Received: 8 March 2015 | Revised: 10 April 2015 | Accepted: 19 April 2015
DOI: 10.37917/ijeee.11.1.5 | Vol. 11| Issue 1 | June 2015
Open Access
Iraqi Journal for Electrical and Electronic Engineering
Original Article

Multilevel Permutation with Different Block Size/ Stream Cipher Image Encryption

Dr. Abbas A. Jasim
Computer Engineering Department
University of Basrah
Basrah, Iraq
abbas.a.jasim@ieee.org

Hiba Hakim
Computer Engineering Department
University of Basrah
Basrah, Iraq
hebahakem@yahoo.com

Abstract: *In this work, a new image encryption method using a combined multilevel permutation with stream cipher is proposed. In the permutation algorithm, image is divided into blocks in each level and its blocks are rearranged by using pseudorandom permutation method. A new non linear stream cipher algorithm is also proposed that is based on combining several keys generated by Linear Feedback Shift Register (LFSR). The results shown that the proposed algorithm has a high security feature and it is efficient for image encryption. Practical tests proved that the proposed encryption algorithm is robust, provides high level of security and gives perfect reconstruction of the decrypted image.*

Index Terms— Image encryption, Permutation, Stream cipher, LFSR.

I. INTRODUCTION

Due to the rapid increase of information transmission throw the available unsecure channel, it became important to protect the confidentiality of information from intrusions arbitrary which may affect user's privacy [1, 2]. In daily live, digital images are widely used on the communication network; it is very necessary to confirm the security for such information transmitted on open networks such as internet. The perfect solution to achieve these requirements is information protection [3, 4]. There are two ways to protect digital images. The first way is image hiding such as watermarking and steganography. The other is image encryption. The difference between the two ways is that the image hiding concentrates on the existence of an image is kept secret, however the encryption protect the contents of an image without hiding its existence [5, 6].

Image encryption can be performed using stream cipher that is based on pseudorandom bit sequence, key. Two types of keys can be used to encrypt image data: Symmetric keys and Asymmetric keys. When the encryption and decryption keys are same, this is symmetric keys. If these keys differ, it is called asymmetric keys. Stream cipher is one type of Symmetric ciphers which encrypt one bit at a time [7]. From its name indication, stream ciphers use stream of key bit which is generated by key stream generator. Stream cipher based on secret key commonly generated using Linear Feedback Shift Register (LFSR). Stream cipher can be more secure using nonlinear key. One way to obtain nonlinear key is the combination of more than one LFSR.

In this paper, the proposed encryption algorithm is used to obtain secure image encryption using multi-level block permutation and nonlinear key stream cipher. The secret keys can be generated by using nonlinear filter generator based on linear feedback shift registers (LFSRs) each with the size of digital image pixels. In addition to this introductory section, this paper includes six other sections are organized as follows Section II gives an overview of the pseudorandom permutation system. The next Section III demonstrates the generation of key stream using LFSR. The new proposed encryption algorithm is proposed in Section IV. Section V and VI presents the visual and analytic results of the proposed system. Finally, Section VII concludes the paper.

II. PSEUDORANDOM PERMUTATION

Pseudorandom chaotic maps have been developed for image encryption to perform pixel permutation in image dimension space. Such that image pixels are rearranged using a 2D chaotic map to the newly calculated positions. Each pixel located in a given position x_n, y_n is relocated to the location calculated by the chaotic map x_{n+1}, y_{n+1}. The position is calculation depends on the predefined chaotic equation and two parameters a and b [8, 9, 10]. There are several chaotic transformation maps used for permutation purpose such as Henon, Baker, Cat ...etc.

Henon chaotic map system is a simple two dimension map was proposed by M. Henon (1976) as simplified model of Poincare map for Lorenz model [11].
The following two equations described the Henon map equations:

$$x_{n+1} = 1 - ax_n^2 + y_n \quad \dots (1)$$
$$y_{n+1} = bx_n \quad \dots (2)$$

III. LINEAR FEEDBACK SHIFT REGISTER

Key stream is used for encryption to encrypt given secret information. Key stream is a well-known in encryption especially for stream cipher. One way for key stream usage in encryption is done by performing bitwise XOR function between the secret information (plain text) and the key [11]. Linear feedback shift registers (LFSRs) is widely used as key stream generators. LFSRs as shown in Fig. 1 are suited for hardware implementation; they produce sequences having large periods and good statistical properties. The Key stream is used for encryption to encrypt information. The sequences $s = s_0, s_1, \dots\dots\dots$ produced by linear feedback shift register, depending on the following equation:
$s_n = \sum_{i=1}^{L} c_i s_{n-i}$, $n \geq L$, where L is the LFSR length. This function is called the feedback function.
The shift register state $S_n = (s_n, \dots\dots, s_{n+L-1}) = (s_n)_{n=0}^{\infty}$ is called the state sequence. Initially the first output states $s_0, s_1, \dots\dots, s_{L-1}$ are loaded into LFSR as initial states. They are called the LFSR secret key with period $2^L - 1$. The generated sequence (key stream) depends on both the initial state of the shift register and the feedback function [12].

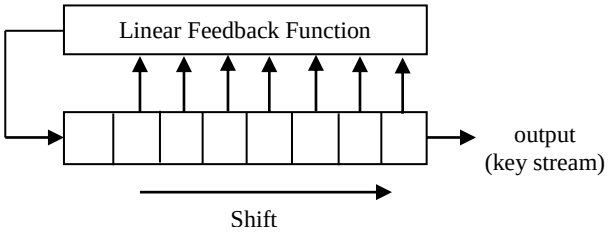


Fig. 1 Key stream generation

Stream cipher which use combinations of several LFSRs is applied in the prosed work to give strong cryptosystems. It is also make the encrypted image more homogenous and smoother than that resulting from permutation stage.

IV. THE PROPOSED ALGORITHM

The proposed image encryption algorithm consists of two stages iterative (multilevel) block permutation and nonlinear key stream cipher. In the first stage, the multi-level block permutation process is applied on the original image with the size (N × M) pixels in iterative manner. At each iteration, block size is changed and the block permutation is performed with new permutation parameters and so on. Initially the whole image is divided into four blocks each with size (N/2 × M/2) and (2 × 2) blocks permutation is done. These blocks are rearranged based on the chaotic map system such as Henon map in level-1. The 1st block permutated image resulting from the previous level is transferred to 2nd level that divides it into 16 (4 × 4) blocks and also passed to permutation process with new chaotic parameters. The blocking and permutation process repeated till reaching the last level where the number of blocks equal to number of pixels in the original image as shown in Fig. 2-a. In the second stage, stream cipher based on LFSR process was depended. In this stage, each pixel of the ciphered image resulted from the first stage considered as 8-bit binary code in order to be bitwise XOR-ed with the secret keys. (N × M) length key stream codes each with 8-bits are produced based on

LFSR and combining function. Now, the first bit of each pixel in ciphered image from first stage take to gather to be encrypted by using this formula $E(m,n)_i = X(m,n)_i$ xor $K(m,n)_i$. Where m [1: M], n[1:N], and i[1:8]. All bits of each pixel in ciphered image are ciphered by the key and resulting the final encrypted image as shown in Fig. 2-b.

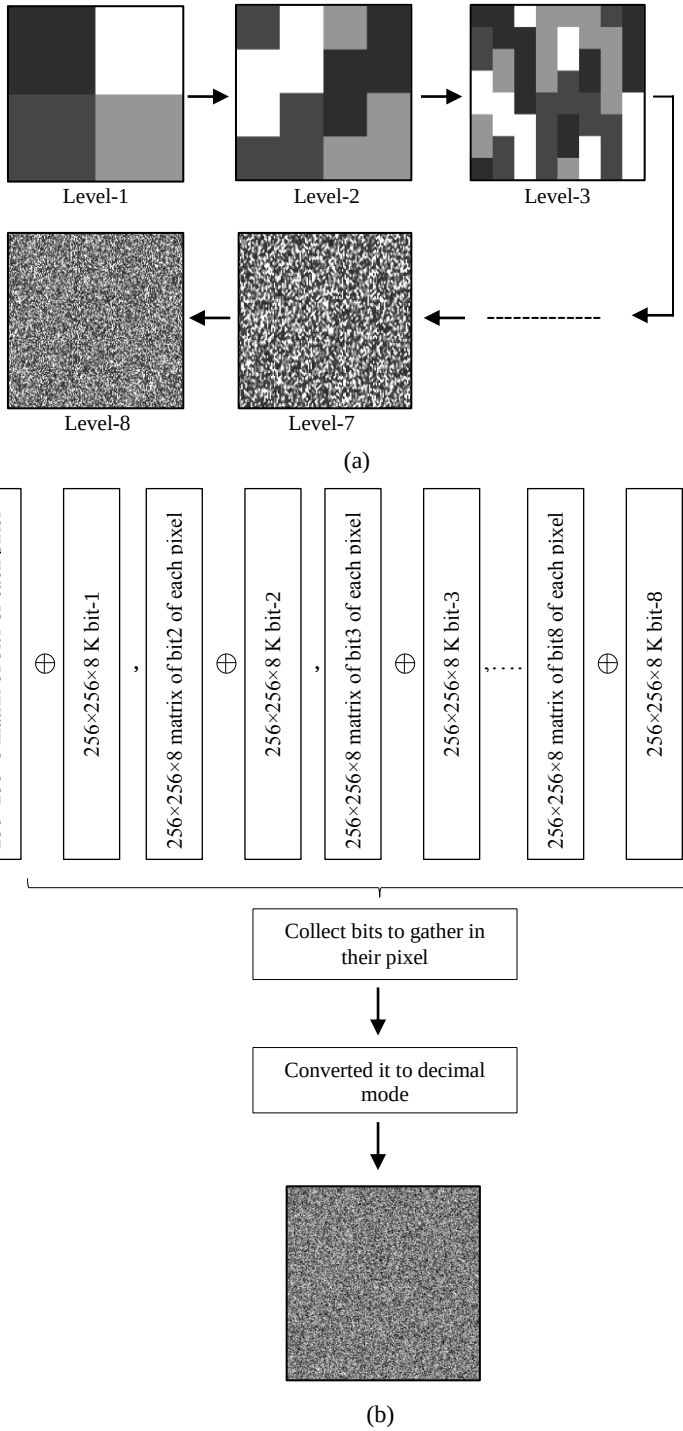


Fig. 2 Proposed system: (a) Permutation stage (b) Stream cipher stage

A. The Proposed Nonlinear Key Stream

The stream cipher stage of the proposed algorithm is based on nonlinear key stream generator. It supports 8-secret keys $k = k_1, k_2, \ldots\ldots, k_8$ each of length of (M×N). Each key is generated using LFSR that produced a binary sequence.

All these LFSRs are combined together using combining function F to produce the final nonlinear key. The combining function puts LFSRs together as 8-bit words then rotate this word located in the position i, j by (i + j) mod 7 to produce a non-linear stream key as shown in Fig. 3. Each 8-bit word of the key K is to be used in bitwise XOR operation with the permutated image resulting from the previous stage.

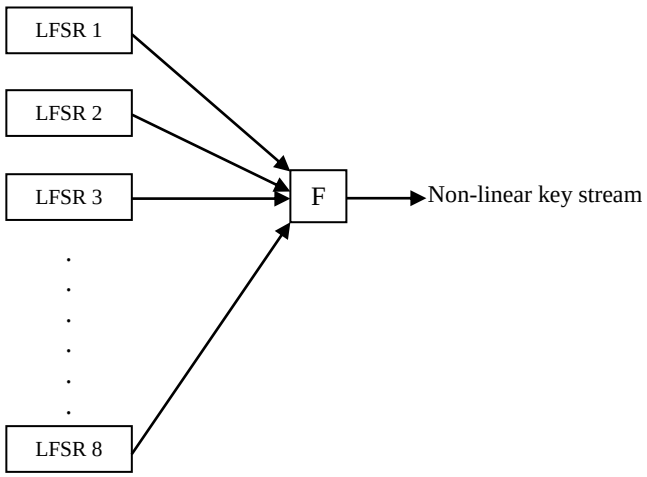


Fig. 3 Non-linear key stream generator

Combining multiple separate keys using combining function produces high complexity key. This key represents one of the strength factors of the proposed encryption algorithm.

B. Encryption Process

The proposed image encryption algorithm can be summarized in the following steps:

1. Load the original image of dimension N and M (in power of 2) for example (256×256);
2. Divide the image into blocks of size (N/2 × M/2) ;
3. Set chaotic parameters and map;
4. Compute the new location of each block;

5. Permute these block according to chaotic map;
6. Make Block size = Block size /2;
7. Repeat steps(3-6) until block size = one pixel;
8. Generate key stream for $k_1, k_2, \dots\dots, k_8$ with length (N × M) binary bits;
9. Combine LFSR outputs keys using the defined combining function to generate the nonlinear key K(N×M×8);
10. Arrange each pixel of resultant block permutated image to 8-bit binary code $(b_1, b_2, \dots\dots, b_8)$ to X(N×M×8);
11. Calculate final encrypted image: $E(n,m,i) = X(n,m,i)\ XOR\ K(n,m,i)$;
12. Arrange the new ciphered image to decimal code after return each bit to its position in a pixel;
13. Send the ciphered image.

C. Decryption Process

In the decryption process, the original image can be constructed by using the process much similar to that considered for the encryption algorithm but with the reverse order. The proposed image decryption algorithm can be summarized in the following steps:

1. Load the encrypted image, that is originally encrypted using the proposed encryption algorithm.
2. Generate key stream for $k_1, k_2, \dots\dots, k_8$ with length (N × M) binary bits;
3. Combine LFSR outputs keys using the defined combining function to generate the nonlinear key K(N×M×8);
4. Arrange each pixel of the received encrypted image to 8-bit binary code $(b_1, b_2, \dots\dots, b_8)$ to X(N×M×8);
5. Calculate stream cipher stage decryption: $S(n,m,i) = E(n,m,i)\ XOR\ K(n,m,i)$;
6. Arrange the new ciphered image to decimal code after return each bit to its position in a pixel;
7. Divide the image into blocks of initial size of (1 × 1) pixel;
8. Set chaotic parameters and map;
9. Compute the new location of each block;
10. Permute these block according to chaotic map;
11. Make Block size = Block size *2;
12. Repeat steps (8-11) until block size = (N/2×M/2);

V. VISUAL TRSTING

The proposed encryption algorithm has been done by using MATLAB R2008b on several original images of (256 × 256) pixels shown in Fig. 4-a in order to obtain the encrypted images shown in Fig. 4-b. The decrypted images illustrated by Fig. 4-c.

By comparing the original and encrypted images, the original images were successfully encrypted without any visual information observed in the encrypted images.

VI. ANALYTIC RESULTS

The proposed system can be evaluated by applying many analyses like correlation coefficient, mean square error, information entropy, and signal-to-noise ratio. The analysis results prove the suggested encryption algorithm is safe and has high security.

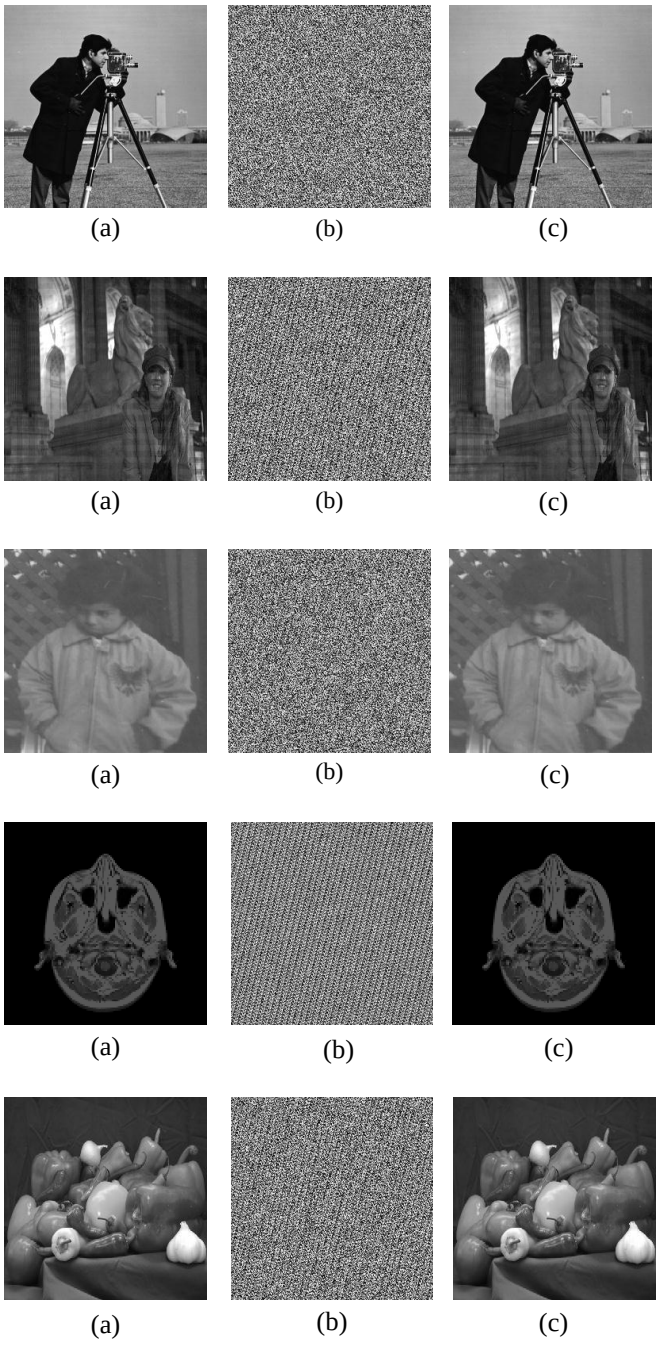
1) Correlation Coefficient:

Correlation gives good indication that tells about the relationship between two images. It is computed between the encrypted and the original images. If the correlation coefficient equal to zero, then the encrypted image is completely different from the original image [12]. The following formula demonstrates the Correlation Coefficient (*Cor*):

$$Cor = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j)-I_1')(I_2(i,j)-I_2')}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(I_1(i,j)-I_1')^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(I_2(i,j)-I_2')^2\right]}} \quad \dots(3)$$

Where: $I_1' = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} I_1(i,j)$ and $I_2' = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} I_2(i,j)$ referred to the mean of the original image $I_1(i,j)$ and encrypted image $I_2(i,j)$ respectively.

The correlation coefficient values between the original and encrypted images are listed in the first column of Table (I).



(a) (b) (c)

(a) (b) (c)

(a) (b) (c)

(a) (b) (c)

(a) (b) (c)

Fig. 4 Visual testing: (a) Original image of cameraman, Mandi, child, and peppers, (b) encrypted image, and (c) decrypted image.

2) Mean Square error:

The mean square error (MSE) is used to measure the difference between the original and decrypted image [13]. MSE can be determined by applying the following formula:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I_1(i,j) - I_2(i,j)]^2 \dots (4)$$

Where $I_1(i,j)$ represents the original image pixel and $I_2(i,j)$ is the decrypted image pixel. $N \times M$ represents the size of the image.
The mean square error values for the decrypted images are given in second column of Table (I). This value is equal to zero which indicated a perfect decrypted operation without any data distortion.

3) Peak Signal-to-Noise Ratio:

PSNR is defined as a ratio between the original image and encrypted image. It is usually measured in dB. This parameter is used to estimate the quality of encryption system. Lower value of PSNR shows the randomness of the encrypted image [14]. PSNR can be computed by the following equation:

$$PNSR = 10\ log_{10} \frac{(G-1)^2}{MSE} \dots (5)$$

Where G is the number of image in gray scale level. The PSNR value is small as seen in the third column of Table (I) which means that our proposed encryption system is strong.

4) Information Entropy:

Entropy is defined to show the data randomness in the system. It can be calculated as:

$$E(m) = \sum_{i=0}^{G-1} p(m_i) log_2 \frac{1}{p(m_i)} \dots (6)$$

That G is the gray level number in the image. $p(m_i)$ denotes the probability distribution of the image. The entropy value of encrypted image should ideally be 8 [11, 12]. The fourth column of Table (I) gives the entropy values of original images and their encryptions images. As seen, the entropy values of the encryption images are nearest to the theoretical value of 8. This means that the encryption system is secure against entropy attack.

TABLE (I) ANALYTIC RESULTS

Image	Cor	MSE	PSNR	Entropy
cameraman	0.0028	0	56.5319	7.9918
mandi	0.0043	0	56.0443	7.9251
child	0.0072	0	58.4022	7.9726
mri	0.0034	0	53.9283	7.9528
peppers	0.0030	0	56.3204	7.9391
Image 6	0.0027	0	56.6883	7.9652
Image 7	0.0012	0	56.8601	7.9932
Image 8	0.0050	0	56.2238	7.9954
Image 9	0.0004	0	54.6209	7.9757
Image 10	0.0035	0	54.6678	7.9517

VII. CONCLUSIONS

It is proposed a new combination of a permutation and stream cipher method for image encryption. This method is depends on blocking the original image to permute the block of image instead of the classical method which permuted the pixel itself. Chaotic map methods are utilized to change the block position in each level of permutation operation. The blocking operation begins with the four block of image pixel in the first level till reach to the smallest block size (pixel) in the last level. A nonlinear key stream is used in stream cipher operation. It is generated by non-linearly combining eight key each of them generated using separate LFSR. Each one of the eight LFSR has different length, initial state, and feedback function. These features make the proposed method has many points of strength. Many tests have been calculated to test the security of the encryption algorithm. Visual tests show that the encrypted image is drastically different from the original image and give no indication about the original image. The first stage, multilevel permutation produce different information chunks with different size interleaving. The second stage, stream cipher provides dual purposes. Its high complexity key production increase security. On the other hand, the stream cipher stage makes the final encrypted image more smooth and homogenous. According to the results obtained from adopted metrics, the entropy value is almost equal to the ideal and very low correlation value between the original and encrypted image that means high level of security and less similarity with the original image respectively. MSE value is equal to zero and correlation values between decrypted image and original image is equal to 1 for all tests which indicate that the proposed encryption technique can transmit the image data in unsecure channel efficiently and securely without any loss of original image data after reconstruction.

REFERENCES

[1] O. M. Abu Zaid, N. A. El-Fishawy, E. M. Nigm, and O. S. Faragallah, "A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Secuerity", International Journal of Computer Applications (0975 – 8887) Vol. 61, No. 5, pp. 29-39, January 2013.

[2] M. Prasad, and K.L.Sudha, "Chaos Image Encryption using Pixel shuffling", D.C. Wyld, et al. (Eds): CCSEA 2011, Computer Science & Information Technology (CS & IT) 02, pp. 169–179, October 2011.

[3] G. A. Sathishkumar, K. Bhoopathy, and N.Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps", International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 2, pp. 181-194, March 2011.

[4] S. Shekhar, H. Srivastava, and M. Dutta, "An Efficient Adaptive Encryption Algorithm for Digital Images", International Journal of Computer and Electrical Engineering, Vol. 4, No. 3, pp. 380-383, June 2012.

[5] S. Laskar, and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol. 4, No. 6, pp. 57-68, December 2012.

[6] C. Guang-hui1, H. Kai, Y. He and E. Xu, "Algorithm of Image Encryption based on Permutation Information Entropy", International Proceedings of Computer Science & Information Tech (IPCSIT), Vol. 53, pp. 102-108,October 2012.

[7] C. Paar, and J. Pelzl, "*Understanding Cryptography*", Springer-Verlag Berlin Heidelberg, 2010.

[8] R. K. yadava, B. K. Singh, S. K. Sinha, and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, Vol. 3, No. 6, pp. 14-20, June 2013.

[9] D.L. Mancilla, J. H. Lopez, R. J. Reategui, R. Chiu, E. Rauda, C. E. Hernandez, and G. H. Cuellar, " Statistical Analysis of Imaging Encryption Using Chaos", Latest Ternds in Circuit, Systems,Signal Processing and Automatic Control, pp. 86-90, March 2010.

[10] O. M. Abu Zaid, N. A. El-Fishawy, and E. M. Nigm, "Cryptosystem Algorithm Based on Chaotic Systems for Encrypting Colored Images", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No. 2, pp. 212-224, July 2013.

[11] A. Jolefaei, and A. Mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, vol. 19, Issue 2, pp. 117-125, October 2010.

[12] B. Aissa, D. Nadir, and R. Mohamed, "An Image Encryption Approach Using Stream ciphers Based on Nonlinear Filter Generator", Journal of Theoretical and Applied Information Technology, Vol. 41 No. 1, pp. 1-7, July 2012.

[13] D. C. Mishra and R. K. Sharma, " Grayscale-Image Encryption Using Random Hill Cipher over SLn(F) Associated With Discrete Wavelet Transformation", Applications and Applied Mathematics: An International Journal (AAM), Vol. 8, Issue 2, pp. 777-791, December 2013.

[14] P. Jagadeesh, P. Nagabhushan, and R. P Kumar, "A Novel Perceptual Image Encryption Scheme Using Geometric Objects Based Kernel", International Journal of Computer Science & Information Technology (IJCSIT) Vol. 5, No. 4, pp. 165-173, August 2013.