

Cancelable Multi-biometric Template Generation Based on Dual-Tree Complex Wavelet Transform

Ahmed M. Ayoup^{1,*}, Ashraf A. M. Khalaf¹, Fahad Alraddady², Fathi E. Abd El-Samie³,
Walid El-Shafai^{3,5} and Salwa M. Serag Eldin^{2,4}

¹Electrical Communications Engineering Department, Faculty of Engineering, Minia University, Minia, 61111, Egypt

²Department of Computer Engineering, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia

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

⁴Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University, Tanta, Egypt

⁵Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh, 11586, Saudi Arabia

*Corresponding Author: Ahmed M. Ayoup. Email: ayoup.2012@hotmail.com

Received: 15 October 2021; Accepted: 06 December 2021

Abstract: In this article, we introduce a new cancelable biometric template generation layout depending on selective encryption technology and Dual-Tree Complex Wavelet Transform (DT-CWT) fusion. The input face biometric is entered into the automatic face-segmentation (Viola-Jones) algorithm to detect the object in a short time. Viola-Jones algorithm can detect the left eye, right eye, nose, and mouth of the input biometric image. The encoder can choose the left or right eye to generate a cancelable biometric template. The selected eye image of size $M \times N$ is XORed with the created pseudo-random number (PRN) matrix $C_{M \times N}$ to provide an initial primary image. Arnold Cat Map (ACM) is used to scramble the PRN matrix pixel by pixel for primary image encryption keeping the pixel values themselves unchanged. Finally, the ACM scrambled eye images are encrypted using Advanced Encryption Standard (AES) algorithm for database storage. Moreover, the PRN and Initial Key (IK) of the AES algorithm for the same person are used for the biometric model authentication process for database storage. The IK is generated from the right finger and right eye fusion using DT-CWT technique. To avoid injury of a single eye, both right-eye and left-eye models are developed.

Keywords: Viola-Jones face detection; machine learning; AES; ACM; DT-CWT; statistical security analysis

1 Introduction

Biometric identification methods based on human physiological characteristics such as face, iris, and fingerprints have become common practice. A cancelable biometric system is required to manage biometric data through irreversible transformations to obtain biometric templates to maintain privacy. The



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

protection of huge biometric database templates from unauthorized access can be achieved using selective encryption, chaos encryption, and strong encryption techniques like AES [1–4].

Selective encryption is the process of encrypting selected portions of the original biometric identifier in order to shorten the time it takes to complete the encryption process and improve the security of the encrypted biometric data with low cost. Any biometric system has many advantages and at the same time faces many problems, such as sensor data tampering. Moreover, biometric data may be contaminated due to imperfect data collection conditions, which may lead to false rejection. Multimodal biometric systems can reduce the Failure-To-Capture and Enroll (FTC/FTE) and provide greater resistance to plagiarism, since it is difficult to tamper with multiple biometric sources at the same time. The performance of multi-modal biometric systems can be enhanced by extracting fingerprint and iris features and merging them [1–4].

Cancelable biometrics systems use irreversible transformations in one way to create transformed templates from the biometric data. Cancelable biometric systems provide resistance to template rebuilding, even if the spoofing process has access to both templates and transform parameters [5]. This paper is divided into five sections as follows. In the first section, we provide an introduction to cancelable biometrics concept, biometric system security and confidentiality issues, and the main contributions of the proposed cancelable biometric system. In the second section, we describe the related work of various researchers in this field. In the third section, we introduce the main contributions of the proposed cancelable biometric system. In the fourth section, we offer the simulation results. Finally, in the last section, we give the conclusions.

1.1 Cancelable Biometrics Concept

Cancelable biometrics, also known as feature transformation, was developed to meet the main requirements of biometric template security. Template protection layouts are prepared to follow certain criteria such as non-invertibility, diversity, reusability, and high performance [6] (See Fig. 1).

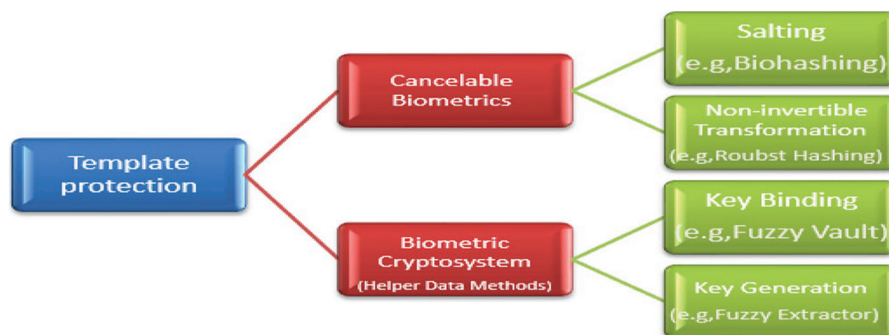


Figure 1: Schematic diagram of various branches of template protection schemes [6]

Cancelable biometrics fall into two categories: salting and non-invertible transformations. Different researchers suggested different methods for cancelable biometrics. In biometric processing, explicit customer information, such as password, is first combined with biometric information to produce the distorted version of the biometric template. In fact, the strategy can be changed by changing the password if the biometric salting is subject to additional external data (see Fig. 2) [6].

In non-invertible transforms, biometric data is transformed by applying a one-way transform. The transformation options can be changed to provide updatable templates. The advantage of the non-invertible conversion is that the fraudster cannot recover an authenticated biometric template, even if the conversion is compromised (see Fig. 3).

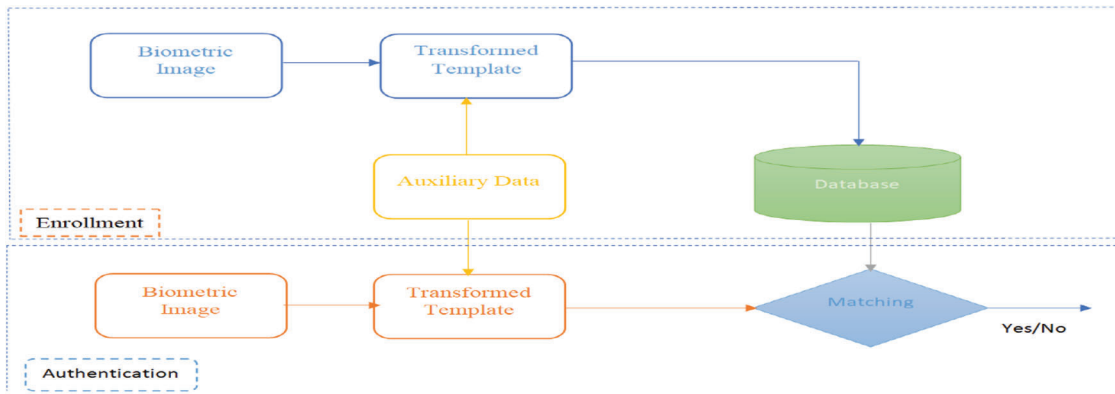


Figure 2: Layout of biometric salting technique [6]

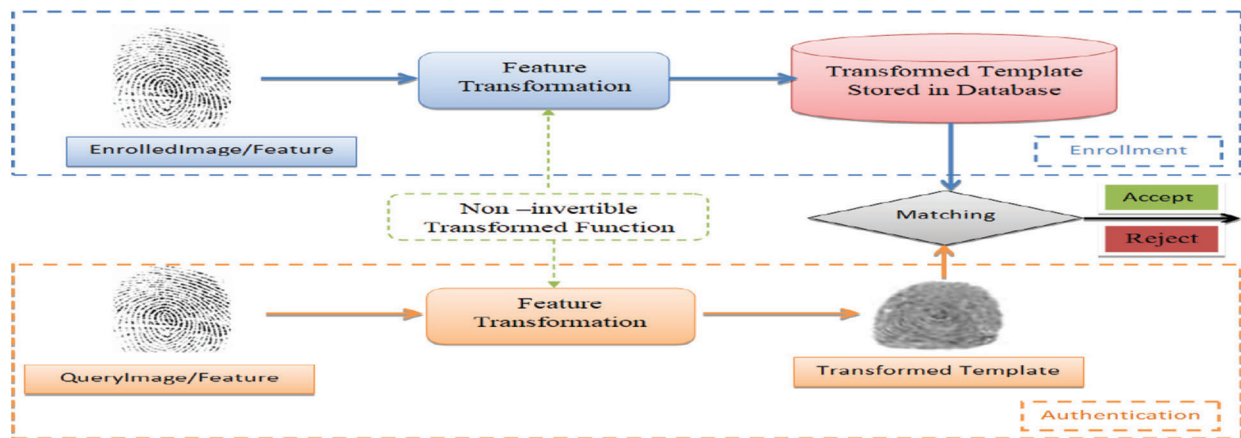


Figure 3: Layout of the non-invertible transformation [6]

1.2 Security and Data Protection Problems with Biometric Systems

Biometrics is a form of secure authentication. Impostors have come up with new ways to hack biometric systems. There are eight different attacks on biometric systems [7,8]. Fig. 4 shows different hacking scenarios at different points on the biometric and verification system.

2 Related Work

Mhaske et al. [9] presented a review about the idea of multi-biometric security. A multi-modal biometric framework that integrates fingerprint and handprint distinctive features has been presented to overcome some of the limitations of single-mode biometrics. Preprocessing is the heart of the image step to generate cancelable templates. The modified Gabor filter is used to freely separate unique tag and handprint to provide more accuracy when compared to the traditional Gabor filter.

Ahlawat Mamta et al. [10] proposed a multi-modal biometric framework dependent on the ear, eye, and face shading. It demonstrated its proficiency over the current biometric methods. Fouad et al. [11] proposed a secure iris pattern recognition framework using a combination of cryptography and watermarking techniques. The iris image is protected with a key and is embedded in the cover image using Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT) methods. The embedding area is encoded with a certain key. Two keys (iris and embedded keys) are important in the iris extraction process.

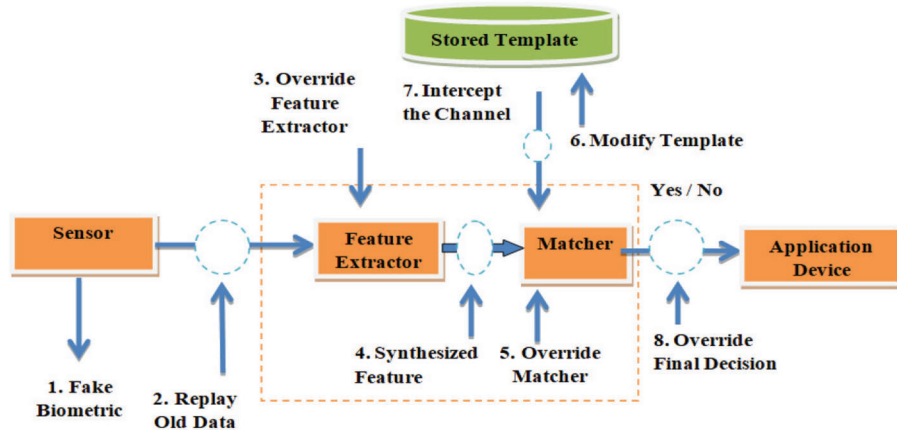


Figure 4: Different attacks at different points of a biometric system [7,8]

Paunwala et al. [12] inserted a finger and an iris into an isolated cover image in blocks. Each square gives a 2D DCT and is organized into blocks with or without edges. The biometrics features are implanted in the low-frequency region of the 8×8 DCT block and the edges are removed.

Ayoub et al. [13] proposed an Efficient Selective Image Encryption (ESIE) technology. This technology depends on the integration of pseudo-random number sequences, Arnold’s cat map and AES encryption. The primary image maintains randomness and low correlation. Arnold’s cat map speeds up the operation and the AES allows reliability. The ESIE technology aims at reducing the execution time of the encoding process and increasing the reliability of the encoded images. The achieved execution time is 7.44 s for 64 combinations of biometric data selected from the input face.

Namita Chandra et al. [14] described the security and authentication of an online application system using a One-Time Password (OTP) to scan fingerprints in daily life, as in banking applications. The security of this type of online applications is very important. Current online applications that provide security, such as security cards and passwords for user authentication, do not provide the required security level for users. Raid An et al. [15] introduced a specific encryption method depending on the integration of Arnold’s cat map, image masking, and the International Data Encryption Algorithm (IDEA).

3 Proposed Cancelable Biometric Scheme Using Selective Encryption Technique

A new cancelable biometric scheme based on selective encryption is presented here. The proposed scheme follows six steps as shown in Fig. 5. First, the image is applied to the Viola-Jones algorithm, which identifies and locates the human face regardless of the size of the mouth, nose, left and right eyes.

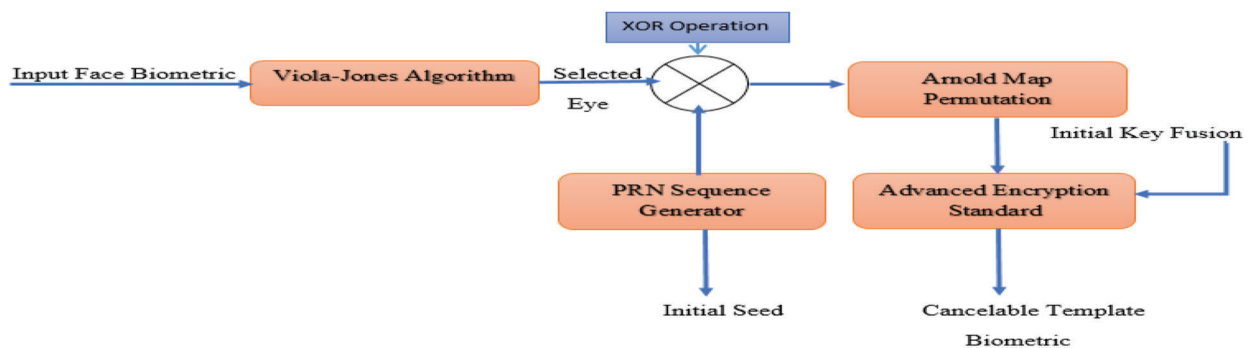


Figure 5: Flowchart of the proposed cancelable biometric recognition scheme

The encoder can select any part of the face to encode and store in the generated template. In this article, we select either the left eye or the right eye to work on. This process reduces the correlation between the biometric portion of the input face and the primary biometric image. It is also safe as it changes the histogram of the entered biometric data. The coded part of the selected face is processed with Arnold's cat map technique. There is only one defect in the Arnold permutation. Its period is fixed. So, the histogram of the graph of the encoded biometric information is the same as that of the input biometric image. The values of the pixels themselves do not change. Therefore, we used PRN coding for the original biometric data before the Arnold transform. Finally, the permuted image is processed with the AES encryption algorithm.

The IK of the AES is generated using the DT-CWT algorithm. The right finger and right eye of the input face are fused to obtain IK, which is stored with the PRN and the encoded eyes in the database. Fig. 6 shows a layout of the proposed key generation technique for the authentication scheme.

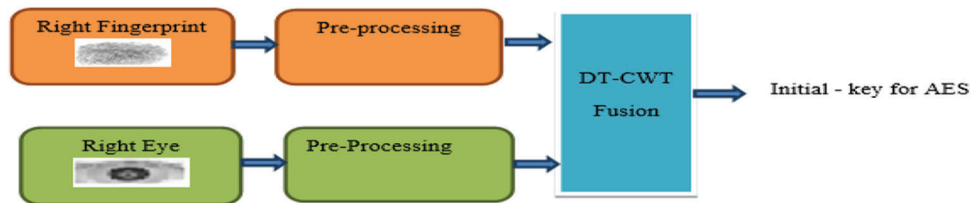


Figure 6: Layout of the proposed key generation technique

Step 1: Viola-Jones Face Detection Algorithm

One of the first object detection frameworks was Viola-Jones, which was used to provide a competitive real-time object detection rate. It was proposed in 2001 by Paul Viola and Michael Jones [16–18]. The Viola-Jones algorithm is used for automatically recognizing faces in an image. It is used to identify and locate a human face regardless of its size, situation and environment. It was reported that computational speed is increased through the use of Haar functions and machine learning AdaBoost, and a face in a frame can be detected in milliseconds [19]. This system can be trained to detect many different types of objects. First, the values of all black pixels of the image in grayscale are accumulated, and then they are subtracted from the total number of white squares. Finally, the result is compared with a given threshold. As part of this work, the built-in MATLAB functions are used to detect parts of the body, nose, mouth and eyes, etc.

Viola-Jones face detection algorithm depends on a computer vision system toolbar. The detection method includes four key concepts:

- 1) Simple rectangular Haar function.
- 2) Comprehensive visualization for fast feature detection.
- 3) AdaBoost machine learning method.
- 4) Cascading classifier for efficiently combining multiple features.

Step 2: Pseudo-Random Number Matrix Generation

The PRN is generated by a Linear Feedback Shift Register (LFSR). The PRN generator has other application areas, where it is desirable to obtain unexpected correlations [13]. This algorithm has an unexpected output, which is sufficient to satisfy the randomness requirement. Generators are created using different methods. They have several applications such as major telecom operators, data encryption and secure banking communication channels. etc. Moreover, the original seed remains secret.

The maximum length of the linear feedback shift register constitutes the sequence M . It iterates over all possible states $(2^n - 1)$ in the shift register. The sequence generated by this method is random, and the sequence period is $(2^n - 1)$, where n is the number of shift registers used in the circuit, or the polynomial arrangement of the generator $P(x)$. The total number of internal random states generated by the LFSR is $(2^n - 1)$, and it depends on the degree of the polynomial generator $P(x)$ (See Fig. 7).

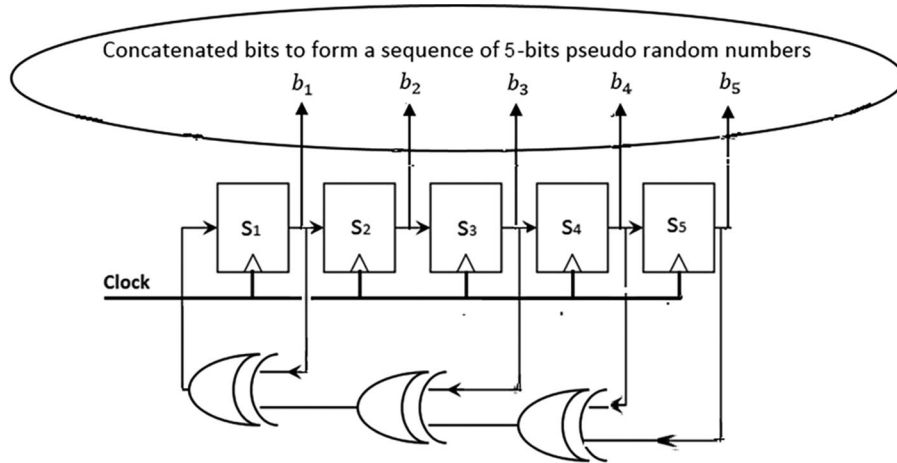


Figure 7: Layout of the designed $n = 5$ stages LFSR for generator polynomial [13]

The clock shift state register i is a vector of finite length b_i ; where the seed of the concatenated bits must form a sequence of 5-bit pseudo-random numbers $(b_1, b_2, b_3, b_4, b_5)$

$$b_i = (b_i(1), b_i(2), \dots, b_i(n-1), b_i(n)) \quad (1)$$

The output c_i at the pulse of the clock i is a series of these states. The output is inserted in C_M . The generated pseudo-random matrix has a size of $M \times M$, the same as the size of the input biometric image to perform XOR operation.

$$c_i = (b_i(1) \& b_i(2) \& \dots \& b_i(n-1) \& b_i(n)) \quad (2)$$

A series of pseudo-random numbers c_i of volume M is introduced as follows;

$$C_M = (c_1, c_2, c_3, \dots, c_M) \quad (3)$$

For an input $M \times M$ image, an $M \times M$ matrix of pseudo-random numbers $C_{M \times M}$ is generated. Considering a sequence of pseudo-random numbers of length C_M , the rows of the cryptographic matrix $C_{M \times M}$ are sequentially shifted versions of the C_M sequence, where;

$$C_{M \times M}(i) = \text{circleshiftby}((i-1)*L) \text{ of } C_M \quad (4)$$

where i is the row index of the $C_{M \times M}$ matrix, and L is the number of shifts. To generate a PRN sequence of length 31 an $n = 5$ rounds LFSR is used. For a maximum-length sequence, the LFSR satisfies the generator polynomial $P(x)$ from Eq. (5). We generate $n = 2^5 - 1 = 31$ internal random states. Fig. 8 shows a block diagram of an LFSR with $n = 5$ stages. The line C_{32} of length 32 consists of 31 random states plus the first state.

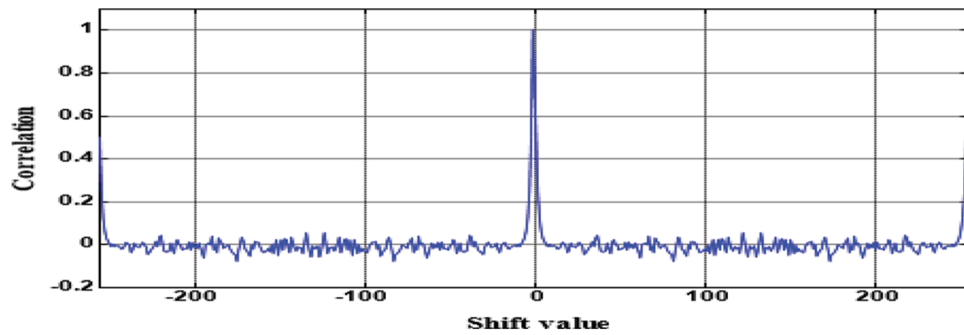


Figure 8: Auto-correlation among the PRN sequence [13]

$$P(x) = x^5 + x^3 + x + 1 \quad (5)$$

The main advantage of a PRN sequence is that it has low autocorrelation properties, which improves the encoding process (See Fig. 8).

Step 3: Encryption of Selected Eye Image using PRN Sequences

An $M \times M$ selected eye biometric is XORed with the generated $C_M \times M$ matrix to obtain an encrypted primary image. This operation removes the correlation between the selected eye and encrypted primary image.

Step 4: Arnold Image Transformation

Arnold cat map is a chaos map named after Vladimir Arnold. This is a combining and cropping operation to reshape a digital image matrix, known as transform. The ACM is a coding technique [20] that can be applied on an image that is safer and more efficient. The image is created by randomly transforming the original one. Unfortunately, the ACM has two major drawbacks:

Sometimes, the original image reverts to itself when repeating the map, and the histogram of the encoded image and the original image are the same. The values of the pixels themselves do not change [21,22]. This is the reason to apply the PRN coding to a simple image before the Arnold transform.

Step 5: Dual-Tree Complex Wavelet Transform (DT-CWT)

Kingsbury [23] introduced a new DWT implementation called DT-CWT, suitable for many signal and image processing applications. The DWT can provide an ideal reconstruction using critical sampling, however, DT-CWT eliminates artifacts in the image fusion. The Stationary Wavelet Transform (SWT) was the first attempt to integrate variance changes in the DWT by removing all subsampling.

Although image synthesis algorithms using SWT tend to give more intuitive composite results than algorithms using DWT, SWT is more computationally expensive due to its redundancy. In addition, no additional orientation is achieved compared to DWT [24–27]. The idea behind the dual-tree approach is that it uses two real DWTs. The first DWT provides the real part of the transformation and the second one provides the imaginary part. The analysis and synthesis filter banks used to implement DT-CWT and its inversion are shown in Figs. 9 and 10.

Two real wavelet transforms are implemented using two different filters. The two filters are designed together for an almost analytical overall transformation. Let $h_0(n)$ and $h_1(n)$ represent a low / high pass filter pair for the upper filter bank, and $g_0(n)$ and $g_1(n)$ represent a low / high pass filter pair for the lower filter bank. The two wavelets are denoted by $\psi_h(t)$ and $\psi_g(t)$ [24,25]:

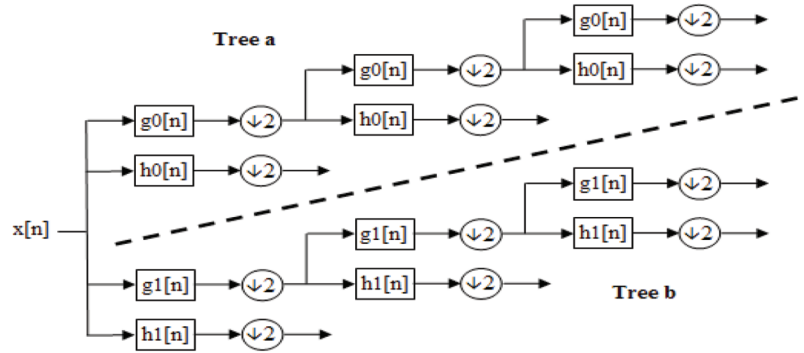


Figure 9: Analytical filter bank for the DT-CWT [24–27]

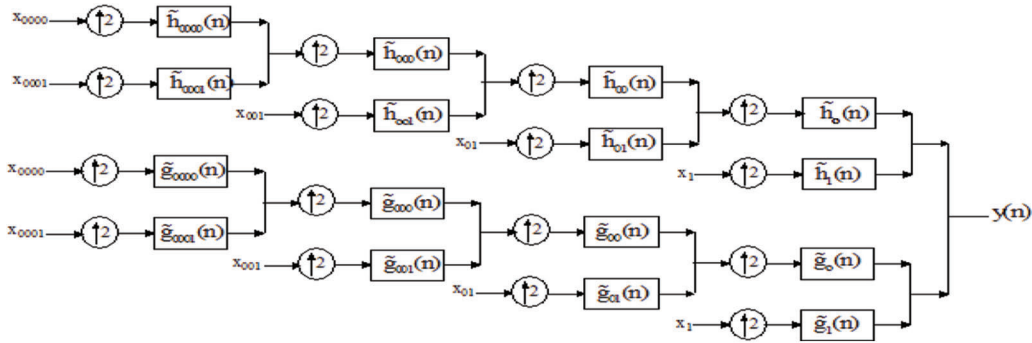


Figure 10: Synthesis filter bank for the DT-CWT [24–27]

F_h and F_g represent two real DWTs, and the composite WT tree can be represented by a rectangular matrix:

$$F = \begin{bmatrix} F_h \\ F_g \end{bmatrix} \quad (6)$$

Let $w_h = F_h x$ and $w_g = F_g x$ represent the real and imaginary parts of the DT-CWT, when the x vector is a real signal. The complex coefficient is set. The inverse is given by: $w_h + jw_g$. The inverse of F is given by [6]:

$$F^{-1} = \frac{1}{2} \begin{bmatrix} F_h^{-1} & F_g^{-1} \end{bmatrix} \quad (7)$$

We can verify

$$F^{-1} \cdot F = \frac{1}{2} \begin{bmatrix} F_h^{-1} & F_g^{-1} \end{bmatrix} \cdot \begin{bmatrix} F_h \\ F_g \end{bmatrix} = \frac{1}{2} [I + I] = I \quad (8)$$

It is possible to halve the coefficient between forward and inverse transformations to obtain

$$F := \frac{1}{\sqrt{2}} \begin{bmatrix} F_h \\ F_g \end{bmatrix}, F^{-1} := \frac{1}{\sqrt{2}} \begin{bmatrix} F_h^{-1} & F_g^{-1} \end{bmatrix}. \quad (9)$$

The DT-CWT introduces a more computationally efficient calculation method. In addition, the DT-CWT also provides much better directional selectivity, when filtering of multidimensional signals. At each level n , the 2D DT-CWT creates one real low-pass image and six complex high-pass images, $i = 1, \dots, 6$ [24,27].

Step 5.1: DT-CWT Image Fusion

In this article, the right eye is converted using 2D DT-CWT. The merging rule is utilized to combine the approximation coefficients at the highest decomposition level. The second rule is used to mix the details at each decomposition level. As a result, the inverse transformation gives the final merged result (See Fig. 11).

Considering $y_{i_1,0}^{(N)}$ and $y_{i_2,0}^{(N)}$, the sub-ranges of the approximation coefficients of the images, at the highest decomposition level N are merged as follows [24,27]:

$$y_{f,0}^{(N)} = \frac{y_{i_1,0}^{(N)} + y_{i_2,0}^{(N)}}{2} \quad (10)$$

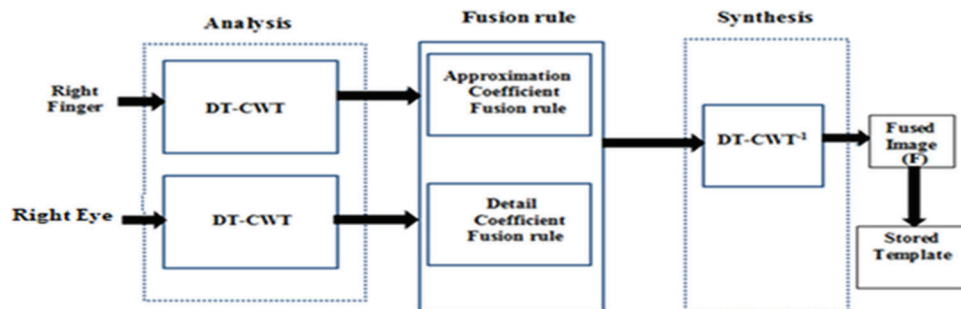


Figure 11: DT-CWT fusion [24–27]

In contrast, the details correspond to prominent features such as edges, lines, or areas. Thus, mixing rules for the detail ratios at each decomposition level can be formulated in relation to the human visual system in order to preserve the characteristics of the source images. One of the many merging rules proposed in the literature is the popular fidelity merging rule [24,27]:

Step 6: Advanced Encryption Standard (AES)

The AES is a repeating cipher, not a Feistel cipher. The AES encryption can be divided into four phases: the SubBytes phase, the ShiftRows phase, the MixColumns phase, and the AddRoundKey phase. The same sub-operators are used in different combinations. The loops are repeated in a specific number in each round of the AES. The AES-128 utilizes ten main loop iterations, the AES-192 uses 11 rounds, and the AES-256 uses 14 round. We will utilize the 128-bit version of the AES [1].

The novelties of the proposed cancelable multi-biometric scheme compared to previous research are:

1. Proposal of a multi-model cancelable biometric technique that achieves a cost reduction of the enrollment process compared to the ESIE [13], which has a total runtime of 7.44 seconds. The total runtime of this paper of 3.88 s, making it more suitable for real-time applications.
2. The fingerprint features and the user eye features are the primary standards for key generation for the AES. The merged key is converted to hexadecimal (HEX key) to be added to the AES code.
3. The result of the proposed cancelable biometric scheme, such as entropy, correlation, etc., are more favorable in security tests. The rating metrics for the suggested cancelable biometric scheme in the presence of noise, ROC, and AROC are good in the presence of noise. This makes the proposed technology more suitable for real-time applications. Moreover, the proposed technology applies Viola-Jones, which is a faster face detection technology.

- The database search process is speeded up by generating the applicant key and matching it with the keys stored in the database to see if the person is authenticated or not, and in the case of the fake attempts, the authentication process fails.

4 Authentication System

The proposed authentication system technology addresses most of the threat models for the biometric authentication. First, the initial key created for the input operator is obtained through the right fingerprint and the right eye of the user with the DT-CWT. Then, the generated IK is matched to the stored IK in the database. If it matches the stored IK, the input operator is authenticated. For further authenticated, PRN codes are called from the database, and the proposed template is generated. Finally, the generated encoded template is matched with the stored templates. If it matches, the input face is genuine otherwise it is an imposter. Fig. 12 shows a block diagram of the proposed scheme.

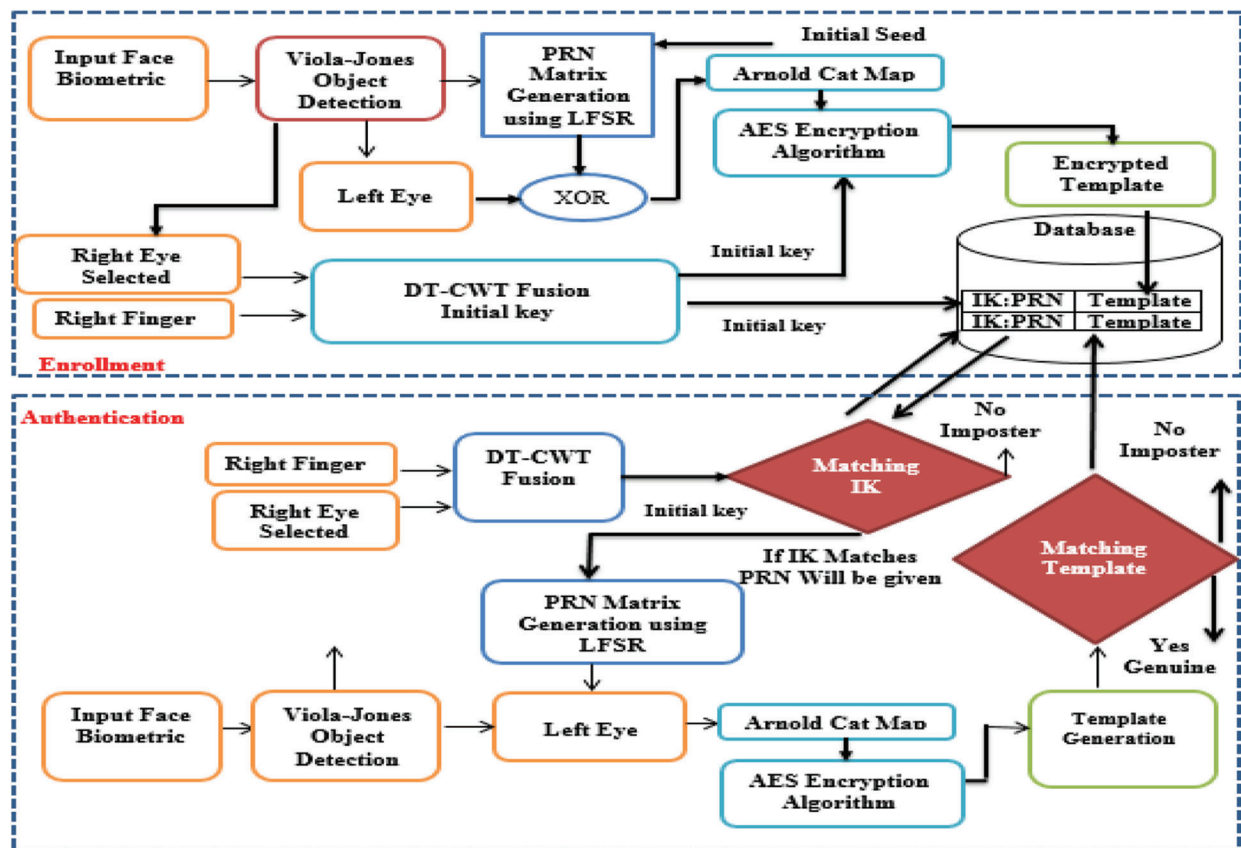


Figure 12: Layout of the proposed authentication scheme

5 Simulation Results and Comparisons

The proposed cancelable biometric recognition scheme is applicable to any image formats. We evaluate the performance of a cancelable biometric system by evaluating metrics such as genuine and imposter distributions and ROC curves. Results were obtained with MATLAB 2014a on Intel (R), core (TM) i74600U, 8 GB 2.10 GHz CPU running Windows 7. 256×256 . Lena image is used for unauthorized data and 128×128 Cancelable face templates are created as shown in Tab. 1.

Table 1: Output stages of cancelable face template generation



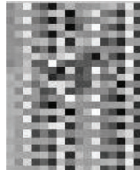
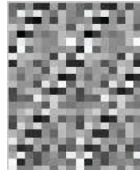
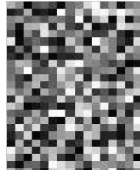



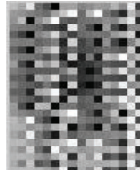
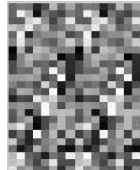
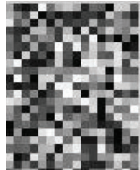


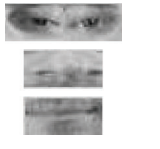
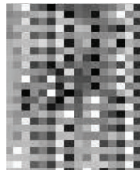
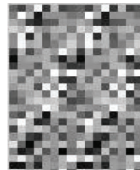
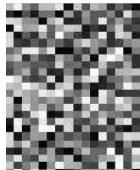



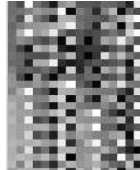
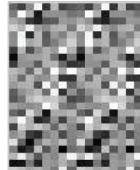
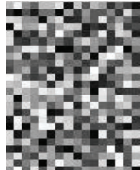


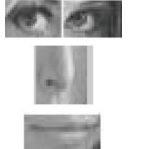
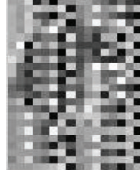
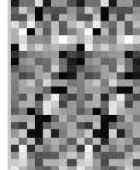
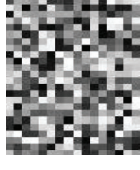

Faces [28]	Auto segmentation	Right eye encrypted PRN	Arnold permutation	AES encryption	Initial key = iris sprint
 Authorized Data					
 Authorized Data					
 Authorized Data					
 Authorized Data					
 Unauthorized Data					

Table 2: Assessment of the suggested cancelable biometric scheme for 256×256 Lena.jpg unauthorized data

Metrics [29]	Proposed cancelable biometric scheme	
	Right eye	Left eye
Encryption Time (s)	3.80	3.85
Entropy	7.4235	7.4826
Correlation among an original biometric and encrypted template	0.0649	0.0278
ID	0.9036	0.9505
NCPR	100	100
UACI	0	0
MDMF	0.9240	0.7836

Table 3: Assessment of the proposed cancelable biometric recognition scheme for 128×128 cancelable face template authorized data in Fig. 13a

Metrics [29]	Proposed cancelable recognition scheme	
	Right eye	Left eye
Encryption Time (s)	3.80	3.85
Entropy	7.4594	7.4423
Correlation among an original biometric and encrypted template	0.0190	0.0013
ID	0.9661	0.9714
NCPR	100	99.6246
UACI	0	27.7787
MDMF	0.9240	0.9240

The proposed reversible biometric test includes real and false distributions and ROC curve at different noise levels. The ROC curve refers to the relationship between true positive rate (TPR) and false positive rate (FPR) indicators of systematic assessment. The FRR measures the probability of falsely rejecting a face as a fake version (intra-classes), and FPR measures the probability of falsely accepting a fraudulent face pattern as a true face model (between classes). Fig. 14 shows a uniform bandwidth. This is a desirable property for a high degree of security in evaluating the numerical classification of proposed cancelable biometric scheme. Fig. 15 shows the performance curves for optimal separation. If the two curves do not intersect at all, this means that the system is perfectly distinguishing. We can distinguish between positive and negative classes. Fig. 16 shows the high security of the proposed face encryption scheme. Tabs. 2 and 3 reveal the assessment of the proposed cancelable biometric recognition scheme for unauthorized and authorized cancelable face templates. Tabs. 4 and 5 show the effect of noise on the proposed scheme in addition to a comparison study.

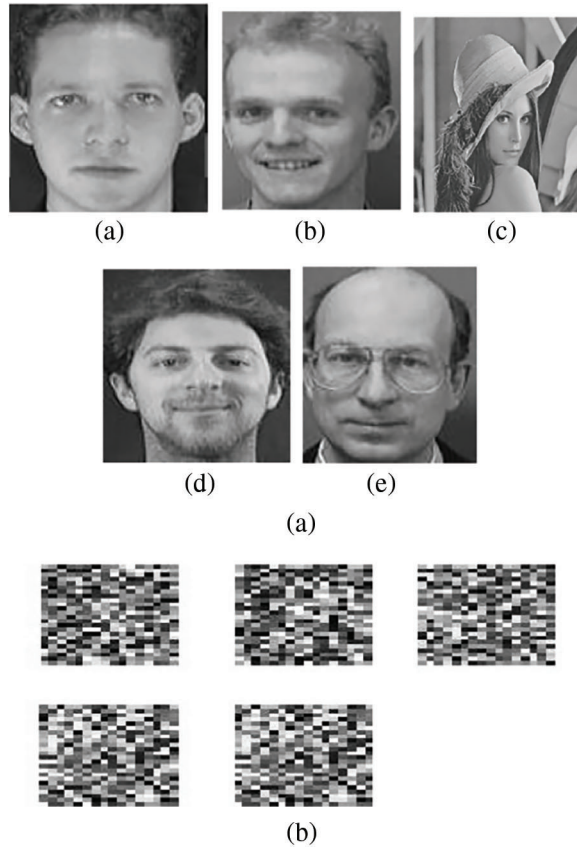


Figure 13: Encrypted templates created with the suggested scheme (a) Authenticated faces [28] (b) Output encrypted face templates

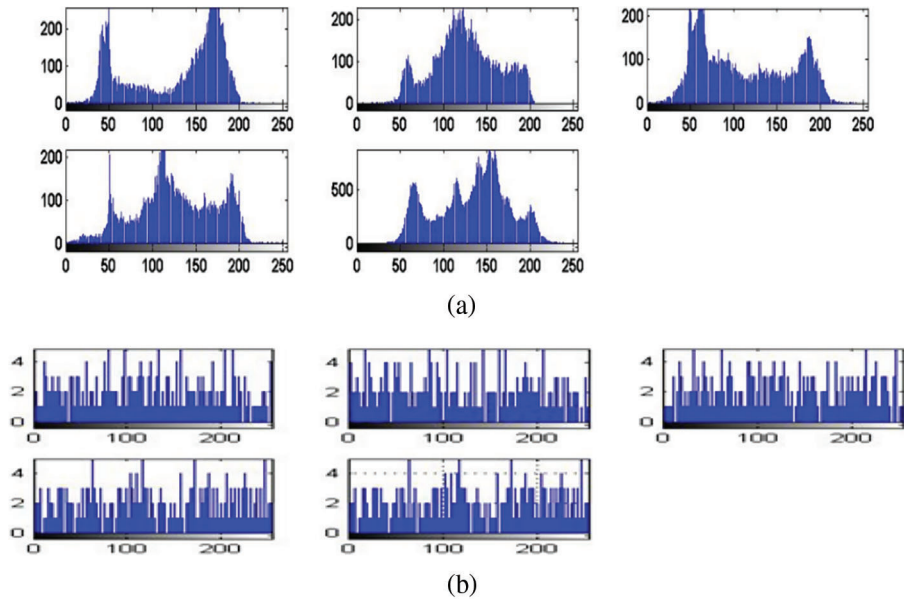


Figure 14: Histograms of (a) Original faces and (b) Histogram of templates created with the suggested scheme

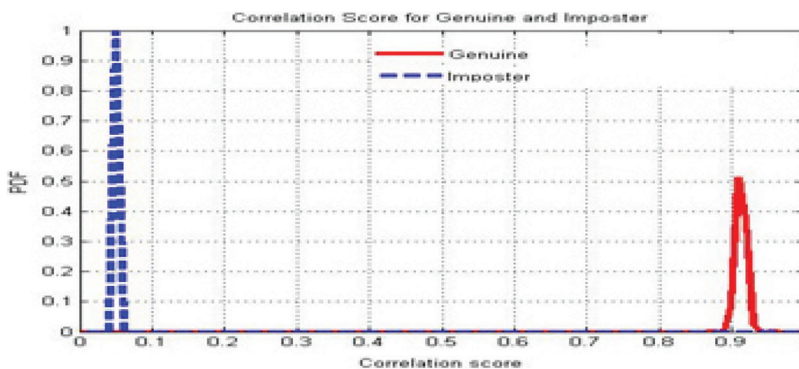


Figure 15: Genuine and imposter distributions using the proposed cancelable biometric recognition scheme

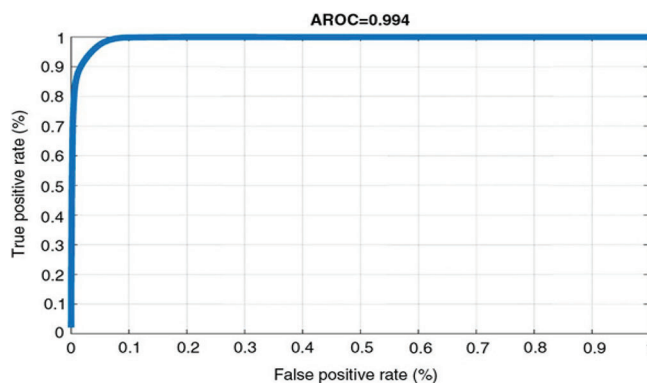


Figure 16: Genuine and imposter ROC curves using the proposed cancelable biometric recognition scheme

Table 4: Evaluation the proposed cancelable biometric recognition scheme in the presence of noise

Noise variance	EER	AROC
0.01	0.0016	0,9945
0.02	0.0019	0,9940
0.03	0.0018	0.9917
0.04	0.0098	0.9908
0.05	0.0098	0.9857

Table 5: Comparison between the suggested cancelable biometric recognition scheme using (DT-CWT) and that of Soliman et al. [29]

Noise variance	Soliman et al. [29]		Suggested algorithm	
	EER	AROC	EER	AROC
0.01	0.0098	0,9475	0.0016	0,9945
0.02	0.0098	0,9057	0.0019	0,9940
0.03	0.0098	0.8757	0.0018	0.9917
0.04	0.0098	0.8364	0.0098	0.9908
0.05	0.0098	0.8057	0.0098	0.9857

6 Conclusion

This article explored current trends and challenges in the area of cancelable biometrics as a means of authentication. The study attempts to create a compact overall framework and evaluate the proposed multi-modal cryptosystem on large-scale datasets. The selective encryption method reduces the time spent on the registration process and increases the reliability of the encrypted template generation. In addition, the proposed plan gives a shorter implementation time compared to those of the previous work. Simulation results show that the proposed scheme provides higher entropy, lower correlation with the original biometrics, and less encryption times than that obtained with the full biometric image encryption using AES. Authentication results obtained by cancelable biometric schemes provide low EERs and high AROCs in the presence of noise.

Acknowledgement: The authors thanks the researchers of Taif University for their support. They support project number (TURSP-2020/214), Taif University, Taif, Saudi Arabia.

Funding Statement: This research was supported by Taif University Researchers Supporting Project Number (TURSP-2020/214), Taif University, Taif, Saudi Arabia (www.tu.edu.sa).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] W. Stallings, *Cryptography and Network Security Principles and Practice*. USA, Prentice Hall 5th, 2011.
- [2] E. Lupu and P. Pop, "Multimodal biometric systems overview," *ACTA Technica Napocensis*, vol. 49, no. 3, pp. 39–44, 2008.
- [3] C. Rathageb and A. Uhl, "A survey on biometric cryptosystem and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, pp. 1–25, 2011.
- [4] A. Bastanfard, O. Bastanfard, H. Takahashi and M. Nakajima, "Toward anthropometrics simulation of face rejuvenation and skin cosmetic," *Computer Animation and Virtual Worlds*, vol. 15, no. 3–4, pp. 347–352, 2004.
- [5] P. Lacharme and A. Plateaux, "PIN-based cancelable biometrics," *International Journal of Automated Identification Technology (IJAIT)*, vol. 3, no. 2, pp. 75–79, 2011.
- [6] R. Bolle, J. Connel and N. Ratha, "Biometrics perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.
- [7] N. Ratha, J. Connel and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM System Journal*, vol. 40, no. 3, pp. 614–634, 2001.
- [8] K. Kamaldeep, "A review of various attack on biometrics system and their known solutions," *International Journal of Computer Technology and Application*, vol. 2, no. 6, pp. 1980–1992, 2011.
- [9] V. Mhaske and A. Patankar, "Multimodal biometrics by integrating fingerprint and palm print for security," in *Proc. Conf. on Computational Intelligence and Computing Research (ICCIC)*, Enathi, India, pp. 1–5, 2013.
- [10] M. Ahlawat, A. Yadav and C. Kant, "A multimodal approach to increase the security of biometric system," *International Journal of Computer Science & Communication*, vol. 6, no. 2, pp. 102–115, 2015.
- [11] M. Fouad, A. ElSaddik, Z. Jiying and E. Petriu, "Combining cryptography and watermarking to secure revocable iris templates," in *Proc. IEEE Int. Instrumentation and Measurement Technology Conf.*, Hangzhou, china, pp. 1–4, 2011.
- [12] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Machine Vision and Applications*, vol. 25, no. 1, pp. 263–275, 2014.
- [13] A. Ayoup, A. Hussein and M. Attia, "Efficient selective image encryption," *Multimedia Tools Application*, vol. 7, no. 3, pp. 17171–17186, 2016.
- [14] N. Chandra, A. Taksal, D. Shinde and A. Lomte, "Sensitive data protection using bio-metrics," *International Journal of Advanced Research in Computer Science and Software*, vol. 4, no. 3, pp. 1–14, 2014.

- [15] A. Riad, A. Hussein, H. Kasem and A. El-Azm, "A new efficient image encryption technique based on Arnold and idea algorithms," in *Proc. Int. Conf. on Image and Information Processing (ICIIP 2012)*, Singapore, pp. 46–53, 2012.
- [16] A. Lanitis, C. Taylor and T. Cootes, "An automatic face identification system using flexible appearance models," *Image and Vision Computing*, vol. 13, no. 5, pp. 393–401, 1995.
- [17] H. Rein-Lien, M. Abdel-Mottaleb and A. Jain, "Face detection in color images," *IEEE Transactionson Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 696–706, 2002.
- [18] P. Math, "Surveillance system using internet of things," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 4, no. 3, pp. 120–123, 2016.
- [19] P. Wilson and J. Fernandez, "Facial feature detection using Haar classifiers," *Journal of Computing Sciences*, vol. 21, no. 4, pp. 127–133, 2006.
- [20] L. Wu, J. Zhang, W. Deng and D. He, "Arnold transformation algorithm and anti-arnold transformation Algorithm," in *Proc. Int. Conf. on Information Science and Engineering (ICISE)*, Nanjing, China, pp. 1164–1167, 2009.
- [21] Y. Wang and T. Li, "Study on image encryption algorithm based on Arnold transformation and chaotic system," in *Proc. IEEE Int. Conf. on Intelligent System Design and Engineering Application (ISDEA)*, Changsha, China, pp. 449–451, 2010.
- [22] S. Lian, *Multimedia Content Encryption Techniques and Applications*. USA, CRC Press, Taylor & Francis Group, 2009.
- [23] N. Kingsbury, "The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters," *IEEE Digital Signal Processing*, vol. 3, no. 2, pp. 1022–1131, 1998.
- [24] S. Necessian, K. Panetta and S. Agaian, "Image fusion using the parameterized logarithmic tree complex wavelet transform," in *Proc. IEEE Int. Conf. on Technologies for Homeland Security (HST)*, Woburn, MA, USA, pp. 294–302, 2010.
- [25] I. Selesnick, R. Baraniuk and N. Kingsbury, "The dual tree complex wavelet transform," *IEEE Signal Processing Magazine*, vol. 22, no. 6, pp. 123–151, 2005.
- [26] S. Ioannidou and V. Karathanassi, "Investigation of the dual-tree complex and shift-invariant discrete wavelet transforms on quick bird image fusion," *IEEE Geosciences and Remote Sensing Letters*, vol. 4, no. 1, pp. 166–170, 2007.
- [27] ORL Database, 2021. [Online]. Available: <https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html>. last access on 1-06-2021.
- [28] H. Ahmed, H. Kalash and O. Allah, "An efficient chaos-based feedbackstream cipher (ECBFSC) for image encryption and decryption," *Informatica*, vol. 31, no. 1, pp. 1–29, 2007.
- [29] R. F. Soliman, G. M. El Banby, A. D. Algarni, M. Elsheikh, N. F. Soliman *et al.*, "Double random phase encoding for cancelable face and iris recognition," *Applied Optics*, vol. 57, no. 35, pp. 10305–10316, 2018.