IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Reliable Biometric Data Encryption Using Chaotic Map

Jincey John[1], Ashji S.Raj[2]

Student, Computer Science and Engineering, Amal Jyothi College of Engineering, Kanjirapally, India [1]

Assistant Professor, Computer Science and Engineering, Amal Jyothi College of Engineering, Kanjirapally, India [2]

Abstract: Recently, one of the significant methods of user identification is biometric identification. It has gained its popularity because of the non-repudiation of data, though it suffers problems such as biometric template storage, biometric spoof and the resulting security problems. To alleviate the problems, biometric encryption has become the focus of present studies. User's biometric data includes data such as face, fingerprint, iris, retinal scan, palmprint and hand vein etc. The traditional algorithms of encryption such as AES and DES are not suitable for biometric image encryption. The recent research on image encryption is in the chaos based encryption. In this paper, we propose a novel reliable algorithm for enhancing the security of biometric data using the chaotic map. A user intrinsic key from the biometric data is used to generate the chaotic sequence for encryption and for increasing the reliability.

Keywords: Biometric security; chaos; logistic map; diffusion.

I. INTRODUCTION

A biometric system is a reliable, robust, and basic pattern recognition system, widely used in today's life. Biometrics is a unique, physical or physiological characteristics or behavioral traits of an individual to recognize the identity or authenticate the claimed identity of an individual. Physiological biometrics is related to the shape of the body such as retina, iris, fingerprint, face, DNA, vein patterns and hand geometry. Behavioral biometrics is related to the user's behavior while he interacts with a computing system for identification purpose, ie. typing rhythm, mouse dynamics, gait, and voice. The main applications of biometrics include access controls, national ID card, border control, passport control, criminal investigation and terrorist identification. The uniqueness property of biometrics makes it a very powerful tool and an area of interest for the research community for security purposes [1]-[4].

Even though automated biometrics can outcome the problems associated with the traditional methods of user authentication, hackers can easily find the vulnerable points of attack. A critical vulnerability that is unique to biometric systems is the compromise of the biometric data. The biometric traits are permanent and unique to an individual, so it requires to be tightly secured. Stolen biometric data can be used by an adversary to create biometric spoofs, which may lead to gain illegitimate access to systems that employ the same biometric trait of the user. Stolen data can also be used to access information about the user such as race, gender and certain medical conditions. Unlike passwords, it is not possible for an authorized user to revoke his biometric data and switch to another uncompromised one. Hence, ensuring the security of biometrics is essential for any security system based on the biometric recognition.

The latest trend to protect biometric data is to use chaotic encryption techniques [5], [6]. Chaotic encryption techniques inherit several unique characteristics such as sensitivity to initial conditions, control parameters, ergodicity, and randomness. These schemes have gained more attention as a small deviation in the local area causes a dramatic change in the wholespace.

II. RELATED WORKS

To ensure the privacy and security of the biometric system, many scholars have conducted researches to explore the possible risk of biometric network and feasible measurement to guarantee the security. Uludag et al. analyzed the challenges involved in biometric application in authentication system and limitations of the biometric cryptosystems [7]. Many techniques have been introduced since to reduce the vulnerability of biometric data. Soutar et al.[8], proposed an algorithm on biometric encryption. Alghamdi et al. [9] states that image encryption cannot be used for large amount of data and high resolution images. Ross and John Daugman et al. [10] presented a secure way to integrate iris biometric with cryptography.

Numerous cryptographic techniques based on numerical theory or algebraic concepts were introduced. But conventional transformation algorithm like AES , DES [11] involves large number of operations which will consume more time for transformation. Chaos-based cryptography is the latest and efficient way to develop fast and secure cryptography for image encryption. The chaotic behavior is the random behavior of a nonlinear system and the important characteristics of chaos is its extreme sensitivity to initial conditions of the system. In [12], Baptista proposed a novel chaotic encryption algorithm. Several research have been conducted based on his proposed method and some improved methods were proposed, [13], [14]. L. Chen and D. Zhao introduced a method to encrypt images, in which fractional order of fractional wavelet packet transform is used as the key [15]. They achieved data confidentiality but limited key space.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Maung et al.proposed a fast encryption scheme [16] based on chaotic maps. Wang et al. presented an algorithm [17] that produces chaotic stream based on logistic map.

A number of new techniques, extensions or improved versions of the earlier techniques, have been proposed in recent years. The improvement is primarily based upon making a good security versus computational time tradeoff. The state-of-the-art methods have been thoroughly discussed in [18]. The main idea behind this paper is to develop a secure and reliable encryption technique using chaotic functions. Many chaotic maps exist such as Logistic map, Arnold cat map, Baker map, Sine map, Standard map and Lorenz map. In the proposed algorithm, we have used the integrated Logistic-Sine map for chaotic sequence generation. Then, a user intrinsic key is generated from the biometrics and used as the initial value of the chaotic sequence. The random sequence produced by the chaotic phenomenon is used to encrypt and secure the biometric data. It should be noted that the proposed method is generic ie. all the biometrics such as iris, face, fingerprint, vein can be protected using the algorithm.

The rest of our paper is organized as follows. The main principles of the techniques mentioned in the proposed method are introduced in Section III and Section IV sums up the performance analysis of our scheme in terms of correlation and distribution of pixels. Conclusions are provided in Section V.

III.PROPOSED SYSTEM

The method we propose is based on the encryption of biometric data using diffusion and user intrinsic key. The user biometric data is encrypted using the chaotic sequence generated by aggregated logistic-sine map. The system overview can be shown as below.

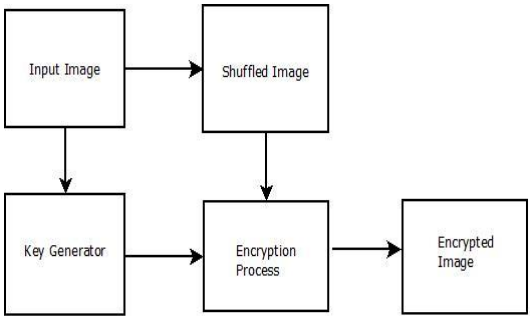


Fig.1. System overview

A. Shuffling

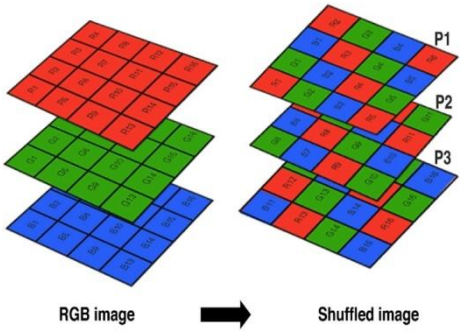


Fig.2. Shuffling process

The pixels of an image are shuffled by intermixing the pixels of each channel. The pixels are shuffled initially to get a shuffled image as shown in Figure 2 [19].

B. Key Generation

A user-intrinsic key is extracted from the user's biometrics and used for generating the initial parameters and initial values for the system to be in a chaotic state. The key is directly generated from user biometrics, which makes it more difficult to compromise when compared to external secret key. Consider the pixel value of an image and extract one channel (RGB) at a time. It can be either a red channel or green channel or blue channel. The key is generated based on the following steps.

- Obtain processed biometric data.
- Consider the single channel matrix of the image from the three ie, Red, Green or Blue component. Let the size of matrix be 100 x 100.
- Then we group the pixels into 10 groups such that each group consists of equal numbers of pixels.
- RMS (Root Mean Square) value for the diagonal values of each group is calculated.
- Each RMS value is converted to hexadecimal digits and forms the key.

From each rms value a 2 digit hexadecimal number is obtained. The above procedure is repeated for each channel and we get the three keys namely K1, K2 and K3. Each key from each channel will consist of 20 hexadecimal digits for the encryption process.

C. Logistic-Sine Map

A chaotic logistic-sine map [20] is used for sequence generation. The Logistic map is a simple, one-dimensional chaotic system described as:

$$x_{i+1} = r\, x_{(i)}\, (1 - x_{(i)})$$

where $x_{(i)} \epsilon (0,1)$ is the discrete state, with initial value $x_{(0)} \epsilon (0,1)$ and control parameter $r \epsilon [3.9,4)$ to generate chaotic sequences.

The Sine map is another 1D chaotic map and has a similar chaotic behavior as the Logistic map. Its definition can be described by the following equation:

$$x_{(i+1)} = r \sin(\textstyle\prod x_{(i)} / 4)$$

where parameter $r \epsilon [0,4)$. One dimensional chaotic systems have a simple structure and is easy to implement. Though they have limited or/and discontinuous range of chaotic behaviours and are vulnerable to low-computation-cost. Hence, in paper [20] a new chaotic system was developed with better chaotic performance. In this paper the authors integrated existing 1D chaotic maps to generate a new chaotic map and claims excellent chaotic properties, including a wide range of parameter settings and the uniform-distributed variant density function.

Because of the said advantages, we have used the integrated Logistic-Sine map for chaotic sequence generation ie.,

$$x_{(i+1)} = r\, x_{(i)}\, (1\text{-}x_{(i)}) + (4\text{-}r) \sin(\textstyle\prod x_{(i)})/4 \mod 1$$

DOI 10.17148/IJARCCE.2015.41113

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

where r parameter ϵ (0,4] . To calculate the initial condition $x_{(0)}$ and r, the secret key is used. The user key from each channel will be of the form K = $k_1, k_2, k_3, \ldots k_{19}, k_{20}$. For finding the initial parameters the following values are calculated,

a = $k_1, k_2, k_3, \ldots k_{10}$

b = $k_{11}, k_{12}, k_{13}, \ldots k_{20}$

$x_{(0)}$ = sum(a) / 100 (mod 1)

r = 3.9 + (sum(b) / 100 (mod 1))

Thus the initial parameter for the Logistic-Sine chaotic sequence for each channel is obtained. The chaotic sequence is iterated till the total number of pixels of the image.

D. Encryption and Decryption Algorithm

The steps of proposed encryption and decryption algorithms are presented below. Consider the user biometric image U, of size P x Q, where P and Q is the width and length of the image. For each channel ie, Red, Green and Blue the below procedure is followed;

1) From each channel of image U, extract the key as explained in the Key Generation algorithm.
2) The initial values for the chaotic map are obtained from the extracted key as explained above.
3) Shuffle the pixels.
4) Encrypt each shuffled pixel by XORing with respective chaotic sequence generated.

An encrypted image is obtained after performing the above steps. To decrypt the encrypted image repeat the same steps as in encryption by reversing the process.

IV. EXPERIMENTAL ANALYSIS

The following section describes the experimental setup and results obtained from the implementation of the system. The color face images from reliable sources have been used for encryption. Statistical analysis on the proposed algorithm, demonstrates its diffusion properties to strongly resist statistical attacks. This is done by key analysis, testing the distribution of pixels of the cipher-images and study of correlation among the adjacent pixels in the cipher-image. Figure 3 shows the original image and encrypted image. The details are provided in the subsequent sections.

Fig.3. Plain image and cipher image

A. Key space analysis

The key space size is the total number of different keys that can be associated with the encryption framework. For a secure encryption framework, the key space should be large enough to make the system susceptible to brute-force attacks. From the cryptographic point of view, the size of the key space should not be smaller than 2^{100}. In the proposed technique, we use 240 bit space key, therefore the key space is 2^{240}. So, the key space is large enough to resist the brute-force attacks

B. Key sensitivity analysis

Key sensitivity is defined as the change in the encrypted image due to change in the key. High key sensitivity is needed for secure image cryptosystem so that the original image cannot be decrypted correctly, even though there is a marginal difference in the correct key. The key sensitivity (S) can be computed by

$$S = \frac{Diff\,(E,E')}{M \times N}\ 100\ \%$$

where E and E' are the encrypted images using correct and wrong keys respectively with M x N as the dimension of encrypted images. Mathematically, Diff(E, E') is defined as

$$\text{Diff}\,(E, E') = \sum_{i=1}^{M} \sum_{j=1}^{N} E(i,j) \infty E'(i,j)$$

where

$$E(i,j) \infty E'(i,j) = \begin{cases} 1, & E(i,j) \neq E'(i,j) \\ 0, & E(i,j) = E'(i,j) \end{cases}$$

Generally, for a good encryption scheme, the value of S is about 75%. Respective results are shown in Figure 4 for visual assessment, and the values of S are found to be 100% for each channel namely Red, Green and Blue (Table I). In each case, all the pixels are different in the images, which can be further justified from Figure 4. Hence, the proposed scheme is highly sensitive to the keys according to both human perception and simulations.

(a) (b)

Fig.4. (a) Encrypted image with correct keys,
(b) Encrypted image with 1 bit change in key1, key2 and key3

TABLE I: KEY SENSITIVITY BETWEEN FIGURE 4 (A,B)

Channel	Key sensitivity (%)
Red channel	100
Green channel	100
Blue channel	100

C. Histograms of the encrypted images

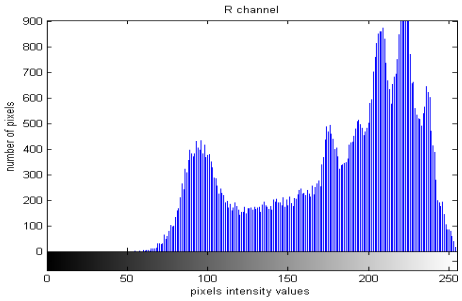
Histogram is a graphical representation of the pixel intensity distribution of an image. Thus, histogram provides a clear illustration of how the pixels in an image are distributed by plotting the number of pixels at each intensity level. Histograms of the original image and

IJARCCE

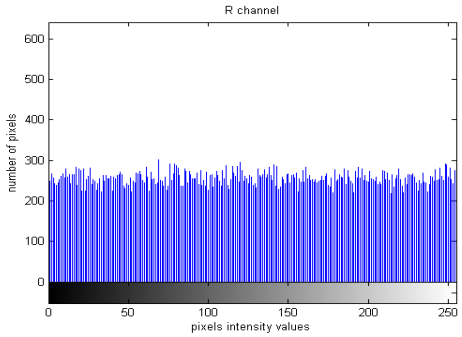
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

cipher-image are shown in Figure 5 - 7. The encrypted histograms are entirely different from the original image histograms.

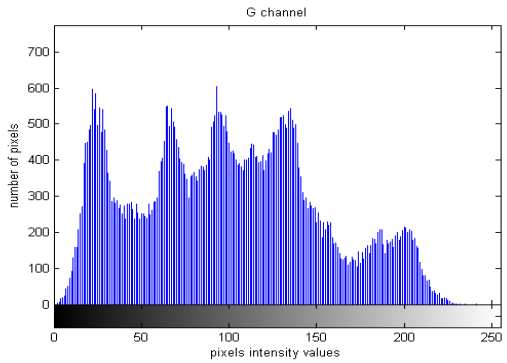


(a)

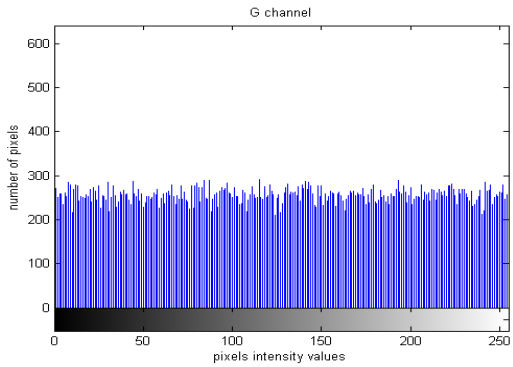


(b)

Fig. 5. Histogram analysis: (a) histogram of red component of original image; (b) histogram of encrypted image

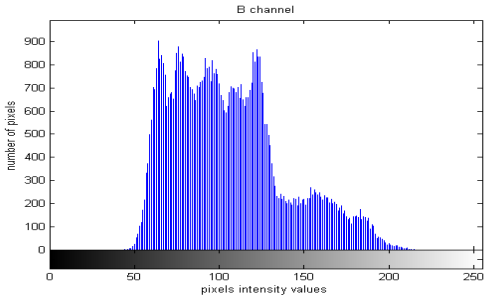


(a)

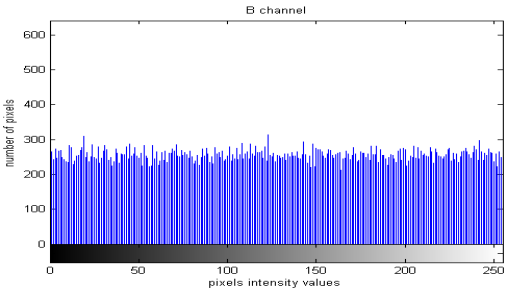


(b)

Fig. 6. Histogram analysis: (a) histogram of green component of original image; (b) histogram of encrypted image



(a)



(b)

Fig.7. Histogram analysis: (a) histogram of blue component of original image; (b) histogram of encrypted image

D. Correlation of two adjacent pixels

Correlation between two adjacent pixels can be tested in three ways, by taking two vertically adjacent pixels or by taking two horizontally adjacent pixels or by taking two diagonally adjacent pixels in the encrypted image. First, randomly select 1000 pairs of adjacent pixels and then calculate their correlation coefficient, r_{xy} of each adjacent pair is calculated for the plain and ciphered images using the following formulae:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{Dx}\sqrt{Dy}}$$

$$cov(x,y) = cov(x,y) = E[(x-E(x))(y - E(y))]$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i$$

$$Dx = \frac{1}{L}\sum_{i=1}^{L}(x_{i-E(x)})^2$$

where x and y are values of two adjacent pixels in an image and L denotes the total number of samples taken. Figure 8-10 shows the correlation distribution of two horizontally adjacent pixels of Red, Green and Blue components in the original images.

Tables II-IV shows the correlation coefficient values of two horizontally, vertically and diagonally adjacent pixels in the original and encrypted images for each channel. From the table it is observed that the adjacent pixels are highly correlated in original iris images and as encryption takes place then correlation reduces and reaches to zero whereas the decryption process binds adjacent pixels with high correlation.

Hence, the proposed technique is able to break the high correlation among the pixels. Therefore, the proposed technique is robust against statistical attacks.

DOI 10.17148/IJARCCE.2015.41113

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

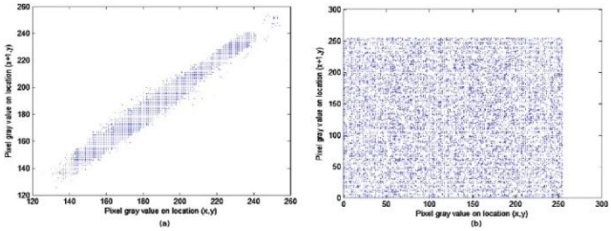


Fig. 8. Correlation distribution of two horizontally adjacent pixels in the (a) plain red plane, (b) cipher red plane

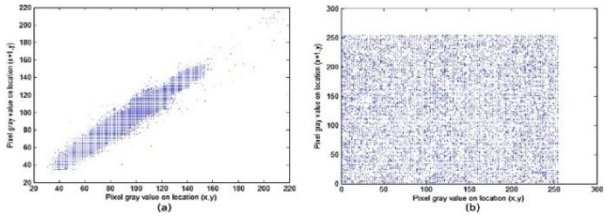


Fig. 9. Correlation distribution of two horizontally adjacent pixels in the (a) plain green plane, (b) cipher green plane

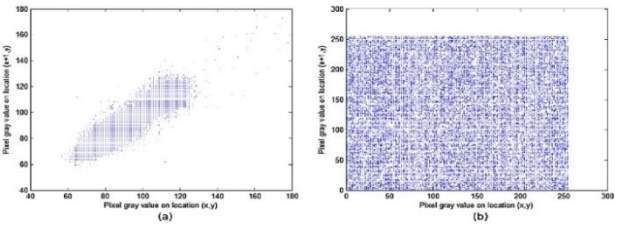


Fig. 10. Correlation distribution of two horizontally adjacent pixels in the (a) plain blue plane, (b) cipher blue plane

TABLE II: CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN RED CHANNEL

	Horizontal	Vertical	Diagonal
Original Image	0.9798	0.9893	0.9697
Encrypted Image	0.0037	-0.0073	0.0033

TABLE III: CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN GREEN CHANNEL

	Horizontal	Vertical	Diagonal
Original Image	0.9691	0.9825	0.9555
Encrypted Image	-0.0092	-0.0052	-0.0033

TABLE IV: CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN BLUE CHANNEL

	Horizontal	Vertical	Diagonal
Original Image	0.9327	0.9576	0.9183
Encrypted Image	0.0000	-0.0031	0.0065

V. CONCLUSION

Biometric authentication is becoming the most popular and most reliable user authentication mechanism, even it is vulnerable to attacks. The interest in biometric approaches for authentication is increasing for their advantages such as security, accuracy, reliability, usability, and friendliness. In this work, a new reliable method of securing biometric data is used. The proposed approach involves user intrinsic key extraction and the extracted key is used in encryption process. The key space is increased by selecting high dimensional chaotic system. Also, complex non-linearity is preserved by choosing suitable chaotic maps. Further, pixel values are changed by the diffusion function, avoiding repeated permutations. All these techniques, speed up the process of encryption but make the decryption process unmanageable especially in the case when there is no information of the correct keys and their correct alignment. The encryption pattern and large key space increase the robustness of the proposed cryptosystem. This work can be continued to study and test the properties and efficiencies of the proposed approach and also extend the study to other biometrics, e.g., evaluate the performance of this proposed methods on face, palm vein, etc. Also the proposed system is limited to color biometric data and can be extended to secure gray scale biometric data.

REFERENCES

[1] C.Soutar, G.J.Tomko, "Secure private key generation using a fingerprint," Proceedings of CardTech/SecurTech Conference, vol.1, 1996, pp.245–252.
[2] C.Soutar, D.Roberge, A.Stoianov, R.Gilroy, B.V.K.V.Kumar, "Biometric encryption using image processing," Proceedings of Optical Security and Counterfeit Deterrence Techniques II, SanJose, CA, vol.3341, 1998, pp.178–188
[3] N.K.Ratha, J.Connell, R.Bolle, "A biometrics-based secure authentication system," Proceedings of Workshop on Automatic Identification Advances Technologies, 1999, pp.70–73.
[4] N.K. Ratha, J.Connell, R.Bolle, "Enhancing security and privacy in biometrics based authentication systems, IBM Syst.J.40(2001)614–634..
[5] D. Moon,Y.Chung, S.B.Pan, K.Moon, K.I.Chung, "An efficient selective encryption of fingerprint images for embedded processors",ETRIJ.28(2006) 444–452.
[6] M.K.Khan, J.Zhang, "An intelligent fingerprint-biometric image scrambling scheme", Proceedings of International Conference on Intelligent Computing, Qingdao, China,vol.2,2007,pp.1141–1151.
[7] U. Uludag, S.Pankanti, A.K. Jain, "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June 2004.
[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption," ICSA Guide to Cryptography, McGraw-Hill, 1999,\\http://www.bioscrypt.com/assets /Biometric_Encryption.pdf.
[9] A. S. Alghamdi and Hanif Ullah, "A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm", International Journal of Computer and Network Security, 2(4), 2010, pp. 78-84.
[10] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," University of Cambridge, Tech. Rep. UCAMCL-TR-640, 2005.
[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", Boca Raton, FL: CRC Press, 1996.
[12] MS Baptista, "Cryptography with chaos", Physics Letters A, 240(1998), pp.50–54, 1998.
[13] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori, "A secret key cryptosystem by iterating a chaotic map", Advances in Cryptology, pp. 127–140. Springer, 1991.
[14] Ljupco Kocarev, "Chaos-based cryptography: a brief overview", Circuits and Systems Magazine, IEEE , vol. 1, no. 3, pp. 6–21, Aug. 2001.
[15] Chen, L., and Zhao, D, "Image encryption with fractional wavelet packet method", Optik – International Journal for Light and Electron Optics,119(6), 286-291.
[16] Su Su Maung, and Myitnt Myint Sein, "A Fast Encryption Scheme Based on Chaotic Maps", GMSARN International Conference on Sustainable Development: Issues and Prospects for the GMS, 2008.
[17] J. Wang , "A Self-Adaptive Parallel Encryption Algorithm Based on Discrete 2D-Logistic Map", International Journal of Modern Nonlinear Theory and Application, vol 2, pp. 89-96, 2013.
[18] P.R. Sankpal, P.A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey", International Conference on Signal and Image Processing, pp. 102 - 107, Jan 2014.
[19] Manish Kumar, Pradeep Powduri, Avinash Reddy, "An RGB image encryption using diffusion process associated with chaotic map", Journal of Information Security and Applications, Elsevier, Vol.21, 20-30, 2015.
[20] Yicong Zhou, Long Bao,C.L.Philip Chen, ``A new 1D chaotic system for image encryption", Signal Processing, Elsevier, Vol.97, 172–182, 2014.