Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025902
Article

Tech Science Press

Cancellable Multi-Biometric Template Generation Based on Arnold Cat Map and Aliasing

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

[1]Electrical Communications Engineering Department, Faculty of Engineering, Minia University, Minia, 61111, Egypt
[2]Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menoufia University, 32952, Menouf, Egypt
[3]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[5]Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University, Tanta, Egypt
*Corresponding Author: Ahmed M. Ayoup. Email: ayoup.2012@hotmail.com

Received: 08 December 2021; Accepted: 15 February 2022

Abstract: The cancellable biometric transformations are designed to be computationally difficult to obtain the original biometric data. This paper presents a cancellable multi-biometric identification scheme that includes four stages: biometric data collection and processing, Arnold's Cat Map encryption, decimation process to reduce the size, and final merging of the four biometrics in a single generated template. First, a 2D matrix of size 128 × 128 is created based on Arnold's Cat Map (ACM). The purpose of this rearrangement is to break the correlation between pixels to hide the biometric patterns and merge these patterns together for more security. The decimation is performed to keep the dimensions of the overall cancellable template similar to those of a single template to avoid data redundancy. Moreover, some sort of aliasing occurs due to decimation, contributing to the intended distortion of biometric templates. The hybrid structure that comprises encryption, decimation, and merging generates encrypted and distorted cancellable templates. The simulation results obtained for performance evaluation show that the system is safe, reliable, and feasible as it achieves high security in the presence of noise.

Keywords: Aliasing technique; selective encryption; ACM; decimation process

1 Introduction

Compared with traditional authentication systems, biometric authentication systems have certain advantages over systems that adopt passwords and Personal Identification Number (PIN) codes. In biometric systems, authorized users only should have the ability to access personal information. Hence, information security needs to be guaranteed. These systems require authenticated persons to provide their unique personal data during the authentication period [1]. Therefore, a biometric authentication system is a reliable and safe choice. Biometric identification is a method of identifying people based on their certain personal characteristics [2]. Physiological biometric technology uses a person's unique physical characteristics, such as fingerprints, faces, palm prints, iris, or Deoxyribonucleic Acid (DNA) sequences, to identify users, and it has proven to be a powerful tool in identity verification systems. The main advantage of biometrics is that they are not vulnerable to theft and loss. They are independent of users' memory. Moreover, they do not change significantly over time, and it is difficult for a person to change his own physiological biometrics or imitate someone else measurements. Among the various biometrics in security applications with the scope of the digital collection, palm prints have recently received more attention among researchers [3].

The popularity of biometrics is driven by two factors: technological progress and safety requirements. For a long time, the need to use special sensors to collect biometric data has been considered a disadvantage, especially when viewing multiple biometric data. There should be an ability to collect data using modern sensors. For example, smartphones contain several potential biosensors, some of which are designed to be used, such as fingerprint scanners, while others can capture biometric data as auxiliary tools, such as digital cameras. High-resolution images are used for face recognition, iris recognition, and retina scanning. Microphones are used for recording. In addition, walking needs an inertial sensor. Of course, the same computer can be used to collect personal data, which requires further research on the security of the system [3].

The biometric devices may be defective, and errors may occur. There are two types of error measurement metrics in biometric systems: False Rejection Rate (FRR) and False Acceptance Rate (FAR). If the device rejects an authorized person, this counts into the FRR, and if the device accepts an unauthorized person, this counts into the FAR. By combining two or more physical characteristics to determine the FAR and the FRR, a multi-biometric system has been built with other levels of precautions [4].

Biometric systems are usually prone to problems such as sensor data corruption, missing characters, under-representation, overshoot, and incompleteness. The multi-modal biometric identification system can reduce the Failure-To-Capture (FTC) and Failure-To-Enroll (FTE) values and provide the highest level of anti-counter-feting protection, because it is difficult to develop multiple biometric sources at the same time. In the feature extraction process, fingerprint and iris feature extraction can be implemented with multi-modal biometric systems. We improve the realization of multi-modal biometric characteristics.

This article is divided into five parts. The first part introduces the cancellable biometric concepts, biometric security and privacy issues, and the main contributions of the proposed cancellable biometric algorithm. The second part introduces the related work of various researchers in this field. In the third part, we introduce the proposed algorithm and the authentication strategy. In the fourth part, we introduce the simulation results. Finally, we give the conclusion and future work.

1.1 Cancellable Biometric Concepts

The cancellable biometric transformation is designed to be computationally difficult to obtain the original biometric data. As shown in Fig. 1, the original image is not used, but an irreversible image transformation is used, alternatively. In case the cancellable template is stolen, it can be overwritten through another transformation. This can protect user privacy, because it is computationally difficult to restore the original patterns from the transformed templates. In addition, the templates can be changed easily in hacking scenarios. This methodology prevents database overlap, because each application has a different conversion (See Fig. 2). In addition, this methodology does not affect the accuracy of the matching process, because the statistical properties of the attributes are roughly preserved after conversion [5–7].

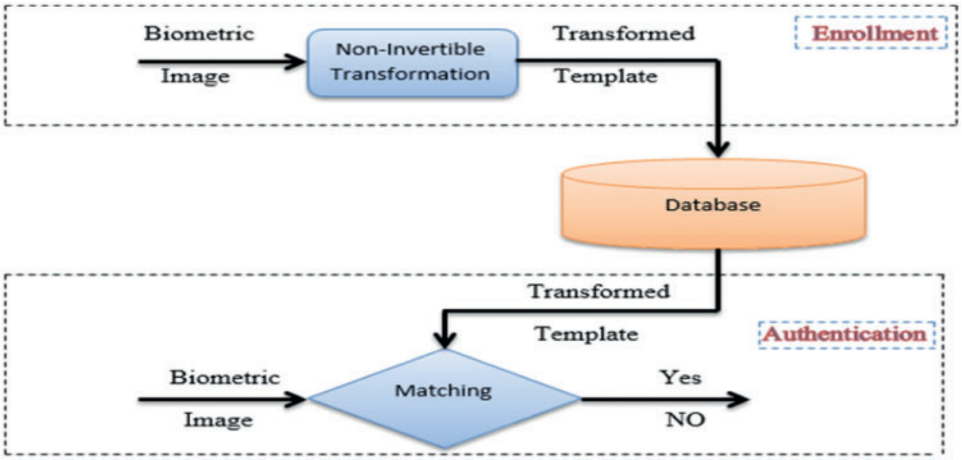


Figure 1: Layout of a cancellable biometric authentication system [5–7]

1.2 Security and Privacy Aspects of Biometric Systems

Biometric systems are considered as secure tools of identity verification, but fraudsters have also developed new methods to bypass the security of biometric systems. The problem with biometric authentication systems is that the biometric data is not confidential. There are eight possible attacks on biometric systems [8]. Fig. 2 shows various attacks at different points in the biometric verification system.

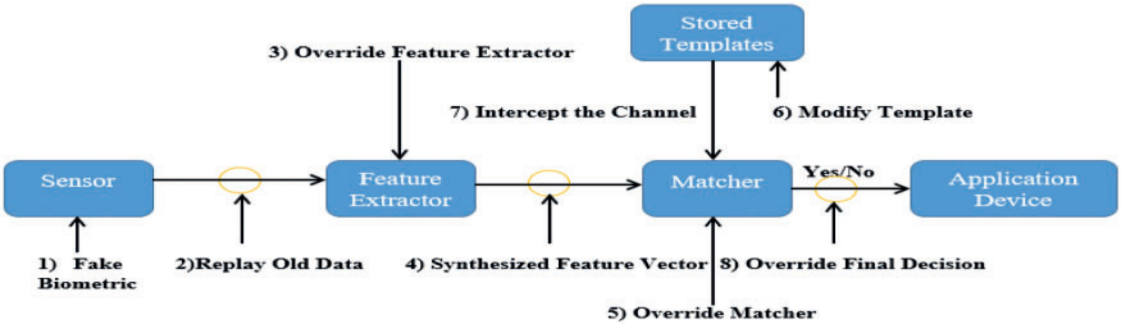


Figure 2: Various attacks at different points of the biometric system [9]

Attackers can display fake biometric data in front of the sensor [9]. For example, a person can create a fake finger with a fake fingerprint at the sensor. We can bypass the facial recognition system and take a photo of a legitimate user in front of the camera. In addition, we can use some lenses to avoid scanning of the iris [8]. Fig. 1 shows the possible attacks and possible solutions for biometric systems.

1.3 Contributions and Novelty

The main contributions of this paper are summarized as follows:

1) Proposal of a cancellable multi-biometric encryption technique that achieves a decrease in the over-execution enrollment process compared with the cancellable biometric technique in [10]. This proposal has a total runtime of 19.8 s, which makes it more suitable for real-time and Internet-of-things (IoT) applications.
2) Introducing a new cancellable biometric recognition technique using a combination of decimation and aliasing with the help of chaotic Arnold's Cat Map (ACM).
3) Performance evaluation of the proposed cancellable biometric system with metrics including entropy, correlation, etc. The proposed system is more favorable compared to traditional ones.
4) The proposed cancellable biometric system reveals high immunity to noise effect.

2 Related Work

Several attempts have been presented in this field by several researchers for cancellable biometrics [11]. Ross et al. [12] provided an overview of optical image coding. The numerical simulation of this method for cancellable biometrics shows its robustness and the high sensitivity to the correct switching offset. The presented results quantify the robustness of this method based on Mean Square Error (MSE) values with the same number of key changes. We can say that for the same key value, a higher MSE can indicate a higher resistance to noise and attacks.

Ross et al. [13] presented a cancellable multi-modal biometric system. The widespread use of Double Random Phase Encoding (DRPE) allows to create a fragile multi-biometric identification system. The purpose of the system is to provide storage space for the biometric database, and improve security. Kamaldeep et al. [14] proposed a reversible multi-index iris recognition method based on several important parameters in a mixed mode. The feature vectors generated by the left and right iris of the same subject are merged into the safety symbol. The DRPE method is used in the Fractional Fourier Transform (FrFT) domain to generate irreversibly encrypted codes. The cancellable biometric system avoids sending the keys and improves the confidentiality of authentication, because each user has a unique key to receive the encrypted iris code. Experimental results show that the use of this iris recognition method improves privacy, while maintaining authentication performance, achieving a 0.63% energy efficiency and a 99% accuracy. It was concluded that the DRPE is a valid candidate to obtain revocable biometric templates.

Jain et al. [15] proposed an effective method for identifying revocable fingerprints based on the identification process used to verify fingerprints without restoring the original fingerprints. This helps to protect fingerprints from attacks, because the authors used an irreversible transformation. Liu et al. [16] presented a multimedia biometric system based on a combination of fingerprints and faces. The Gabor transform is applied on the image in the mixed pixel layer. This scheme is very effective for small sample scenarios. Zakaria et al. [17] presented a new strategy using the nested sequence array method. The Discrete Cosine Transform (DCT) is used to extract facial features and hand-prints, but serialized into a nested array. The parameters of the feature sequence and its statistical distribution can be estimated. The main advantage of this method is that it supports large databases compared to classic methods. The authors compared their method with other methods, and showed that the detection accuracy of their proposed method is 99.7%, which is higher than those of other methods.

Soliman et al. [18] have worked on four different categories: left and right palms, crossed left palms, left palms with fingerprint samples, and right palms with fingerprints. Left and right fingerprints of the same subject can be used to create matching scores to improve the matching accuracy. Both left and right palm print scores can be compared for better recognition. Ahmad et al. [19] proposed a multi-model system of the left thumb and left ear. The main feature of this system is to improve the stage of thumb imaging before feature extraction. The authors applied Gaussian smoothing of the thumb image. To optimize the performance, Zhang Suen (ZS) dilution algorithm turned out to be a good algorithm. Hearing aids use 5 of 9 functions. The system can operate at a reliability level/range of 80%. It can be increased to100% by adding 4 additional ear functions. Taher and Mosseb et al. [20] proposed a cancellable iris recognition scheme based on the combination of encoding and irreversible transformations to conceal the characteristics of the iris. Its recognition rate reaches 99.9%.

3 Proposed Cancellable Biometric Recognition Framework

The proposed approach begins with four biometric acquisition. After that, Arnold's Cat Map (ACM) encryption is applied on all biometrics. Decimation by 2 is adopted on encrypted templates to generate four decimated and encrypted versions of all biometrics. These four versions are merged together to a single 3D matrix. Some sorts of decimation in rows and decimation in columns are applied to get two templates that have both encryption and aliasing effects. Finally, a sophisticated merging operation is implemented on these two versions to get a final 256 × 256 cancellable biometric template that can be used for biometric verification (See Fig. 3).

Step 1: Acquisition of Biometric Images

Input biometric data is collected by various sensors. For example, human face images are taken by cameras and video cameras; fingerprints and hand geometry are recorded by sensors; iris and retina are scanned by infrared cameras. In this article, all face biometric data of individuals used in the proposed cancellable biometric system are extracted from the faces database [21].

Step 2: Arnold's Cat Map

Arnold's Cat Map (ACM) is a confusion map named after Vladimir Arnold. ACM [22–24] can be used to encode images to increase security. The image (not necessarily a cat) is treated by random changes in the original pixel arrangement. However, the map has a constant period. ACM has two main disadvantages. It is sometimes possible to restore the original image. In addition, the histogram of the encoded image is the same as that of the original image, because the values of the pixels are not changed [24].

Step 3: Decimation Process

In the decimation or down-sampling process, the image dimensions are reduced to one-half or one-third of the original ones. The decimation process eliminates redundant pixels that are not necessary for the generation of cancellable templates (See Fig. 4).

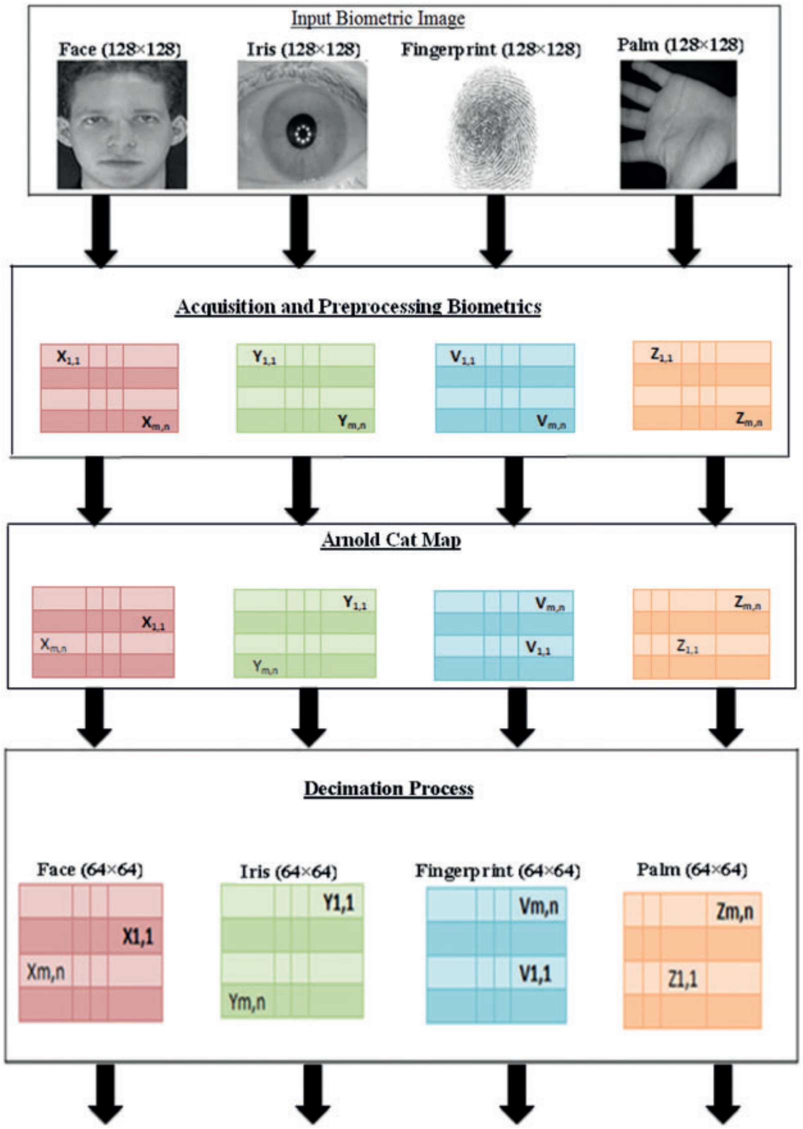


Figure 3: (Continued)

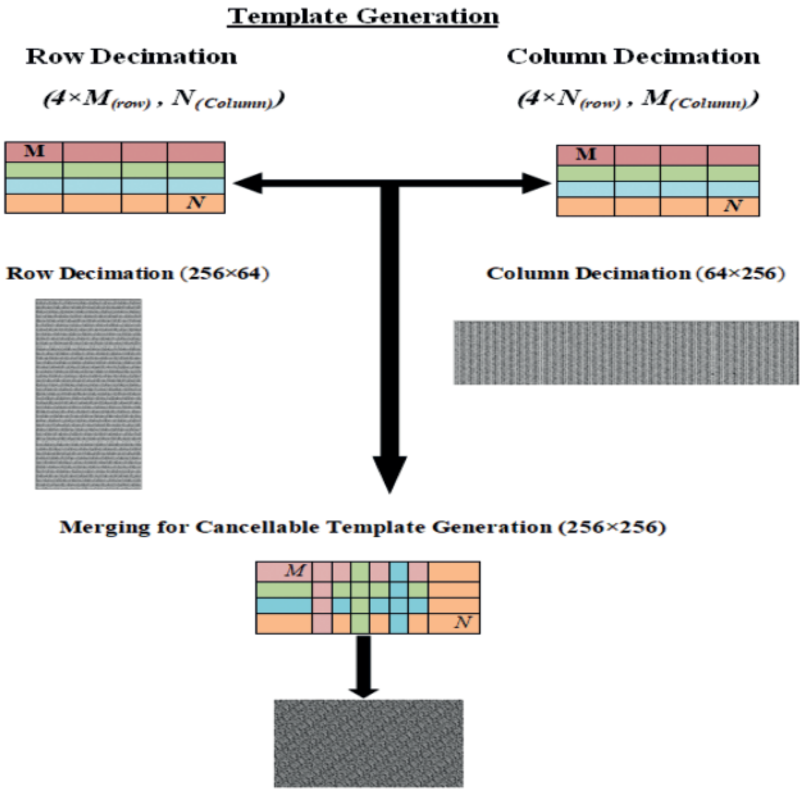


Figure 3: The layout of the proposed cancellable template generation

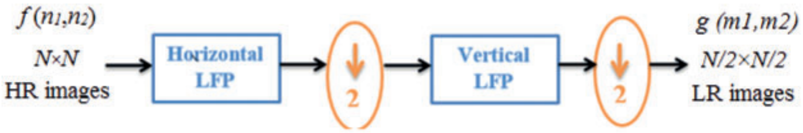


Figure 4: Down-Sampling process from the $N \times N$ image to an $(N/2) \times (N/2)$ image [25–28]

The decimation model can be represented as follows [25–28]:

$$\mathbf{g} = \mathbf{Df} \tag{1}$$

where **f, g** are lexicographicly ordered versions of the original encrypted image and the decimated version, respectively. **D** is the decimation operator given as follows:

$$\mathbf{D} = \mathbf{D}_1 \otimes \mathbf{D}_1 \tag{2}$$

where ⊗ is the Kronecker product, $\mathbf{D}_1$ represents a filtering operation.

$$\mathbf{D}_1 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix} \tag{3}$$

Step 4: Merging Process

The four obtained biometric templates ACM encryption, and decimation processes are merged together, as illustrated in Fig. 3. The four biometrics are arranged in a single 2D matrix through the selection of certain rows and discarding others. A row is taken, and three other rows are discarded. This process is also repeated for columns. Hence, the final obtained matrix has dimensions of 256 × 256. The discarding strategy does not affect the cancellable biometric template generation as few pixels can represent each template differently if derived based on the original biometric template [29–32].

4 Authentication Strategy

The authentication strategy of the proposed system is shown in Fig. 5. A correlation-based strategy necessitates the generation of cancellable templates in the testing process in the same manner used for training. Correlation is estimated, and the decision is made based on a threshold value for verification.

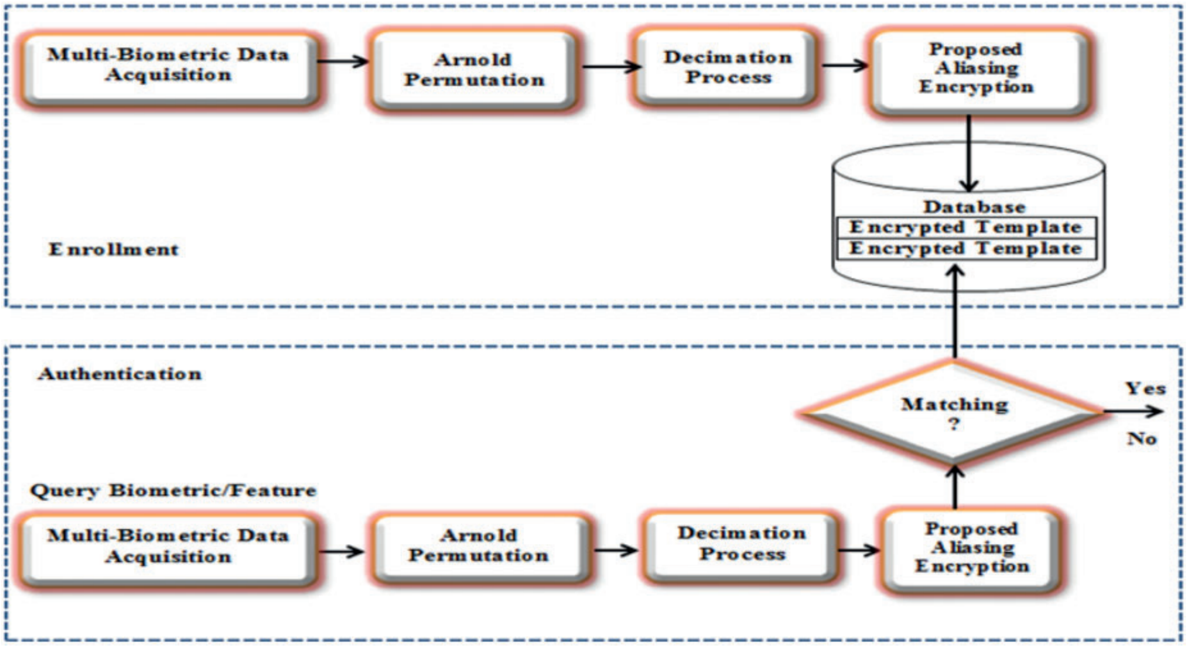
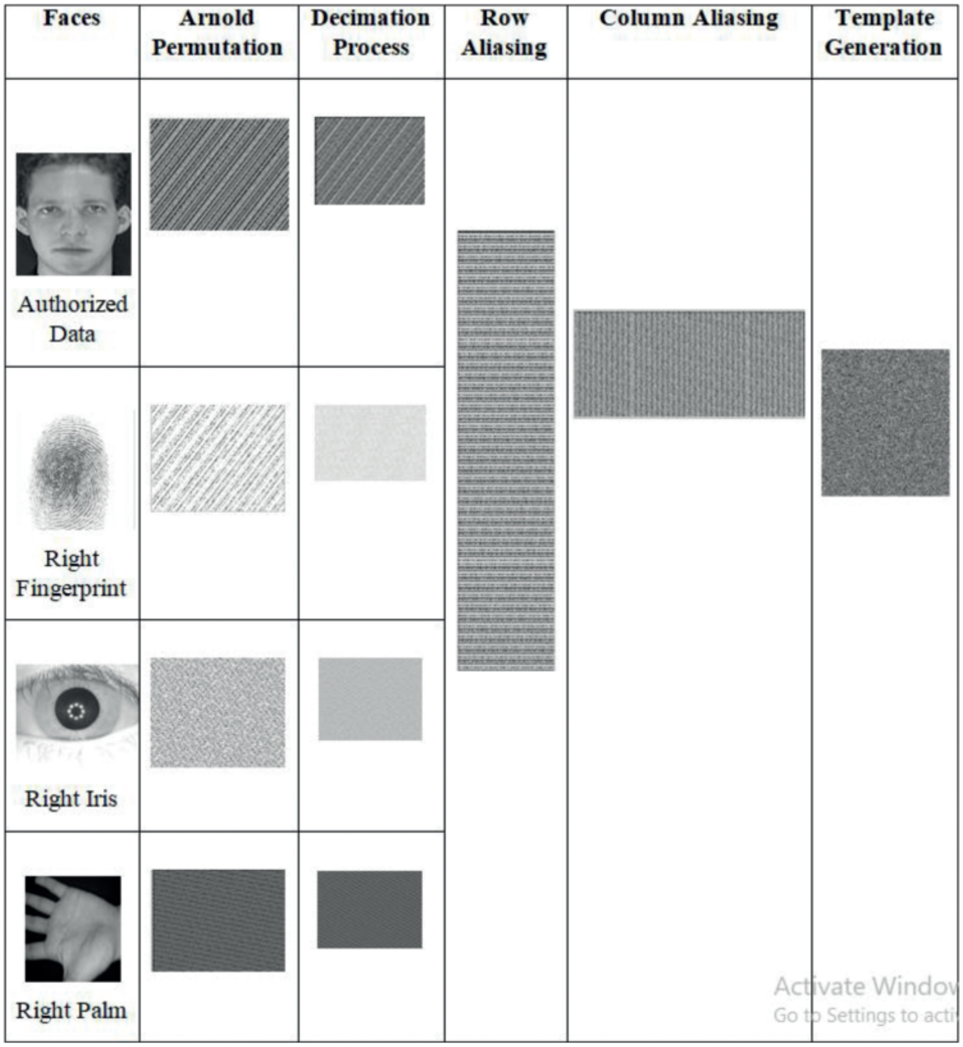


Figure 5: Block diagram of the proposed system revealing the authentication strategy

5 Simulation Experiments and Results

The proposed system is applicable to biometric images of different sizes. Performance assessment is implemented based on Equal Error Rate (EER) and Receiver Operating Characteristic (ROC) curve in addition to some cryptographic test criteria. Simulation experiments shown in Tabs. 1 to 7 have been carried out on MATLAB 2014a, Core(TM) i74600U, CPU 2.10 GHz, 8GB Windows 7 on an Intel(R) laptop. The girl image is used to allow the imposter test.

Table 1: Output of different stages of the proposed cancellable biometric recognition system in Fig. 7a



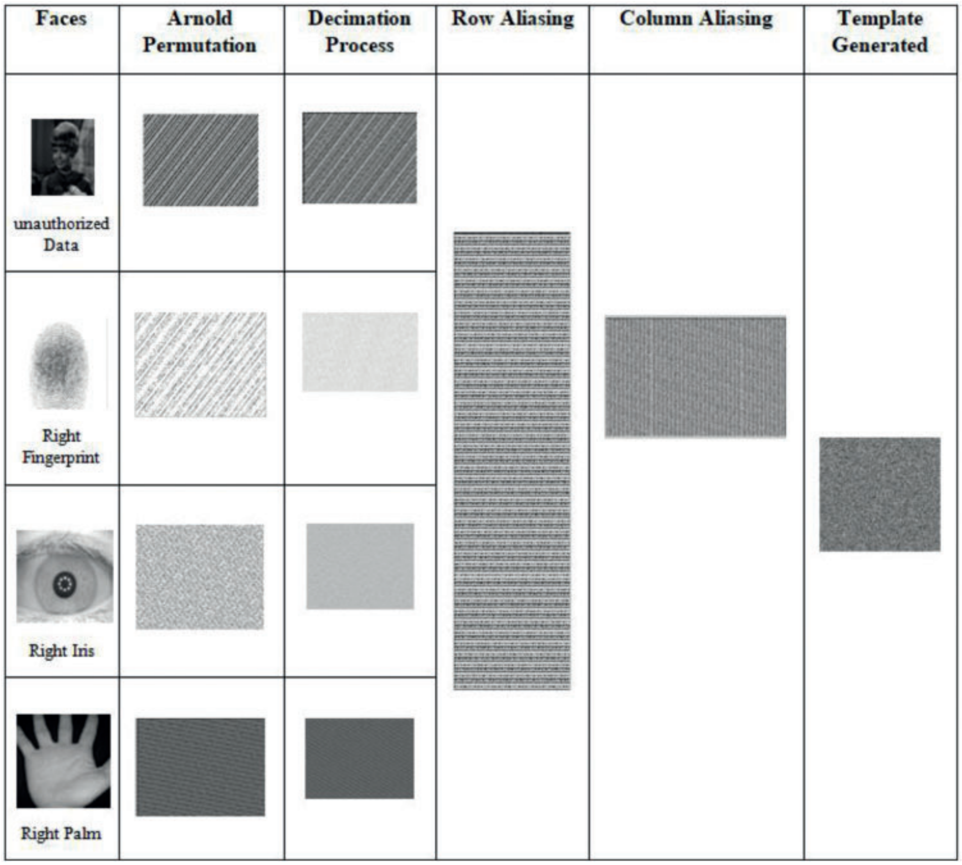
Faces	Arnold Permutation	Decimation Process	Row Aliasing	Column Aliasing	Template Generation
Authorized Data					
Right Fingerprint					
Right Iris					
Right Palm					

5.1 *Quality Assessment*

There are several metrics that are widely used to evaluate the image quality, such as MSE, entropy, Peak Signal-to-Noise Ratio (PSNR), correlation, differential maximum deviation, and Feature Similarity Index Method (FSIM). Statistical tests are applied to evaluate the performance of the encryption process. Tab. 3 shows the measurement of the Proposed cancellable biometric technique for an unauthorized face.

Tabs. 4–7 shows the measurement of the proposed cancellable biometric technique for an authorized face.

Table 2: Output of different stages of the proposed cancellable biometric recognition system in Fig. 6



Faces	Arnold Permutation	Decimation Process	Row Aliasing	Column Aliasing	Template Generated
unauthorized Data					
Right Fingerprint					
Right Iris					
Right Palm					

Table 3: Metrics for the proposed cancellable biometric recognition technique for 256 × 256 girl. jpg unauthorized data IN Fig. 6

Metrics	Proposed cancellable biometric technique
Encryption time (s)	19.8
Entropy	7.9985
Correlation Between Original Biometric and Encrypted Biometric	0.0013
Irregular Deviation (ID)	0.9341
Number of Changing Pixel Rate (NPCR)	99.59
Unified Averaged Changed Intensity (UACI)	20.2855
Maximum Deviation Measuring Factor (MDMF)	0.9909

(Continued)

Table 3: Continued

Metrics	Proposed cancellable biometric technique
FSIM	0.4114
PSNR	12.33
MSE	3.7989×10^3

Table 4: Measured metrics for the proposed cancellable biometric recognition system for 128 × 128 authorized data in Fig. 7a

Metrics	Proposed cancellable technique
Encryption time (s)	19.8
Entropy	7.9986
Correlation Between Original Biometric and Encrypted Biometric	0.0017
ID	0.9341
NCPR	99.52
UACI	20.2855
MDMF	0.8909
FSIM	0.4114
PSNR(dB)	12.33
MSE	3.7989×10^3

Table 5: Measured metrics for the proposed cancellable biometric recognition system for 128 × 128 authorized data in Fig. 7c

Metrics	Proposed cancellable technique
Encryption Time (s)	19.8
Entropy	7.9986
Correlation between Original Biometric and Encrypted Biometric	0.0015
ID	0.7580
NCPR	99.2523
UACI	27.2554
MDMF	0.8211
FSIM	0.3697
PSNR(dB)	9.7564
MSE	6.8776×10^3

Table 6: Measured metrics for the proposed cancellable biometric recognition system for 128 × 128 authorized data in Fig. 7b

Metrics	Proposed cancellable technique
Encryption time (s)	19.8
Entropy	7.9985
Correlation Between Original Biometric and Encrypted Biometric	0.0012
ID	0.9341
NCPR	99.5934
UACI	29.7532
MDMF	0.8909
FSIM	0.4478
PSNR(dB)	8.8292
MSE	8.5145×10^3

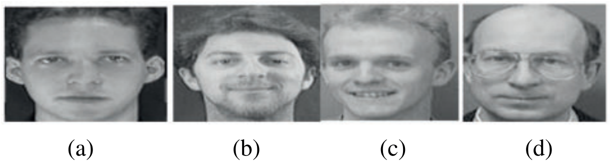
Table 7: Measured metrics for the proposed cancellable biometric recognition system for 128 × 128 authorized data in Fig. 7d

Metrics	Proposed cancellable technique
Encryption time (sec)	19.8
Entropy	7.9976
Correlation Between Original Biometric and Encrypted Biometric	0.0016
ID	0.7029
NCPR	99.6101
UACI	28.3557
MDMF	0.8909
FSIM	0.4089
PSNR(dB)	9.3354
MSE	7.5778×10^3

5.2 *Performance in the Presence of Noise*

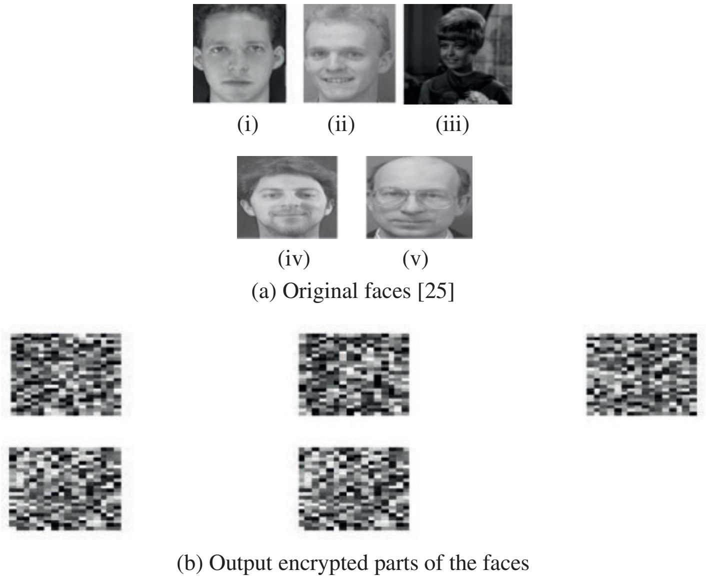
In the presence of different levels of noise and different degrees of correlation between pixels, the authorized user correlation distribution, the unauthorized user correlation distribution, and the ROC curve are analyzed. Fig. 8 shows the samples of face templates created according to the proposed system. Fig. 9 shows a better degree of uniformity in histograms after encryption, which ensures more security of the cancellable templates. The correlation distributions for both genuine and imposter tests are illustrated in Fig. 10. In addition, the ROC curve is illustrated in Fig. 11. Tab. 8 illustrates the evaluation metric values of the proposed system in the presence of different levels of noise. It is clear from this table that the performance of the system deteriorates with the increment of the noise level, but the system still works, and it is still able to discriminatebetween users.

Figure 6: The 256 × 256 girl image



(a) (b) (c) (d)

Figure 7: The 128 × 128 original imposter and genuine templates [21]



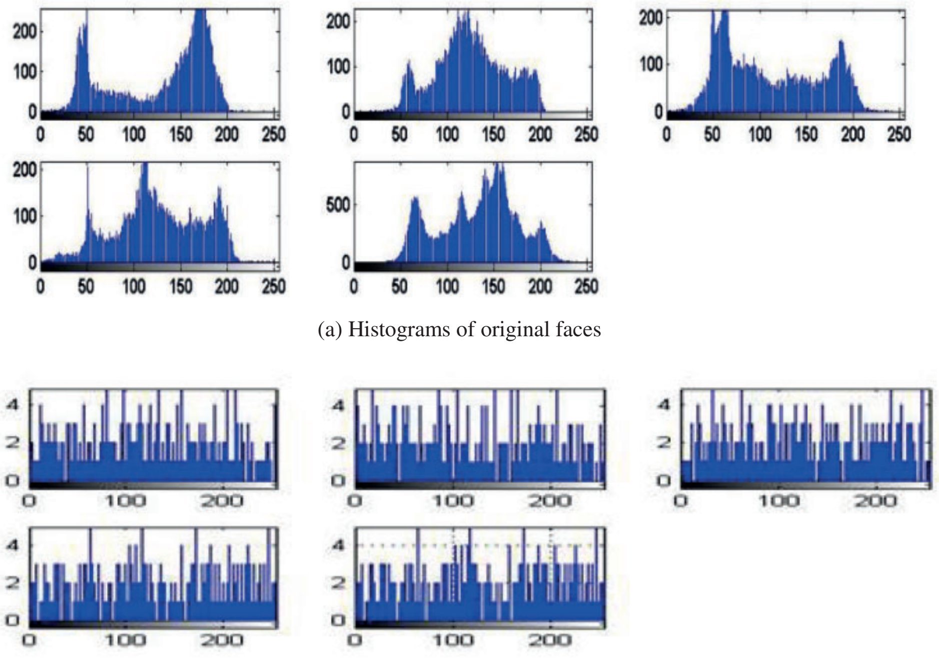
(i) (ii) (iii)

(iv) (v)

(a) Original faces [25]

(b) Output encrypted parts of the faces

Figure 8: Samples of face templates created according to the proposed system. (a) Original face, (b) Encrypted face template output



(a) Histograms of original faces

(b) Histograms of cancellable face templates generated with the proposed system

Figure 9: (a) Original faces and (b) Histograms of the cancellable face templates created with the proposed system

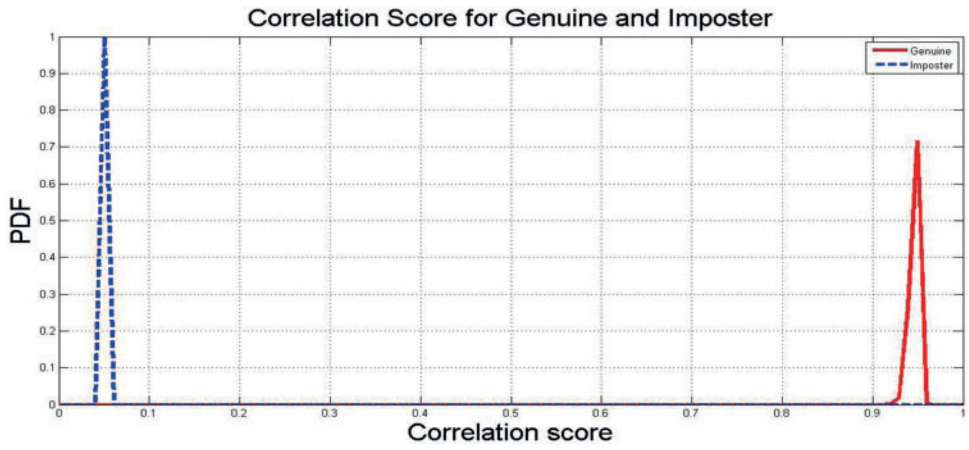


Figure 10: Genuine and impostor distributions

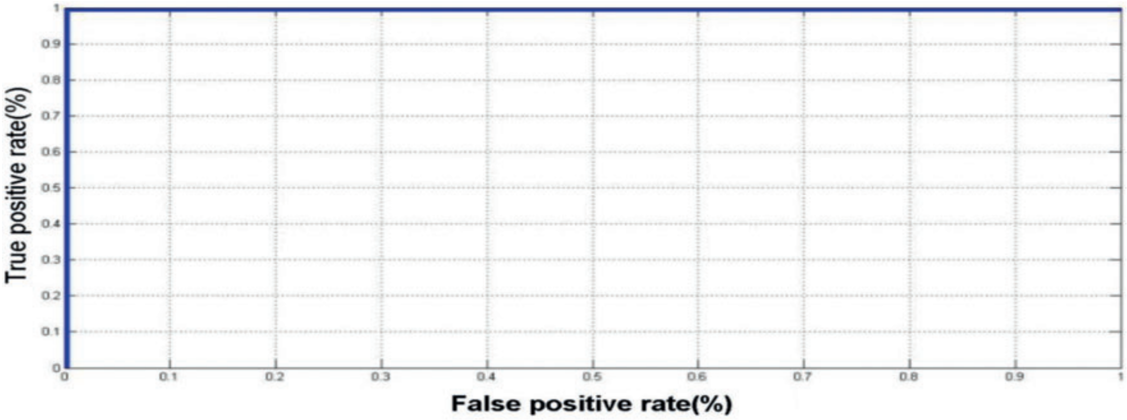


Figure 11: ROC curve

Table 8: Performance metrics of the proposed cancellable biometric recognition system in the presence of noise

Noise Variance	EER	ROC
0.01	0.0005	0.9995
0.02	0.0019	0.9996
0.03	0.0013	0.9965
0.04	0.0008	0.9966
0.05	0.0008	0.9990

6 Conclusions and Future Work

This paper examined the benefits and challenges of using biometrics as a means of identity verification and presented a multi-biometric encryption scheme as a solution to the different security and privacy issues faced by users of biometric authentication systems. The proposed scheme combines a variety of biometrics with the help of Arnold's Cat Map (ACM), a decimation process to induce aliasing, and a merging process to create cancellable templates. The obtained templates ensure randomness due to the utilization of the ACM fusion and aliasing strategies. The proposed system aims to reduce the time of the registration process and increase the reliability of the template change process. By calculating the EER and the AROC, the superiority of the proposed system is demonstrated. A comparative study of the proposed system with other ones has been presented. The simulation results obtained for performance evaluation show that the system is safe, reliable, and feasible as it achieves high AROC values in the presence of noise. Future work may include the development of new algorithms for security in healthcare applications. We will also take into consideration the investigation of the effect of complex channel degradations on the proposed system.

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 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] M. Kabatoff and J. Daugman, "Pattern recognition: Biometrics, identity and the state-an interview with john daugman,"*BioSocieties*, vol. 3, no. 1, pp. 81–86, 2008.

[2] N. Ratha, J. Connell and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[3] M. Dabbah, W. Woo and S. Dlay, "Secure authentication for face recognition," *IEEE Symp. on Computational Intelligence in Image and Signal Processing*, vol. 2, no. 4, pp. 121–126, 2007.

[4] C. Potter, G. Hancke and B. Silva, "Machine-to-machine: Possible applications in industrial networks," in *Proc. IEEE Int. Conf. on Industrial Technology (ICIT),* Cape Town, South Africa, pp. 1321–1326, 2013.

[5] C. Opperman and G. Hancke, "Using NFC-enabled phones for remote data acquisition and digital control," in *Proc. IEEE Africon'11,* Victoria Falls, Zambia, pp. 1–6, 2011.

[6] R. Serra, D. Knittel, P. Di. Croce and R. Peres, "Activity recognition with smart polymer floor sensor: Application to human footstep recognition,"*IEEE Sensors Journal*, vol. 16, no. 14, pp. 5757–5775, 2016.

[7] H. Ma, Z. Liu, S. Heo, J. Lee, K. Na *et al.,*"On-display transparent half-diamond pattern capacitive fingerprint sensor compatible with AMOLED display,"*IEEE Sensors Journal*, vol. 16, no. 22, pp. 8124–8131, 2016.

[8] L. Francis, G. Hancke, K. Mayes and K. Markantonakis, "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms," in *Proc. IEEE Int. Conf. on Internet Technology and Secured Transactions, (ICITST)*, London, UK, pp. 1–8, 2009.

[9] G. Hancke, K. Markantonakis and K. Mayes, "Security challenges for user-oriented RFID applications within the internet of things,"*Journal of Internet Technology*, vol. 11, no. 3, pp. 307–313, 2010.

[10] E. POP, "Multimodal biometric systems overview," *ActaTechnicaNapocensis Electronics and Telecommunications*, vol. 49, no. 3, pp. 1–17, 2008.

[11] X. Jing, Y. Yao, D. Zhang, J. Yang, M. Liet *et al.,* "Face and palm print pixel level fusion and kernel DCV-RBF classifier for small sample biometric recognition," *Pattern Recognition*, vol. 40, no. 11, pp. 3209–3224, 2007.

[12] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70–81, 2010.

[13] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in *Proc. IEEE Int. Conf. European Signal Processing*, Barcelona, Spain, pp. 554–558, 2011.

[14] 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. 201–219, 2011.

[15] A. Jain, K. Nandakumar and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 3, no. 5, pp. 1–17, 2008.

[16] S. Liu, C. Guo and J. Sheridan, "A review of optical image encryption techniques," *Optics & Laser Technology*, vol. 5, no. 7, pp. 327–342, 2014.

[17] Y. Zakaria, R. Nassar and O. Zahranet "Cancellable multi-biometric security system based on double random phase encoding and cepstral analysis," *Multimedia Tools and Applications*, vol. 78, no. 22, pp. 32333–32355, 2019.

[18] R. Soliman, M. Amin and F. El-Samie, "A double random phase encoding approach for cancellable cancellable iris recognition," *Optical and Quantum Electronics*, vol. 50, no. 8, pp. 1–12, 2018.

[19] A. Maha, H. Fatma and A. Mohamed, "Efficient storage and classification of color patterns based on integrating interpolation with ANN/SVM," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 947–978, 2020.

[20] M. Ahmad, W. Woo and S. Dlay, "Non-stationary feature fusion of face and palm print multi-model biometrics," *Neurocomputing*, vol. 17, no. 7, pp. 49–61, 2016.

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

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

[23] Y. Wangand 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*, Changsha, China, pp. 449–451. 2010.

[24] S. Lian, "*Multimedia Content Encryption Techniques and Applications*," Crc Press, Taylor & Francis Group, 2009.

[25] S. El-Khamy, M. Hadhoud, M. Dessouky, B. Salam and F. El-Samie, "Adaptive least squares acquisition of high resolution images," *International Journal of Information Acquisition*, vol. 2, no. 1, pp. 45–53, 2005.

[26] S. El-Khamy, M. Hadhoud, M. Dessouky, B. Salam and F. El-Samie, "Efficient implementation of image interpolation as an inverse problem,"*Journal of Digital Signal Processing*, vol. 15, no. 2, pp. 137–152, 2005.

[27] S. El-Khamy, M. Hadhoud, M. Dessouky, B. Salam and F. El-Samie, "Optimization of image interpolation as an inverse problem using the LMMSE algorithm," in *Proc. IEEE Mediterranean Electrotechnical Conf. (MELECON),* Dubrovnik, Croatia, pp. 247–250, 2004.

[28] S. El-Khamy, M. Hadhoud, M. Dessouky, B. Salam and F. El-Samie, "Sectioned implementation of regularized image interpolation,"in *Proc. IEEE Midwest Symp. on Circuits and Systems (MWSCAS)*, Cairo, Egypt, pp. 656–659, 2003.

[29] G. Dolecek and J. Suarez, "Improving alias rejection in comb decimation filters for odd decimation factors," in *Proc. IEEE Int. Midwest Symp. on Circuits and Systems (MWSCAS)*, Boston, USA, pp. 397–400, 2017.

[30] R. Nasiri and Z. Wang, "Perceptual aliasing factors and the impact of frame rate on video quality," in *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, Beijing, China, pp. 3475–3479, 2017.

[31] H. Ahmed, H. Kalash and O. Faragallah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption,"*Informatica*, vol. 31, no. 1, pp. 105–113, 2007.

[32] R. Deshpande, L. Ragha and S. Sharma, "Video quality assessment through PSNR estimation for different compression standards,"*Indonesian Journal of Electrical Engineering and Computer Science*, vol. 11, no. 3, pp. 918–924, 2018.