ISSN: 0976-9102(ONLINE)
DOI: 10.21917/ijivp.2014.0114

A NEW CHAOTIC IMAGE ENCRYPTION USING PARAMETRIC SWITCHING BASED PERMUTATION AND DIFFUSION

R. Ranjith Kumar[1] and M. Bala Kumar[2]
[1]*Department of Electronics and Communication Engineering, P.A. College of Engineering and Technology, India*
E-mail: rranjithkumar7@gmail.com
[2]*Department of Electrical and Electronics Engineering, Dr. Mahalingam College of Engineering and Technology, India*
E-mail: balakumar862@gmail.com

Abstract
In this paper, a new loss-less symmetric image encryption using a permutation and diffusion structure is proposed. A new key generation process generates secondary keys that act as control parameter for permutation order and diffusion bit generator. The Image pixels are scrambled in bit level. Permutation order is generated using the parametric switching type that permutes the pixel in bit wise manner. In the diffusion stage the different keys were used to diffuse in each round. In the diffusion stage the image pixel bits are masked with the randomly generated binary sequence. Three chaotic systems employed to generate the secondary key, permutation order and diffusion bits. The simulation results prove the satisfactory level of security for image encryption.

Keywords:
Image Encryption, Bit Wise Permutation, Logistic Map, Diffusion, Tent Map, Sine Map, Parametric Switching

1. INTRODUCTION

In the modern communication the sharing of multimedia contents, medical imaging and telemedicine over the internet security of these contents plays a major role. Images are the real integral part of the information in internet communication. To protect the information from unauthorized snooping is to use an encryption algorithm to disguise the information. In the past decades various number theory based encryption techniques such as DES, AES, RSA, etc. [1,2]. The conventional encryption techniques does not seems to be appropriate for images due to some characteristics of images bulk data, solid correlation between adjacent pixels and high redundancy. The significant characteristics of chaotic dynamical systems are ergodicity, mixing property, sensitivity to initial conditions and system parameters [3]. Due to these properties of chaos the researchers enticed to make chaotic cryptosystem for image encryption.

Lian et al. [4] proposed a cryptosystem based on permutation and diffusion architecture and in that algorithm the standard map is used for the permutation and logistic map for diffusion. Wong et al. [5] encryption algorithm has two stages one is permutation and another one is diffusion, and this algorithm uses simple pixel modification in permutation stage to ensure the cipher security. In the diffusion stage the new ciphered pixel obtained by manipulating with the previous ciphered pixel. Chen et al. [6] proposed an image encryption with 3D cat map to shuffle the positions of the pixels and logistic map is used to mask the pixel. The above mentioned algorithm uses the one time keys or key stream to encrypt the image. Guanet al. [7] used a 2D cat map for pixel position rearrangement and the discretized Chen's chaotic system for diffusion stage to mask the shuffled image pixels. Wang et al. [8] encryption technique permutation process control parameter is updated at each round. In diffusion process the shuffled pixels are diffused with its previously ciphered pixel and also manipulated with the key stream generated by logistic map. To deliver better solution to image security problems different types of image encryption techniques [4-18] have been suggested during past two decades. Among these techniques chaotic systems (chaos based) offer good combination of speed, high security and complexity.

Many chaos-based image encryption algorithms have security weakness that can be cracked by cryptanalysis. Rhouma et al. [9] cryptanalyzed a hyper chaos based image encryption technique proposed by T. Gao and Z. Chen in [10], this technique uses logistic map to scramble the pixel position and masks the pixel value by Chen's hyper chaotic system. For each round the one time generated key stream is used to encrypt image. Chosen-plain text and chosen- cipher text attack revealed the ciphered information of Chen's algorithm. Chengqing Li et al. [11] studied and explored weakness of an image encryption scheme based on a compound chaotic sequence by [12]. The compound chaotic sequence does not have randomness, by iterating the compound chaotic sequence the pseudo random numbers are generated. Generated keys are repeated more than single round for encryption process causes weakness of keys. The chosen plain text attack exposes the encrypted information. David Arroyo et al. [13] explored weakness of an image encryption technique by [14]. In this method permutation stage row and column permutations were performed to shuffle the pixel position and substitution block pixel values modified by masking with the generated key sequence. This haziness gives the low sensitivity to variation of plain image performed by this technique. Chengqing Li et al. [15] examined and discovered the defects of the encryption technique proposed by [16]. It has flexibility to expose due to secret keys and keys be determined by the plain image via chosen plain text attack the cipher information is taken out. The above stated algorithms fail to endure against chosen plain text and chosen cipher text attack. The cryptanalytic result shows that they have security defects. Due to the strong correlation between the image pixels only permutation of their position will not give the required levels of security. To obtain a robust encryption scheme we need to confuse and diffuse the position and intensity value of the pixels respectively.

The hybrid1D chaotic system is denoted as Logistic-Tent system, Logistic-Sine system and Tent-Sine system. The use of hybrid 1D system generates the different chaotic sequences. When any one of the seed map is out of the chaotic range, then generated sequence is chaotic due to hybrid chaotic system. To analyze and overcome the problems of 1D chaotic maps and

security analysis of the chaos based image encryption the hybrid chaotic system is used in this encryption algorithm. To demonstrate the security analysis a chaos based permutation-diffusion image encryption is proposed, which has the excellent permutation and diffusion properties to resist the different attacks, particularly chosen-plain text attacks. Parametric switching based PO generation is more random than using single chaotic map based random sequence generation. While applying this encryption algorithm to plain image at each round the diffusion bits are updated. This diffusion bits updating produces the different cipher images for each round. This confirms that the proposed algorithm able to resists the differential attack. This rest of the paper is organized as follows section 2 explains about the proposed permutation – diffusion encryption scheme in detail. Section 3 deals with the simulation results of the proposed scheme and section 4 conclusion.

2. PROPOSED METHOD

In this section a simple and effective technique for image encryption using chaotic map is introduced. This algorithm encrypts the image by typical permutation – diffusion architecture shown in Fig.1. Key generation process increases the security of the algorithm and diffusion bits updation protects algorithm from various attacks.

2.1 CHAOTIC MAP

Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions-an effect which is commonly referred to as the butterfly effect. Small changes in initial conditions cause widely deviating results for such dynamical systems, rendering long-term prediction difficult in common. Chaotic functions have mainly used to develop mathematical models of nonlinear systems. The chaos based image encryption uses one-dimensional (1D) chaotic maps logistic, tent, sine, etc. and multi-dimensional (MD) chaotic maps baker, cat map, etc. The use of multi-dimensional chaotic maps increases the security of the encryption algorithm due its complex structure and also presence of multiple parameters it leads to increase difficulty in implementation of the algorithm in hardware and software. The simple form of 1D chaotic map is easy to use in chaotic image encryption and they have problems in the continuous chaotic behavior (i.e.) only in the limited range all the 1D system produces the chaotic behavior. For the small number of iterations chaotic behavior is not good due to transient effect. For some parametric value 1D system produced chaotic sequence is non-uniform.

The logistic map, tent map and sine map were analyzed and their behaviors are discussed. The logistic map is one of the popular 1D chaotic map [13]. The mathematical expression of logistic map is given by following equation:

$$x_{n+1} = rx_n(1-x_n) \tag{1}$$

where, r is a parameter with the range of 0 to 4 and x_n is the output of chaotic sequence. Its chaotic range is limited only within [3.57, 4]. The chaotic sequence of the logistic map can be periodic if r is in small and also these values can be repeatable, this region is called the periodic region. The parameter value is above the 3.5699456 it behaves as a chaotic. Even in this range some parameters which make the logistic map to have a non-chaotic behavior is confirmed by the blank zone in its bifurcation diagram.

Tent map is known as its tent like shape in the graph of its bifurcation diagram. For certain parameter values, the tent map undergo stretching and folding transformations and displays sensitivity to initial conditions and periodicity.

It can be expressed by the following equation:

$$x_{n+1} = \begin{cases} ux_n/2 & x_i < 0.5 \\ u(1-x_n)/2 & x_i \geq 0.5 \end{cases} \tag{2}$$

where, u is the parameter within the range [0, 2].

The sine map is same as that of the logistic map chaotic behavior. It can be defined by following equation:

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

where, parameter a is in the range of (0 to 4).

Y Zhou et al. [17] proposed a chaos based system of Logistic, Sine, Tent chaotic maps combined together to form three 1D chaotic systems as hybrid form. This hybrid form of chaotic map produced the chaotic sequence in uniform manner. This 1D chaotic system improves the randomness. The hybrid1D chaotic system is denoted as Logistic-Tent system, Logistic-Sine system and Tent-Sine system. The logistic-tent system can be expressed in Eq.(4), Eq.(5) is the Logistic-sine system and Eq.(6) Tent-Sine system are given by,

$$x_{n+1} = \begin{cases} \left(rx_n(1-x_n)+(4-r)x_n/2\right)\bmod 1 & x_i < 0.5 \\ \left(rx_n(1-x_n)+(4-r)(1-x_n)/2\right)\bmod 1 & x_i \geq 0.5 \end{cases} \tag{4}$$

$$x_{n+1} = \left(rx_n(1-x_n)+(4-r)\sin(\pi x_n)/4\right)\bmod 1 \tag{5}$$

$$x_{n+1} = \begin{cases} \left(rx_n/2+(4-r)\sin(\pi x_n)/4\right)\bmod 1 & x_i < 0.5 \\ \left(rx_n(1-x_n)/2+(4-r)\sin(\pi x_n)/4\right)\bmod 1 & x_i \geq 0.5 \end{cases} \tag{6}$$

In these systems the chaotic maps are the seed maps used to produce complex chaotic behavior. Due to the presence of combinations of two chaotic maps leads to wide range of chaotic behavior of any parametric value.

The proposed encryption algorithm has two stages as permutation and diffusion. In the permutation stage the pixel positions are modified and in the diffusion stage the pixel values are modified. This method performs the permutation and diffusion in bit level. In the permutation process the plain image pixel bits are scrambled based on the generated permutation order. The bit level permutation slightly modifies the pixel intensity value. In the diffusion process the randomly generated bits are masked with the permuted pixel bits. A key generation process is introduced to improve the key security of the encryption algorithm. This process is repeated for number of rounds to avoid the attacks form the unauthorized persons. This encryption algorithm repeated for four rounds to achieve the highly secured cipher image.

2.1.1 Key Generation Process:

In the key generation process external keys (K_1, K_2, K_3 and K_4) are given to the key generator. The Logistic-Tent system (LT) iterated for hundred iterations and the final resultant value of the LT system masked with the neighboring keys shown in

Fig.2 and the resultant value feed to the next stage of LT system, this process is repeated for 3 stages. This key generation process breaks the relationship between the external key and the secondary keys (PK_1, PK_2, PK_3 and PK_4). Using these secondary keys the Permutation Order (PO) and Diffusion Bits (DFB) were generated. The chaotic system is very sensitive to its initial conditions, so small change in external keys will diverge large in the secondary key value.

2.1.2 Permutation Order Generator:

In the Permutation Order Generator the secondary keys C_i is feed to the control system of the PO generator shown in Fig.3. The Logistic-Sine system (LS) acts as a control system to generate a new chaotic sequence. Based on the LS system value either logistic or sine map generates the next random value as parametric switching. Using this parametric switching generated chaotic sequence has more randomness than the single chaotic system produced sequence. The Y_i is the initial condition for logistic or sine system. C_i is the combination of PK_1 and PK_2 and Y_i is the combination of PK_3 and PK_4. The permutation sequence will be generated by iterating the permutation order generator according to the pixel size requirement. The plain image is converted into binary sequence. Using the generated permutation sequence the pixel bits are scrambled.

2.1.3 Diffusion Bit Generator:

The secondary keys are feed one by one to the tent and sine system according to rounds shown in Fig.4. For round one the first secondary key is given to tent and sine system and it is iterated according to size of pixel in bits. PK_i is the i^{th} round secondary key; in each round the secondary key is updated. The output of sine and tent map values are compared using Eq.(7) and it produces the random binary sequence. In the diffusion process the shuffled image pixel bits are masked with the random binary sequence generated by DFB. Result of the sine and tent chaotic system compared by the following equation:

$$DFB_i = \begin{cases} DFB = 0 & if \;\; Tent > Sine \\ DFB = 1 & elsewhere \end{cases} \quad (7)$$

For each round the one secondary key is seed to the Diffusion Bit generator, this type of seed produces the different diffusion bits for each round. This DFB generation will resist the chosen plain text attack.

2.1.4 Encryption Algorithm:

The proposed encryption algorithm has the following steps to get the uncorrelated cipher image.

Step 1: The external keys (K_1, K_2, K_3 and K_4) are fed into the key generator to produce the secondary keys (PK_1, PK_2, PK_3 and PK_4) plain image is converted to binary form of $N \times M \times 8$ length.

Step 2: Feeding secondary key to the permutation order generator (PO). The permutation sequence will be generated by using the permutation sequence the pixel bits are shuffled.

Step 3: For i^{th} round the secondary key feed as the initial condition for Tent and Sine chaotic system. The system iterated for length of the shuffled binary sequence to generate the diffusion bits (DFB).

Step 4: Permuted image pixel bits are masked with the generated random bits and this will be repeated for four rounds. For each round the secondary key will be updated.

2.1.5 Decryption Algorithm:

In the decryption process is the reverse process of the encryption algorithm. The external keys are sent through the secured channel between the users. The same key generation is processed in retrieval side. The decrypted image is as original image without any lossless of original image information. The produced cipher image is secure against statistical and differential attacks. Experimental results are shown in section 3 simulation results.

3. SIMULATION RESULTS

To test the security of the image encryption algorithm various performance analysis such as security analysis, statistical analysis and differential analysis were performed. The randomness test performed to check the randomness of encrypted image using NIST test suite.The robustness and key sensitivity of the proposed scheme are demonstrated using MATLAB platform. Different size of images was used to test the proposed algorithm. Fig.5(a) is the plain image and its respective histogram. Results Fig.5(b), Fig.5(c), Fig.5(d), Fig.5(e) show the encrypted image and its histogram for each round. The proposed diffusion generator efficiently masks the information of the plain image and in first round itself the histogram of the encrypted image is very flat, there is no clue about its original image histogram. The attacker has no chance to predict the plain image.

3.1 SECURITY ANALYSIS

To prove security of encryption algorithm the secret key must have very sensitive to its variation and also the length of the key space should be greater than 2^{128} to avoid brute force attack. Security analysis shows the key space and its variation results.

Security Key Analysis: Security keys are very important to an encryption algorithm to make sure the safety protected images from various attacks and brute force attacks. Generally the security of an image encryption algorithm rest on its security key design [26]. For that a key generation process is used in this algorithm.

Key Space Analysis: The security key of the proposed algorithm is a combination of four external keys. In the key generation process shown in Fig.2 combine the keys and produce a resultant key this process repeated for three stages. The mixing of the key protects the keys form attack. The logistic-tent system is used to generate the secondary keys. There is no chance to predict the keys to break the algorithm because they could be decimal numbers with an arbitrary length.This key generation sets the length of the external key 60 bits each. Total key space this paper is 2^{240} it is greater than 2^{128} to avoid brute force and cipher text only attack.

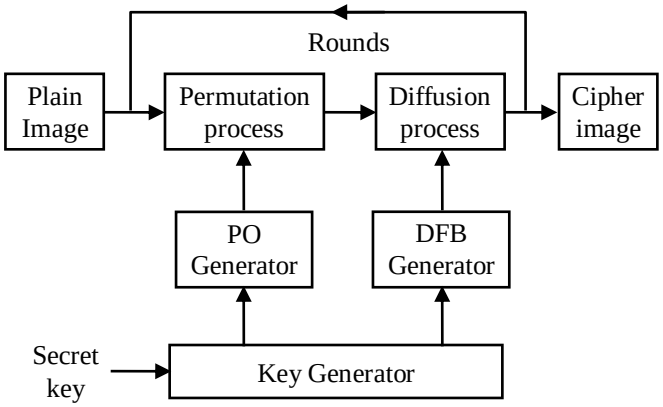


Fig.1. Proposed Encryption Technique

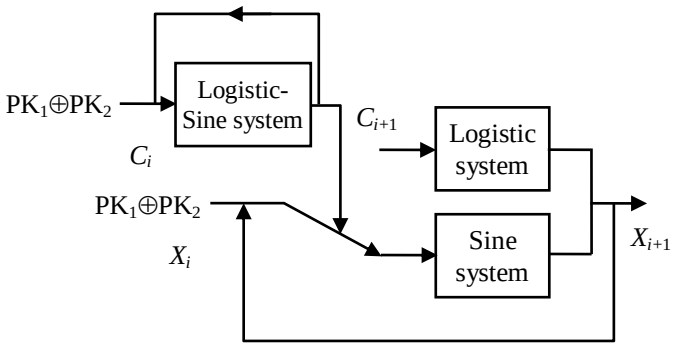


Fig.3. Permutation Order Generator

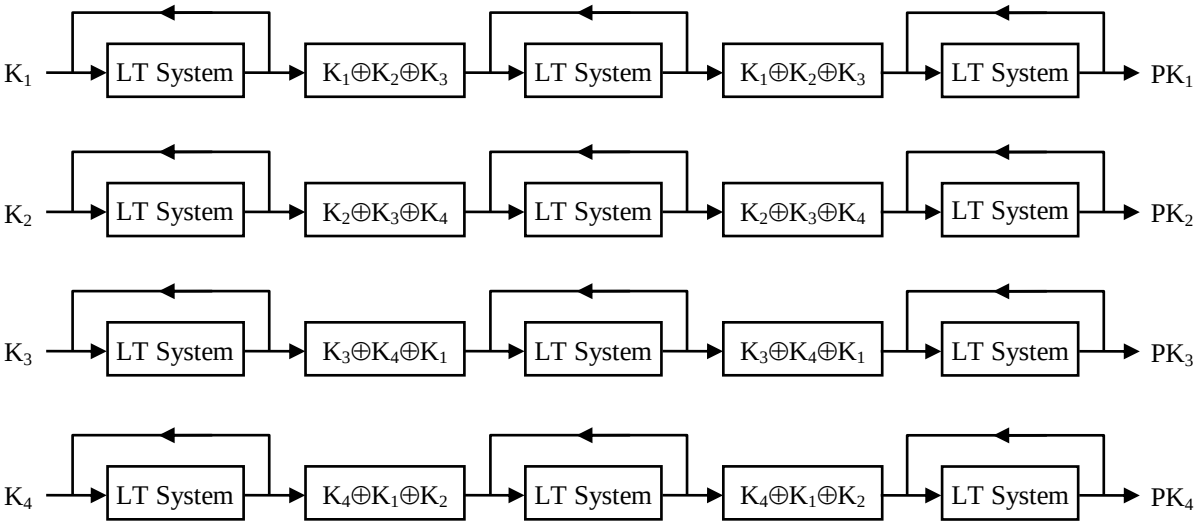


Fig.2. Key generator structure

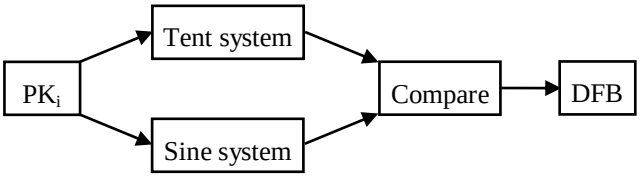


Fig.4. Diffusion Bit Generator

Key sensitivity: In the key generation process uses the 1D chaotic map. It is sensitive to its initial conditions if any small difference in the external key that highly deviate the generated secondary key. An encryption algorithm should be very sensitive to its secret key variations. Here, sensitivity analysis is performed to prove the key generation process is highly sensitive to its initial variations. Fig.6 shows encryption results using the initial secret key set and modified sets with a small change applied to each external secret key, respectively. In Fig.6(b) – Fig.6(e), all encrypted outcomes looks like noisy images with even spread histograms. Images in Fig.6(g) – Fig.6(j) are pixel-to-pixel differences between two encrypted images obtained by the initial and modified secret key sets. These results prove that a little variation in any secret key will lead to a completely different encryption results.

3.2 STATISTICAL ANALYSIS

An effective encryption algorithm should be very strong against statistical attack. To prove the toughness of the proposed image encryption technique, statistical analyses have been executed on encrypted image to determine its greater confusion and diffusion properties which powerfully resist statistical attacks. This is exposed by computing the histogram, the information entropy and the correlation analysis of the encrypted image.

Histogram Analysis: An image histogram is a graphical representation of the tonal (pixel intensity value) distribution in a digital image. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The histogram of several original images is widely different. Fig.5(b) – Fig.5(e) shows the encrypted images at different rounds and their histograms and Fig.6(f) encrypted image at initial set of key and its histogram. Fig.6(b) – Fig.6(e) shows the encrypted image and its respective histograms with the variation in its initial secret key. The histogram distributions of all encrypted images are flat. This analysis proves that there is no chance for statistical attacks on the proposed scheme.

Correlation Coefficient Analysis: Correlation between the pixels of the image (Elaine) must also be to check the robustness against the statistical attacks. To be a best encryption scheme the correlation between the pixels must be zero. This analysis shows the correlation between the randomly selected pairs of both plain image and encrypted image. This analysis carried out by following the procedures, Randomly 5,000 pairs are selected and they are selected like horizontally, vertically and diagonally adjacent. The correlation is calculated by the following equations,

$$r_{xy} = \frac{E\{[x - E(x)][y - E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}} \quad (8)$$

$$E(x) = \frac{1}{s}\sum_{i=1}^{s} x_i \quad (9)$$

$$D(x) = \frac{1}{s}\sum_{i=1}^{s} [x_i - E(x)]^2 \quad (10)$$

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. R_{xy} is the correlation between the adjacent pixels. The correlation co-efficient value is 1 means the image is plain image the correlation between the adjacent pixels are not broken. The value is -1 means that the image is the exact negative of the plain image. The value is 0 means the correlation between the pixels are broken. For the encrpted image ideal correlation co-efficient value is 0.

The Table.1 shows the correlation coefficient of the plain and encrypted image (Elaine) in horizontal, vertical and diagonal direction. It is compared with the various encryption techniques. The plain image values are nearly equal to 1 because the correlation between the adjacent pixels is high. The encrypted image values are approximately 0. So the encrypted image is highly uncorrelated. Fig.7 shows the correlation plots of plain and encrypted image in horizontal, vertical and diagonal direction. Encrypted image correlation plot displays the correlation between neighbouring pixels were broken.

Information Entropy Analysis: In Information Theory, information entropy is the most important feature of randomness. To calculate the entropy $H(m)$ of a source, we have,

$$H(m) = -\sum_{i=0}^{2^{N-1}} P(m_i)\log_2 P(m_i) \quad (11)$$

where, $P(m_i)$ represents the probability of symbol m. For a truly ran-dom source emitting 2^n symbols, the entropy is $H(m) = m$. Thus, the entropy should ideally be $H(s) = 8$ for an encrypted image with 256 gray levels, which shows that the information is random. Hence the information entropy of the encrypted image should be close to 8. The closer it gets to 8, the less possible for the cryptosystem to divulge information. Hence the proposed algorithm is robust against entropy attacks. In our algorithm the entropy value is approximately (average entropy = 7.9974) equal to 8. Table.2 shows the information entropies of the various images.

Differential Attack: To resist differential attack, a minor alternation plain image should cause a substantial change in the encrypted image. The NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are commonly used to calculate sensitivity to plain image and secret key. They are given by the following equations,

$$NPCR = \frac{1}{n}\left\|\{i | x_i \neq y_i, i = 0,1,....n-1\}\right\| \quad (12)$$

$$UACI = \frac{1}{n}\sum_{i}^{n-1}\frac{|x_i - y_i|}{255} \quad (13)$$

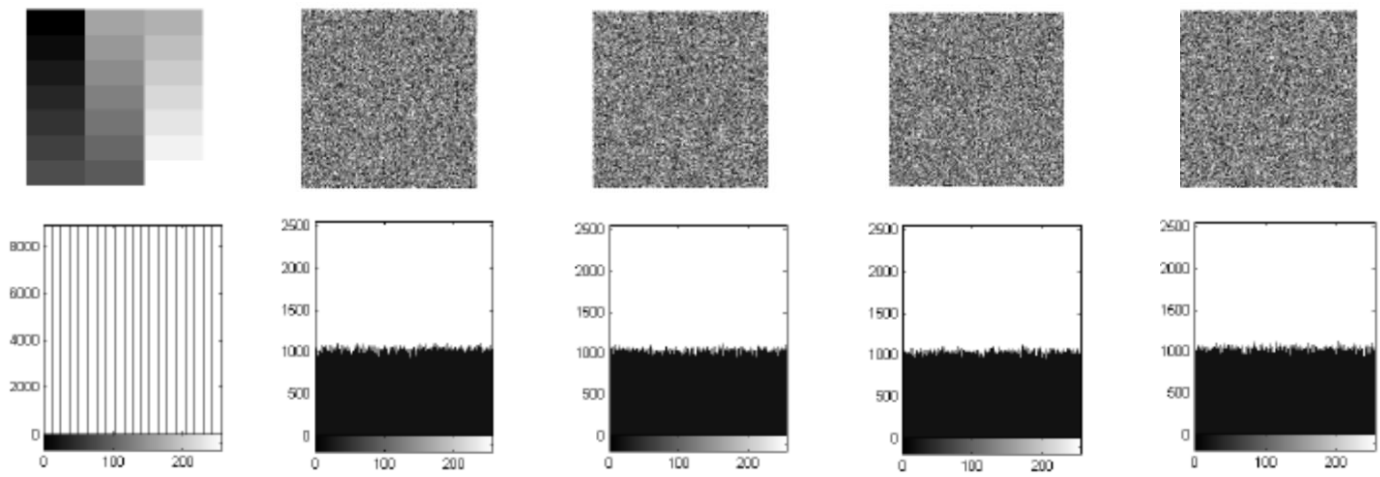
Given two images $x = \{x_0, x_1,... x_{n-1}\}$ and $y = \{y_0, y_1,... y_{n-1}\}$, the NPCR and UACI are defined as Eq.(12) and Eq.(13) [19]. For two random images, the average NPCR is about 0.9961, and the average UACI is about 0.3346 [20]. The NPCR and UACI values for various images calculated and 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 [24], the Number of Bit Change Rate (NBCR) is to measure the SAC performance using Eq.(14). The NBCR calculates the percentage of changed bit numbers between two bit streams. The ideal NBCR is 50% in average [25]:

$$NBCR = \frac{H_m[s_1, s_2]}{L_b} \times 100 \quad (14)$$

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.

From Table.2 it clearly shows that the NPCR and UACI values average of 0.9960 and 0.3341. For the security purpose maximum 4 rounds the proposed algorithm performed. The NPCR of our scheme can reach 99.61% in the first round.



(a) (b) (c) (d) (e)

Fig.5. Image and its respective histograms: (a). Original Image (b). Encrypted Image at Round one (c). Encrypted Image at Round two (d). Encrypted Image at Round three (e). Encrypted Image at Round four

This indicates the cryptosystem is very sensitive to even a 1-bit modification in the plain image. The proposed algorithm performed on various image files to test security, differential and entropy analysis [22].

Chosen plain text attack: An image encryption technique with the excellent diffusion property is able to resist the chosen-plaintext attack. However, when several existing image encryption algorithm uses the same security keys to encrypt a plain image, their encrypted images are duplicate. This security flaw provides the chance for attackers to break the encryption techniques using the chosen-plaintext attack. To state this problem, proposed image encryption algorithm for every round the diffusion bits are updated. It gives the encryption algorithm to generate a totally different encrypted image each time when encryption is applied to the same original image with the same set of secret keys.

Randomness test with sp800-22 test suite: NIST recommends two strategies to perform the analysis of the generator. 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.(15). 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:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - N/10)}{N/10} \tag{15}$$

where, F_i is the number of occurrences that the P–value is in the i^{th} interval and N denotes the sample size (N = 100). The P–value of the P–values is calculated using Eq.(16).

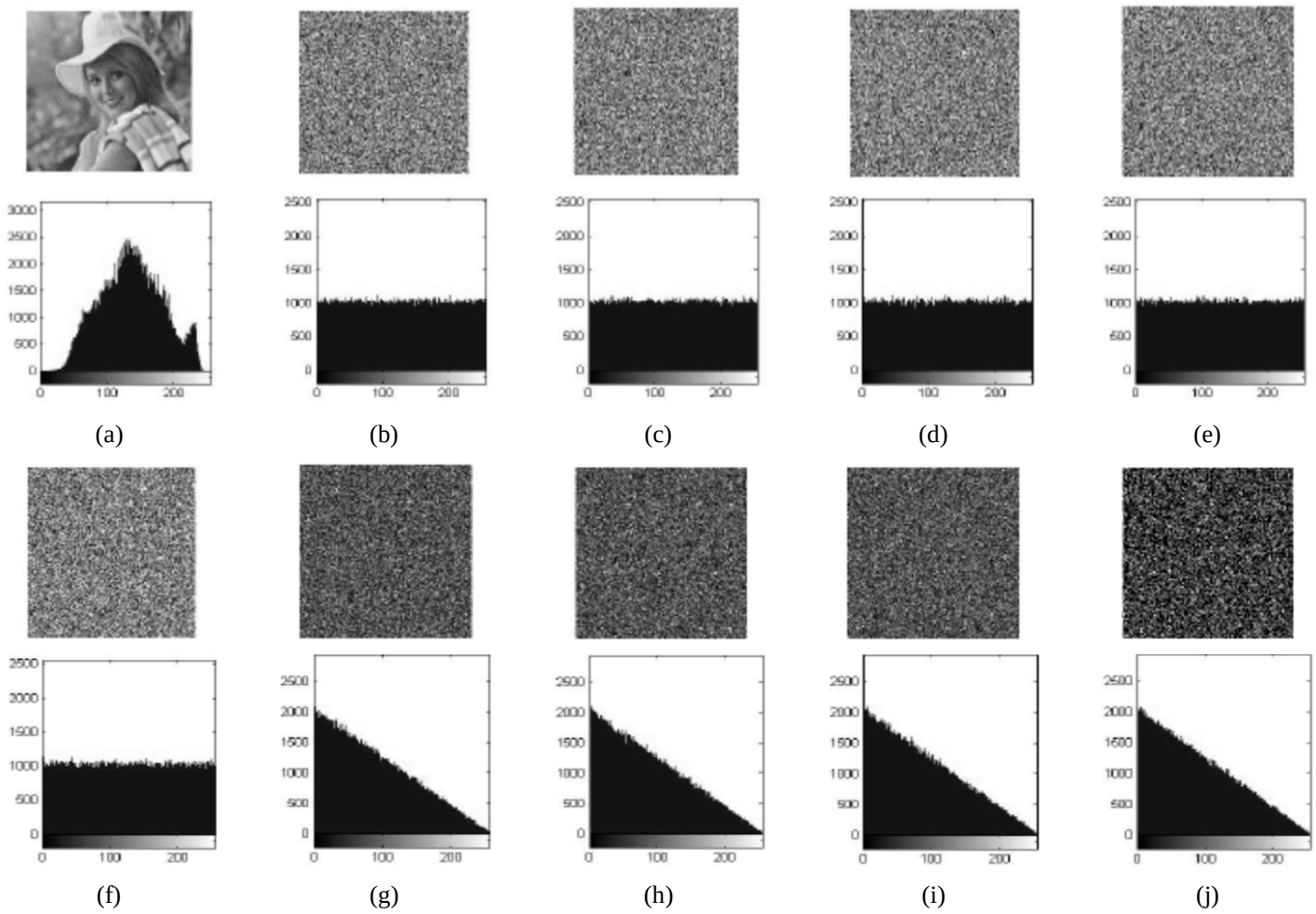
$$P-value = igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right) \tag{16}$$

where, *igamc* is the incomplete Gamma function [21]. If P–values are greater than or equal to 0.0001 then the 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.

4. CONCLUSION

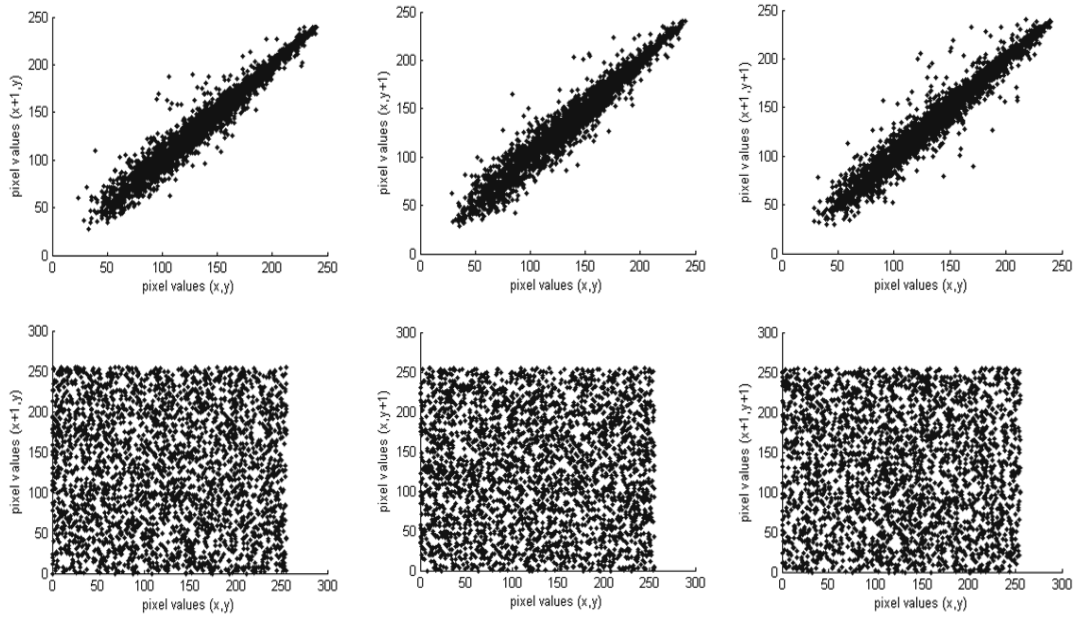
In the proposed method a new key generation process is used to generate the secondary key, which improves the security of the cipher image. This encryption algorithm is based on the combination of three chaotic maps. The maps are initialized by external keys. The bit level permutation and diffusion process are performed here for every round. The secondary key updated in the diffusion bit generator for each round 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.



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

Fig.6(a). Plain image and its histogram (b-e). Encrypted image with slight modification in external keys 1st, 2nd, 3rd, 4th and its histograms (f). Encrypted image of the plain image with the initial set of keys (g-j). Pixel to pixel difference between encrypted image with initial set of key and key modified encrypted image and their respective histograms



(a) (b) (c)

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

Table.1. Correlation coefficients

Encryption Technique	Horizontal	Vertical	Diagonal
Plain image	0.9741	0.9731	0.9704
Proposed method	-0.0094	-0.0003	0.0039
Chen's [6]	0.9728	0.0442	0.0469
AES [23]	0.8018	-0.0160	-0.0140

Table.2. Entropy and differential analysis

File name	Information entropy analysis		Differential Analysis		SAC
	Plain image	Cipher image	NPCR	UACI	NBCR
5.1.09	6.7093	7.9975	0.9963	0.3346	50.0711
5.1.10	7.3118	7.9972	0.9965	0.3365	50.1093
5.1.12	6.7057	7.9975	0.9962	0.3350	50.0917
5.1.13	1.5483	7.9965	0.9963	0.3377	50.0423
5.1.14	7.3424	7.9977	0.9962	0.3321	50.0558
5.2.08	7.5237	7.9991	0.9961	0.3331	49.9692
File name	**Information entropy Analysis**		**Differential Analysis**		**SAC**
	Plain image	**Cipher image**	**NPCR**	**UACI**	**NBCR**
5.2.10	5.7056	7.9991	0.9961	0.3331	50.0538
5.3.01	7.5237	7.9998	0.9960	0.3342	49.9825
5.3.02	6.8303	7.9996	0.9962	0.3329	50.0143
7.1.01	6.0274	7.9996	0.9959	0.3325	50.0728
7.1.02	4.0045	7.9992	0.9962	0.3353	49.9739
7.1.03	5.4957	7.9993	0.9953	0.3329	50.0153
7.1.04	6.1074	7.9992	0.9952	0.3331	50.0100
7.1.05	6.5632	7.9995	0.9959	0.3323	49.9802
7.1.06	6.6953	7.9996	0.9962	0.3332	49.9709
7.1.07	5.9916	7.9994	0.9960	0.3325	49.9906
7.1.08	5.0534	7.9992	0.9956	0.3326	50.0205
7.1.09	6.1898	7.9996	0.9966	0.3336	50.0559
7.1.10	5.9088	7.9991	0.9962	0.3333	49.9508
7.2.01	5.6415	7.9996	0.9959	0.3358	50.0001
Boat.512	7.1914	7.9995	0.9961	0.3342	49.9736
Elaine.512	7.5060	7.9998	0.9961	0.3336	49.9609
Gray21.512	4.3923	7.9996	0.9961	0.3338	50.0303
Numbers.512	7.7292	7.9993	0.9960	0.3337	50.0136
Ruler.512	0.5000	7.9997	0.9961	0.3376	49.9592
Testpat.1k	4.4077	7.9996	0.9962	0.3339	50.0125
mean	5.9304	7.9989	0.9960	0.3341	50.0133

Table.3. Randomness Test

Statistical test		P value	Result
Frequency		0.8391	Success
Block frequency		0.2460	Success
Runs		0.6990	Success
Statistical test		P value	Result
Long runs of one's		0.4855	Success
Binary Matrix Rank		1.0000	Success
Spectral DFT		0.2185	Success
No overlapping templates		0.9960	Success
Overlapping templates		0.2553	Success
Universal		0.9985	Success
Serial	P value1	0.9427	Success
	P value2	0.3810	Success
Approximate entropy		0.1495	Success
Cumulative sums		0.7598	Success
Random excursions		0.1301	Success
Random excursions variant		0.6019	Success

REFERENCES

[1] Bruce Schneier, "*Applied Cryptography Protocols: Algorithms and Source code in C*", Second Edition, Wiley, 1996.

[2] William Stallings, "*Cryptography and Network Security: Principles and Practice*", Fifth Edition, Prentice Hall 2010.

[3] Gonzalo Alvarez and Shujun Li, "Some basic cryptographic requirements for chaos-based cryptosystems", *International Journal of Bifurcation and Chaos*, Vol. 16, No. 8, pp. 2129-2151, 2006.

[4] Shiguo Lian, Jinsheng Sun and Zhiquan 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.

[5] 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. 515, pp. 2645-2652, 2008.

[6] Guanrong Chen, Yaobin Mao and Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons & Fractals*, Vol. 21, No. 3, pp. 749-761, 2004.

[7] Zhi-Hong Guan, Fangjun Huang and Wenjie Guan, "Chaos-based image encryption algorithm", *Physics Letters A*, Vol. 346, No. 1-3, pp. 153-157, 2005.

[8] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Tao Xiang and Guanrong Chen, "A chaos-based image encryption algorithm with variable control parameters", *Chaos, Solitons & Fractals*, Vol. 41, No. 4, pp. 1773-1783, 2009.

[9] Rhouma Rhouma and Safya Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos", *Physics Letters A*, Vol. 372, No. 38, pp. 5973-5978, 2008.

[10] Tiegang Gao and Zengqiang Chen, "A new image encryption algorithm based on hyper-chaos", *Physics Letters A*, Vol. 372, No. 4, pp. 394-400, 2008.

[11] Chengqing Li, Shujun Li, Guanrong Chen and Wolfgang A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence", *Image and Vision Computing*, Vol. 27, No. 8, pp. 1035-1039, 2009.

[12] Xiaojun Tong and Minggen Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically", *Image and Vision Computing*, Vol. 26, No. 6, pp. 843-850, 2008.

[13] David Arroyo, Jesus Diaz and F.B. Rodriguez, "Cryptanalysis of a one round chaos-based Substitution Permutation Network", *Signal Processing*, Vol. 93, No. 5, pp. 1358-1364, 2013.

[14] 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.

[15] Chengqing Li, Shujun Li and Kwok-Tung Lo, "Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 16, No. 2, pp. 837-843, 2011.

[16] Patidar Vinod, Pareek N.K and Sud K.K, "Modified substitution–diffusion image cipher using chaotic standard and logistic maps", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 14, No. 7, pp. 2755-2765, 2009.

[17] Yicong Zhou, Long Bao and C.L. Philip Chen, "A new 1D chaotic system for image encryption", *Signal processing*, Vol. 97, pp. 172-182, 2014.

[18] 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.

[19] Guo Chen, Yong Chen and Xiaofeng Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps", *Chaos, Solitons & Fractals*, Vol. 31, No. 3, pp. 571-9, 2007.

[20] H.S. Kwok and Wallace K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", *Chaos, Solitons & Fractals*, Vol. 32, No. 4, pp. 1518-1529, 2007.

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

[22] The USC- SIPI Image Database, http://sipi.usc.edu/database/database.php.

[23] Jorg J. Buchholz, "*Matlab implementation of the Advanced Encryption Standard*", 2001.

[24] R. Forre, "*The strict avalanche criterion: spectral properties of Boolean functions and an extended definition*", 1990.

[25] Julio Cesar Hernandez Castro, Jose Maria Sierra, Andre Seznec, Antonio Izquierdo and Arturo Ribagorda, "The strict avalanche criterion randomness test", *Mathematics and Computers in Simulation*, Vol. 68, No. 1, pp. 1-7, 2005.

[26] Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1997.