Design and Analysis of Secured, Revocable Iris based Biometrics Authentication System

Supriya V G
KSIT, ECE Department, VTU
Research Scholar, Jain university, Bangalore- 560004
Karnataka, India)
supriyavg2007@yahoo.co.in

Dr Ramachandra Manjunatha
Professor, Jain University, Bangalore- 560004
Karnataka, India
manju_r_99@yahoo.com

***Abstract*—In the present scenario, the major concern in today's society is about securing information and providing personal privacy. Researches from decade proven that Biometric authentication systems are commercially spreading and widely used for large scale authentication systems. Due to this, there is an immense growth in biometric authentication systems for data protection. This paper is mainly concerned about protection of biometric templates generated and stored in the system to avoid the misuse of these templates by fraudulent user in order to access the data of the legitimate. We make use of chaotic logistic maps, to obtain highly random keys which are highly sensitive to initial conditions, for providing security to iris templates.**

Index Terms— Biometric cryptosystem, Cancellable biometrics, chaotic properties, Logistic maps.

I. INTRODUCTION

Biometrics (or **biometric authentication**) consists of methods for uniquely recognizing human beings based upon one or more intrinsic physical or behavioral traits associated with the person viz. facial thermo gram, hand vein, gait, keystroke, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature for the purpose of providing security. Biometric verification for personal authentication is becoming increasingly common in corporate and public security systems, consumer electronics and recent one being its usage in the Aadhar card or the Unique Identification card for the citizens of India. This paper concentrates on protection of iris templates which are stored in the database for authentication. Biometric system involves two processes. Initially during enrollment process, person's biometric trait is captured and unique features are extracted and processed using suitable algorithm to produce templates and stored in the database. During authentication (verification) process, the same procedure is repeated in order to obtain the desired template and compared with the already stored templates in database to provide results of matching based on whether the access is approved or denied.

The passwords and tokens which are issued to the user (through which they can protect or secure personal information/data) are highly vulnerable to attacks as the passwords and tokens can be easily guessed or stolen by the hackers or it may be forgotten by the user. To overcome these limitations of password and token based information security systems, biometrics came into existence. Since biometric characteristics are unique and immutable, once biometrics is compromised, it is compromised forever and it cannot be revoked and reissued to the user. In order to ensure security for the templates, as well as the data, further investigations are being made in providing security in the biometric authentication system. One such approach is to make use of Cancellable biometrics.

Cancelable biometrics [1] refers to the inclusion of intentional and systematically repeatable distortion of biometric features for the protection of sensitive user-specific data, so that even if template data is compromised, the existing template can be cancelled and a new template can be obtained by changing the distortion characteristics.

In this paper, we are using chaotic maps for the protection of biometric templates. **Chaos theory** which was proposed by Edward_Lorenz is a field of study in mathematics, which explains the behavior of dynamical systems that are highly sensitive [2] to initial conditions. This response is called butterfly effect. Chaos uses permutation and substitution architecture in order to produce deterministic and random elements. It does not mean that the behavior is completely random. But we cannot predict the behavior since the future behavior of it, in a very sensitive way, depends on present condition thus making it deterministic, unpredictable and highly random in nature. This nature of chaotic output makes it suitable to be used for biometric feature transformation.

The application of chaotic signals in biometric template encryption is presented in [2,3,4,5,6,7,8]. Reena Mary George [2] proposed a scheme for face template protection based on chaotic encryption and visual cryptography where keys were generated by 1D Logistic Maps and thus obtained a simple and secure method to protect the biometric images.

Sruthi B Asok et al. [3] implemented iris based cryptography, generated Edge maps (secret keys) from images and generated 128 bit key from normalized image which is used to encrypt data and tested for randomness of keys. They used AES for encryption and decryption.

Marius Iulian Mihailescu in [4] with the idea of creating a strong and powerful scheme for enrollment in biometric systems proposed the usage of Rossler map for Pseudo random bit generation i.e. key generation and encrypted using Hash-chaos based cryptography for biometric template protection.

Ankit Jat and Sandeep Raghunathan [5] encoded finger print images using orthogonal code scheme, where shuffling of image pixels was done by 2D Cat Map and encryption shuffled pixels were obtained using 2D standard map. Finally encoding was done using Hadamard transformation. Authors conclude that the following scheme gives a high key sensitivity and large key space.

978-1-4673-8286-1/16 $31.00 © 2016 IEEE
DOI 10.1109/IACC.2016.66

Divya James et al. [6] proposed a scheme which makes use of visual cryptography and 3D chaotic maps to design novel security architecture for biometric templates. Author reported that 2 keys differing by 0.000001 while used for encryption gave 50.09% difference in output i.e. key sensitivity was shown to be very high. Simulation results that were observed had reported that it was efficient algorithm and possess a high level of security against attacks.

Lein-Heng-Jian et al. [7] proposed a scheme for palm-print template protection where chaotic keys were generated using Pseudo-Random Bit Generator (PRBG) based on Nonlinear Dynamic Filter (NDF). They encrypted the Competitive code to chaotic codes with XOR operation and obtained GAR (Genuine Acceptance Rate) of 99.94%, FAR (False Acceptance Rate) of 10^{-5}%, FRR (False Rejection Rate) of 0, EER (Equal Error Rate) of 0.02% and key space of $0.5 \mathrm{x} 10^{128}$ and thus have large template re-issuance ability. Key Sensitivity is shown to be relatively down by 10^{-1} in coupled key scale and thus provide a better separation between genuine and imposter populations. This scheme shows very low hamming distance for the inter-class subjects and maintained intra-class distance of the same subjects.

Arian Rahimi et al. [8] proposed a scheme for online credit card transactions in which human identification was implemented using iris recognition for which authors makes use of Logistic map for key generation, Henon map for encryption and Steganography and Cryptography during transmission while resizing the image using nearest neighbor interpolation and 2D Haar Transform. Author suggests an innovative method of applying the algorithm on half of the iris by which the obstruction problem of the iris caused by the eyelids was overcome.

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

- The main challenge regarding biometric template is the alignment during template generation, which in turn degrades recognition performance.
- To satisfy the property of unlinkability, transformed templates generated from a single biometric template applying different parameters should be unique.
- The transformed templates need to exhibit high entropy with sufficient key size to prevent biometric keys from being guessed.

In this paper, Design and Analysis of Secured, Revocable Iris based Biometrics Authentication system is proposed to address the above challenges**.**

The biometric template transformation is done by permuting the template data (diffusion) and then confusion is carried out by bitwise-XNOR or XOR operation on each bit of template data based on the chaotic sequences. The proposed algorithm is designed to handle any biometric template size, making it suitable for the practical applications. In the proposed algorithm key space is enlarged approximately equal to 2^{319}, thus improving the security against exhaustive attacks. In practice biometric template will be of different scheme and hence care is taken in the design of the algorithm such that a good transformation speed is achieved. The absence of computationally heavy operations such as division or exponential makes this algorithm particularly attractive.

The remaining part of this paper is organized as follows. In Section II the proposed biometric transformation scheme is discussed. Section III presents the experimental results of the proposed biometric template transformation algorithm. Algorithms efficiency is demonstrated through the results and investigating on its security by analyzing sensitivity of key, entropy of the transformed and key space analysis. Conclusions are presented in section IV.

II. PROPOSED BIOMETRIC TEMPLATE PROTECTION SCHEME

The block diagram described in Fig. 1 extracts user biometric characteristics and processes as template during enrollment. The biometric template is then transformed using chaotic keys derived from logistic map and suitable cryptographic algorithm. The transformed biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be compared with query template. During verification, query biometric image features are extracted, processed as template and then transformed using same chaotic keys derived during enrollment process and cryptographic algorithm as shown in Fig.2. The matching result of transformed query template with transformed template stored during enrollment determines identity.

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 II.C.

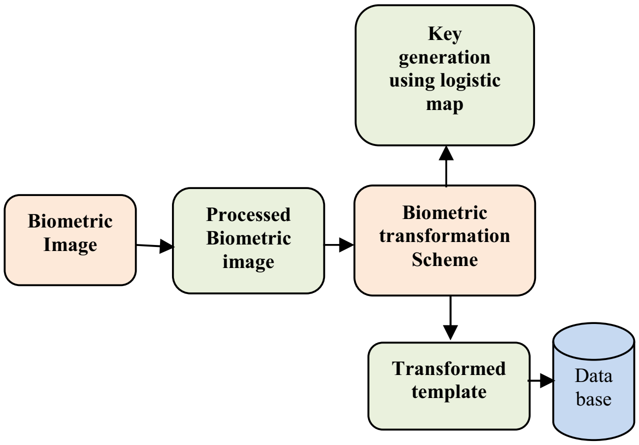
Key generation using logistic map
Biometric Image
Processed Biometric image
Biometric transformation Scheme
Transformed template
Data base

Figure 1. Block diagram of Proposed Enrollment Scheme

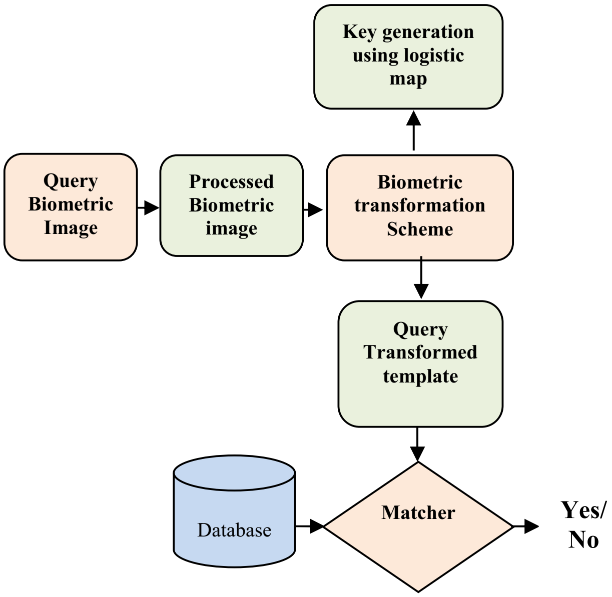
Key generation using logistic map
Query Biometric Image
Processed Biometric image
Biometric transformation Scheme
Query Transformed template
Database
Matcher
Yes/ No

Figure 2. Block diagram of Proposed Authentication Scheme

Keys are generated from the chaotic logistic map equation 3. The key set used for generating the key streams is unique among each user and is secretly shared between the sender and receiver in the system through a secure channel. It must be guaranteed that the key is shared securely without any errors in between sender and receiver.

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

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

The 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 1 & key stream 2 are used for permutation of template data by considering whether digit is odd or even in key stream 1 & bit is 0 or 1 in key stream 2.Key stream 3 is used for substitution of template data $T_I(x,y)$ by bit-wise XOR^{ing} or $XNOR^{ing}$ with the keystream 3 and it is described in the equation 1.

Let $T_T(x, y)$ = transformed template data &
$T_B(x, y)$ = biometric template data.

$$T_T(x, y) = T_B(x, y) \oplus KS3(x, y), \quad \oplus = XNOR \qquad (1)$$

either {KS2(x, y) = 1 and KS1(x, y) is even}
or {KS2(x, y) = 0 and KS1(x, y) is odd}

$$T_T(x, y) = T_B(x, y) \oplus KS3(x, y), \quad \oplus = XOR \qquad (2)$$

either {KS2(x, y) = 1 and KS1(x, y) is odd}
or {KS2(x , y) = 0 and KS1(x, y) is even}

B. Authentication Scheme

Fig.2 represents block diagram of authentication scheme. User biometric template is once again transformed using the same algorithm with the same key streams as explained in section II.A and bitwise compared with user transformed template from the database for providing authentication.

C. Generation of Key stream

Generation of Key stream is as shown in Fig. 3. Chaotic real valued discrete sequence is generated by Logistic map equation by selecting a key.

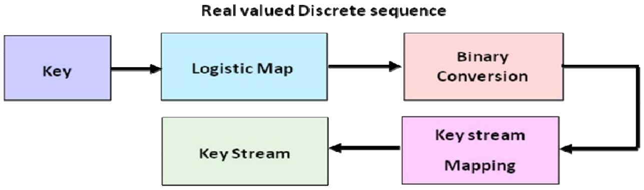

Figure 3. Block diagram of Key Stream Generation

The Logistic map equation is given by [9,10,11],

$$x_{n+1} = r * x_n[1 - x_n], \quad 0<x< 1 \qquad (3)$$

Where r is the bifurcation factor, x_n is the initial value and dynamics of the generated chaotic sequence changes dramatically depending on the value of r, x_n. The sequence is found to be non periodic and non-converging [11] for the value of bifurcation factor between 3.57 and 4. The logistic map exhibits symmetric probability density function [10] and hence the binary conversion is done by using equation 4.

$$a_i = 0 \text{ for } x_n < 0.5 \quad \text{and}$$
$$a_i = 1 \text{ for } x_n \geq 0.5 \qquad (4)$$

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

The Keys = {Key stream 1, Key stream 2, Key stream 3} composed of three sub-keys (SB), where each sub key is of the form SB = {Initial Value, bifurcation factor}. SB1 is used for generating keystream1, SB2 is used for generating keystream2 and SB3 is used for generating keystream3. Keystream 2 and Keystream 3 is as shown in equation (5)

Key Stream 1 = Key Stream2 = $a_1, a_2, a_3, \ldots a_n$
Where bn Є [0,1]
$a_i = 0$ for $x_n < 0.5$, $a_i = 1$ for $x_n \geq 0.5$ (5)

Key Stream 3 = $C_1, C_2, C_3, \ldots\ldots C_j$,
Where C = Decimal Number
$C1 = a_1, a_2, \ldots\ldots\ldots\ldots a_k$,
$D2 = a_{k+1}, a_{k+2}, \ldots\ldots\ldots a_{2k} \ldots C_J$ (6)
Where J = 0, 1, ….(MXN).

Thus the Key stream 1 = {$C_1, C_2, \ldots C_J$}, Where $C_1, C_{2\ldots}$etc denotes decimal numbers obtained by combining k-binary numbers for each streams respectively. The length of key stream 2 and key stream 3 which is used for permutation is same as the size of the template to be transformed (MXN) and the range is [0, 1], the required length of keystream1 is also same as size of biometric template to be transformed i.e. MXN and range is [0, (MXN)-1] which is used for bitwise XOR^{ring} or XNOR^{ing} (i.e. substitution based on permutation)

During generation of key stream 1, it must be assured that there is no duplicate element in the two streams by discarding the repeated sequence as explained in section II.D, Since key stream 1 is used for position permutation.

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 Fig.4.

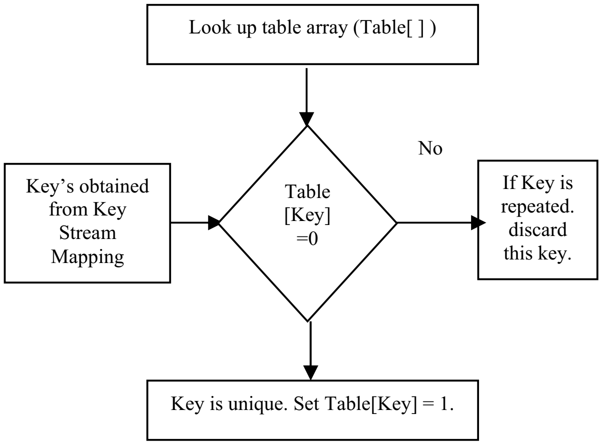
Look up table array (Table[ ])
Key's obtained from Key Stream Mapping
Table [Key] =0
No
If Key is repeated. discard this key.
Key is unique. Set Table[Key] = 1.

Figure 4. Lookup table to generate keystream 1

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

III. EXPERIMENTAL ANALYSIS

For the experimental analysis of the proposed algorithm, the Iris database in [12,14] which contains 108 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 [13]. The bifurcation factor r value is taken as 3.89 and key is given as shown in table 1. The proposed algorithm was implemented using template as shown in Fig. 5 and histogram of input template is as shown in Fig. 6. After transformation, the transformed biometric template stored in database is as shown in Fig. 7 and histogram of transformed template is as shown in Fig. 8 and Fig. 19 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 2 and Table 3, result of authentication is checked with correct and wrong keys. There were three different evaluations implemented in this paper.

Evaluation 1: Analysis on Key space.

As the maximum computation precision of most commonly used PC platform is 16 decimal digits, cryptosystem based on chaos can provide key space of size $10^{16}\approx2^{53}$ [15], which is a little smaller than standard cryptographic algorithms Data Encryption Standard algorithm (2^{56}) and by far smaller than Advanced Encryption Standard algorithm (2^{128}). Since keys = {Key stream 1, Key stream 2, Key stream 3} and is composed of three sub-keys with each key consisting of key = (initial value, bifurcation factor), the key space of the proposed algorithm is $(10^{16})^{6}\approx2^{319}$, which is larger than the acknowledged most secured Advanced Encryption Standard algorithm. Besides, since the scheme adopts both permutation and substitution operations, it is secure against known/chosen-plaintext attack [15].

Evaluation 2: Entropy of transformed templates.

Entropy of a random binary biometric template source is expected to be in which each pixel is 1-bit. Normally it is observed that the input template entropy is low for biometric templates. Applying proposed algorithm on Iris biometric template, as per the simulation results, 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.

Evaluation 3: Analysis on sensitivity of keys.

An efficient biometric feature transformation scheme should exhibit high uniqueness among transformed templates even for very small changes in the keys used for transformation. In the proposed scheme with a small change in the sixth decimal position of key, it is not possible to get the transformed user biometric template back and matching fails. The observed results by selecting the wrong keys are tabulated in Table 3.

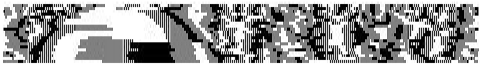

Figure 5. Input Template

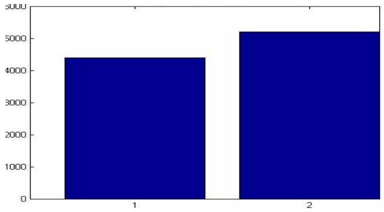

Figure 6. Input Template Histogram

Figure 7. Transformed Template

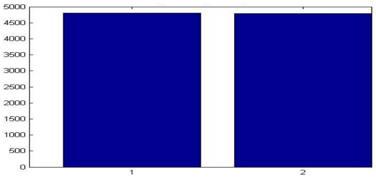

Figure 8. Transformed Template Histogram

Table 1. Key Streams for 5 Sample Template

Template No	Key Streams		
	Key 1	Key 2	Key 3
1	0.342891	0.373916	0.395772
2	0.365432	0.384613	0.409681
3	0.362997	0.354766	0.367845
4	0.357878	0.398762	0.321456
5	0.301575	0.316174	0.3498714

Table 2. Results of Transformed User Biometric Template

Template	Key Streams			Result of
No	Key 1	Key 2	Key 3	Authenication
1	0.342891	0.373916	0.395772	Matched
2	0.365432	0.384613	0.409681	Matched
3	0.362997	0.354766	0.367845	Matched
4	0.357878	0.398762	0.321456	Matched
5	0.301575	0.316174	0.3498714	Matched

Table 3. Results of Transformed Biometric Template with wrong keys

Template	Key Streams			Result of
No	Key 1	Key 2	Key 3	Authenication
1	0.342881	0.373919	0.395792	Unmatched
2	0.365462	0.384623	0.409661	Unmatched
3	0.362945	0.354740	0.367810	Unmatched
4	0.357832	0.398742	0.321433	Unmatched
5	0.301595	0.316194	0.3498780	Unmatched

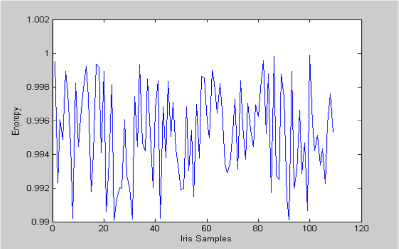

Figure 10. Entropy of Transformed Templates for 100 samples

IV. CONCLUSION

In this paper a novel Biometric feature transformation scheme is proposed for biometric applications. The proposed scheme exhibits the advantage of enlarged key space of 2^{319}, which improves the security against exhaustive attack and highly sensitive to very small changes in any one of the three keys which provides good security for biometric templates. It is observed from simulation results that the entropy of the transformed biometric template stored in database of the proposed scheme is very close to the ideal one and hence the transformed biometric template appears to be highly random which is observed from the histogram in Fig. 9 and average entropy in Fig. 10. Since the algorithm output does not depend on the biometric scheme used for template creation The proposed algorithm operates on any biometric template size and this makes the proposed algorithm highly reliable for any application (Iris, Finger print, Face Recognition etc).

REFERENCES

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

[2] Reena Mary George, "Facial Template Protection Using Extended Visual Cryptography And Chaotic Encryption," International Journal of Technology and Emerging Engineering Research (IJTEEE-2013), Vol 1, Issue 4, pp 94-96.

[3] Sruthi B. Asok, Karthigaikumar, Sandhya R, Naveen Jarnold K, Siva Mangai, " Iris Based Cryptography," International Journal

of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2013, pp 1310-1313.

[4] Marius Iulian Mihailescu, "New Enrollment Scheme for Biometric Template Using Hash-Chaos Based Cryptography," 24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013.

[5] AnkitJat, Prof. Sandeep Raghuwanshi,"Strengthen Fingerprint Data Security Using Chaotic Map Approach," International Journal of Engineering Research & Technology (IJERT), Vol.2, Issue 7, July-2013, pp 2726-2730.

[6] Divya James, Mintu Philip "A Novel Architecture for Biometric Templates Using Visual Cryptography and Chaotic Image Encryption," Proceedings of International Conference on Eco-friendly Computing and Communication Systems (ICECCS)-2012, Kochi, India, August 9-11, 2012, pp 239-246.

[7] Li Heng-Jian, Zhang Jia-Shu,"A Novel Chaotic Stream Cipher and Its Application to Palmprint Template Protection," Chinese Physical Society and IOP Publishing Ltd, 2010, Vol-19, No.4.

[8] Arian Rahimi, Sharhriar Mohammadi, Rozita Rahimi, "An Efficient Iris Authentication Using Chaos Theory-based Cryptography for E-commerce Transactions," Proceedings of Internet Technology and Secured Transactions, 2009 (ICITST-2009), London, pp. 1-6.

[9] 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

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

[11] Xiao Huijuan, Qiu Shuisheng, Qiu Shuisheng," A Composite Image Transformation Scheme Using AES and Chaotic Series", First International Symposium on Data, Privacy and E-Commerce, 2007, pp. 277 – 279.Advanced Technologies (AutoID), pp. 21-26, 2005.

[12] 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.

[13] 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 .

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

[15] C Chong Fu,Zhiliang Zhu, "A Chaotic Image transformation scheme based on circular bit space shift method", The 9th International Conference for Young Computer Scientists, IEEE Computer Society, pp. 3057 – 3061, 2008.