ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2015.0149

A NEW ONE ROUND IMAGE ENCRYPTION ALGORITHM BASED ON MULTIPLE CHAOTIC SYSTEMS

R. Ranjith Kumar[1], B. Saranraj[2] and S. Pradeep[3]

Department of Electronics and Communication Engineering, P.A. College of Engineering and Technology, India

E-mail: [1]rranjithkumar7@gmail.com, [2]saranraj2011@gmail.com, [3]pradeep11452@gmail.com

Abstract

This paper presents a bit level pixel by pixel chaotic image encryption scheme with a permutation–diffusion structure. In this scheme, a Neural Network Like Structure (NNLS) is proposed to do the diffusion efficiently. The plain image, split into 16 blocks is permuted by the keys from the key generator. Each key will produce different permutation order (PO) generated using a chaotic map. After permutation, the pixels of the permuted image is converted into bits and given to the proposed NNLS, where the diffusion takes place. The bit by bit diffusion performed by NNLS on the pixels will give more randomness to the cipher image. The performance of the NNLS is contingent upon sensitivity of the keys from the key generator. The test results and analyses performed using several security standards shows that the proposed scheme is more secure, reliable and can be used for real time image encryption.

Keywords:

One Round Encryption, Permutation, Diffusion, NPCR, UACI, NIST

1. INTRODUCTION

Due to the growth of World Wide Web and technologies there is an increase in the transmission and processing of digital images. Fields like medical, Army, industry, multimedia etc. are mostly deals with the transmission of the digital images. After the intensification of internet there are millions of images transferred through the internet by the above mentioned fields. Even in personal millions of images are stored and transmitted through the internet every day. To ensure secure transmission we need a technique called encryption. These techniques defend our information from the eavesdropper. So many encryption schemes have been put forwarded during most recent years. Some of these encryption schemes are based on scan pattern methodology [4], random permutations, random phase encoding and chaos maps etc. Among these, due to the intrinsic and ergodicity characteristics, chaotic map based encryption schemes afford an appropriate response in secure image encryption. Dynamical systems which have the ability to generate numbers that are random in nature and highly sensitive to initial conditions are used to encrypt the image in chaos based methods. Since the map is greatly sensitive to the initial conditions it provides more complexity in permutation and diffusion stages of encryption. It also satisfies the speed required in Real-time. The main inspiration of employing chaotic systems in image encryption is its simplicity in form and complexity in dynamics. Because of the strong correlation among the image pixels, permutation alone will not give the required levels of security. To obtain a robust encryption scheme we need to permute and diffuse the position and values of the pixels respectively. Conditions like key space, key sensitivity, and randomness of cipher must be satisfied by the encryption scheme [7]-[9]. A first application for transmitting signals using chaos was proposed by Pecora and Carroll [1]. Baptista designed a cryptosystem that encrypt text messages [2], this system is the base for all chaos based cryptographic proposals found at present, [3] – [15] are some encryption schemes based on chaotic maps. A noteworthy scheme based on Baptista‘s design that uses a dynamic look-up table in the cryptographic scheme [4], provides more security as a result of the dynamic lookup table updating and dimension concern to next input block and encryption speed is faster than the previous methods [1], [5]. The image encryption is not analogous to data encryption. A good encryption scheme must adapt permutation and diffusion with optimum trade-off. In Chaotic image encryption the dynamical system‘s output are converted to do permutation and diffusion processes. Fridrich [6] proposed the chaos based image encryption based on permutation and diffusion prototype. Permutation and diffusion on the pixels in an iterative manner will result in a better encryption scheme. Such schemes are [7] - [10]. In [7] and [8], chaotic standard maps were used for permutation and diffusion of the pixels. Ref [8] is the customized version of [7], where a simple pixel adjustment is made in permutation phase itself to trim down the time taken for diffusion phase. The encryption time is lesser than the Lian et.al method, anyway the sequential add and a shift operations in the diffusion phase leads to large computation, which is the drawback. The technique [9] based on bit stream permutation along with diffusion put forwarded by Francois et.al using the chaotic function was inspired by recurrences of pseudo-random numbers generation, such a function is used to compute the positions to which the bit stream has to be swapped. In the diffusion process the pixel values are diffused by the current pixel with newly generated pixel [16]. Lian et.al recommended standard map for permutation and logistic map for diffusion to achieve the reasonable level of security. In this method permutation of 4 rounds, permutation along with diffusion 4 rounds leads to 16 total rounds(minimum) for encrypting the image. The overall encryption is still not fast enough. In Wong et.al method, standard map is used for permutation and the current pixel of the plain image is added with the pervious permutated pixel in diffusion. The ‘add and shift’ operation in Wong et.al leads to longer duration for the image encryption. François et.al encryption algorithm satisfies the NIST standards for image encryption and need a minimum of 22 rounds to achieve the security level. The technique [17] is based on hyper-chaotic systems, realized encryption easily in one round diffusion process and is computationally very simple while attaining high security level, high key sensitivity, high plaintext sensitivity and other properties simultaneously. The key stream generated by hyper-chaotic system is related to the original image. The proposed algorithm [17] yields much better security performance in comparison to the results obtained from other algorithms. The drawbacks of the earlier methods are overcome by the proposed method. A new bit level pixel by pixel image encryption scheme proposed in this paper focuses on key generation process and a new structure that resembles neural network for diffusion, considerably increases the randomness of the cipher image. The proposed NNLS reduces the number of rounds to one and it achieves more security. The plain image is block permuted before diffusion. The rest of this paper is organized as follows, section two describes proposed method, and section 3 gives the results of various analyses and section 4 is the conclusion.

2. PROPOSED METHOD

2.1 INTRODUCTION

Figure 1 shows the structure of proposed encryption scheme. The plain image is given to the permutation block, which obtains the keys from the key generator [18]. The process is shown in Fig.2. The plain image is segregated as 16 equal squares. First each square is permuted. After this four squares are combined and are permuted. As this is done the 4 squares that are present in the centre of the images are permuted. And at last as a whole the full image is permuted. Each block is permuted by separate permutation order generated using Eq.(1),

$$\text{CO} = \text{indices}\ \{\text{Xi (logistic)* 1014) mod N}\} \tag{1}$$

where, Xi(logistic) is the value obtained from the logistic map iteration and N is equal to the number of pixels present in a block. After Permutation each pixel of the permuted image is converted into binary (8 bits per pixel) and given to the proposed NNLS shown in Fig.4. Each bit will travel through the nodes specified as H1, H2…H16 as shown in Fig.4. Nodes will be filled with random bits generated by the chaotic maps and further randomized by the biasing values given to each node as shown in Fig.3. The biasing values are the iteration values of the Map 1 and 2 as shown in Fig.3.

Based on the condition in Eq.(3) all node values will be randomized and this randomness is proved by NIST test suite [19] in Table 3. Each bit travelling through these nodes is XOR-ed with the values present in the nodes. This process completely randomizes the pixel values in a reversible manner. This diffusion is carried out for all the pixels and it completely breaks the correlation among the pixels after permutation. Since the proposed structure is complex and performs bit by bit operation, roughly single round is enough for attaining the required security level. The results obtained in this scheme are analyzed and tested against various standard values in the next section.

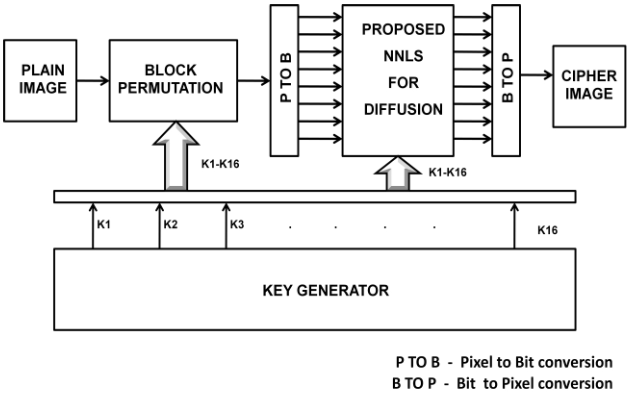

Fig.1. Proposed structure

$$\text{Map 1 \& 2} = \left\{ \begin{array}{ll} Xi(logistic) & i = 2,3,\ldots,m \\ Xi(tent) & n = i > m \end{array} \right\} \tag{2}$$

where, m = n/2 and n is number of nodes available in total. Based on the values of Map 1 & 2 Values present in each node is modified to increase the randomness. The condition to set the values at each node is given by,

$$\text{Node value} = \left\{ \begin{array}{ll} 1 & if\ \ Map\,1 \geq Map\,2 \\ 0 & else \end{array} \right\} \tag{3}$$

K1	K2	K3	K4
K5	K6	K7	K8
K9	K10	K11	K12
K13	K14	K15	K16

XOR (K1, K2, K5, K6)	XOR (K3, K4, K7, K8)
XOR (K9, K10, K13, K14)	XOR (K11, K12, K15, K16)

	XOR (K6, K7, K10, K11)		

Fig.2. Block permutation

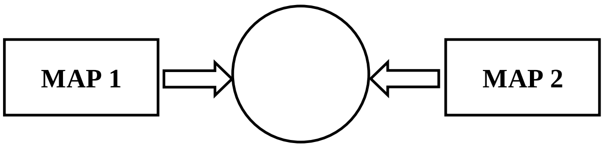

Fig.3. Biasing a node in NNLS

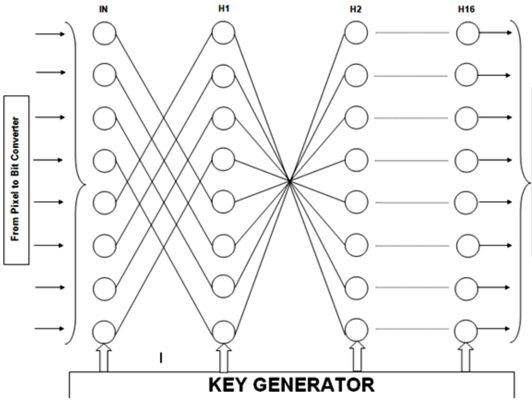

Fig.4. Proposed NNLS

3. PERFORMANCE ANALYSIS

3.1 KEY SPACE ANALYSIS

A key space which is of size smaller than 2^{128} is not enough secure for today‘s computer speed and is generally accepted for image encryption standards. There are two aspects that are contained by the secret key. First aspect is the key space size that characterizes the capability of resisting brute-force attack which can also be called as exhaustive search. The second is key non recovery property that must be computationally infeasible to recover the key. In this system LR chippers can be generated by increasing the value of R. In order to satisfy the relation $L^R > 2^{128}$ and to avoid the success of brute-force attacks, the minimum number of rounds R can be obtained from the relation [9],

$$\text{R} = \text{floor}\left[\frac{128}{\log_2 L}\right] + 1 \tag{4}$$

Lian [7] suggested that the key space should be at least 2^{64} for the sufficient security from the brute-force attacks. But in our encryption algorithm we are proposing the value of L is equal to 2414. For this value the total number of rounds will be equal to one. Though the value of R is 1 it proves not only the good encryption but also increases the complexity. The values of NPCR (number of pixel change rate), UACI (unified average changing intensity) and NBCR (Number of Bit Change Rate) which are measured between the two ciphers having slightly different plain images (or) keys are considered for fixing the value of R. Hence this method surely proves that this method stands against all the type of brute-force attacks.

3.2 STATISTICAL ANALYSIS

Statistical analysis is mainly employed in investigate the robustness of the proposed system against statistical attacks. To prove the robustness of the system proposed statistical analysis is performed by calculating histograms and correlation coefficients of the plain text and their corresponding cipher text produced by the algorithm.

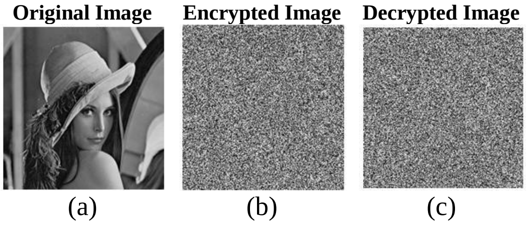

Fig.5.(a) Plain Image. (b) Encrypted Image. (c) Decrypted Image with single bit change in key

3.2.1 Histogram analysis:

A histogram which shows how the pixels are distributed on the image, is a graph drawn between pixel density and their color intensity level. The original and encrypted images of widely distributed contents are analyzed using this method. The histograms are fairly uniform and have better statistical properties which resembles as a white noise and it is illustrated. The results of such analyses are shown in the figure. The Fig.6(a) shows the original image and Fig.6(b) shows its cipher. Fig.6(c) and Fig.(d) shows their corresponding histograms. The encrypted image histogram is completely flat and not providing any possibility to the hacker to estimate the plain image.

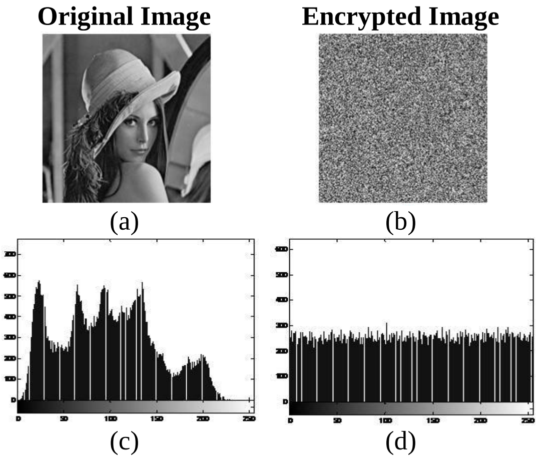

Fig.6.(a) Plain Image. (b) Cipher Image. (c) Histogram of Plain Image. (d) Histogram of Cipher Image

3.2.2 Correlation coefficient analysis:

Correlation between the pixels of the image must also be analyzed to check the robust of the system. Generally the correlation between the adjacent pixels in the original images is high, generally -1 or +1 (positive or negative correlation). Hence it has to be reduced deeply to provide a good encryption. This analysis shows the correlation between the randomly selected pixels of plain and encrypted images. This correlation coefficient analysis is carried out by selecting 10,000 pairs randomly in the manner that they are horizontally, vertically & diagonally adjacent. Since it appears like a 2 dimensional random variable the correlation can be calculated by using the formula mentioned below,

$$\mathrm{cov}(x,y) = E\{ (x-E(x))-(y-(E(y)) \} \tag{5}$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x,y)}\sqrt{D(y)}} \tag{6}$$

where, x and y denoted the two adjacent pixels in the image and E(x) and D(y) denotes the mean and standard deviation of corresponding grey levels. Therefore the proposed scheme efficiently reduces the correlation among the horizontal and vertical pixels and the pixels that are adjacent diagonally. From the table it can be clearly understood that the correlation among the pixels of plain image is nearly equal to one which is a positive value. But for cipher image the correlation among the pixel is merely zero and hence it shows that there is no correlation among those pixels. Fig.7 shows the correlation plot of plain and cipher images. Fig.7(a), Fig.7(b) and Fig.7(c) shows the horizontal, vertical and diagonally adjacent elements and Fig.7(d), Fig.(e) and Fig.(f) shows the corresponding plot of cipher image. Table 1 shows the correlation coefficient of the plain image and cipher image obtained by the scheme that has been proposed in this paper and three comparable block cipher [20] - [23].

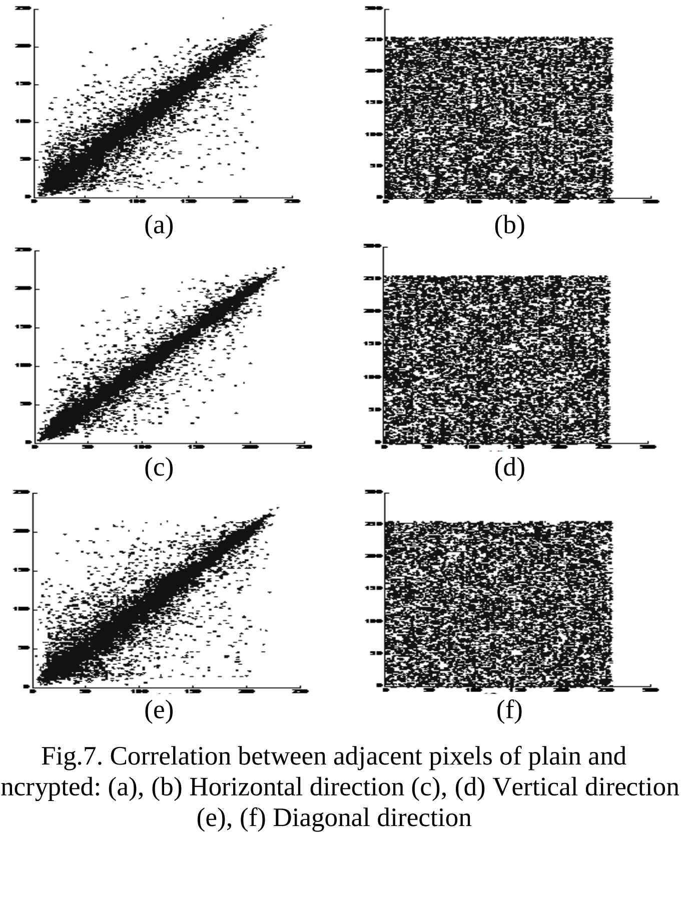

Fig.7. Correlation between adjacent pixels of plain and encrypted: (a), (b) Horizontal direction (c), (d) Vertical direction (e), (f) Diagonal direction

3.3 INFORMATION ENTROPY ANALYSIS

Information entropy is usually to describe the degree of uncertainty present in the system. For a given system the entropy can be calculated by using the below mentioned formula,

$$H(m) = \sum_{i=0}^{M-1} p(m_i)\log\frac{1}{p(m_i)} \tag{7}$$

where, m and p (m_i) represents the total number of symbols and probability of occurrence of the symbol. Since practical information entropy generates random messages the resulting information entropy is expected to be smaller than the ideal one. When designing the algorithm for the process of encryption one could expect the value of entropy that is as close as to the ideal one but the distribution of the cipher is major consideration here. Hence if it is not flat enough it gives way the enemy to guess some part of the image but not the complete one. The proposed method shows that both the plain and the cipher image have equal entropy which is nearly equal to 8 bits. It is shown in Table 2. Hence this scheme stands as a wall for those who are trying to decrypt the image without the keys.

3.4 DIFFERENTIAL ATTACK

NPCR and UACI: In order to resist all kind of differential attack the system must be highly sensitive even to a minute change in the plaintext. The methods which are most commonly used for the measurement of the sensitivity are NPCR and UACI which has been proposed by NIST [19] and they are given by the equations that are given below.

$$NPCR = \frac{1}{n}\left\|\{i | x_i \neq y_i, i = 0,1,..n-1\}\right\| \tag{8}$$

$$UACI = \frac{1}{n}\sum_{i}^{n-1}\frac{|x_i - y_i|}{255} \tag{9}$$

Given two images $x = \{x_0, x_1, \ldots, x_{n-1}\}$ and $y = \{y_0, y_1, \ldots, y_{n-1}\}$, the NPCR and UACI are defined as Eq.(8) and Eq.(9) [24]. For two random images, the average NPCR is about 0.9961, and the average UACI is about 0.3346 [25]. The NPCR and UACI values for various images calculated and tabulated in Table 2.

MAE (Mean absolute error): Mean Absolute Error (MAE) as another criterion to examine the performance of resisting differential attack [17]. Let C(i, j) and P(i, j) be the gray level of the pixels at the i^{th} row and j^{th} column of a M×N cipher and plain-image, respectively. The MAE between these two images is defined as:

$$MAE = \frac{1}{M \times N}\sum_{j=0}^{N}\sum_{i=0}^{M}\left|C(i,j) - P(i,j)\right| \tag{10}$$

The larger the MAE value, the better the encryption security. MAE is calculated and the results are tabulated in Table 2.

Strict Avalanche Criterion: The strict avalanche criterion (SAC) is proposed to observe the changes in bit-level and it is different from NPCR and UACI that quantitatively estimate the pixel-level deviations. The SAC states that a very small difference (i.e. one bit change) in the input will lead to an avalanche change in the output. According to the SAC‘s definition in [26], the Number of Bit Change Rate (NBCR) is to measure the SAC performance using Eq.(11). The NBCR calculates the percentage of changed bit numbers between two bit streams. The ideal NBCR is 50% in average [27]:

$$NBCR = \frac{H_m[s_1, s_2]}{L_b} \times 100 \tag{11}$$

where s_1 and s_2 are two bit streams with the bit length of L_b. The function H_m [.] is to calculate the Hamming distance of two bit streams. Dissimilar from the differential attack, s_1 be the encrypted image bit sequence with initial secret key and s_2 be the encrypted image bit sequence with modified secret key. Their NBCR is measured and the results are listed in Table 2.

Table.1. Correlation coefficients of the original Lena image and the encrypted images obtained by the proposed scheme and the three comparable block ciphers

Scheme		Vertical	Horizontal	Diagonal
Original Lena image		0.9882	0.9856	0.9669
AES[20]		0.0770	0.0660	-
Algorithm[21]		0.0845	0.0681	-
Algorithm[22]		0.0965	-0.0318	
Algorithm[23]		0.0009	-0.0011	0.0011
Proposed algorithm	Lena	0.0015	0.0069	0.0018
	cameraman	-0.0051	0.007	-0.0014
	Couple	0.0031	-0.0012	0.0013
	Barbara	-0.0021	0.0031	0.0057

Table.2. Entropy and differential analysis (Images from SIPI database)

Sl. No.	IMAGE	ENTROPY		NPCR	UACI	NBCR	MAE
		Plain	Cipher				
1	Leopard	6.5264	7.9975	0.9965	0.3354	49.9426	89.93
2	Aerial	7.3118	7.9973	0.9958	0.3360	50.0277	72.90
3	Airplane	6.4523	7.9973	0.9963	0.3363	50.1944	85.31
4	Airport	6.6955	7.9968	0.9963	0.3366	50.0544	85.88
5	baboon	7.3903	7.9580	0.9956	0.3365	50.0357	71.27
6	Barbara	7.5838	7.9968	0.9962	0.3360	49.9090	75.56
7	Boat	7.1583	7.9976	0.9960	0.3364	50.0048	72.31
8	Cameraman	7.0097	7.9970	0.9957	0.3353	50.0437	79.40
9	Car and APC	6.7718	7.9974	0.9962	0.3362	50.1215	71.01
10	Chemical plant	7.3424	7.9967	0.9960	0.3355	49.9929	73.06
11	Clock	6.7057	7.9973	0.9960	0.3369	49.9632	89.86
12	Couple	7.1720	7.9972	0.9961	0.3350	50.0048	72.73
13	Einsteen	6.8841	7.9971	0.9959	0.3359	50.0605	71.90
14	Eline	7.4878	7.9973	0.9968	0.3352	49.9762	72.27
15	Lena	7.5683	7.9971	0.9963	0.3368	50.0788	78.08
16	Man	7.5360	7.9973	0.9962	0.9962	49.9876	82.27
17	Moon surface	6.7093	7.9972	0.9958	0.3366	49.9781	73.17
18	Peppers	7.5327	7.9967	0.9958	0.3368	50.0723	75.18
19	Resolution chart	1.5483	7.9959	0.9962	0.3358	50.0296	123.41
20	Stream and bridge	7.6682	7.9972	0.9965	0.3335	49.9922	75.50
21	Tank	6.4473	7.9969	0.9960	0.3353	50.0311	73.25
22	Truck and apc	7.0526	7.9966	0.9960	0.3364	49.9235	70.40
23	256 level test pattern	7.6695	7.9968	0.9961	0.3360	50.0864	77.34
24	Galaxy	5.6538	7.9974	0.9963	0.3360	50.1719	74.95
25	estatue	6.7807	7.9970	0.9957	0.3347	49.9891	70.10
26	All zeroes	0	7.9950	0.9961	0.3359	50.1023	126.78

Randomness test with sp800-22 test suite: NIST recommends two strategies to perform the analysis of the generator [18]. First, to check if the P-values are uniformly distributed in the interval [0, 1] with a goodness of fit test, and second, to calculate proportion of sequences passing a test and compare it with the expected value Eq.(12). The distribution of P-values for a large number of binary sequences (N=100) has been examined to check the uniform distribution of P-values for each test. The computation is as follows:

$$\chi^2 = \sum_{i=1}^{10} \frac{\left(F_i - N/10\right)}{N/10} \tag{12}$$

where F_i is the number of occurrences that the P- value is in the ith interval and N denotes the sample size (N=100). The P-value of the P-values is calculated using Eq.(13),

$$P - value = igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right) \tag{13}$$

where, *igamc* is the incomplete Gamma function [19]. If P-values greater than or equal to0.0001thenthe P-values are considered to be uniformly distributed. The results of each statistical test are presented in Table 3. The encrypted image has passed all the tests and also the distribution of the encrypted image is in uniform. NIST test proves the encrypted image information is in random.

Table.3. Randomness Test

Statistical Test		**Generated random bits**	**Cipher image**	**Results**
		P-value	**P-value**	
Frequency		0.8967	0.8967	Success
Block Frequency		0.5486	0.5486	Success
Runs		0.4344	0.4344	Success
Statistical test		0.8003	0.8003	Success
Long runs of one‘s		1.0000	1.0000	Success
Binary Matrix Rank		0.8572	0.8572	Success
Spectral DFT		0.7079	0.7079	Success
No overlapping templates		0.8248	0.8248	Success
Overlapping templates		0.9964	0.9964	Success
Universal		0.5412	0.5412	Success
Serial	P-value 1	0.7955	0.7955	Success
	P-value 2	0.4201	0.4201	Success
Approximate Entropy		0.6782	0.6782	Success
Cumulative sums		0.4831	0.4831	Success
Random excursions		0.7565	0.7565	Success
Random excursions variant		0.9002	0.9002	Success

4. CONCLUSION

The proposed encryption scheme is based on bit level diffusion using chaotic maps and various analyses have been done to prove the security level of proposed encryption scheme. In the proposed method a new key generation process is used to generate the secondary key, which improves the security of the cipher image. This encryption algorithm is based on the combination of chaotic maps. The maps are initialized by external keys. It has a greater sensitivity to the minute change in the key due to the structure proposed for key generation and has one round to achieve the required security. This scheme has proved the performance analysis tests and guarantees a negligible correlation between the pixels in the cipher. These methods are future extended for encryption and compression during the image transmission. The secondary key updated in the diffusion bit generator, it resists the chosen plain text attack. This updation provides different random bits for diffusion process. The statistical, key space and key sensitivity analysis shows that the proposed method is robust and provides secure image transformation.

REFERENCES

[1] Louis M. Pecora and Thomas L. Carroll, “Synchronization in chaotic systems”, *Physical Review Letters*, Vol. 64, No. 8, pp. 821–824, 1990.

[2] M.S. Baptista, “Cryptography with Chaos”, *Physics Letter A*, Vol. 240, No. 1-2, pp. 50–54, 1998.

[3] Frank Dachselt and Wolfgang Schwarz, “Chaos and Cryptography”, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48, No. 12, pp. 1498–1509, 2001.

[4] K.W. Wong, “A fast chaotic cryptographic scheme with dynamic look-up table”, *Physics Letters A*, Vol. 298, No. 4, pp. 238–242, 2002.

[5] Wai-kit Wong, Lap-piu Lee and Kwok-wo Wong, “A modified chaotic cryptographic method”, *Computer Physics Communications*, Vol. 138, No. pp. 234-236, 2001.

[6] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps”, *International Journal of Bifurcation Chaos*, Vol. 8, No. 6, pp. 1259-1284, 1998.

[7] S. Lian, J. Sun and Z. Wang, “A block cipher based on a suitable use of chaotic standard Map”, *Chaos, Solitons and Fractals*, Vol. 26, No. 1, pp. 117–129, 2005.

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

[9] M. Francois, T. Grosges, D. Barchiesi and R. Erra, “A new image encryption scheme based on a chaotic function”, *Image Communication*, Vol. 27, No. 3, pp. 249–259, 2012.

[10] A. Ahmed, Abd El-Latif, Li Li, Tiejun Zhang, Ning Wang, Xianhua Song and Xiamu Niu, “Digital image encryption scheme based on multiple Chaotic systems”, *Sensing and Imaging*, Vol. 13, No. 2, pp. 67–88, 2012.

[11] 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 Numeric Simulation*, Vol. 14, No. 7, pp. 3089–3099, 2009.

[12] Yang Tang, Zidong Wang and Jian-an Fang, “Image encryption using chaotic coupled map lattices with time-varying delays”, *Communications in Nonlinear Science and Numeric Simulation*, Vol. 15, No. 9, pp. 2456–2468, 2010.

[13] T.S. Parker and L.O. Chua, “Chaos: a tutorial for engineers”, *Proceedings of the IEEE*, Vol. 75, No. 8, pp. 982–1008, 1987.

[14] Pareek N.K, Patidar V and Sud K.K, “Image encryption using chaotic logistic map”, *Image and Vision Computing*, Vol. 24, No. 9, pp. 926-934, 2006.

[15] L. Blum, M. Blum and M. Shub, “A simple unpredictable pseudorandom number generator”, *SIAM Journal on Computing*, Vol. 15, No. 2, pp. 364–383, 1986.

[16] Benyamin Norouzi, Sattar Mirzakuchaki, Seyed Mohammad Seyedzadeh and Mohammad Reza Mosavi, “A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process”, *Multimedia Tools and Applications*, Vol. 71, No. 3, pp. 1469-1497, 2014.

[17] 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.

[18] National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[19] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, "A modified AES based algorithm for image encryption", *International Journal of Computer Science & Engineering*, Vol. 1, No. 1, pp. 70–75, 2007.

[20] R. Rhouma, S. Meherzi and S. Belghith, "OCML based color image encryption", *Chaos, Solitons & Fractals*, Vol. 40, No. 1, pp. 309–318, 2009.

[21] Hongjun Liu and Xingyuan Wang, "Color image encryption based on onetime keys and robust chaotic Maps", *Computers & Mathematics with Applications*, Vol. 59, No. 10, pp. 3320–3327, 2010.

[22] Nooshin Bigdeli, Yousef Farid and Karim Afshar, "A robust hybrid method for image encryption based on Hopfield neural network", *Computers and Electrical Engineering*, Vol. 38, No. 2, pp. 356–369, 2012.

[23] Yicong Zhou, Long Bao and C.L. Philip Chen, "Image encryption using a new parametric switching chaotic system", *Signal Processing*, Vol. 93, No. 11, pp. 3039–3052, 2013.

[24] G. Chen, Y. Chen and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps", *Chaos, Solitons & Fractals*, Vol. 31, No. 3, pp. 571–579, 2007.

[25] J. J. Buchholz, "Matlab implementation of the Advanced Encryption Standard", http://buchholz.hs-bremen.de/aes/aes.htm, 2001.

[26] R. Forre, "The strict avalanche criterion: spectral properties of boolean functions and an extended definition", *Proceedings on Advances in Cryptology*, pp. 450–468, 1990.