Journal of Engineering and Applied Sciences 13 (18): 7642-7647, 2018
ISSN: 1816-949X

Visual Cryptography and CSK for Biometric Template Security

Ashwaq T. Hashim and Zina A. Saleh
Department of Control and Systems Engineering, University of Technology, Baghdad, Iraq

Abstract: Biometrics recognition systems are widely used in many areas of application, so, security and privacy vulnerabilities have attracted the attention of the biometric community recently. The stored reference data are prevented from detecting special biometric information and the security of biometrics systems are enhanced against attacks such as identity theft and cross matching by using template protection techniques. This study focuses on a template protection algorithm that combines between the methods from Chaotic Shift Keying (CSK) and Visual Cryptography (VC). The key component of the algorithm is to use CSK modulation for coding biometric templates into chaotic signal. Then, using (2, 2) VC to generate two shares, these two shares are stored in two separate servers of the database, so that, the coded template can be detected only when both shares are available at the same time also, the identity of the private template does not detect through single share. It is noted that the generated shares should be robust, uniformly distributed, collision-free and statistically independent for improving authentication performance and avoiding information seepage. Biometric template protection techniques are capable of solving the problem of the vulnerability that undermines the biometric template.

Key words: Verification, biometric, template security, CSK, secret sharing, visual cryptography, chaotic system

INTRODUCTION

Biometrics makes highest level of security over traditional methods like passwords and PIN numbers. Biometric is the study of automated identification by use of physical (fingerprint, iris, hand, dna, face, etc.) or behavioral (voice, signature, keystroke, etc.,) traits. Thus, the biometrics has no risk of forgetting it (Nithyakalyani *et al*., 2018).

There are many damaging attacks on a biometric system and one of the most these attacks is that related to the biometric templates stored in the system database. Attacks on the template can result in the following three vulnerabilities: the template can be exchanged with an impostor's template in order to make an unauthorized access. Physical spoof can be created from template in order to make unauthorized access to the system (in addition to other systems using the same biometrics (attributes) and the template can be restarted by matcher in order to make unauthorized access. The potential offense of biometric identifiers is cross-matching or function creep where biometric identifiers are used for purposes other than the prepared purpose. For example, a stolen fingerprint template can be used from a bank database to search a criminal fingerprint database or crosslink to a person's health records (Kisku *et al*., 2016).

Encrypting the templates (image) is the remedy to this susceptible attack. In practices, cryptography approach is usedfor encryption. In the area of cryptography, various algorithms such as DES, AES, IDEA, Rabin, Elgamal, RC4, ECC and Blow fish, etc. were designed in past years which is notefficient for practical image encryption due to high processing power and time complexity of encryption/decryption is high, high in data capacity and also high correlation among the adjacent pixels. The proposed new research algorithms of image encryption are aimed to limit repetitions in image content's by special processes for example, the chaos-based ciphers (Nithyakalyani *et al*., 2018).

The privacy of digital biometric data (e.g., iris template) that stored in a central database has become of major importance and it should be preserve. It demands high speed decryption/encryption process with restricted computational powers. In this research, the potential of using visual cryptography with chaotic encryption suitable is explored for adding security to biometric data such as fingerprint images. In this study a new way is proposed to preserve the biometric template protection. The template is coded by CSK then the coded template is protected by additional layer of Visual Cryptography (VC). In order for authorized users to recover the secret image, a matching between their shares and the corresponding shares stores on the server's database.

Literature review: Numerous template protection methods have been presented in the works alongside the

Corresponding Author: Ashwaq T. Hashim, Department of Control and Systems Engineering, University of Technology, Baghdad, Iraq

goal of safeguarding non-invariability, revocability and non-linkability lacking compromise/iknng on the credit performance

Revenkar *et al*. (2010) used visual cryptography to protect iris template by adding extra layer of authentication. The results indicate that by employing visual cryptography techniques to the iris template for adding greater safety, iris matching performance is not affected by an extra layer of authentication but the computation time of the iris authentication is slower which can be improved using another systems. Muhammed (2011) proposed a more secured system to improve biometric information privacy using (2, 2) VCS in which the templates are scrambled and analysed into two noise like images and they used XOR operator to put togeher the two noisy images to get the scrambled image. James and Philip (2012) introduced a security approach for biometric templates. They preserved the privacy of biometric image by exploring the use of visual cryptography and also they ensured protection as well as privacy for image using a fast encryption algorithm based on chaotic encryption. George (2013) suggested a simple and safe method to protect the biometric images through applying visual cryptography and chaotic encryption. She ensures that implementing a visual cryptographic scheme alone does not ensure complete privacy and protection of biometric images thus the shares are again encrypted by implementing chaotic encryption technique using 1D logistic map is used. Hajare *et al*. (2013) proposed a method for providing two fold securities to the iris template by using visual cryptography which provides an extra layer of authentication. They stored extracted image of the template and assigned a unique number to every template which is encrypted using visual cryptography. Supriya and Manjunatha (2014) introducedan approach depending on cancellable biometrics using chaotic maps which are known to own eligible properties of pseudo randomness, high allergy to initial conditions and very big key space. Abdullah *et al*. (2016) presented an improved security approch for protecting the security of iris images and templates by employing watermarking and Visual Cryptography (VC). The proposed approach provides a full protection for the iris biometrics which composes of two layers, the first layer is implemented by using a strong watermarking algorithm to protect the security of the iris image and the second layer is implemented using (2, 2) visual cryptography to protect the iris template. In this method the privacy of the iris images and templates are preserved while it does not have a distinct impact on the recognition performance. Verma and Kant (2016) improved the template security in biometrics authentication by using ways to produce protected biometric templates employing present technologies and cancellable biometrics. They proposed a hybrid schemes that benefit from the advantages of the various template protection ways. They secures a "Salted" template employing a biometric cryptosystem could have the gains of both salting and biometric cryptosystem approaches, they used a chaotic map to generate authentic image for storing in database instead of original image. Jacob and Baby (2017) proposed a novel method for ensuring additional level of privacy for the images using visual cryptography with chaotic encryption. It also provides high speed decryption/encryption process although the specific computational power. The use of original fingerprint images yielded an EER probe of 8%. It is noted that the threshold of 180 gives 9.13% of an EER. These experiments indicate the potential for decomposition and storage of a fingerprint image using VCS.MR. Nithyakalyani *et al*. (2018) proposed a new scheme in which the human fingerprint is encrypted using DNA code properties and chaotic logistics map with a path encoding that ensures the preservation of template privacy. Through digital experimentation and security analysis, the proposed algorithm proved to have a better encryption effect and a large master space and high enough sensitivity for secret keys. Furthermore, the proposed algorithm has the ability to resist all types of attacks such as comprehensive, statistical and differential attacks. All of these salient aspects illustrate that combining a 1D anarchic map with path encoding and DNA coding can be appropriate to document the fingerprint template effectively and safely.

Chaos Shift Keying (CSK): In binary chaos shift keying modulation, the binary information is transferred by chaotic signals which are taken different bit energies. The encoding of information signal is done by transmitting one chaotic signal $x_1(t)$ or $x_0(t)$ at a time. For example, at time t, if binary bit "1" of the information signal occurs, the chaos signal $x_1(t)$ will be transmitted and if binary bit "0" occurs, the chaos signal $x_0(t)$ will be transmitted. The modulation and demodulation of CSK are shown in Fig. 1. The two chaotic signals can be resulted from two distinct chaos systems or from the same system with various parameters. The transmitted signal can be given by Lau (2006):

$$X_1(t)S(t) = X_0(t)\begin{cases}1 \text{ is transmitted}\\0 \text{ is transmitted}\end{cases} \quad (1)$$

Chaotic system: A chaotic system is a deterministic system that shows non-linear systems behaviour with certain distinct features. There exists many definitions for the chaotic system, the simplest one is "A system that becomes aperiodic (non-linear) if its parameter internal, variable, external signals, control variable or even initial value is selected in a specified method" this unpredictable conduct of a deterministic system is known as chaos theory or chaos system (Driebe, 1999).

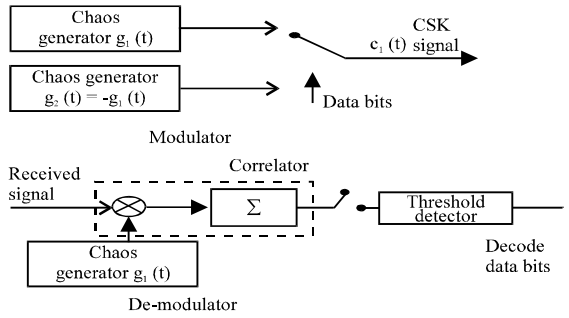

Fig. 1: Block diagram of modulator and demodulator for CSK (Lau and Hussain, 2005)

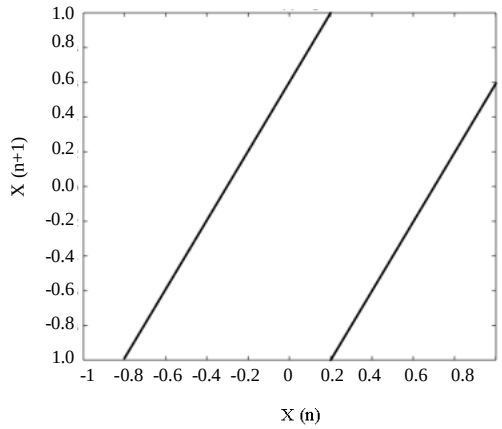

Fig. 2: The Bernoulli map

The Bernoulli map: The one-dimensional dyadic Bernoulli map acts in the phase space, M = (0, 1) of the unit interval. The dynamical law is $X_{t+1} = SB(X_t)$ where:

$$S_B(x) = 2x \bmod 1 = \begin{cases} 2x & 0 \le x < 1/2 \\ 2x-11/2 \le x<1 \end{cases} \quad (2)$$

The map is shown in Fig. 2. The uniform stretching factor of 2 means that this map has a global Lyapunov exponent of log 2. This system is not invertible since, S_B has two inverse branches: $(S_B^{-1})_1 = x/2$ and $(S_B^{-1})_2 = x/2+1/2$. It preserves Lebesgue measure in that the inverse image of an interval, say [a, b] where a<b<1 is the union of the two intervals [a/2, b/2] and [a/2+1/2, b/2+ 1/2] so that $\mu([a, b]) = b-a$ and $\mu(S^{-1}[a, b]) = b/2-a/2 +(b/2 + 1/2)- (a/2+1/2) = b-a$ (Chen *et al*., 2004).

MATERIALS AND METHODS

The existing systemis included one layer of verification to the biometric verification system. The templates are stored in database and thus they are vulnerable to attack. The proposed system suggested a method of hybrid techniques to protect the stored template in the database and obtain an additional layer of verification. The proposed method consists of two phases: template coding phase using CSK and share construction phase using VC as shown in Fig. 3.

Template coding phase: In this phase the CSK modulation idea is employed to encode template which is treated as signal to generate noise signal (encoded template) using algorithm 1. In this study, an antipodal CSK modulation technique is used. The sentsignal can be expressed as follows:

$$X_1(t)\, S(t) = \begin{cases} 1 \text{ transmitted} \\ -X_0(t), 1 \text{ transmitted} \end{cases} \quad (3)$$

Algorithm 1; Template coding:

Input:
Template //2D array of binary
W, H, //Width and Height of Template
Output:
B Coded Template // 2D array of binary
Step1: Convert Template into Vector
Set K = 1
For I = 1 to W
For J = 1 to H
V(k) = Template(I, J)
k = k+1
EndFor J
EndFor I
Step 2: Generation random sequence using Bernoulli
Set B = 1.99, A = 1, phin = 0.25
Let Seq(1) = (B × Seq) - A
For I = 2 to W×H
IF Seq (I-1)>0
Seq(I) = (B×Seq(I-1))-A
Else
Seq(I) = (B×Seq(I-1))+A
EndIF
EndFor
Step 3: Convert generated chaotic sequence to binary
For I = 1 to W×H
SeqBin = Round (Seq+0.5)
EndFor I
Step 4: Coding the Template Using Bipodal Chaotic Shift Keying
For I = 1 to W×H
IF Template (I) = 1
CodedTemplate (i) = Seq(i)
Else
CodedTemplate (I) = - Seq(i)
EndIF
EndFor
Step 5: Convert the Generated Coded Template to binary For I = 1 to W×H BcodedTemplate = Round(CodedTemplate+0.5) (4)
EndFor I

Shares construction phase: Visual cryptography schemes can be implemented to secure the coded template. Visual cryptography permits security an extra layer of authentication and authorization. The coded template is divided into two shares using suggested (2, 2) visual cryptography method as shown in algorithm 2. The size of the generated shares is the same size as the original template (i.e., 40×240).

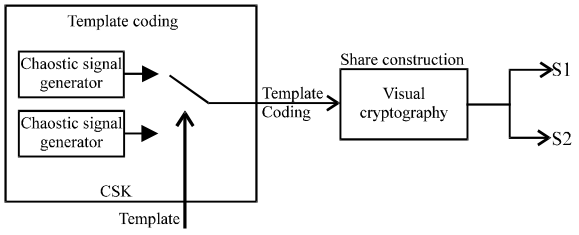

Fig. 3: Block diagram of proposed system

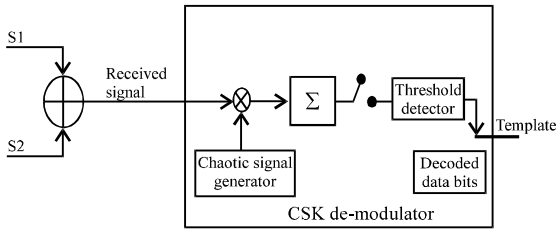

Fig. 4:The block diagram of proposed revealing

Algorithm 2; Shares construction:

Input:
CodedTemplate // A binary image
W // Image width
L // Image Height
Output:
S1 // Generated share 1
S2 // Generated share 2
Step 1: White pixel processing
Step1.1: In this substep set the pixel share combinations:
Set s1a = [0 1], s1b = [1 0]
Step1.2: Find the positions of white pixels in Coded Template and store them in two vectors X and Y
Step1.3: Count the number of white pixelslen
Step1.4: For I = 1 to len
Let a = X(I) and b = Y(I)
Pass s1a and s1b for random permuting the white share pixels generation pixShare using algorithm (2.1)
Set the white pixels in two generated shares
S1((a),(b)) = pixShare(2,1);
S2((a),(b)) = pixShare(1,1);
EndFor I
Step 2: Black Pixel Processing
Step 2.1: In this substep set the pixel share combinations:
Set s0a = [1 0], s0b = [1 0]
Step 2.2: Find the positions of black pixels and store them in two vectors X and Y
Step 2.3: Count the number of black pixelslen2
Step 2.4: For I = 1 to len2
Let a = X(I), = Y(I)
Pass s0a and s0b to for random permuting of the black share pixels generation pixShare using algorithm (2.1) Set the black pixels in two generated shares
S1((a), (b)) = pixShare(2,1),
S2((a), (b)) = pixShare(1,1),
EndFor I

Algorithm 3; Share generation:

Input
Sa, Sb // Two input binary vectors
Output
PSa,PSb // Two permuted output binary vectors
Step2: Set randNumber for random permutation using following formula:
randNumber= Round((rand*10)) mod 2(5)
Step3: IFrandNumberequal 0 then
Psa(1) = Sa(1)
PSa(2) = Sa(2)
PSb(1) = Sb(1)
PSb(2) = Sb(2)
ElseIFrandNumber equal 1 then
PSa(1)= Sa(2)
Psa(2) = Sa(1)
PSb(1) = Sb(2)
PSb(2) = Sb(1)
EndIF

Revealing template: To reveal the original template the inverse of each phase is applied as shown in Fig. 4. During the authentication process, the trusted entity sends a request to the server and the corresponding share is transferred to it. Then the two shares S_1 and S_2 are super imposed to reconstruct the encoded template coded template.

At the receiver the same random chaotic sequence Seq is generated using the same initial condition of that is used in sender and then the template is reconstructed using the following substeps:

Algorithm 4; Reconstrvcted template:

For i= 1 to W×H
OUT(i) = Seq(i)×Round ((CodedTemplate-0.5))
IF OUT(i)>T)//T is the threshold value
RTemplate (I) = 1
Else
RTemplate (I) = 0
EndIf
EndFor

RESULTS AND DISCUSSION

The extracted iris region is normalized into a rectangular block withradial resolution of 20 pixels andangular resolution of 240 pixels was selected for MMU1 data set. For normalization it has been used a technique based on Daugman's rubber sheet model. These encrypted parameters create a biological template that contains 9600 bits of information. Finally, from 1D Log-Gabor filters, the phase data was extracted and quantized to four levels to encode the unique pattern of the iris into a bit-wise biometric template. Some examples of encoded iris templates are showed in Fig. 5.

Chaotic signal is characterized by being a sensitive to initial condition and the random-like behaviour of chaotic signals as well their broadband spectrum. It was believed that information could be hidden effectively in chaos. So, it is impossible to predict in the long term. This merit indicates that the two signals from the same chaotic systems with little change in initial conditions diverge with the time growing and will become uncorrelated signals with each other as illustrated in the Fig. 6.

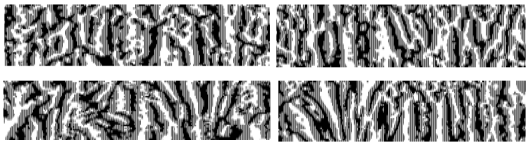

Fig. 5: Example of encoded Template of size 20×240 (9600 bits)

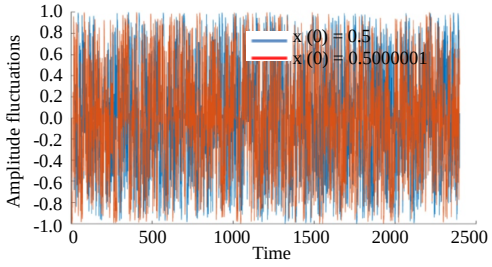

Fig. 6: Chaotic signals are sensitive to initial conditions: bernouili map

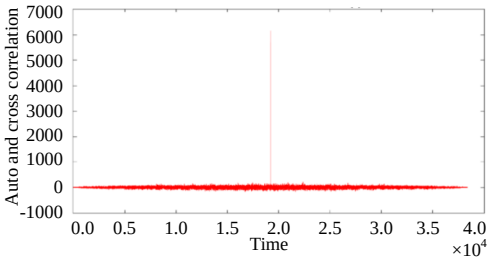

Fig. 7: Auto correlation performance for Burnoli chaos generator: Auto correction with initial condition x(0) = 0.5

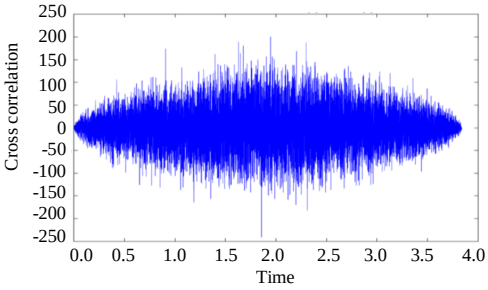

Fig. 8: Cross correlation performance for Bernoulli chaos generator: auto correction with initial condition x(0) = 0.5 and x(0) = (0.000005)

Figure 7 and 8 illustrate the auto and cross-correlation performance of the Bernoulli chaos generator with various values for the initial condition. It is very clear that Bernoulli chaos has auto and cross-correlation characteristics looks like those of random white noise in spite of the fact that their initial conditions are somewhat different. It can be concluded

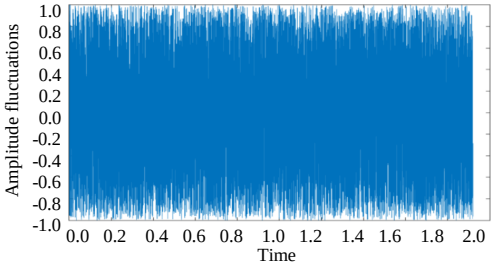

Fig. 9: Encoded template using antipodal CSK: antipodal chaotic output

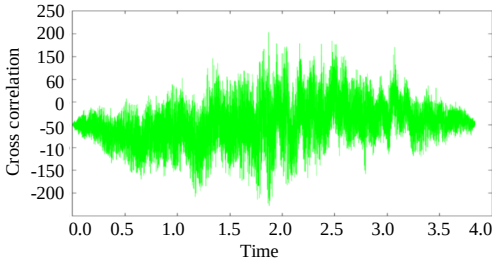

Fig. 10: Cross correlation between coded template and original template

that Bernoulli can generate sequences that are uncorrelated. Hence, generation of a chaos sequence is very critical to the initial condition. A completely different chaotic sequence will be generated from a little difference in the initial condition.

From Fig. 7 and 8 it is notice that the Bernoulli chaos generatoris exhibited good autocorrelation properties making a call for using in security applications. Fig. 9 depicts the encoded template (i.e., the first template in Fig. 5) after applying antipodal CSK while Fig. 10 depicts the cross correlation between encoded template and original template.

From Fig. 9 and 10 we are noticed that the characteristics of outputs look like those of random AWGN (Additive White Gaussian noise).

Using the CSK were produced 45 sequences of 9600 bits by using different initial condition. Results from all statistical tests are appeared in Table 1. It shows that all p-value are >α (i.e., 0.1) value and the pass rate the ratio of sequences passing the statistical test.The NIST (Bassham *et al*., 2010) test is completely passed successfully. This shows very good randomness properties of the generated sequences.

CONCLUSION

Preserving the security of templates (e.g., fingerprint/iris templates) that stored in a central database has become of fundamental importance. To improve

template security in biometrics authentication and ensure higher level of security an efficient data encryption technology like CSK, visual cryptography and chaotic map etc. is used. This study introduced ways to produce protected biometric templates employing present secure technologies. For template protection, schemes were suggested which consists of two layers of security. In the first layer the CSK is used which is a technique of bit by bit is coding to generate coded template and then visual cryptography for storing one of two shares in the database instead of original template. The second layer included the use of VC to protect the coded iris template by analyzing the coded template into two shares using (2, 2) VC where one share is granted to the user on a smart card while the other is stored in a database.The proposed VC scheme allows perfectly restore the iris template with the same quality and size when the shares are available and thus it does not hinder the iris recognition performance. For this purpose, an extra layer of security is introduced to the iris template because the original template cannot be recovered even if either of the two shares in the database or the smart card is compromised.

REFERENCES

Abdullah, M.A., S.S. Dlay, W.L. Woo and J.A. Chambers, 2016. A framework for iris biometrics protection: A marriage between watermarking and visual cryptography. IEEE. Access, 4: 10180-10193.

Bassham, L., A. Rukhin, J. Soto, J. Nechvatal and M. Smid *et al*., 2010. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Special Publication 800-22, Revision 1, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland. https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals, 21: 749-761.

Driebe, D.J., 1999. Fully Chaotic Maps and Broken Time Symmetry. Vol. 4, Springer, Boston, ISBN: 9780792355649, Pages: 164.

George, R.M., 2013. Facial template protection using extended visual cryptography and chaotic encryption. Intl. J. Technol. Emerging Eng. Res., 1: 94-96.

Hajare, N., A. Borage, N. Kamble and S. Shinde, 2013. Biometric template security using visual cryptography. J. Eng. Res. Appl., 3: 1320-1323.

Jacob, S. and M. Baby, 2017. Visual cryptography with chaotic encryption for biometric templates. Intl. J. Recent Innovation Trends Comput. Commun., 5: 125-130.

James, D. and M. Philip, 2012. A novel security architecture for biometric templates using visual cryptography and chaotic image encryption. Proceedings of the 2012 International Conference on Eco-Friendly Computing and Communication Systems (ICECCS'12), August 9-11, 2012, Springer, Kochi, India, ISBN:978-3-642-32111-5, pp: 239-246.

Kisku, D.R., P. Gupta and J.K. Sing, 2016. Advances in Biometrics for Secure Human Authentication and Recognition. Taylor & Francis, Abingdon, England, UK., ISBN:9781138033771, Pages: 352.

Lau, Y., 2006. Techniques in secure chaos communication. Ph.D Thesis, RMIT University, Melbourne, Australia.

Lau, Y.S. and Z.M. Hussain, 2005. A new approach in chaos shift keying for secure communication. Proceedings of the 3rd International Conference on Information Technology and Applications (ICITA'05) Vol. 2, July 4-7, 2005, IEEE, Sydney, Australia, pp: 630-633.

Muhammed, R.P., 2011. A secured approach to visual cryptographic biometric template. Intl. J. Inf. Technol., 2: 15-17.

Nithyakalyani, M.R., V. Palanisamy and R. Anandhajothi, 2018. Fingerprint template encryption scheme based on chaotic Map and DNA sequence. Intl. J. Pure Appl. Math., 118: 297-305.

Revenkar, P.S., A. Anjum and W.Z. Gandhare, 2010. Secure iris authentication using visual cryptography. Intl. J. Comput. Sci. Inf. Secur., 7: 217-221.

Supriya, V.G. and S.R. Manjunatha, 2014. Chaos based cancellable biometric template protection scheme-a proposal. Intl. J. Eng. Sci. Invention, 3: 14-24.

Verma, U. and C. Kant, 2016. Secure biometric template protection approach using chaotic maps. Intl. J. Adv. Res. Comput. Sci., 7: 121-124.