Date of publication MAR-29, 2021, date of current version JAN-30, 2020.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.20.1.2095

Secure Verifiable Scheme for Biometric System based on Secret Sharing and CSK

ASHWAQ T. HASHIM
Control and Systems Engineering Department, University of Technology-Iraq, Baghdad, Iraq
(e-mail: 60102@uotechnology.edu.iq)

Corresponding author: Ashwaq T. Hashim (e-mail: 60102@uotechnology.edu.iq).

ABSTRACT Biometric templates stored in a database introduce a number of security and privacy risks. The requirements for an architecture that does not suffer from these risks are needed. Therefore, the reference information that is stored in the database must not give sufficient information to make successful impersonation possible. Also, the reference information must be retrieved as little as possible about the original biometrics; in particular it reveals no sensitive information. The proposed system introduces a novel method for template protection and a verification using the merging techniques of chaotic shift keying (CSK) and secret image sharing (SIS). The proposed architecture assures a complete protection framework for the biometric templates, which involves two phases: the first phase is to protect the ID image; a watermark ID image that includes the personal information embedded in the template using a novel watermarking algorithm to generate two shares, and then it is utilized to verify the accuracy of the revealed template. The second phase is for template protection, where the generated shares are encoded separately using CSK and then one share is stored in the database and the other kept with the user. The experimental and comparative results demonstrate that the proposed framework retains the protection of the template and preserves robustness to malicious attacks, while it does not have a discernible effect on the quality of the template.

KEYWORDS verification, biometric, template security, CSK, secret sharing, chaotic map.

1. INTRODUCTION

A major problem in any organization is the security management which is required to protect its copyrighted data or information. But the globalization and the wide spread of the Internet causes increased use of the information technology day after day. User verification is applied to everyone who wants to access that data in each organization to protect and maintain data privacy. An individual is authenticated to use the source or access the data only if his identity is properly verified and accepted [1].

Verification systems based on biometrics characteristics and data is one of the most important tendencies in the development of society. In the near future, biometrics systems will be everywhere in society, such as government, education, smart cities, banks, etc. Because of their uniqueness, characteristic biometrics systems will become more vulnerable, and privacy will be one of the most important challenges. Classic cryptographic primitives are not appropriate to ensure a strong level of privacy security [2].

Despite the advantages of biometrics as an identity verification technique, some concerns are raised because of the high sensitivity of biometric data: a leak of information poses a serious threat to privacy. To resolve these issues, protected templates must only be stored or exchanged for identification purposes [3].

The security issue is related to attackers who seek illegal access to protect the privacy of users, especially their biometric templates. The process of securing templates against probable identity theft caused a lot of research activity in the past decade [4].

Various recent developments in this area have exploited the advances in cryptography like homomorphic encryption [5], but still there are no general suitable solutions to produce secure biometric templates at the same time 1) non-invertible, 2) non-linkable, and 3) with high discrimination [6].

Numerous template protection methods are presented in the research alongside with the goal of safeguarding non-invariability, revocability; and non-link ability lacking compromise on the credit performance. James, D et al., in [7] proposed secure method for biometric templates protection by employing a visual cryptography approach and a 3D chaotic map. The combinations of these techniques are used to provide most appropriate solution to privacy or protection. Mohammed A. M. Abdullah et al et al. in [8] introduced a method to maintain image integrity of iris and template. Two layers are involved in the suggested approach. At first one, a watermark algorithm is employed to protect the integrity of the iris image; and at the second layer the iris template is protected by applying visual cryptography technique. Uma Verma et al. in [9] presented an approach for biometric templates protection using a hybrid scheme that takes advantage of the powerful method of the different template protection methods. A system of chaotic is employed for creating an authentic image which is kept in a central database as a replacement for the original image. Smitha Jacob et al., in [10] suggested a method to ensure an extra level of privacy by using both visual cryptography and chaotic encryption. The system provides a decryption/encryption process at extremely high speed and computational capability. Nithyakalyani et al., in [11] presented a scheme that encrypted the human fingerprint using DNA code properties and a chaotic logistics map with route cipher that would keep template privacy. Through digital testing and security analysis, the proposed algorithm proved to have a better encryption effect and a big key space and high enough sensitivity for secret keys. Yang W. et al. in [12] presented an inclusive overview where the latest developments in biometrics-based study are highlighted. The paper shows that researchers are still facing challenges of the biometric systems attacks, i.e., attacks on template databases and the user interface. How to design appropriate countermeasures to prevent these attacks and thus provide strong security while maintaining high accuracy of recognition, is the subject of hot research currently, as well as in the predictable future. In [13] an advanced version of the user authenticated key agreement approach that offers security improvement was suggested. Joshy et al., [14] in 2017, proposed a biometric verification system on the basis of IOT. The suggested scheme is based on recognition of iris, as it offers enhanced accuracy and security with comparison to other biometrics. For ensuring the verification the IoT is used. To offer security for information transmitted via the Internet they used a hybrid encryption algorithm that merges Blowfish and RSA algorithms. The two-step verification system offers improved security and reliability. In 2018, Riaz et al. [15] offered an overview and survey of various techniques of features transformation and biometric cryptosystems. They concluded that these techniques offered consistent biometric security at a high level. There are numerous techniques that offer verifiable security at workable application recognition rates. However, there are still many problems and challenges that are being encountered while deploying these technologies. Arjona et al. [16], in 2018, proposed a hybrid fingerprint matching approach on the basis of P-MCCs (Protected Minutia Cylinder-Codes) developed from images of fingerprint and PUFs (Physically Unclonable Functions) produced from SRAMs (Static Random Access Memories) device. By joining the fingerprint ID with the device ID results in a safe template the distinguishability, irreversibility, and non-cancellable characteristics are highly required for data privacy and security. The experimental results show the advantages of the suggested hybrid authentication mechanism in improving personal devices security using authentication schemes of biometric. Yang et al. [17], in 2019, made it clear that researchers still face challenges in addressing the two most serious biometric systems attacks, namely, attacks to the user interface and databases of template.

This paper is organized as follows: Section II presents the proposed method in detail, in Section III the performance of the proposed method is tested and discussed. Finally, the conclusions are presented in Section IV.

II. PROPOSED SYSTEM

The suggested system introduces a hybrid technique to securely stored and protected template in the database, as well as additional layer of verification. The proposed method consists of two phases: the *image hiding phase* using SIS and *coding phase* using CSK as illustrated in Fig. 1.

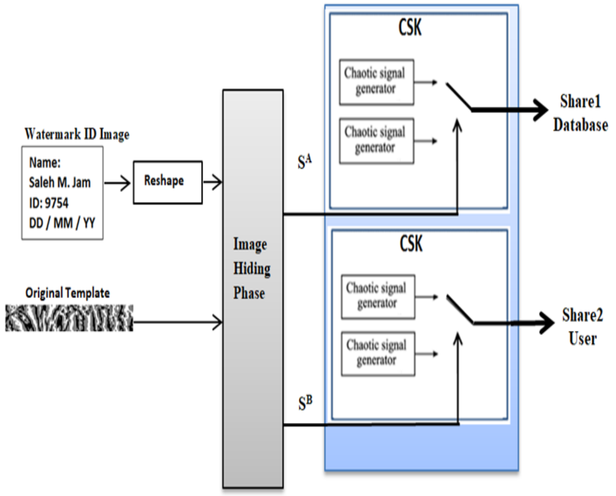


Figure 1. Block diagram of proposed system

A. IMAGE HIDING PHASE

In the suggested method a watermark ID image can be embedded into a template where each of which has a size of H×W then constructing two shadows which are used later to verify the reconstructed image. Checking to determine the consistency of all shadows before they are used to retrieve the secret ID image prevents incidentally or deliberately providing invalid data by a participant. The proposed method has low computation requirements, so it is appropriate for real-time applications.

Image hiding phase consists of four steps as illustrated in algorithm 1. Dealer initiates the activities of shares construction carrying out at bit-level using Eq. (1) and Eq. (2).

Dealer generates two shadows, called S^A and S^B, from the Watermark ID image *ImgID* and a binary template *T*. The resulted shares are then given to the next phase.

Algorithm 1: Image Hiding

```
Input:
      ImgID            // Watermark ID image (i.e., $S1_{ij}$)
      T                  // Template
      W, H                 // Width and Height of template
Output:
       $S^A$= ($S_{ij}^A$), $S^B$= ($S_{ij}^B$)
Step1:  For i=1 to W
             For j=1 to H
             Read two pixels from ImgID $_{ij}$ and $T_{ij}$
             Find pixel of share $S^A$, utilizing Eq.(1):

             $S_{ij}^A = \left\lfloor \left( \left( ImgID_{IJ} \times 2 + T_{IJ} + 1 \right) mod\ 4 \right) /2 \right\rfloor .$      (1)

             Compute the pixel value of $S^B$ share, using
             Eq.(2):

             $S_{ij}^B = \left\lfloor \left( ImgID_{IJ} \times 2 + T_{IJ} + 1 \right) mod\ 2 \right\rfloor .$      (2)

             EndFor j
           EndFor i
```

B. CODING PHASE

In this phase the CSK modulation idea is employed to encode generated shares S^A and S^B which are treated as signals to generate two noise signals = *Share1* and *Share2* based on CSK modulation as presented, in algorithm (2). The sent signal can be expressed as follows

$$S(t) = \begin{cases} Seq(t), & 1\ is\ transmitted \\ -Seq(t), & 0\ is\ transmitted \end{cases} . \qquad (3)$$

In the algorithm 2 two sequences are generated using chaotic shift keying. The two binary shares S^A and S^B are coded based on these two sequences using Bipodal Chaotic Shift Keying (CSK) [19] then the generated coded sequences are rounded to binary sequences.

Algorithm 2: Share Coding

```
     Input:
          $S^A$, $S^B$,                      // 2D array of binary
          width, height,
    Output:
          $BinShare_1$, $BinShare_2$         // 2D array of binary
     Step1: Convert $S^A$ and $S^B$ into 1D
                 Let L=1
                 For I ← 1.. width
                        For J ← 1.. height
                            $V_1$ (L) = $S^A$ (I, J)
                            $V_2$ (L) = $S^B$ (I, J)
                             Increment L
                        EndFor J
                 EndFor I
    Step2: Generate two random sequences $Seq_1$, $Seq_2$
         using Bernoulli's chaotic system [18].
    Step3: Coding the $S^A$ and $S^B$ using CSK.
               For I ←1.. width×height
                    IF $S^A$ (I)=1
                           $Share_1$ (I) = $Seq_1$ (I)
                    Else
                           $Share_1$ (I) = - $Seq_1$ (I)
                   EndIf
                   IF $S^B$ (I )=1
                           $Share_2$ (I) = $Seq_2$ (I)
                    Else
                           $Share_2$ (I) = - $Seq_2$ (I)
                   EndIf
             EndFor I
    Step4: The $Share_1$ and $Share_2$ are converted to
         binary by the following:
                 For I ←1.. Width × Height
                   $BinShare_1(I)$= Round ($Share_1(I)$ + 0.5)        (4)
                   $BinShare_2(I)$= Round ($Share_2(I)$ + 0.5)        (5)
               EndFor I
```

C. REVEALING TEMPLATE

For reconstructing the original template the reverse of each stage is performed as illustrated in Fig. 2.

Throughout the verification phase, a request to the server is sent from trusted entity then the corresponding share is send to it. On the author hand, two random chaotic sequences Seq_1 and Seq_2 are created at the receiver by using the same initial condition that is used for the transmitter, and then the S^A and S^B are recovered by the following algorithm (3) substeps:

Algorithm 3: Share revealing

```
Input:
        $BinShare_1$, $BinShare_2$,      // 2D array of binary
        $Seq_1$, $Seq_2$,                  // Two random chaotic sequences
        Width, Hight
Output:
       $S^A$, $S^B$
Step1: Generate two random sequences $Seq_1$, $Seq_2$
       using Bernoulli's chaotic system with the
       same secure initial conditions of share
       coding algorithm
Step2: Apply the following formula:
        R(I)=$Seq_1$(I)×Round( ($BinShare_1$(I)+ - 0.5)).
                                                       (6)
Step3: Convert to binary by thresholding
          For I←1.. Width×Height
                IF $R_1$ (I) > T)        // T is the threshold value
                              $S^A$ (I) = 1
                    Else
                              $S^A$ (I) = 0
                EndIf
         EndFor
Step4:  For I←1.. Width×Height
         $R_2(I)=Seq_2(I)\times Round((BinShare_2(I)+ -0.5))$,
                                                   (7)
                  IF R(I)  > T )        // T is the
threshold value
                        $S^B$ (I) = 1
                  Else
                        $S^B$ (I) = 0
                EndIf
         EndFor
```

The following example illustrates the coding and encoding shares stages in details.

-Example

- Share Coding Algorithm

-Let S^A in binary = 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 10 0 1 1 0 0 1 1 0 1 0 1 1 0 0 0

- Seq1 is generated by step2 based on chaotic map

Seq_1= -0.5025 0.0000 -1.0000 -0.9899 -0.9699 -0.9301 -0.8509 -0.6933 -0.379 0.2444 -0.5136 -0.0222 0.9559 0.9022 0.7954 0.5829 0.1601 -0.6815 -0.3561 0.2913 -0.4204 0.1635 -0.6747 -0.3426 0.3182 -0.3668 0.2701 -0.4624 0.0798 -0.8412 -0.6740 -0.3412

- Share1 is generated by step3 using CSK

- Share1= 0.5025 0.0000 -1.0000 0.9899 -0.9699 0.9301 -0.8509 -0.6933 -0.3797 -0.2444 0.5136 -0.0222 -0.9559 0.9022 -0.7954 0.5829 -0.1601 0.6815 -0.3561 0.2913 0.4204 -0.1635 -0.6747 -0.3426 -0.3182 -0.3668 -0.2701 -0.4624 0.0798 0.8412 0.6740 0.3412

-Convert Share1 to binary by step4

BinShare = 1 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 11

- Share Decoding Algorithm

- Seq1 generated by step 1

Seq_1= -0.5025 0.0000 -1.0000 -0.9899 -0.9699 -0.9301 -0.8509 -0.6933 -0.379 0.2444 -0.5136 -0.0222 0.9559 0.9022 0.7954 0.5829 0.1601 -0.6815 -0.3561 0.2913 -0.4204 0.1635 -0.6747 -0.3426 0.3182 -0.3668 0.2701 -0.4624 0.0798 -0.8412 -0.6740 -0.3412

-The output after applying step2

R1= -0.5025 0.0000 1.0000 -0.9899 0.9699 -0.9301 0.8509 0.6933 0.3797 -0.2444 -0.5136 0.0222 -0.9559 0.9022 -0.7954 0.5829 -0.1601 -0.6815 0.3561 0.2913 -0.4204 -0.1635 0.6747 0.3426 -0.3182 0.3668 -0.2701 0.4624 0.0798 -0.8412 -0.6740 -0.3412

-The output after applying thresholding by step3:

```
IF R (I) > T)     // T is the threshold value
    $S^A$ (I) = 1
Else
    $S^A$ (I) = 0
EndIf
```

-Decoding S^A = 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 0 1 1 0 0 0

This is corresponding to original S^A

Original S^A = 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 10 0 1 1 0 0 1 1 0 1 0 1 1 0 0 0

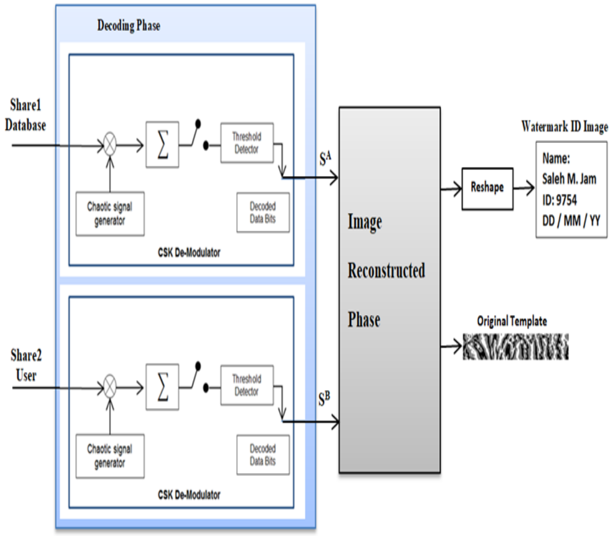


Figure 2. Block diagram of proposed revealing system

A decryption of the two shares S^A and S^B is performed to obtain the original template and watermark ID image using algorithm (4).

Algorithm 4: Shares Reconstructed

```
 Input:
     $S^A$, $S^B$,           // 2D array of binary
     W , H          // Width and Height
 Output:
      Template, ID       // Original Template and
watermark ID
Step1:  For i=1 to W
                 For j=1 to H
          Read two pixels from $S^A_{ij}$ and $S^B_{ij}$
          Reconstruct pixel of template using Eq.4.

     $Template = \left\lfloor \left( \left( S^A_{ij} \times 2 - S^B_{ij} + 3 \right) mod\ 4 \right) / 2 \right\rfloor.$   (8)

         Reconstruct pixel of watermark ID image
         using Eq.5.

               $ID = \left\lfloor \left( S^A_{ij} \times 2 - S^B_{ij} + 3 \right) mod\ 2 \right\rfloor,$
                                                   (9)
   EndFor j
EndFor i
```

III. RESULTS AND DISCUISSIONS

The suggested architecture is applied in Matlab 2015 b. In this section the results of the general achievements of the proposed system in terms of security, accuracy and pixel expansion criteria are discussed. An approach to iris segmentation, normalization using Daugmans Rubber Sheet Model [20], features extraction based on 1-D Log Gabor Filter [21] to construct biometric template is applied. The suggested system is tested on the templates that are generated after performing the above steps on MMU1 V1 dataset includes 45 classes [22]. The binary iris templates are 40×480. Fig. 3 depicts an example of template generation.

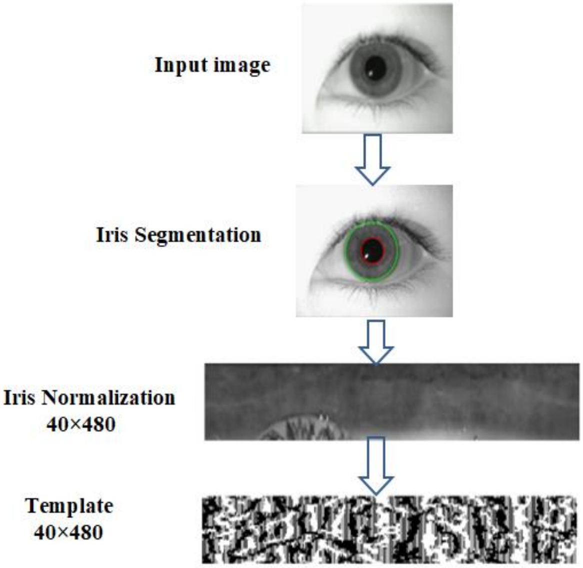


Figure 3. Template generation

The template and verification ID image which are used as the testing sample are shown in Fig. 4.

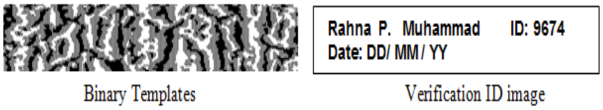

Rahna P. Muhammad ID: 9674
Date: DD/ MM/ YY

Figure 4. Test images

The sensitivity to initial condition and random-like behavior are important and valuable features of chaotic signals as well as their wide spectrum; the information could by concealed in chaotic signal effectively as a result is difficult to predict in the long term. By exploiting the merit of the sensitivity to initial condition a two different chaotic sequences could be generated with increasing time and become uncorrelated to each other from the same chaotic system by only slight change in the initial conditions as illustrated in Fig. 5.

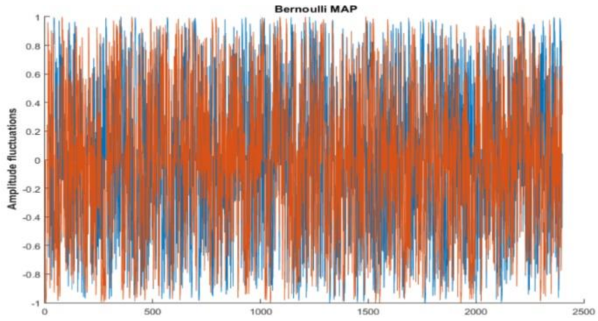


Figure 5. Sensitivity to initial conditions of two chaotic signals

Fig. 6 illustrates the performance of the auto- and cross correlation of the Burnoli chaos generator with various values of the initial state. It is clear that the Burnoli has the characteristics of an auto- and cross-correlation similar to that of random white noise, although its initial conditions vary only slightly. This shows that Burnoli can generate irrelevant sequences. Thus, the chaotic sequence generated is very sensitive to the initial condition. A slight difference in the initial condition will produce a totally different chaotic sequence.

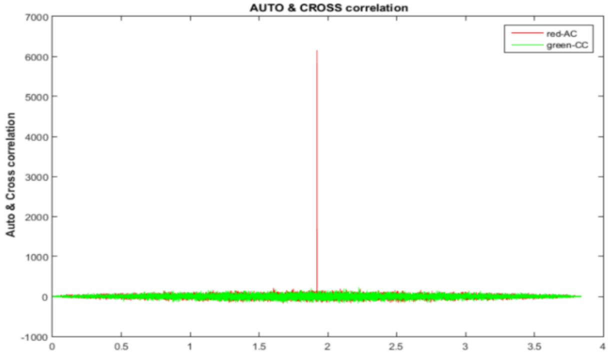


Figure 6. Auto correlation performance for Burnoli chaos generator

From Fig. 6 it is clear that the Burnoli chaos generator is exhibiting good autocorrelation properties, thus calling for its use in security applications.

The secret template and verification image ID are passed to the image hiding phase; the generated shares are depicted in Fig. 7.

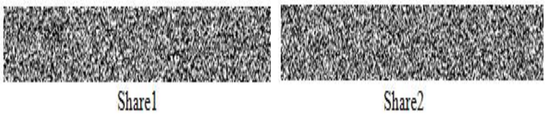


Figure 7. Resulting shares

Fig. 8 shows share$_1$ after applying antipodal CSK, while Fig. 9 and Fig. 10 show the auto- and cross- correlation between share$_1$ and the original template respectively.

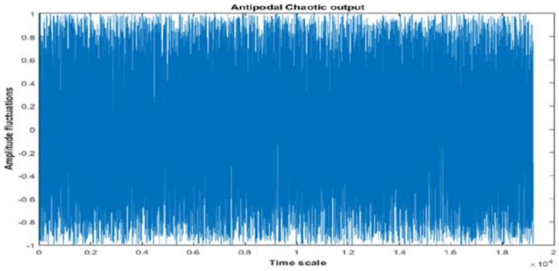


Figure 8. Encoded share$_1$ using chaotic shift keying

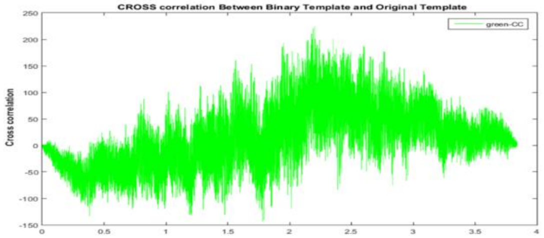


Figure 9. Cross-correlation between original template and coded share$_1$

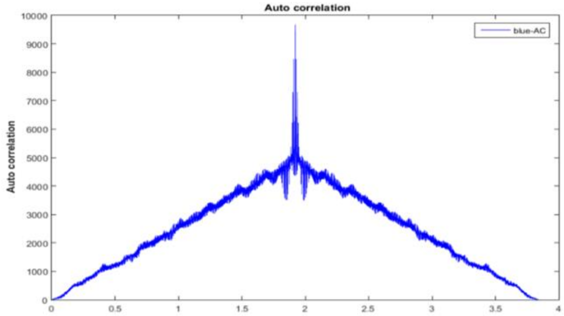
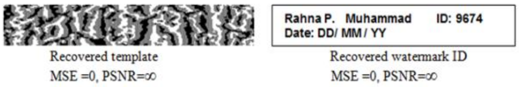


Figure 10. Original and coded templates cross correlation

Fig. 8 and Fig. 9 depict that the outputs characteristics are like those of random AWGN (additive white Gaussian noise) [23].

To ensure that the proposed scheme meets the security requirements, i.e., it entirely avoids any information about the original secret template, secret sharing method is used. This rearranges and confuses the constructed shared pixels after they have been generated. The CSK technique further ensures the security of the template. In our experiments, the peak signal-to-noise ratio (PSNR) is used to evaluate the reconstructed secret template. Fig. 11 illustrates the reconstructed original template and watermark ID image with PSNS=∞ and MSE=0.



Recovered template
MSE =0, PSNR=∞

Recovered watermark ID
MSE =0, PSNR=∞

Figure 11. Reconstructed images

The proposed approach creates two shares each of which is the same size as the original template. Table 1 shows a comparison of the size of the original template and that of the generated shares. As it is noticed the correlation coefficients are very small (C≈0), this means that the encryption template and generated shares are totally uncorrelated.

Table 1. Size Comparisons

Images	Binary images Size
Original template	19200 bits
Watermark ID image	19200 bits
Share1	19200 bits
Share2	19200 bits

Table 2. Cross correlation between generated shares and original images

Images	Share1	Share2	S^A	S^B
Template image	-0.0071	0.00046	-0.0058	0.0074
Watermark ID image	7.4395e-04	5.5724e-04	0.0051	-0.0059

Table 3 shows the entropies of shares, S^A, S^B, original watermark ID image and template. The highest entropy is *H* =1, which corresponds to an ideal case for binary image. Practically, the information entropies of encrypted images are less compared to the ideal case. To design a good image encryption scheme, the entropy of cipher image should be as close as possible to the highest value.

Table 3. Entropy test

Image	Entropy
Watermark ID image	0.59
Template	0.89
Share1	0.99
Share2	0.99
S^A	0.99
S^B	0.99

Using the CSK shares were produced for each 45 templates of 9600 bits by using different initial condition. Results from all statistical tests are given in Table 4. It shows that all P-values are greater than α (i.e., 0.1) value and the pass rate – the ratio of sequences passing the statistical test. The NIST [24] test is completely passed successfully. This shows very superior randomness properties of the generated sequences.

Table 4. NIST test for coded shares

NIST Statistical	Share1		Share1	
	P-value	Pass rate	P-value	Pass rate
Frequency (monobit)	0.132	450/450	0.278	450/45
Block-frequency	0.302	448/450	0.419	446/45
Cumulative sums (Forward)	0.551	447/450	0.187	442/45
Cumulative sums (Reverse)	0.221	442/450	0.201	443/45
Runs	0.092	448/450	0.088	446/45
Longest run of Ones	0.204	440/450	0.237	442/45
Rank	0.132	448/450	0.401	446/45
FFT	0.342	441/450	0.728	443/45
Non-overlapping templates	0.721	447/450	0.412	448/45
Overlapping templates	0.334	446/450	0.155	444/45
Universal	0.291	442/450	0.450	443/45
Approximate entropy	0.412	446/450	0.223	447/45
Serial 1	0.912	447/450	0.520	447/45
Serial 2	0.822	448/450	0.353	449/45
Linear-complexity	0.441	442/450	0.737	445/45

The proposed system has low computation requirements. The time consumed by the proposed system is 0.165 seconds and thus it is suitable for real-time applications.

IV. CONCLUSIONS

The secret image sharing approach to verification permits participants to be sure that no other persons have claimed their share contents. Preserving secure storage of templates in a central database currently is essential significance. To improve template security in biometrics authentication and ensure a higher level of security, efficient data encryption technology like CSK, is used. This paper introduces ways to produce protected biometric templates by employing the present secure technologies**.** For template protection, schemes are suggested that consist of two layers of security. The first layer includes the use of SIS to protect the template by analyzing the template into two, where one share is granted to the user while the other is stored in a database. At the second layer the CSK is used, which is a technique of involving bit-by-bit coding to generate a coded template and then store one of two shares in the database instead of the original template. The suggested SIS method permitted the template to be retrived exactly with the identical size and quality after the two shares are presented, and therefore does not thwart the performance of the recognition. As a result, a layer of security has been added to protect the inventory template. In this case, the genuine template could not be retrieved even with either of the two shares in the database or if the user is at risk.

References

[1] K. Dharavath, F. A. Talukdar, R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research*, India, December 26-28, 2013, pp. 1-7. https://doi.org/10.1109/ICCIC.2013.6724278.

[2] S. L. Nita, M. I. Mihailescu, V. C. Pau, "Security and cryptographic challenges for authentication based on biometrics data," *Cryptography*, vol. 2, issue 4, 39, pp. 1-12, 2018. https://doi.org/10.3390/cryptography2040039.

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

[4] K. Nandakumar, A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, issue 5, pp. 88-100, 2015. https://doi.org/10.1109/MSP.2015.2427849.

[5] M. Gomez-Barrero, J. Galbally, A. Morales, J. Fierrez, "Privacy preserving comparison of variable-length data with application to biometric template protection," *IEEE Access*, vol. 5, pp. 8606-8619, 2017. https://doi.org/10.1109/ACCESS.2017.2691578.

[6] A. K. Jain, K. Nandakumar, A. Ross, "50 years of biometric research," *Pattern Recogn. Lett.*, vol. 79, pp. 80-105, 2016. https://doi.org/10.1016/j.patrec.2015.12.013

[7] D. James, M. Philip, "A novel security architecture for biometric templates using visual cryptography and chaotic image encryption," *Proceedings of the International Conference on Eco-friendly Computing and Communication Systems ICECCS'2012*, 2012, pp. 239-246. https://doi.org/10.1007/978-3-642-32112-2_29.

[8] M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A framework for iris biometrics protection: A marriage between watermarking and visual cryptography," *IEEE Access*, vol. 4, pp. 10180-10193, 2016, https://doi.org/10.1109/ACCESS.2016.2623905.

[9] U. Verma, C. Kant, "Secure biometric template protection approach using chaotic maps," *International Journal of Advanced Research in Computer Science*, vol. 7, issue 3, pp. 121-124, 2016.

[10] S. Jacob, M. Baby, "Visual cryptography with chaotic encryption for biometric templates," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 5, issue 4, pp. 125-130, 2017.

[11] M. R. Nithyakalyani, V. Palanisamy, R. Anandhajothi, "Fingerprint template encryption scheme based on chaotic map and DNA sequence," *International Journal of Pure and Applied Mathematics*, vol. 118, issue 7, pp. 297-305, 2018.

[12] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, issue 141, pp. 1-19, 2019. https://doi.org/10.3390/sym11020141.

[13] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and secure biometric-based user authenticated key agreement scheme with anonymity," *Security and Communication Networks*, vol. 2018, pp. 1-14, 2018. https://doi.org/10.1155/2018/9046064.

[14] A. Joshy, M. J. Jalaja, "Design and implementation of an IoT based secure biometric authentication system," *Proceedings of the 2017 IEEE International Conference on Signal Processing Informatics Communication and Energy Systems (SPICES)*, 2017, pp. 1-13. https://doi.org/10.1109/SPICES.2017.8091360.

[15] N. Riaz, A. Riaz, and S. Khan, "Biometric template security: An overview," *Sensor Review*, vol. 38, issue 1, pp. 120-127, 2018. https://doi.org/10.1108/SR-07-2017-0131.

[16] R. Arjona, M. A. Prada-Delgado, I. Baturone, A. Ross, "Securing minutia cylinder codes for fingerprints through physically unclonable functions: An exploratory study," *Proceedings of the 2018 International Conference on Biometrics (ICB), Gold Coast*, Australia, February 20-23, 2018, pp. 54-60. https://doi.org/10.1109/ICB2018.2018.00019

[17] W. Yang, S. Wang, J. Hu, Z. Guanglou, C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, issue 141, pp. 1-19, 2019. https://doi.org/10.3390/sym11020141.

[18] Y. Seng Lau, *Techniques in Secure Chaos Communication*, Ph. D Thesis, RMIT University, School of Electrical and Computer Engineering Science, Melbourne, Victoria, Australia, February 2006.

[19] D. J. Driebe, "Fully chaotic maps and broken time symmetry," *Springer Science & Busines*, Media: Berlin/Heidelberg, Germany, 1999. https://doi.org/10.1007/978-94-017-1628-4.

[20] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis a nd Machine Intelligence*, vol. 25, issue 11, pp. 1148-1161, 1993. https://doi.org/10.1109/34.244676.

[21] R. P. Wildes, "Iris recognition: An emerging biometric technology," *Proceedings of the IEEE*, vol. 85, issue 9, pp. 1348-1363, 1999. https://doi.org/10.1109/5.628669.

[22] Multimedia University, Iris database. [Onine]. Available on: (http://www.persona.mmu.edu.my/~).

[23] A. Binti-Idris, R. F. Bin-Rahim, D. Ali, "The effect of additive white gaussian noise and multipath rayleigh fading on ber statistic in digital cellular network," *Proceedings of the International RF and Microwave Conference, Putrajaya*, Malaysia, September 12-14, 2006, pp. 97-100, https://doi.org/10.1109/RFM.2006.331046.

[24] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2001. https://doi.org/10.6028/NIST.SP.800-22.

__ASHWAQ T. HASHIM__ is working as Assistant Professor in Control and Systems Engineering Department, University of Technology Iraq, Baghdad, *Iraq. She obtained M.Sc. from computer science/ University of Basrah in 2003 and Ph.D. from University of Babylon in 2014. She published more than 35 papers in information security, pattern recognition, image compression and VHDL.*