Australian Journal of Basic and Applied Sciences, 9(27) August 2015, Pages: 200-208

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Image Encryption in Bit Wise and Key Generation using Multiple Chaotic Maps

[1]T. Gopalakrishnan and [2]S. Ramakrishnan

[1]*Assistant Professor(SS), Department of Electronics and Instrumentation Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi-642 003, Tamilnadu, India.*
Email: tgkme@yahoo.com
[2]*Professor and Head, Department of Information and Technology, Dr. Mahalingam College of Engineering and Technology, Pollachi-642 003, Tamilnadu, India.*

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
Image Encryption, Bit wise permutation, Chaotic function, Logistic map, Permutation, Diffusion, Tent map, Key generation.

ABSTRACT

An image encryption algorithm using permutation-diffusion process with key generation is proposed. In the permutation phase the proposed algorithm uses external key as input to the tent map to generate intermediate keys which form the inputs to the logistic maps. The intermediate keys are encoded using XOR operation. The encoded bits are fed to the logistic maps to generate permutation order (PO) for the input image. In the diffusion phase, each intermediate keys are encoded by multiple chaotic maps in parallel to produce diffusion bits which are rearranged by PO bits to generate the permuted diffusion bits (PDFB). Multiple chaotic systems are employed in the diffusion bit generation process with key rotation in every round. The image bit stream is iteratively permuted and diffused with permutation order (PO) and diffusion bits (DFB) respectively to produce cipher image in minimum number of rounds. The simulation results proves that the proposed algorithm demonstrates better performance compared to the state-of the art in terms of entropy which reveals the suitability of the algorithm against attacks.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: T. Gopalakrishnan and S. Ramakrishnan., Image Encryption in Bit Wise and Key Generation using Multiple Chaotic Maps. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 200-208, 2015*

INTRODUCTION

Image encryption algorithms are used for secured transfer of digital images. The image encryption algorithms can be divided into two groups viz., chaos based and non-chaos based method. The advantages of chaotic image encryption are its simplicity, and more randomness. Additionally, Chaos based method provides dynamic changes for permutation-diffusion architecture in the image encryption. Dynamic systems which have the ability to produce numbers using maps that are random in nature and highly sensitive to initial conditions are used for encryption in chaos based systems. For decryption, the same numbers can be produced without any degradation due to hyper sensitivity of the initial conditions. Even a minute change in initial condition can produce a totally different sequence. On the other hand non-chaos based algorithm uses a secret key to produce cipher image by Nirmala Saini *et al*. In non-chaos based algorithm the image is divided into number of blocks and permutation - diffusion is done without using any map. However, the non-chaos based algorithms leads to tedious computation process to impercanate security to the image.

Baptista introduced a cryptosystem for the text messages. This uses logistic map to develop the integer sequence. The encrypted text is composed of alphabets and symbols by the author. W.K.Wong *et al*. uses the logistic map for random number generation. The drawback of the baptista method is overcome by a single random number generation for each block of message text and it produces a flatter distribution of cipher text. Wong *et al*. used dynamic look-up table to confuse digital images. The look up table is updated dynamically by current index value with the new index value. This method provides better security because of continuous updates in the dynamic lookup table. The encryption speed is faster than the previous methods developed by author Baptista and Wai-kit Wong *et al*. The chaos behaviour for different image encryption schemes were discussed**.** Fridrich *et al*. introduced a two stage chaotic image encryption in which positions of the pixels are modified in permutation stage and the values of the pixels were modified in the diffusion stage.

Corresponding Author: T. Gopalakrishnan, Department of Electronics and Instrumentation, Dr.Mahalingam College of Engineering and Technology, Pollachi, TN, India.
E-mail: tgkme@yahoo.com

In another novel work, Lian *et al*. used standard map in both permutation – diffusion process. Due to add and shift operations in diffusion process, the latency of the system increases. The draw back in this system is that permutation stage requires with 'n' number of rounds and in diffusion stage 'm' number of rounds. Thus the overall processing time of the algorithm increases. Kwok-Wo Wong *et al*. used chaotic standard map to do position permutation – diffusion using simple pixel modification in the permutation stage. The main drawback is the computation complexity in this encryption process. An encryption technique using both permutation and diffusion which provides simultaneous change in pixel position and pixel value are proposed by Francois M *et al*. and Blum L *et al*. . The approaches developed by Francois M *et al*. and Blum L *et al*. uses chaotic function for pixel position change. The confused image is used as the input for the diffusion process in which the pixel values of current pixel are replaced with a newly computed value.

In this brief, we propose a bitwise image encryption algorithm in which each bit of pixel is considered for both permutation and diffusion process which results in better encryption standard and security. The internal keys used in the process are generated using chaotic tent map. These internal keys in turn are used to generate the PO and DFB. Based on the PO, the pixel positions of the input image are shuffled in permutation process and the DFB are again confused using PO. Multiple one dimensional chaotic maps are used in the diffusion bit generation and for each round internal keys are rotated. Due to rotation of internal keys in each round will produce a different diffusion bits and encrypted image at each round is different. This type of diffusion bit generation will resist chosen plain text attacks. The proposed algorithm results better security against cryptographic attacks. The paper is organized into four sections. second section explains about the chaotic maps for the image encryption and Section three explains the proposed permutation-diffusion structure, encryption algorithm, decryption algorithm and key generation process. Section four deals with the simulation results and performance analysis of the proposed scheme and the Section five concluding remarks.

II. *An Overview Of 1-D Chaotic Maps:*

A. Tent Map:

Tent map is an iterated function in the shape of tent forming a discrete-time dynamic system. Tent map is used to increase the unpredictability of the initial seeds that are given to Logistic map introduced by Pareek N.K *et al*. . It exhibits a chaotic behavior for the given input according to the control parameter.

The tent map is given by the equation (1).

$$y_{i+1} = f_\mu = \begin{cases} \mu y_i & for\ y_i < \frac{1}{2} \\ \mu(1-y_i) & for \frac{1}{2} \le y_i \end{cases} \quad (1)$$

Where y_i, y_{i+1} are the ith and the i+1th state of the chaotic map, and μ is the control parameter in the range of 1.7 to 2. Tent map was used for creation of S-box and permutation - diffusion order generation. In the proposed method tent map is used for key generation process.

B. Logistic Map:

Logistic map is used due to its ergodic property i.e., the time average of its properties equals to the average over the entire phase space [0 to 1]. The logistic map function is symmetric about the midpoint of the interval in the bifurcation diagram. This iterative map has a complex behaviour for the system parameter value b > 3.56, where the map never repeats its values again and it is termed as chaos. The logistic map is given by,

$$X_{n+1} = bX_n(1 - X_n) \quad (2)$$

where X_n is a state variable, which lies in the interval [0,1] and b is the system parameter, that can have an value between 1 to 4.

C. Sine Map :

The sine map has a similar chaotic behavior with the logistic map. The definition is described by the following equation

$$x_{n+1} = r\sin(\pi x_n)/4 \quad (3)$$

where r is in the range of 0 to 4. In proposed method the parameter taken as r =0.99.

D. Cubic Map:

Cubic map is another 1D chaotic map. Its mapping is similar to the logistic map. The chaotic value is calculated by the power of 3 and their range lies between 0 to 1.

$$x_{n+1} = rx_n(1 - x_n^2) \quad (4)$$

Where r is the system parameter value it is in the range of 0 to 4. In proposed method r=2.59 as threshold for the cubic map parameter.

These four chaotic maps with initial conditions act as an external key for key generation. The generated internal keys were used for permutation and diffusion order generation to produce cipher image with various rounds for the proposed image encryption algorithm.

III. Proposed Method:

In the first phase of permutation the positions of the pixels in the image are changed with high randomness. In the second phase of diffusion the pixel values are changed with a newly computed value. There exists a high correlation between adjacent pixels of a digital image in the two phase scheme. A brief description of the steps that follows

to create cipher image based on the proposed methodology is given below.

A. Permutation and Diffusion structure:

A bitwise chaos based permutation - diffusion structure for image encryption is shown in Figure 1. The two parts are permutation and diffusion stages. In the proposed method PO and DFB are generated. The permutation stage permutes the pixels without modifying the pixel value and in the diffusion stage the pixel values are modified sequentially bit wise.

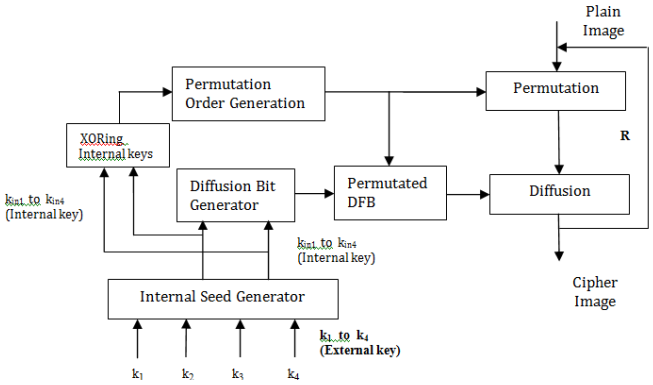

Fig. 1: Proposed Image Encryption Structure.

In the proposed method the plain image is first converted to bit stream, that is, in a sequential order of pixels. This bit stream is given as the input to the permutation - diffusion blocks. The key generator uses tent map to obtain the external keys (k_1, k_2, k_3, k_4) from the sender and these keys are used to generate the internal keys as shown in Figure 2. These keys are then fed into the structure formed by the logistic map, shown in Figure 3(a) and 3(b). The generated permutation order (PO) and diffusion bits (DFB) are given to the permutation - diffusion blocks to encrypt the bit stream. This combined process of permutation and diffusion is repeated iteratively. When specified rounds (R=3) are reached, encrypted bit stream is converted into pixels that form the cipher image.

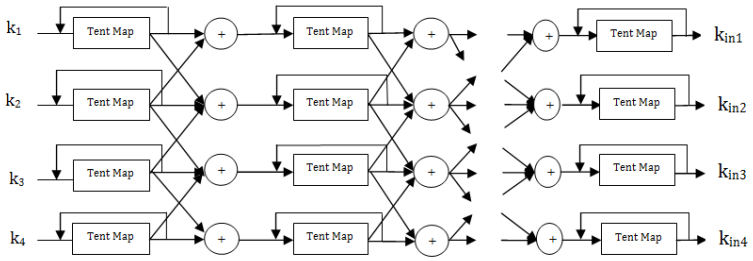

Fig. 2: Key Generation Process.

Fig. 3(a): Permutation order Generation.

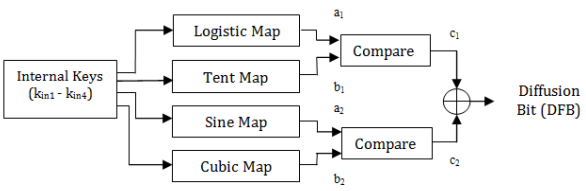

Fig. 3(b): Diffusion Order Generation.

The generated internal keys (k_{in1}, k_{in2}, k_{in3}, k_{in4}) are given to permutation order and diffusion bit generator. The generation of PO and DFB are shown in Figure 3(a) and 3(b). A single logistic map is used to generate the permutation order (PO) using the following relationship,

$$PO = indices\{(b * X_i * (1 - X_i) * N) \bmod N\} \quad (5)$$

where N is the total number of pixels multiplied by the number of bits required to represent the bit present in the image and X_i is the value generated by the logistic map at i^{th} iteration. PO is a one dimensional vector of size N and it has no repeated values. Using the PO the plain image pixel bits are permuted. Another block, that receives four internal keys, will generate a random bit sequence by comparing the values produced by the multiple chaotic maps. These bits are then confused using the PO from the nearby block. To increase the complexity of the diffusion process the diffusion bits are permuted. The permuted diffusion bits are manipulated with the confused pixel bits. The bit stream coming out of the diffusion block is given back as a plaintext to the permutation block and the rounds are repeated to achieve the security level.

B. Description of the Proposed Algorithm:

A chaotic bit wise function is integrated into encryption and decryption algorithm. The detailed process is composed through the following steps.

1. The plain image is converted to 1D binary sequence. The size of the sequence is m=8xNxM for gray level image and for colour image the size is m=3x8xNxM.
2. The External keys (k_1,k_2,k_3,k_4) are given to internal seed generator for generating the Internal keys(k_{in1}, k_{in2}, k_{in3}, k_{in4}).
3. The internal seeds are given to PO and DFB block to generate the permutation order (PO) and diffusion bits (DFB).
4. PO and DFB are given to the permutation - diffusion block in the proposed algorithm.
5. Internal keys (k_{in1}, k_{in2}, k_{in3}, k_{in4}) were converted to single key by XOR operation and it act as initial key to logistic map for permutation order generation.
6. Internal keys (k_{in1}, k_{in2}, k_{in3}, k_{in4}) were given to four different maps to generate the diffusion bits (DFB) for first round. Internal key order is rotated for next rounds.
7. The permutation-diffusion process is repeated for R rounds with internal key rotation to get the highly uncorrelated cipher image.
8. Decryption is achieved by reverse process of encryption.

A key generation process is based on one dimensional chaotic map, which iterates the external keys to generate initial seeds for the next tent map. The output of tent map is further manipulated to strengthen the internal keys according to the structure. The advantage of the tent map over the logistic map is calculations are simplified considerably.

In particular, higher-order iterates of the tent map, which are involved in the study of the asymptotic dynamics, are themselves piecewise linear maps for easy computation. This formation is mainly designed to increase the sensitivity of the key as shown in Figure 2. Each tent map in the formation is fed with an initial seed i.e.., external keys (k_1, k_2, k_3, k_4) and it is iterated for hundred times. The final values obtained from the iteration are fed to the next tent map and so on. Internal keys (k_{in1}, k_{in2}, k_{in3}, k_{in4}) are obtained at the final tent maps and this kind of feeding will increase the sensitivity of the key.

C. Key Generator:

A small change in the external key will result in scattering. Each round leads to change in the results that will have high resistance to the brute force attack. For example, if four external keys are used then the total number of possible keys will be equal to 2^{212} (approximately 6.58 x 10^{63}). For the present computer speed, it is commonly accepted that a key space of size smaller than 2^{128} is not secure enough proposed by Francois M *et al.* . In the present case this phenomena is satisfied. This structure is more suitable, very sensitive and good enough to generate the internal keys in an unpredictable manner.

It is clear from the above analysis that the proposed structure for generating the initial seed is very sensitive to its initial conditions. A small change in key space will completely deviate from the original one in the final result. Internal keys (k_{in1}, k_{in2}, k_{in3}, k_{in4}) are given to the logistic, tent, sine and cubic maps. Each map is iterated for N times. Where 'N' is equal to the length of bit stream. The resulting values are compared to produce the diffusion bits (DFB). If map-1 produces value a_1 and map-2 produces value b_1, then the random bits (DFB) are generated by the following relation,

$$DFB = \begin{cases} = 0, & if \ a > b \\ = 1, & if \ a \le b \end{cases} \quad (6)$$

After receiving the DFB, bits are permuted and given to the diffusion block, where diffusion bits are generated for a round. In the next rounds the internal keys are rotated such as (k_{in2}, k_{in3}, k_{in4}, k_{in1}) and so on. The algorithm is repeated for number of rounds to produce the cipher image. By key rotation in each round makes different DFB for every round. Due to different DFB for diffusion block results different cipher images in every round. Most of the image encryption algorithms are crypt analyst due to their weakness such as one time generation keys repeated of number of rounds in which cipher taken out by chosen plain text attacks. In our proposed method the chosen plain text attack is overcomed by key rotation in each round for DFB generation.

IV. Performance Analysis:

The encrypted image was tested with different rounds for various statistical analysis, sensitivity analysis and NIST standard test suite by the author Rukhin A. The proposed algorithm proves that the encrypted image is resistive to various attacks.

A. Key space Analysis:

An image encryption system should be very sensitive to cipher keys and key space should be large enough to make brute force attacks. for the proposed algorithm the key space be of variable four and eight keys were selected for a 256x256 and 512x512 images respectively. Each key is of 53 bits and the total bits required for the key will be 212 bits (256x256) and 414 bits (512x512). Images of greater size (> 512x512) will be partitioned and processed in parallel. Total number of possible keys that avail larger images was found to be 4.23 x 10^{124}, which is near to the infinity. This assures that the proposed method has very high resistance to the brute-force attack. To fix the value of number of rounds R, values of NPCR (Number of pixel change rate) and UACI (unified average changing intensity) are considered. NPCR is measured between the two ciphers, which have slightly different plain images i.e., one pixel change between the plain images. UACI are the cipher images whose plain images have a slight difference in one pixel. NPCR≥0.995 and UACI≥0.333 should achieve maximum security for the number of rounds (R= 1 to 6) to in order to yield better cipher image as shown in the Table 6.

Considering the key space as a variable four and eight keys are selected for a 256x256 and 512x512 images respectively. Each key is of 53 bits and the total bits required for the key will be 212 bits (256x256) and 414 bits (512x512). Images of greater size (> 512x512) will be partitioned and processed in parallel. Total number of possible keys that avail larger images was found to be 4.23 x 10^{124}, which is near to the infinity. This assures that the method has very high resistance to the brute-force attack.

B. Statistical Analysis:

An effective encryption algorithm should be robust against any statistical attack. To test the robustness statistical analysis is performed on ciphered image to demonstrate its permutation - diffusion properties which strongly resist statistical attacks. This is found by calculating the histograms, correlation of two adjacent pixels in the ciphered image and the information entropy. Chaos based encryption algorithms were tested and also compared with the existing algorithms developed by Zeghid M *et al.* , Rhouma R *et al.* , Hongjun L *et al.* , Nooshin Bigdeli *et al*. and X.Wang *et al.* .

C. Histogram analysis:

A histogram of an image shows how pixels are distributed in that image. Histograms of several encrypted and original images of widely different content are calculated and analyzed. It is clear that the histograms of encrypted images are flat and they have no clue about the original histogram of the image. Figures 4(a) show the plain images, Figures 4(b) (f) show the encrypted image, Figures 4(c) (g) show the histograms of plain image it is absorbed that from Figure 4(d) (h) histogram of encrypted images were completely flat and have no clue about the histograms of 4(c) (g).

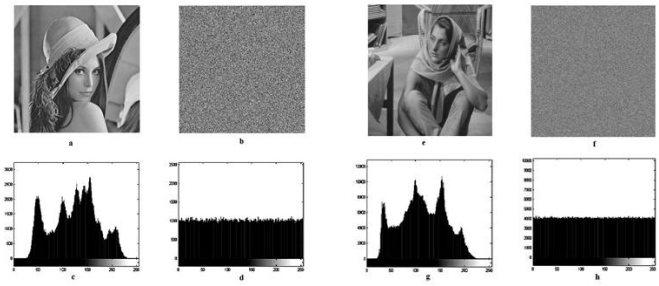

Fig. 4(a): Lena plain image (b) Cipher image (c) Histogram of plain image (d)Histogram of cipher image (e) Barbara plain image (f) Cipher image (g) Histogram of plain image (h)Histogram of cipher image.

D. Correlation coefficient analysis:

Correlation between the pixels of the image must also be analyzed to check its robustness against the statistical attacks. This analysis shows the correlation between the randomly selected pairs of both plain image and cipher image. The analysis is carried out between two horizontally, vertically and diagonally adjacent pixels. Correlation is calculated using equations (7) and (8)

$$Cov(x,y) = E\{(x - E(x)) - (y - E(y))\} \qquad (7)$$

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (8)$$

where x and y are the gray level values of the two adjacent pixels in the image, E(x) and D(x) are the mean and standard deviation of the corresponding gray level values.

Tables 1 and Tables 2 show the correlation coefficients of the plain image and its cipher image. Correlation coefficient value ranges from -1 to +1. If the correlation among the pixels in plain image

approximately equals to 1, it has positive correlation among the pixels. If it nearly equals to zero, it shows that there is no correlation among the pixels. If it is minus one, then the encrypted image is the negative of the original image. From this table the correlation among various grey and color images were tested and the proposed scheme entirely reduces the correlation among the pixels. The correlations of vertical, diagonal and horizontal adjacent pixels are plotted by randomly selected 10000 pixels which are adjacent in horizontal, vertical and diagonal. It is clear that it is very hard to predict the correlation of original image from the cipher image.

Table 3 shows the correlation coefficients of the plain image (Lena) and cipher image obtained by the proposed scheme with other existing algorithm. From table, it is inferred that the correlation among the pixels present in plain image is approximately equal to 1. And it shows that there is a positive correlation among the pixels. For cipher images the correlation coefficients of adjacent pixels are nearly equal to 0, which shows that there is no correlation among the pixels. From the observation of other chaos based image encryption algorithm, it is clear that the proposed scheme entirely reduces the correlation among horizontally, vertically and diagonally adjacent pixels as shown in Figure.5. The proposed method has better correlation coefficient among the pixel as compared to other algorithms.

Table 1: Correlation Coefficient of adjacent pixels.

Image Grey	Adjacency	Correlation Coefficient	
		Plain image	Cipher image
Lena(256x256)	Horizontal	0.9882	-0.0019
	Vertical	0.9856	0.0023
	Diagonal	0.9669	0.0018
Lena(512x512)	Horizontal	0.9711	0.0101
	Vertical	0.9853	-0.0103
	Diagonal	0.9591	0.0211
Barbara(1024x1024)	Horizontal	0.9647	0.0034
	Vertical	0.9896	0.0114
	Diagonal	0.9486	-0.0088

Table 2: Correlation Coefficient of adjacent pixels (color).

Image color	Adjacency	Correlation Coefficient					
		Plain image			Cipher image		
		Red	Green	Blue	Red	Green	Blue
Lena Image (512x512)	Horizontal	0.9588	0.9865	0.9175	-0.0278	-0.0504	-0.0925
	Vertical	0.9220	0.9709	0.9456	-0.1224	-0.1153	-0.1284
	Diagonal	0.9822	0.9744	0.8983	-0.0033	-0.0362	-0.0222
Baboon Image (512x512)	Horizontal	0.9372	0.9264	0.8897	-0.0807	-0.0429	-0.0982
	Vertical	0.8821	0.7847	0.9005	-0.0873	0.0460	-0.1158
	Diagonal	0.7623	0.6643	0.8372	-0.0249	0.1248	0.1943

Table 3: Correlation coefficients of the original Lena image and the encrypted images obtained by the proposed scheme.

Scheme	Vertical	Horizontal	Diagonal
Original Lena image	0.9882	0.9856	0.9669
Zeghid M *et al*. Algorithm	0.0770	0.0660	-
Rhouma R *et al*. Algorithm	0.0845	0.0681	-
Hongjun L *et al*. Algorithm	0.0965	-0.0318	0.0362
Nooshin Bigdeli *et al*. Algorithm	0.0009	-0.0011	0.0011
Proposed scheme			
Lena	-0.0019	0.0023	0.0018
Barbara	-0.0003	0.0030	0.0094
Baboon	-0.0016	-0.0043	-0.0019

E. Information entropy analysis:

The entropy of a message source can be measured by,

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)} \quad (9)$$

where M is total number of symbols, $p(m_i)$ represents the probability of occurrence of symbol m_i, and log denotes the base 2 logarithm, so that the entropy is expressed in bits. The 256 symbols are emitted by a random source and its entropy is equal to 8 bits.

For the cipher images, the entropies are also equal to that of the plain images as shown in Tables 4. This shows that both plain and cipher image have same entropy, nearly equal to 8 bits. Table 5. shows the information entropies and its comparisons. The grey image value of pixel was observed to be H(m) = 7.9970 which is further compared with AES algorithm suggested by Zeghid M et.al which has H(m) = 7.91. This shows that the proposed algorithm is robust against the entropy attacks.

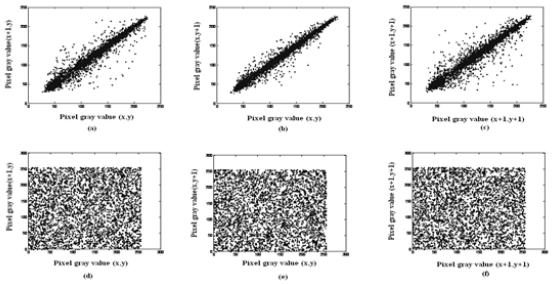

Fig. 5: Correlation of two adjacent pixels (a), (b) and (c) Horizontal, Vertical and Diagonal direction of the plain image, (d), (e) and (f) Horizontal, Vertical and Diagonal direction of the cipher image.

Table 4: Information Entropy for grey images.

Test Image	Proposed		X.Wang *et al*.	
	Original Image	Cipher Image	Original Image	Cipher Image
Lena	7.4288	7.9970	7.3482	7.9970
Baboon	7.1527	7.9992	7.1273	7.9974
Cameraman	7.0189	7.9991	7.0097	7.9967

Table 5: Information Entropies of Encrypted Images obtained by the Proposed Scheme and the Three comparable block Ciphers.

Scheme	Red	Green	Blue
Zeghid M *et al*. Algorithm	Entropy for grey image 7.91		
Rhouma R *et al*. Algorithm	7.9732	7.9750	7.9715
Hongjun L *et al*. Algorithm	7.9851	7.9852	7.9832
Nooshin Bigdeli *et al*. Algorithm	7.9983	7.9979	7.9985
Proposed scheme			
Lena	7.9993	7.9994	7.9993
Barbara	7.9993	7.9992	7.9994
Baboon	7.9993	7.9991	7.9993

F. Differential Attack:

The cipher image is resistive from differential attacks are very sensitiveness to the small change in the plaintext. The common measures used to measure this sensitivity are NPCR (Number of pixel change rate) and UACI (unified average changing intensity) are given by the following equations,

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (10)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (11)$$

where C_1 and C_2 are the cipher images whose plain images have a slight difference in one pixel. C_1 (i, j) denotes the position of pixel in C_1.W and H are width and height of the cipher image. D(i,j) is determined as 1, if $C_1(i,j) = C_2(i,j)$, otherwise D(i,j) = 0.

NPCR is measured between the two ciphers having slightly different plain images i.e., one pixel change between the plain images. The resulting NPCR and UACI values are tabulated in Table 6. and Table 7. for different rounds(R). The table clearly indicates that NPCR reaches approximately a constant and a slight variation in UACI, when it reaches more rounds. To resist the differential attack the NPCR and UACI values should be NPCR≥0.995 and UACI≥0.333. The pixel change rate in this encryption scheme shows that at first round itself achieves the maximum security level as NPCR, UACI and entropy. P*, Q*, R*, S*, T*, U*, V* and W* keys represents the small change in the key space for which the NPCR and UACI are calculated.

Table 6: NPCR and UACI values for Lena (Grey) image with rounds (R=3).

Lena 256x256	R=1		R=2		R=3	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
P*	0.9962	0.3342	0.9958	0.3333	0.9965	0.3354
Q*	0.9965	0.3349	0.9957	0.3348	0.9964	0.3338
R*	0.9958	0.3340	0.9959	0.3349	0.9964	0.3350
S*	0.9962	0.3343	0.9962	0.3361	0.9963	0.3346

Table 7: NPCR and UACI values for Lena (Grey) image with rounds (R=6).

Lena 512x512	R=1		R=2		R=3		R=4		R=5		R=6	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
P*	0.9961	0.3351	0.9961	0.3349	0.9960	0.3344	0.9961	0.3347	0.9962	0.3343	0.9961	0.3345
Q*	0.9963	0.3349	0.9961	0.3340	0.9963	0.3352	0.9961	0.3343	0.9961	0.3348	0.9961	0.3344
R*	0.9961	0.3344	0.9962	0.3351	0.9960	0.3339	0.9962	0.3351	0.9960	0.3352	0.9961	0.3338
S*	0.9961	0.3347	0.9962	0.3330	0.9960	0.3346	0.9960	0.3347	0.9959	0.3346	0.9960	0.3348
T*	0.9961	0.3340	0.9962	0.3348	0.9963	0.3343	0.9961	0.3342	0.9960	0.3348	0.9959	0.3342
U*	0.9961	0.3346	0.9961	0.3343	0.9960	0.3340	0.9961	0.3348	0.9960	0.3347	0.9960	0.3343
V*	0.9960	0.3341	0.9961	0.3345	0.9962	0.3347	0.9961	0.3354	0.9962	0.3349	0.9961	0.3346
W*	0.9963	0.3347	0.9960	0.3352	0.9961	0.3344	0.9960	0.3346	0.9962	0.3352	0.9961	0.3350

Table 8: Results of Correlation coefficients, NPCR and UACI between the four cipher images of Lena using four slightly different keys in the proposed method and Three cipher Images of Lena Using Three slightly different Keys.

Four slightly different keys for proposed method.				Three slightly different Keys by Francois M *et al*.			
Keys	Correlation coefficient	NPCR	UACI	Keys	Correlation Coefficient	NPCR	UACI
α^a/α^b	0.0005	0.9962	0.3345	K^a/K^b	0.0008	0.9962	0.3345
α^b/α^c	0.0040	0.9962	0.3339	K^a/K^c	0.0014	0.9964	0.3347
α^c/α^d	0.0027	0.9960	0.3341	K^b/K^c	0.0004	0.9963	0.3347
α^d/α^a	-0.0004	0.9960	0.3348				

Table 8. shows the results of Correlation coefficients, NPCR and UACI between cipher images of Lena (Grey) by slight change in two keys. For sample, the change in the two different key combinations with correlation coefficients, NPCR and UACI were listed out in four set of keys. With two different key the correlation coefficient is almost zero. NPCR and UACI are greater than the required level. From table 9, it has been observed that there is no correlation between the pixels. Correlation coefficient is nearly zero. NPCR and UACI values show that the pixel changing rate is greater than the minimum required level of 0.9960 and 0.3337.

Conclusion:

The encryption scheme is based on bit wise permutation and diffusion using multiple chaotic maps. Various analyses have been performed to prove the security of proposed image encryption scheme. This method has a greater sensitivity to the minute change in the external keys due to the key generation process. In our algorithm NPCR, UACI and entropy reaches maximum level at first round itself with the use multiple chaotic maps. To improve complexity of encryption the rounds are repeated with internal key rotation provides robust against chosen plain text attacks. These methods could be extended in future for encryption and compression during the image transmission.

REFERENCES

Nirmala Saini, 2010. Key management of the double random-phase- encoding method using public-key encryption, *International Journal for Optics and Laser in Engineering*, 48(3): 329-334.

Baptista, M.S., 1998. Cryptsography with Chaos, *International Journal for Physics Letter A* , 240(1-2): 50-54.

Frank Dachseltet, 2001. Chaos and Cryptography, *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, 48(12): 1498-1501.

Wong, K.W., 2002. A fast chaotic cryptographic scheme with dynamic look-up table, *International Journal for Physics Letter A*, 298: 238–242.

Wai-kit Wong, 2001. A modified chaotic cryptographic method, *International Journal for Computer Physics Communications*, 138: 234–236.

Fridrich, J., 1998. Symmetric ciphers based on two dimensional Chaotic maps, *International Journal of Bifurcation Chaos*, 8: 1259-1284.

Lian, S.G., 2005. A block cipher based on a suitable use of chaotic standard Map, *International Journal for Chaos, Solitons and Fractals*, 26(1): 117-129.

Kwok-Wo Wong, 2008. A Fast Image Encryption Scheme based on Chaotic Standard Map, *International Journal for Physics Letter A*, 2645–2652.

Francois, M., 2012. A new image encryption scheme based on a chaotic Function, *International Journal for Signal Processing: Image Communication*, 27(3): 249-259.

Gopalakrishnan, T., 2013. "Random Permutation Based Chaotic Image Encryption", *Proceedings on International Conference on Cloud and Big Data Analysis (ICCBDA 2013)*, at Department of Information Technology, PSG College of Technology, Coimbatore, 86-89.

Ahmed, A., 2012. Digital image encryption scheme based on multiple Chaotic systems, *International Journal for Sensing and Imaging*, 13(2): 67-88.

Gopalakrishnan, T., 2013. A New Chaotic Image Encryption Scheme using Random Permutation and Logistic Map", *Proceedings of International Conference Biosignals, Images and Instruments ICBSII-2013*, at SSN College of Engineering, SSN Nagar, Chennai, 34-43.

Yong Wang, 2012. A block cipher with dynamic S-boxes based on tent map, *International Journal for Communication in Nonlinear Science and Numeric Simulation*, 14(7): 3089-3099.

Gopalakrishnan, T., 2014. Image Encryption using Chaos and Parity Based Pixel Modification in Permutation", *Proceedings of International conference on Simulation in Computing Nexus'14 - ICSCN-2014*, at Coimbatore Institute of Engineering and Technology, Coimbatore, 5.

Yang Tang, 2010. Image encryption using chaotic coupled map lattices with time-varying delays, *International Journal for* Communication in Nonlinear Science and Numeric Simulation, 15(9): 2456-2468.

Parker, S., 1987. Chaos: a tutorial for engineers, *Proceedings of the IEEE*, 75(8): 982–1008.

Kwok-Wo Wong, 2008. A Fast Image Encryption Scheme based on Chaotic Standard Map,

2008; *International Journal for Physics Letters A*, 372(15): 2645–2652.

Pareek, N.K., 2006. Image encryption using chaotic logistic map, *International Journal for Image and vision computing*, 24(9): 926-934.

Blum, L., 1986. A simple unpredictable pseudo-random number generator, *International Journal for SIAM Journal on Computing*, 15(2): 364–383.

einstein.drexel.edu/~bob/PHYS750_NLD/ch2.pdf.

Rukhin, A., 2010. A statistical test suite for Random and pseudo random number generators for cryptographic applications, *NIST special publication, Revision 1a*.

Zeghid, M., 2007. A modified AES based algorithm for image encryption, *International Journal for World academy of science Engineering Technology*, 27: 206-211.

Rhouma, R., 2009. OCML based color image encryption, *International Journal for Chaos, Solitons & Fractals*, 40(1): 309-318.

Hongjun, L., 2010. Color image encryption based on one-time keys and robust chaotic Maps', *International Journal for Computers & Mathematics with Applications*, 59(10): 3320-3327.

Nooshin Bigdeli, 2012. A robust hybrid method for image encryption based on Hopfield neural network, *International Journal for Computers and Electrical Engineering*, 38(2): 356-369.

Wang, X., 2008. An image scrambling encryption using chaos-controlled poker shuffle operation, *Proceedings of International Symposium on Biometrics and Security Technology*, pp 1-6.

Chang e Dong, 2014. Color image encryption using one-time keys and coupled chaotic systems, *International Journal for Signal Processing: Image Communication*, 29: 628-640.