Double Phase Image Encryption and Decryption Using Logistic Tent Map and Chaotic Logistic Map

Preeti Kori[1], Prof. Ratnesh Dubey[2], Dr. Vineet Richhariya[3]
[1, 2, 3] Department of Computer Science
[1, 2, 3] LNCT, Bhopal

Abstract- *Doing a digital image transmission over internet need a secure protection against illegal copying. Unfortunately, many current data encryption methods such as DES, RES, AES, and other only suitable for test data, but not for digital image. Encryption security and encryption speed are two important aspects of image encryption algorithm. Digital image encryption is one of the secure methods to protect digital images against illegally copying when transmitted over unsecure channel. In this paper we use, properties of the chaotic maps such as sensitivity to initial conditions and random like behavior have attracted the attention to develop image encryption algorithms.*

Keywords- Digital image encryption; Digital image decryption; Chaotic logistic map; Logistic Tent map.

I. INTRODUCTION

Image Encryption, as the core technology of the image security is a direct and effective means of protecting the image's security. At the same time, image encryption is an indispensable technology in information hiding. Image encryption is different from text encryption due to some inherent features such as bulk data capacity and high correlation among pixels. Most image encryption adapts symmetric key crypto-system way. At present, the research of image encryption is mainly focused on the following aspects: spatial domain image encryption, transforming domain image encryption, image encryption based on the neural networks, image encryption based on chaotic, image encryption based on cellular automat and quantum code technology. In most of the natural digital images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). This unique characteristic lead to huge changes of each pixel of plain-image is not going to drastically reduce the quality of the cipher-image which will makes the content of cipher-image can still be visually identified by human.

One solution to overcome these problems is using chaotic system (i.e. chaotic logistic map) in a cipher because chaos is very sensitive to a small changes in the initial value and will produce the same effect as diffusion and confusion..

The chaotic functions have numerous properties such as randomness, ergodicity, and sensitivity to initial conditions. These properties create a close relationship between cryptosystems and chaos systems. Chaotic maps produce long Period, random like chaotic sequences, which are change significantly as a result of a small difference of the initial value or system parameters.

Decryption operation is similar to the encryption operation. The only differences being that the key is traversed in the reverse direction rather than the forward direction and the rotations based on the key bits are performed in a direction opposite to that used in Encryption. For Eg in encryption the row was rotated right-ward, then in decryption it is rotated left-ward. And in order to retain the correct sequence of rotation, the key is traversed in the reverse direction in all the rotation loops.

II. RELATED WORK

In 2008 Mohammad Ali Bani Younes and Aman Jantan [1] proposed a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. First of all the original image was divided into blocks, Before going through an encryption process, these blocks are transformed. At the receiver side these blocks are retransformed in to their original position and decryption process is performed. Advantage of this approach, is that it reproduce the original image with no loss of information for the encryption and decryption process we used a blowfish algorithm. The results implies that when we increased the number of blocks by using smaller block sizes, decreased correlation and increased entropy.

In 2008 Mohammad Ali Bani Younes and Aman Jantan [2] introduced a new permutation technique based on the combination of image permutation followed by encryption I.e. well known encryption algorithm called RijnDael. Their proposed technique work as follows: The original image was divided into 4 pixels × 4 pixels blocks then the blocks were transformed into new locations which were rearranged to make a permuted image using a permutation process presented, and then the generated image was encrypted using

the RijnDael algorithm. The correlation between image pixels was significantly decreased, due to rearrangement of the blocks and therefore it becomes very difficult to predict the value of any given pixel from the values of its neighbors. Furthermore, this process of dividing and shuffling the positions of image blocks confuses the relationship between the original image and the generated one. At the receiver, the original image can be reproduced by the inverse permutation of the blocks.

Amitava Nag et.al. [3] proposed a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation in year 2011.With the help of four 8-bit key applied, the pixel values are redistributed on different location using affine transform technique. In the next stage the transformed image divided into 2 pixels x 2 pixels blocks and every block is encrypted using XOR operation by using four 8-bit keys. The key used in this algorithm is s 64 bit long. Their results proved that after the affine transform the correlation between pixel values was significantly decreased.

Yicong Zhou and Sos Agaian [4] introduces a new method of applying the image steganography concept for image encryption. They used the concept of e PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image, it generates an encrypted image. The parameterized logarithmic image processing (PLIP) model is a mathematical framework based on set of precise operations that can be applied to the processing of intensity images valued in a bounded range. Result analysis shows that the algorithm has a very large key space and can withstand several common attacks.

In 2011 Yun sen and Gunayi Wang [5] proposed a modified chaotic map technique In order to improve the security of chaotic encryption algorithm. One of the advantage of their technique is that when we compared it with original logistic map, their proposed map makes it always be chaotic, and expands the iteration range from original (0, 1) to (0, 4λ) (λ>0.25). This is important for expanding key space of chaotic sequence and enhancing rate of change of chaotic signal. An encryption algorithm is designed based on this chaotic map and some analysis is presented to show its good efficiency. Experimental results show that the modified Logistic map possesses faster encryption, faster sequence generation rate, bigger key space and speed against the original logistic map in 2011.

In 2011 Zhang et al**.** proposed an image encryption method based on total shuffling scheme [6]. This method is characterized in that the secret code stream used in encryption is not only associated with the key, but also related to the plain image. Because the random number used in the diffusion process is obtained by iterating the skew tent map, and the number of iterations is determined by the previous pixel value of cipher image which includes the information of previous pixel value of plain image, the next random number is indirectly related to the previous pixel value of plain image. This plain image related encryption method is strongly against chosen plaintext attacks [7]. However, the first secret code is not safe enough to resist the chosen plaintext attack, which is pointed out and crypt analyzed in [8].

In 2012 Qiudong Sun et.al. **[**9] presented a random scrambling algorithm based on bit-planes decomposition of image. Their Algorithm starts by decomposing a gray image into bit-plane images, each image for separate bit plane. In the next step every bit plane image is shuffled by using a random scrambling algorithm. At last, all the shuffled bit plane images are merged according to their original levels on bit-planes and we obtained an encrypted image. Experimental results show that the proposed algorithm scrambled an image effectively as well as changed its histogram apparently. It has better efficiency and properties than the general random scrambling method. Therefore it has more stable scrambling degree than the classical method like Arnold transform.

In 2012 Sukalyan Som and Atanu Kotal [10] presented multiple chaotic maps based a new symmetric image encryption algorithm. In the proposed algorithm, with the help of generalized Arnold Cat Map, the plain image is first scrambled. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one-dimensional Logistic Map after preprocessing them to integers. The results indicates that the proposed algorithm can successfully encrypt and decrypt grayscale images with secret keys. it also exhibit that the proposed method is secure , loss-less, and efficient .

In 2013 AKester [11] proposed a new technique that contribute to the general body of knowledge in the area of cryptography application by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. With the help of RGB pixels, this algorithm ultimately encrypts and decrypts the images. The algorithm was implemented using MATLAB. In this method, neither the bit values of the pixel are affected and nor pixel expansion at the end of the encryption and the decryption process. In place of the numerical values are transposed, reshaped and concatenated with the RGB values, it shifted away from its

respective positions and the RGB values interchanged in order to obtain the cipher image. This shows that, the total change in the sum of all values in the image is zero. Therefore there is no change in the total size of the image during encryption and decryption process. Advantage of their method is that the characteristic sizes of image will remain unchanged, while the encryption process is being performed.

In 2013, Eslami et al. [12] suggested an improved algorithm over these shortcomings described in [8]. Two major improvements, such as using previous cipher image pixels to execute "add modulus and x-or" operations instead of plain image pixels, and enlarging the iteration times of chaotic system in every round, make the image encryption scheme proposed in [6] higher security against the chosen plaintext attacks with slower encryption speed as a trade off. Yong zhang [13] proposed a lookup table based encryption improvement on the schemes proposed in [6, 12] to improve the encryption speed.

III. PROPOSED METHODOLOGY

To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. There are many types of methods available that can do Image Encryption, and the majority of them are scrambling algorithms based on pixel shuffling. In pixel shuffling process, pixels positions of sub-image are scrambled within itself. Pixels shuffling based image encryption techniques have one problem that it cannot change the histogram of an image. Hence, their security performances are not good. The encryption method that combines the pixel exchanging and gray level changing can handles reach a good chaotic effect. The Proposed method focus on a image encryption technique based on pixel wise shuffling with the help of Logistic tent map and Chaotic map based pixel substitution. Figure shows the flow chart of proposed methodology.

Logistic Tent Map Based Pixel Permutation:

1). Convert the 2-D 8-bit grayscale and of size M×N, into 1-D which is denoted by $X = \{x_0, x_1, ..., x_{MN-1}\}$ using from top to bottom and then from left to right scanning method.

2). Iterate eq. 1.1 to obtain a pseudo random sequence of size M×N, denoted by.

$$F(x) = \begin{cases} x/p & x \in [0, p] \\ (1-p)/(1-p), & x \in (p, 1] \end{cases} \quad \text{...eq. 1.1}$$

3). Sort R in ascending order to get $S = \{s_0, s_1, ..., s_{MN-1}\}$.

4). According to the relationship of R and S, a scrambling vector $T = \{t_0, t_1, ..., t_{MN-1}\}$ is obtained such that $s_i = r_{t_i}$, i = 0, 1, …, MN-1.

5). Permute the plain image X with T to get $Y = \{y_0, y_1, ..., y_{MN-1}\}$ such that $y = x_{t_i}$, i = 0, 1, …, MN-1.

6). Convert the 1-D 8-bit grayscale permuted image Y, into 2-D which is denoted as:
$Y = \{y_{IJ} | 1 \le i \le M, 1 \le j \le N, y_{ij} \in \{0,1,\ldots.255\}\}$

using from top to bottom and then from left to right scanning method. Now this image is ready to transform to other end.

Chaotic Map Based Substitution:

A chaotic logistic map used to achieve the goal of image encryption is described as follow:

$$X_{n+1}=3.9999X_n(1-X_n);$$

Throughout the algorithm, we keep the value of the system parameter of the both logistic maps to be constant (i.e. 3.9999) which corresponds to a highly chaotic case while the initial conditions X0 for this maps is calculated using some mathematical manipulations on session keys.

We generate a sequence of L real numbers $f_1, f_2, ., f_L$ by iterating the logistic map using the initial condition. Where L=N*M and N and M is the size of Transformed image. Keeping in mind that we have considered only those values, which fall in the interval [0.1,0.9], the other values are discarded from the sequence. The real number sequence is converted into an integer sequence using the following formula

$$K_i = \mathrm{mod}(1000 * f_i, 256) \text{ Where i=1,2,3,…,L}$$

Next we transformed these 1-D L integer sequence into 2-D matrix of size M and N by using row major order. And apply bit wise XOR operation between Permuted imageY and Chaotic map Sequence P that yields the encrypted image Z.

$$Z = Y \oplus K$$

Where $Z = \{z_{ij} | 1 \le i \le M, 1 \le i \le N, z_{ij} \in \{0\ to\ 255\}\ 255\}$
and $z_i = y_i \oplus z_i$
$z_i = y_i \oplus z_i\}$

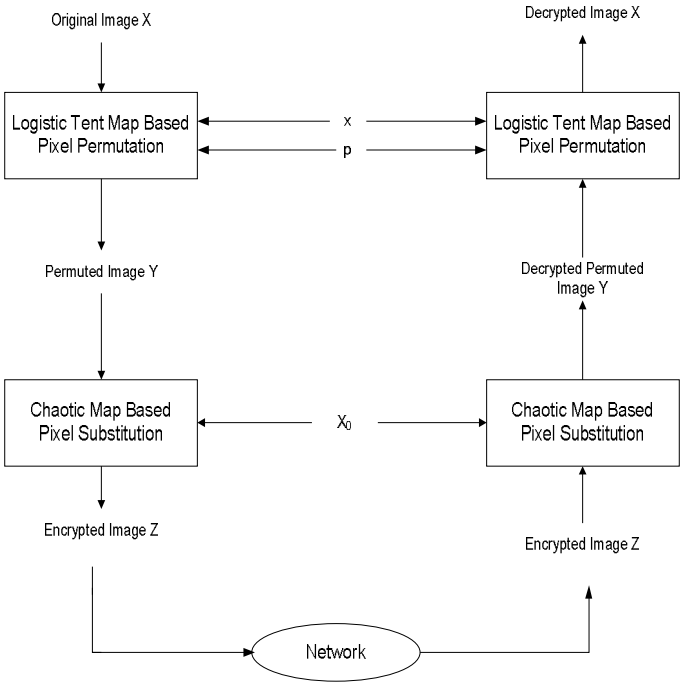


Figure: Image Encryption And Decryption Using

PERFORMANCE PARAMETER

The quality of the encrypted image is measured by calculation of certain parameters. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values.

A. Mean Square Error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE can be defined as the measure of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE = \frac{1}{MN} \sum_{I=1}^{M} \sum_{J=1}^{N} (C(i,j) - C'(i,j))^2$$

Where C(i, j) is the original image and C'(i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

B. Peak Signal to Noise Ratio (PSNR)

The PSNR depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR = \frac{20\ log 255^2}{MSE}$$

A low value of PSNR shows that the constructed image is of poor quality.

C. UACI and NPCR

Attacker tries to find out a relationship between the plain image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Trying to make a slight change such as modifying one pixel of the encrypted image, attacker observes the change of the plain-image. To test the influence of one pixel change on the whole encrypted image by the proposed algorithm, two common measures are used :

Number Of Pixel Change Rate (NPCR)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100\%$$

Unified Average Change Intensity (UACI)

$$UACI = \frac{1}{W * H}\left[\sum_{i,j} \frac{C1(i,j) - C2(i,j)}{255}\right] * 100\%$$

C1 and C2: two ciphered images, whose corresponding original images have only one-pixel difference. C1 and C2 have the same size.

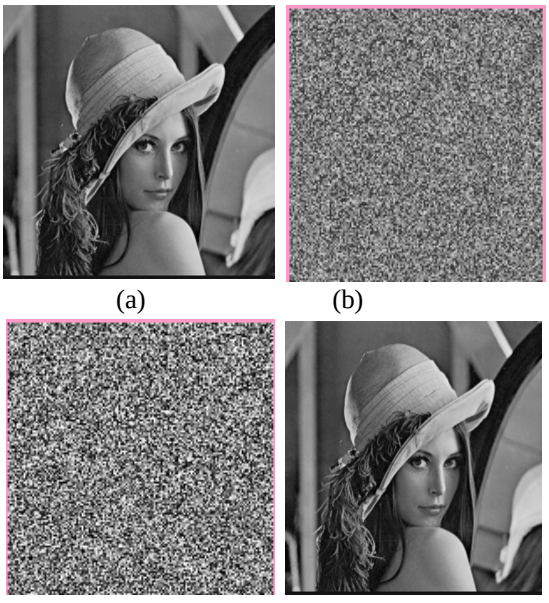
C1(i, j) and C2(i, j): grey-scale values of the pixels at grid (i,j). D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.W and H: columns and rows of the image.

IV. EXPERIMENTAL RESULTS

Proposed technique, are implemented on Windows PC having Intel 2.4 GHz processor and 2GB RAM, and run using Matlab 9a. We have considered 8 different image files in this experiment. All the images are 8 bit gray scale images and the dimension of all the image is 512× 512 pixels. In this paper we take an example of one image of Lenna and see the experimental result.

To demonstrated our method we used the gray image Lena as Shown in Fig.1(a), The results after permutation and text substitution with the help of secret key (x=0.12345 and X_0=.98765) are shown as in Fig.1(b) and (c) respectively. The pixel shuffling effect is very good and the encrypted image is very like the salt and paper noise. Fig.1(d) is the result of decryption, comparing with original image as shown in Figure 1(a), there is nothing to be lost.

Fig.2 (a) is the histogram of original image Lena. Figure 2(b) is the histogram of the encrypted image permuted by the proposed method. Fig. 2 shows that the histogram of the both image are not same so we can say that in encrypted image, the gray values of pixels are changed .



(a) (b)

(c) (d)

Figure 1 Results after image encryption and Decryption system for Lena.

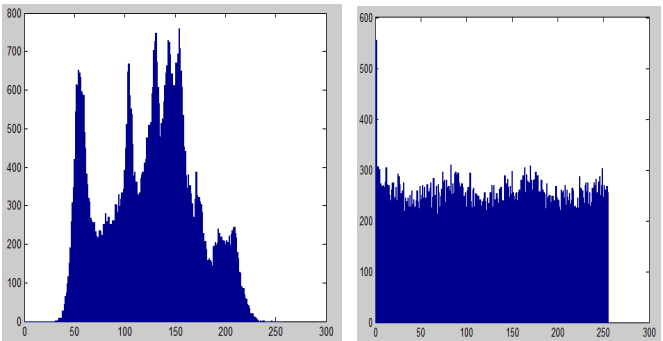


Figure 2 Histograms of the image Encryption and Decryption system for Lena

COMPARATIVE ANALYSIS :

We take the plain image Lena as an example to do 100 times of experiments, in each experiment randomly generate the secret key, and then calculate the NPCR and UACI and CC of produced cipher images. The average value of NPCR, UACI and CC are tabulated in Table 1. From Table 2, we can say that NPCR are better than that obtained using the other considered methods. We can see also from Tables 2 that the plain image is highly correlated in horizontal, vertical and diagonal directions, while the correlation coefficients of two adjacent pixels in proposed methods are close to zero, which demonstrate the proposed methods can well resist the statistical attacks. Fig. 3 and Fig. 4 shows the comparison graph of proposed method with other considered method with respect to NPCR and CC respectively.

Table 1 comparative analysis of proposed encryption technique

Methods	NPCR	UACI	CC
Zhang et.al	99.6100	33.4613	0.0094
Eslami et.al.	99.6115	33.4622	0.0481
Yong Zhang	99.6094	33.4635	0.0172
Proposed	99.6225	32..4515	0.0038

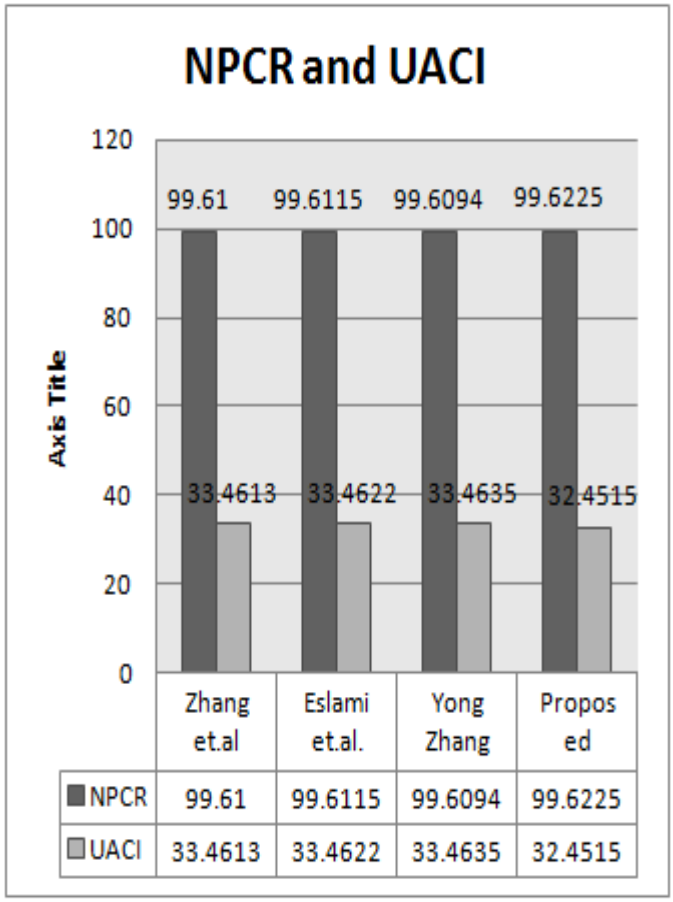


Figure 3 Average NPCR comparison with different image Encryption Methods.

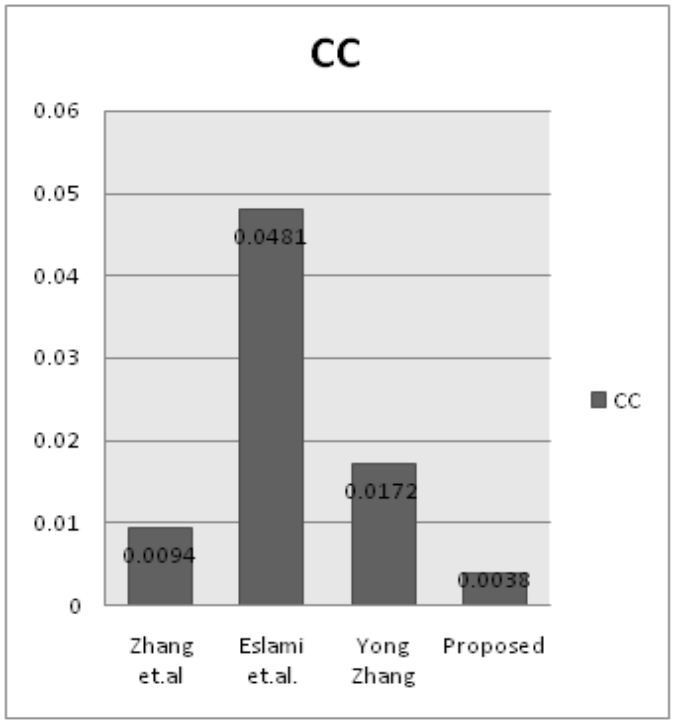


Figure 4 Shows average Correlation between pixel values and compare different image Encryption Methods.

V. CONCLUSION

In this paper we proposed a image encryption technique based on pixel wise shuffling with the help of skew tent map and Chao based pixel substitution. The encryption and decryption process are simple enough to be carried out on any large sized image, but provides enough security. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the gray image based data as well as in storage. The proposed encryption algorithm can ensure minimum distortion, maximum performance and maximum speed. The proposed encryption method in this study has been tested on different gray images and showed good results. The security level of image encryption and decryption is further increased.

We have designed our image Encryption and Decryption System using Matlab 7.8.0 to accomplish this research work. We have evaluated our proposed image Encryption and Decryption System on gray Scale image of 512*512. The experimental result proved that Correlation between pixel values are significantly decreased. The PSNR and NPCR obtained by our technique shows that the proposed technique gives better result than the existing techniques. We will future investigate in our proposed algorithm also can be applying to color image and Efficient encryption of large block size of data.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan,” Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03,2006.

[2] Mohammad Ali Bani Younes and Aman Jantan ,”an image encryption Approach using a combination of permutation technique followed by Encryption”, International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[3] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, “Image Encryption Using Affine Transform and XOR Operation”,IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011.

[4] Yicong Zhou, Sos Agaian,” Image Encryption Using the Image Steganography Concept and PLIP Model”, Proceedings of 2011 International Conference on System Science and Engineering, Macau, China - June 2011.

[5] Yue Sun, Guangyi Wang,” An Image Encryption Scheme Based on Modified Logistic Map”, Fourth International Workshop on Chaos-Fractals Theories and Applications,2011

[6] G. Zhang, and Q. Liu, “A novel image encryption method based on total shuffling scheme,” Opt. Commun. vol. 284, pp. 2775-2780, 2011.

[7] Y. Zhang, J. Xia, P. Cai, and B. Chen, “Plaintext related two-level secret key image encryption scheme,” TELKOMNIKA. vol. 10, pp. 1254-1262, 2012.

[8] X. Wang, and G. He, “Cryptanalysis on a novel image encryption method based on total shuffling scheme,” Opt. Commun. vol. 284, pp. 5804-5807, 2011.

[9] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma,” Image Encryption Based on Bit-plane Decomposition and Random Scrambling”, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012 .

[10] Sukalyan Som, Atanu Kotal,” Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps”, National Conference on Computing and Communication Systems (NCCCS),2012.

[11] Quist-Aphetsi Kester," A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, January 2013.

[12] Z. Eslami, and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," Opt. Commun. vol. 286, pp. 51-55, 2013.

[13] Yong Zhang," Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling" International Conference on Sensor Network Security Technology and Privacy Communication System, 2013.