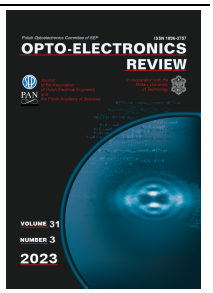
PAN

Opto-Electronics Review

journal homepage: https://journals.pan.pl/opelre



Cancelable template generation based on quantization concepts

Rana M. Nassar[1], Ashraf A. M. Khalaf[1], Ghada M. El-Banby[2], Fathi E. Abd El-Samie[3,4], Aziza I. Hussein[5], Walid El-Shafai[3,6*]

[1] Department of Electrical Engineering, Faculty of Engineering, Minia University, Minia 61519, Egypt
[2] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[4] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdurrahman University, Riyadh 84428, Saudi Arabia
[5] Electrical and Computer Engineering Department, Effat University, Jeddah, Kingdom of Saudi Arabia
[6] Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia

Article info

Article history:
Received 28 Nov. 2022
Received in revised form 31 Mar. 2023
Accepted 01 Apr. 2023
Available on-line 28 Jun. 2023

Keywords:
Cancelable biometrics;
quantization concepts;
DCT;
JPEG;
access control;
authentication.

Abstract

The idea of cancelable biometrics is widely used nowadays for user authentication. It is based on encrypted or intentionally-distorted templates. These templates can be used for user verification, while keeping the original user biometrics safe. Multiple biometric traits can be used to enhance the security level. These traits can be merged together for cancelable template generation. In this paper, a new system for cancelable template generation is presented depending on discrete cosine transform (DCT) merging and joint photographic experts group (JPEG) compression concepts. The DCT has an energy compaction property. The low-frequency quartile in the DCT domain maintains most of the image energy. Hence, the first quartile from each of the four biometrics for the same user is kept and other quartiles are removed. All kept coefficients from the four biometric images are concatenated to formulate a single template. The JPEG compression of this single template with a high compression ratio induces some intended distortion in the template. Hence, it can be used as a cancelable template for the user acquired from his four biometric traits. It can be changed according to the arrangement of biometric quartiles and the compression ratio used. The proposed system has been tested through merging of face, palmprint, iris, and fingerprint images. It achieves a high user verification accuracy of up to 100%. It is also robust in the presence of noise.

1. Introduction

Individual biometric traits, whether behavioural or physical, are different and they can be used to distinguish each person from the others. For this reason, biometric traits have become efficient tools for critical system authentication. Unfortunately, saving biometric traits in their original forms might face database assaults. Hence, systems that depend on biometrics in their original versions are not secure enough. To solve this problem, researchers developed the idea of cancelable biometrics. Cancelable biometric systems (CBS) are based on biometric templates that have been purposely altered or encrypted. Any biometric authentication system has two stages, namely enrollment and authentication [1]. Increasing the user biometric secrecy and preserving a high degree of discrimination between users are the two goals of biometric authentication systems. It is important to achieve a trade-off between these two conflicting goals [2].

The term "cancelable biometrics" was originally used in 2008 by Ratha *et al.* [2]. In CBS, dummy biometric identities are stored in the database during enrollment. The same dummy biometric identities are created for verification purposes using the original biometrics that were obtained during authentication. In CBS, matching is performed between the cancelable dummy biometric

*Corresponding author at: eng.waled.elshafai@gmail.com

https://doi.org/10.24425/opelre.2023.145940
1896-3757/ Association of Polish Electrical Engineers (SEP) and Polish Academic of Sciences (PAS). Published by PAS

templates. If a hacker is able to obtain these dummy biometric identities, new ones are generated. They should be entirely distinct from those that have previously been compromised. This meets the two essential criteria of CBS, which are revocability and diversity.

Biometric salting and non-invertible transforms are the most popular methods used in CBS. CBS based on salting can be built with random noise addition, random convolution, and random permutation [2, 3]. Random projection is one of the widely-used tools for the generation of cancelable biometric templates. Random projection means the projection of extracted feature vectors from a higher-dimensional space onto a lower-dimensional space using a random matrix.

There is another CBS classification to unimodal and multimodal systems. Unimodal biometric systems depend on only one biometric in the authentication, but multimodal systems depend on more than one biometric. Each of them has its advantages and disadvantages, and only the application and the requirements determine the appropriate system.

1.1. Paper motivation

Compression is one of the essential tools that are applied to images. Compression is performed to reduce the size of the image, decrease the memory used, and decrease the processing time [3–5]. One of requirements of image compression is keeping the high image quality. On the other hand, the main idea of CBS is to obtain new patterns that have low correlation with the original ones. The motivation of this paper is generating cancelable templates based on quantization concepts used in image compression in a way that distorts the biometric images. Image compression is applied to different biometric images including face, fingerprint, iris, and palmprint. This paper presents a unimodal system by applying the proposed compression algorithm on each biometric, separately. The system performance with different biometric traits is investigated. The paper also presents a multimodal system that works by applying the proposed compression algorithm on four combined biometrics.

The main idea of this paper is taken from the JPEG image compression standard. It is implemented as follows:

- In the unimodal system, the proposed compression algorithm is applied on each biometric, separately.
- In the multimodal system, four biometric images that belong to the same individual are comressed after combinig them by the DCT. The first quartile of the DCT of each biometric image is kept. Hence, only strong DCT coefficients are kept. After that, the first quartiles of all biometric images are combined together in a single matrix. Finally, the obtained new matrix is compressed with the designed quantization table to induce distortion.

1.2. Paper contributions

The paper contributions can be summarised as follows:

1. The image is divided into blocks and the DCT is applied on each block to obtain the high-, mid- and low-frequency coefficients.
2. In most images, the low-frequency coefficients carry most of the energy, which lies in the upper left quartile of the DCT. Keeping this quadrtile maintains the image information.
3. Unlike compression, a quntization table is designed to attenuate the low-frequency coefficients and maintain the mid- and high-frequency coefficients to obtain a distotred compressed image. The quntization table has the same size as that of the blocks.

1.3. Paper structure

This paper is divided into several sections. Section 2 gives an explanation of the related work. Section 3 introduces the idea of the proposed cancelable biometric systems that depend on JPEG compression. Simulation results are shown in section 4. Conclusion is finally provided in section 5.

2. Related work

In recent years, different works about CBS have been presented based on different tools. Iris segmentation and localisation have been utilized by Soliman *et al*. [6] for iris-based authentication. This system achieved a 99.67% average accuracy and an equal error rate (EER) of 0.58%. The Johnson-Lindenstrauss lemma represents the basis for this idea. Soliman *et al*. [7] presented another system based on convolution kernels created with chaotic maps to construct encrypted Gabor features from iris images. In this system, the encryption key is determined by the extracted feature vector. An accuracy of 99.08% and an EER of 1.17% have been achieved with an enhanced logistic map.

Qiu *et al*. [8] designed a look-up table-based system for cancelable palmprint recognition. Using chaotic matrices and Gabor filtering, features are extracted. Based on the chosen check bits, the built-up blocks are converted to comprehensive decimals and delivered to look-up databases. With a high identification accuracy of 99.92%, the CBS based on palmprint templates achieved high security levels. Additionally, Soliman *et al*. [9] introduced an efficient bio-convolving system that depends on an encrypted feature matrix to guarantee user privacy. The scale-invariant feature transform (SIFT) has been used to extract features from face images. An EER of 0.0017 and an area under the receiver operating characteristic curve (AROC) of 0.993 have been achieved with this system. Jin *et al*. introduced a unimodal CBS based on fingerprint minutiae features [10]. It depends on minutiae proximity decomposition (MVD) to generate the cancelable templates from the fingerprints. This system achieved an EER of 1.77. In Ref. 11, Gowthamim and Mamatha used linear binary patterns to extract fingerprint features. The fingerprint image is sectioned into nine sectors with equal size. Each sector gives its linear binary pattern. This system achieved an average accuracy of 94.28%.

A multimodal system that depends on adaptive Bloom filters was introduced by Christian and Fierrez [12]. This system achieved an EER of 0.4%. Abd El-Samie *et al*. [13] presented a cancelable multi-biometric security system in which several biometric traits for the same person are treated to obtain a single cancelable template. Optical scanning holography is applied during the acquisition of

each biometric to guarantee robustness of the system in noisy environments. Abdellatef *et al*. [14] presented a system based on merging hand-crafted and extracted deep-learned features using a fusion network. The results of the trials conducted on various datasets showed that this system has recognition accuracies ranging from 95.59% to 99.22%. Tarif *et al*. presented a multimodal CBS based on features extracted from the fingerprint and iris images and hidden into face images by means of the slantlet transform singular values (SLT-SVs) [15].

Abdullatif *et al*. presented a cancelable biometric recognition system based on a convolutional neural network (CNN) model with bio-convolution [16]. The system achieved high accuracy, while maintaining the capacity to discard compromised biometric traits. Additionally, the rates of recognition ranged from 95.48% to 99.15%.

3. The proposed cancelable biometric recognition system

Image compression is an important branch of image processing. It means reducing image size without degrading the image quality. There are two types of compression, one is lossless and the other is lossy. Lossless compression means reducing the image size by removing the unnecessary data or redundancy. This type preserves the image quality [17]. On the other hand, lossy compression does not preserve the image quality and may cause image distortion during compression. The JPEG compression is one of the lossy compression types. Its steps can be summarised as follows:

1. The image is first divided into 8 × 8 blocks.
2. The grayscale image pixel values range from 0 to 255, but the DCT is designed to work on pixel values ranging from −128 to 127. So firstly, the original block pixels are leveled-off by subtracting 128 from each pixel value.
3. The DCT is applied on each block as follows:

$$D(i,j) = \frac{1}{\sqrt{2N}} c(i)c(j) \cdot \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} p(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right], \quad (1)$$

where N is the block size, (i,j) is the pixel position in the DCT domain and (x,y) is the spatial pixel position in the block.

4. The cancelable template generation is based on the quantization table. The compression level and image quality depend on the selected quantization table. Quantization is performed on each block. There is a standard quantization table for compression. It maintains good quality of compressed images.
5. To obtain the cancelable templates, a rotated quantization table is used for obtaining the quantized DCT coefficients. The traditional table of JPEG is shown in Fig. 1(a). The rotated table used in the proposed system is shown in Fig. 1(b). The main objective of rotation is to induce distortion rather than keeping the main energy coefficients. The low-frequency components are damped. On the other hand, the high-frequency components are high. This leads to some sort of distortion. This modification gives the ability to distort the biometric image, while keeping its spectral signature.

Each element in the $D(i,j)$ matrix is divided by the corresponding element in the quantization table. Then, the result is rounded to the nearest integer value,

$$c(i,j) = \text{round}\left(\frac{D(i,j)}{\text{rotate } Q(i,j)}\right). \quad (2)$$

Figure 1 shows the standard quantization table, the modified quantization table, and the corresponding image obtained with each table.

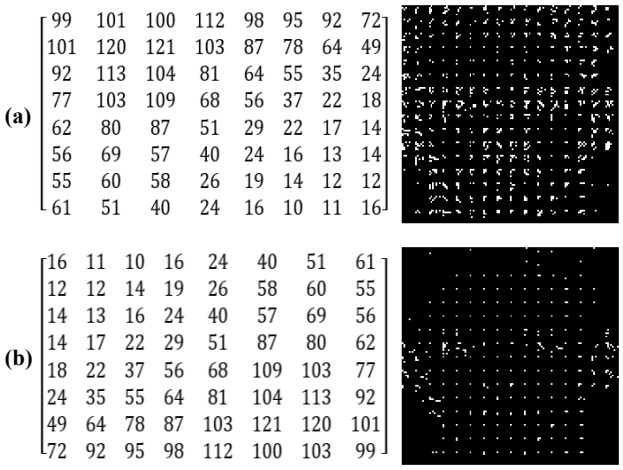


Fig. 1. Quantization table and the corresponding compressed image in the DCT domain: standard quantization table (a) and rotated quantization table (b).

In this paper, the steps shown in Fig. 2 are used to intentionally distort the biometric image to obtain a cancelable template. A unimodal biometric system is presented through adopting only one biometric to verify users. The cancelable template is generated by applying the destructive compression directly on the biometric image. The system is applied on face, fingerprint, palmprint, and iris images, individually. Verification is performed through cancelable templates.

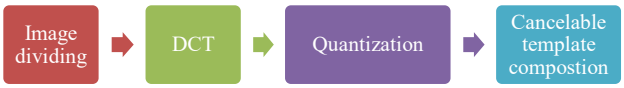


Fig. 2 Cancelable template generation.

A multimodal biometric system is also presented by first merging four biometric images together before the destructive compression. The DCT is applied on each biometric image. It divides the image into four quartiles. The first quartile holds the basic information that characterises the image. The first quartiles of all biometric images are combined together in a single matrix. Hence, the first quartile of the composite image carries the DCT of the face, the second quartile carries the DCT of the iris, the third quartile carries the DCT of the fingerprint, and the fourth quartile carries the DCT of the palmprint. Finally, the combined matrix is distorted through quantization.

Figure 3 shows the multimodal cancelable template generation by DCT and quantization. Figure 4 shows the whole system with enrollment and verification phases.

The DCT is often used for compression and quantization applications. While discrete wavelet transform (DWT) has its own advantages, such as being more suitable for certain types of signals with irregularities or discontinuities, the choice between DCT and DWT ultimately depends on the specific application and signal characteristics. In this work, it was decided to use DCT, because it is well-suited for image and video compression, which is the primary application that is focused on. So, DCT and DWT are both commonly used for compression and quantization in signal and image processing applications. However, there are some reasons why DCT is preferred to DWT in certain situations. These reasons include:

- ***Computational complexity:*** DCT is computationally simpler than DWT, which means it requires less processing power and time. This makes it more suitable for real-time applications, where speed is important.
- ***Energy compaction:*** DCT has better energy compaction than DWT, which means it can represent more of the signal energy with a smaller number of coefficients. This makes it more efficient for compression purposes.
- ***Higher frequency resolution:*** DWT provides better frequency resolution at higher frequencies than DCT, but this is not always necessary in compression applications where the focus is on preserving the lower frequency components.
- ***Availability of standards:*** DCT is widely used in image and video compression standards such as JPEG, MPEG, and H.264, which makes it more convenient for interoperability and compatibility with existing systems.

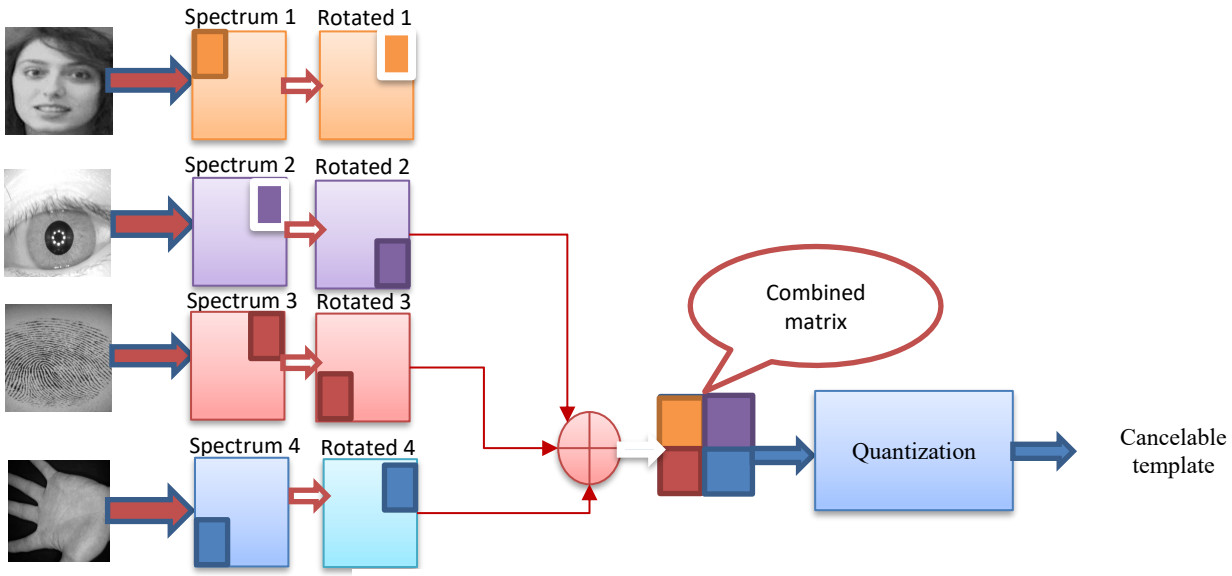


Fig. 3. Multimodal cancelable template generation.

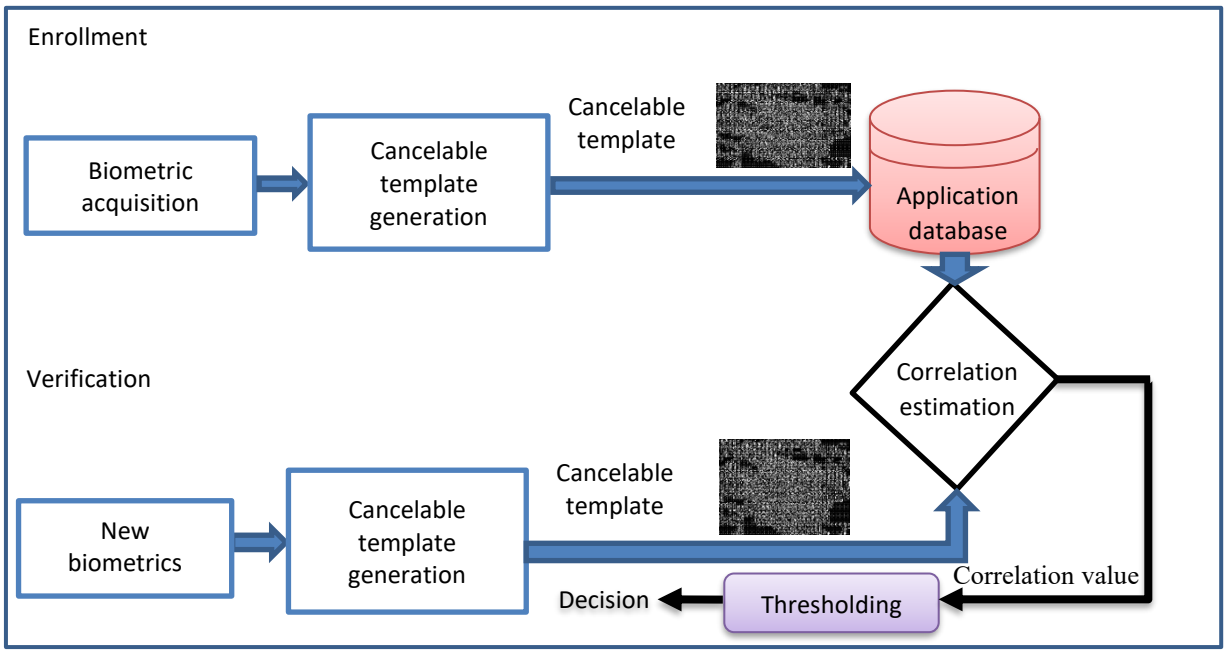


Fig. 4. The proposed multimodal biometric system.

Overall, the choice between DCT and DWT depends on the specific requirements and constraints of the application. While DWT has some advantages over DCT, DCT is often preferred due to its simplicity, efficiency, and compatibility with existing standards.

In addition, cancelable template generation based on quantization concepts involves generating a biometric template from a user biometric data (such as fingerprint or iris) that can be securely stored and used for authentication purposes. The template is generated using a quantization process that discretises the continuous biometric data into a finite set of values. In this context, DCT is preferred over DWT for the following reasons:

- ***Lower complexity:*** DCT has lower computational complexity than DWT, which makes it more efficient for the quantization process used in template generation.
- ***Better energy compaction:*** DCT has better energy compaction properties than DWT, which means it can represent more of the signal energy with less coefficients. This is important for generating a compact template that can be easily stored and transmitted.
- ***Standardization:*** DCT is a widely-used standard in image and video compression, which means that there are well-established algorithms and libraries available for implementing it. This makes it easier to integrate DCT-based quantization into existing systems.
- ***Security considerations:*** DWT-based quantization may be vulnerable to certain attacks, such as the wavelet denoising attack, which can compromise the security of the generated template. DCT-based quantization, on the other hand, is less vulnerable to such attacks and can provide stronger security guarantees.

Thus, DCT is preferred to DWT for cancelable template generation based on quantization concepts due to its lower complexity, better energy compaction, and stronger security guarantees.

Also, the decision to use conventional DCT instead of deep learning for the proposed work depends on various factors, including the problem requirements, data availability, computational complexity, and interpretability of the solution.

Here are some reasons why conventional DCT might be preferred to deep learning:

- ***Interpretability:*** Conventional DCT is a well-established and interpretable mathematical transform that is widely used in image and signal processing. The output of the DCT can be easily understood and analysed in terms of the frequency components of the input signal. This makes it easier to explain and validate the results obtained from the DCT-based cancelable template generation.
- ***Computational efficiency:*** DCT is a computationally efficient algorithm that can be easily implemented on various hardware and software platforms. On the other hand, deep learning requires significant computational resources, including high-end GPUs and specialized software frameworks, making it less feasible for some applications.
- ***Data availability:*** Deep learning algorithms require large amounts of labelled data to train the models, effectively. However, in some applications, such as biometric template generation, collecting and storing large amounts of biometric data can raise privacy concerns. In such cases, DCT-based cancelable template generation can be a viable alternative, as it requires only a small number of reference templates to generate the cancelable templates.
- ***Security and privacy:*** Cancelable templates generated using DCT-based methods can be more secure and privacy-preserving than those generated using deep learning. This is because DCT-based methods generate cancelable templates by applying quantization to the reference templates, which makes it difficult for attackers to recover the original templates from the cancelable templates.

In summary, the use of the conventional DCT for the proposed work is preferred to the use of deep learning due to its interpretability, computational efficiency, data availability, security and privacy advantages.

4. Simulation results

4.1. Tested datasets

Four datasets of face images, fingerprints, iris images, and palmprints are used to test the proposed CBS. The datasets employed in these tests include the ORL database for faces [18], the FNC2002 DB 1 for fingerprints [19], the CASIA-V3 for iris [20], and the CASIA-V1 for palmprints [21]. The ORL database of faces contains 400 images for 40 distinct subjects. The size of each image is 92×112 pixels, with 256 grey levels per pixel. The FNC2002 fingerprint dataset contains 800 images that have been acquired with an optical sensor with 500 dots per inch resolution and a size of 388×374. CASIA-IrisV3 dataset contains a total of 22035 iris images for more than 700 subjects [22–28]. All iris images are 8-bit grey-level JPEG files, collected under near-infrared illumination. CASIA palmprint image dataset contains 5502 palmprint images captured for 312 subjects. All palmprint images are 8-bit grey-level JPEG files.

4.2. Simulation environment

The outcomes of the proposed systems have been obtained on a workstation havig an Intel Core (TM) i5-7200U CPU 2.71 GHz, 8.00 GB of RAM, Windows 7, 64-bit operating system, and MATLAB R2016a.

4.3. Authentication evaluation metrics

Authentication performance evaluation has been made through:

Histogram analysis: Histogram of a cancelable template must satisfy the conditions [29]:

1. Total difference from that of the original biometric template.
2. Uniform distribution.

Correlation coefficient (c_r): The correlation is estimated between the original and encrypted biometric templates. As the value of c_r decreases, the encryption system becomes stronger. The c_r is calculated as follows [30–33]:

$$c_r = \frac{\mathrm{cov}(x,y)}{\partial_x \partial_y} = \frac{\sum_{i=1}^{M}(x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^{M} x_i - E(x))^2)}\ \sqrt{(\sum_{i=1}^{M} y_i - E(y))^2)}}, \quad (3)$$

where x and y are the grey-level pixel values of the original and encrypted biometrics, and M is the number of pixels. in each template

Probability of true distribution (PTD) and probability of false distribution (PFD): PTD and PFD are used to determine the discrimination threshold based on the correlation values. The EER is estimated at the intersection point of both distributions [34, 35].

Receiver operating characteristic (ROC) curve analysis: With different cut-off points, the true positive rate (sensitivity) is plotted in the ROC curve as a function of the false positive rate (100-specificity). The area under the ROC curve reflects the efficiency of the CBS [36, 37].

4.4. Simulation analysis

Two systems are presented. One is unimodal based on applying the proposed quantization-based compression on the different biometric images, individually. Figure 5 shows random samples of the utilized biometric datasets. Figure 6 shows the cancelable templates generated from the unimodal system. Figure 7 shows the distribution curves in addition to ROC curves for the systems based on different biometrics. It indicates that the iris-based identification achieves the best performance. In addition, Table 1 gives the numerical values in each case.

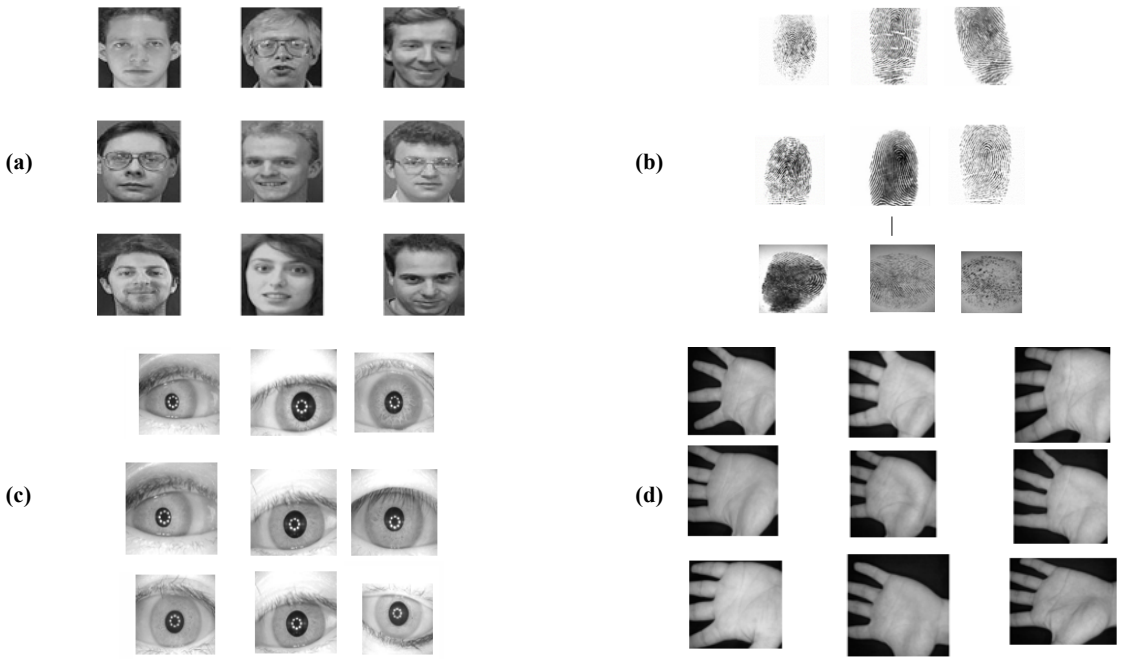


Fig. 5. Random samples of the tested biometrics from: ORL face database (a), FNC2002 DB_1 fingerprint dataset (b), CASIA-V3 iris dataset (c), and CASIA-V1 palmprint dataset [22–25] (d).

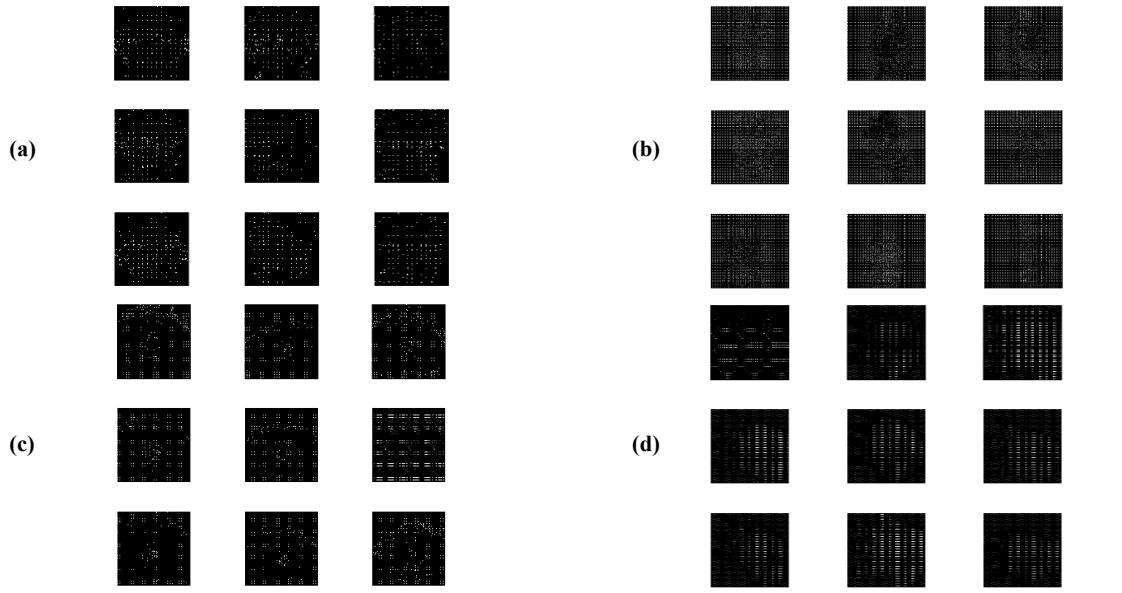


Fig. 6. Cancelable templates for the proposed unimodel CBS: ORL face database (a), FNC2002 DB_1 fingerprint dataset (b), CASIA-V3 iris dataset (c), and CASIA-V1 palmprint dataset (d).

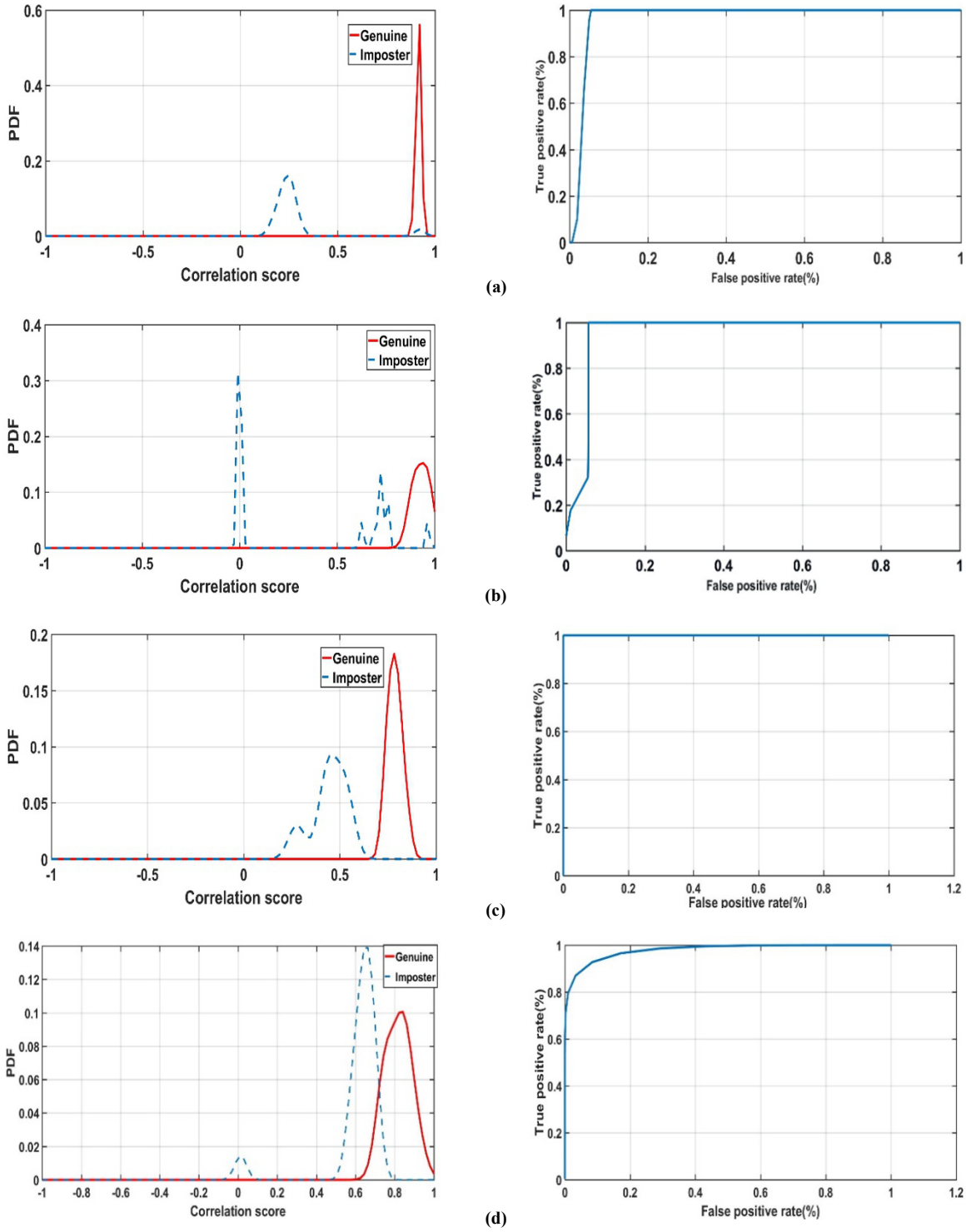


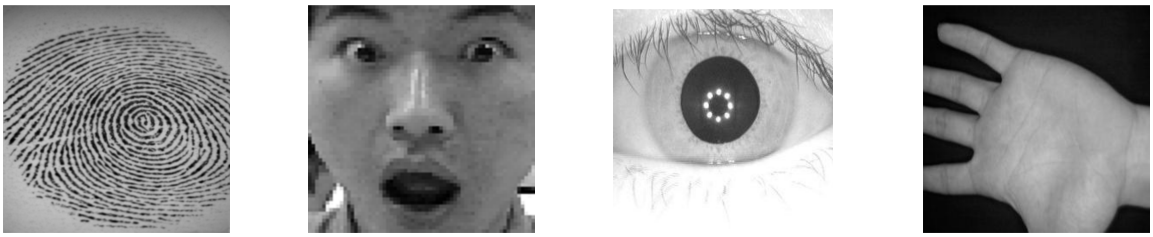
Fig. 7. PTD, PFD, and ROC curves for the proposed unimodal CBS at a noise variance of 0.01: face (a), fingerprint (b), iris (c), and palmprint (d).

Table 1.
Different evaluation metric values for the proposed unimodal CBS at a noise variance of 0.01.

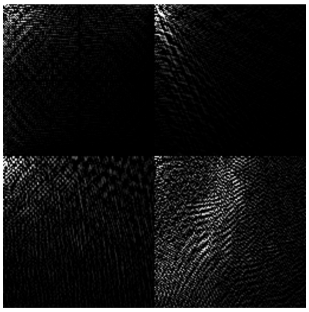
Noise variance	EER	AROC	FRR	FAR
Face	$3.4249 \cdot 10^{-4}$	0.9640	$3.9857 \cdot 10^{-4}$	0.0555
Fingerprint	$2.1144 \cdot 10^{-86}$	0.9569	$4.22287 \cdot 10^{-86}$	0.04449
Iris	$6.8588 \cdot 10^{-10}$	1	$1.3569 \cdot 10^{-9}$	$1.5527 \cdot 10^{-11}$
Palmprint	0.0543	0.9790	0.1298	0.0837

FAR – false acceptance rate, FRR – false rejection rate.

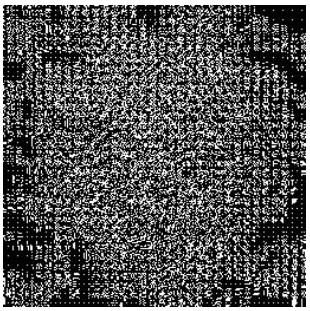
In the proposed multimodal system, to create a single biometric template for each person, four separate biometric images that are thought to belong to the same person are combined. The DCT of each biometric must be obtained in order for the merging scenario to work, and only the first quartile of the DCT should be kept. These biometric quartiles are organized into a single matrix for a composite DCT. First, four specific biometrics are used to test the proposed multimodal system. Figure 8 displays an example of the merged biometrics, the composite DCT, and the obtained cancelable template. Each cancelable template has a size of 256×256, and the verification procedure takes an average of 2.3 sec to complete. Figure 9 shows random samples of the cancelable templates and their histograms.



(a) A set of four biometric images (fingerprint, face, iris and palmprint).



(b) The four images at the DCT stage (DCT composite image).



(c) Result of the destructive quantization step.

Fig. 8. Results for the proposed multimodal CBS at each stage.

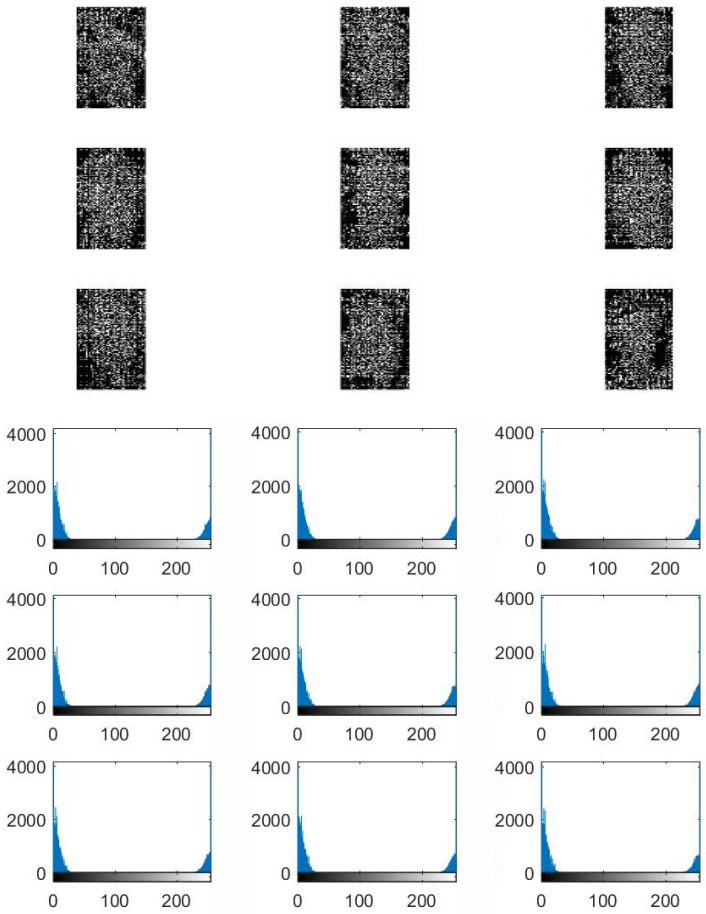
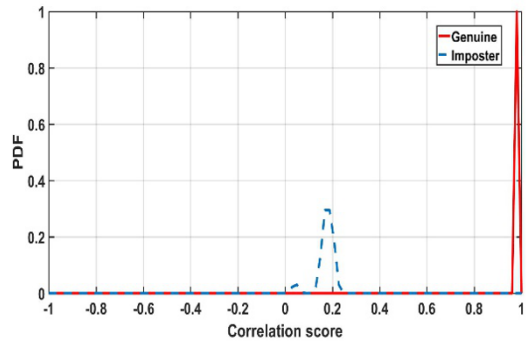
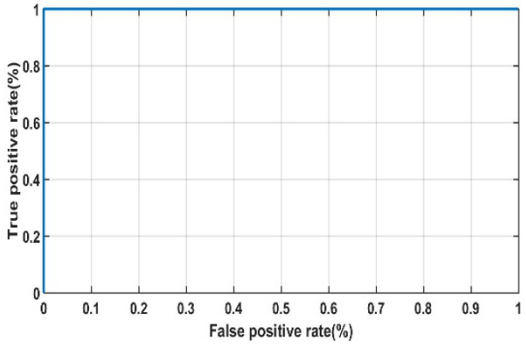


Fig. 9. Random samples of cancelable templates and their histograms for the proposed multimodal CBS.

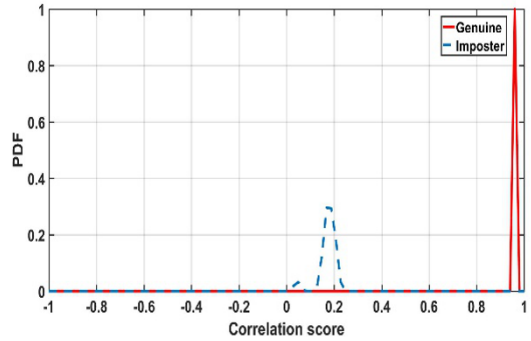
The multimodal system achieves high performance as in Fig. 10, which shows the distribution and ROC curves at different levels of noise. The high system performance is indicated in the close-to-zero EER and the close-to-one AROC. Numerical values of different evaluation metrics are given in Table 2. In addition, Table 3 gives a comparison of the proposed system with other state-of-the-art works.



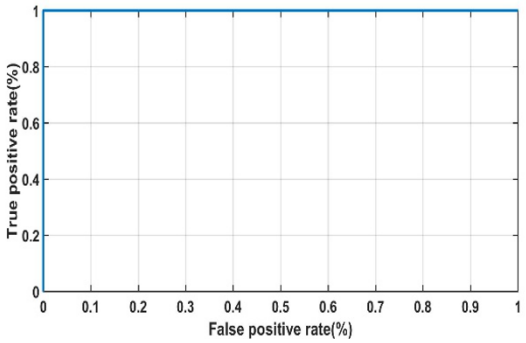
(a) PTD and PFD curves for the quantization-based CBS, at a noise variance of 0.01.



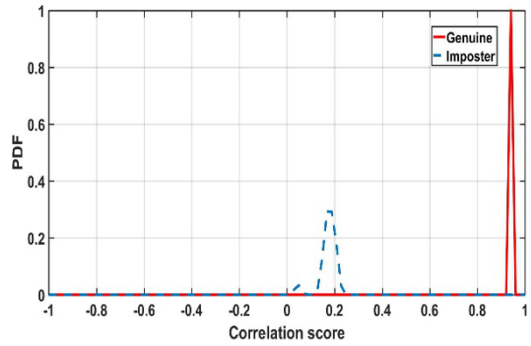
(b) ROC curve for the quantization-based CBS, at a noise variance of 0.01.



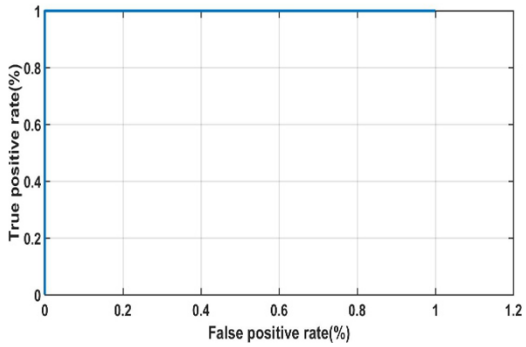
(c) PTD and PFD curves for the quantization-based CBS, at a noise variance of 0.03.



(d) ROC curve for the quantization-based CBS, at a noise variance of 0.03.



(e) PTD and PFD curves for the quantization-based CBS, at a noise variance of 0.05.



(f) ROC curve for the quantization-based CBS, at a noise variance of 0.05 .

Fig. 10. PTD, PFD, and ROC curves for the proposed multimodal CBS.

Table 2.
Different evaluation metric values at different noise levels for the proposed multimodal CBS.

Noise variance	EER	AROC	FRR	FAR
0.01	0.5000	1	1	0
0.03	$6.4187 \cdot 10^{-136}$	1	$1.2837 \cdot 10^{-163}$	0
0.05	$4.9012 \cdot 10^{-164}$	1	$9.8024 \cdot 10^{-136}$	0

Table 3.
Comparison of different systems with the proposed multimodal CBS.

Cancelable biometric system	Year	Accuracy rate (AROC)
Proposed multimodal quantization-based CBS	–	1
Gowthamim *et al*. [11]	2015	0.9428
Soliman *et al*. [7]	2018	0.9908
Qiu *et al*. [8]	2018	0.9992
Soliman *et al*. [9]	2018	0.9930
Soliman *et al*. [6]	2019	0.9967
Abdellatef *et al*. [16]	2020	0.9789
Abd El-Samie *et al*. [13]	2021	0.9990
Abdellatef *et al*. [14]	2022	0.9922

5. Conclusions and future work

This paper introduced an efficient CBS for user verification based on image merging and destructive quantization. The compression ratio can be altered to generate multiple distorted cancelable templates in case of compromise. The verification process has been performed on both single and multiple biometrics. In addition, the accuracy levels obtained with multiple biometrics are up to 100%. Hence, the security of the presented system is guaranteed through the use of multiple biometrics, while the discrimination ability is kept high. The proposed system can be considered for remote access applications. This work can be extended in the future by considering other types of compression algorithms in addition to encryption tools.

Conflicts of Interest

The authors declare that they have no conflict of interest to report regarding the present study.

Data availability

Data underlying the results presented in this paper may be obtained from the authors upon reasonable request.

Acknowledgements

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

References

[1] Jegede, A., Udzir, N. I., Abdullah, A. & Mahmod, R. Cancelable and hybrid biometric cryptosystems: current directions and open research issues. *Int. J. Adv. Appl. Sci*. (*IJAAS*) **4**, 65–77 (2017). https://doi.org/10.21833/ijaas.2017.011.010

[2] Zuo, J., Ratha, N. K. & Connell, J. H. Cancelable Iris Biometric. in *19th International Conference on Pattern Recognition* (*ICPR*) 1–4 (IEEE, 2008). https://doi.org/10.1109/ICPR.2008.4761886

[3] Algarni, A. D. *et al*. (2020). Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. *Entropy* **22**, 1361 (2020). https://doi.org/10.3390/e22121361

[4] Elashry, I. F. *et al*. (2020). Efficient chaotic-based image cryptosystem with different modes of operation. *Multimed. Tools Appl*. **79**, 20665–20687 (2020). https://doi.org/10.1007/s11042-019-08322-5

[5] Faragallah, O. S. *et al*. Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication. *J. Ambient Intell. Humaniz. Comput.* **13**, 1215–1239 (2022). https://doi.org/10.1007/s12652-020-02832-z

[6] Soliman, R. F., Amin, M. & Abd El-Samie, F. E. A modified cancelable biometrics scheme using random projection. *Ann. Data Sci.* **6**, 223–236 (2019). https://doi.org/10.1007/s40745-018-0172-1

[7] Soliman, R. F. *et al*. Efficient cancelable iris recognition scheme based on modified logistic map. *Proc. Natl. Acad. Sci. India Sect. A Phys. Sci.* **90**, 101–107 (2020). https://doi.org/10.1007/s40010-018-0555-x

[8] Qiu, J., Li., H. & Dong, J. Design of Cancelable Palmprint Templates Based on Look up Table. in *IOP Conference Series: Materials Science and Engineering* 60–70 (IOP Publishing, 2018). https://doi.org/10.1088/1757-899X/322/5/052050

[9] Soliman, R. F. *et al*. Double random phase encoding for cancelable face and iris recognition. *Appl. Opt.* **57**, 10305–10316 (2018). https://doi.org/10.1364/AO.57.010305

[10] Jin, Z., Lim, M. H., Teoh, A. B. J. & Goi, B. M. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognit. Lett.* **42**, 137–147 (2014). https://doi.org/10.1016/j.patrec.2014.02.011

[11] Gowthami, A. T. & Mamatha, H. R. Fingerprint recognition using zone based linear binary patterns. *Procedia Comput. Sci.* **58**, 552–557 (2015). https://doi.org/10.1016/j.procs.2015.08.072

[12] Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J. & Fierrez, J. Towards Cancelable Multi-Biometrics Based on Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris. in *3rd International Workshop on Biometrics And Forensics (IWBF)* 1–6 (IEEE, 2015).

[13] Abd El-Samie, F. E. *et al*. Efficient implementation of optical scanning holography in cancelable biometrics. *Appl. Opt.* **60**, 3659–3667 (2021). https://doi.org/10.1364/AO.415523

[14] Abdellatef, E. *et al*. Fusion of deep-learned and hand-crafted features for cancelable recognition systems. *Soft Comput.* **24**, 15189–15208 (2020). https://doi.org/10.1007/s00500-020-04856-1

[15] Tarif, E. B., Wibowo, S., Wasimi, S. & Tareef, A. A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. *Multimed. Tools Appl.* **77**, 2485–2503 (2018). https://doi.org/10.1007/s11042-016-4280-7

[16] Abdellatef, E. *et al*. A. cancelable face and iris recognition system based on deep learning. *Opt. Quantum Electron.* **54**, 1–21 (2022). https://doi.org/10.1007/s11082-022-03770-0

[17] Badr, I. S. *et al*. Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion. *Digit. Signal Process.* **116**, 103103 (2021). https://doi.org/10.1016/j.dsp.2021.103103

[18] *Finger Verification Competition*. http://bias.csr.unibo.it/fvc2002/databases.asp (Accessed July 2018).

[19] *ORL database*. https://www.kaggle.com/datasets/kasikrit/att-database-of-faces (Accessed July 2018).

[20] *CASIA-IrisV3 database*. http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp (Accessed July 2018).

[21] *CASIA Palm Print Database*. http://biometrics.idealtest.org/ (Accessed July 2018).

[22] El-Shafai, W., Hossam Eldein Mohamed, F. A., Elkamchouchi, H. M. A., Abd-Elnaby, M. & Elshafee, A. Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access* **9**, 77675–77692 (2021). https://doi.org/10.1109/ACCESS.2021.3082940

[23] El-Shafai, W., El-Rabaie, S., El-Halawany, M. M. & Abd El-Samie, F. E. Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication. *Int. J. Commun. Syst.* **31**, e3478 (2018). https://doi.org/10.1002/dac.3478

[24] El-Hameed, H. A. A. *et al*. Cancelable biometric security system based on advanced chaotic maps. *Vis. Comput.* **38**, 2171–2187 (2021). https://doi.org/10.1007/s00371-021-02276-2

[25] Elazm, L. A. *et al*. Hardware Implementation of Cancellable Biometric Systems. in *2020 Fourth International Conference on I-SMAC* 1145–1152 (IEEE, 2020). https://doi.org/10.1109/I-SMAC49090.2020.9243390

[26] El-Gazar, S. *et al*. Cancelable speaker identification system based on optical-like encryption algorithms. *Comput. Syst. Sci. Eng.* **43**, 87–102 (2022). https://doi.org/10.32604/csse.2022.022722

[27] Elazm, L. A. *et al*. Efficient hardware design of a secure cancellable biometric cryptosystem. *Intell. Autom. Soft Comput.* **36**, 929–955 (2023). https://doi.org/10.32604/iasc.2023.031386

[28] Almomani, I. Proposed biometric security system based on deep learning and chaos algorithms. *Comput. Mater. Contin.* **74**, 3515–3537 (2023). https://doi.org/10.32604/cmc.2023.033765

[29] El-Shafai, W. *et al*. Optical ciphering scheme for cancellable speaker identification system. *Comput. Syst. Sci. Eng.* **45**, 563–578 (2023). https://doi.org/10.32604/csse.2023.024375

[30] Ayoup, A. M. *et al*. Cancelable multi-biometric template generation based on dual-tree complex wavelet transform. *Intell. Automat. Soft Comput.* **33**, 1289–1304 (2022). https://doi.org/10.32604/iasc.2022.024381

[31] Ayoup, A. M. *et al*. Cancellable multi-biometric template generation based on Arnold cat map and aliasing. *Comput. Mater. Contin.* **72**, 3687–3703 (2022). https://doi.org/10.32604/cmc.2022.025902

[32] Ayoup, A. M. *et al*. Selective cancellable multi-biometric template generation scheme based on multi-exposure feature fusion. *Intell. Automat. Soft Comput.* **33**, 549–565 (2022). https://doi.org/10.32604/iasc.2022.024379

[33] Faragallah, O. S. *et al*. Efficient chaotic-Baker-map-based cancelable face recognition. *J. Ambient Intell. Humaniz. Comput.* **14**, 1837–1875 (2023). https://doi.org/10.1007/s12652-021-03398-0

[34] 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. *Comput. Mater. Contin.* **69**, 1571–1595 (2021). https://doi.org/10.32604/cmc.2021.016980

[35] Abd Al Rahim, M., El-Shafai, W., El-Rabaie, E. S. M., Zahran, O. & Abd El-Samie, F. E. Comb filter approach for cancelable face and fingerprints recognition. *Menoufia J. Electron. Eng. Res.* **28**, 89–94 (2019). https://doi.org/10.21608/mjeer.2019.76776

[36] 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). https://doi.org/10.1016/j.ijleo.2022.168773

[37] Ali, A. M. *et al*. Vision transformers in image restoration: A survey. *Sensors* **23**, 2385 (2023). https://doi.org/10.3390/s23052385