Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map

Marutesh Chandra Sharma
M.Tech. Scholar
Computer Science & Engineering Department
Sachdeva Institute of
Technology Mathura ,India

Pankaj Sharma, PhD
Professor
Sachdeva Institute of
Technology Mathura, India

ABSTRACT

The Key encryption technique for any image that are being proposed here is initially applies scrambling to the location of the given or selected pixels. Afterward it applies chaotic map with using the format of 32 bit keys which currently the values of pixel image.

The one dimensional vector techniques which basically breaks the correlation of the pixels which are neighbouring and thus making the image unidentifiable and in such manner the scrambling operation is done.

After this chaotic mapping operation is applied to them which change the pixel values and this makes the image very meaningless. Hence by applying of keys so that the security of encryption level is increased further.

Infact at any images which are of large size the encryption and decryption operation are simple enough to be carried out but this provide very high level (enough level) security.

The encryption method which here is proposed for the study has been tested on different gray images and this has been showed some remarkable and good results. This is how the security level of encryption of image and decryption of image is further increased.

Keywords

Random Scrambling, Image Encryption and Chaotic Gauss Iterative Maps

1. INTRODUCTION

As in present time this has been observed that e-commerce, e-governance and e-government increasing day by day which requires lot of information which is multimedia based, this in turns transmission and information exchanges over the network is required every day.

Because of multimedia data characteristics it is easy for illegal interception of the information while the transmission over the network, hence there occurs a very great problem which is infact hidden in turns of information security and its validation [1]. Presently there are following principles types techniques are available for solving such problems [2,3]: first is the data encryption of data based on multimedia and next is to watermarking and embedding into the multimedia Digital Data.

First technique involves the scrambling of image and Chaotic Gauss Iterative Map. Using exchange of the positioning of pixels image scrambling can shuffle the image and the gray levels or colors can be changed by chaotic Gauss Iterative map. The objective of the above technique is to the image encryption.

So far there are so many types of methods are available which can be used to do the scrambling [1-6], and the majority of such algorithms are based on exchanging of pixels, which cansnot change the histogram of an image so the performances for the security are not good enough. The method which are based on bit-plane for the scrambling can combine the exchanging the pixels and gray level changing handily to reach a chaotic effect which is good.

Infact the chaotic map characteristics has drawn the focus of so many cryptographers to develop an encrypted new algorithm. The main property of chaotic maps are ergodicity, mixing, property and sensitivity to the initial condition or to the parameters based on system (system parameters) and this can be considered analogous to some cryptographic properties of ideal ciphers such as diffusion confusion, balance and avalanche property etc [7].

So many images based upon chaos encryption scheme have been developed in the recent years [8-12].

In such communication, the new evolution of the pattern which is called as scheme have developed which is based on shuffling the pixels of the image using random scrambling and then encrypting the resulting image using Chaotic Gauss iterative Map so that it can matched with the requirement that the transfer of the image is secure. In the next advancement in the scheme to encrypt the image as proposed solution a key which is hidden or can say secret as external key (as chen et al. [12] used for image encryption) of 32-bit and one chaotic Gauss Iterative maps are employed. The condition which set initial by using iterative map are derived using the external secret key by providing different weightage of its bits.

The organization of this paper is, with section two (2) refers the proposed methodology which will be used to encrypt the image, section three (3) deals with encrypted image quality parameters, section four (4) presents analysis of results of proposed method and their comparison with the other available methods, section five (5) summaries the research contribution of the paper and suggest the scope of this research work in future in the field of encryption and decryption.

2. PROPOSED IMAGE ENCRYPTION SCHEME

2.1 Encryption Algorithms

Image Encryption process of a given image is divided in to the following steps:

2.1.1. firstly let us select a gray scale image X of M×N pixel size with L bit per pixel .

2.1.2. Second step of proposed image encryption method based on decomposition of the input gray image X into bit plane. Since every pixel is form by L bits plane. So when it is decomposed, thus can get L bit plane image which is described by X(l) .where l=0, 1….L-1.Decomposition of image X into lth bit plane is computed by the formula expressed as below.

$$\mathrm{X}^{(l)} = B^{(l)}\left(X\right) \quad ....(1)$$

If X(m, n) is a pixel located at (m, n), then the lth bit of X(m,n) is:

$$\mathrm{X}^{(l)}\left(m,n\right) = B^{(l)} = \begin{Bmatrix} 1 \;\; if \left(x\left(m,n\right)/2^{(l)}\right) \bmod 2 = 1 \\ 0 \qquad\qquad otherwise \end{Bmatrix} \quad ....(2)$$

2.1.3. Next step is to applying Random Scrambling on every bit plane of decomposed image. First there is transformation of the bit plane image X(l) into a 1-D vector V(l).Then it uses a random natural number generator to produce random sequence RS and RD .it takes two different seeds to generate RS and RD .The length of RS and RD as same length of the rule of bit plane Scrambling given as.

$$V\left(R_S\left(i\right)\right) \leftrightarrow V\left(R_D\left(i\right)\right) i = 0,1,...,(M \times N - 1) \quad ...(3)$$

Once the Scrambling has been done for every bit plane .Hence merge the scrambled bit planes image to create a transform image XT (Scrambled). Next step it's to reconstruct the scrambled bit plane image according to their original level on bit plane. The Reconstruction of Scrambled image is done by the following formula.

$$X_T = \sum_{l=0}^{L-1} B^{-1(l)}\left(X^{(l)}\right) \quad ....(4)$$

For a pixel at position (m,n) ,this also have.

$$\mathrm{X}_T\left(m,n\right) = \sum_{l=0}^{L-1} 2^{(l)} \times X^{(l)}\left(m,n\right) \quad ....(5)$$

2.1.4. Next step is based on encryption of transformed image XT using Gauss iterative map .To achieve this the following steps are to be performed .

2.1.4.1 Encryption process utilizes an external secret key of 32-bit long. this secret key is divided into blocks of 8-bit each, referred as session keys.

K =k1*k2*k3*k4*k5*k6*k7*k8 (in hexadecimal)

Here, ki's are the alphanumeric characters (0–9 and A–F) and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as

K =K1*K2*K3*K4.(in ASCII).............(6)

Here, each Ki represents one 8-bit block of the secret key i.e. Session key.

2.1.4.2 A Gauss iterated map is used to achieve image encryption. In mathematics, the Gauss map (also known as Gaussian map or mouse map), is a nonlinear iterated map of the real values into a real interval. The function of Gauss iterated map is as follows:

Xn+1 = exp (-αXn2) + β ; ....(7)

Where α and β are real parameters. In the parameter real space Xn {\displaystyle x_{n}} can be chaotic for the value of β ranges from -1 to +1. The map function is symmetric about x = 0, and its maximum value is equals to c + 1 at x =0. For large values of |x|, the function approaches to the minimum value equals to c. Parameter b decides the width of the map function.

In our proposed method we have taken value of β as -0.58. The value of α is considered as 4.90.

So the Gauss iterated map for our algorithm is:

Xn+1 = exp (-4.9Xn2) – 0.58; ....(8)

The initial condition X0 for this map is calculated using some mathematical manipulations on session keys.

2.1.4.3 To calculate the initial condition X0 for the Gauss Iterative map, choose two blocks of session keys i.e. K1 K2 and convert them into a binary string as:

B =K11K12K13…K18K21K22…K28; ....(9)

Next, compute a real number X01 using the above binary representation as:

X01 = decimal (B)/216 ....(10)

Further, let us compute another real number X02 as follows

$$X_{02} = \sum_{i=5}^{8} (k_i)_{10} \,/\, 64 \quad ....(11)$$

Here ki's are parts of secret key in hexadecimal mode as explained above. Now compute the initial condition X0 for the first Gauss Iterative map using X01 and X02 as:

$$X_0 = (X_{01} + X_{02}) \bmod 1. \quad ....(12)$$

2.1.4.4 Now generate a sequence of Z real numbers f1,f2,.,fZ by iterating the Gauss Iterative map using the initial condition obtained in step 2.1.4.3 Where Z=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

$$P_k = \mathrm{mod}(1000 * f_k, 256) \quad ....(13)$$

Where k=1, 2,3,…,Z

2.1.4.5 Next, now transformed these 1-D Z integer sequence into 2-D matrix of size M and N by using row major order. And apply bit wise XOR operation between transformed image and chaotic map that yields the encrypted image Xc.

Now this image is ready to transmit to other end.

2.2. Decryption Algorithm

A process which is reversed to the image encryption is called decryption, it is procedure which is symmetric by which the cipher image can be converted into the original image. It has the following steps :

2.2.1. The input is a gray scale encrypted image XC of M×N pixel size with L bit per pixel.

2.2.2. The process of decryption using Gauss Iterative chaotic map is completely similar to the encryption process described above; now select same 32 bit session key to decrypt image called XT.

2.2.3. Bit plane decomposition of the Decrypted image XT into lth bit plane is computed using the formula described as.

$$\mathrm{X}^{(l)}(m,n) = B^{(l)} = \begin{Bmatrix} 1if\left(x(m,n)/2^{(l)}\right)\mathrm{mod}\,2 = 1 \\ 0 \qquad\qquad\qquad otherwise \end{Bmatrix} \quad .....(14)$$

Then it transforms the bit-plane image XT(l) into a 1-D vector V(l) .

2.2.4. The Next step is to applying anti scrambling on every bit plane image of decrypted image XT . now use again random natural number generator and use the same a couple of seeds used at encryption time to produce same random sequences RS and RD with the same length as V, and Anti scrambles the 1-D vector V as given formula.

$$V^{(l)}\left(R_S(i)\right) \leftrightarrow V^{(l)}\left(R_D(i)\right) i = 0,1,....(M \times N - 1); l = 0,1,....L-1 \quad ...(15)$$

When the anti-scrambling has been done, final step is to merge the anti scrambled bit-plane images according to their original levels on bit-planes and gained an Original image X.

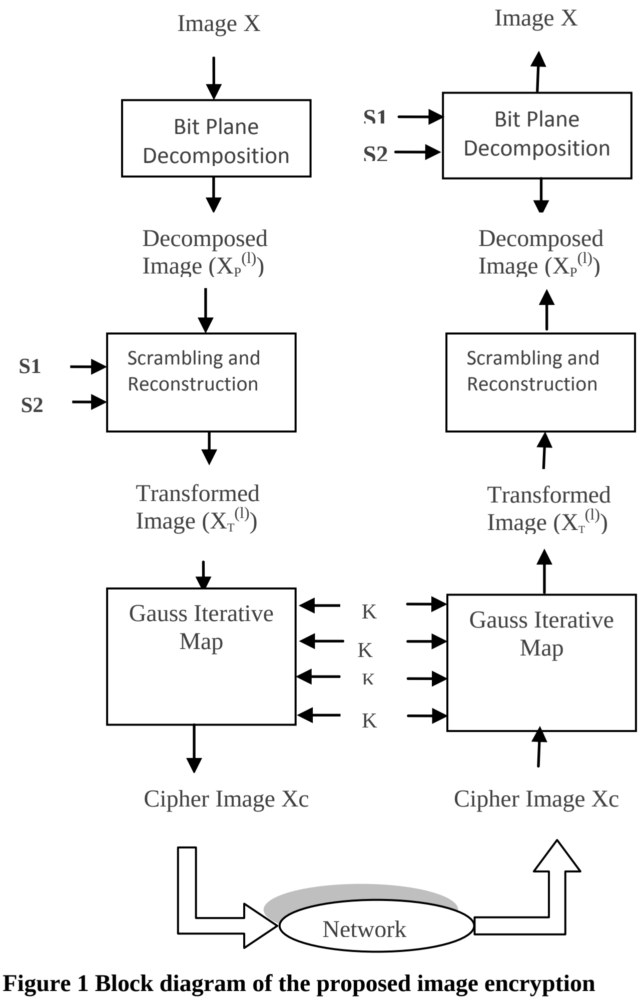


Image X
Bit Plane Decomposition
Decomposed Image ($X_P^{(l)}$)
S1
S2
Scrambling and Reconstruction
Transformed Image ($X_T^{(l)}$)
Gauss Iterative Map
K
K
K
K
Cipher Image Xc
Image X
S1
S2
Bit Plane Decomposition
Decomposed Image ($X_P^{(l)}$)
Scrambling and Reconstruction
Transformed Image ($X_T^{(l)}$)
Gauss Iterative Map
Cipher Image Xc
Network

Figure 1 Block diagram of the proposed image encryption system working

3. EVALUATION METRICS

The encryption algorithm ability is evaluated on the basis of evaluation metrics to substitute the original image with uncorrelated encrypted image, which are the deviation of histogram HD, and the correlation coefficient rxy .

3.1 The Histogram Deviation

The histogram deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [13]. The steps of calculating this metric are:

- Estimate the histogram of both the original and the encrypted images.
- Estimate the absolute difference between both histograms.
- Estimate the area under the absolute difference curve, divided by the total area of the image, as follows:

$$\boldsymbol{DH} = \frac{\left(\frac{\boldsymbol{d0}+\boldsymbol{d255}}{\boldsymbol{2}} + \sum_{\boldsymbol{i=1}}^{\boldsymbol{254}} \boldsymbol{di}\right)}{\boldsymbol{MXN}} \quad ....(16)$$

Where di is the amplitude of the absolute difference curve at the gray level i. M and N are the dimensions of the image to be encrypted. The higher the value of DH is, the better the quality of the encrypted image [13].

3.2 The Correlation Coefficient

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images [13]. This metric can be calculated as follows:

$$\boldsymbol{r_{xy}} = \frac{\boldsymbol{cov}\ (\boldsymbol{x},\boldsymbol{y})}{\sqrt{\boldsymbol{D}(\boldsymbol{x})}\sqrt{\boldsymbol{D}(\boldsymbol{y})}} \quad \textbf{....................(17)}$$

Where x and y are the gray-scale values of two pixels at the same indices in the plain and cipher images. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i$$
$$D(x) = \frac{1}{L}\sum_{i=1}^{L} \left(x_i - E(x)\right)^2$$
$$cov(x,y) = \frac{1}{L}\sum_{i=1}^{L} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \quad ....(18)$$

Where L is the number of pixels involved in the calculations. The closer the value of rxy to zero is, the better the quality of the encryption algorithm.

3.3 Number of Pixel Change Rate (NPCR)

It is a common measure used to check the effect of one pixel change on the entire image. This indicates the percentage of different pixels of two images. Let Io(i, j) and Ienc(i, j) be the pixel values of original and encrypted images Io and Ienc at the ith pixel row and jth pixel column respectively [34]. This metric can be evaluated as follows-

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad ..(19)$$

Where D(i,j) = 0 if Io(i,j) = Ienc(i,j); else D(i,j) = 1.

W and H: columns and rows of the image.

3.3.1 Unified Average Changing Intensity (UACI)

A small change in plaintext image must cause some significant change in ciphertext image. UACI identifies the average intensity of difference in pixels between the two images [34]. It can be measured as-

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \qquad ...(20)$$

Where 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).

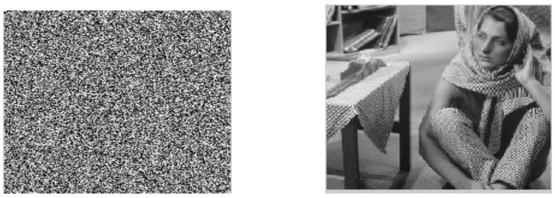
D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.

W and H: columns and rows of the image.

4. SIMULATION RESULT

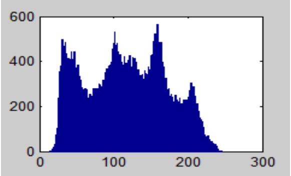
In this experiment , it does bit-plane scrambling and Chaotic Gauss Iterative Map one tismeover the gray image Lena as shown in Fgure 2(a), the size of the image is 256*256. The results of the same has been shown in the Figure2(b). Apparently, just through one time or two times bit-plane random scrambling, the scrambling effect is very good and the scrambled image is very like the white noise. Figure 2(c) is the result of anti-scrambling, comparing with original image as shown in Figure 1(a), there is nothing to be lost.Figure 3(a) is the histogram of original image Lena. Figure 3(b) is the histogram of the result image scrambled by the proposed method .Figure 3(c) shows the histogram of the decrypted image .

(a) Original image of Lena.

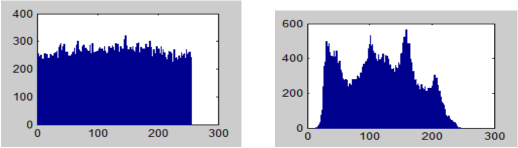


(b) Encrypted Image (c) Decrypted image

Figure 2 Results after image encryption and Decryption system for Lena.



(a)Histogram of the Original Image of Lena



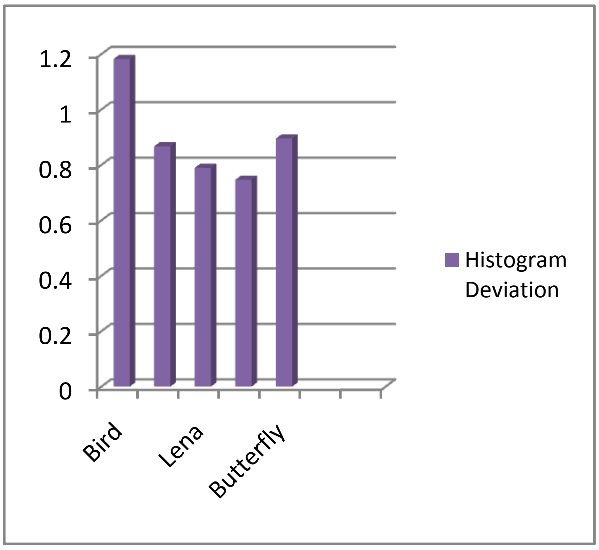
(b) Histogram of the Encrypted image (c) Histogram of the Decrypted image

Figure 3 Histograms of the image Encryption and Decryption system for Lena.

The Histogram Deviation calculation of the Seven Gray scale encrypted images Flower, Bird, Lena, Hours, Nature, X-Plane and Airplane X-Plane and Airplane are tabulated in Table 1, from which it can be said that the Histogram Deviation than that obtained using Random Scrambling and X-OR operation .

Table 1 Show Histogram Deviation Calculation.

Image Name	Histogram Deviation
Bird	1.1823
Airplane	0.8675
Lena	0.7896
Cat	0.7465
Butterfly	0.8954

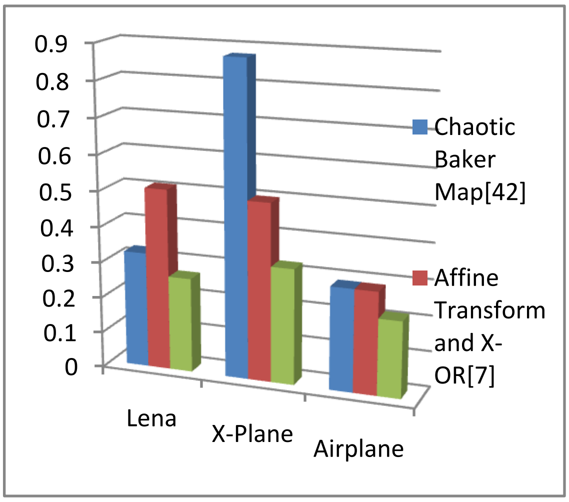


Graph 1: Show Histogram Deviation Calculations.

The Average correlation coefficients between the corresponding pixels values of the three encrypted images Lena, X-Plane and Airplane are tabulated in Table 2, from which it can be said that the correlation coefficients are worse than that obtained using secret key of an image X-OR operation and Compare average correlation coefficient between pixel values on three different images encryption method.

Table 2 Shows average Correlation between pixel values and compare different image Encryption Methods

Image Name	Chaotic Baker map [42]	Affine Transform and X-OR [7]	Proposed Method.
Lena	0.3247	0.5088	0.2654
X-plane	0.8762	0.4983	0.3242
Airplane	0.2877	0.2873	0.2144

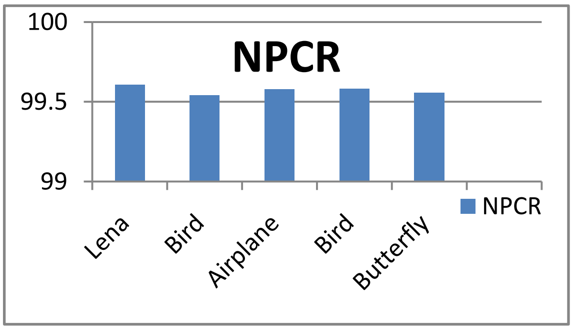


Graph 2: Graph average Correlation between pixel values and Compare different image Encryption Methods.

NPCR is a common measure used to check the effect of one pixel change on the entire image. This indicates the percentage of different pixels of two images. We used five images to analyze the NPCR, which are Lena, Cat, Airplane, Bird, and Butterfly.

Table 3 Shows Number of Pixel Changing Rate Calculation between plaintext image and encrypted image

Image Name	NPCR
Lena	99.6094
Cat	99.5422
Airplane	99.5804
Bird	99.5834
Butterfly	99.5575



Graph 3: shows Pixel Changing Rate of proposed method

The NPCR of the proposed method shows better results as it has NPCR value more than 90 as compare to the methods which has been taken into consideration for the further study.

High value of NPCR refers that the change in pixel value has high impact on the appearance of image.

The unified average changing intensity (UACI) represents the average intensity of difference in pixels between the two images: the plaintext image and the encrypted image. Table 5.4 below represents the UACI for three different plaintext images and their corresponding ciphertext images.. Figure 5.14 shows the graphical representation of UACI for the original images and encrypted images.

Table 4 Shows Unified average Changing Intensity Calculation for plaintext image and encrypted image

Image	UACI
Lena	6.8893
Airplane	22.5342
Butterfly	4.7379

5. CONCLUSION

The Image encryption technique that has been proposed using the symmetric key that basically scrambles the location of the pixels first and the applies chaotic map with the help of 32 bit keys which eventually chages the pixel values of the image. The encryption and decryption process are enough simple for the execution on any image of large sizes with enhanced security. Here in this proposed encryption algorithm we are ensuring many criteria and these are lossless, maximum performance , minimum distortion and maximum speed. This has been done using MatLab 7.8.0 to design the system of image encryption and image decryption to eventually accomplish the research.

The proposed image encryption and image decryption have been evaluated on the basis of Gray Scale Image. The experimental outcome assured that Correlation between the Pixels Value are decreased significantly.

In future we will be investigating this proposed algorithm , can be applied to the colour image, in defence sector for variety of information exchange such as maps exchange, plan of defence forces, information exchange of miscreants. In medical science there can be instances where critical information are to be transformed over the network in a secured manner. Now a days there evolving a system in many countries where the judiciary department seeks some critical information regarding a case such as retina scan report, finger print scan on the other side, this needs a serious role of encryption technique as failing it may lead to a wrong judgement. Hence proposed encryption technique will overcome such issues.

6. REFERENCES

[1]. Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University , vol. 09 , 2012.

[2]. H. Zhao, W. Y. Wen, "A Survey of Digital Image Scrambling Techniques," Fujian Compute, No. 12, pp. 10-12, 2007.

[3]. Z. J. Tang, X. Lu, W. M. Wei, S. Z. Wang, et al, “Image Scrambling Based on Bit Shuffling of Pixels,” Journal of Optoelectronics • Laser, vol. 18, no. 12, pp. 1486-1488, 1495, 2007.

[4]. W. Ding, W. Q. Yan, D. X. Qi, “Digital Image Scrambling Technology Based on Arnold Transformation,” Journal of Computer-aided Design & Computer Graphics, vol. 13, no. 4, pp. 338-341, 2001

[5]. Y. P. Cheng, D. S. Fu, X. Wang, “Compound Chaotic Sequence Based Encryption Algorithm for Image,” Computer Applications and Software, vol. 23, no. 12, pp. 102-103, 115, 2006.

[6]. C. Zou, R K. Ward, D. X. Qi, “A new digital image scrambling method based on fibonacci number,” Proceeding of the IEEE Inter Symposium on Circuits and Systems, Vancouver, Canada, vol. 3, pp. 965-968, 2004

[7]. N.K. Pareek , Vinod Patidar , K.K. Sud “Image encryption using chaotic logistic map” Image and Vision Computing volume 24, pp.926–934, 2006

[8]. Fridrich Jiri, “Symmetric ciphers based on two dimensional chaotic maps”, Int. J. Bifurcat Chaos vol. 8, No. 6, pp. 1259–1284, 1998

[9]. J.C. Yen, J.I. Guo, “An efficient hierarchical chaotic image encryption algorithm and its VLSI realization”, IEEE Proc. Vis. Image Process, 147, pp. 167–175, 2000

[10]. C.C. Chang, M.S. Hwang, T.S. Chen, “A new encryption algorithm for image cryptosystems”, J. Syst. Software 58 (2001) 83–91.

[11]. S. Li, X. Zheng, “Cryptanalysis of a chaotic image encryption method,” Proceedings of the IEEE International. symposium on circuits and systems, Scottsdale, AZ, USA, 2002.

[12]. G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, Chaos Solitons Fractals, vol. 21, pp. 749–761, 2004.

[13]. S. Mandal and S. Banerjee, "A chaos-based spread spectrum communication system," Nat. Conf. Nonlinear Sys. Dynamics, Indian Institute of Technology, Kharagpur, Dec 28-30, 2003