposed cancelable biometric recognition approach

levels. Noise variance may change according to several causes, such as the thermal effect of the sensor or the environmental changes like light and cloud.

3 Simulation results

In this section, the evaluation of the proposed approach is presented. Firstly, the security of the proposed ECC is assessed in terms of visual analysis, histogram analysis, correlation analysis, entropy analysis, differential attack analysis, and key sensitivity analysis as given in Figs. 6, 7, 8 and Table 1. It is known that an encryption system must break correlation between adjacent pixels. Therefore, it is noticed from the results that the encryption system succeeds in destroying the very strong correlation of the plain image pixels in the biometric templates. In addition, the encryption system should produce a different encrypted image from the original one even with a correlated key. Figure 8 shows an original image and its encrypted versions using very related private keys $K_1(8, 3)$, $K_2(8, 4)$, and $K_3(7, 3)$. The histograms are almost uniform, which indicates an equal probability of the encrypted pixel levels.

Furthermore, Table 1 shows the values of correlation, Number of Pixels Change Rate (NPCR), and Unified Average Changed Intensity (UACI) between two encrypted biometrics using the related keys: K_1, K_2, and K_3. The results indicate that the cryptosystem is very sensitive to the encryption key. All obtained results prove that the proposed ECC technique can be implemented, efficiently, for designing a secure and efficient cancelable biometric recognition system. So, this motivated us to use it in our proposed work.

To evaluate the performance of the proposed cancelable biometric recognition approach using ECC, three different databases have been used (Database 2020a, 2020b, 2020c): Research Laboratory for Olivetti and Oracle (ORL) database (Database 2020a), NiST Face Recognition Technology (FERET) dataset (Database 2020b) and Mass Labelled Faces in the Wild (LFW) dataset of the University of Massachusetts' Computer Vision Laboratory (Database 2020c). Twenty images have been used from each

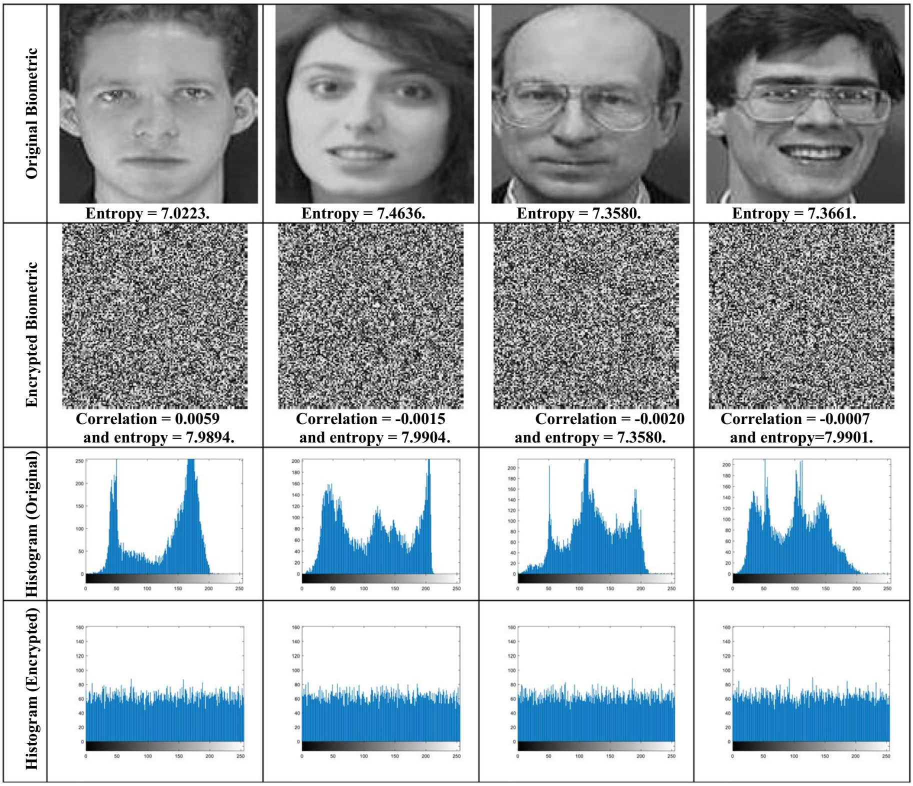

Fig. 6 Histogram analysis of the original and encrypted biometric templates

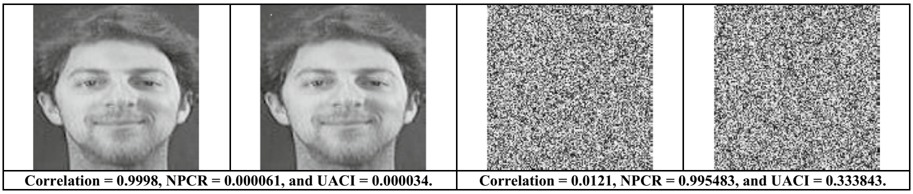
Correlation = 0.9998, NPCR = 0.000061, and UACI = 0.000034.
Correlation = 0.0121, NPCR = 0.995483, and UACI = 0.333843.

Fig. 7 Differential attack analysis of the difference between two original biometrics with only a random one-pixel change

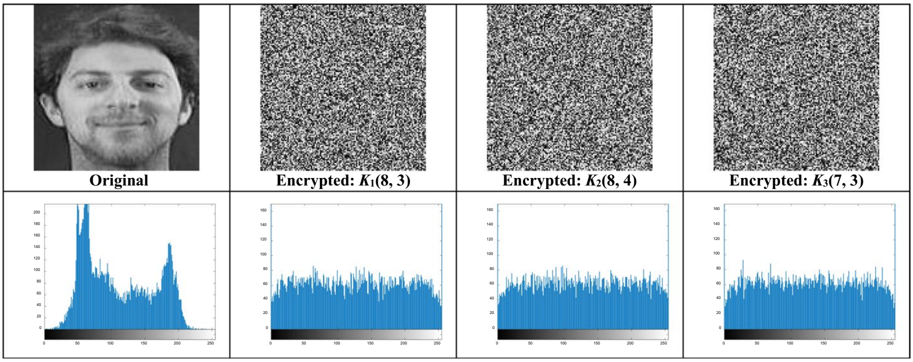

Fig. 8 Key sensitivity analysis with different related keys

Table 1 The correlation, NPCR and UACI values of encrypted biometrics with different related keys

Evaluation metric	K_1(8, 3) and K_2(8, 4)	K_1(8,3) and K_3(7, 3)	K_2(8,4) and K_3(7, 3)
Correlation	0.0042	0.0107	0.0053
NPCR	0.9956	0.9963	0.9962
UACI	0.3369	0.3339	0.3357

database and the correlation coefficient and ROC curve have been estimated for each case. All used encrypted biometrics and their histograms are shown in Figs. 9, 10 and 11 for the three databases.

The block diagram shown in Fig. 5 has been used to obtain the encrypted images from the original ones for the three databases. These images are stored in the database for matching afterwards. For checking the recognition and security levels, the correlation coefficient and AROC are estimated. The correlation scores for genuine and imposter distributions for the studied cases are shown in Figs. 12, 13, 14 and 15. The noise variances are changed to be 0.01, 0.02, 0.03, 0.04, and 0.05 to investigate the effect of noise on the performance.

The results shown in the figures ensure the feasibility to add the encrypted images with ECC in the database and use them for biometric authentication. The evaluation metrics with different levels of noise variance in the proposed ECC-based cancelable face recognition approach for ORL, FERET, and LFW databases are shown in Table 2.

To prove the high performance of the proposed approach compared to the existing approaches (Soliman et al. 2021a; El-Hameed et al. 2022; Ibrahim et al. 2020; Ratha

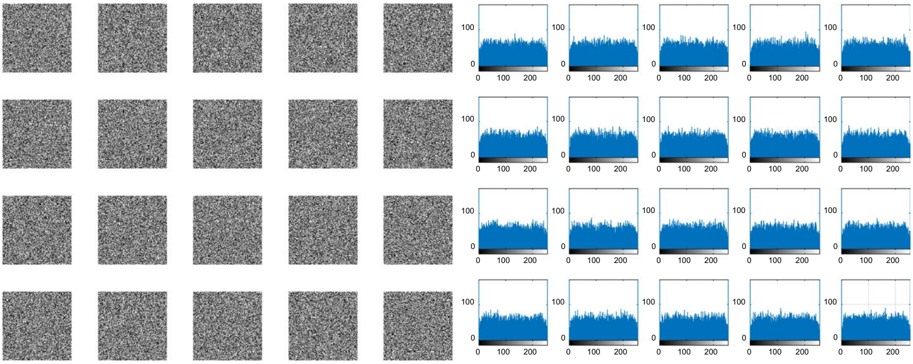

Fig. 9 ORL encrypted images and their histograms

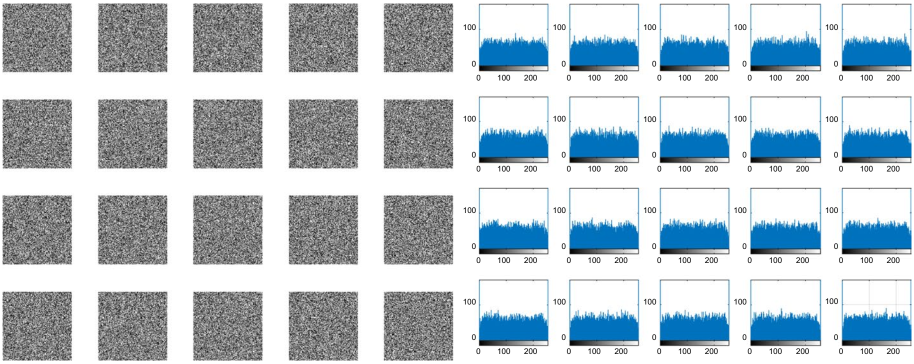

Fig. 10 LFW encrypted images and their histograms

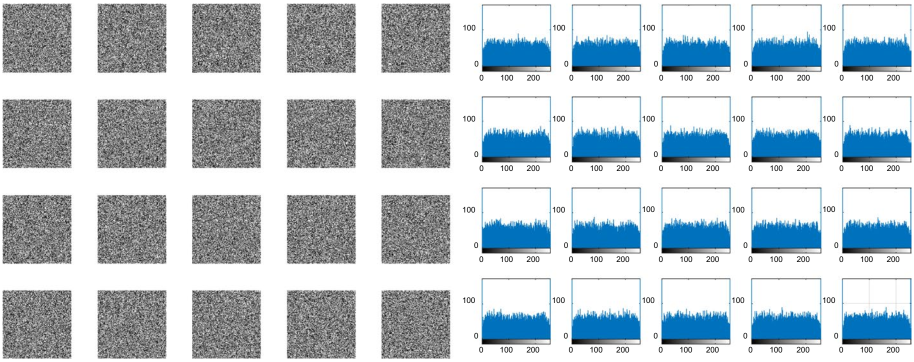

Fig. 11 FERET encrypted images and their histograms

et al. 2007; Kaur and Khanna 2016), different simulation tests have been performed on the same used biometric datasets (Database 2020a, 2020b, 2020c). Table 3 presents the obtained results of the comparative study, which prove the high security performance of the proposed approach compared to other related and existing approaches.

4 Conclusions and future works

This paper presented an efficient approach for cancelable face recognition based on the concepts of ECC. The main achievement of this approach is the utilization of ECC for biometric encryption in order to achieve biometric security from intruders. The ECC is classified as a public-key encryption (asymmetric) technique. The proposed approach guarantees full distortion and encryption of the original biometric traits to be saved in the database in order to ensure that no access of original biometrics can be achieved by intruders. Investigation tests validated the inspiring attainment of the suggested approach in well ciphering and distortion of the stored biometrics. Thus, it is more suitable for generating secure biometric patterns compared to traditional encryption methods. The capability of the proposed approach to satisfactorily cipher and distort a variety of biometric datasets has been proved. So, the suggested cancelable biometric recognition approach is a good candidate

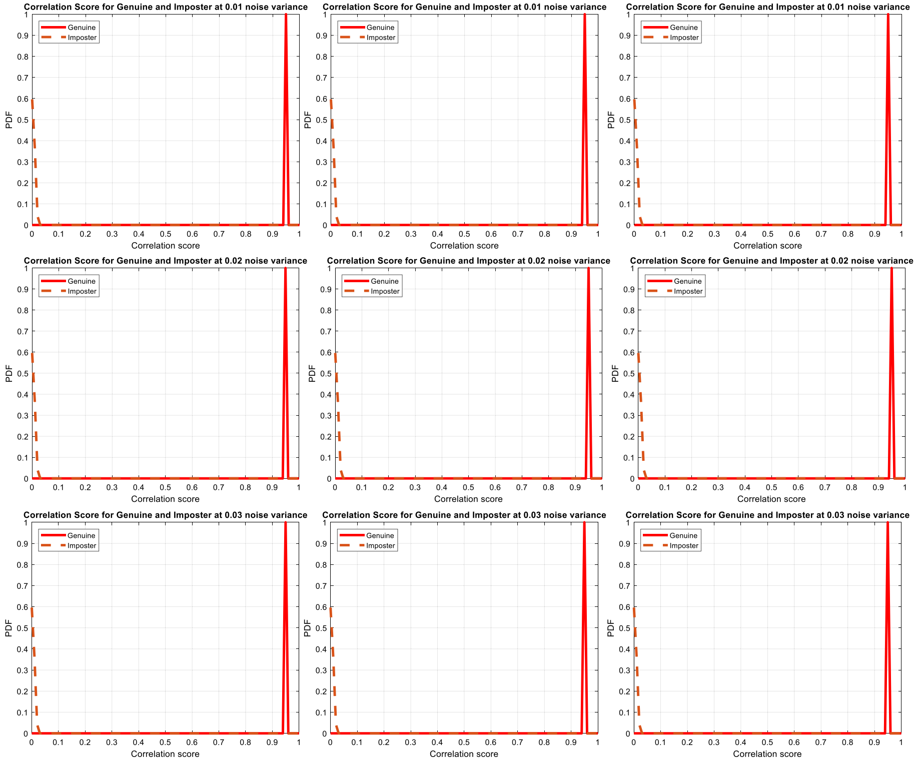

Fig. 12 Correlation scores with the FERET in the first column, ORL in the second column and the third column is for LFW dataset for 0.01, 0.02 and 0.03 noise variances

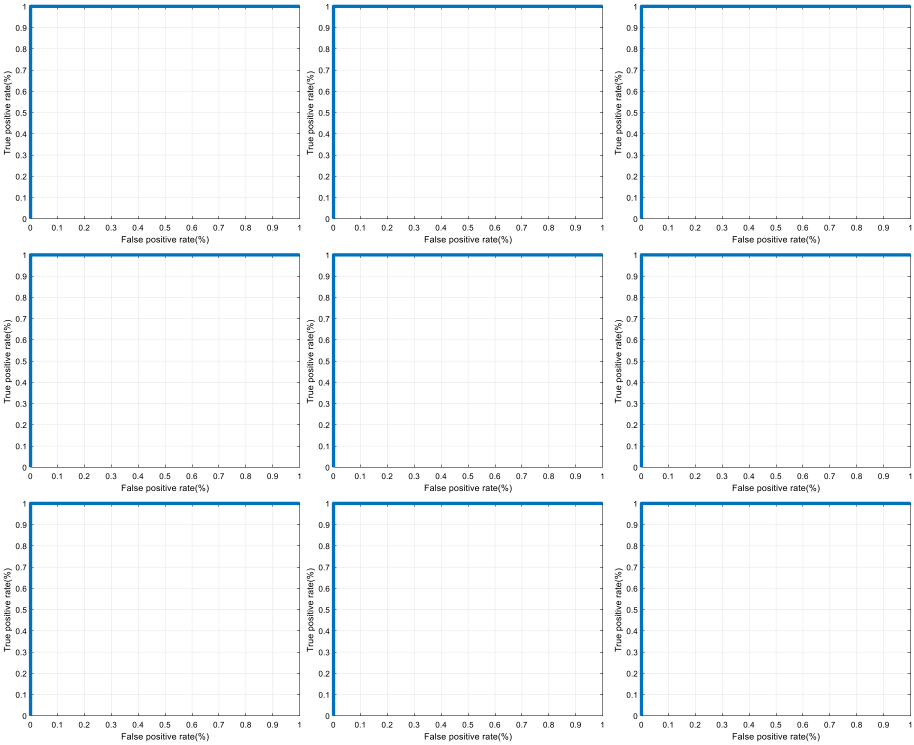

Fig. 13 ROC with the FERET in the first column, ORL in the second column and the third column is for LFW dataset for 0.01 noise variance at the first row, 0.02 at the second row and 0.03 at the third row

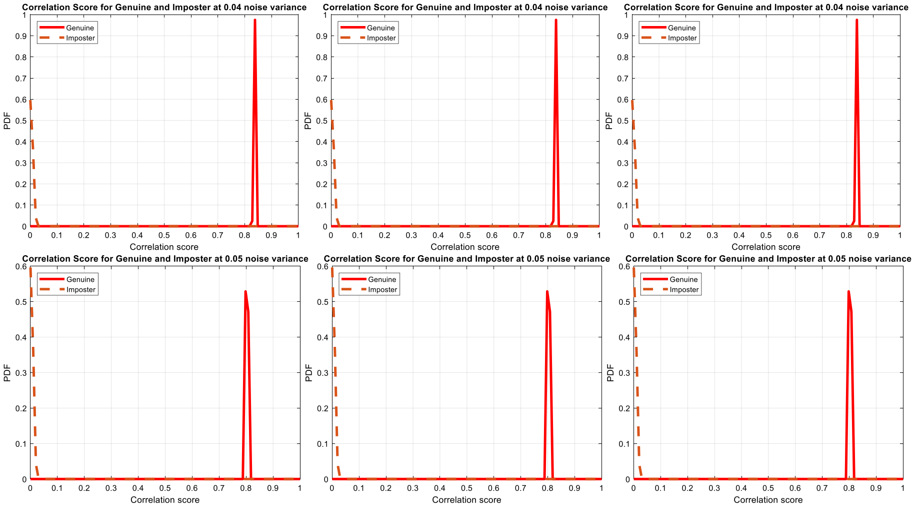

Fig. 14 Correlation scores with the FERET in the first column, ORL in the second column and the third column is for LFW dataset for 0.04 and 0.05 noise variances

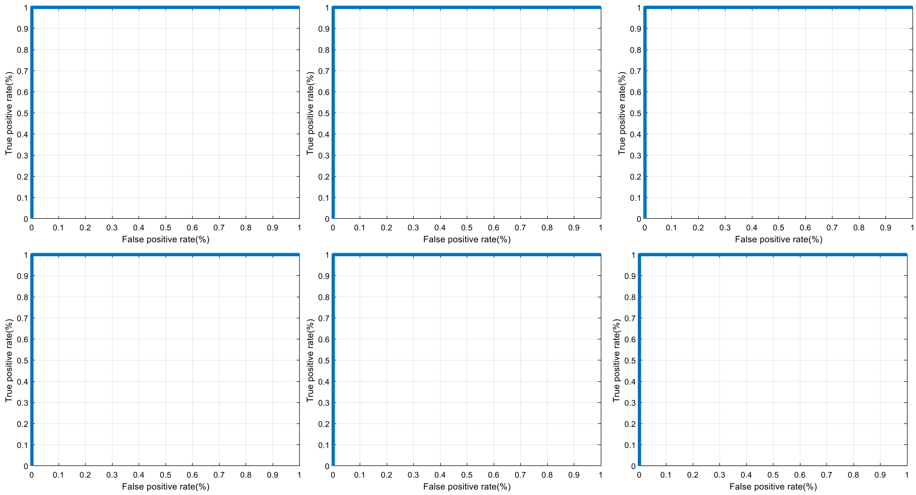

Fig. 15 ROC with the FERET in the first column, ORL in the second column and the third column is for the LFW dataset for 0.04 noise variance at the first row and 0.05 at the second row

Table 2 Evaluation metrics with different levels of noise variance for the proposed ECC-based cancelable face recognition approach for ORL, FERET, and LFW databases

Database	ORL		FERET		LFW	
Variance	EER	ROC	EER	ROC	EER	AROC
0.01	0	1	0	1	0	1
0.02	0	1	0	1	0	1
0.03	0	1	0	1	0	1
0.04	0	1	0	1	0	1
0.05	0	1	0	1	0	1

Table 3 Comparative analysis

Approach	EER	AROC
Proposed	0.00726	0.9999
Soliman et al. (2021a)	3.1524×10^{-5}	0.8630
El-Hameed et al. (2022)	8.7546×10^{-4}	0.7187
Ibrahim et al. (2020)	0.0046	0.8837
Ratha et al. (2007)	0.0016	0.8737
Kaur and Khanna (2016)	9.5647×10^{-3}	0.8684

for modern access technology. In the future work, we plan to design a cancelable biometric system based on steganography, encryption, and watermarking concepts for achieving a higher level of security. In addition, a further improved deep learning model for cancelable biometric recognition will be introduced for cloud-based applications.

Acknowledgements The researchers would like to acknowledge Deanship of Scientific Research, Taif University for funding this work.

Author contributions All authors equally contributed.

Funding The researchers would like to acknowledge Deanship of Scientific Research, Taif University for funding this work.

Availability of data and materials All data are available upon request from the corresponding author.

Declarations

Conflict of interest The authors have neither relevant financial nor non-financial interests to disclose.

Ethical approval Not applicable—The manuscript does not contain any human or animal studies.

Consent to participate All authors contributed and accepted to submit the current work.

Consent to publication All authors accepted to submit and publish the submitted work.

References

Abd El-Samie, F.E., Nassar, R.M., Safan, M., Abdelhamed, M.A., Khalaf, A.A., El Banby, G.M., El-Shafai, W.: Efficient implementation of optical scanning holography in cancelable biometrics. Appl. Opt. **60**(13), 3659–3667 (2021)

Abdelwahab, K.M., El-atty, A., Saied, M., El-Shafai, W., El-Rabaie, S., El-Samie, A.: Efficient SVD-based audio watermarking technique in FRT domain. Multimed. Tools Appl. **79**(9), 5617–5648 (2020)

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 (2020a)

Alarifi, A., Sankar, S., Altameem, T., Jithin, K.C., Amoon, M., El-Shafai, W.: A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications. IEEE Access **8**, 128548–128573 (2020b)

Algarni, A.D., El Banby, G., Ismail, S., El-Shafai, W., El-Samie, F.E.A., Soliman, N.F.: Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy **22**(12), 1361 (2020a)

Algarni, A.D., El Banby, G.M., Soliman, N.F., El-Samie, F.E.A., Iliyasu, A.M.: Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancelable face recognition. Electronics **9**(6), 1046 (2020b)

Buriro, A., Crispo, B., Conti, M.: AnswerAuth: a bimodal behavioral biometric-based user authentication scheme for smartphones. J. Inf. Secur. Appl. **44**, 89–103 (2019)

El-Hameed, H.A.A., Ramadan, N., El-Shafai, W., Khalaf, A.A., Ahmed, H.E.H., Elkhamy, S.E., El-Samie, F.E.A.: Cancelable biometric security system based on advanced chaotic maps. Vis. Comput. **38**(6), 2171–2187 (2022)

El-Shafai, W.: Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission. 3D Res. **6**(1), 1–13 (2015)

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 Access **9**, 77675–77692 (2021a)

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 (2021b)

Faragallah, O.S., AlZain, M.A., El-Sayed, H.S., Al-Amri, J.F., El-Shafai, W., Afifi, A., Soh, B.: Secure color image cryptosystem based on chaotic logistic in the FrFT domain. Multimed. Tools Appl. **79**(3), 2495–2519 (2020)

FERET Database. Available online: https://www.nist.gov/itl/products-and-services/color-feret-database (2020b). Accessed 1 June 2020

Gowthami, A., Mamatha, H.: Fingerprint recognition using zone based linear binary patterns. Procedia Comput. Sci. **58**, 552–557 (2015)

Harkanson, R., Kim, Y.: Applications of elliptic curve cryptography: a light introduction to elliptic curves and a survey of their applications. In: Proceedings of the 12th Annual Conference on Cyber and Information Security Research, pp. 1–7. (2017, April)

Hayat, U., Azam, N.A.: A novel image encryption scheme based on an elliptic curve. Signal Process. **155**, 391–402 (2019)

Helmy, M., El-Shafai, W., El-Rabaie, E.S.M., El-Dokany, I.M., Abd El-Samie, F.E.: A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications. Optik **258**, 168773 (2022)

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**(10), 14053–14078 (2020)

Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)

Kaur, H., Khanna, P.: Biometric template protection using cancelable biometrics and visual cryptography techniques. Multime. Tools Appl. **75**(23), 16333–16361 (2016)

Kaur, G., Verma, C.K.: Comparative analysis of biometric modalities. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(4), 603–613 (2014)

Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)

Laiphrakpam, D.S., Khumanthem, M.S.: Medical image encryption based on improved ElGamal encryption technique. Optik **147**, 88–102 (2017)

Laiphrakpam, D.S., Khumanthem, M.S.: A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimed. Tools Appl. **77**(7), 8629–8652 (2018)

Lauter, K.: The advantages of elliptic curve cryptography for wireless security. IEEE Wirel. Commun. **11**(1), 62–67 (2004)

LFW Database. Available online http://vis-www.cs.umass.edu/lfw/ (2020b). Accessed 1 June 2020

Menezes, A.J., Okamoto, T., Vanstone, S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**(5), 1639–1646 (1993)

Miller, V. S.: Use of elliptic curves in cryptography. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 417–426. Springer, Berlin, Heidelberg (1985)

Nishchal, N.K.: Optical cryptosystems. IOP Publishing (2019)

ORL Database. Available online https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html (2020c). Accessed 1 June 2020

Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Signal Process. Mag. **32**(5), 54–65 (2015)

Punithavathi, P., Subbiah, G.: Can cancelable biometrics preserve privacy? Biom. Technol. Today **2017**(7), 8–11 (2017)

Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)

Rathgeb, C., Busch, C.: Multi-biometric template protection: issues and challenges. New Trends Dev. Biom. (2012). https://doi.org/10.5772/52152

Soleymani, A., Nordin, M.J., Hoshyar, A.N., Ali, Z.M., Sundararajan, E.: An image encryption scheme based on elliptic curve and a novel mapping method. Int. J. Dig. Content Technol. Appl. **7**(13), 85 (2013)

Soliman, R.F., El Banby, G.M., Algarni, A.D., Elsheikh, M., Soliman, N.F., Amin, M., Abd El-Samie, F.E.: Double random phase encoding for cancelable face and iris recognition. Appl. Opt. **57**(35), 10305–10316 (2018)

Soliman, N.F., Algarni, A.D., El-Shafai, W., Abd El-Samie, F.E., El Banby, G.M.: An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics. CMC-Comput. Mater. Contin. **69**(2), 1571–1595 (2021a)

Soliman, N.F., Khalil, M.I., Algarni, A.D., Ismail, S., Marzouk, R., El-Shafai, W.: Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. Multimed. Tools Appl. **80**(3), 4789–4823 (2021b)

Toughi, S., Fathi, M.H., Sekhavat, Y.A.: An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. Signal Process. **141**, 217–227 (2017)

Washington, L.C.: Elliptic curves: number theory and cryptography. CRC Press (2008)

Xu, K.: Monolithically integrated Si gate-controlled light-emitting device: science and properties. J. Opt. **20**(2), 024014 (2018)

Zhang, X., Wang, X.: Digital image encryption algorithm based on elliptic curve public cryptosystem. IEEE Access **6**, 70025–70034 (2018)

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

Authors and Affiliations

Rania A. Eltaieb[1] · Ghada M. El-Banby[2] · Walid El-Shafai[1,3] · Fathi E. Abd El-Samie[1,4] · Alaa M. Abbas[5]

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

Rania A. Eltaieb
raniaantar2017@gmail.com

Ghada M. El-Banby
ghadaelbanby75@gmail.com

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

Alaa M. Abbas
a.alaa@tu.edu.sa

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

[2] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

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

[4] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

[5] Department of Electrical Engineering, College of Engineering, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia