A Novel Image Encryption Method with Z-Order Curve and Random Number

T. Sivakumar
Assistant Professor (Senior Grade)
Department of Information Technology
PSG College of Technology, Tamilnadu-641 004, India.

R. Venkatesan
Professor
Department of Computer Science and Engineering
PSG College of Technology, Tamilnadu-641004, India.

ABSTRACT

Information security has become an important issue for data storage and transmission due to growth of communication development and exchange of sensitive information through Internet. The services like confidentiality, integrity, and digital signature are required to protect data against unauthorized modification and misuse by anti social elements. Image encryption is widely used in multimedia, medical imaging, telemedicine and military communications to provide confidentiality service. A novel and simple image encryption method using Z-Order (ZO) curve based scan pattern and random number is proposed in this paper. The proposed method resists the statistical and differential attacks. The method provides optimal entropy value and assures security from the additive noise and cropping attacks.

Keywords: Image Encryption, Scan Pattern, Z-Order Curve, Random Number

1. INTRODUCTION

Cryptography is the art of achieving security by encrypting messages to make them non-readable and decrypting the messages to obtain the original information by the authorized users. IBM introduced the Data Encryption Standard (DES) algorithm which was initially used for the encryption of electronic data and it is now considered to be insecure because of brute force attack. It has a block size of 64-bits as plaintext and key size is 56-bits. The Advanced Encryption Standard (AES) proposed by Daemen and Rijmen has a fixed block size of 128-bits and key size of 128,192 or 256 bits. The International Data Encryption Algorithm (IDEA) is designed by James Massey and it operates on 64-bit block as plaintext with 128-bit as encryption key [25].

The conventional encryption algorithms are not desirable when the input size is large. The conventional algorithms are mainly used to encrypt text messages and are not sufficient to encrypt digital images. The volume of data that represent an image is always greater than textual data and hence the traditional algorithms take long time to encrypt digital images [9]. Unlike textual data, images have special features such as bulk capacity, high redundancy and high correlation among pixels. The high redundancy and bulk capacity generally make encrypted image vulnerable to attacks via cryptanalysis. Since pixels in images have high redundancy and strong correlations, adjacent pixels likely to have similar gray-scale values or nearby blocks have similar patterns. On average 8 to 16 adjacent pixels are correlative in all the directions for both natural and computer-graphical images. Thus, the image encryption methods should break such correlations among the pixels to provide confidentiality.

Typically, the image encryption methods use both substitution and transposition/permutation processes to convert the plain image into cipher image. In diffusion, the statistics of the original image is dissipated into long-range statistics of the encrypted image and this is achieved by repeatedly performing several permutations. The confusion process seeks to make the relationship between the statistics of the encrypted image and the encryption key as complex as possible and this is achieved by substitution methods [25].

The major types of image encryption methods based on permutation are classified as bit level permutation [16], pixel permutation [1, 5, 6, 8, 14, 17], and block permutation [20, 22]. In the case of bit level permutation, the bits of each pixel taken from the image are permuted with the key chosen from the set of keys by using the pseudorandom index generator. In pixel permutation, the pixel position of the image is rearranged using the key selected from the set of keys and the size of pixel group is same as the length of the keys. In the case of block permutation, the image is divided into blocks and these blocks are permuted based on the random key. Among the methods, in block permutation better result can be obtained by choosing smaller block sizes.

The key idea of the proposed method is to rearrange the pixels position of the plain image and change the pixel values after pixel permutation. The pixel shuffling is done by scan patterns and the pixel values are changed by simple and efficient bitwise XOR operation. The proposed method provides improved security over unauthorised disclosure of image.

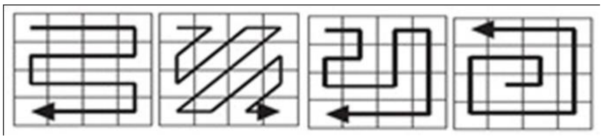
The rest of the paper is organized as follows. The basic concepts used in the proposed method are given in Section 2. Section 3 describes the proposed image encryption method. Section 4 gives the experimental results and Section 5 presents the performance and security analysis. The paper is concluded in Section 6.

2. PRELIMINARY

After having described the introduction methods and organization of the paper, to begin with an overview of certain topics is presented in this section. This will serve as a background for the easy understanding of the proposed image encryption method.

2.1 Scan Pattern

The encryption method based on the SCAN methodology is a formal language-based two-dimensional spatial access, which could generate large number of scanning paths [24]. SCAN is a special purpose context-free language devoted to describe and generate a wide range of 2-D array accessing algorithms from a short set of simple ones. These algorithms represent sequential scanning techniques used for image processing, such as generation of image data structures (pyramids and trees), encryption, and compression of images [19]. The most frequently used scan patterns are continuous raster (C), continuous diagonal (D), continuous orthogonal (O), and spiral (S) as shown in Figure 1. This paper intends to introduce a new scan pattern approach based on the notion of Z-Ordering.



(a) Raster (b) Diagonal (c) Orthogonal (d) Spiral

Fig 1: Basic scan patterns

2.2 Z-Order Curve

The concept of Z-Order (ZO) curve is used in spatial, text, and multimedia databases to implement one-dimensional index and search on multi-dimensional data. In the propsoed method, the scan pattern to permute the pixels position is implemented by using the notion of Z-Order curve. The structure of Z-Order is presented in Figure 2 for the dimensions 4 x 4 and 8 x 8 respectively.

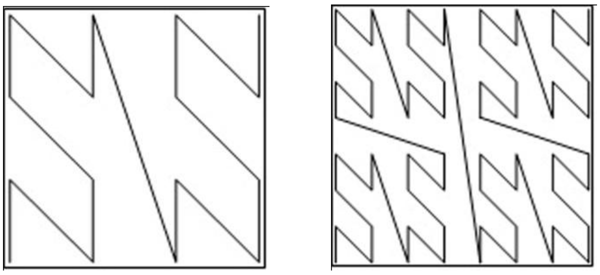
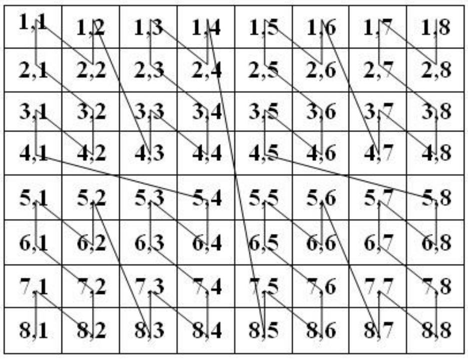


Fig 2: (a) Z-Order curve (4 x 4) (b) Z-Order curve (8 x 8)

In the proposed method, pixels position permutation is performed by the above scan model.

2.3 Proposed Pixel Position Permutation

To describe the proposed scan pattern, consider the Z-Order curve structure shown in Figure 3(a) with the starting coordinate (8, 1). The equivalent scan coordinate (pattern) is shown in Figure 3(b). The original 8 x 8 image matrix is shown in Figure 3(c) and the corresponding scrambled image matrix is shown in Figure 3(d).



1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8
2,1	2,2	2,3	2,4	2,5	2,6	2,7	2,8
3,1	3,2	3,3	3,4	3,5	3,6	3,7	3,8
4,1	4,2	4,3	4,4	4,5	4,6	4,7	4,8
5,1	5,2	5,3	5,4	5,5	5,6	5,7	5,8
6,1	6,2	6,3	6,4	6,5	6,6	6,7	6,8
7,1	7,2	7,3	7,4	7,5	7,6	7,7	7,8
8,1	8,2	8,3	8,4	8,5	8,6	8,7	8,8

(a) Z-Order curve (8 x 8)

8,1	7,1	8,2	7,2	6,1	5,1	6,2	5,2
8,3	7,3	8,4	7,4	6,3	5,3	6,4	5,4
4,1	3,1	4,2	3,2	2,1	1,1	2,2	1,2
4,3	3,3	4,4	3,4	2,3	1,3	2,4	1,4
8,5	7,5	8,6	7,6	6,5	5,5	6,6	5,6
8,7	7,7	8,8	7,8	6,7	5,7	6,8	5,8
4,5	3,5	4,6	3,6	2,5	1,5	2,6	1,6
4,7	3,7	4,8	3,8	2,7	1,7	2,8	1,8

(b) Scan coordinates

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) Input image matrix

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

(d) Output image matrix

Fig 3: Proposed pixels position permutation

From the illustration, it is observed that the pixel elements are permuted for an acceptable level. The original image pixels values are taken as 1 to 64 continuously to verify the effect of pixel permutation.

2.4 Random Number in Cryptography

Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs) are the two main approaches to generation of random numbers [25]. The PRNGs are deterministic and periodic but TRNGs are non-deterministic and a-periodic. TRNGs are considered as the most suitable candidate for cryptography. True random sources can be considered unconditionally un-guessable, while pseudo-random sources are good only against computationally limited adversaries. The cryptographically secure pseudo random bit generator (PRBG) Blum Blum Shub (BBS) is used by the proposed method to generate random number.

3. PROPOSED IMAGE ENTRYPTION METHOD

The basic idea of proposed method is to scramble the original image using pixels position permutation with the notion of Z-Ordering. The scrambled image is XORed with the random number to obtain the cipher image. The working model of the proposed system is shown in the form of a block diagram in Figure 4.

First, the image is given as input and divided into blocks, such that, the order of the block and the Z-Order are same. Then, the pixels coordinate are permuted by using the Z-Ordering based scan pattern to obtain the scrambled image. The pixels value of the scrambled is changed by the symmetric bitwise XOR operation to obtain the encrypted image.

The random number to perform XOR operation is generated by using Blum Blum Shub (BBS) generator. The decryption function is the inverse of the encryption function. The encryption key consists of two parts, namely, the scan pattern generated from Z-Ordering and the seed values of random number generator. The encryption keys are known and securely shared by the sender and receiver.

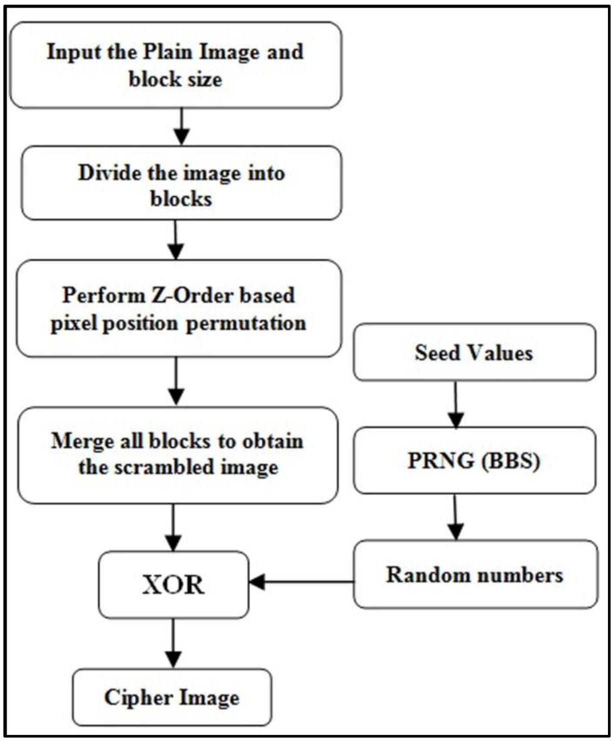

Input the Plain Image and block size
Divide the image into blocks
Perform Z-Order based pixel position permutation
Seed Values
Merge all blocks to obtain the scrambled image
PRNG (BBS)
XOR
Random numbers
Cipher Image

Fig 4: Block diagram representation of the proposed method

3.1 Encryption Algorithm

The encryption algorithm of proposed method is presented in this section. The following sequence of steps to be performed to convert the original image into cipher image.

Input: Plain Image, Scan pattern, block size, random number

Output: Cipher image

Step 1: Let I[m][n] be the plain image, where m and n are the number of rows and columns.

Step 2: Input the block size (b) and seed value to generate random number.

Step 3: Resize the input image into square and divided it into blocks of size b x b pixels.

Step 4: Generate the scan pattern corresponding to the order b.

Step 5: Perform pixels position permutation using scan pattern.

Step 6: Repeat step 5 until all the blocks are processed.

Step 7: Combine all the blocks to obtain the scrambled image.

Step 8: Generate random number by using the BBS generator.

Step 9: The scrambled image obtained in step (7) is XORed with the random number generated in step (8) to get cipher image.

Step 10: Store the cipher image.

3.2 Random Number Generator

In this section, the random number generator algorithm is described. The cryptographic secure Blum Blum Shub (BBS) pseudorandom number generator is used to generate the random numbers. The BBS generator produces a sequence of bits according to the following algorithm [30].

```
$X_0 = S^2 \bmod n$
for i = 1 to $\infty$
    $X_i = (X_{i-1})^2 \bmod n$
    $B_i = X_i \bmod 2$
```

Where, S is the seed value and n is the product of two prime numbers, p and q. Both p and q have a remainder of 3 when divided by 4 and S is relatively prime to n. In the proposed method, the BBS random bit generator is used to generate random numbers.

4. IMPLEMENTATION RESULTS

The proposed method is implemented in Matlab 2010a using Windows (32 bit) operating system with P-IV Processor, 2.80GHz, 2 GB RAM, and 160 GB HDD.

The method is tested with standard gray-scale images Lena, Baboon, Cameraman, and Peppers of size 256 x 256 pixels. The block size considered for pixels position permutation is 8 and 16. The implementation result of proposed image encryption method is presented using the Lena image in Figure 5 for visual perception.

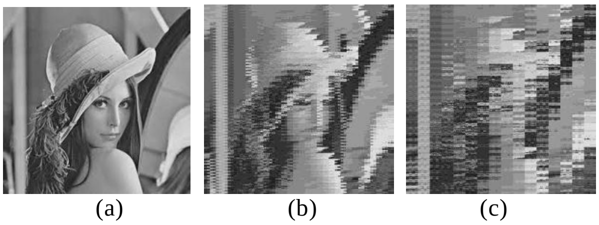

(a) (b) (c)

Fig 5: Results of pixel permutation: (a) Original image, Pixel permuted image of (b) Order of 8, (c) Order of 16

From, the result it is observed that increasing the dimension of the Z-Ordering provides better permutation result.

The corresponding encrypted images with order 8 and 16 are shown in Figure 6(a) and (b) respectively.

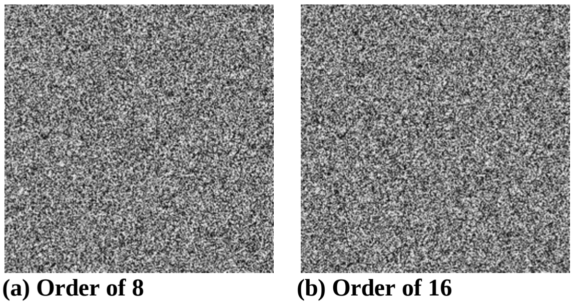

(a) Order of 8 **(b) Order of 16**

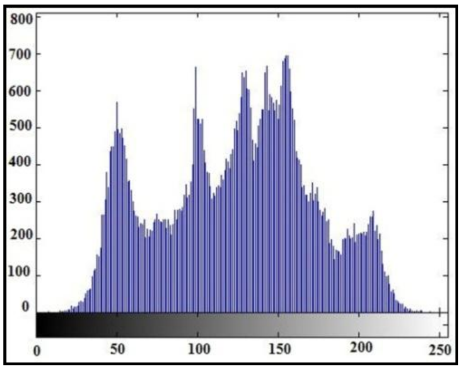
Fig 6: Encrypted Lena image

5. ANALYSIS AND DISCUSSION OF RESULTS

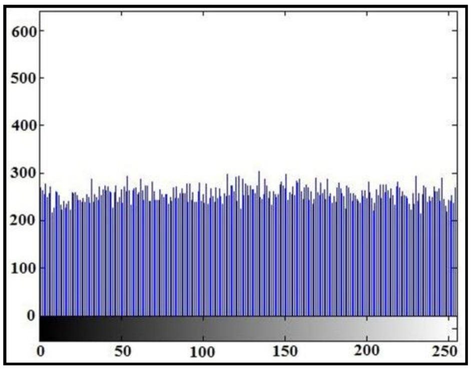
In this section, to confirm the security level of the proposed method various evaluation parameters are measured, compared with recent existing image encryption methods, and analyzed.

5.1 Histogram Analysis

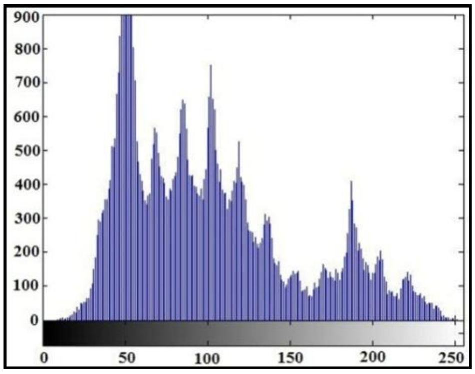
It is important to ensure that the encrypted and the original images do not have any statistical similarities. The histogram analysis reveals how the pixel values of an image is distributed before and after the encryption process. The histogram of an original image contains great rises followed by sharp declines but the histogram of the encrypted image should be flat. The histogram of the original and the corresponding encrypted Lena, Peppers, and Baboon images are shown in Figure 7(a) to Figure 7(f).



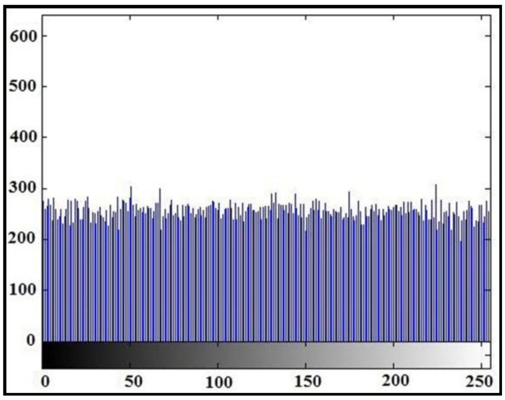
(a) Original Lena image



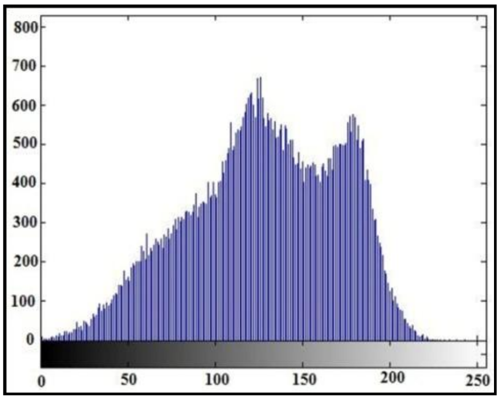
(b) Encrypted Lena image



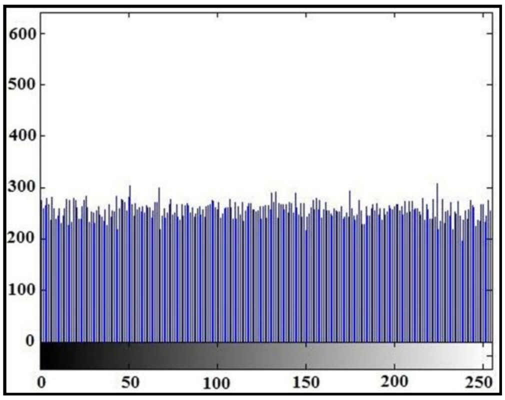
(c) Original Peppers image



(d) Encrypted Peppers image



(e) Original Baboon image



(f) Encrypted Baboon image

Fig 7: Histogram of original and encrypted images

The histogram of the encrypted image is flat and the gray-scale values are uniformly distributed over the entire cipher image. Thus, the proposed method resists the statistical attacks based on analysis of histogram of an image.

5.2 Correlation Analysis

The correlation coefficient is a useful measure to judge the security level of any image cryptosystem. It is used to find the degree of similarity between the original and the corresponding encrypted images and between adjacent pixels of the encrypted image. An arbitrarily chosen pixel in an original image is strongly correlated with adjacent pixels, in horizontal, vertical and diagonal directions. A secure image encryption algorithm must produce an encrypted image having low correlation between adjacent pixels in all the directions. The correlation co-efficient is computed by using the equation (1).

$$\gamma_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

$$\mathrm{Cov}(x,y)= \frac{1}{N}\sum_{i=1}^{N}\big(xi - E(x)\big)\big(yi - E(y)\big) \quad (2)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^{2} \quad (3)$$

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

Where, Cov(x,y) is the covariance between x and y; N is the number of pixel pairs (x_i, y_i), and E(x) and D(y) are the mean and standard deviation of the pixel values of x_i and y_i respectively. The adjacent pixel correlation value obtained by the proposed method in given in Table 1 and the same is given for few existing image encryption methods in Table 2.

Table 1. Adjacent pixel correlation - proposed method

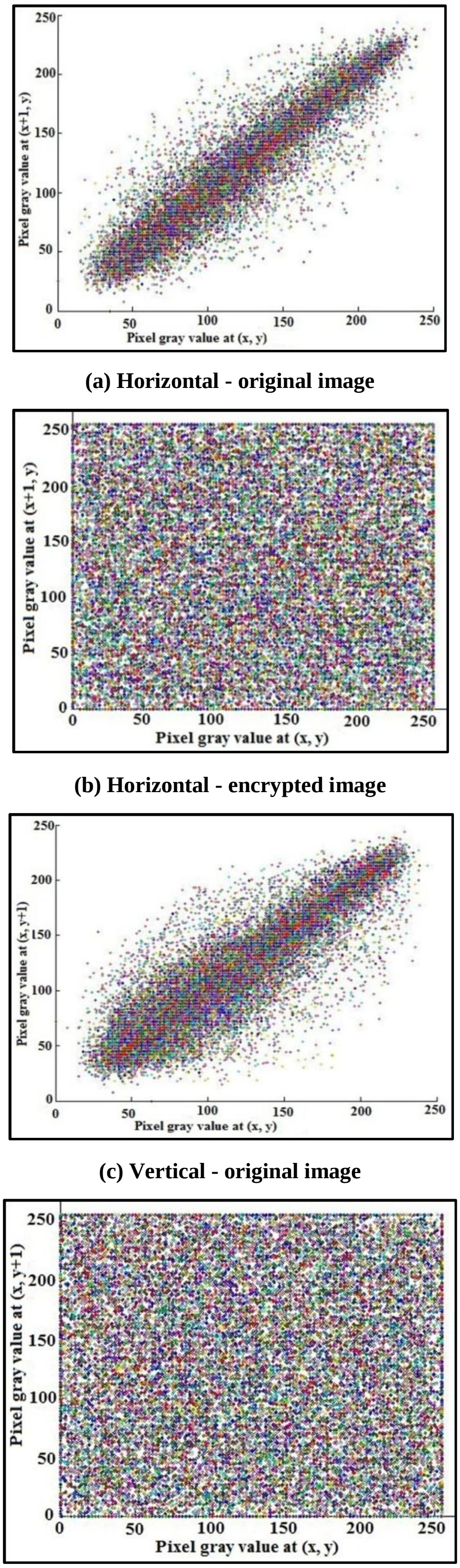
Images	Directions		
	Horizontal	Vertical	Diagonal
Lena Image: Original: Encrypted:	 0.9846 0.0161	 0.9756 0.0066	 0.9690 0.0075
Peppers Image: Original: Encrypted:	 0.9752 0.0063	 0.9830 0.0007	 0.9651 0.0029
Baboon Image: Original: Encrypted:	 0.6265 0.0092	 0.7022 0.0019	 0.5340 0.0025

Table 2. Adjacent pixel correlation – existing methods

Existing Methods	Directions		
	Hori.	Vert.	Diag.
Adrian Viorel Diaconu *et. al.* [1]	0.0002	0.0006	0.0043
Haojiang Gao *et. al.* [10]	-0.0158	-0.0653	-0.0323
Kamlesh Gupta *et. al.* [13]	0.0010	0.0060	0.0910
Khaled Koukhaoukha *et. al.* [14]	0.0068	0.0091	0.0063
Liang Zhao *et. al.* [15]	0.0199	0.0431	-0.0034
P. Vidhya Saraswathi *et. al.* [20]	0.0177	0.0491	0.0034
Qiang Zhang *et. al.* [21]	0.1366	0.0166	0.0021
Rasul Enayatifar *et. al.* [23]	-0.0051	0.0078	-0.0009

Hori.- Horizontal, Vert.- Vertical, Diag.- Diagonal

The correlation between the adjacent pixels of the encrypted images optimal and is close to zero. It is found that the obtained values are better than the methods in [10, 15, 20, 21], comparable with those methods in [13, 14, 23] and slightly lesser than the method in [1]. The pictorial view of relationship between the adjacent pixels in horizontal, vertical, and diagonal directions in the original and encrypted Lena images are shown in Figure 8.

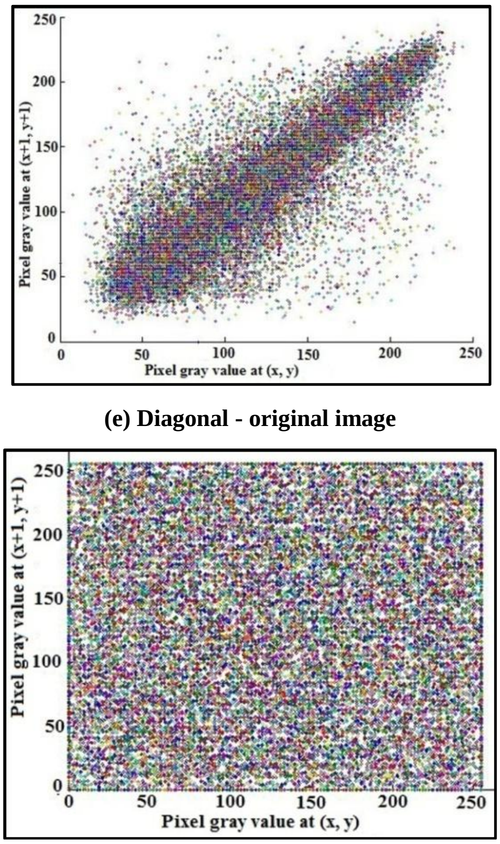


(a) Horizontal - original image

(b) Horizontal - encrypted image

(c) Vertical - original image

(d) Vertical - encrypted image



(e) Diagonal - original image

(f) Diagonal - encrypted image

Fig 8: Adjacent pixel correlation

From the graph, it is seen that the correlation between adjacent pixels is much reduced in the encrypted image and hence the proposed method resists the statistical attacks based on analysis of correlation of encrypted images.

The correlation between the original and encrypted images is given in Table 3. The cross correlation value shows that there is no exact relationship between the original image and the corresponding encrypted image. The result obtained by the proposed method is matches with the existing methods in [7, 18].

Table 3. Comparison of cross correlation

Encryption Method	Correlation Value
Proposed	Lena : 0.0018 Peppers: 0.0071 Baboon: 0.0028
G.A Sathishkumar *et al*. [7]/A-I	-0.0535
G.A Sathishkumar *et al*. [7]/A-I & A-II	0.0074
Narendra K Pareek et. al. [18]	0.0211

5.3 Visual Testing

The perceptual relationship between the original image and the corresponding encrypted image should be reduced after the encryption process. That is, the encrypted image should be completely different from its original version. To quantify this requirement, the parameters Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) parameters are measured and analyzed [14].

5.3.1 Number of Pixel Change Rate (NPCR)

The Number of Pixels Change Rate (NPCR) indicates the percentage of difference in pixels between two images. For the original image $I_o(i, j)$ and the encrypted image $I_{ENC}(i, j)$ the mathematical formula to compute the NPCR value is given in equation (5) [12].

$$\textbf{NPCR} = \frac{\sum_{i,j} D(i,j)}{W*H} * 100\% \qquad (5)$$

Where, W and H are the width and height of the images. If $I_o(i, j) = I_{ENC}(i, j)$, then D(i,j) = 0; else D(i,j) = 1. The algorithm is better when obtained NPCR value is greater than 99.5% [26]. The NPCR value obtained by the proposed method and few relevant existing image encryption methods are given in Table 4.

Table 4. Comparison of NPCR value

Encryption Method	NPCR Value (in %)
Proposed	Lena: 99.6704 Peppers: 99.6490 Baboon: 99.6140
Adrian Viorel Diaconu *et. al.* [1]	99.6120
C.K. Huang *et. al.* [6]	99.5400
Kamlesh Gupta *et. al.* [13]	99.6300
Khaled Koukhaoukha *et. al.* [14]	99.5850

From the result, it is found that the NPCR value obtained by the proposed method is optimal, better than the methods in [6, 14] and comparable with the methods in [1, 13].

5.3.2 Unified Average Changing Intensity (UACI)

The UACI measure is used to identify the average intensity difference in pixels between two images. For the plain image $I_o(i, j)$ and encrypted image $I_{enc}(i, j)$ the equation (6) gives the mathematical formula to compute the UACI value [12].

$$\textbf{UACI} = \frac{1}{W*H}\left[\sum_{i,j}\frac{Io(i,j)-Ienc(i,j)}{255}\right] * 100\% \qquad (6)$$

Where, W and H are the width and height of the images. The encryption algorithm is better when obtained UACI value is around 33% [26]. The UACI value obtained by the proposed method and some of the existing image encryption methods are tabulated in Table 5.

Table 5. Comparison of UACI value

Encryption Method	UACI Value (in %)
Proposed	Lena : 28.3340 Peppers: 30.1392 Baboon: 27.8491
Adrian Viorel Diaconu *et. al.* [1]	30.5997
C.K. Huang *et. al.* [6]	28.2700
Kamlesh Gupta *et. al.* [13]	28.8700
Khaled Koukhaoukha *et. al.* [14]	28.6201

From the result, it is observed that the UACI value obtained by the proposed method is acceptable and comparable with those methods in [1, 6, 13, 14]. Both NPCR and VACI results designates that the suggested method resists the differential attacks for an acceptable level.

5.4 Information Entropy

The entropy of a message source is a measure of the amount of information the source has. The measure is in the form of a function of the probability distribution over the set of all possible messages the sources may output [2, 4]. The entropy of gray-scale images is theoretically equal to 8 Sh, if each level of gray is assumed to be equiprobable. In image encryption, the encrypted image should provide an equiprobable gray level. If the entropy values of the encrypted images are close to the ideal value of 8 Sh, then the encryption algorithm is highly robust against entropy attacks [3, 14]. The entropy of the information is computed by using the equation (7).

$$\boldsymbol{H(m) = \sum_{i=0}^{m-1} p(mi) log \left({}^{1}\!/_{p(mi)}\right)} \qquad (7)$$

Where, m is the total number of symbols in $m_i \in m$; $p(m_i)$ represents the probability of occurrence of the symbol m_i and log denotes the base 2 logarithm. The obtained entropy value of the proposed method and few existing methods are compared and given in Table 6.

Table 6. Comparison of entropy value

Encryption Method	Entropy Value (Sh)
Proposed	Lena: 7.9969 Peppers: 7.9955 Baboon: 7.9972
Adrian Viorel Diaconu *et. al.* [1]	7.9992
G.A. Sathishkumar *et. al.* [8]	7.8101
Kamlesh Gupta *et. al.* [13]	7.9981
KhaledLoukhaoukha *et. al.* [14]	7.9968
Liang Zhao *et. al.* [15]	7.9719
Qiang Zhang *et. al.* [21]	7.9975
Rasul Enayatifar *et. al.* [23]	7.9931
Z. Lin *et. al.* [27]	7.9890

It is observed that the result obtained by the proposed method is acceptable, better than those methods in [8, 15, 27] and comparable with the existing method in [1, 13, 14, 21, 23].

5.5 Analysis of Noise Attacks

The attackers or intruders may introduce additive noise and cropping attacks on the encrypted image while transit. These attacks destroy the information condition so that the authorized person couldn't use the image even after successful decryption.

5.5.1 Additive noise attack

An additive noise attack consists in adding random noise to the intercepted encrypted image [1]. The additive noise attack is tested by using salt and pepper noise and speckle noise to confirm the resistance against this attack. The obtained result of additive noise attack by using the encrypted Lena image is shown in Figure 9(a), (b), (c) and (d) with density 0.05 and 0.1 for salt and pepper noise and variance 0.01 and 0.02 for speckle noise respectively.

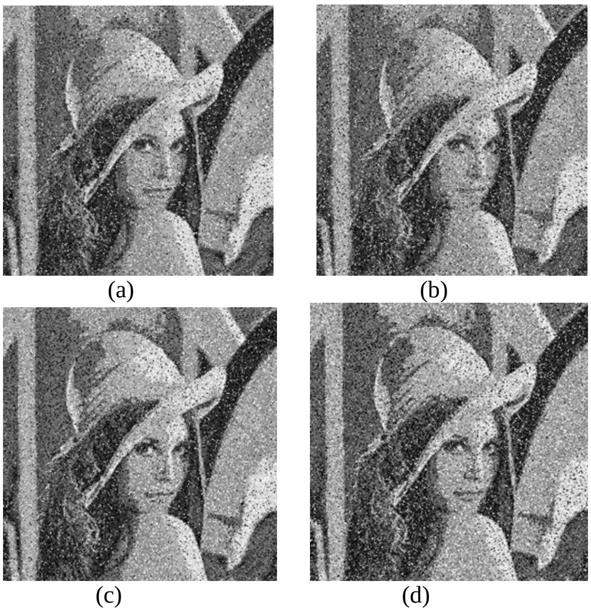


Fig 9: Decrypted Lena images with additive noise

From the analysis, it is found that the proposed method has good resistance against additive noise attacks. Also, better result is obtained when compared with the method in [1] for high density and variance of salt and pepper and speckle noises and comparable with the result reported in [16].

5.5.2 Cropping attack

The cropping attacks consist of modifying the intercepted cipher image by destroying few regions [1]. The cropping attack is tested using the encrypted Lena image by removing 10 regions each of size 10 x 10 pixels and three regions each of size 50 x 15 pixels as shown in Figure 10(a) and 10(b) respectively. The corresponding decrypted images are shown in Figure 10(c) and 10(d). The decrypted images are significantly distorted and could be recognized as a Lena image.

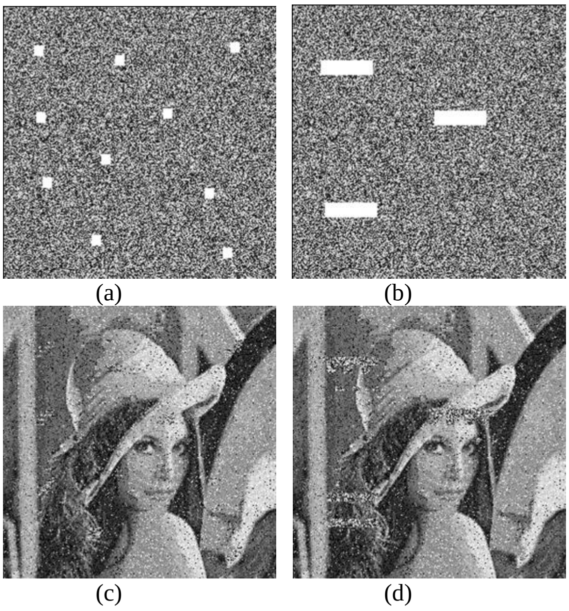


Fig 10: Decrypted Lena image with cropping attack

It is observed that the proposed method has acceptable resistance against cropping attacks, result is better when compared with the method in [1] and comparable with the result reported in [16].

6. CONCLUSION

In this paper, a new image encryption method is introduced based on pixels position permutation and random number using the notion of Z-Ordering and the BBS random bit generator. The obtained results of histogram and correlation coefficient prove the resistance of proposed method against statistical attacks. The NPCR value is greater than 99.5% and the UACI value approaches to 30%, and this confirms the resistance of differential attacks. The obtained entropy value is acceptable and near to the standard value 8 Sh. The proposed encryption method confirms is secure against additive noise and cropping attacks.

7. REFERENCES

[1] Adrian Viorel Diaconu and Khaled Loukhaoukha, “An improved secure image encryption algorithm based on Rubik’s cube principle and digital chaotic cipher”, Mathematical Problems in Engineering, Article ID 848392, vol. 2013, 2013, pp. 1-10.

[2] Alfred J.Menezes, Paul C.van Oorschot, and Scott A.Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 2010.

[3] Avi Dixit, Pratik Dhruve and Dahale Bhagwan “Image encryption using permutation and rotational XOR technique”, Computer Science & Information Technology, vol. 2, no. 3, 2012, pp. 01-09.

[4] C.E Shannon, “A mathematical theory of communications”, Bell Systems Technical Journal, vol. 27, no. 3, 1948, pp. 379-423.

[5] 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.

[6] C. K. Huang, C.W. Liao, S.L. Hsu and Y.C. Jeng, “Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system”, Telecommunication Systems – Springer, vol. 52, no. 2, 2013, pp 563-571.

[7] G. A Sathishkumar, K. Bhoopathy and R. Sriraam, “Image encryption based on diffusion and multiple chaotic maps”, International Journal of Network Security & its Applications, vol. 3, no. 2, 2011, pp. 181-194.

[8] 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.

[9] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos, Solutions and Fractals, vol. 21, no. 3, 2004, pp. 749–761.

[10] 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.

[11] Hongjun Liu, Xingyuan Wang, and Abdurahman kadir, “Image encryption using DNA complementary rule and chaotic maps”, Applied Soft Computing - Elsevier, vol. 12, no. 5, 2012, pp. 1457-1466.

[12] Jawad Ahmad and Fawad Ahmed, “Efficiency analysis and security evaluation of image encryption schemes”, International Journal of Video & Image Processing and Network Security, vol. 12, no. 04, 2012, pp. 18-31.

[13] Kamlesh Gupta and Sanjay Silakari, “New approach for fast color image encryption using chaotic map”, Journal of Information Security, vol. 2, 2011, pp. 139-150.

[14] 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, Article ID 173931, vol. 2012, 2012, pp. 1-13.

[15] Liang Zhao, Avishek Adhikari, Di Xiao, and Kouichi Sakurai, “On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption”, Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 8, 2012, pp. 3303-3327.

[16] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, “Image Encryption Using Fibonacci-Lucas Transformation”, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, pp. 131-141, September 2012.

[17] N.G Bourbakis, and C. Alexopoulos, “Picture data encryption using scan patterns”, Pattern Recognition, Volume 25, Issue 6, June 1992, Pages 567-581, ISSN 0031-3203.

[18] Narendra K Pareek, Vinod Patidar and Krishan K Sud, “Substitution-diffusion based Image Cipher”, International Journal of Network Security & its Applications (IJNSA), Vol.3, No.2, pp. 149-160, March 2011.

[19] Nikolaos G. Bourbakis, Chris Alexopoulos, “A fractal-based image processing language: formal modeling”, Pattern Recognition, Volume 32, Issue 2, February 1999, Pages 317–338.

[20] P. Vidhya Saraswathi and M. Venkatesulu, “A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal”, Journal of Computer Science, vol.8, no. 9, 2012, pp. 1541-1546.

[21] Qiang Zhang, Xianglian Xue, and Xiaopeng Wei, “A novel image encryption algorithm based on DNA subsequence operation”, The Scientific World Journal, vol. 2012, Article ID 286741, 2012, pp. 1-10.

[22] Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B, “Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping”, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.1, pp. 49-57, March 2012.

[23] Rasul Enayatifar, “Image encryption via logistic map function and heap tree”, International Journal of the Physical Sciences, vol. 6, no. 2, 2011, pp. 221-228.

[24] S. S. Maniccam and N. G. Bourbakis, “Image and video encryption using SCAN patterns”, Pattern Recognition Society, vol. 37, no. 4, 2004, pp. 725-737.

[25] William Stalling, Cryptography and Network Security – Principles and Practices, Pearson Education, New Delhi, 2013.

[26] Yue Wu, Joseph P. Noonan, and Sos Agaian, "NPCR and UACI randomness tests for image encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, pp. 31-38.

[27] Z. Lin and H. Wang, "Efficient image encryption using a chaos-based PWL memristor", IETE Technical Review, vol. 27, no. 4, 2010, pp. 318–325.