Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.024379
Article

Tech Science Press

Selective Cancellable Multi-Biometric Template Generation Scheme Based on Multi-Exposure Feature Fusion

Ahmed M. Ayoup[1,*], Ashraf A. M. Khalaf[1], Fahad Alraddady[2], Fathi E. Abd El-Samie[3], Walid El-Safai[3,5] and Salwa M. Serag Eldin[2,4]

[1]Electrical Communications Engineering Department, Faculty of Engineering, Minia University, Minia, 61111, Egypt
[2]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, 32952, Egypt
[4]Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University, Tanta, Egypt
[5]Security 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: 16 November 2021

Abstract: This article introduces a new cancellable multi-biometric system based on the combination of a selective encryption method and a deep-learning-based fusion technology. The biometric face image is treated with an automatic face segmentation algorithm (Viola-Jones), and the image of the selected eye is XORed with a PRNG (Pseudo Random Number Generator) matrix. The output array is used to create a primary biometric template. This process changes the histogram of the selected eye image. Arnold's Cat Map is used to superimpose the PRN pixels only on the pixels of the primary image. Arnold's cat map deformed eyes are encrypted using the Advanced Encryption Standard (AES) to encrypt the biometric data stored in the database. In addition, the AES master key is used for the same person in the identity verification process to verify the biometric identity. It is created from the fingers of the right hand, and the right eye is integrated into this process using deep learning technology. The deep learning fusion process can prevent attacks on the biometric system as a whole. In order to avoid damage to the eye or fingerprint images, the design considers the other eye and fingerprint images.

Keywords: Viola-Jones Algorithm; PRNG; AES; Arnold's Cat Map; Deep Learning Fusion

1 Introduction

Biometric systems automatically recognize individuals based on unique characteristics or types of characteristics they possess. The development of biometric systems is based on fingerprints, facial features, voice, hand geometry, hand-writing, and retina. The biometric template database is protected to prevent unauthorized access. It is possible to realize secure dynamic transmission of biometric templates through strong encryption methods such as the Advanced Encryption Standard (AES) [1].

A long time is taken to encrypt all biometric data to speed up the encryption process, increase the strength of the encrypted templates, and achieve high security through partial or selective encryption of some parts of the original biometric image. As a result, the biometric acquisition device is not safe and may suffer a malfunction. Two types of error may exist and affect the False Acceptance Rate (FAR)and False Rejection Rate (FRR) of the system. When the device rejects an authorized personnel, the FRR is incremented, and when the device accepts an unauthorized personnel, the FAR is incremented.

A multi-modal biometric identification system aims to combine multiple physical features to reduce FRRandFAR. Multiple biometrics are mandatory in large international biometric databases to accommodate for newly developed security requirements other than uni-modal biometrics. A multi-biometric system recognizes people based on a single source of vital information [2]. These types of systems are often affected by several problems such as disturbed sensor data, lack of individuality, static representation, circumvention, and lack of comprehensiveness. Cancellable biometrics is one of the main trends for protecting biometric templates.

This article is split into five parts. In the first part, we introduce the concept of cancellable biometrics, in addition to biometric protection and privacy problems. In the second part, we introduce some associated research works in this field. The foremost contributions of the suggested approach are presented in the third part. The fourth part gives the simulation results, and finally, the fifth part presents the conclusion and future work.

Biometric structures are stable authentication structures. Unfortunately, fraudsters have devised new methods for passing on the integrity of biometric structures. The first difficulty with biometric authentication is that everyone with prosthetic wax hands can make fake hands. It is possible to take a picture of a certain person in front of a digital camera to pass the face verification tool. It is also possible to use a lens to pass the iris scanner, etc. There are eight applicable assaults on a biometric system. Fig. 1 shows the validation of various assaults on a unusual agents of the biometric device and indicates the applicable assaults on the biometric devices, and the applicable solutions.

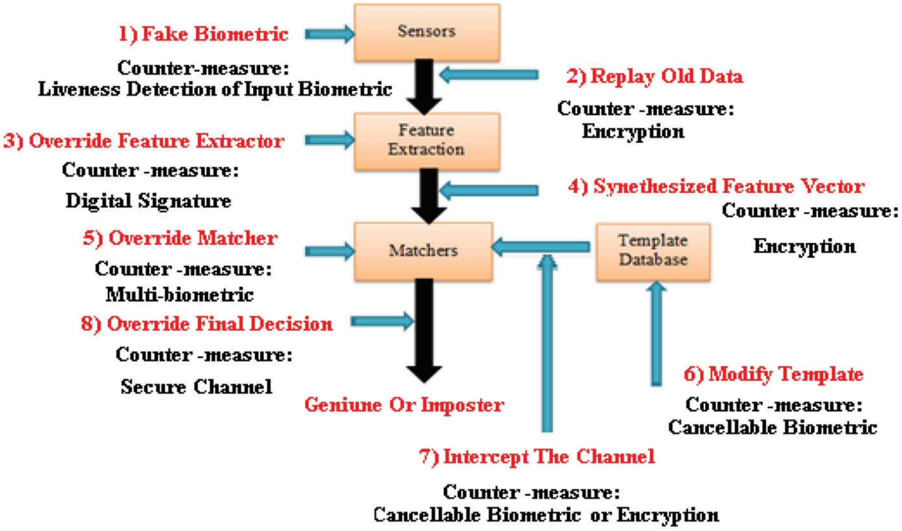


Figure 1: Verification of different biometric attacks [3]

This work presents a cancellable multi-biometric system. The novelty of system compared to previous research is summarized as:

1) The fingerprint and iris features are used as the initial key for the AES standard. In addition, the merged key is converted to hexadecimal (HEX key) format to be added to the AES code.
2) The evaluation metrics such as correlation, entropy, etc., are higher and more favorable in security tests.
3) The system performance in the existence of noise, ROC, and AROC are good. This makes the proposed technology more suitable for real-time applications.
4) The proposed technology depends on Viola-Jones algorithm, which is a faster face detection technology. It produces good detection results suitable for machine learning applications. Moreover, the proposed algorithm enrolment is 3.28 s compared to the algorithm in [4] with an enrollment time of 7.42 s. In addition, the proposed algorithm is better than the algorithm in [5] in EER and AROC.
5) The proposed algorithm speeds up the database search process by generating the applicant key and using the key stored in the database to find out if the person is authenticated or not, and in the case of unauthorized persons, the authentication rejects the person.

2 Related Work

Numerous efforts have been performed by different researchers in the field of biometric security. Neha Singh et al. [3] introduced the idea of biometric security. At the same time, the authors used biometrics to confirm and check individual authentication. This formatting can be distorted if any unauthorized person knows it.

Rupesh wagh et al. [4] presented a security framework using a proprietary coding technology to scramble biometric templates. Cryptography is used for information security, and it is used in the framework of biometrics. The focus on biometric security is the main concern in this paper. Multimodal biometrics depends on two methods of fingerprint and iris recognition. The features are taken from the biometric traits. These features are positioned away using an accentuation plane combination, and the cross-linked vector is blended using distinct security innovations. The collection was completed using the methods of salient feature separation [4].

Mamta Ahlawat et al. [5] suggested a multiple biometrics framework depending on eye and face colors and have presented effective over-current uni-biometric systems. The combination of multiple biometrics enhances the performance efficiency of the biometric system [5]. Shweta Malhotra et al. [6] offered a way to deal with upgrading issues of the imperceptible watermarking with cryptography. The biometric characteristics are changed using undetectable watermarks and cryptography. The encryption algorithm utilized is solid and appropriate for interactive media and text information. It is possible to use encryption methods like AES and Modified Advanced Encryption Standard (MAES) [6].

Vincenzo Conti et al. [7] presented an inventive multiple-trait identity framework depending on iris and fingerprints. Ahmed Ayoup et al. [8] presented an Efficient Selective Image Encryption (ESIE) method based on a combination of pseudo-random number sequences. Arnold's Cat Map and AES technology have been used. This method allows randomness and good correlation of pseudo-random number sequences, Arnold's cat map speed, and AES reliability. Therefore, the presented ESIE technology aims to decrease the execution time of the encryption process. The selective encryption techniques are based on image compression. Moreover, the total runtime for the presented method is 7.44 s for the selected 64 combinations of input face biometrics.

3 The Proposed Cancellable Multi-Biometric Algorithm

The proposed technology follows six steps. First, the input face image is captured from the face sensor and processed by the Viola-Jones automatic face detection algorithm. It determines the position of the human face regardless of the size of the mouth, nose, left, and right eyes. In this paper, we select the left or right eyes to create the templates to be stored. To avoid attacksin the transfer of data from the sensor, the selected eye is XORed with the unique seed value (PRNG) to generate the primary image [8]. This process reduces the correlation between the original eye pixels and encrypted eye pixels. Moreover, it changes the histogram of the primary image and provides a spread over the entire band. The primary image is processed with Arnold's cat map. This primary selected region is encrypted with Arnold's cat map. It achieves more security. There is a drawback for the Arnold's cat map. It needs several rounds to achieve security.

To scramble the input image, the AES encryption algorithm is applied to override the final decision. The proposed initial key generation technology is based on the person's right iris and finger feature fusion using deep learning to obtain the initial key of the AES, which is stored with the cancellable eye template in the database as showns in Figs. 2 and 3.

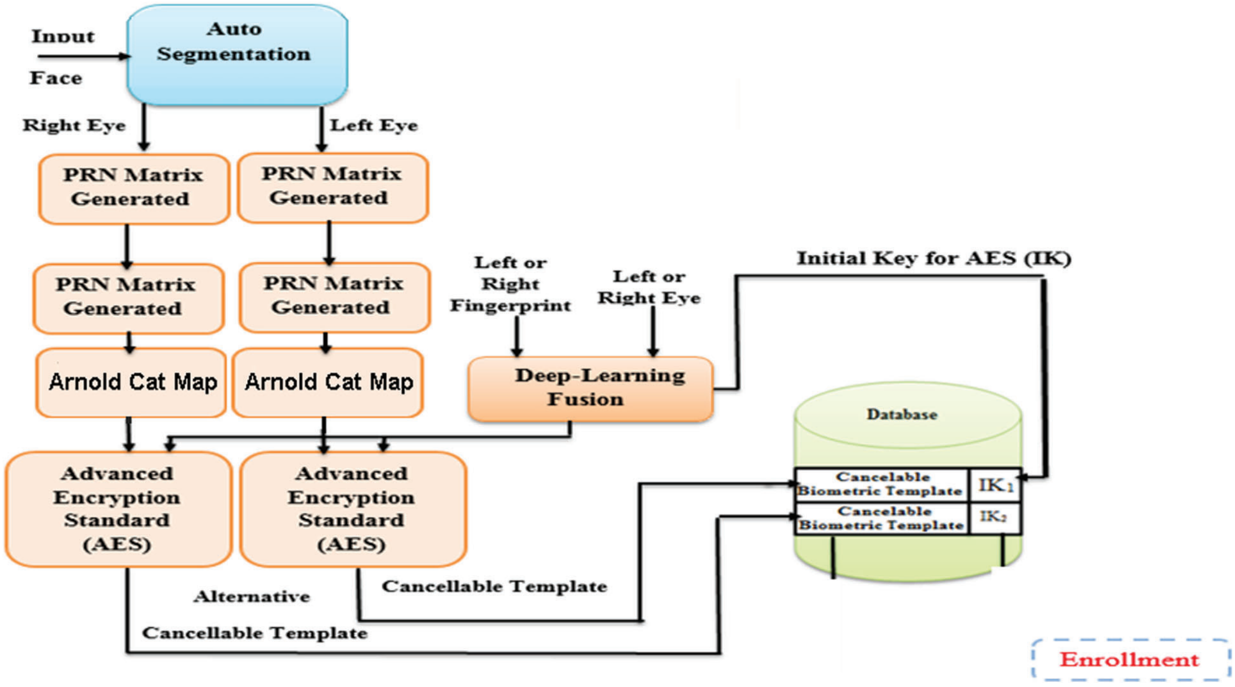


Figure 2: Layout of the proposed cancellable biometric generation technique

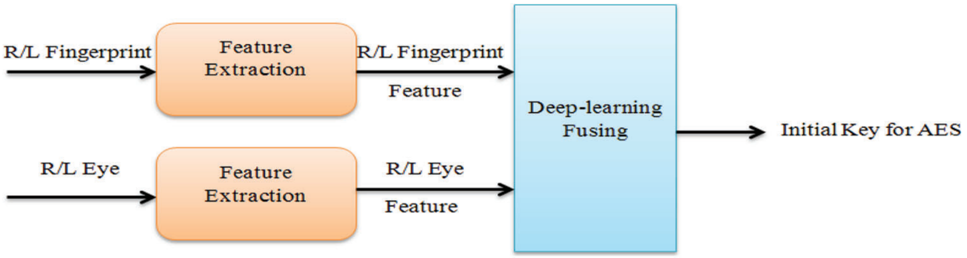


Figure 3: The proposed key generation technology

Step 1: Viola-Jones Face Detection Algorithm

The first object recognition framework is the Viola-Jones segmentation algorithm, which provides a competitive real-time object recognition performance. It was proposed by Paul Viola and Michael Jones in 2001 [9–13].

The Viola-Jones algorithm is utilized for the automatic segmentation of the face image, and this algorithm is used to identify and localize the human face regardless of its size, position, and circumferences. Face detection is a technique that detects the human face and ignores anything else, such as trees, bodies, and buildings. It is commonly used in mobile phone cameras, safety perimeters, and the list continues. The arithmetic speed increases due to the Haarand machine learning AdaBoost feature, and the face can be detected in a frame within milliseconds [14]. A model can be trained to detect from various categories of objects. First, the values of all pixels in a grayscale image are cumulatively black. Then, they are subtracted from the sums of the white squares.

Finally, the result is compared with a specified threshold. If the condition is met, then the feature is considered a hit. In this paper, a MATLAB built-in Application Programming Interface (API) is used to detect the face, upper body, nose, mouth, eyes, etc. In Jones face detection algorithm, the computer vision system toolkit contains vision. A sequential object detection system that detects objects based on the above-mentioned algorithm is used. MATLAB 2014 is used in this work, containing a computer vision system toolbox in the default toolbox list. This method of object recognition combines four key concepts:

a) Simple rectangular elements are defined as hair elements.
b) The complete image is used for rapid feature recognition.
c) The AdaBoost machine learning method is used (adaptive enhancement).
d) A cascaded classifier is used to effectively combine several functions.

Step 2: Generation of Pseudo-Random Numbers

The PRNG depends on a Linear Feedback Shift Register (LFSR). It should have unpredictable values [15]. Under normal circumstances, the random number generator cannot predict the next number in the sequence. The initial seed yields unpredictable inputs and outputs (assuming that no-one knows the initial conditions). This characteristic is sufficient to meet the requirements of randomness.

The generator is a pseudo-random. It is also used in various cryptographic applications such as data and media encryption keys, and banking security. A maximum length linear feedback shift register creates M rows (i.e., it iterates over all possible $2^n - 1$ states). 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 number of polynomial generators $P(x)$. The total number of internal random states generated by the LFSR is $2^n - 1$, depending on the order of the generator polynomial $P(x)$.

The state of the shift register in clock pulse i is a vector b_i of finite length;

$$b_i = (b_i(1),\ b_i(2),\ \ldots,\ b_i(n-1),\ b_i(n)) \tag{1}$$

The output c_i in the i-th term is the union of these states.

$$c_i = (b_i(1) \& b_i(2) \& \ \ldots . \& b_i(n-1) \& b_i(n)) \tag{2}$$

The pseudo-random number sequence c_i of length M is expressed as follows:

$$C_M = (c_1,\ c_2,\ c_3,\ \ldots,\ c_M) \tag{3}$$

For an $M \times M$ input image, a $C_{M \times M}$ pseudo-random number matrix must be generated, and the rows of the coding matrix $C_{M \times M}$ are pseudo-random numbers. The length of C_M in the random number sequence is M.

$$C_{M\times M}(i,\ :) = circleshiftby((i-1)*L)\ of\ C_M \tag{4}$$

where i is the row index of the $C_{M\times M}$ matrix, and L is the pseudo-random sequence.

The output shifted versions have low auto-correlation, which improves the encryption process. When performing the XOR operation on the $C_{M\times M}$ matrix, this very important property plays an important role in encrypting the input image, because it tends to increase entropy. The encrypted image has a low autocorrelation with the original image, and a uniform histogram.

An n-array linear feedback shift register is used to generate C_M from the PRN sequence. For a simplean 32 × 32 image, a 32-bit PRN sequence must be generated. In this case, $n = 5$. The LFSR layers are used. The LFSR satisfies the generator polynomial *P(x)* in Eq. (5) for the maximum-length sequence. We generate $n = 2^5-1\ =\ 31$ internal random states. Fig. 4 shows the block diagram of the developed LFSR with $n = 5$ layers. The C_{32} sequence has 31 random states. We add the first condition.

$$P(x) =\ x^7 + x^5 + x^3 + x + 1 \tag{5}$$

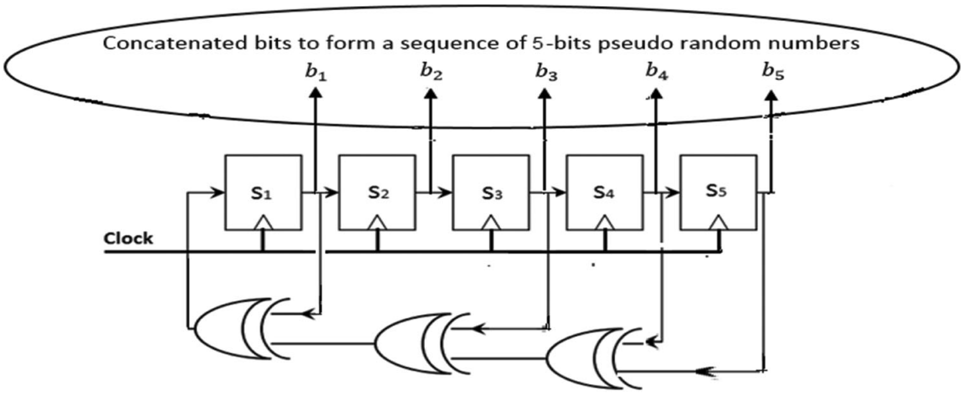

Concatenated bits to form a sequence of 5-bits pseudo random numbers
b_1
b_2
b_3
b_4
b_5
S1
S2
S3
S4
S5
Clock

Figure 4: Layout of the designed $n = 5$ stage LFSR for generating a polynomial [15]

We have a 32 × 32 PRN coding matrix. Each row of the $C_{32\times 32}$ encoding matrix is a continuous version with 5 changes from the original C_{32} sequence. The difference between two adjacent PRN sequences in the coding matrix is 5. We minimize the correlation between adjacent pixels in the same column. Fig. 5 shows the autocorrelation between the original PRN sequence and its 5 consecutive offset versions.

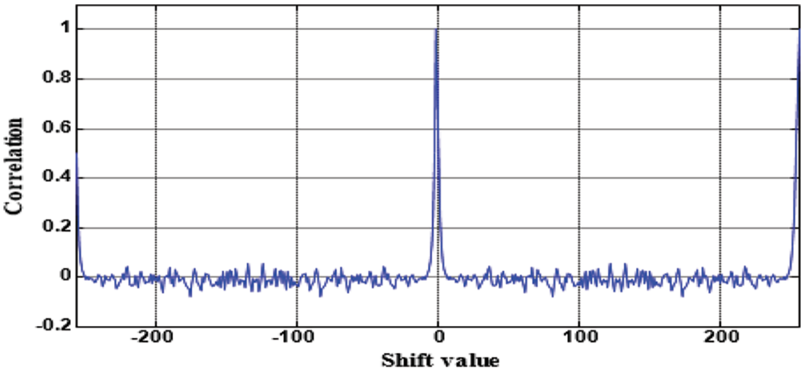


Figure 5: Correlation among the original PRN sequence and its 5 consecutive modified versions [15]

Step 3: Utilization of PRN sequence for image encryption

First, wegenerate the PRN code. The $M \times M$ eye image is XORed with the generated $C_{M \times M}$ PRN matrix to generate an encrypted PRN main image. This process reduces the correlation between biometric eyes and encrypted eyes. We change the histogram and propagate the change.

Step 4: Arnold's CatMap

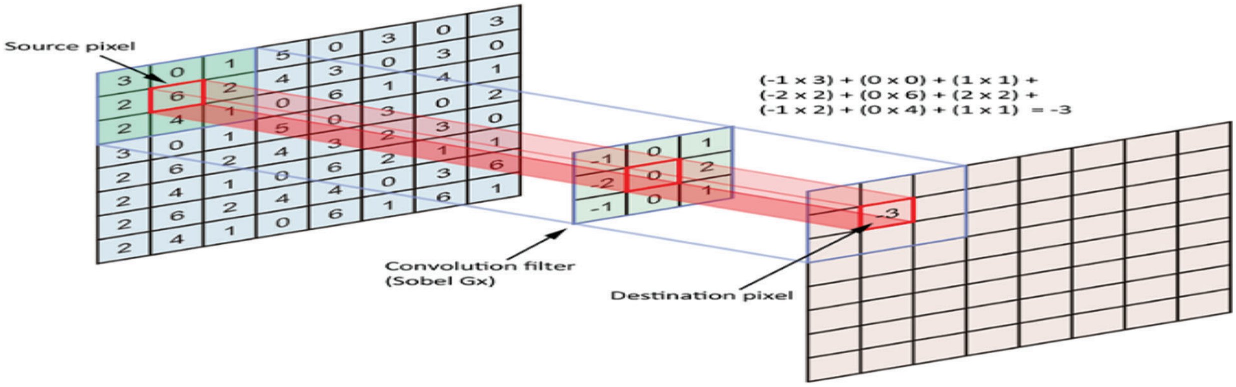
It is used for rearranging the digital image matrix, in a process called transformation. When encoding images, we adopt Arnold's [15–17] cat map technology. It is a safer and more effective technology. The image gets a random change in the original pixel arrangement. Sometimes, the original image is inverted, and the histogram of the coded image matches the histogram of the original one [16].

Step 5: Image Fusion Using Deep Learning

The merging process is performed between the fingerprint and iris images with the original AES key. In this paper, the fusion of iris and fingerprint images based on deep learning is performed by Convolutional Neural Networks (CNNs) [18]. The convolutional layer contains filters used to perform two-dimensional (2D) convolution on the input image. The resulting properties of the convolutional layer vary depending on the convolution filters used. This concept is very suitable for tumor detection, because it can capture any subtle changes in the local activity levels in the image. Fig. 5 shows an example of what happens in the convolutional layer.

It is believed that the CNN can learn complex input-output associations through sufficient training data. The CNN achieves the optimal model parameters based on an optimization process, so that the prediction input of the loss function is as close as possible to the desired target. With the help of the transformation function *f*, the input *x* is assigned to the desired output *y*. The CNN can be trained to evaluate the function *f*, which minimizes the error between the expected output and the received output *y*. The goal is to minimize the loss function through the optimization process to achieve sufficient learning.

Fig. 6 shows a general overview of the proposed method. First, the input images are converted to Y Cb Cr color channel data. The CNN is implemented on the luminance channel of the input image, because the structural details are displayed in this channel. Another reason is that the brightness changes in the luminance channel are more pronounced than in the chrominance channels (Cb and Cr). On the other hand, weighted mixing is applied on chrominance channels. The resulting luminance channel is combined with the chrominance channel generated by a weighed mixing.


Source pixel
(-1 x 3) + (0 x 0) + (1 x 1) +
(-2 x 2) + (0 x 6) + (2 x 2) +
(-1 x 2) + (0 x 4) + (1 x 1) = -3
Convolution filter
(Sobel Gx)
Destination pixel
-3

3	0	1	5	0	3	0	3
2	6	2	4	3	0	3	0
2	4	1	0	6	1	4	1
3	0	1	5	0	3	0	2
2	6	2	4	3	2	3	0
2	4	1	0	6	2	1	1
2	6	2	4	4	0	3	6
2	4	1	0	6	1	6	1

-1	0	1
-2	0	2
-1	0	1

Figure 6: Example of the process taking place in the convolutional layer [19]

The following subsections describe the network architecture, loss function, and learning process. The Deep-Fuse CNN fusion method shows that the learnability of the CNN is largely affected by the correct architecture and choice of the loss function. The proposed image fusion network architecture is shown in Fig. 7. The proposed architecture consists of three parts: feature extraction layer, merging layer, and reconstruction layer. Fig. 8 illustrates the fusion process with deep learning.

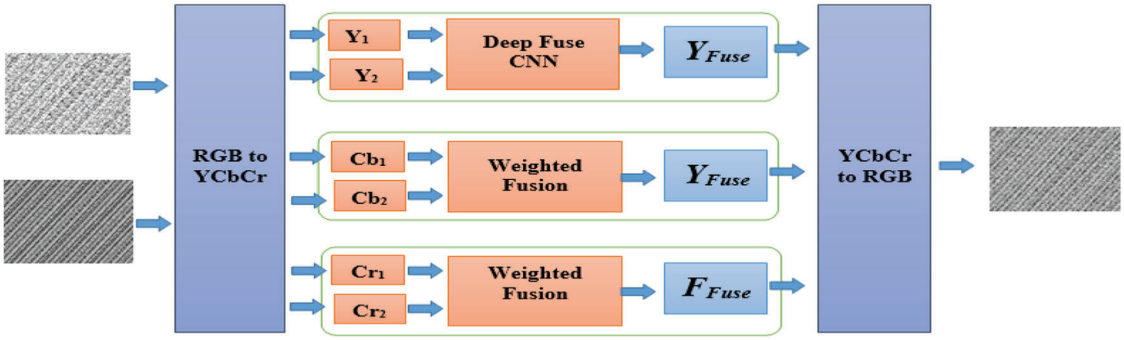


Figure 7: Suggested deep learning fusion [19]

As shown in Fig. 8, the underexposed and overexposed images (Y1 and Y2) are sent on different channels (channel 1 (C1) is composed of C11 and C21, and channel 2 (C2) is composed of C12 and C22), level (C11 and C12) contains 5 × 5 filters for extracting low-level objects such as edges and corners. The weights of the deflection channel are related; C11 and C12 (C21 and C22) have the same weight.

This architecture has three advantages. First, the network is forced to learn the same attributes for the input images, so that the output attributes of the C1 and C2 graphs have the same type of features. Hence, we can simply combine the corresponding images into an overlay. That is, the first function diagram (F11) in Fig. 1 and the first function diagram (F21) in Fig. 2 are added together, and this process is also applicable to the remaining function diagrams. We can combine these functions as needed. The network must calculate weights to combine them.

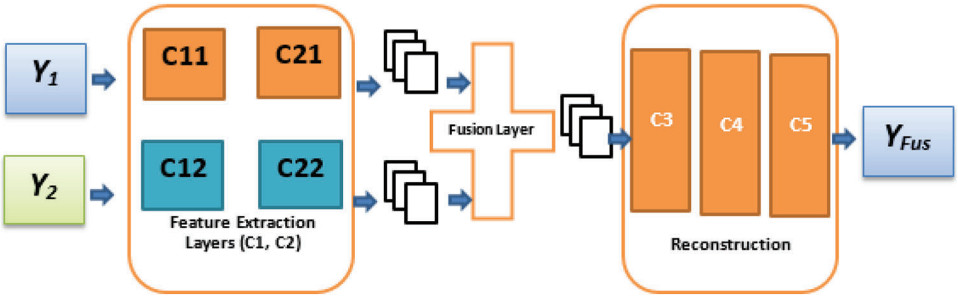


Figure 8: Suggested three-part architecture: feature extraction layer, fusion layer, and reconstruction layer [19]

Experiments show that the function chain can also achieve similar results by increasing the number of filters and layers after C3 to increase the number of training iterations. This is understandable, because the network needs more iterations to determine the appropriate merging weights. In this configuration of binding weights, we force the network to learn filters that remain constant for brightness changes. In the case of coupled weights, the centers of several highly active filters surround the receptive field. These filters are learned to remove the average value of the neighborhood, which effectively keeps the brightness of the object constant. The number of learnable filters is halved. Convergence isquick, because the network has few parameters. The fusion layer combines features derived from C21 and C22.

Step 6: AES Encryption

Advanced Encryption Standard (AES) is an encryption algorithm for encryption security. For a 128-bit key, a brute-force attack requires 2^{128} tests. In addition, the structure of the algorithm and the rounding function used in it ensures a high degree of resistance to linear and differential cryptanalysis.

The proposed authentication system addresses most of the threats for biometric authentication systems. First, the initial key created for the input operator is integrated with the right fingerprint, and the right eye features of the input operator using deep learning technology, and then the initial key is generated. The primary key matches the stored primary key template (IK) database. If it matches the stored primary key, the input subject is authenticated. For further authentication, the PRNG codes are fetched from the database; the corresponding template is generated, and, finally, the generated template is matched with the stored ones. Fig. 9 shows a schematic diagram of the suggested authentication technology.

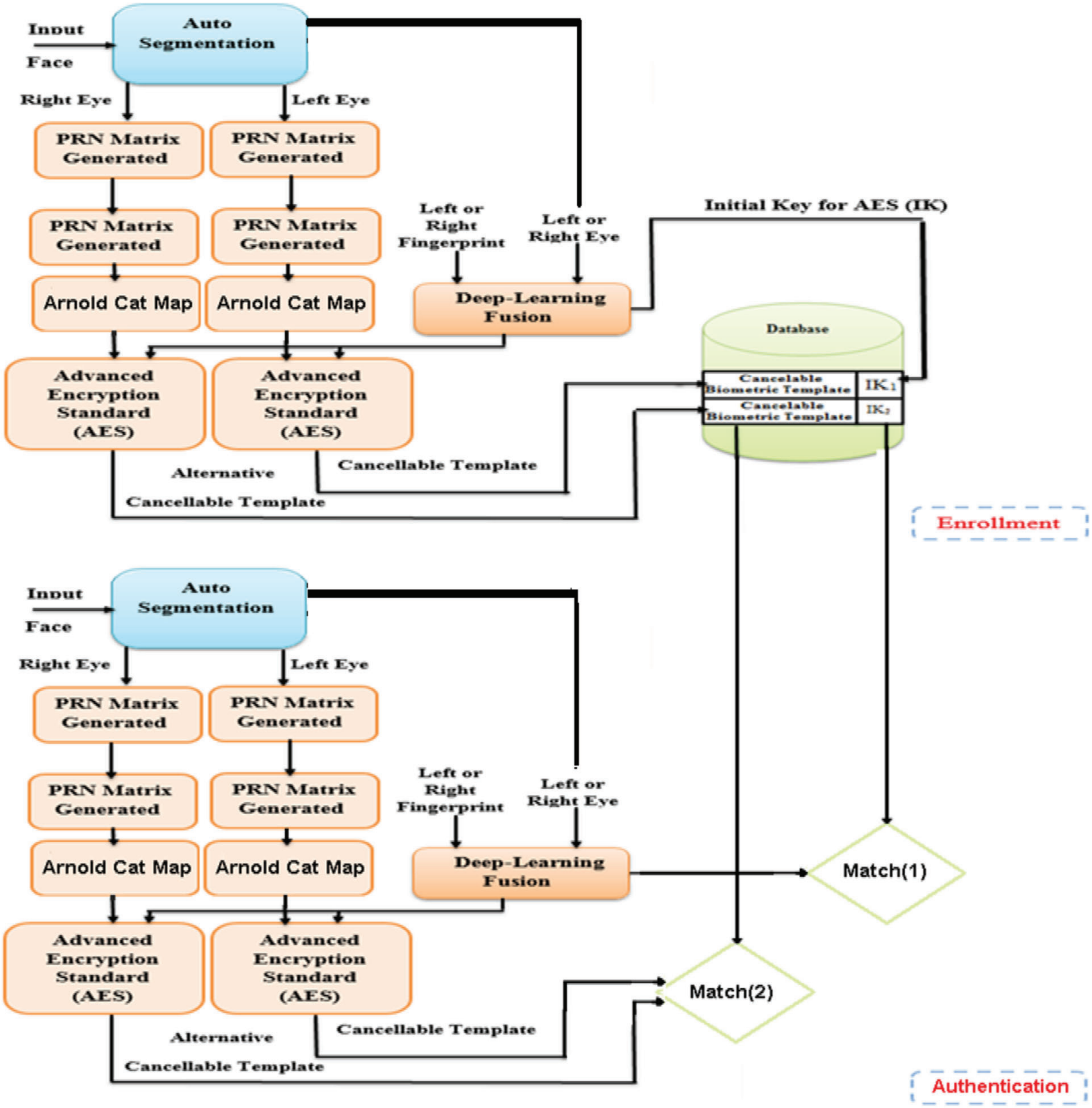


Figure 9: Proposed authentication system

4 Simulation Experiments and Results

The planned cancellable multi-biometric technique is applied on any image format. The performance rating and analysis depends on some metrics such as genuine and impostor distributions, ROC curves, and encryption parameters. The 256 × 256 Lena image is used for unauthorized data with a size of 128 × 128 in Fig. 10, and samples of faces for authorized data simulations are given in Fig. 11. Examples of the cancellable face templates created using the suggested scheme are shown in Tab. 1.

Figure 10: Lena unauthorized image

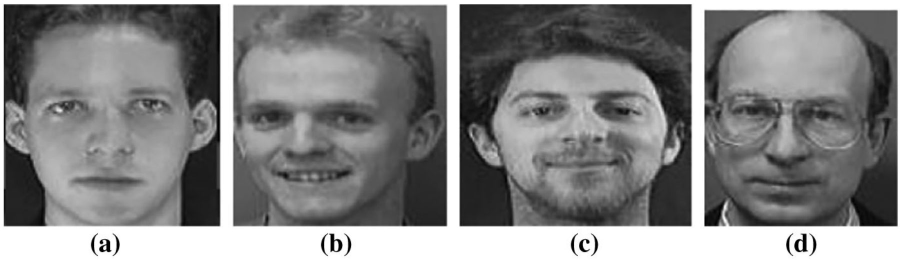


Figure 11: Samples of 128 × 128 face images [20]

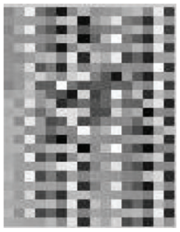
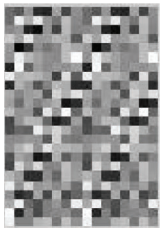
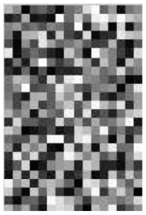
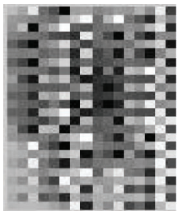
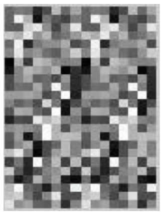
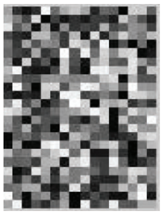
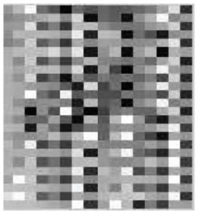
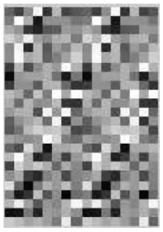
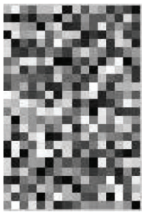
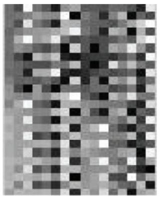
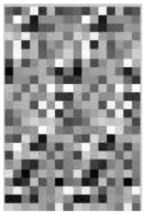
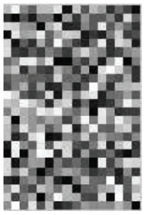
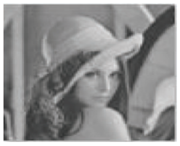
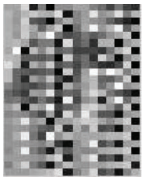
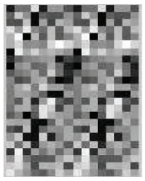
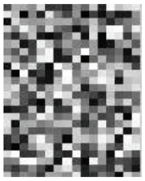
4.1 *Quality Assessment*

Statistical tests of the proposed cancellable biometric system are applied on the individual face templates.

4.2 *Performance Evaluation*

The genuine and imposter distributions and the ROC curves are created in the presence of noise with exclusive levels. The ROC curve connection reveals the relation between the True Positive Rate (TPR) and the False Positive Rate (FPR) at exclusive threshold values. The FRR measures the probability that a face can be falsely rejected as an imposter facial sample, and the FPR measures the probability of accepting an imposter facial sample as being genuine [21,22]. Fig. 12 reveals the closeness to uniformity over a positive bandwidth, which is a preferred function for an excessive degree of protection in Fig. 13. Fig. 14 shows good properites of Imposter and genuine distributions of the proposed scheme. Fig. 15 shows ROC curve for the proposed cancellable biometric. Tab. 2 measurement index for the unauthorized template in Fig. 10. Tabs. 3–6 shows measurement index for the authorized templates of Fig. 11 (a,c,b, and d). Tab. 7 shows the assessment metrics in the presence of noise.

Table 1: Output stages of the cancellable face template generation of the proposed cancellable biometric scheme

Input Face Biometrics	Output Auto Segmentation	Generated Right Eye Encrypted PRN	Output of Arnold Permutation	Output AES Encryption	Generated Initial Key (IK) Fusion
 Authorized User					
 Authorized User					
 Authorized User					
 Authorized User					
 Unauthorized User					

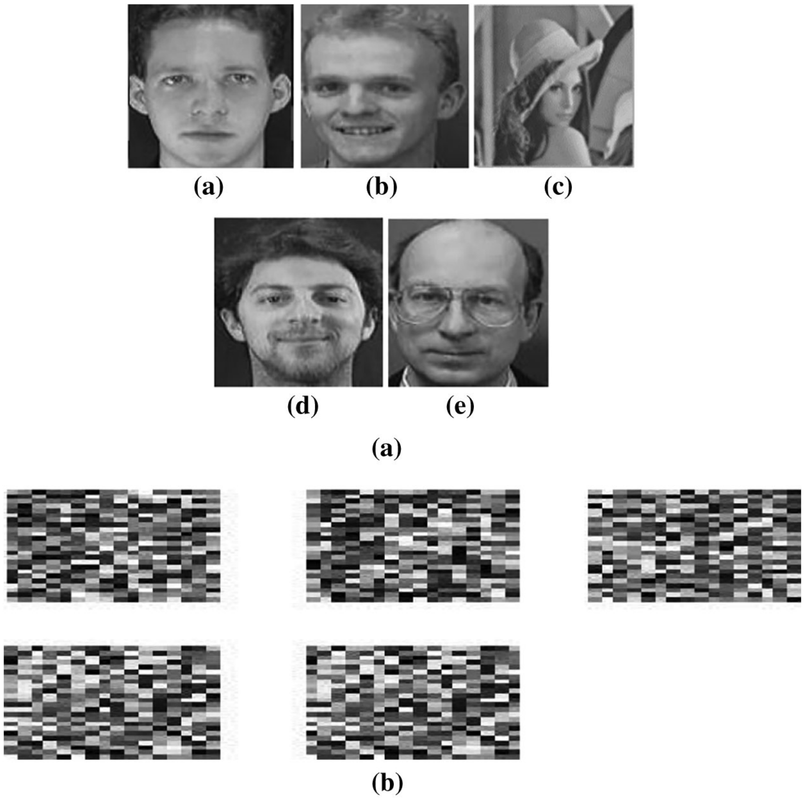


Figure 12: Biometric templates. (a) Original templates [20] (b) Output cipheredtemplates

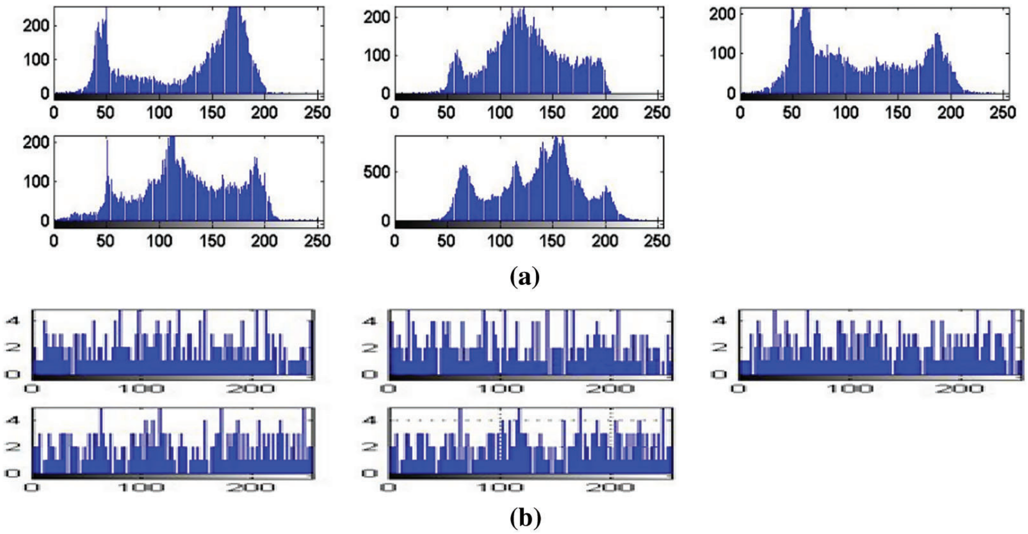


Figure 13: (a) Original template histograms, (b) Ciphered template histograms

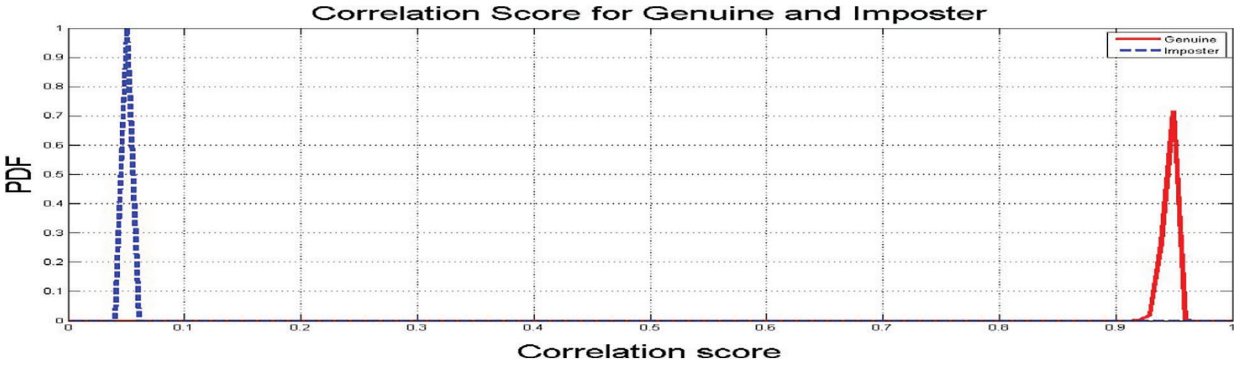


Figure 14: Imposter and genuine distributions of the proposed scheme

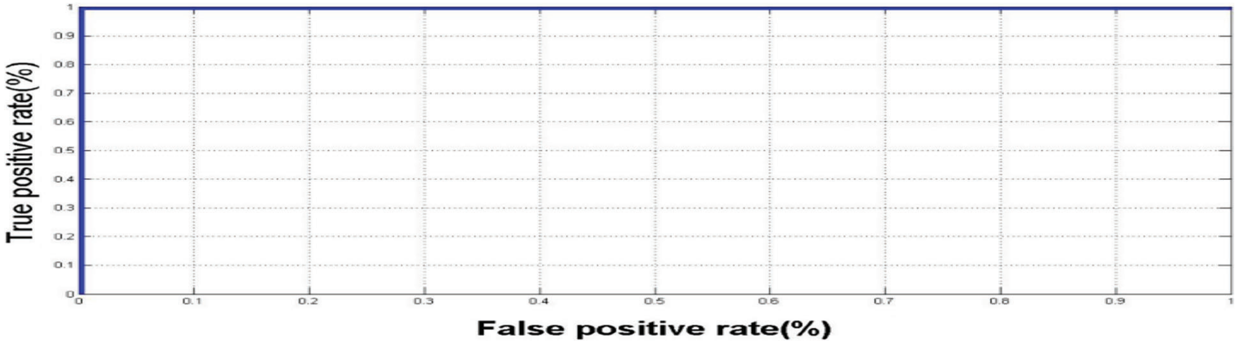


Figure 15: ROCcurve for the proposed cancellable biometric scheme

Table 2: Measurement index for the unauthorized template

Assessment metrics	Proposed scheme	
	Right eye	Left eye
Ciphering time (sec)	3.28	3.30
Entropy [21]	7.4502	7.9977
Correlation among the original biometric and encrypted template [21]	0.0603	0.0013
ID [21]	0.9089	0.9583
NCPR [21]	100	100
UACI [21]	0	0
MDMF [21]	0.9240	0.9240

Table 3: Measurement index of the authorized templates in Fig. 11a

Assessment metrics	Proposed scheme	
	Right eye	Left eye
Ciphering time (sec)	3.30	3.35
Entropy	7.4594	7.4423
Correlation among the 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

Table 4: Measurement index of the authorized templates in Fig. 11c

Assessment metrics	Proposed scheme	
	Right eye	Left eye
Ciphering time (sec)	3.30	3.35
Entropy	7.4235	7.4826
Correlation among the 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 5: Measurement index of the authorized templates in Fig. 11b

Assessment metrics	Proposed scheme	
	Right eye	Left eye
Ciphering time (sec)	3.30	3.35
Entropy	7.4454	7.5130
Correlation among the original biometric and encrypted template	0.0041	0.0102
ID	0.9531	0.9427
NCPR	100	100
UACI	0	0
MDMF	0.6900	0.7836

Table 6: Measurement index of the authorized templates in Fig. 11d

Assessment metrics	Proposed scheme	
	Right eye	Left eye
Ciphering time (sec)	3.30	3.35
Entropy	7.3950	7.4550
Correlation among the original biometric and encrypted template	0.0255	0.0533
ID	0.9453	0.9245
NCPR	100	100
UACI	0	0
MDMF	0.9240	0.9240

Table 7: Score index of the proposed biometric scheme with different noise levels

Variance of noise	EER	AROC
0.05	0.0008	0.999
0.04	0.0009	0.996
0.03	0.0013	0.995
0.02	0.0019	0.996
0.01	0.0016	0.995

5 Conclusions and Future Work

This article investigated the current trends and open research issues of cancellable and hybrid biometric encryption systems. The combination of pseudo-random number sequences, Arnold's cat map, and the AES technique creates the cancellable templates. It allows randomness and good correlation properties of pseudo-random number sequences, Arnold's cat map, and AES encryption. Moreover, we have increased the strength of the enrollment phase using a selective encryption technology. It encodes a portion of the face biometrics, not the whole face image, and thus small storage space is used to store the personal data in the database. It is supposed that no one knows enough initial conditions to break the randomness of codes. In addition, the simulation results show that the proposed scheme offers higher entropy and lower correlation between the original eye and the encrypted template. Cancellable biometric results guarantee low EER. Deep learning integrates two biometrics into more representatives, reliable and detailed outputs using deep learning. In future directions, we can apply the proposed framework for medical image communication using machine learning techniques.

Acknowledgement: The authors thank 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 Arbia (www.tu.edu.sa).

Conflicts of Interest: The authors state that they have not disclosed any conflicts of interest relating to this research.

References

[1] W. Stallings, *Cryptography and Network Security Principles and Practice*, 5th ed., New York, USA, Prentice Hall, 2011.

[2] E. POP, "Multi-modal biometric systems overview," *Acta Technical Napocensis Electronics and Telecommunication*, vol. 49, no. 3, pp. 1–11, 2008.

[3] S. Sheena and M. Sheena, "Review paper optimizing security of multi-modal biometric system," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 15, no. 3, pp. 93–98, 2014.

[4] M. Wagh and M. Choudhari, "Analysis of multi-modal biometrics with security key," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 3, pp. 1363–1365, 2013.

[5] M. Ahlawat and C. Kant, "A multi-modal approaches to enhance the performance of biometric system," *International Journal of Innovations & Advancement in Computer Science*, vol. 6, no. 4, pp. 41–46, 2014.

[6] N. Ratha, S. Chikkerur, J. Connell and R. Bolle, "Generating cancellable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[7] V. Conti, C. Militello, F. Sorbello and S. Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multi-modal biometric identification systems," *IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews*, vol. 40, no. 4, pp. 384–395, 2010.

[8] A. Ayoup, A. Hussein and M. Attia, "Efficient selective image encryption," *Multimedia Tools and Applications*, vol. 75, no. 24, pp. 17171–17186, 2016.

[9] A. Asker, F. Elsharkawy, S. Nassar, N. Ayad, F. Abd El-Samie *et al.,* "A novel cancellable Iris template generation based on salting approach," in *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 3703–3727, 2021.

[10] K. Kamaldeep, "A review of various attack on biometrics system and their known solutions," *International Journal of Computer Technology and Application*, vol. 6, no. 2, pp. 1980–1992, 2011.

[11] H. Rein-Lien, M. Abdel-Mottaleb and A. Jain, "Face detection in color images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 696–706, 2002.

[12] M. Chaudhari, C. Vanjare, D. Thakkar, M. Shah and A. Kadam, "Intelligent surveillance and security system," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 3, pp. 2291–2299, 2015.

[13] A. Georghiades, P. Belhumeur and D. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 643–660, 2001.

[14] P. Wilson and J. Fernandez,"Facial feature detection using haar classifiers," *Journal of Computing Sciences in Colleges*, vol. 21, no. 4, pp. 127–1330, 2006.

[15] H. Rowley, S. Baluja and T. Kanade, "Neural network-based face detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 1, pp. 23–38, 1998.

[16] W. Schindler, "Functionality classes and evaluation methodology for deterministic random number generators," *Anwendungshinweise and Interpretation*, vol. 2, no. 5, pp. 5–11, 1999.

[17] S. Lian, "Multimedia content encryption techniques and applications," *CRC press*, *Taylor & Francis Group*, 2009.

[18] Y. Wang and T. Li, "Study on image encryption algorithm based on arnold transformation and chaotic system," in *Proc. Int. Conf. on Intelligent System Design and Engineering Application (ISDEA)*, Changsha, China, pp. 449–451, 2010.

[19] L.Wu, J. Zhang, W. Deng and D. He, "Arnold transformation algorithm and anti-arnold transformation algorithm," in *Proc. First IEEE Int. Conf. on Information Science and Engineering*, Nanjing, China, pp. 1164–1167, 2009.

[20] K. Ma, K. Zeng and Z. Wang, "Perceptual quality assessment for multi-exposure image fusion," *IEEE Transactions on Image Processing*, vol. 24, no. 11, pp. 3345–3356, 2015.

[21] ORL Database, [Online]. Available: https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html*, last access on 1–06–2020.*

[22] H. Ahmed, H. Kalash and O. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," *Informatica*, vol. 31, no. 1, pp. 121–120, 2007.