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

R. Ranjith Kumar¹, B. Saranraj² and S. Pradeep³
Department of Electronics and Communication Engineering, P.A. College of
Engineering and Technology, India
E-mail: 'rранjithkumar7@gmail.com, 'saranraj2011@gmail.com, '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,
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 Francoise 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 permuted 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),

\[
\text{CO} = \text{indices } \{X_i (\text{logistic}) \ast 1014 \text{ mod } N\} \quad (1)
\]

where, \(X_i (\text{logistic})\) 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.

\[
\text{Node value } = \begin{cases} 1 & \text{if } \text{Map } 1 \geq \text{Map } 2 \\ 0 & \text{else} \end{cases} \quad (3)
\]

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,

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 \(L^{0.5} > 2^{128}\) and to avoid the success of brute-force attacks, the minimum number of rounds \(R\) can be obtained from the relation [9],

\[
R = \lceil\frac{128}{\log_2 L}\rceil + 1 \quad (4)
\]

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,

\[
\text{cov}(x,y) = \text{E}\{ (x-\text{E}(x))(y-\text{E}(y)) \} 
\]

\[
\rho_{xy} = \frac{\text{cov}(x,y)}{\sqrt{\text{D}(x)\text{D}(y)}}
\]

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](a) Plain Image. (b) Cipher Image. (c) Histogram of Plain Image. (d) Histogram of Cipher Image. (e) Horizontal direction. (f) Vertical direction. (g) 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,

\[
H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)}
\]

(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.

\[
NPCR = \frac{1}{n} \sum_{i=0}^{n-1} |x_i \neq y_i, i = 0,1,...,n-1|
\]

(8)

\[
UACI = \frac{1}{n} \sum_{i=0}^{n-1} \frac{|x_i - y_i|}{255}
\]

(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:

\[
MAE = \frac{1}{M \times N} \sum_{j=0}^{N} \sum_{i=0}^{M} |C(i, j) - P(i, j)|
\]

(10)

The larger the MAE value, the better the encryption security.

**NBCR (Number of Bit Change Rate):** The 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]:

\[
NBCR = \frac{H_m[|s_1,s_2|]}{L_h} \times 100
\]

(11)

where \(s_1\) and \(s_2\) are two bit streams with the bit length of \(L_h\). 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

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

R RANJITH KUMAR et al.: A NEW ONE ROUND IMAGE ENCRYPTION ALGORITHM BASED ON MULTIPLE CHAOTIC SYSTEMS
Table 2. Entropy and differential analysis (Images from SIPI database)

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>IMAGE</th>
<th>ENTROPY</th>
<th>NPCR</th>
<th>UACI</th>
<th>NBCR</th>
<th>MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Plain</td>
<td>Cipher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Leopard</td>
<td>6.5264</td>
<td>7.9975</td>
<td>0.9965</td>
<td>0.3354</td>
<td>49.9426</td>
</tr>
<tr>
<td>2</td>
<td>Aerial</td>
<td>7.3118</td>
<td>7.9973</td>
<td>0.9958</td>
<td>0.3360</td>
<td>50.0277</td>
</tr>
<tr>
<td>3</td>
<td>Airplane</td>
<td>6.4523</td>
<td>7.9973</td>
<td>0.9963</td>
<td>0.3363</td>
<td>50.1944</td>
</tr>
<tr>
<td>4</td>
<td>Airport</td>
<td>6.6955</td>
<td>7.9968</td>
<td>0.9963</td>
<td>0.3366</td>
<td>50.0544</td>
</tr>
<tr>
<td>5</td>
<td>baboon</td>
<td>7.3903</td>
<td>7.9580</td>
<td>0.9956</td>
<td>0.3365</td>
<td>50.0357</td>
</tr>
<tr>
<td>6</td>
<td>Barbara</td>
<td>7.5838</td>
<td>7.9968</td>
<td>0.9962</td>
<td>0.3360</td>
<td>49.9090</td>
</tr>
<tr>
<td>7</td>
<td>Boat</td>
<td>7.1583</td>
<td>7.9976</td>
<td>0.9960</td>
<td>0.3364</td>
<td>50.0048</td>
</tr>
<tr>
<td>8</td>
<td>Cameraman</td>
<td>7.0097</td>
<td>7.9970</td>
<td>0.9957</td>
<td>0.3355</td>
<td>50.0437</td>
</tr>
<tr>
<td>9</td>
<td>Car and APC</td>
<td>6.7718</td>
<td>7.9974</td>
<td>0.9962</td>
<td>0.3362</td>
<td>50.1215</td>
</tr>
<tr>
<td>10</td>
<td>Chemical plant</td>
<td>7.3424</td>
<td>7.9967</td>
<td>0.9960</td>
<td>0.3366</td>
<td>50.0357</td>
</tr>
<tr>
<td>11</td>
<td>Clock</td>
<td>6.7057</td>
<td>7.9973</td>
<td>0.9961</td>
<td>0.3350</td>
<td>50.0048</td>
</tr>
<tr>
<td>12</td>
<td>Couple</td>
<td>7.1720</td>
<td>7.9972</td>
<td>0.9959</td>
<td>0.3359</td>
<td>50.0605</td>
</tr>
<tr>
<td>13</td>
<td>Einsteen</td>
<td>6.8487</td>
<td>7.9971</td>
<td>0.9968</td>
<td>0.3352</td>
<td>49.9762</td>
</tr>
<tr>
<td>14</td>
<td>Lena</td>
<td>7.5683</td>
<td>7.9971</td>
<td>0.9963</td>
<td>0.3368</td>
<td>50.0788</td>
</tr>
<tr>
<td>15</td>
<td>Man</td>
<td>7.5360</td>
<td>7.9973</td>
<td>0.9962</td>
<td>0.9962</td>
<td>49.9876</td>
</tr>
<tr>
<td>16</td>
<td>Moon surface</td>
<td>6.7093</td>
<td>7.9972</td>
<td>0.9958</td>
<td>0.3366</td>
<td>49.9781</td>
</tr>
<tr>
<td>17</td>
<td>Peppers</td>
<td>7.5327</td>
<td>7.9967</td>
<td>0.9958</td>
<td>0.3368</td>
<td>50.0723</td>
</tr>
<tr>
<td>18</td>
<td>Resolution chart</td>
<td>1.5483</td>
<td>7.9959</td>
<td>0.9962</td>
<td>0.3358</td>
<td>50.0296</td>
</tr>
<tr>
<td>19</td>
<td>Stream and bridge</td>
<td>7.6682</td>
<td>7.9972</td>
<td>0.9965</td>
<td>0.3335</td>
<td>49.9922</td>
</tr>
<tr>
<td>20</td>
<td>Tank</td>
<td>6.4473</td>
<td>7.9969</td>
<td>0.9960</td>
<td>0.3365</td>
<td>50.0311</td>
</tr>
<tr>
<td>21</td>
<td>Truck and apc</td>
<td>7.0526</td>
<td>7.9966</td>
<td>0.9960</td>
<td>0.3364</td>
<td>49.9235</td>
</tr>
<tr>
<td>22</td>
<td>256 level test pattern</td>
<td>7.6695</td>
<td>7.9968</td>
<td>0.9961</td>
<td>0.3360</td>
<td>50.0864</td>
</tr>
<tr>
<td>23</td>
<td>Galaxy</td>
<td>5.6538</td>
<td>7.9974</td>
<td>0.9963</td>
<td>0.3360</td>
<td>50.1719</td>
</tr>
<tr>
<td>24</td>
<td>estatue</td>
<td>6.7807</td>
<td>7.9970</td>
<td>0.9957</td>
<td>0.3347</td>
<td>49.9891</td>
</tr>
<tr>
<td>25</td>
<td>All zeroes</td>
<td>0</td>
<td>7.9950</td>
<td>0.9961</td>
<td>0.3359</td>
<td>50.1023</td>
</tr>
</tbody>
</table>

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:

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

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),

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

where, \(\text{igamc}\) is the incomplete Gamma function [19]. If P-values 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.
Table 3. Randomness Test

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

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


