IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. IV (Sep. – Oct. 2015), PP 48-55
www.iosrjournals.org

A Novel Irreversible Transformation Scheme for Biometric Template Protection

Supriya V G, Dr Ramachandra Manjunatha
KSIT, ECE Department, VTU Research Scholar, Jain university, Bangalore- 560004, Karnataka, India
Professor, Jain University, Bangalore- 560004, Karnataka, India

Abstract: *Modern biometric technologies claim to provide alternative solution to traditional authentication processes. Even though there are various advantages of biometric process, it is vulnerable to attacks which can decline its security. In this paper, we propose a Novel Irreversible Transformation Scheme (ITS) to Secure Biometric Templates based on Chaotic Maps which are known to posses desirable properties of pseudo randomness, high sensitivity to initial conditions and very large key space. The simulation and analysis results shows that the proposed chaos based ITS is computationally simple compared to standard traditional cryptographic algorithms and provides better security performance.*

Keywords: *Biometrics, Security, Biometric Cryptosystems (BCS), Cancelable Biometrics (CB), Chaotic maps, Key stream.*

I. Introduction

Biometrics identify/verify an individual using his/her physiological or behavioral characteristics. Any Biometric process performs two activities namely enrollment & authentication process. During the enrollment process, the user's physiological or/and behavioral characteristics are captured by the sensitive sensor. Different feature extractors or key binding algorithms are used to create biometric template. This template stored during enrollment process is compared with the one produced during an authentication process using matching algorithm and matching result (yes/no) is produced. Based on the match response sent to the application, a decision algorithm grants or deny access to the user.

There are various application where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport, mobile phones, health and social services, etc., recent one being its usage in the Aadhar card or the Unique Identification card for the citizens of India The emerging need of present electronic cum computerized world is Security of Information and ensured personal privacy.

Most of the biometric systems store the extracted biometric template in a centralized database for authentication applications. From a privacy perspective, major concerns against the common use of biometrics are storage and misuse of biometric data. Since biometric characteristics are permanently associated with user, a compromise of biometric templates results in permanent loss of a subject's biometrics. Standard encryption algorithms compare biometric templates in decrypted domain and leave biometric templates exposed during every authentication attempt [1] which are vulnerable to attacks and can decline its security. Ratha et al [2] analyzed these attacks and grouped them into eight classes. The proposed paper considers only template database attacks like adding new template, modifying an existing template, removing template etc.

The different schemes proposed in the literature to protect template database from imposter can be broadly classified into two categories.

- Biometric Cryptosystem
- Feature Transformation

Biometric cryptosystems were originally developed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features, known as helper data-based methods. Biometric cryptosystems can be further classified as key binding and key generation systems depending on how the helper data is obtained.

- When the helper data is obtained by binding a key with the biometric template, it is referred as a key-binding biometric cryptosystem. Note that given only the helper data, it is computationally hard to recover either the key or the original template. Matching in a key binding system involves recovery of the key from the helper data using the query biometric features.
- When the helper data is derived only from the biometric template and the cryptographic key is generated directly from the helper data and query biometric features, it is referred as a key generation biometric cryptosystem.

Some template protection techniques make use of more than one basic approach [10].

In the feature transform approach, biometric template (T) is transformed appling transformation function (F) and only the transformed template [F (T; K)] is stored in the database. The parameters of the transformation function are typically derived from a random key (K) or password. The feature transform schemes can be further categorized as invertible and non-invertible transforms. In invertible transforms, an adversary gains access to the key and the transformed template, it can recover the original biometric template. Hence, the security of the invertible scheme is based on the secrecy of the key or password. On the other hand, non-invertible transformation schemes typically apply a one-way function on the template and it is computationally hard to invert a transformed template even if the key is known.

Bio-hashing or salting is one of the invertible transformation biometric protection scheme approaches, in which user specific key or password is used for transformation. In this approach key needs to store securely or password needs to be remembered by the user and present during authentication. [11]

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect biometric template. If a cancelable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancelable biometrics is non- invertible approach and provide a comparison of biometric templates in the transformed domain" [3]. The application of transforms provides irreversibility and unlinkability of biometric templates [4], which prevents the use of same captured template for other applications.

In this paper, A new Irreversible Transformation Scheme (ITS) to Secure Biometric Templates based on Chaotic logistic map is proposed. The chaotic logistic map systems give excellent pseudorandom sequences [5] and hence this map would be the best choice for the biometric template transformation algorithm. This is also evident from the related work [6,7,8].

Chaos theory is a field of study in mathematics which studies the behavior of dynamical systems that are highly sensitive to initial conditions

The properties of chaotic systems are:

- Deterministic i.e. they have some determining mathematical equations controlling their behavior.
- Unpredictable and non-linear i.e. they are highly sensitive to initial conditions. Even a very slight change in the starting point can lead to entirely different outcomes.

The highly unpredictable and random nature of chaotic output is the most attractive feature of deterministic chaotic system that makes it suitable to use in template transformation techniques.

Logistic Map is a one-dimensional chaotic map proposed by R.M.May [78]. It represents an idealized conservation model for describing yearly variation in the population of an insect specie. The population at $(n+1)^{th}$ year is related to that at the $(n)^{th}$ year by the following mathematical equation:

$$x_{n+1} = r * x_n [1 - x_n], \quad 0<x< 1 \qquad (1)$$

Where x_0 (n=0) is the initial value, r is the bifurcation parameter and depending on the value of r, x_0 the dynamics of the generated chaotic sequence can change dramatically. For $3.57 < r \leq 4$, the sequence is found to be non periodic and non-converging [9]. The function for probability density of logistic map is symmetric and proven in [15].

The rest of this paper is organized as follows: In Section 2 , literature concerned to Cancellable Biometrics is reviewed, discussed and open issues and challenges are presented. In section 3, a Novel Irreversible Transformation Scheme (ITS) to Secure Biometric Templates based on Logistic Map is proposed. In section 4, Algorithms efficiency is demonstrated through the results and investigating on its security through analysis including, key space analysis, Information entropy and key sensitivity analysis. Finally, conclusions are given in Section 5.

II. Literature Review

Reena Mary George[12] proposed method to protect Facial biometric templates by using visual cryptography and chaotic encryption. Author used visual cryptography on each private face image and decomposed into two public host images. The original image gets revealed only when both of these images are available simultaneously. Extra protection as well as privacy for these images is ensured by applying chaotic encryption onto each share. But author has not discussed about the performance of proposed method.

A recursive visual cryptography method proposed by Monoth et al., [13] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a visual cryptography technique proposed by Kim et al., [14] also suffers from computational complexity, though it avoids dithering of the pixels.

Zhang Yong [17], proposed Image Encryption with Logistic Map and Cheat Image in which author chooses the initial condition and control parameter of logistic map as the secret key. The author selects cheat image from the most common images in public network, together with the chaotic matrices generated by logistic maps, employed both in encryption and decryption processes to encrypt and recover the plain image. The experimental results presented states the key space of 10^{20}, high key sensitivity and good entropy of encrypted image.

Two Layer Chaotic Network Based Image Encryption Technique proposed by Anchal Jain et al.,[18] encrypt the image using two layer chaotic network in which first chaotic neuron layer realizes diffusion and second layer realizes substitution property. The author experimentally evaluated proposed technique in terms of brute-force attack, chosen or known-plaintext attack and statistical analysis. The results reveals key sensitivity of 2^{80} with uniform histogram.

Sanaa Ghouzali et.al.,[19], proposed Private Chaotic Biometric Template Protection Algorithm based on chaotic map for biometric authentication which allows the user to have control over the original template features provided by a unique user key (K). The author uses chaotic matrix (C) for the diversity requirement and both (K) and (C) are used to transform the original biometric template (T) into the protected template (Tp) which prevents database from having access to the original biometric template. The author validates the performance of this proposed scheme, by carrying out experiments on YALE and UMIST face databases using MATLAB to test privacy and diversity protection, and template revocability.

Face Template Protection Using Chaotic Encryption proposed by Weichun Cheng et. al.,[20] extracts the original template by Fisherface, then scrambles by the chaotic sequences generated based on logistic map in order to protect the privacy of original template. Author carries experimental results on ORL database consisting 40 individuals and 10 images for each person with different expression and presents FAR of 96.79 % and ERR of original template and disturbed template are 4.28% and 5.35%, respectively.

From literature survey major challenges need to be addressed can be summarized as:

- Need for a biometric template transformation algorithm such that if the biometric template in an application is compromised, the biometric signal itself is not lost forever and a new biometric template can be issued.
- Need for a biometric template transformation algorithm such that different applications are not able to use the same biometric template, thus securing the biometric signal as well as preserving privacy.

Proposed Novel Irreversible Transformation Scheme (Its) For Biometric Template Protection

The Biometric system works in two modes of operation. An Enrolment mode for adding transformed templates to a database, and Verification mode, where a transformed template is created for an individual and then a match is searched for in the database of pre-enrolled templates.

The model of the proposed Transformation scheme is shown in Figure 1. During enrolment, user biometric characteristics can be captured by suitable capturing device. The sample is then transformed using key streams derived from chaotic function and cryptography into a distorted biometric template. The distorted biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity.

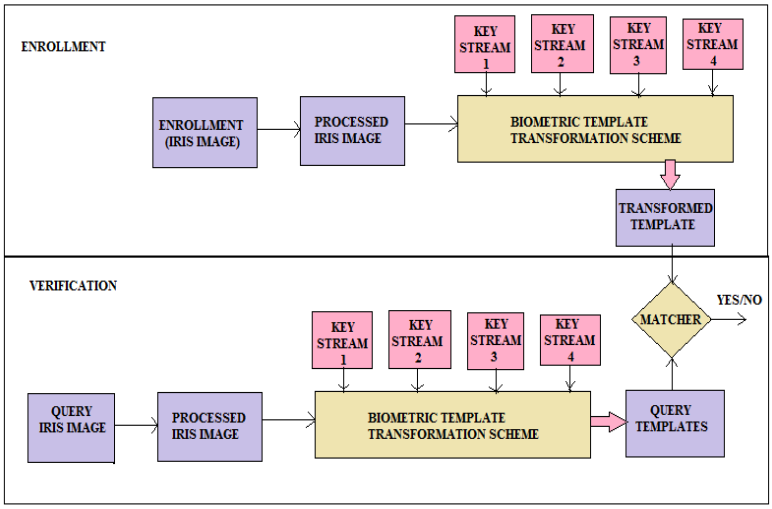

Fig.1 Over view of proposed template protection scheme

A. Enrollment Scheme

The proposed enrollment scheme as shown in Fig.1 consists of key streams and biometric transformation algorithm. Key streams form the important component in the proposed algorithm. The key streams are generated from the keys, using key stream generator which is explained in the section C. Key streams are generated using the chaotic logistic map equation. The key set used for generating the key streams is unique among each user.

Keys = {Key stream 1, Key stream 2, Key stream 3, Key stream 4}.

Key stream 1 is a Transformation key consisting of digital numbers; Key stream 2 is an index key consisting of digital numbers. Key stream 3 is a binary key & key stream 4 is a mixing key consisting of binary bits.

The first stage Cartesian transformation is applied on original biometric template data by using key stream 1 as explained in equation 2 & 3.

Let **TI (x, y) = Biometric template data**

TCT (x, y) = Cartesian Transformed template data

T1 (x, y) = T1 (x, y)/16 blocks = T1 (B1), T (B2),…….Bi **(2)**

TCT (x, y) = T (Bi) ⊕T1 [K4(x, y)], ⊕ =XOR **(3)**

The second stage of transformation algorithm is mainly based on confusion and diffusion. Permutation component is responsible for the actualization of the concept confusion. Diffusion is accomplished by the substitution component. The key stream 2 & key stream 3 are used for permutation of template data by considering whether digit is odd or even in key stream 2 & bit is 0 or 1 in key stream 3.

Key stream 4 is used for substitution of template data $\mathbf{T_{CT}(x, y)}$ by bit-wise XORing or XNORing with the key stream 4 and it is described in the equation 4 & 5.

Let $\mathbf{T_{ET}(x, y)}$**= Transformed template data.**

$\mathbf{T_{CT}(x, y)}$**= Cartesian Transformed Biometric template data**

$\mathbf{T_{ET}(x, y) = T_I(x, y) \oplus KS3(x, y)}$, **⊕ =XOR** **(4)**

either {KS2(x , y) = 1 and KS1(x, y) is even}

or {KS2(x , y) = 0 and KS1(x, y) is odd}

$\mathbf{T_{ET}(x, y) = T_I(x, y) \oplus KS3(x, y)}$, **⊕ =XNOR** **(5)**

either {KS2(x , y) = 1 and KS1(x, y) is odd}

or {KS2(x , y) = 0 and KS1(x, y) is even}

where KS denotes Key stream, x = 1, 2, 3,……..M and y = 1, 2, 3,……..N

B. **Verification Scheme**

The block diagram of Verification scheme is as shown in Figure.1. Biometric template transformation algorithm is just same as explained in Section A using same key streams. The transformed template data is bitwise compared with user transformed biometric template data stored in database during enrollment and output is used for providing authentication.

C. **Key Stream Generator**

Key stream generator is as shown in Figure. 2. Logistic map is used for generating chaotic real valued discrete sequence by selecting a key.

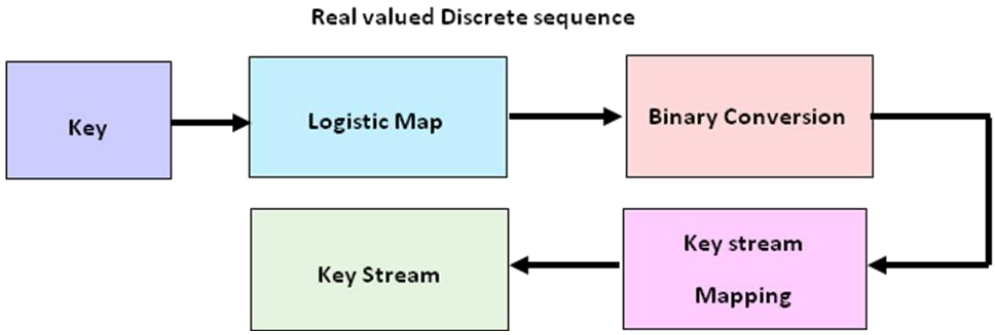

Fig. 2 Flow Chart of Key Stream Generation

The most commonly used chaotic map is Logistic map equation [5, 6, 7] is given by,

$$X_{n+1} = r * x_n [1+ x_n], \qquad 0<x<1 \qquad (6)$$

Where x0 (n=0) is the initial value, r is the bifurcation parameter and depending on the value of r, x0 the dynamics of the generated chaotic sequence can change dramatically. For $3.57 < r \leq 4$, the sequence is found to be non periodic and non-converging [9]. The probability density function of logistic map is symmetric [5] and hence the binary conversion is done by using equation 7.

$$b_i = 0 \text{ for } x_n < 0.5 \quad \text{and} \quad b_i = 1 \text{ for } x_n \geq 0.5 \qquad (7)$$

Where $0 < i < n$, n = length of the chaotic sequence.

The key = {key1, key2, key3, key4} is composed of four sub-keys, where each sub key is of the form sub-key = {Initial Value, r value}. Sub-key1 is used for generating keystream1, sub-key2 is used for generating keystream2, sub-key3 is used for generating keystream3 and sub-key4 is used for generating keystream4. Key stream 3 and Key stream 4 is as shown in equation 8.

$$\text{Key Stream 3} = \text{Key Stream4} = b1, b_2, b_3, \ldots b_n \quad \text{where } b_n \in [0,1] \qquad (8)$$

Key stream mapping for generating keystream1and key stream 2 is as shown in equation 9 &10.

Key Stream 1 = Key stream 2 = $D_1, D_2, D_3, \ldots\ldots D_j$, Where D = Decimal Number

$$D_1 = b_1,b_2,\ldots\ldots\ldots..b_k, \quad D_2 = b_{k+1},b_{k+2},\ldots\ldots\ldots b_{2k} \ldots. D_J \qquad (9)$$

Where J = 0, 1, ….(MXN).

$$\text{Key stream 2} = D_1, D_2, D_3, \ldots\ldots D_j, \quad \text{Where } J= 0,1,\ldots\ldots..(MXN)/16 \qquad (10)$$

Thus the KS1 = KS2 = $\{D_1, D_2,\ldots\ldots D_J\}$, Where D_1, $D_2\ldots$etc denotes decimal numbers obtained by combining k-binary numbers for each streams respectively. Thus if the template to be transformed is of size MxN then required length of key stream 2 and key stream 3 which is used for permutation is MXN and the range is [0, 1], the required length of keystream1 which is used for bitwise XOR^{ring} or $XNOR^{ing}$ (i.e. substitution based on permutation) is MxN and the range is [0, (MxN)-1].

Since the keystream2 is used for position permutation, during the key stream generation it must be guaranteed that there is no duplicate element in the two streams by discarding the repeated sequence as explained in section D.

D**. Unique Permutation Key Selection**

In order to achieve the uniqueness in the permutation key stream1, look up table based selection is done as shown in the Figure. 3.

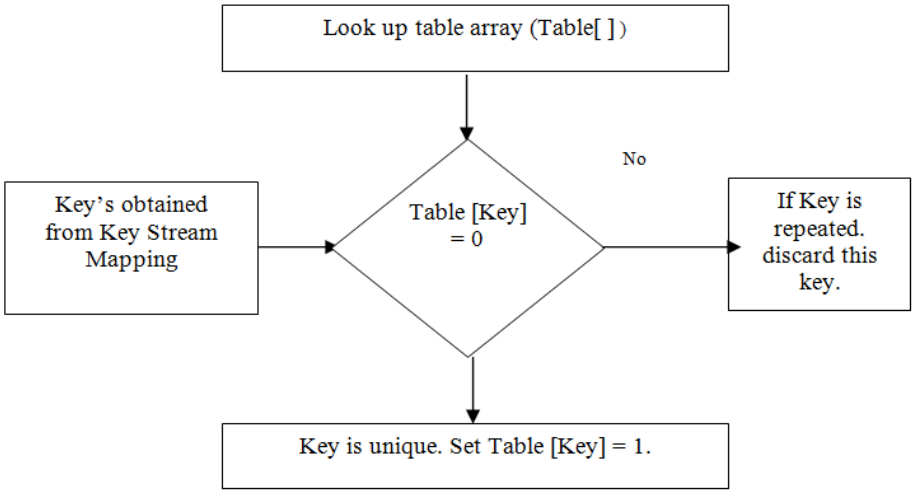

Fig.3. Unique Key Selection

Here the key stream2 generated from the key stream generator is taken as the input. A look up table with the key stream1 of size M x N is taken and filled with zeros. This table acts like a flag array. Each key from the key stream2 is checked for the corresponding flag in the table. If the flag is zero, it means that we have not come across that key in the key stream. Thus this key is retained in the key stream, and the corresponding bit in the table is set. If the same key is encountered for the second or successive times, as the flag bit corresponding to that key was set on the first occurrence indicating the key is not unique and is repeated, it is discarded. Thus duplicate element in the key stream is discarded and permutation key stream is made unique.

III. Experimental Results

For the experimental analysis of the proposed work, the Iris database in [22, 23] which contains 109 images obtained from different persons with 2 images each was utilized for evaluation. Biometric templates of size 20 X 480 were created using MATLAB source code in [21]. The bifurcation factor r value is taken as 3.89 and key is given as shown in table1. The proposed algorithm was implemented using template as shown in Figure 4 and histogram of input template is as shown in Figure 5. After transformation, the transformed biometric template stored in database is shown in Figure 6 and histogram of transformed template is shown in Figure 7 and Figure 10. The average entropy of transformed templates for 100 samples were found to be almost equal to ideal entropy which is equal to 1. The result has been tabulated in Table 1 and Table 2, result of authentication is checked with correct and wrong keys. There were three different evaluations implemented in this work.

4.1 Evaluation 1: Key space analysis

Considering most commonly used PC platform as an example, the computation precision is 16 decimal digits, therefore a chaos-based cryptosystem can only provide $10^{16} \approx 2^{53}$ size key space, which is a little smaller than DES(2^{56}) and by far smaller than AES(2^{128}). Since key = {key1, key2, key3, key 4} and is composed of three sub-keys with each key consisting of key = (x_0, r_0), initial value and bifurcation factor, the key space size is $\mathbf{(10^{16})^8 = 2^{425}}$, which is larger than the acknowledged most secured AES algorithm. Besides, the scheme is secure against known/chosen-plaintext attack [24], since it adopts both permutation and substitution operations.

4.2 Evaluation 2: Information entropy

Entropy of a random biometric template source is expected to be 1 for iris template in which each pixel is 1-bit. Normally it is observed that the input template entropy is low for biometric templates. The entropy of transformed biometric template stored in database was found to be 0.9991, which is close to the theoretical value. And hence it is observed that the entropy of the transformed biometric template stored in database of the proposed scheme is very close to the ideal one.

4.3 Evaluation 3: Key sensitivity

A good cancelable biometric transformation scheme should be sufficiently sensitive to small changes in the key. In the proposed scheme with a small change in the key it is not possible to get the transformed user biometric template. This was observed by selecting the wrong key as shown in Table 2.

Fig. 4. Input Template

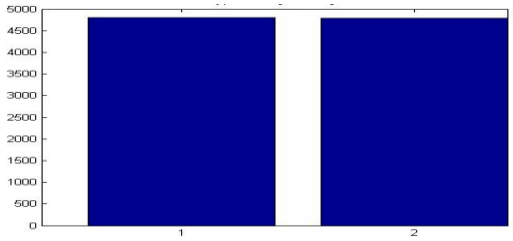

Fig. 5. Transformed Template Histogram

Fig. 6. Transformed Template

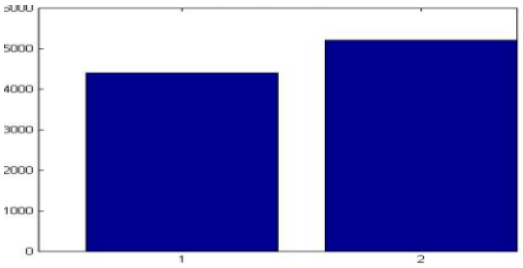

Fig. 7. Input Template Histogram

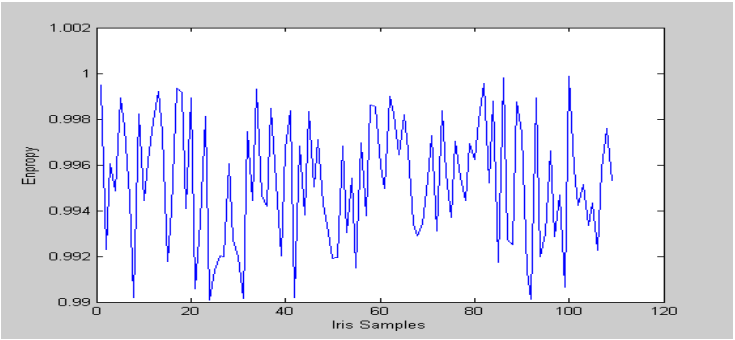

Fig. 8. Entropy of Transformed Templates for 100 samples

Table 1 Sub keys for Transformation

Test Number	Initial Value x1	Initial Value x2	Initial Value x3
1	0.3534423	0.3534422	0.3534421
KEY1 = (r1,x1), KEY2 = (r2, x2), KEY3 = (r3, x3) r1 = r2= r3 = 3 .99			

Fig. 9. Transformed Template with wrong keys

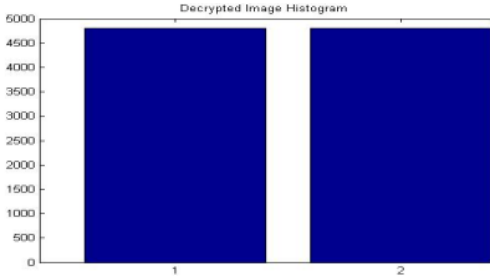

Fig. 10. Histogram of Transformed Template with wrong keys

Table 2 Sub keys for Transformation

Test	Initial Value x1	Initial Value x2	Initial Value x3	Decrypted image Entropy
1	0.3534423001	0.3534422	0.3534421	0.9966
KEY1 = (r1,x1), KEY2 = (r2, x2), KEY3 = (r3, x3) r1 = r2= r3 = 3 .99				

IV. Conclusion

In this paper a new Irreversible Transformation Scheme for Biometric Template Protection is proposed for biometric applications. The proposed scheme mainly has the advantage of the key space enlarged to 2^{425}, which improves the security against exhaustive attack. It is observed that the entropy of the transformed biometric template of the proposed scheme is very close to the ideal one and hence the transformed template appears to be highly random which is observed from the histogram in Figure 5 and average entropy from Figure 9. The proposed algorithm operates on any biometric template size. Algorithm output does not depend on the biometric scheme used for template creation. This makes the proposed algorithm highly reliable for any application (Iris, Finger print, Face Recognition etc). The simulation result shows that the proposed scheme has very good key sensitivity which provides good security for biometric templates.

References

[1] Jain AK, Ross A, Prabhakar S: An introduction to biometric recognition .IEEE Trans Circ Syst Video Technol 2004, 14:4-20.

[2] N K Ratha, JH Connell, RM Bolle, Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40, 614–634 (2001) .

[3] Ratha NK, Connell JH, Bolle RM (2011) Enhancing security and privacy inbiometrics-based authentication systems. IBM Syst J 40: 614-634

[4] A Cavoukian, A Stoianov, Biometric encryption. Encyclopedia of Biometrics (Springer, 2009)

[5] A. Juels and M. Sudan. A Fuzzy Vault Scheme. In IEEE International Symposium Information Theory, pp- 408-413, 2002.

[6] Prof. Maithilli Arjunwaddkar, Prof.Dr.RV.Kulkarni, "Robust Security Model For Biometric template Protection Using Chaos Phenomenon". International Journal of Computer Science and Security. 2009.

[7] Muhammad Khurram Khan, Jiashu Zhang," Investigation on Pseudorandom Properties of Chaotic Stream Ciphers", 1-4244-0457-6/06/$20.OO ©2006 IEEE.

[8] Muhammad Asim and Varun Jeoti "On Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme", IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp.65-69.

[9] Xu Shu-Jiang, Wang Ying-Long, Wang Ji-Zhi, TianMin," A Novel Image Transformation Scheme Based on Chaotic Maps", Proc. IEEE-ICSP 2008, pp. 1014– 1018.

[10] Biometric risk and controls by Christos K. Dimitriadis in Information Systems control Journal Vol 4 2004.

[11] Uludag U, Jain AK (2004) Attacks on Biometric Systems: A Case Study in Fingerprints. In Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI 5306:622{633 }

[12] Reena Mary George, "Facial Template Protection Using Extended Visual Cryptography And Chaotic Encryption", International Journal Of Technology Enhancements And Emergin Engineering Research, VOL 1, ISSUE 4 94 ISSN 2347-4289. Copyright © 2013 IJTEEE

[13] T. Monoth and A. P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion",. in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.

[14] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, "An Innocuous Visual Cryptography Scheme", in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[15] Liu, J., Xie, J., Wang, P. (2000), One way hash function construction based on chaotic mappings. Journal of Tsinghua University (Sci. & Tech.) 40(7), 55-58.

[16] A.Nagar and A. K. Jain, "Multibiometric cryptosystems based on feature level fusion". IEEE transaction on information forencis and security, , ,volume 7 ,issue 1, pp 255-268,2012 .

[17] Zhang Yong, "Image Encryption with Logistic Map and Cheat Image" 978-1-61284-840- 2/11/$26.00 ©2011 IEEE, page 97-101.

[18] Anchal Jain, Professor Navin Rajpal, "A Two Layer Chaotic Network Based Image Encryption Technique" 2012 National Conference on Computing and Communication System (NCCCS), 978-1-4673-1953-9/12/$31.00 ©2012 IEEE.

[19] Sanaa Ghouzali, Wadood Abdul, "Private Chaotic Biometric Template ProtectionAlgorithm", proceedings of the 2013 IEEE second International Conference on Image Information Processing (ICIIP-2013), PP. 655-659.

[20] Weichun Cheng, Gaoyun An, "Face Template Protection Using Chaotic Encryption", ICWMMN 2013 Proceedings, pp 245-248.

[21] M L. Masek, P Kovesi. MATLAB Source Code for a Biometric Identification System Based on Iris Patterns. The University of Western Australia ,2003. Available at http:/www.csse.uwa.edu.au/students projects/ libor/sourcecode.html .

[22] Chinese Academy of Sciences Institute of Automation. Page, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.

[23] B L. Masek, P Kovesi, "Recognition of human iris patterns for biometric Identification".Tech. Rep., The School of Computer Science and Software Engineering, The university of Western Australia, http://www.csse.uwa.edu.au/pk/studentprojects/libor/index.html, 2003.

[24] T Ignatenko, F Willems, Achieving secure fuzzy commitment scheme for optical pufs. Int Conf on Intelligent Information Hiding and Multimedia Signal Processing, 1185–1188 (2009).