International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 339~348
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp339-348

Biometric iris templates security based on secret image sharing and chaotic maps

Marwa Fadhel Jassim[1], Wafaa mohammed Saeed Hamzah[2], Abeer Fadhil Shimal[1]
[1]Department of Control and Systems Engineering, University of Technology-Iraq, Baghdad, Iraq
[2]Department of Software, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received Feb 28, 2021
Revised Jun 22, 2021
Accepted Jul 2, 2021

Keywords:

Authentication
Biometric
Gabor filter
Recognition system
Secret image sharing
Segmentation
UBIRIS v1

ABSTRACT

Biometric technique includes of uniquely identifying person based on their physical or behavioural characteristics. It is mainly used for authentication. Storing the template in the database is not a safe approach, because it can be stolen or be tampered with. Due to its importance the template needs to be protected. To treat this safety issue, the suggested system employed a method for securely storing the iris template in the database which is a merging approach for secret image sharing and hiding to enhance security and protect the privacy by decomposing the template into two independent host (public) iris images. The original template can be reconstructed only when both host images are available. Either host image does not expose the identity of the original biometric image. The security and privacy in biometrics-based authentication system is augmented by storing the data in the form of shadows at separated places instead of whole data at one. The proposed biometric recognition system includes iris segmentation algorithms, feature extraction algorithms, a (2, 2) secret sharing and hiding. The experimental results are conducted on standard colour UBIRIS v1 data set. The results indicate that the biometric template protection methods are capable of offering a solution for vulnerability that threatens the biometric template.

Corresponding Author:

Marwa Fadhel Jassim
Department of Control and Systems Engineering, University of Technology-Iraq
Baghdad, Iraq
Email: Marwa.F.Alkubaissy@uotechnology.edu.iq

1. INTRODUCTION

Biometric authentication technique includes of uniquely verified people by using their behavioral or physical features, such as iris or face. The popularity of biometric system is quite high as it is a more trusted technique than systems that are based on password security. Since biometric systems are difficult to copy and no passwords are required to remember [1]. The biometric based authentication obtains data from an individual. Features set are extracted, and are compared to the features stored in the server database in which the action is executed based on the result of the comparison algorithm. Biometric recognition system provides a natural and reliable solution to identification problem [2]. Since the information of biometric is permanent and immutable, this information can be used to create a verification system. Nevertheless, if the biometric information is leaked, it is difficult to exchange the leaked biometric information. Consequently, the vital information requires ways for storing safely [3], [4]. In biometric authentication process, templates play a vital role. At first, biometric traits such as fingerprints and iris are captured by the sensor, using some feature transformation technique to extract the feature and convert it into digital form. This digital

information is known as biometric template which is stored in the database. Later on, the template is used in authentication step [5].

The template that is kept in the database may be exposed to eavesdropping which makes the protecting of it a challenging task in the biometric system. Because of these reasons, many researches used cryptography, stenography and watermarking for biometric data and template protection in the system [6]. Despite the biometrics advantages as an approach of identity verification, some concerns are raised because of the high sensitivity of biometric data: Information leakage poses a serious privacy threat. To solve these problems, secured templates must be kept or interchange for identification purposes only [7].

The proposed secret sharing system has generated shares which overcome the problem in traditional methods. The two generated shares can be hiding randomly in selected images from the public database, it then can store one of shares in the system database giving the other share to an authorised person (user). The security of system would be improved, since the attacker must have the ability to access the two shares. The rest of paper is structured such as following: In section 2, the related works is reviewed. Section 3 the proposed system is presented in detail. The experiential results are showed in section 4. Finally, the conclusions are listed in section 5.

2. RELATED WORKS

A different approach is offered to protect templates in business along with the goal of protecting instability, eliminating access, and being unable to link to a compromise. Revenkar *et al.* [5] applied visual cryptography to add extra layers of authentication to secure the iris template. Sonali *et al.* [8] proposed a system that divides the template of finger prints into different shares (two shares) using visual cryptography techniques, keeping one with the identity person and the other one stored in a database. Ankita *et al.* [9] proposed a biometric privacy using visual cryptography with pixel sharing, using fingerprint images where a private fingerprint image is separated into two host images and stored in a two-separate database. Sunhant *et al.* [10] used visual cryptography to divide original images into different images but the shares image does not guide any information about original one, and for added more security by using asymmetric watermarking. Rupali *et al.* [11] proposed that centraled database will be split by using secret sharing across different locations, this will reduce threats against the centralised database and reducing the size of database. Patel *et al.* [12] illustrated that it is desirable to modify biometric patterns to prevent the theft of them through transforming them through revocable and noninvertible transformations to create cancelable biometric templates. Ashish and Sinha [13] proposed an encryption approach for template security. A template protection scheme, which has proven safety and acceptable reputation, has remained elusive. Elena and Aikaterini [14] presented the most challenging concern that must be considered while layout security and privacy protocols for the authentication of biometric. They also described the chief threats against privacy-preserving biometric authentication systems and provided guidance on possible countermeasures to design secure and privacy-preserving biometric authentication protocols. Ashwaq and Zina [15] introduced a method for template protection which is merged between the chaotic shift keying (CSK) and visual cryptography (VC). They employed the CSK modulation for biometric template coding. Then, used (2, 2) VC for shares generation, these shares are stored in two separate servers of the database and then the identity of the private template does not detect through single share.

In 2018 [16] a method based on visual cryptography is presented to keep the biometric iris template. Hikal *et al.* [17] introduced an encryption method for preserving security to palm print image using hybrid chaotic maps. The proposed method performed a mixture of different chaos maps for a specific choice of the control parameters. The security analysis results confirmed the strengths of the suggested cryptosystem various attacks. Ashwaq and Suhad [18] suggested a (r, n) multiple secret image sharing using discrete Haar wavelet transform to encode m secret images into n noisy images that are stored on different servers. To retrieve m secret images r noise images are in demand. Wadood *et al.* [19] presented a multimodal approach to biometric template protection with fusion at score level using the templates of fingerprint and face. This approach includes two stages, enrollment and verification stages. During the enrollment stage, discrete wavelet transform (DWT) is performed on the face images embedding the features of fingerprint. Then, the inverse DWT is applied to get the watermarked image. Lastly, a hyper-chaotic map is employed to generate a key stream to cipher a watermarked image by block cipher method. Jae and Ik [20] introduced two cancellable schemes for template generation. The first scheme is to enhance the accuracy of the Dwivedi *et al.* method by the partial sort technique, and the second scheme is alignment-free which enhances the effectiveness of the Dwivedi *et al.* method. The suggested schemes fulfill four requests of the cancellable template generation which are irreversibility, revocability, diversity, and efficiency. Manisha and Kumar in 2020 [21] proposed a structure for production Cancellable biometric templates by visual secret sharing. In the proposed scheme, n different shares corresponding to a single biometric image are generated with the

assistance of n-1 other images called cover images. The generated Secret Shares are stored in a distributed manner instead of the original Biometric image. Shafiqua and Muddannavar [22] presented schemes to solve the problem of biometric security. At first implemented a watermarking to protect the integrity of biometric images. In particular, a watermark text image which accommodates the bio data of the person to be authenticated, is embedded in the iris image by interchanging the middle band coefficients using discrete cosine transform (DCT). At the second the VC technique is employed to safeguard the iris template by decomposing the original iris template into two shares.

3. PROPOSED SYSTEM

The proposed system emphasises on the preserved iris template by combining the secret image sharing and hiding approaches. The main component of the algorithm is employed (2, 2) secret image sharing to construct two shares, then hidden into two meaningful image shares which are kept later in separated database servers. If the hidden share is extracted, the template may not be revealed without the two shadows that are provided at the same time. The identity of the template cannot be revealed by one of these shares. Biometric model protection technologies are able to offer a solution to the vulnerabilities that threaten the biometric template. There are two modules in the proposed system: enrollment module and authentication module.

3.1. Enrollment module

The required biometric images are captured for authorised users to access the secure resource and then stored in the database. Enrollment module consists of three sub stages: i) generating template module that is a result of iris recognition system, ii) construction shares module and iii) hiding shares module. Figure 1 depicts the components of the proposed enrollment module.

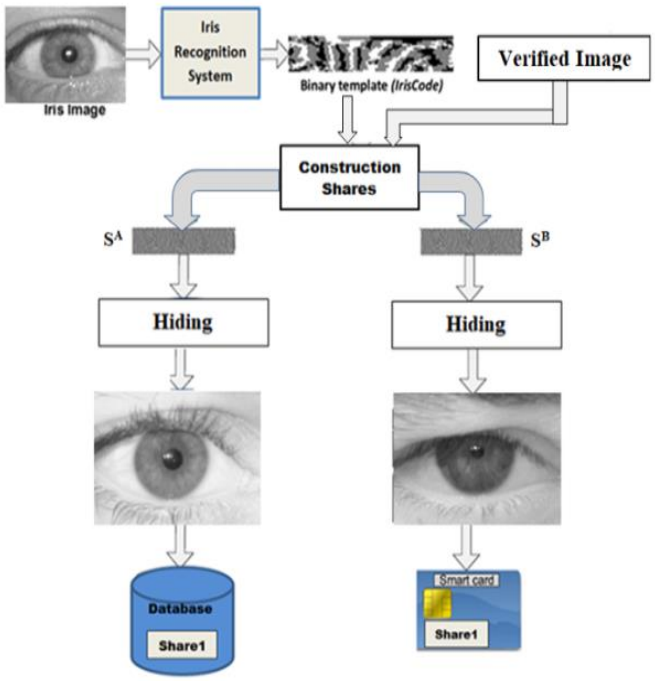


Figure 1. Enrolment module

3.2. Iris recognition system

The generating templates included the pre-processing, segmentation and extraction of feature techniques which have been essential to extract the iris characteristics. This was providing for the enrollment and then it is return to the next step in the proposed system. Figure 2 depicts the block diagram of generating templates.

Iris localisation is an active stage for iris recognition system; it is related to the exact localisation of iris borders. it has been decided to use daugman's integro-differential operator for localisation. Daugman's

algorithm is based on applying an integro-differential operator to find the iris and pupil contour [23]. The normalisation is accomplished using daugman's rubber sheet model [24] and the extraction of features is based on 1-D log gabor filter [25] to generate iris template.

3.3. Construction shares module

Current systems have included a single layer of validation for the biometric authentication system. Biometric templates are kept in a database and therefore are vulnerable to attack. The suggested system offers a double protection by an additional layer of validation to the templates stored in the database by using hybrid technologies. At this stage the generated secret templates will be encrypted into two shares. These shares appear as a noisy random set of pixels. The shares could be reformulated as natural images known as host images in the next step where each share is hiding into a fixed host image. The dealer generates two shadows, called S^A and S^B from template T and verified image V as shown in Figure 3. The algorithm 2 illustrated the construction shares steps.

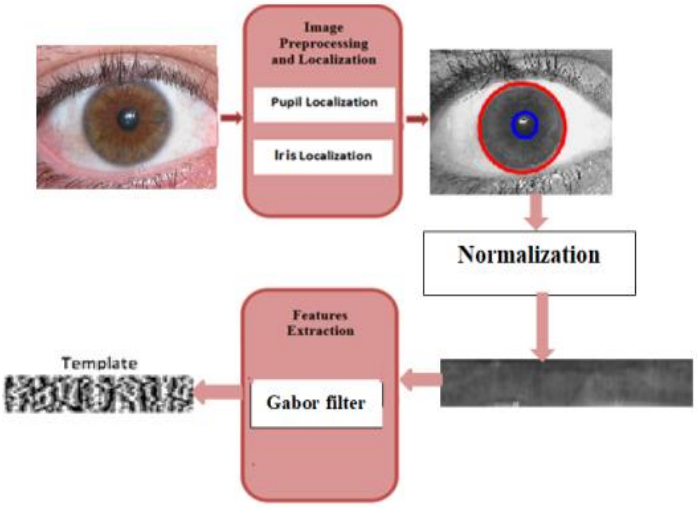


Figure 2. Iris recognition system

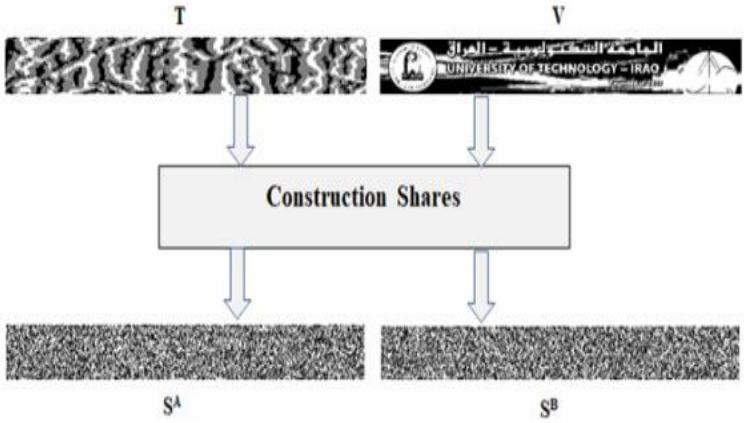


Figure 3 Construction shares

Algorithm 2. Construction shares

```
Input:
T, V, // template and verified image binary images
W, H // width and height
Output:
S^A, S^B
```

Step1: compute the pixel value of S^B share, using (1):
For i=1 to W
For j=1 to H
Read two pixels from V and T
Find pixel of share S^A, utilising (1):

$$S_{ij}^{A} = \left| \left((V_{IJ} \times 2 + T_{IJ} + 1) \bmod 4 \right) / 2 \right| \quad (1)$$

Step2: compute the pixel value of S^B share, using (2):

$$S_{ij}^{B} = \left| (V1_{IJ} \times 2 + T_{IJ} +) \bmod 2 \right| \quad (2)$$

EndFor j
EndFor i
Step3: generate random sequence *PixeOrd* of length W×H based on bernoulli chaotic map [26]
Step4: convert S^A and S^B to 1D arrays of length W×H
Step 5: apply pixels scrambling for S^A such as following:
For I=2: W×H

$$PixeOrd = abs(fix(PixeOrd(\mathrm{I}) \times 10^{\mathrm{DigNum}})) \quad (3)$$

// DigNum=5 if size of *T* is 128×128 (16384)
S^A (I)=S^A (*PixeOrd*);
EndFor
Reshape S^A to 2D array
Step6: repeat step 5 for S^B

The proposed share construction ensures that the generated shares are the same size of the original template and the verified images. On the other hand, they are like noisy images. These results indicate that they are capable to offer a solution to the vulnerabilities that compromises biometric templates.

3.4. Hiding shares

In this stage, two host images are selected from the public standard database. The Bernoulli chaotic map is employed to generate two random indices which are represented by the x's and y's coordinates. These generated coordinates are used to hide the bits of generated shares into two host images as presented in the following algorithm:

Algorithm 3. Share hiding

Input:
S^A, S^B, // two shares
W, H, // width and height of each shares
$HostImage_1$, $HostImage_2$ // two host images
Output:
$StegoImage_1$, $StegoImage_2$ // two stego images
Step1: Convert the S^A and S^B into two 1D sequences of length W×H
Step2: Generate two Random Sequences based on Bernoulli chaotic map Seq_1 and Seq_2. The Seq_1 is employed to become the Xs coordinates and other sequence Seq_2 is used as Ys coordinates. These generated coordinates are used as indices to hide the shares bits
Step3: Repeat step1 to generate Seq_3 and Seq_4 using different initial condition
Step4: Convert the generated Seq_1 and Seq_2 into integer using following formula:

$$IntSeq_1 = abs((round\ (Seq_1 \times 101) + 1)) \bmod 20 \quad (4)$$

// the range of $IntSeq_1$=1,.., 20

$$IntSeq_2 = abs((round\ (Seq_2 \times 1001) + 1)) \bmod 240 \quad (5)$$

// the range of $IntSeq_2$=1,.., 240
Step5: repeat step4 to generate $IntSeq_3$ and $IntSeq_4$
Step6: sort the two sequences $IntSeq_1$ and $IntSeq_2$ in descending order
Step7: hide the S^A and S^B in host images such as following:
For I=1 to W
For J=1 to H
$HostImage_1$ ($IntSeq_1$, $IntSeq_2$)=S^A (I, J)
$HostImage_2$ ($IntSeq_3$, $IntSeq_4$)=S^B (I, J)
Increment $ntSeq_2$
Increment $ntSeq_4$
Endfor J
Increment $IntSeq_1$
Increment $IntSeq_3$
Endfor I

3.5. Authentication module

Throughout the authentication phase, a request to the server is sent from a trusted entity which then the corresponding share is sent to it. On the other hand, four sequences $IntSeq_1$, IntSeq2, IntSeq3, and $IntSeq_4$ are generated at the receiver by using the same initial condition that is exploited at the transmitter to extract the bits of the S^A and S^B. Finally, the original template T and verified image are recovered as shown in the algorithm 4. Figure 4 shows the authentication module.

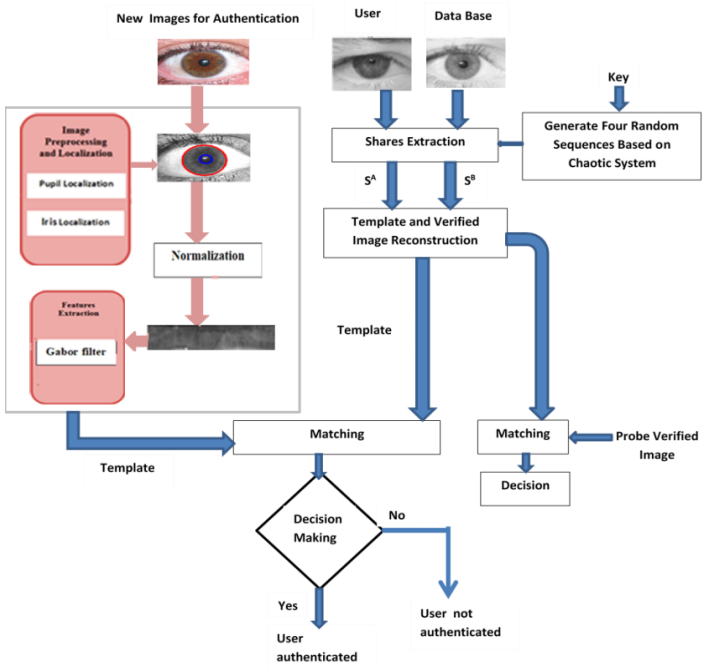


Figure 4. Authentication module

Algorithm 4. Template and verified image reconstruction

```
Input:
S^A, S^B, // 2D array of binary
W , H // width and height
Output:
T, V //original template and verified image
Step1: Generate random sequence PixeOrd of length W×H based on bernoulli chaotic map.
Step 2: Apply pixels rescrambling for S^A such as following:
For I=2: W×H
```

$$PixeOrd = abs(fix(PixeOrd\,(I) \times 10^{DigNum})) \quad (6)$$

```
/ DigNum=5 if size of T is 128×128 (16384)
S^A (PixeOrd)=S^A (I)
EndFor
Reshape S^A to 2D array
Step3: Repeat step 2 for S^B
Step4: For i=1 to W
      For j=1 to H
Read two pixels from S_ij^A and S_ij^B
Reconstruct pixel of template T using (7)
```

$$T = \left|\left(\left(S_{ij}^{A} \times 2 - S_{ij}^{B} + 3\right) mod\ 4\right) / 2\right| \quad (7)$$

```
Reconstruct pixel of Verified image using (8).
```

$$V = \left|\left(S_{ij}^{A} \times 2 - S_{ij}^{B} + 3\right) mod\ 2\right| \quad (8)$$

```
EndFor j
EndFor i
```

4. RESULTS

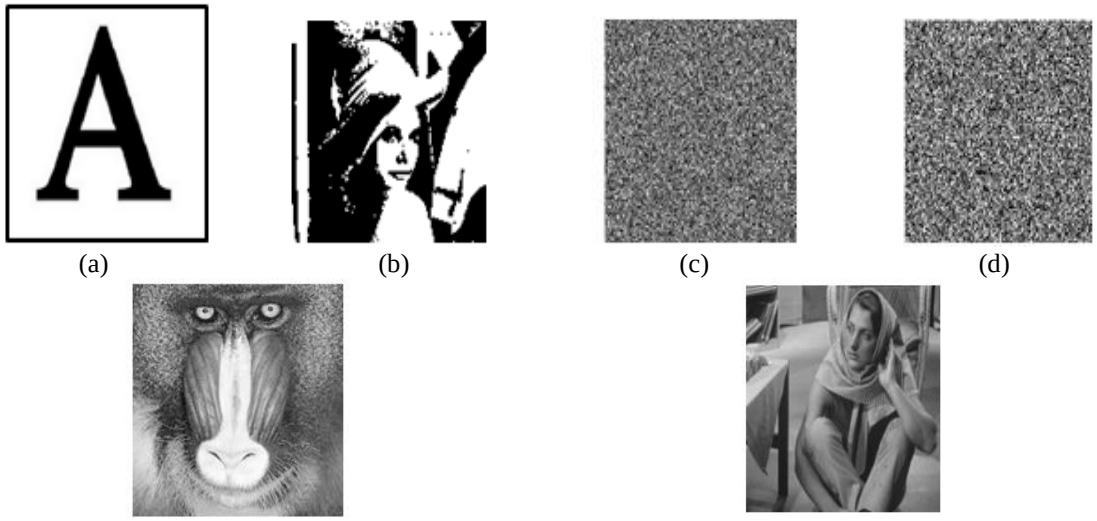
The visual quality (PSNR value) [27] of the stego images has been computed using (9). Figure 5(a)-(d) shows the secret images with 128×128 pixels and the corresponding generated shares SA and SB. The two cover images 'Baboon' and 'Barbara' with 512×512 pixels are used as host images as shown in Figure 5(e)-(f). Two shadow images are generated by algorithm 1 and then, the proposed system uses LSB method to hide each shadow image in the corresponding host image randomly using the random sequences that are generated by Bernoulli chaotic map. The experimental results are shown in Figure 6.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)(dB) \quad (9)$$

$$MSE = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(X_{ij} - X'_{ij})^2 \quad (10)$$

Figure 7 shows the experimental results of hiding shares SA and SB that are generated from share construction stage and two stego images from UBIRIS v1 data set with 300×400 pixels. As seen, all PSNR values of the stego images are larger than 51 dB. It is clear that the proposed system has an advantage in achieving acceptable visual quality.

Table 1 shows a comparison of the size for the original template *T* and verified image *V* with the constructed shares S^A and S^B as shown in Figure 3. Table 2 depicts the cross correlation between constructed shadows and plain images (T and V). As noticed, the correlation coefficients are very small (C≈0), which is recommended. The shadows are totally uncorrelated.



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

(e) (f)

Figure 5. The test images; (a) and (b) secret images, (c) SA, (d) SB, (e) and (f) host images

PSNR=53.67 PSNR=54.44

Figure 6. The generated stego images with the PSNR values

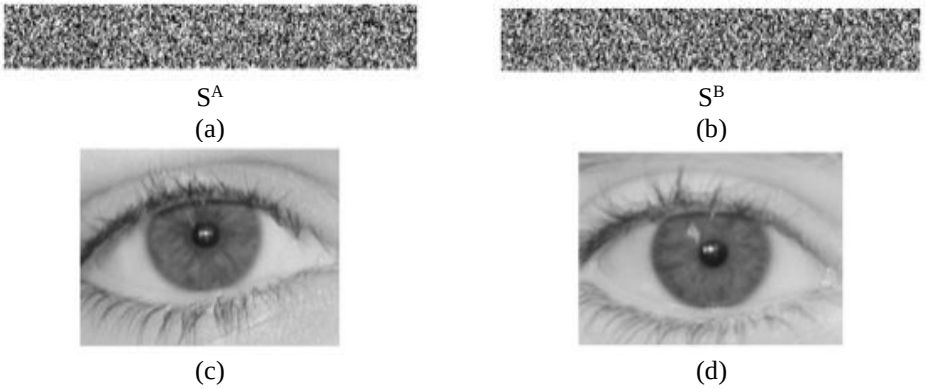


Figure 7. Shares constructing and hiding: (a) and (b) the generated shares, (c) and (d) the generated stego eye images with the PSNR values 51.45 dB, 51.67 dB respectively

Table 1. Comparison of size

Images	Binary Images Size
Original Template	19200 bits
Verified Image	19200 bits
S^A	19200 bits
S^B	19200 bits

Table 2. Cross correlation between constructed shares and plain images

Images	S^A	S^B
Template Image *T*	-0.0003	-0.0033
Verified Image *V*	0.0007	0.0002

The chaotic signal is described by its initial condition's sensitivity and the random behavior of the chaotic signals as well as its broadband spectrum, as it was thought that information could be efficiently hidden in chaos. Consequently, it is unattainable to foretell in the long term. This feature indicates that two signals from the same chaotic systems with little change in initial conditions diverge with increasing time, and it will become unrelated signals with each other, as illustrated in Figure 8.

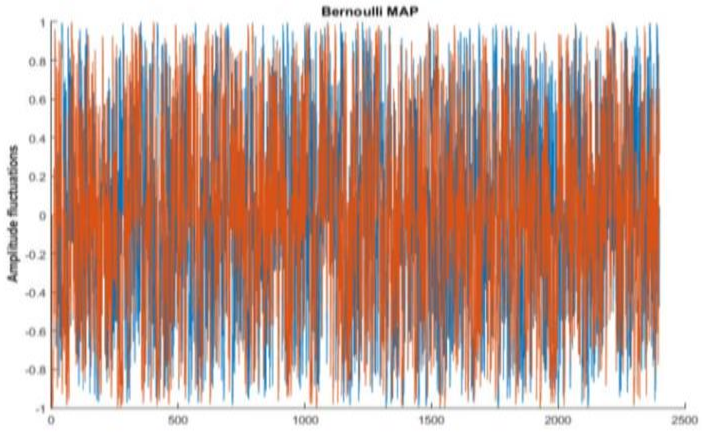


Figure 8. Initial conditions sensitivity

Figure 9 depicts that Burnoli chaos generator is exhibiting good autocorrelation properties, thus it is suitable for using in security applications. Figures 10 and 11 show the auto and cross-correlation between SA and the original template respectively. Figures 10 and 11 depict that the outputs characteristics are like to those of random additive white gaussian noise (AWGN).

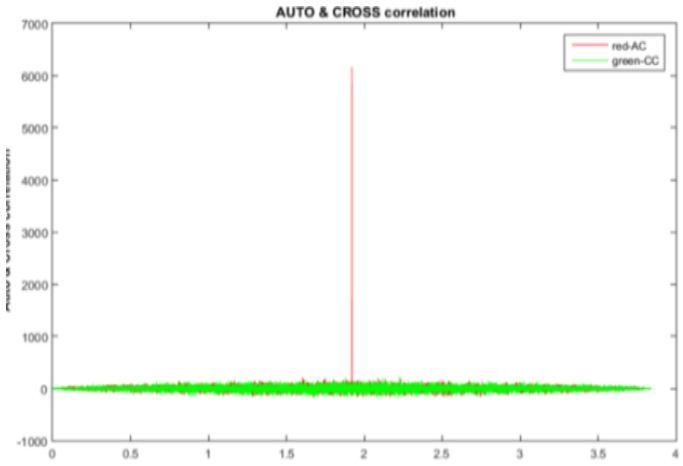


Figure 9. Performance of auto and cross correlation for burnoli chaos generator

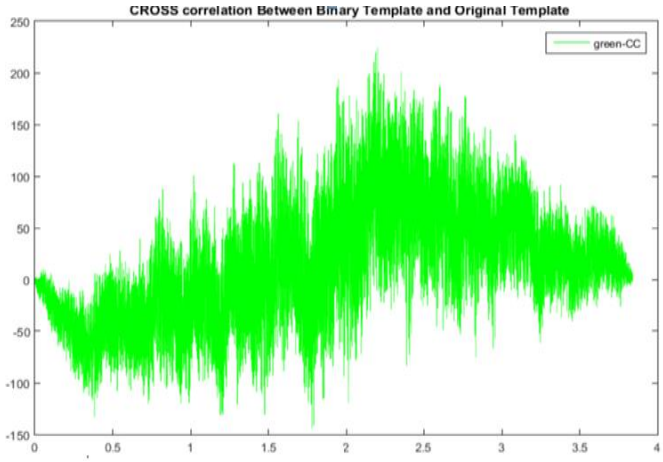


Figure 10. Cross-correlation between generated SA and original template

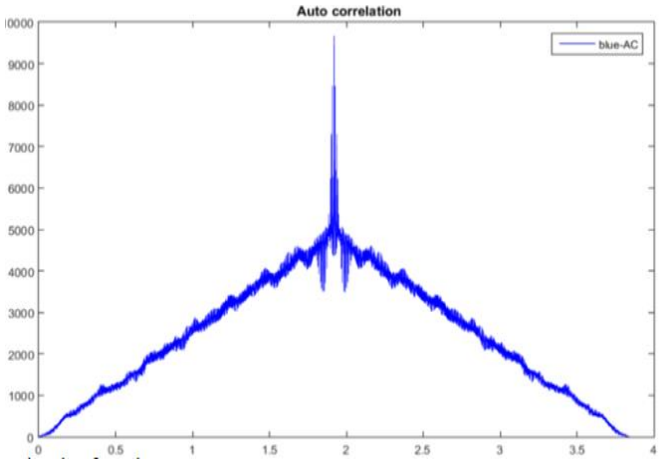


Figure 11. Auto correlation between coded and plain template

5. CONCLUSION

The proposed secret sharing technique is used to protect the template of the iris in the database and offer an additional layer of authentication for the existing iris authentication system. It is preserved the security of iris templates stored in a central database is maintained with robust data encryption technology

based on a chaotic map. The template is divided into two shares using (2, 2) secret sharing system. One is kept in the database and other with the user as the ID card. Security is provided to the iris template because using the only one share which is, hidden in meaningful image can be then stored in the database. No information can be retrieved for the enrolled eye image. In this case access from an unauthorised user is avoided. This system will be more secure and reliable in security-critical applications. The proposed secret sharing scheme allows the original iris template to be restored as soon as shadows are available, and thus does not impede iris recognition performance. An additional layer of security is presented to the iris template because the original template cannot be revealed even if any of the shares in the database or smart card is compromised.

REFERENCES

[1] A. Cavoukian, A. Stoianov, and F. Carter, "Biometric encryption: Technology for strong authentication, security and privacy," *Policies and Research in Identity Management*, vol. 261, pp. 57-77, May 2008, doi: 10.1007/978-0-387-77996-6_6.

[2] S. Omran and M. Salih, "Design and implementation of multi-model biometric identification system," *International Journal of Computer Applications*, vol. 99, no. 15, pp. 14-21, Aug. 2014, doi: 10.5120/17448-8255.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," in *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001, doi: 10.1147/sj.403.0614.

[4] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," in *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081-1088, Sept. 2006, doi: 10.1109/TC.2006.138.

[5] P. S. Revenkar, A. Anjum, and W. Z. Gandhare, "Secure iris authentication using visual cryptography," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 7, no. 3, Apr. 2010.

[6] P. Poongodi and P. Betty, "A study on biometric template protection techniques," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 7, no. 4, pp. 202-204, Jan. 2014, doi: 10.14445/22315381/IJETT-V7P244.

[7] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognition*, vol. 67, pp. 149-163, Jul. 2017, doi: 10.1016/j.patcog.2017.01.024.

[8] S. Patil, K. Tajane, and J. Sirdeshpande, "Secret sharing schemes for secure biometric authentication," *International Journal of Scientific and Engineering Research*, vol. 4, no. 6, pp. 2890-2895, Jun. 2013.

[9] A. Gharat, P. Tambre, Y. Thakare, and S. M. Sangave, "Biometric privacy using visual cryptography," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, vol. 2, no. 1, Jan. 2013.

[10] S. Kumar, M. Yadav, R. Pawar, and M. Patil, "Security using biometrics template and visual cryptography: a two fold approach," *International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)*, vol. 2, no. 1, pp. 10-15, Feb. 2015.

[11] R. S. Patil, S. Patil, and S. D. Thepade, "Secret sharing based secure authentication system," *International Journal of Computer Applications*, vol. 118, no. 22, pp. 8-11, May 2015, doi: 10.5120/20875-3613.

[12] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: a review," in *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54-65, Sept. 2015, doi: 10.1109/MSP.2015.2434151.

[13] Ashish and Sinha, "Biometric template protection," *Biometrics and Biostatistics International Journal*, vol. 1, no. 2, pp. 156-161, Jun. 2017, doi: 10.15744/2455-765X.2.102.

[14] E. Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: challenges and directions," *Security and Communication Networks*, vol. 2017, pp. 1-9, Oct. 2017, Art. no. 7129505, doi: 10.1155/2017/7129505.

[15] A. T. Hashim and Z. A. Saleh, "Visual cryptography and CSK for biometric template security," *Journal of Engineering and Applied Sciences*, vol. 13, no. 18, pp. 7642-7647, Jan. 2018, doi: 10.36478/jeasci.2018.7642.7647.

[16] C. Kant, R. Nath, and S. Chaudhary, "Secure iris recognition with visual cryptography," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 11, no. 4, pp. 9-20, Aug. 2018, doi: 10.14257/ijsip.2018.11.4.02.

[17] N. A. Hikal and M. M. Eid, "Anew approach for palm print image encryption based on hybrid chaotic maps," *Journal of King Saud University – Computer and Information Sciences*, vol. 32, no. 7, pp. 870-882, Sep. 2020, doi: 10.1016/j.jksuci.2018.09.006.

[18] A. T. Hashim and S. A. Ali, "Reversible multiple image secret sharing using discrete haar wavelet transform". *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 6, pp. 5004-5013, Dec. 2018, doi: 10.11591/ijece.v8i6.pp5004-5013.

[19] W. Abdul, O. Nafea, S. Ghouzali, and D. Tzovaras, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," in *The Computer Journal*, vol. 63, no. 1, pp. 479-493, Jan. 2020, doi: 10.1093/comjnl/bxz047.

[20] J. Y. Jeong and I. R. Jeong, "Efficient cancelable iris template generation for wearable sensors," *Security and Communication Networks*, vol. 2019, pp. 1-13, Jul. 2019, Art. no. 7473591, doi: 10.1155/2019/7473591.

[21] Manisha and N. Kumar, "On generating cancelable biometric templates using visual secret sharing," in *Advances in Intelligent Systems and Computing*, vol. 1230, p.p.532-544, 2020, doi: 10.1007/978-3-030-52243-8_38

[22] S. Noorain and M. L. Muddannavar, "Secured biometric Authentication of iris image using visual cryptography," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 6, pp. 281-284, Aug. 2020, doi: 10.35940/ijeat.F1393.089620.

[23] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, Nov. 1993, doi: 10.1109/34.244676.

[24] R. P. Wildes, "Iris recognition: an emerging biometric technology," in *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348-1363, Sept. 1997, doi: 10.1109/5.628669.

[25] D. J. Driebe, "The bernoulli map," in *Fully Chaotic Maps and Broken Time Symmetry*, vol. 4, pp. 19-43, 1999, doi: 10.1007/978-94-017-1628-4_3.

[26] R. C. Gonzales and R. E. Woods, "Digital image processing," 2nd Ed., Prentice Hall, 2006.

[27] H. Proenca and L. A. Alexandre, "Ubiris iris image database," in *International Conference on Image Analysis and Processing*, vol. 3617, pp. 970-977, 2005, doi: 10.1007/11553595_119.