DOI: 10.21917/ijivp.2016.0177

IMAGE ENCRYPTION IN BLOCK-WISE WITH MULTIPLE CHAOTIC MAPS FOR PERMUTATION AND DIFFUSION

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

[1]*Department of Electronics and Instrumentation Engineering, Dr. Mahalingam College of Engineering and Technology, India*
E-mail: tgkme@yahoo.com

[2]*Department of Information and Technology, Dr. Mahalingam College of Engineering and Technology, India*
E-mail: ram_f77@yahoo.com

Abstract

This paper presents an efficient block-wise image encryption method based on multiple chaotic maps. The image is divided into four overlapping blocks and each block is permutated with Cat map and its parameters are controlled by Henon map using multiple keys. Due to overlapping division of blocks, it produces effect of double permutation in the middle portion of overlapped image in single permutation itself. For diffusion, the whole image is divided into four non-overlapping blocks and diffused with logistic map. Each block pixel values were completely modified in the diffusion process in order to avoid known-plaintext and chosen-plaintext attacks. For each division of blocks different keys were selected for both permutation and diffusion process in the proposed method. The simulation results of several statistical analysis shows that the proposed cryptosystem is efficient and highly secured.

Keywords:

Image Encryption, Cat Map, Henon Map, Logistic Map, Permutation, Diffusion

1. INTRODUCTION

With the ever increasing growth of image transmission through computer networks especially the multimedia, internet and security of digital images has become a major concern. A secure computing environment would not be complete without considering encryption technology. Image encryption, in particular, is a challenging task due to some intrinsic properties like bulk data capacity, high storage redundancy, which are generally difficult to handle by traditional techniques. The image encryption is well known and it has extensive applications in multimedia systems, internet communication, medical imaging, telemedicine and so on. In spatial domain, the basic ideas for image encryption involves bit-wise permutation, pixel transformation etc. Among several existing methods the tree-structure based methods, chaos based methods and cellular automata based methods are most popular. During the past decades, there has been an increased interest in chaos based encryption. Because the characteristics of the chaotic maps have attracted the attention of cryptographers as they have many fundamental properties like periodicity, mixing and sensitivity to initial conditions so that good ciphers can be obtained. The two-dimensional or the high dimensional chaotic maps are usually employed to encrypt an image.

A chaos-based image encryption scheme typically comprises two processes: Permutation and substitution. Permutation involves confusion of pixels and diffusion just replaces a pixel by another value. The chaotic maps were achieved by using Logistic map, Cat map, Tent map, Baker map, etc. In the diffusion process pixel values are altered sequentially based on previous pixel values. The Fridrich architecture becomes the base for many chaos based image encryption schemes. There are varieties of approaches for permutation and diffusion process. Lian et al. [1] used the modified standard map for confusion step and tent map for diffusion. The origin point of standard map is taken as randomly selected point so that image can be well shuffled. In [2], dynamic S-boxes were designed to get block ciphers. Permutation is done with these block ciphers and Tent map is used here to generate the block ciphers whereas cyclic shifting operations are used in diffusion. In [3], a new cryptosystem based on Fridrich architecture is proposed in which bit-level permutation is performed. It replaces pixel wise permutation and is more secure as it alters not only the position but also the value. It employs cat map for bit-level permutation and Logistic map for diffusion. Wang et al. [4] used the chaotic structure for colour images and tried to encrypt the R, G, B components separately and also to reduce the correlation in order to increase the security.

In [5], encryption system employs shuffling matrix to shuffle the position of pixels and hyper-chaotic system for diffusion phase to make the weak relationship between the original pixel and the cipher image. Huang et al. [6] utilized the concept of multi-chaotic systems to get cipher image in which pixel shuffling is done with the help of combined effect of four different maps. By this even the outlines of image gets distributed well which decreases the probability of attacks. In [7] chaos based image encryption based on permutation and diffusion using Logistic maps and Tent map with minimum number of three rounds. It discusses about the key generation process [8] with multiple chaotic map for image encryption and it achieves higher level of security in cryptanalysis. A 1D hybrid chaotic system [9] for image encryption using parametric switching based on permutation and diffusion. In this method for every round diffusion, bit keys were changed in order to avoid chosen plain text attacks. In [10]-[11], cryptanalysis is employed and found out problems on weak keys and attacks. It also suggests improvement methods to overcome the defects in security. Yang et al. [12] uses hash function to produce hash value which acts a key for the entire process. Also satisfactory performance is achieved in overall one round which improves the speed efficiency. The encryption scheme [13] involves coupling of chaotic function and XOR operation to get large key space and it is very easy for implementation purposes without using any chaotic maps. The other algorithms use compound chaos and adaptive wave transmission. In [14], a new compound chaotic function with two one- dimensional dynamically shifting chaotic functions is proposed. The image encryption is done with new two-dimensional chaotic function and dynamically dividing 3D baker model. To confuse the relationship between the cipher image and

plain image a fast confusion process among pixels based on dynamical dividing 3D baker is performed using compound chaotic function. The results show that the cipher is sensitive to key, resist statistical analysis and it has good randomness. In [15] self-adaptive technique is used for encryption. Here with the help of one half of the image pixels the other half gets shuffled which is done in parallel manner. This parallel operation reduces the time and is computationally simple. In both schemes [14]-[15] at least two rounds of substitution-diffusion process are employed to achieve the satisfactory performance.

K.W. Wong et al. [16] proposed a single round architecture by using simple add-shift diffusion effect in the confusion stage. Here diffusion process is done in permutation process itself in order to achieve shorter encryption time. An encryption scheme proposed by Tao Xiang et al. [17] gives necessary confusion-diffusion effects based on random number generation from chaotic Logistic map and the encryption is by shifting and masking. In [18] chaotic key based encryption algorithm along with its VLSI architecture was proposed. In this method, chaotic binary sequence is created which acts as a key. As per the sequence the image pixels are being XORed. The approach is very simple, and it has low computational complexity. In [19], a new scheme based on 3-D chaotic cat map is used to shuffle the pixel positions and compared with 2-D cat map. Though 3-D cat map performs faster than 2-D one and gives better data mixing, it fails in case of keyspace as it is same as the 2D one.

Y. Zhang et al. [20] introduces cryptosystem using rotation matrix along with non-overlapping division for confusion phase in which each block is permutated by rotation matrix. The diffusion phase also involves block separation followed by sequence of operations to produce the cipher image. Here both processes involves block operations which eliminates noise in communication channel. In the encryption scheme [21] combined permutation-diffusion effect is proposed in order to accelerate the time. It involves spatiotemporal chaos for shuffling the pixels in partitioned image.

To achieve a robust encryption scheme, the proposed method involves the combined effect of both overlapping and non-overlapping blocks along with multiple chaotic maps in order to meet the requirements of secure image transfer. The maps involved are cat map and Henon map. Permutation phase utilizes non-overlapping division in which each block is permutated by Cat map. Diffusion is carried out by dividing the image into non-overlapping blocks and XORing with pseudorandom sequence from logistic map. The rest of this paper is organized as follows: Section 2 provides a detailed description of the proposed image encryption algorithm. An efficient measuring methods and security analysis are presented in section 3. Finally, a brief conclusion of the work is presented in section 4.

2. PROPOSED ENCRYPTION METHOD

The proposed image encryption relays on block separation and multiple chaotic maps. A chaotic map is a map (merely a quadratic function) that exhibits some sort of chaotic behaviour of continuous or in discrete manner. But usually discrete maps will be used for their iterative manner. They often generate fractals and is used to study about dynamic systems. The maps used here are Cat map, Henon map and logistic map.

2.1 CAT MAP

Cat map is often represented as Arnold's cat map and it is of one-to-one transformation. It is given by,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N) \tag{1}$$

where, 'p' and 'q' are its parameters and N is the length. It is invertible because the matrix has determinant 1 and therefore its inverse has integer entries and is of area preserving. One of this map's features is that the image can be apparently randomized by the transformation but returning to its original state after a number of steps.

2.2 HENON MAP

Henon map is another form of chaotic map. It takes a point (x_n, y_n) in the plane and maps it into a new point. It is a 2D map also it depends on two parameters 'a' and 'b'. For classical Henon map the values of 'a' and 'b' are 1.4 and 0.3. It is given as,

$$\begin{aligned} x_{n+1} &= y_n + 1 - a x_n^2 \\ y_{n+1} &= b x_n \end{aligned} \tag{2}$$

Control parameter (p, q) is derived by the equation,

$$\begin{aligned} p_i &= floor(x_{2000+i}) \times \mathrm{mod}\ N\ \mathrm{mod}\ L_i(AE) \\ q_i &= floor(y_{2000+i}) \times \mathrm{mod}\ N\ \mathrm{mod}\ L_i(AE) \end{aligned} \tag{3}$$

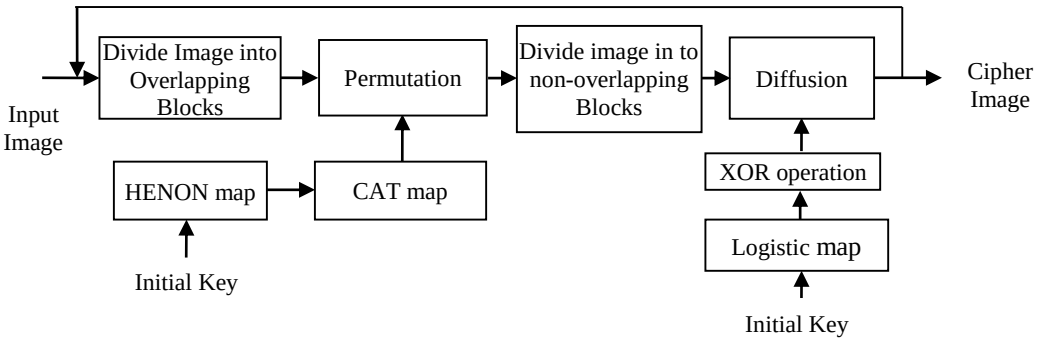


Fig.1. Structure of proposed Image Encryption method

The process of encryption is based on permutation-substitution architecture shown in Fig.1 the image is divided into overlapping blocks. Cat map is utilised for permutation process and the blocks here are divided into overlapping ones. In case of diffusion, pseudorandom numbers are generated and are being XORed with the Image pixels to change the pixel values and these operations are usually performed in non-overlapping blocks.

2.3 PERMUTATION

In this process, chaotic maps like cat map and Henon map are recommended to shuffle the pixels for confusion phase. Compared with all other maps, cat map has the smallest key space so that security can't be achieved more enough. To overcome this defect, the image is divided into overlapping blocks so that the centre part of the image gets shuffled well so that key space can be improved well. Recent research on encryption proves that block-wise permutation provides better results than to be operated in bit level and pixel level.

In order to produce a large key space, a new cat map named separated block Cat map [22] is designed and more control parameters are added in this process for permutation to improve the security. These control parameters are taken from Henon map. The image is divided into four overlapping blocks as shown in Fig.2 and each block is processed by cat map. The four squares of the entire image is divided into AEKF, FLGD, EBHJ and IHCG. The sizes of four squares depend on length of AE. Let the length of AE be chosen as 185 and then length of EB is calculated by the relation,

$$\begin{aligned} Li(EB) &= N - Li(AE); \\ Li(AF) &= Li(AE); \\ Li(FD) &= Li(EB); \end{aligned} \tag{4}$$

where, N is the size of the image. For Experimental purpose, the Lena image of size 256×256 is taken and is divided into blocks. Each block is considered as a separate square and is permutated by cat map as in Eq.(1).

The permutation using cat map is explained as:

Step 1: The pixel in one location will be shifted to another location and hence the position of pixels gets shuffled two times due to overlapping block division.

Step 2: 'p' and 'q' are the control parameters of cat map its value were derived by Henon map.

Step 3: After each block gets processed, finally the whole image is permutated.

In this scheme by overlapping division centre part of image (IJKL) get confused two times, which proves image retrieval, is not much easy. The Fig.3 shows the original image, permuted image, cipher image and decrypted image of the proposed image encryption method.

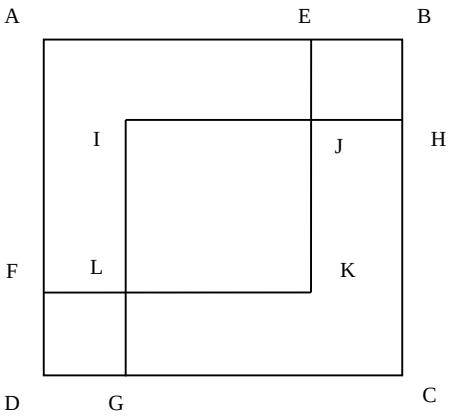


Fig.2. Overlapping Blocks Division

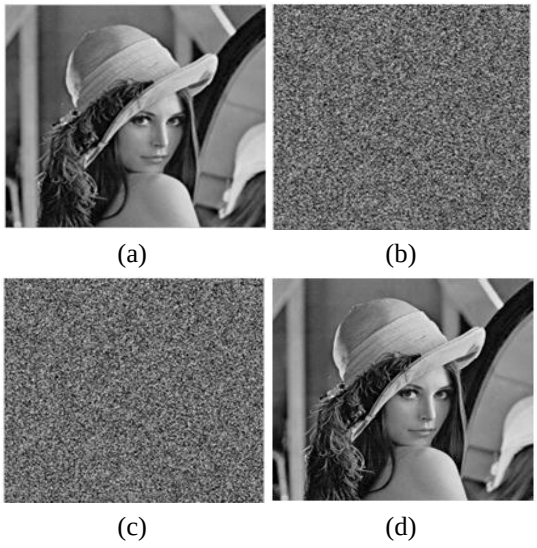


Fig.3. (a). Original image, (b). Permuted Image (c). Cipher image, (d). Decrypted image

2.4 DIFFUSION

To avoid known-plaintext and chosen-plaintext attacks, the pixel values are altered dramatically in diffusion process since the change made to particular pixel depends on the effect of all the previous pixel values. The Logistic map [7] employed in this phase is defined as,

$$z_{i+1} = \lambda z_i (1 - z_i) \tag{5}$$

where, 'λ' is a system parameter lies between 0 and 4. It acts as an initial condition of the map and 'i' be the number of iterations. Based on initial condition the iterative values were generated. By varying the system parameter 'λ', behaviours of map can be changed. Only if the value becomes greater than or equal to 3.57, it is converted into chaotic maps because a slight variations in the initial condition produces different iterative values.

The permuted image is divided into four non-overlapping blocks. From the Logistic map z_i, pseudorandom numbers are generated for the entire diffusion process. For each block division different keys are selected for logistic map. Convert each 2D image block into 1D sequence $s = \{s_i\}$. The diffusion process is given the Eq.(6), let $q_0 = 64$, $r_0 = 64$ by computing,

$$p(i) = q(i-1) \oplus r(i-1) \oplus s_i \oplus z_i \,, \qquad (6)$$

where, $q(i) = q(i - 1) \oplus r_i$, $r(i) = r(i - 1) \oplus q(i)$. Here s_i be the currently operated permuted pixels and $i = 1,2,\ldots,m\times n$. The random numbers from logistic map are being XORed with the original image pixels to produce diffused image. Let $p = \{p(i)\}$ be the newly generated diffusion sequence from permuted image. The diffusion process is repeated for all blocks and combines all divided blocks to get back the cipher image.

2.5 DECRYPTION

The decryption is similar to the reverse process of encryption. The diffusion process is done first. It is followed by cat map along with block decomposition. After performing these operations, the cipher image is converted into an original image.

3. SECURITY AND PERFORMANCE ANALYSIS

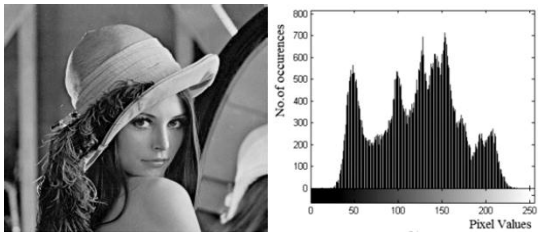
The Standard Lena image of size 256×256 is used as plain image. The corresponding cipher image analysis is provided in the following sections. Experimental parameters used in this algorithm are the control parameters '*a*' and '*b*' were given by, 1.2, 0.3. Initial values were taken as $H(x) = 0.26443$, $H(y) = 0.37724$ for Henon map, and $f(z) = 0.18565$ for logistic map. The proposed scheme is also tested with other standard images and their analysis was discussed.

3.1 STATISTICAL ANALYSIS

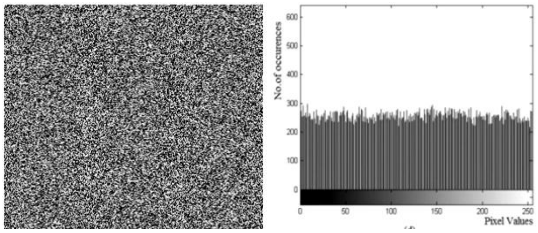
It is known that the generated cipher has to pass the statistical analysis and is of crucial importance for a cryptosystem. To evaluate the security, the following statistical tests are performed. The result proves that the cipher image is robust against any attacks and bears no statistical similarity to the plain image.

3.1.1 Histogram:

The histogram for various images are shown in the Fig.5, Fig.6, Fig.7 and Fig.8 and it is a plot between pixel values and its number of occurrences. The pixels in the histogram of various plain images are highly correlated and form peak like structure resembling the original image. But the histogram of cipher image is highly uniform and the pixels are randomly distributed which shows that it is widely different from the original image and hence it does not provide any clue to employ statistical analysis attack on the encryption image.

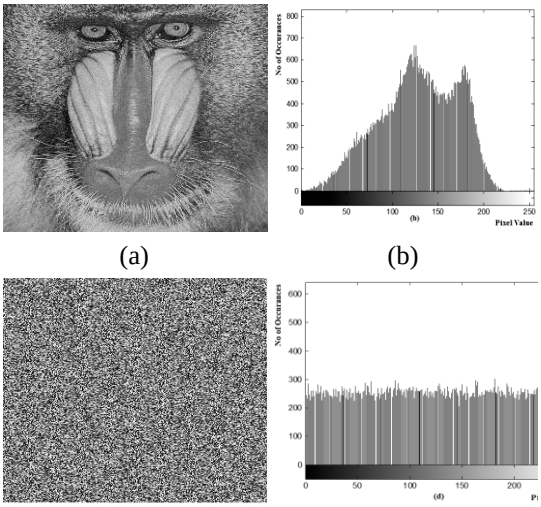


(a) (b)



(c) (d)

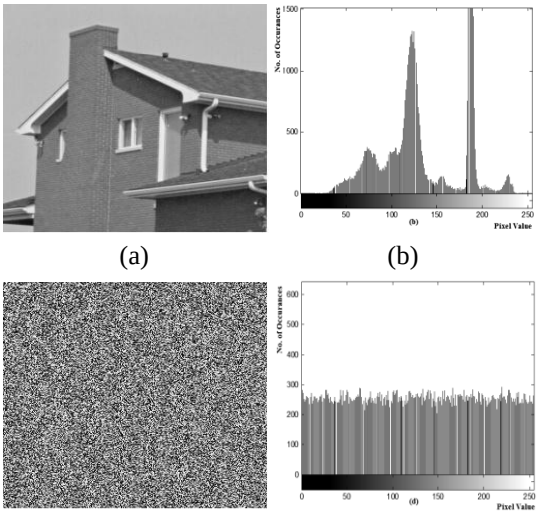
Fig.5. (a). Original Image, (b). Histogram of the Original Image, (c). Cipher Image, (d). Histogram of the Cipher Image



(a) (b)

(c) (d)

Fig.6. (a). Baboon Image, (b). Histogram of the Original Image, (c). Cipher Image, (d). Histogram of the Cipher Image



(a) (b)

(c) (d)

Fig.7. (a). House Image, (b). Histogram of the Original Image, (c). Cipher Image, (d). Histogram of the Cipher Image

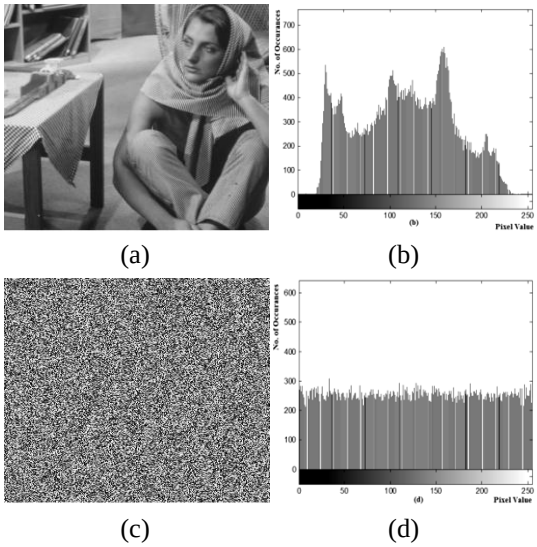


Fig.8. (a). Barbara Image, (b). Histogram of the Original Image, (c). Cipher Image, (d). Histogram of the Cipher Image

3.1.2 Correlation of Adjacent Pixels:

The correlation between two vertically, two horizontally, and two diagonally adjacent pixels in Lena cipher image is carried out and its plots are shown in Fig.9. Correlation coefficient factor is used to measure the relationship between two images, the plain image and its encrypted image. To test this correlation, randomly select 5,000 pairs of adjacent pixels from the image and then calculate the correlation coefficient r_{xy}. The correlation coefficient is calculated using the Eq.(7) and Eq.(8).

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

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

where, x and y are grey values of two adjacent pixels in the image and $E(x)$ and $D(x)$ are the expectation and variance of variable x, respectively.

Table.1. Correlation Coefficients

Correlation coefficient type	Plain image	Cipher image
Horizontal	0.9873	-0.0021
Vertical	0.9452	0.0023
Diagonal	0.9258	0.0132

Table.2. Comparison results of correlation coefficients of proposed algorithm with other algorithms in different directions

Algorithm	Correlation Coefficients		
	Horizontal	Vertical	Horizontal
HuaqianYang et al. scheme [12]	-0.0020	0.0161	-0.0020
Yushu Zhang et al. scheme [20]	0.0018	0.0011	0.0018
Proposed scheme	-0.0021	0.0023	-0.0021

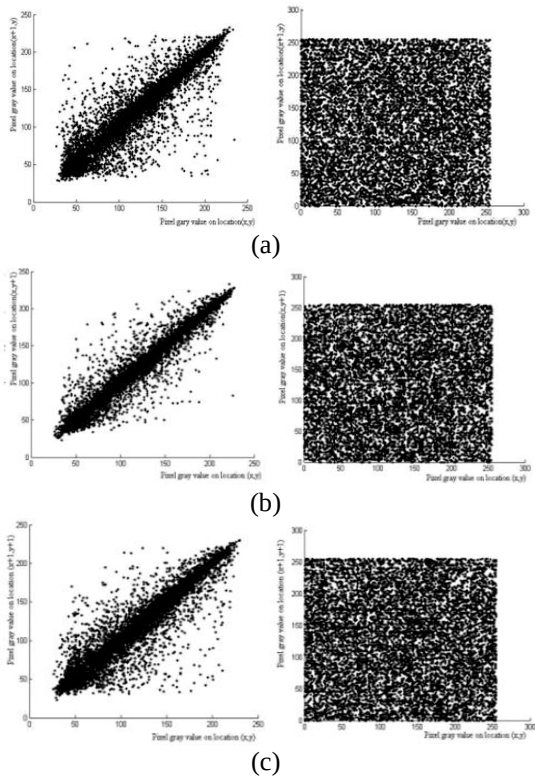


Fig.9. Correlation plots of original and cipher images in (a). Horizontal direction (b). Vertical direction and (c). Diagonal direction

The Table.1 lists the correlation coefficient and it reveals that the correlation coefficient of plain image will be equal to 1 which indicates high correlation among pixels and that of cipher image will be nearly equal to 0 which shows that there is no correlation among the images. Therefore, the proposed algorithm possesses high security against statistical attacks. The Table.2 shows the comparison results of proposed algorithm and other two algorithms which prove better correlation coefficient values that is required for security criterion.

3.1.3 Entropy Analysis:

It is one of the criteria to measure the strength of encryption. The entropy of a message source can be measured by [7],

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

where, M is total number of symbols, $p(m_i)$ represents the probability of occurrence of symbol mi and log denotes the base 2 logarithm so that entropy is expressed in bits. This is because taking 8 bytes as a unit, probability of every symbol in accordance with uniform distribution would be 1/8, entropy should be always 8. The proposed scheme produces the cipher image whose entropy value be 7.99934 which is highly efficient as it is very close to the ideal value 8. From Table.3 it is proved that the information leakage during encryption is negligible and thus the proposed system has good confusion and diffusion properties. The Table.4 shows the entropy values of proposed one along with other algorithms which is equal to 8.

Table.3. Entropy of Different Images

Image types	Plain image	Cipher image
Lena	7.724	7.9993
Baboon	7.6573	7.9964
House	7.5478	7.9876
Barbara	7.4521	7.9652

Table.4. Comparison of Entropy analysis for Lena image

Algorithm	$H(m)$
Yushu Zhang et al. scheme [20]	7.99943
Proposed scheme	7.99945

3.1.4 Differential Attack Analysis:

In general, intruder may make a slight change in the pixels of plain image and check for significant changes in cipher image. To test this, two measures are generally used they are NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [7]. They are calculated by 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 cipher images obtained from the plain images that have a slight difference in one pixel. Similarly, W and H are width and Height of the cipher image. A secure algorithm must reach 99% of NPCR value and 33% of UACI value indicating that the proposed algorithm is key sensitive to both plain and cipher images. Tests are performed on various images and the results are presented in the Table.5. Also from Table.6 it can be seen that the proposed scheme provides better results even in the first round compared to other algorithms.

Table.5. NPCR AND UACI Analysis for various Images

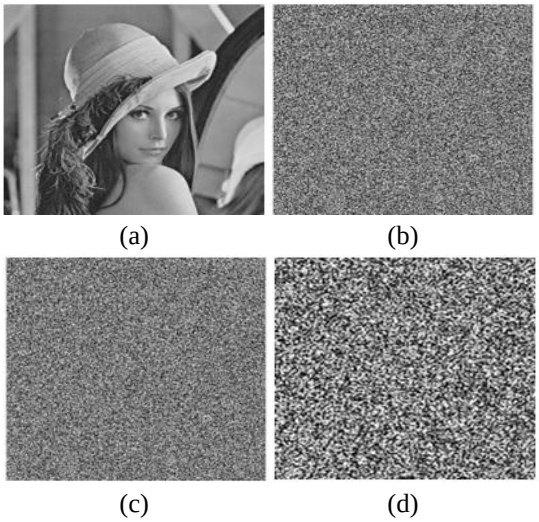
Images	NPCR	UACI
Lena	0.9964	0.3352
Baboon	0.9943	0.3332
House	0.9927	0.3346
Barbara	0.9953	0.3357

Table.6. NPCR and UACI analysis of proposed and other algorithms

Algorithm	NPCR	UACI
Huaqian Yang et al. scheme [12]	0.99618	0.3347
Yushu Zhang et al. scheme [20]	0.99616	0.3343
Proposed scheme	0.99640	0.3352

3.1.5 Sensitivity Analysis:

To test this, first Lena image is encrypted by using a pair of keys as 0.26443 and 0.37724.



(a) (b)

(c) (d)

Fig.7. (a). Plain image, (b). Cipher Image with key 0.26443, 0.37724, (c). Cipher Image with key 0.26444, 0.37725, (d). Difference between two Cipher Images

Then in this, the least significant bit of key is changed from the originals as 0.26444 and 0.37725 and is again processed to get cipher image. Finally, the above two encrypted images of slightly different keys are compared and the result analysis are shown in Fig.7. This Figure indicates even a single bit key change will produce different cipher images.

3.1.6 Randomness Test with SP800-22 Test Suite:

NIST recommends two strategies for performance analysis [23]-[24]. First, the *P-values* that checks for uniform distribution in the interval [0, 1]. Second, to calculate the proportion of sequences that pass the test and comparing it with the expected values which are derived from Eq.(13). If *P-value* ≥ 0.0001, then the condition is met and considered to be uniformly distributed, it is calculated by using the following equations:

$$P - value = \text{igamc}\left(\frac{9}{2}, \frac{\chi^2}{2}\right) \quad (12)$$

where, igamc is the incomplete gamma function.

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - N/10)}{N/10} \quad (13)$$

where, 'F_i' be the number of occurrences and 'i' for i^{th} interval. Here, 'N' denotes the sample size (N = 100). The Table.7 shows the results of randomness test which implies that the proposed cipher has also passed all the statistical tests involved in SP800-22 test suite.

Table.7. Randomness Test

Statistical test	P-value	Result
Frequency test	0.6924	Success
Block frequency test	0.7453	Success

Runs test	0.5241	Success
Long runs of one's	0.5742	Success
Binary Matrix Rank	0.2896	Success
Spectral DFT test	0.5698	Success
Non- overlapping test templates	0.6985	Success
Overlapping test templates	0.8957	Success
Universal test	0.8596	Success
Serial test 1	0.3698	Success
Serial test 2	0.5698	Success
Approximate entropy test	0.2398	Success
Cumulative sums	0.5896	Success
Random excursions test	0.8965	Success
Random excursions variant test	0.7896	Success
Serial test 1	0.3698	Success
Serial test 2	0.5698	Success

4. CONCLUSION

A secure chaotic encryption scheme based on permutation-diffusion architecture has been proposed. In our scheme, both the pixel level and bit level permutation are replaced by block permutation and cat map is used to process each block in such a way its key space can be improved. It involves pseudorandom number generation based on different keys and employs logistic map for diffusion. Simulation results show that satisfactory security performance is achieved in only one encryption round itself. The proposed scheme is verified by the security analyses on its key sensitivity, randomness test, statistical and differential properties and is suitable for real-time application.

REFERENCES

[1] Shiguo Lian, Jinsheng Sun and Zhiquan Wang ang, "A Block Cipher based on a suitable use of the Chaotic Standard Map", *Chaos Solitons and Fractals*, Vol. 26, No. 1, pp. 117-129, 2005.

[2] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao and Tao Xiang, "A Block Cipher with Dynamic S-boxes based on Tent Map", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 14, No. 7, pp. 3089-3099, 2009.

[3] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "A Chaos-based Symmetric Image Encryption scheme using a Bit-Level Permutation", *Information Sciences*, Vol. 181, No. 6, pp. 1171-1186, 2011.

[4] Xingyuan Wang, Lin Teng and Xue Qin, "A Novel Colour Image Encryption Algorithm based on Chaos", *Signal Processing*, Vol. 92, No. 4, pp. 1101-1108, 2012.

[5] Tiegang Gao and Zengqiang Chen, "A New Image Encryption Algorithm based on Hyper-Chaos", *Physics Letters*, Vol. 372, No. 4, pp. 394-400, 2008.

[6] C.K. Huang and H.H. Nien, "Multi-chaotic systems based Pixel Shuffle for Image Encryption", *Optics Communications*, Vol. 282, No. 11, pp. 2123-2127, 2009.

[7] T. Gopalakrishnan, S. Ramakrishnan and M.Balakumar, "An Image Encryption using Chaotic Permutation and Diffusion", *Proceedings of fourth International Conference on Recent Trends in Information Technology*, pp 1-5, 2014.

[8] T. Gopalakrishnan and S. Ramakrishnan, "Image Encryption in Bit Wise and Key Generation using Multiple Chaotic Maps", *Australian Journal of Basic and Applied Sciences*, Vol. 9, No. 27, pp. 200-208, 2015.

[9] R. Ranjith Kumar and M. Bala Kumar, "A New Chaotic Image Encryption Using Parametric Switching Based Permutation and Diffusion", *ICTACT Journal on Image and Video Processing*, Vol. 4, No. 4, pp. 795-804, 2014.

[10] Chengqing Li, Shujun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez and Guanrong Chen, "On the Security defects of an Image Encryption Scheme", *Journal on Image and Vision Computing*, Vol. 27, No. 9, pp.1371-1381, 2009.

[11] Di Xiao, Xiaofeng Liao and Pengcheng Wei, "Analysis and improvement of a Chaos-based Image Encryption Algorithm", *Chaos, Solitons and Fractals*, Vol. 40, No. 5, pp. 2191-2199, 2009.

[12] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang and Pengcheng Wei, "A Fast Image Encryption and Authentication Scheme based on Chaotic Maps", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 15, No. 11, pp. 3507-3517, 2010.

[13] M. Francois, T. Grosges, D. Barchiesi and R. Erra, "A New Image Encryption Scheme based on a Chaotic Function", *Signal Processing: Image Communication*, Vol. 27, No. 3, pp. 249-259, 2012.

[14] Xiaojun Tong and Minggen Cui, "Image Encryption Scheme based on 3D Baker with Dynamical Compound Chaotic Sequence Cipher Generator", *Signal Processing*, Vol. 89, No. 4, pp. 480-491, 2009.

[15] Xiaofeng Liao, Shiyue Lai and Qing Zhou, "A Novel Image Encryption Algorithm based on Self-Adaptive Wave Transmission", *Signal Processing*, Vol. 90, No. 9, pp. 2714-2722, 2010.

[16] Kwok-Wo Wong, Bernie Sin-Hung Kwok and Wing-Shing Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", *Physics Letter A*, Vol. 372, No. 15, pp. 2645-2652, 2008.

[17] Tao Xiang, Xiaofeng Liao, Guoping Tang, Yong Chen and Kwok-wo Wong, "A Novel Block Cryptosystem based on Iterating a Chaotic Map", *Physics Letter A*, Vol. 349, No. 14, pp. 109-115, 2006.

[18] Jui-Cheng and Jiun-In Guo, "A New Chaotic Key-based Design for Image Encryption and Decryption", *Proceedings of the IEEE International Conference Circuits and Systems*, Vol. 4, pp. 49-52, 2000.

[19] Guanrong Chen, Yaobin Mao and Charles K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", *Chaos, Solitons and Fractals*, Vol. 21, No. 3, pp. 749-761, 2004.

[20] Yushu Zhang and Di Xiao, "An Image Encryption Scheme based on Rotation Matrix Bit-Level Permutation and Block Diffusion", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 19, No. 1, pp. 74-82, 2014.

[21] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao and Guanrong Chen, "A New Chaos based Fast Image Encryption Algorithm", *Applied Soft Computing*, Vol. 11, No. 1, pp. 514-522, 2011.

[22] Xiao-Jun Tong, "Design of an Image Encryption Scheme based on a Multiple Chaotic Map", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 18, No. 7, pp. 1725-1733, 2013.

[23] A. Kanso and M. Ghebleh, "A Novel Image Encryption Algorithm based on 3D Chaotic Map", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 17, No. 7, pp. 2943-2959, 2012.

[24] Ali Kassem, Hussein Al Haj Hasson, Youssef Harkouss and Rima Assaf, "Efficient Neural Chaotic Generator for Image Encryption", *Digital Signal Processing*, Vol. 25, pp. 266-274, 2014.