A Novel Image Encryption Approach using Matrix Reordering

T.SIVAKUMAR [1], AND R.VENKATESAN [2]
[1] Department of Information Technology, [2] Department of CSE
PSG College of Technology
Coimbatore, Tamilnadu - 641 004
INDIA
[1]msg2sk@hotmail.com [2]ramanvenkatesan@yahoo.com

Abstract: - Transmission and storage of multimedia data like audio, video, and images over the Internet has increased in today's digital communication. Among the different multimedia data, images are transmitted and used very often. It is essential to protect the multimedia data from unauthorized disclosure during transmit. A novel approach for encrypting digital images using Matrix Reordering (MR), a kind of scanning, and simple XOR operation is proposed in this paper. The MR is applied to permute the pixel positions and the XOR operation is done to diffuse the pixel values. The bitwise XOR operation is performed using pseudorandom numbers generated by the linear congruential method. The image encryption algorithm evaluation parameters such as histogram, correlation, cut test, dispersion test, visual testing, and speed test have been conducted using the suggested method, and the results are analyzed. The analysis shows that the proposed system is resistant to statistical and differential attacks, and could be used in real-time applications to provide confidentiality service for images with less computational overhead.

Key-Words: - Information Security, Image Encryption, Matrix Reordering, Scan Pattern, Image Histogram, Image Correlation, Differential Attack.

1 Introduction

Information security has become a very critical aspect of modern computing systems to protect data from unauthorized access. Securing sensitive information has gained significant importance in the recent years, and security is an important issue in communication and storage. Approximately 20 million photos are viewed and 3,000 images are uploaded on Flickr per minute and 350 million photos are uploaded per day on Facebook. The security of digital images has become essential due to the rapid evolution of the Internet in the digital world and numerous image encryption methods have been proposed to secure digital images.

The conventional algorithms like Data Encryption Standard, International Data Encryption Algorithm, and Advanced Encryption Standard have certain limitations in multimedia data encryption and there is a need to develop specific encryption methods for multimedia data. Position change, value transformation and visual transformation are the different types of image encryption methods introduced by numerous researchers [2, 5, 8, 9, 13]. Chaos based image encryption using wavelet transforms, vector quantization, and random phase encoding for color image encryption are some of the existing image encryption algorithms available in the literature [1, 3, 6, 14]. The advantage of an image encryption over traditional text encryption is that the decrypted image is tolerant with small distortion due to human perception.

1.1 Scan Methodology

The image scanning is a formal language-based two-dimensional spatial-accessing methodology which could efficiently specify and generate a wide range of scanning paths or space filling curves. The scan based pixel permutation and block transformation is a widely used technique for image encryption [2, 8]. Algorithms used to encrypt text messages are not sufficient to encrypt images due to the reasons like (a) image size is always greater than text messages and (b) conventional algorithms take a long time to encrypt digital images.

The objective of this paper is to propose a novel image encryption method based on scan methodology and simple XOR operation. The scan path is derived from the concept of matrix reordering and the random bit stream to perform XOR operation is obtained using Linear Congruential Generator (LCG).

The rest of the paper is organized as follows. Section two reviews some existing image encryption methods. Section three presents the the proposed image encryption method. Section four and five provides the experimental results and result analysis. Section 6 gives the conclusion.

2 Related Works

Guodong Ye [1] presented an efficient image encryption scheme using double logistic maps, in which the digital matrix of the image is confused from row and column respectively. Confusion effect is carried out by the substitution stage and Chens system is employed to diffuse the gray value distribution. Haojiang Gao *et al.* [3] presented a Nonlinear Chaotic Algorithm (NCA) by using power and tangent functions instead of linear function. The encryption algorithm is a one-time-one-password system and is more secure than the DES algorithm. Jawahar Thakur *et al.* [4] presented a comparison between symmetric key algorithms such as DES, AES, and Blowfish. The parameters such as speed, block size, and key size are considered to evaluate the performance when different data loads are used. Blowfish has a better performance than other encryption algorithms and AES showed poor performance results compared to other algorithms due to more processing power.

Khaled Loukhaoukha *et al.* [5] introduced an image encryption algorithm based on Rubik’s cube principle. The original image is scrambled using the principle of Rubik’s cube and then XOR operator is applied to rows and columns of the scrambled image using two secret keys. Liu Hongjun *et al.* [6] designed a stream-cipher algorithm based on one-time keys and robust chaotic maps. The method uses a piecewise linear chaotic map as the generator of a pseudo-random key stream sequence.

M. Zeghid *et al.* [7]analyzed the AESalgorithm, and added a key stream generator (A5/1, W7) to AES to ensure improved encryption performance mainly for the images. The method overcomes the problem of textured zones existing in other known encryption algorithms. Maniccam *el al.* [8] presented a method for image and video encryption and the encryption methods are based on the SCAN methodology. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher. The pixel rearrangement is done by scanning keys and the pixel values are changed by substitution mechanism. Figure 1 shows the basic SCAN patterns used in [8].

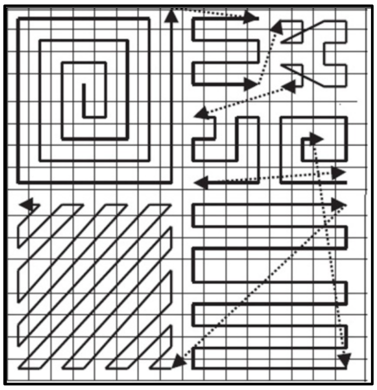


Fig.1 Existing basic SCAN patterns [8]

Mohammad Ali el al. [9] introduced a block-based transformation algorithm based on the combination of image transformation and the Blowfish algorithm. The algorithm resulted in the best performance by the lowest correlation and the highest entropy. The characteristics of AES are its security and resistance against attacks and the major characteristic of RC4 algorithm is its speed [10]. A hybrid cipher by combining the characteristics of AES and RC4 is developed and 20% improvement in speed is achieved when compared to the original AES and a higher security compared to the original RC4 [10].

Rizvi *et al.* [11] analyzed the security issues of two symmetric cryptographic algorithms Blowfish and CAST algorithm and then compared the efficiency for encrypting text, image, and audio with the AESalgorithm across different widely used Operating Systems. For text data, all algorithms run faster on Windows XP but Blowfish is the most efficient and CAST run slower than AES. Blowfish encrypts images most efficiently on all the three platforms. For audio files, CAST performs better than Blowfish and AES on Windows XP but on Windows Vista and Windows 7, there is no significant difference in the performance of CAST and AES; however, Blowfish encrypts audio files at less speed.

Sanfu Wang *et al.* [12] presented an image scrambling method based on folding transform to folding matrix which is orthogonal and enables to fold images either up-down or left-right. When an image is folded this way repeatedly, it becomes scrambled. The scrambling algorithm has an effective hiding ability with small computation burdens as well as wide adaptability to images with different scales.

Sathishkumar G.A *et al.* [13] presented a pixel shuffling, base 64 encoding based algorithm which is a combination of block permutation, pixel permutation, and value transformation. The crypto system uses a simple chaotic map for key generation and a logistic map was used to generate a pseudo random bit sequence. The total key length is 512 bits for each round and the key space is approximately 2512 for ten rounds. Shao Liping *et al.* [15] proposed a scrambling algorithm based on random shuffling strategy which could scramble non equilateral images and has a low cost to build coordinate shifting path. The algorithm is based on permuting pixel coordinates and it could be used to scramble or recover image in real time.

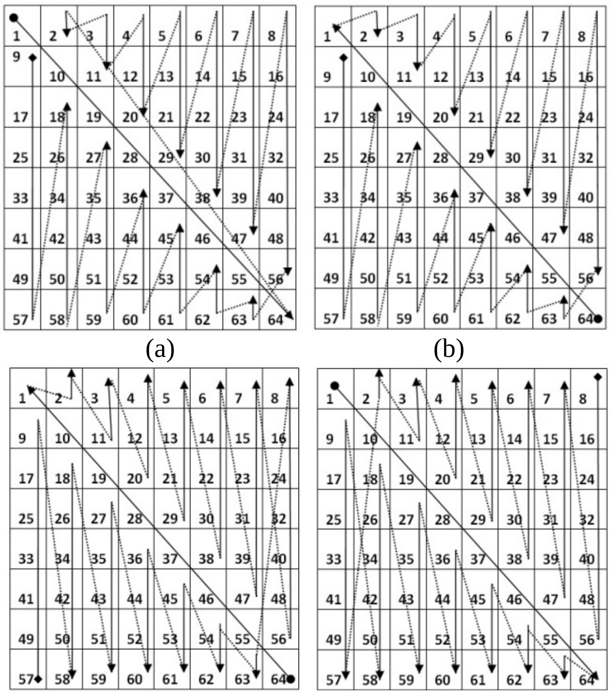
Shashi Mehrotra Seth *et al.* [16] performed comparative analysis of three algorithms such as DES, AES and RSA considering certain parameters such as computation time, memory usage and output byte using text files. The DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is minor in case of AES and DES. The RSA algorithm consumes the longest encryption time, memory usage is very high, and the output byte is the least.

Vishwagupta *et al.* [17] developed a cryptography algorithm based on the block cipher concept using XOR and shifting operations. The algorithm takes less time when compared to the existing symmetric algorithms such as DJSA and AES. To encrypt a text file of size 560 KB, the proposed method takes 0.28 ms, but the DJSA and AES algorithms take 0.37 ms and 0.35 ms, respectively. Xiaomin Wang *et al.* [19] presented an image scrambling method using Poker shuffle, which is controlled dynamically by chaotic system. The pixel positions are scrambled by shuffle sequences which are generated by a chaotic-controlled Poker shuffle process.

Thus, image encryption based on chaotic sequence, scan pattern, permutation, and pseudorandom numbers are applied by researchers in recent years. In this paper, matrix reordering concept is used as a scan methodology to permute the pixel positions of the plain image.

3 The Proposed Method

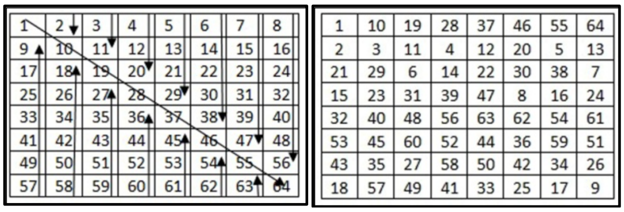
The reordering involves the graph or scarcity pattern of the matrix. By using the matrix reordering, the original image pixel positions are transformed with respect to a specific pattern which results in a scrambled image which is entirely different from the original image. Figure 2 illustrates the basic matrix reordering adopted in the proposed method to permute the pixel positions of a digital image.


(a) (b)

(c) (d)

Fig.2 Illustration of Matrix Reordering

In the proposed method, first, the Matrix Reordering (MR) is applied to the original image to shift the pixel positions. Then, the bitwise XOR operation is performed to diffuse the pixel values. Figure 3 shows the original matrix and its corresponding permuted matrix for three different scan modes (D: Diagonal, LD: Lower Diagonal, and UD: Upper Diagonal). Figures 3(a) – (c) show the original matrix and Figures 3(d) – (f) show the corresponding pixel permuted matrix. The advantage of proposed method is that the MR could be done without dividing the image into blocks and block transformation used in the paper [9]. The bitwise XOR operation is performed row wise using pseudorandom numbers generated by the linear congruential method.

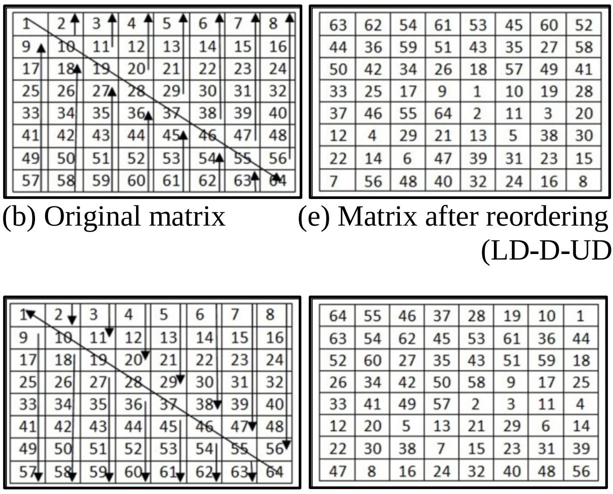


1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(a) Original matrix

1	10	19	28	37	46	55	64
2	3	11	4	12	20	5	13
21	29	6	14	22	30	38	7
15	23	31	39	47	8	16	24
32	40	48	56	63	62	54	61
53	45	60	52	44	36	59	51
43	35	27	58	50	42	34	26
18	57	49	41	33	25	17	9

(d) Matrix after reordering (D-UD-LD)



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Original matrix

63	62	54	61	53	45	60	52
44	36	59	51	43	35	27	58
50	42	34	26	18	57	49	41
33	25	17	9	1	10	19	28
37	46	55	64	2	11	3	20
12	4	29	21	13	5	38	30
22	14	6	47	39	31	23	15
7	56	48	40	32	24	16	8

(e) Matrix after reordering (LD-D-UD)

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(c) Original matrix

64	55	46	37	28	19	10	1
63	54	62	45	53	61	36	44
52	60	27	35	43	51	59	18
26	34	42	50	58	9	17	25
33	41	49	57	2	3	11	4
12	20	5	13	21	29	6	14
22	30	38	7	15	23	31	39
47	8	16	24	32	40	48	56

(f) Matrix after reordering (D-LD-UD)

Fig. 3 Proposed Matrix Reordering

The diagonal elements could be scanned either from the coordinate (1, 1) to (n, n) or from (n, n) to (1, 1). The upper diagonal elements could be accessed either from 2nd column to nth column or in the reverse direction. Similarly, the lower diagonal elements might be accessed either from the 1st column to (n-1)th column or (n-1)th column to 1stcolumn, where n is the column size of the input matrix. The column accessing principle can also be applied to rows for further scrambling. The working model of the proposed system is shown in Figure 4.

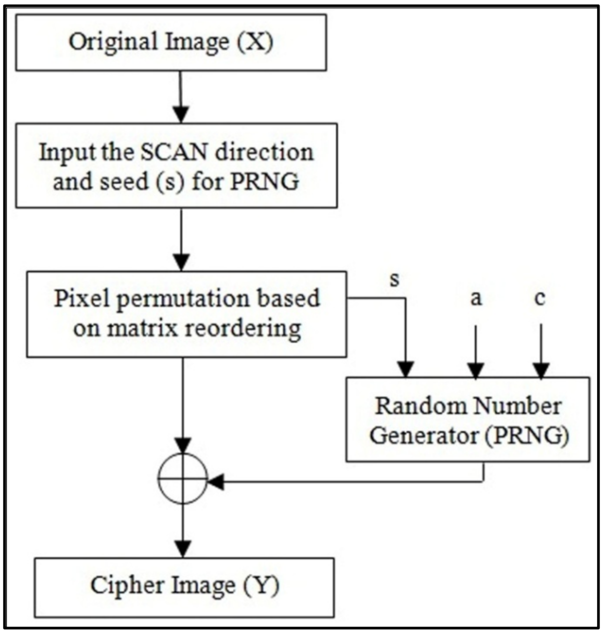

Original Image (X)
Input the SCAN direction and seed (s) for PRNG
Pixel permutation based on matrix reordering
s
a
c
Random Number Generator (PRNG)
Cipher Image (Y)

Fig.4 Block Diagram of Proposed Method

3.1 Pseudorandom Number Generator

The linear congruential generator is a widely used technique to generate pseudorandom numbers. The sequence of random numbers $\{X_n\}$ is obtained by the following iterative equation [18]:

$$\mathbf{X_{n+1} = (aX_n + c) \bmod m} \qquad (1)$$

Where, m is the modulus (m>0, chosen as 255), a is the multiplier, 0<a<m; c is the increment, 0≤c<m; and x_0 is the seed value, $0 \le x_0 < m$.

3.2 EncryptionFunction

Input**:** Plain image of size m x n, seed for random number generator

Output**:** Cipher image of size m x n

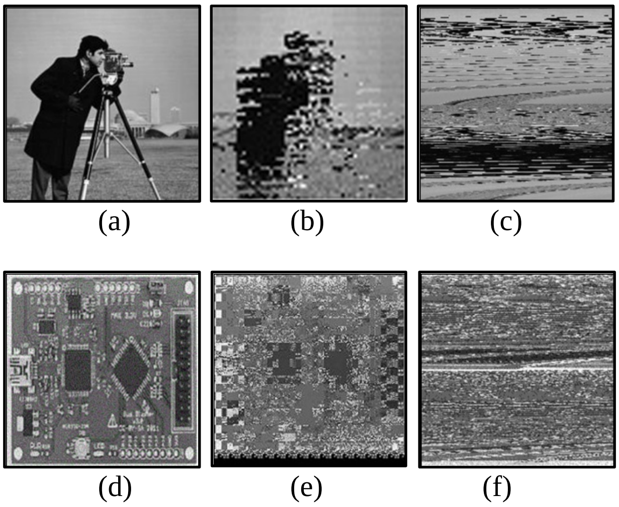
```
1. Let the image to be encrypted is the Original_image[m, n].
2. // to access diagonal elements
   For i varies from 1 to m
   For j varies from 1 to n
   (a) if (i equal to j) then assign
         Cipher_image1[p,q]←Original_image[i, j];
   (b) if(q equal to n) then assign q←1 and
         increment p;
         Else increment q;
3. // to access upper diagonal elements
   Repeat for i varies from 1 to m
   Repeat for j varies from 1 to n
   (a) if (i less than j) then assign
         Cipher_image1[p,q] ← original_image[j, i];
   (b) if(q equal to n) then assign q ← 1 and
         increment p;
         Else increment q;
4. // to access lower diagonal elements
   Repeat for i varies from n to 1
   Repeat for j varies from m to 1
   (a) if (i less than j) then assign
         Cipher_image1[p, q]←original_image[j, i];
   (b) if(q equal to n) then assign q←1 and
         increment p;
         Else increment q;
5. // Pseudorandom number generation
   Let s be the seed value and R be the array to store
   the random numbers of size n.
   (a)     Assign R(1) ← s;
   (b)     Repeat for j varies from 2 to n
         R(j) ← [(a*R(j-1) + c) mod 255]
6. Repeat for i varies from 1 to m // row XOR
   Repeat for j varies from 1 to n
   Cipher_image2(i, j)← uint8(bitxor
                    (Cipher_image1(i, j), s(j)));
```

```
7. Repeat for i varies from 1 to m  // column XOR
   Repeat for j varies from 1 to n
   Cipher_image(i, j)← =uint8(bitxor
                              (Cipher_image2(j, i),s(j)));
8. Return the Cipher_image.
```

4 Implementation and Results

The proposed system is implemented using Matlab R2010a with P-IV processor of 2.50 GHz clock speed, 2 GB RAM, and Windows XP Operating Systems. The proposed approach is tested for gray scale images of dimension 256 x 256 pixels of type JPEG.

Figure 5 shows the result of proposed approach using cameraman and circuit board images and similar results are obtained for other images. The result shows that the encrypted image is completely different from the original image and it is difficult to predict the encrypted images. Also, the result is better than the existing basic scan patterns [8] as shown in Figure 1 without dividing the original image into chunks of blocks.

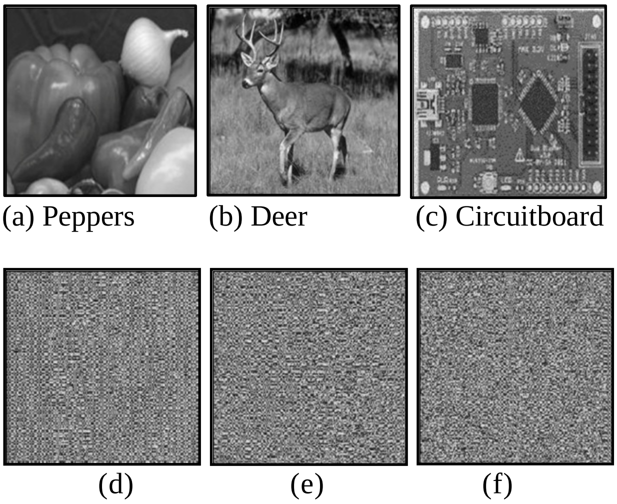

(a) (b) (c)

(d) (e) (f)

Fig. 5. Results of Proposed Matrix Reordering

(a) Original cameraman image, (b) Cameraman image after scan [8], (c) Cameraman image after MR (Proposed), (d) Original circuitboard image, (e) Circuitboard image after scan [8], (f) Circuitboard image after MR (Proposed).

The result of proposed approach using Matrix Reordering and XOR operation is shown in Figure 6. Figures 6(a) – (c) show the original image and (d) - (f) show the corresponding encrypted image. The result shows that the encrypted image is entirely different from the original image and it is not possible to predict the encrypted images.


(a) Peppers (b) Deer (c) Circuitboard

(d) (e) (f)

Fig.6 Results of Proposed Method

(a) - (c): Original images, (d) Encrypted peppers image, (e) Encrypted deer image, (f) Encrypted circuitboard image.

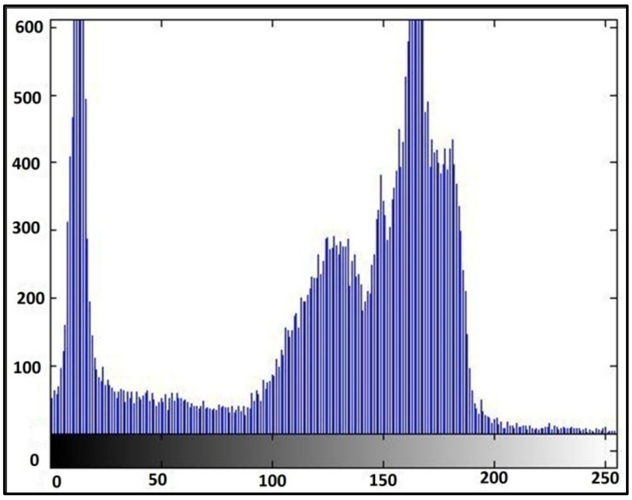
5 Analysis of Resutls

In order to justify the strength of the proposed approach, the evaluation parameters like confusion, diffusion, dispersion, cut test, and visual testing are performed. The results are analyzed and compared with the existing image encryption methods.

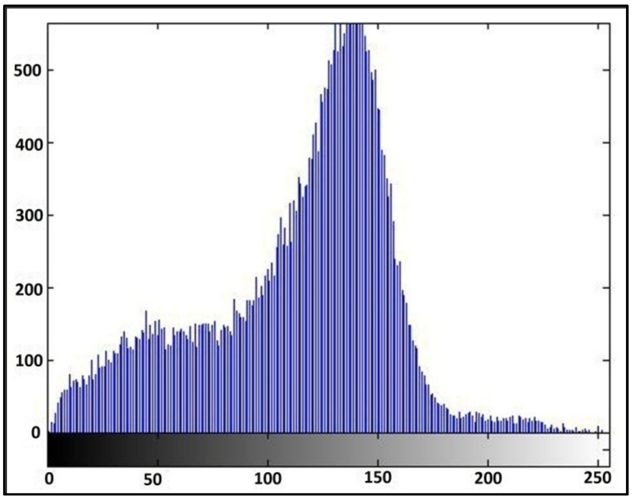
5.1 Histogram Analysis

An image histogram is a graphical representation of the pixel distribution in an image. The histogram for a very dark image will have the majority of its data points to the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph.

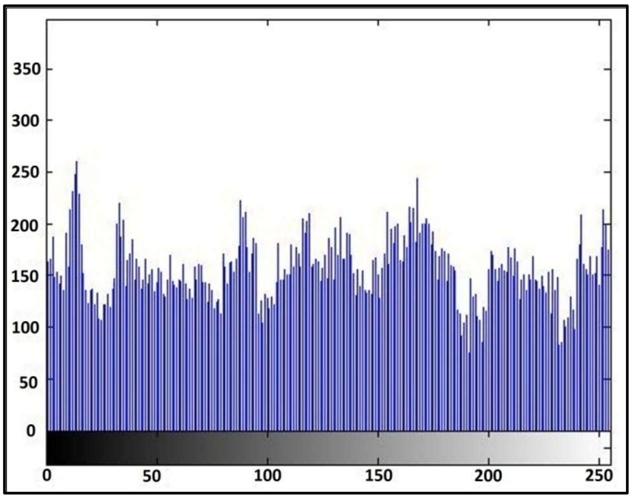
The histogram of original and encrypted cameraman and deer images are shown in Figure 7. The histogram of the encrypted image is completely different from the original image and the histogram shows that the gray values are uniformly distributed in the encrypted image. Thus, the proposed approach satisfies the diffusion property strongly, and does not provide any suspicion to employ statistical attack. The histogram of encrypted image is flat and similar to the methods [1, 7, 8, 14].



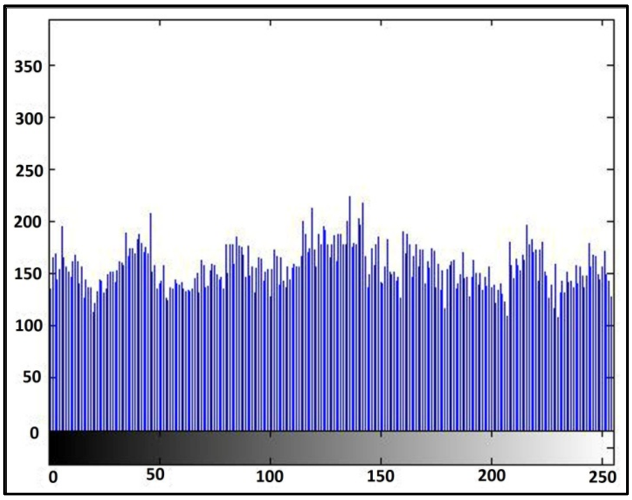
(a) Histogram of cameraman image before encryption



(b) Histogram of deer image before encryption



(c) Histogram of cameraman image after encryption



(d) Histogram of deer image after encryption

Fig.7 Histogram of original and encrypted images

5.2 Correlation Analysis

The correlation is a statistical technique that can show how strongly pairs of variables are related. The range of the correlation coefficient value is- 1 to + 1 and is calculated by,

$$\boldsymbol{\gamma}_{\mathbf{x,y}} = \frac{\mathbf{cov\ (x,y)}}{\sqrt{\mathbf{D(x)}}\,\sqrt{\mathbf{D(y)}}}, \tag{2}$$

where $\mathrm{D(x)} \neq 0$, and $\mathrm{D(y)} \neq 0$

$$\mathbf{cov\ (x,y)} = \frac{\mathbf{1}}{\mathbf{N}}\sum_{\mathbf{i=1}}^{\mathbf{N}}\big(\mathbf{x_i} - \mathbf{E(x)}\big)\big(\mathbf{y_i} - \mathbf{E(y)}\big) \tag{3}$$

$$\mathbf{E(x)} = \frac{\mathbf{1}}{\mathbf{N}}\sum_{\mathbf{i=1}}^{\mathbf{N}}\mathbf{x_i} \tag{4}$$

$$\mathbf{D(x)} = \frac{\mathbf{1}}{\mathbf{N}}\sum_{\mathbf{i=1}}^{\mathbf{N}}(\mathbf{x_i} - \mathbf{E(x)})^{\mathbf{2}} \tag{5}$$

Where n is the number of data pairs, x and y are the original and cipher images, respectively.E(x) and D(x) are the mean and standard deviation of the corresponding gray scale values. A weak relationship exists if the value of *r* is close to 0.

The correlation value between the original and encrypted images for five test images is given in Table 1 and similar results are obtained for other images. The results show that permuting pixels using the proposed MR give less correlation when compared with the basic scan patterns mentioned in the paper [8]. The cross correlation value is close to zero when both matrix reordering and XOR operations are performed.

Table 1. Correlation between original and encrypted images

Image	Existing SCAN [8]	Proposed SCAN	Proposed SCAN with XOR
Lena	0.3546	0.0036	-0.0006
Cameraman	0.3928	0.1489	-0.0037
Baboon	0.3513	0.0241	-0.0015
Deer	0.3218	0.1459	0.0092
Peppers	0.3317	0.0372	0.0114

The cross correlation result is better than the existing method values -0.008 for Lena image and -0.0046 for Cameraman image [14].

The horizontal, vertical, and diagonal correlation between adjacent pixels are calculated separately both for original and encrypted images and results are given in Table 2. The result shows that the correlation between adjacent pixels in the encrypted image is significantly reduced and close to zero.

Table 2. Adjacent pixel correlation distribution - proposed method

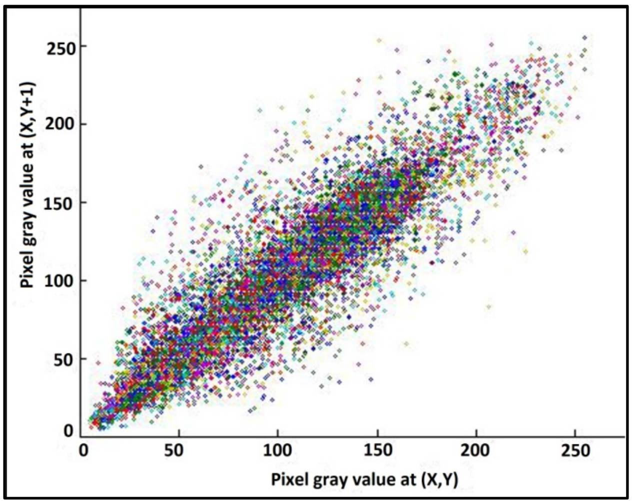
Image	Correlation		
	Horizontal	Vertical	Diagonal
Lena Original : Lena Encrypted:	0.9814 0.1366	0.9737 0.1498	0.9683 0.0225
Cman Original: Cman Encrypted:	0.9907 0.1594	0.9967 0.1300	0.9887 0.0919
Coin Original: Coin Encrypted:	0.9839 0.0253	0.9863 0.1395	0.9747 0.0347
Deer Original: Deer Encrypted:	0.9705 0.1466	0.9407 0.1364	0.9108 0.0087

The adjacent pixel correlation values of existing image encryption algorithms are given in Table 3. From the result, it is observed that the diagonal correlation value of the proposed method is similar to the exising methods and the horizontal and vertical correlation values are approximately close to the methods [6] and [14].

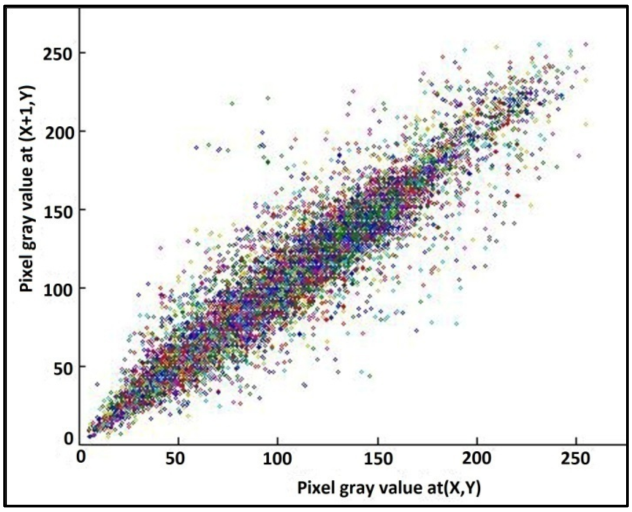
The adjacent pixel correlation distribution in the original and encrypted images are shown for the deer image in Figure 8. The results show the correlation between adjacent pixels in the encrypted image is low and the proposed approach satisfies the confusion property significantly.

Table 3. Adjacent pixel correlation distribution – existing image encryption methods

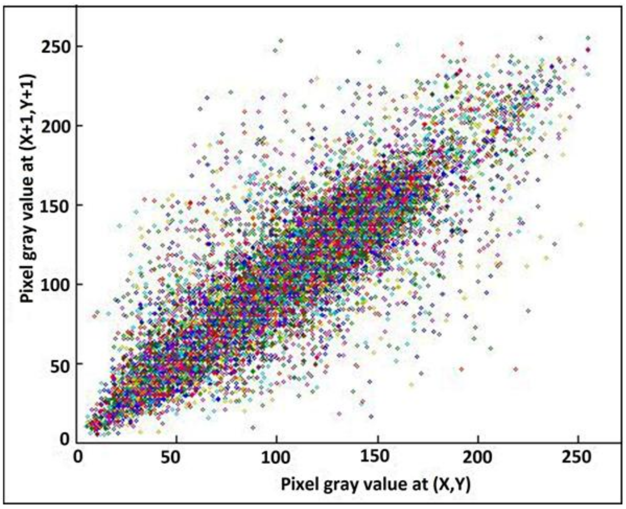
Existing Methods	Horizontal	Vertical	Diagonal
Ref. [5]	0.0068	0.0091	0.0063
Ref. [6]	0.0965	-0.0318	0.0362
Ref. [7]	0.036	0.035	-
Ref. [9] (Block size:3x3)	0.0129	0.0034	0.0014
Ref. [14] (Single map)	0.0781	0.0785	0.0683
Ref. [14] (Multiple map)	-0.0025	-0.0218	0.0167
Ref. [20]	0.01183	0.0002	0.0148



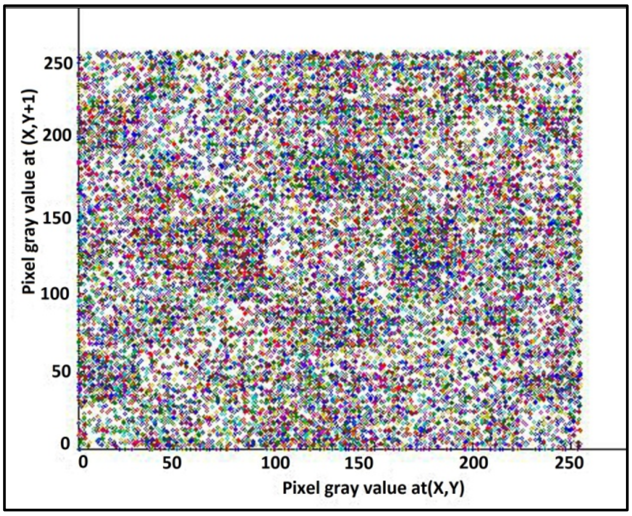
(a) Horizontal direction - original image



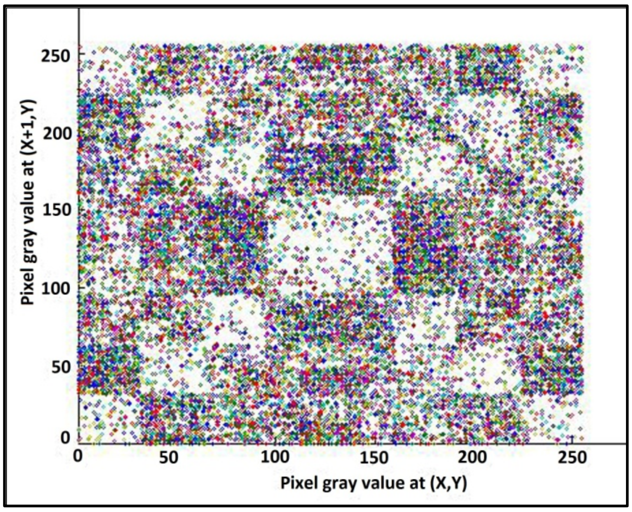
(b) Vertical direction - original image



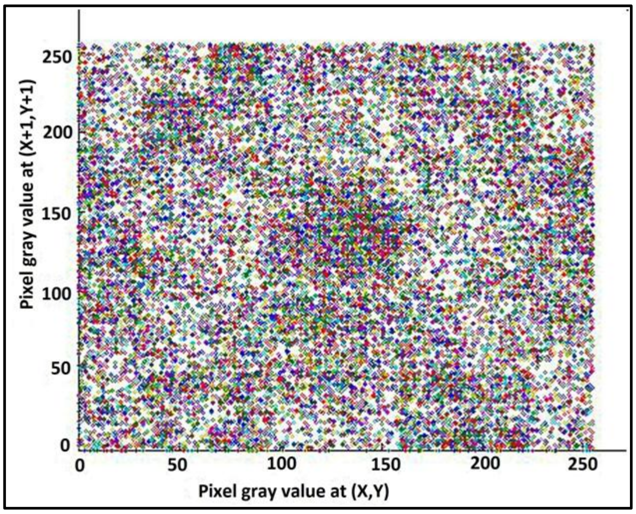
(c) Diagonal direction - original image



(d) Horizontal direction – encrypted image



(e) Vertical direction – encrypted image

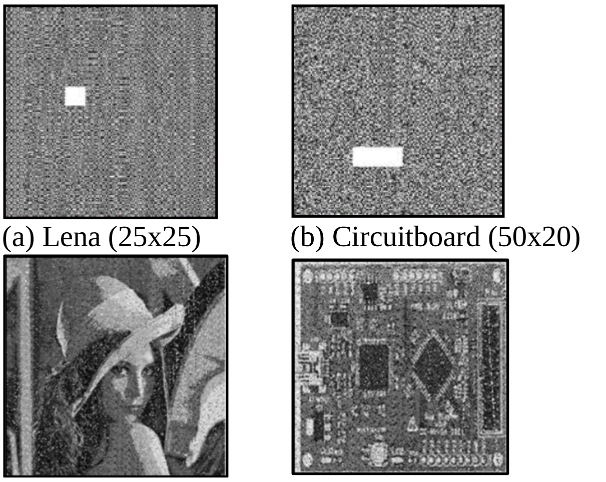


(f) Diagonal direction – encrypted image

Fig.8 Correlation distribution of adjacent pixels in Deer image: vertical, and diagonal directions of encrypted image.

5.3 Cut Test Analysis

The illegitimate users may destroy the information condition so that the authorized person couldn’t view the image after decryption. Figure 9 illustrates the result of cut test analysis on Lena and circuit board images. Figure 9 (a) and (b) shows the encrypted Lena and circuit board images after removing 25x25 and 50x20 pixels, respectively. Figures 9(c) and (d) show the corresponding decrypted images and the decrypted images are significantly distorted and could be recognized as a Lena and circuit board images. Thus, the proposed approach is harmless from partial removal of data or loss of data during transmission.



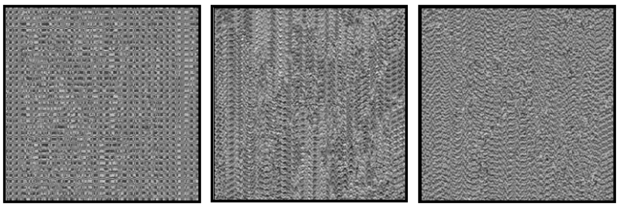
(a) Lena (25x25) (b) Circuitboard (50x20)

(c) Decrypted Lena (d) Decrypted circuitboard

Fig.9 Results of Cut Test Analysis

5.4 Sensitivity of Seed Value

For successful decryption, the initial value (x_0), constant (c) and increment (a) are vital elements for pseudorandom number generator. The proposed method is tested for effect of change in input to random number generator. Figure 10 shows the effect of change in the seed value on Lena image. The results show that the decryption is sensitive with respect to the seed values used to generate pseudorandom numbers. Thus, a small change in seed values will produce a completely different decrypted image and similar results are obtained for other images also.



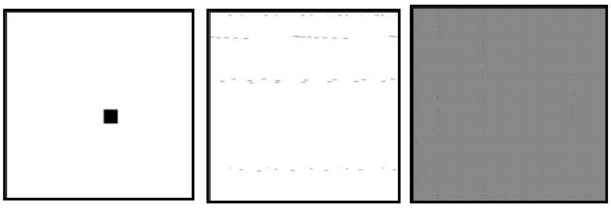
(a) (b) (c)

Fig. 10. Results of seed sensitivity test

(a) Encrypted Lena image (a=32, c = 64, s=32), (b) Decrypted Lena image (a=30, c=62, s=30), (c) Decrypted Lena image (a=34, c=66, s=34).

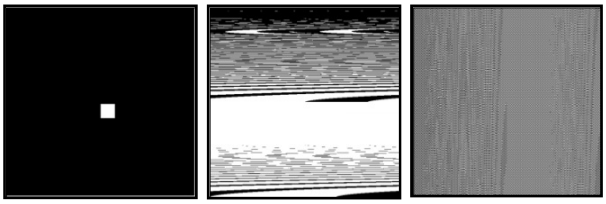
5.5 Dispersion Test Analysis

In order to find how well a small region is dispersed, a white image with 15x15 black region and a black image with 15x15 white region are encrypted. Figure 11(a) is the original white image and (b) and (c) are the images after MR and cipher image, respectively. Similarly, Figure 12(a) is the original black image, 12(b) and (c) show the image after MR and cipher image. The results show that the 15x15 region is distributed across the entire image, and the proposed method has a good pixel scrambling result.



(a) (b) (c)

Fig.11 Dispersion test using white image: (a) Original white image, (b) Image after MR, (c) Cipher image



(a) (b) (c)

Fig.12 Dispersion test using black image

(a) Original black image, (b) Image after MR, (c) Cipher image

5.6 Visual Testing

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two measures used to quantify the visual difference between the original and encrypted images. The NPCR measure indicates the percentage of different pixels between two images and the UACI measures the average intensity of differences in pixels between two images. To approach the performance of an image encryption algorithm, the NPCR values must be as large as possible (greater than 99.5%) and UACI values must be around 33% [5].

Let P[m, n] and C[m, n] be the plain and cipher images. Let P(i, j) and C(i, j) denote the pixel values of plain and cipher images at the ith row and jth column, respectively. The equations (6) and (7) give the mathematical expressions of the NPCR and UACI measures [5]:

$$\mathbf{NPCR} = \frac{\sum_{i,j} D(i,j)}{W*H} * \mathbf{100}\% \qquad (6)$$

$$\mathbf{UACI} = \frac{1}{W*H}\left[\sum_{i,j}\frac{|P(i,\ j)-C(i,\ j)|}{255}\right] * \mathbf{100\%} \qquad (7)$$

Where, the variables W and H represent the width and height of the image. D(i, j) = 1, if P(i, j) is equal to C(i, j) otherwise, D(i, j) is equal to 0. The values of i and j varies from 1 to W and 1 to H respectively.

The visual testing is experimented with standard images and Table 4 gives the NPCR and UACI values obtained for the proposed method.

Table 4. NPCR and UACI values - proposed method

Image	NPCR in % (Scan)	NPCR in % (Scan and XOR)	UACI in %
Lena	99.3881	99.5880	25.8613
Baboon	99.3800	99.5550	24.6523
Coin	97.6700	99.2475	25.5895
Cman	98.7275	99.6625	27.6304

The NPCR value is measured individually for both scan and scan with XOR operation. The NPCR values are high and show that the pixel positions have been randomly changed. The UACI values lie in the range of 24 to 28 and show that the pixel gray-scale values in encrypted image have been changed from their values in the original images.

The NPCR and UACI values of few existing image encryption methods is given in Table 5. From the result, it is observed that the NPCR value of the proposed method is better than the methods [14], [21] and much close to the methods [5], [13]. The UACI value also is better than the methods [13], [21], and similar to the method [5].

Table 5. NPCR and UACI values - existing methods

Existing Methods	NPCR (in %)	UACI (in %)
Ref. [5]	99.5850 (Lena) 99.6094 (Baboon)	28.6210 (Lena) 27.4092 (Baboon)
Ref. [13]	99.6149	13.8349
Ref. [14]	98.4754	32.2128
Ref. [21]	> 99.42	> 24.94

5.7 Speed Test

The comparison of running time between the proposed method and few existing methods are given in Table 6. To encrypt images of size 256 x 256 pixels, the conventional algorithms such as DES, AES, and IDEA take approximately 30 s, 40 s, and 80 s, respectively.

The result shows that the time consumed by the proposed method is less when compared with the existing image encryption methods [3], [19], [20] and approximately close to the method [5].

Table 6 Comparison of Speed

Encryption Methods	Encryption Time	Image Size	System Configuration
Proposed	0.23 s	256 x 256	Matlab R2010a, PC with P-IV, 2.50 GHz, 2 GB RAM, 160 GB hard disk.
Ref. [3]	0.5 s	256 x 256	PC with P-IV, 1.5 GHz, 512 MB RAM, 40 GB hard disk
Ref. [5]	0.12 s	256 x 256	Matlab, PC with AMD Athlon, 2.70 GHz, 1 GB RAM, 160 GB hard disk.
Ref. [19] (A-I)	0.56 s	256 x 256	Matlab, PC with P-IV, 2.6 GHz.
Ref. [19] (A-II)	1.01 s		
Ref. [20]	< 0.4 s	256 x 256	PC with P – IV, 1.0 GHz, 256 RAM, and 40 GB hard disk.

6 Conclusion

A simple image encryption method based on Matrix Reordering (MR) and XOR operation is proposed in this paper. The proposed scan model is placed the adjacent pixel elements randomly and found to give significantly improved performance. The proposed scan model is better than the existing basic scan patterns [8] with respect to the less correlation between the original and encrypted images as well as the original image is not divided into chunks of blocks. The gray-scale values are uniformly distributed in the encrypted image, and the histogram is much flat.

The cross correlation value is close to zero which indicates that the relationship between the original and encrypted images is very low. The horizontal, vertical, and diagonal correlation between the adjacent pixels of the encrypted image is approximately close to zero. Thus, the proposed approach satisfies the confusion property strongly and the diffusion property significantly.

The cut test, dispersion test, seed sensitivity test, and encryption speed results show that the proposed image encryption method can be used in real time applications. The values of NPCR (> 99.5%) and UACI (> 25%) prove that the proposed method is resistant to differential attack.

References:

[1] Guodong Ye, “An Efficient Image Encryption Scheme based on Logistic maps”, *International Journal of Pure and Applied Mathematics*, Vol.55, No.1,2009, pp. 37-47.

[2] Han Shuihua and Yang Shuangyuan, “An Asymmetric Image Encryption Based on Matrix Transformation”, *ECTI Transactions on Computer and Information Technology*, Vol.1, No.2, 2005, pp. pp.126-133.

[3] Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li, “A New Chaotic Algorithm for Image Encryption”, *Elsevier Science Direct*, vol. 29, no. 2, 2006, pp.393-399.

[4] Jawahar Thakur, and Nagesh Kumar, “DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, *International Journal of Emerging Technology and Advanced Engineering*, Vol.1, No.2, 2011, pp.6-12.

[5] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, “A Secure Image Encryption Algorithm Based on Rubik's Cube Principle”, *Journal of Electrical and Computer Engineering*, 2011, pp. pp.1-13.

[6] Liu Hongjun and Wang Xingyuan, “Color image encryption based on one-time keys and robust chaotic maps”, *Journal of Computers and Mathematics with Applications (Elsevier)*, Vol.59, 2010, pp. 3320-3327.

[7] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption”, *World Academy of Science, Engineering and Technology*, Vol.3, 2007, pp.526-531.

[8] S.S. Maniccam, and N.G.Bourbakis “Image and Video Encryption using SCAN Patterns”, *The Journal of the Pattern Recognition Society*, Vol.37, 2004, pp.725-737.

[9] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption using Block-Based Transformation Algorithm”, *IAENG International Journal of Computer Science*, Vol.35, No.1, 2008, pp.3-11.

[10] Prabhudesai Keval Ketan and Vijayarajan V, “An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption”, *International Journal of Computer Applications*, Vol.54, No.12, 2012, pp.29-36.

[11] S.A.M Rizvi, Syed Zeeshan Hussain and Neeta Wadhwa, “A Comparative Study of Two Symmetric Encryption Algorithms Across Different Platforms”, *International Conference on Security and Management (SAM’11)*, World Academy of Science, USA, 2011.

[12] Sanfu Wang, Yuying Zheng and Zhongshe Gao, “A New Image Scrambling Method through Folding Transform”, *IEEE International Conference on Computer Application and System Modeling*, Taiyuan, 22-24 Oct. 2010, pp.v2-395-399.

[13] G.A. Sathishkumar and K.Bhoopathy Bagan, “A Novel Image Encryption Algorithm Using Pixel Shuffling and BASE 64 Encoding Based Chaotic Block Cipher, *WSEAS Transactions on Computers*, Vol.10, No. 6, 2011, pp. 169-178.

[14] G.A Sathishkumar, K.Bhoopathy and R.Sriraam, “Image Encryption Based on Diffusion and Multiple Chaotic Maps”, I*nternational Journal of Network Security & its Applications*, Vol.3, No.2, 2011, pp. 181-194.

[15] Shao Liping, Qin Zheng, Qin Jun, and Li Huan, “Image Scrambling Algorithm Based on Random Shuffling Strategy”, *IEEE International Conference on Industrial Electronics and Applications*, Singapore, 3-5 June 2008, pp.2278-2283.

[16] Shashi Mehrotra Seth, and Rajan Mishra, “Comparative Analysis of Encryption Algorithms for Data Communication”, *International Journal of Computer Science and Technology*, Vol.2, No.2, 2011, pp.292-294.

[17] Vishwa Gupta, Gajendra Singh, and Ravindra Gupta, “Advance Cryptography Algorithm for Improving Data Security*”, International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.2, No.1, 2012.

[18] William Stalliungs, “*Cryptography and Network Security-Principles and Practice*”, Pearson Education, 2011.

[19] Xiaomin Wang, and Jiashu Zhang, “An Image Scrambling Encryption using Chaos-

controlled Poker Shuffle Operation", *IEEE International Symposium on Biometrics and Security Technologies*, Islamabad, 23-24 April 2008, pp.1-6.

[20] G. Chen, Y. Mao, and C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", *Chaos, Solitons and Fractals*, Vol. 21, No. 3, 2004, pp.749–761.

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