Chaos Based Image Encryption using Expand-Shrink Concept

Dr. Naveenkumar S K*, Panduranga H T*, and Kiran**
*Dept. of studies in Electronics , University of Mysore, Hemagangthri-PG Centre, Hassan-Karantaka, INDIA
**Dept. of E and C Engg., Malnad College of Engineering, Hassan, karnataka, INDIA

Article Info

Article history:

Received Feb 26, 2014
Revised May 15, 2014
Accepted May 20, 2014

Keyword:

Chaotic map
Column-expansion
Decryption
Encryption
Row-expansion

ABSTRACT

Image information security plays a vital role in computing and communication technologies. This paper describes a new concept of expand and shrink to enhance the strength of chaos based image encryption technique. This method consists of both permutations as well as substitution process for image scrambling and encryption. In permutation plain image is shuffled using chaos technique. Input image undergo two times chaos permutation in-between expand and shrink process leads to substitution. Permutation decreases the correlation between the pixel and substitution increases the entropy of encrypted image. Proposed encryption technique works for both gray-scale and color image. From the experiment highly scrambled image is obtained at the end of encryption process. Decryption process employs exactly reverse process of encryption which results in the reconstructed images.

Corresponding Author:

Panduranga H.T,
Research Scholar,
DOS in Electronics,
University of Mysore,
+91-9448649438.
Email : ht_pandu@yahoo.co.in

1. INTRODUCTION

With the development of computer network technology, digital image is widely used in various fields of society. However, due to openness of the network, the security of image is threatened seriously, so the image encryption becomes the most effective way to guarantee transmit security of images. Chaos is seemingly a random movement of deterministic system. Chaos system has the properties of ergodicity, boundedness, sensitivity to initial conditions. Therefore, using chaotic system in image encryption can meet certain security requirements. However, the chaotic encryption algorithms,which utilize one-dimensional chaos map, multi-dimensional chaos map and ultra-dimensional chaos map are all to transform the image pixel position and pixel values.

xindyuan Wang.et[1] presented a novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. secret keys will be processed by key generator before they can really be used in the encryption scheme, and in this stage this paper associates plain image with secret keys; Secondly, by imitating the trajectory of water wave movement, encryption algorithm will do scrambling operations to the image. Thirdly, combines water drop motion and dynamic look up table to realize diffusion operations. For an 8 bits pixel, this algorithm will just dispose the higher 4 bits, which is because the higher 4 bits contain the vast majority of information of the image. Ahmed A.abd El-Latif.et[2] all have proposed a hybdird choatic syatem and cyclic elliptic curve for image encryption and provides a external secret key of 256 bit and one generalized chaotic logistic map. using the cyclic elliptic curve to derive generated keystream are mixed with key sequences. Ruisong Ye [3] presented a novel chaos based image encryption scheme with an efficient permution diffusion mechanism. generaly permutaton diffusion ,echanism permuting the positions of image pixels in order to reduce the high correlation between adjacent pixels of plain image and gray value sequences for a two-way diffusion of gray values. The proposed encryption scheme is easy to manipulate and can be applied to any image with unequal width and height as well.Xingyuan Wang [4] have proposed A novel colour image encryption algorithm based on chaos . they uses chaotic system to encrypt the R,G,B components of a colour image at the same time and makes these three components affect each other. so it can reduces correlation between R,G,B components and secrity is increased. G.A.Sathish Kumar et. [5] all proposed A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems.The algorithm makes use of full chaotic property of logistic map and reduces time complexity. The algorithm calculates the permuting address for row by bit xor′ıng the adjacent pixel values of original image. Similarly, the algorithm calculates the permuting address for column by bit xor′ıng the adjacent pixel values of original image.The diffusion is performed after scrambling and is based on two chaotic maps. Liu Hongjun, Wang Xingyuan [6] proposed Color image encryption based on one-time keys and robust chaotic maps. piecewise linear chaotic map as used for the generator of a pseudo-random key stream sequence. The initial conditions were generated by the true random number generators, the MD5 of the mouse positions. Hongjun Liu , Xingyuan Wang [7] presented Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Bit-level permutation and high-dimension chaotic map used to encrypt color image. Firstly, convert the plain color image of size (MN) into a grayscale image of size (Mx3N), then transform it into a binary matrix, and permute the matrix at bit-level by the scrambling mapping generated by piecewise linear chaotic map (PWLCM). Secondly, use Chen system to confuse and diffuse the red, green and blue components simultaneously. Fariborz Mahmoudi.et [8] all, presented Image Encryption Using Chaotic Signal and MaxHeap Tree. Based on chaotic sequence signal and Max-Heap tree image is pixel values are permuted. Zhi-liang Zhu [9] presented A chaos-based symmetric image encryption scheme using a bit-level permutation. Bit level permutation is not only changes the position of the pixel but also alters its value. Here image cryptosystem employing the Arnold cat map for bit-level permutation and the logistic map for diffusion. The rest of this paper is organized as follows. Section 2. briefly explain the concept of chaotic map. Section 3. Explains basics of expand-shrink process.Section 4. describes the proposed different encryption algorithms. Performance analysis and experimental results described in section 5.. Section 7. concludes the paper.

2. CHOATIC MAP

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behavior regarding complexity, chaotic properties cycle length, chaotic interval, periodic windows, etc., sensitivity to initial conditions and reaction to trajectory perturbations, etc., that influence the structure or behavior of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map and efficiency, it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to fulfill the security and efficiency requirements of a good cryptosystem. For their mathematical simplicity there are two options: logistic map and tent map. The logistic map is represented by

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

The logistic map chaotic signal used has primary values of $X_0 \in [0, 1]$ and $r \in [3.57, 4]$.

3. EXPAND-SHRINK CONCEPT

Generally image is represented by a matrix of pixels and each pixel represented by 8 bit intensity value. Expand-Shrink process consists of row-expansion and column-expansion. In row-expansion, image of size $m * n$ is expanded into binary image of size $m * (n * 8)$ as shown in Figure 3 and in column expansion, image of size $m * n$ is expanded into binary image of size $(m * 8, n)$ as shown in Figure 3 (rotated by 90 degree). In shrink process $m (n * 8)$ or $(m * 8) * n$ binary image is converted into $m * n$ gray scale image.

4. PROPOSED METHODS

This section describes two proposed methods along with the basic chaos method for image scrambling. Method 1 explains general chaos based permutation, method 2 explains chaos based encryption by using expandshrink process and method 3 explains colour image encryption by using chaotic map and expand-shrink process.

Figure 1. Lena image

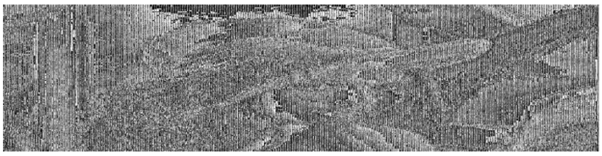


Figure 2. Row-expanded binary image

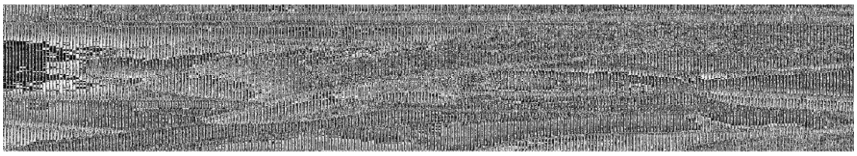
4.1. Method 1

Block diagram of method 1 in shown in Figure 4.3.. Detained Encryption process explained below.
Step 1:Input image of size m ———————————————— n is converted into one dimensional vector
$I = I_1, I_2, ::::::::::::::::, Im * n$
Step 2:With a given initial parameter and r=3.99999 by using Eq.1 chaotic sequence generated.
X = $X_1, X_2, ::::::::::::::::::::::, X_{m * n}$.
Step 3:The chaotic sequence X is sorted in ascending order and we get a new set
$Y = sort\ (X) = y_1, y_2, :::::::, y_{m * n}$.
Step 4:According to set Y value, Input image is permuted and to get an encrypted image.

4.2. Method 2

Block diagram of proposed Method in shown in Figure 4.3.. Input image undergo row-expansion process and steps involving in row-expansion process is explained below.
Step 1:Input image of size m $*$ n is expanded in row wise into binary image of size $m * (n * 8)$.
Step 2:Binary image is converted into one dimensional vector. $I = I_1; I_2; :::::::::::::::::; I\ m * (n * 8)$
Step 3:With a given initial parameter and r=3.99999 by using Eq.1 chaotic sequence generated.
$X = X_1, X_2, ::::::::::::::::::::::, X_{m*(n * 8)}$.
Step 4:The chaotic sequence X is sorted in ascending order and we get a new set
$Y = sort(X) = y1, y_2, ::::::::::, y_{m*(n * 8)}$.
Step 5:According to set Y value, Binary image is permuted and get a Permuted Binary image.
Permuted Binary image is converted back into permuted gray scale image of size $m * n$ using shrink process.

Permuted gray scale image obtained from shrink process is applied to column-expansion process. Steps involving in column-expansion process is described below.
Step 1:Permuted image of size $m * n$ is expanded in column wise into binary image of size $(m * 8) * n$.
Step 2:Binary image is converted into one dimensional vector $I = I_1, I_2, ::::::::::::::::, I\ (m * 8) * n$
Step 3:With a given initial parameter and r=3.99999 by using Eq.1 chaotic sequence generated.
$X = X_1, X_2, ::::::::::::::::::::::, X_{(m * 8) * n}$.
Step 4:The chaotic sequence X is sorted in ascending order and we get a new set
$Y = sort(X) = y_1, y_2, ::::::::::, y_{(m * 8) * n}$.
Step 5:According to set Y value, Binary image is permuted and get a Permuted Binary image.
Step 6:Finally encrypted image is obtained from shrink process.



$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)}$$

Figure 3. column-expanded binary image (rotated by 90)

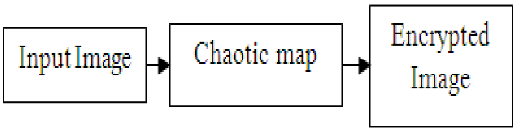


Figure 4. Method 1

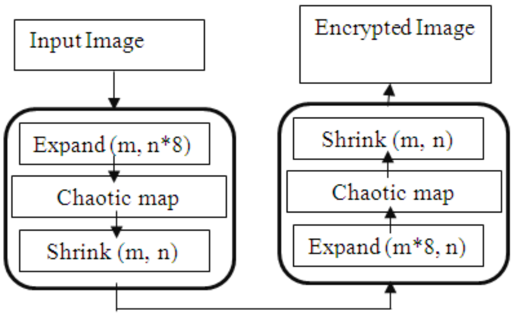


Figure 5. Method 2

4.3. Proposed Method 3

Block diagram of proposed method 3 is as shown in Figure 4.3.. In color image encryption RGB image of 24 bit planes are expanded into binary image of size $m * (3n * 8)$. Remaining process same as explained in method 2.

5. PARAMETERS FOR THE EVALUATION OF IMAGE ENCRYPTION SCHEME

5.1. Histogram analysis

An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each gray scale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should not leak any information about the plain-text or the relationship between plaintext and cipher-text. The histograms of plain-images and its ciphered images generated by the proposed schemes are tabulated. It´s clear from that the histograms of the cipher-images are fairly uniform and significantly different from that of the plain image and hence do not provide any clue to employ statistical attack.

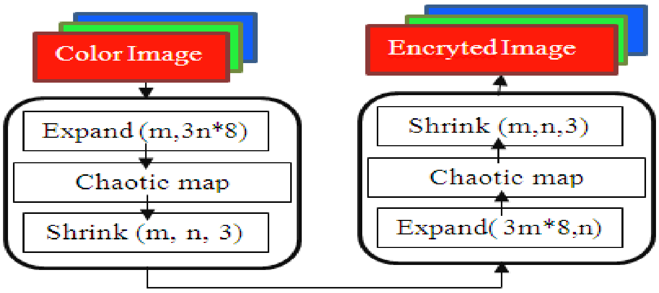


Figure 6. Method 3

5.2. Information Entropy Analysis

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

(2)

$$D(i,j) = \begin{cases} 1 & \text{if C1(i,j)} \neq \text{C2(i,j);} \\ 0 & \text{if C1(i,j)= C2(i,j).} \end{cases}$$

where X denotes the test image, x_i denotes the $i^{t}h$ possible value in X, and Pr(x_i) is the probability of X =x_i, that is, the probability of pulling a random pixel in X and its value is xi. For a truly random source emitting 2N symbols, the entropy is H(X)=N. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be H(X)=8. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

5.2.1. Mean Square Error (MSE)

Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. Let C1 and C2 are input image and encrypted image respectively, then MSE can be calculated as in Eq. 3 [12].

$$MSE = \frac{1}{M*N}\sum_{i=1}^{N}\sum_{j=1}^{M}[c1(i,j) - c2(i,j)]^2 \tag{3}$$

where M, N is the width and height of digital images and C1(i,j) is input image and C2(i,j) is encrypted image.

5.2.2. Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio can be used to evaluate an encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image. Mathematically as in [12].

$$PSNR = 20 * \log_{10}\left[\frac{255}{MSE}\right] \tag{4}$$

Where MSE is mean square error between input image and encrypted image and can be calculated by using Eq. 3

5.2.3. UACI and NPCR

A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain-image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [13]. The equation to calculate UACI is Eq. 5.

$$UACI = \frac{1}{M*N}\sum_{i,j}\frac{|\,C1(i,j) - C2(i,j)\,|}{255} \times 100\% \tag{5}$$

Where, M stands for image's width, N stands for image's height, C1(i,j) and C2(i,j) are the input and encrypted image respectively. NPCR can be calculated by Eq. 6.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{6}$$

Where, M stands for image's width, N stands for image's height and where D(i,j) defined as follows where C1(i,j) and C2(i,j) are the input and encrypted image respectively.

Table 1. Resultant Encrypted Images and its histogram of method 1 for Gray images

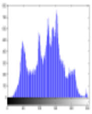
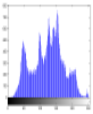
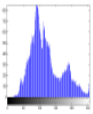
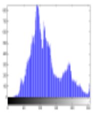
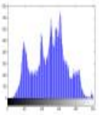
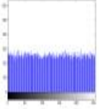
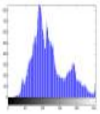
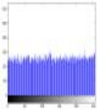
Input image	Histogram	Encrypted image	Histogram
			
			

Table 2. Resultant Encrypted Images and its histogram of method 2 for Gray images

Input image	Histogram	Encrypted image	Histogram
			
			

Experimental results are tabulated in tables from 1 to 11. Results obtained from method 1 for gray scale and colour image are tabulated in table 1 and 3. From this two tables we observed that histograms of both input and encrypted images are same and hence there is a need for better encryption. Results obtained from method 2 for gray scale and colour image are tabulated in table 2 and 4. From this two tables we observed that histograms of input and encrypted images are different and hence encryption by method 2 is better than encryption by method 1. Results obtained from method 3 for colour image is tabulated in table 5. From this table we observed that histograms of input and encrypted images are different and there is an improvement in histogram distribution as compared to resultant histograms of method 2. In tables 6, 7, 8 entropy of input image and encrypted image are same for method 1 but they are different for method 2. Other parameters are changed according to amount of scrambling. In table 8 and 9 entropy of colour encrypted image is more for method 3 and it is near to 8 fentropy of random image with uniformly distributed histogramsg. Results of proposed methods are tabulated and compared with existing methods in table 10 and 11.

7. CONCLUSION

This paper presents an improved version of chaos based image encryption using expand-shrink concept. Generally chaos based permutation only alters the position of the pixel, so entropy remains unchanged. But in proposed method input image undergo chaotic permutation between expand-shrink process which leads to both position and pixel manipulation. The efficiency of colour image encryption is improved in method 3 due to the scrambling of information takes place between RGB layers. From experimental results method 2 and method 3 are more efficient respectively for gray scale and colour images as compared to existing techniques.

Table 3. Resultant Encrypted Images and its histogram of method 1 for color images

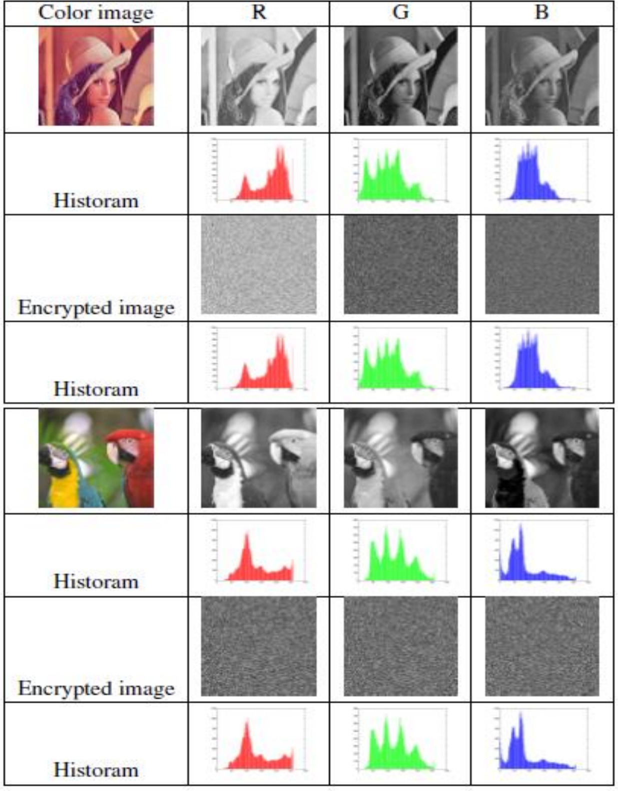

Color image
R
G
B
Historam
Encrypted image
Historam
Historam
Encrypted image
Historam

Table 4. Resultant Encrypted Images and its histogram of method 2 for color images

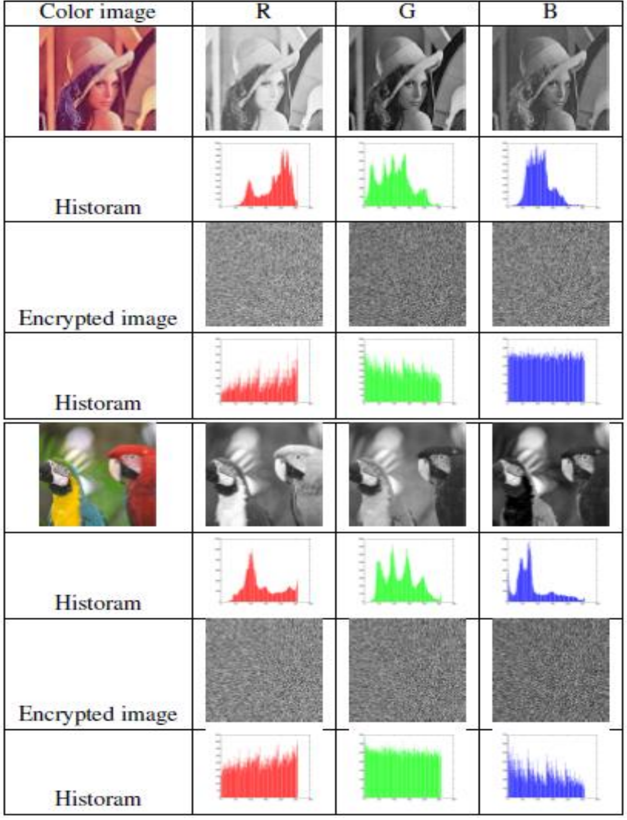

Color image
R
G
B
Historam
Encrypted image
Historam
Historam
Encrypted image
Historam

Table 5. Resultant Encrypted Images and its histogram of method 3 for color images

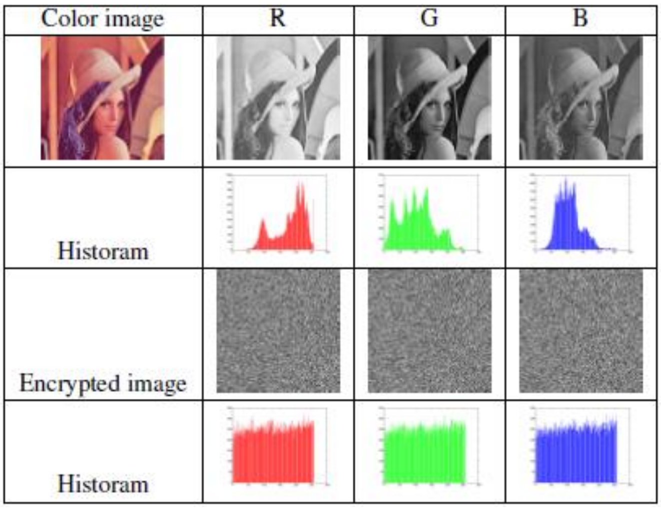


Table 6. Performance parameters of gray images for method 1 and 2

Parameters	Method 1			Method 2
	Lena	Parrot	Lena	Parrot
Entropy of original	7.5110	7.4425	7.5110	7.4425
Entropy of encrypted	7.5110	7.4425	7.9974	7.9964
MSE	111.6748	109.6002	114.4594	107.8736
PSNR	27.6513	27.7327	27.5443	27.8017
NPCR	99.4019	99.2676	99.5941	99.6429
UACI	21.8887	20.8154	28.7339	28.7460

Table 7. Performance parameters of color image for method 1

Parameters	R	G	B	Avg.
Entropy of Lena	7.3014	7.6424	7.1181	7.3540
Entropy of Enc	7.3014	7.6424	7.1181	7.3540
MSE	108.3949	113.1612	105.5265	109.0275
PSNR	27.7807	27.5938	27.8972	27.7572
NPCR	99.2569	99.4247	99.1714	9.2843
UACI	21.6407	24.0016	15.7942	20.4788

Table 8. Performance parameters of color image for method 2

Parameters	R	G	B	Avg.
Entropy of Lena	7.3014	7.6424	7.1181	7.3540
Entropy of Enc	7.8885	7.9665	7.9970	7.9507
MSE	148.6179	99.4569	94.7627	114.2792
PSNR	26.4101	28.1545	28.3644	27.6430
NPCR	99.5682	99.5972	99.6429	99.6028
UACI	30.0376	29.8635	27.8730	29.2580

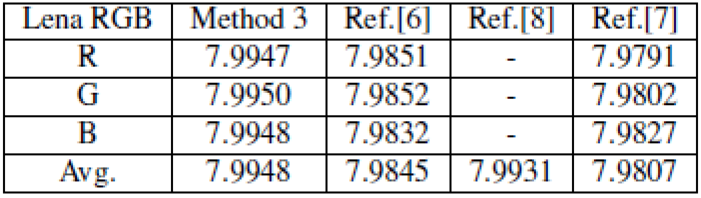
Table 9. Performance parameters of color image for method 3

Parameters	R	G	B	Avg.
Entropy of Lena	7.3014	7.6424	7.1181	7.3540
Entropy of Enc	7.9947	7.9947	7.9950	7.9948
MSE	166.0892	87.2926	90.5484	114.6434
PSNR	25.9274	28.7210	28.5620	27.7368
NPCR	99.5926	99.6307	99.5834	99.6022
UACI	32.4722	30.9244	28.0489	30.4818

Table 10. Entropy Comparison of Lena gray image for method 2 and existing methods

Image	size	Method 2	Ref.[2]	Ref.[10]	Ref.[11]	Ref.[3]
Lena	256x256	7.9974	7.9973	7.9873	7.9963	7.9970

Table 11. Entropy Comparison of Lena color image for method 3 and existing methods



Lena RGB	Method 3	Ref.[6]	Ref.[8]	Ref.[7]
R	7.9947	7.9851	-	7.9791
G	7.9950	7.9852	-	7.9802
B	7.9948	7.9832	-	7.9827
Avg.	7.9948	7.9845	7.9931	7.9807

REFERENCES

[1] Xingyuan Wang, LeiYang,*A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models* ,Optics Communications285(2012)40334042.

[2] Ahmed A. Abd El-Latif , Xiamu Niu, *A hybrid chaotic system and cyclic elliptic curve for image encryption*, Int.I.Electron.Commun.(AEU) 67 (2013) 136-143.

[3] Ruisong Ye, *A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism*, Optics Communications 284 (2011) 52905298.

[4] Xingyuan Wang, LinTeng,Xue Qin, *A novel colour image encryption algorithm based on chaos* ,Signal Processing 92 (2012) 11011108.

[5] G.A.Sathish Kumar , K.Bhoopathy Bagan, V.Vivekanand, *A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems*, Procedia Computer Science 3 (2011) 378387.

[6] Liu Hongjun, Wang Xingyuan, *Color image encryption based on one-time keys and robust chaotic maps*, Computers and Mathematics with Applications 59 (2010) 3320-3327.

[7] Hongjun Liu , Xingyuan Wang, *Color image encryption using spatial bit-level permutation and high-dimension chaotic system*, Optics Communications 284 (2011) 38953903.

[8] Fariborz Mahmoudi, Rasul Enayatifar, and Mohsen Mirzashaeri, *Image Encryption Using Chaotic Signal and MaxHeap Tree*, LNICST 8, pp. 19 28, 2009. ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2009.

[9] Zhi-liang Zhu , Wei Zhang, Kwok-wo Wong , Hai Yu, *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Information Sciences 181 (2011) 11711186.

[10] Ahmed HH, Kalash HM, Faragallah OS. *An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption*, Informatica 2007;31:1219.

[11] Sathyanarayana SV, Aswatha Kumar M, Hari Bhat KN. *Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points*, Int J Netw Secur 2011;12:13750.

[12] Jawad Ahmad and Fawad Ahmed, *Efficiency Analysis and Security Evaluation of Image Encryption Schemes*, International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04.

[13] Yue Wu, Joseph P. Noonan, and Sos Agaian, NPCR and UACI Randomness Tests for Image Encryption Cyber Journals: Multidisciplinary Journals in Science and Technology, *Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2011.

BIOGRAPHIES OF AUTHORS

Dr. Naveenkumar S K received his Ph.D from University of Mysore. He is a Associate Professor at the Department of Studies in Electronics, University of Mysore - Hassan, karnataka. His research interests are related to Nano technology, Nano materials and Image security . He has published research papers at national and international journals, conference proceedings as well as chapters of books.

Panduranga H T Pursuing Ph.D in Dept. of studies in Electronics, University of Mysore and received his M.Tech degree in Digital Electronics and communication systems from Visvesvaraya Technological University, Belagaum, Karnataka, India. His research interests are related to Image security and Partial image encryption. He has published research papers at national and international journals, conference proceedings.

Kiran Pursuing M.Tech in Digital Electronics and communication systems at Malnad Collage of Engineering - Hassan affiliated to Visvesvaraya Technological University, Belagaum, Karnataka, Indi