Image Encryption Based on Pixel Shuffling and Random Key Stream

T. Sivakumar
Department of Information Technology
PSG College of Technology
Coimbatore, Tamilnadu - 641 004, India
Email: sk {at} ity.psgtech.ac.in

R. Venkatesan
Department of Computer Science and Engineering
PSG College of Technology
Coimbatore, Tamilnadu - 641 004, India

Abstract— **Secured data storage and transmission has become an important issue in the digital world due to the increased use of Internet for communication purposes. Information security is becoming more important as the amount of sensitive data being exchanged on the Internet increases. The services like confidentiality and data integrity are required to protect data against unauthorized usage and modification. In recent years, several image encryption methods are introduced by various researchers to secure multimedia information while transit via public networks. A novel image encryption method based on pixels position permutation and random key stream is suggested in this paper. The pixels position permutation is done based on Hilbert Curve (HC). The pixel shuffled image is XORed with random key stream constructed by adopting the random bit pattern procedure used in the MD5 hash function to obtain the cipher image. The results confirm that the proposed method resists the statistical and differential attacks. Also attains acceptable entropy value, good key sensibility and secure against additive noise and cropping attacks.**

Keywords-Image encrytption; Pixel permutation; Hilbert Curve; Random key stream; Hash funciton

I. INTRODUCTION

Cryptography is the art of achieving security by encrypting messages to make them non-readable at the sender's side and decrypting the messages at the receiver's side to obtain the original information. IBM introduced an algorithm named, Data Encryption Standard (DES) which was initially used for the encryption of electronic data and it is now considered to be insecure because of brute force attack. The Advanced Encryption Standard (AES) proposed by Daemen and Rijmen is a symmetric key algorithm for fixed block size of 128-bits and key size of 128,192 or 256 bits. The International Data Encryption Algorithm (IDEA) designed by James Massey is a symmetric key algorithm which operates on 64-bit block using 128-bit key [28]. The conventional and pioneer encryption algorithms such as DES, IDEA, and AES are efficient when the volume of input data is small. These algorithms are widely used to encrypt text messages and not desirable to encrypt images. The volume of data that represent an image is always greater than textual messages and the traditional algorithms takes long time to encrypt digital images. Image encryption is widely used in multimedia communication, medical imaging, telemedicine and military communications where time is critical [1, 22].

Unlike text messages, 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. An image is created by arranging the bits, pixels and blocks in a suitable manner. The correlation among the bits, pixels and blocks in a given arrangement provides the intelligible information present in the image [2]. Thus, the image encryption methods should focus on reducing the correlation among the bits, pixels, and blocks to protect the encrypted images from cryptanalysis; also it should involve less time.

The primary types of image encryption methods based on permutation are classified as bit permutation [3, 4], pixel permutation [5, 6, 7, 8, 9, 10, 11, 12, 13], and block permutation [1, 14, 15, 25]. In the case of bit permutation, the bits of each pixel obtained from the image are permuted with the key generated by using pseudorandom index generator. In pixel permutation, the pixels position of the original image is rearranged using key of size same as the size of the image. In block permutation, the image is divided into chunk of blocks and these blocks are permuted based on random key. Better encryption result can be obtained with blocks of smaller size.

The hash algorithms such as MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are frequently used to convert the variable size input into fixed size output. A hash function is defined as the mapping of bit strings of an arbitrary finite length to strings of fixed length [17, 18]. Abbas Cheddad et. al. [17] proposed a method of encrypting digital images with password protection using SHA-2 hash algorithm coupled with Fourier Transform and XOR operation. S.M Seyedzade et. al. [18] presented an image encryption algorithm based on SHA-512 hash function. The SHA function is used to construct an encryption mask of size half the original image size and this mask is used to encrypt digital images.

In this paper, a novel approach for image encryption using scan based pixels position permutation and random key stream is proposed. The pixel permutation is achieved with the notion of Hilbert Curve (HC) based scan, which is conventionaly used in spatial, text, and multimedia databases to implement one-dimensional index and search on multi-dimensional data. The random key stream is created from the randomized bit pattern generation method used in MD5 hash function. The

proposed method has an improved security over unauthorized disclosure.

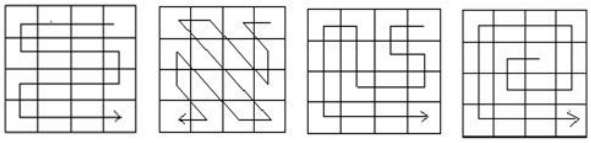
The rest of the paper is organized as follows. Section 2 outlines the basic concepts used in the proposed method. Section 3 describes the proposed image encryption method. Section 4 gives the experimental results and Section 5 presents the performance and security analysis. The conclusion is given in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

II. PRELIMINARY

After having described the introduction and organization of the paper, to begin with an overview of certain topics is presented in this section. This will serve as a background and preamble of the concepts used in the proposed method.

A. 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 [13]. 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 [11, 12]. The scan language uses four basic scan patterns such as continuous raster (C), continuous diagonal (D), continuous orthogonal (O), and spiral (S) as shown in Fig. 1.

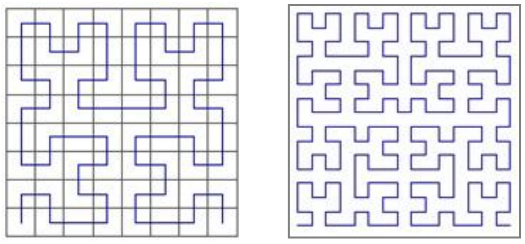


(a) Raster (b) Diagonal (c) Orthogonal (d) Spiral

Figure 1. Basic scan patterns

A. Hilbert Curve

The concept of Hilbert Curve (HC) is used in spatial, text, and multimedia databases to implement one-dimensional index and search on multi-dimensional data. The key idea of the proposed method is to introduce a new method of 2-D array accessing patterns with the notion of HC. This scan pattern is used rearrange the pixels position of the plain image to obtain the scrambled version of the original image. The structure of HC corresponding to the dimensions 8 x 8 and 16 x 16 are shown in Fig. 2.



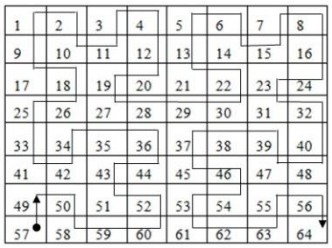
(a) Hilbert Curve of order 8 (b) Hilbert Curve of order 16

Figure 2. Illustrative for Hilbert Curve

There are four possible points to start the scanning process in a Hilbert Curve, and they are considered as Left Bottom (LB), Left Top (LT), Right Bottom (RB), and Right Top (RT). In the proposed method, pixels position permutation is performed by the above scan technique.

B. Proposed Pixel Position Permutation

To describe the proposed scan pattern, let us consider the Hilbert Curve of order 8 as shown in Fig. 3(a) with the starting point LB. The equivalent scan coordinate is shown in Fig. 3(b). The original 8x8 image matrix is shown in Fig. 3(c) and the corresponding scrambled image matrix obtained by applying the scan pattern is shown in Fig. 3(d).



(a) Hilbert Curve (HC)

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

(b) Scan coordinate

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 image matrix

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

(d) Pixel permuted image matrix

Figure 3. Proposed pixel permutation

From the above illustration, it is observed that the pixel elements are shuffled for an acceptable level. For easy visual testing of pixel shuffling, the original image pixels value is taken as continuously.

C. Role of Random Numbers in Cryptography

Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs) are the two main approaches to generation of random numbers [28]. 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 against computationally limited adversaries (www.random.org).

A hash function (H) converts a variable-length block of data M into an output of fixed-size hash value h = H(M). A change to any bit or bits in M results, with high probability, in a change to the hash code. The hash functions satisfy the features like (a) pre-image resistance (one-way property) (b) second pre-image resistant (weak collision resistant), and (c) Collision resistant (strong collision resistant) [18, 28].

The MD5 hash function takes as input a message of arbitrary length and produces as output a 128-bit message digest. It has 64 rounds and each round makes use a randomized 32-bit pattern T_i, where $0 \leq i \leq 63$, which has value equal to the integer part of 2^{32} x abs(sin(i)), where 'i' is in radians. These bit patterns are used to provide a randomized set of 32-bit patterns to eliminate any regularity in the input data [28]. Due to the randomness, this technique is adopted by the proposed method to generate random key stream to enforce the security. In the proposed method, the technique is modulated such that the random key stream is derived from the fractional part of the output of sine function.

III. PROPOSED IMAGE ENCRYTION METHOD

The proposed method uses scan based pixels position permutation to scramble the plain image and random key stream to change the pixel values. The structure of Hilbert Curve (HC) is adopted as scan pattern to rearrange the pixels position. The randomized bit pattern generation method used in the MD5 hash function is used to produce random key stream. The working model of proposed image encryption method is shown by using a flowchart in Fig. 4.

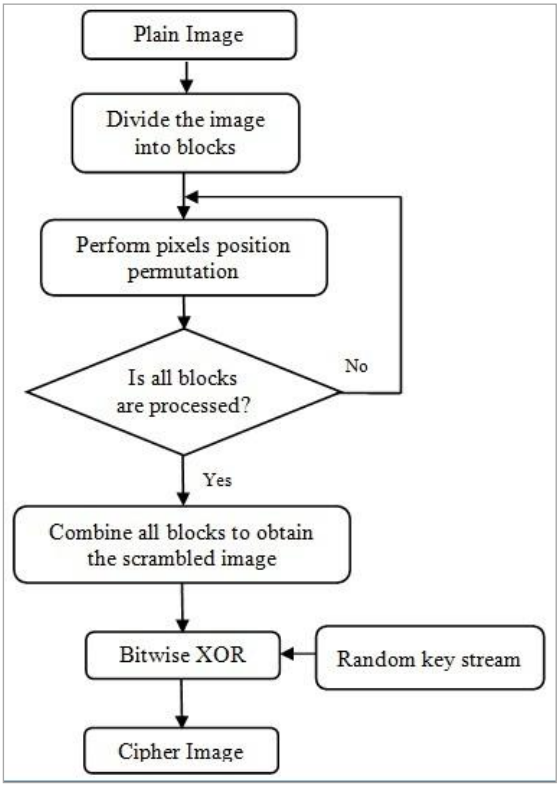


Figure 4. Proposed image encryption method

Initially, the plain image is divided into blocks of size b x b pixels, where 'b' is the order of the chosen Hilbert Curve (HC), and then permutation of pixels position is done on each block with respect to the HC pattern. The pixel shuffled image is XORed with random key stream to obtain the encrypted image. The detailed discussion of random key stream generation process is presented in section 3.2. The encryption key consists of the components, namely, the order of the Hilbert Curve with starting coordinate and the random key stream. These key components are known and securely shared only between sender and receiver.

A. Encryption Algorithm

The algorithm to convert the plain image into encrypted image is presented in this section. The following are the sequence of steps to be followed for encryption.

Input : Plain Image, Order of the Hilbert Curve
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 order of Hilbert Curve (b) and generate the corresponding scan coordinate.
Step 3: Divide the plain image into blocks of size b x b pixels.
Step 4: Perform pixels position permutation on each block.
Step 5: Repeat step 4 until all blocks are processed.
Step 6: Combine all blocks to obtain the scrambled image.
Step 7: Generate random key stream by using the function given in section III-B.
Step 8: Perform bitwise XOR operation between the scrambled image obtained in step 6 and the random key stream generated in step 7 to obtain the cipher image.
Step 9: Store the cipher image.

B. Generation of Random Key Stream

The randomized bit pattern generation method used in the MD5 hash function is adapted to construct a random key stream of length 5,24,288 bits, which converted into 65,536 random numbers each of size 8 bits. To achieve this, the fractional part of output of sine function is converted into binary stream. From the binary stream, the MSB 64 bits are considered to generate eight random numbers by using following sequence of steps:

Algorithm: Random_Key_Stream()

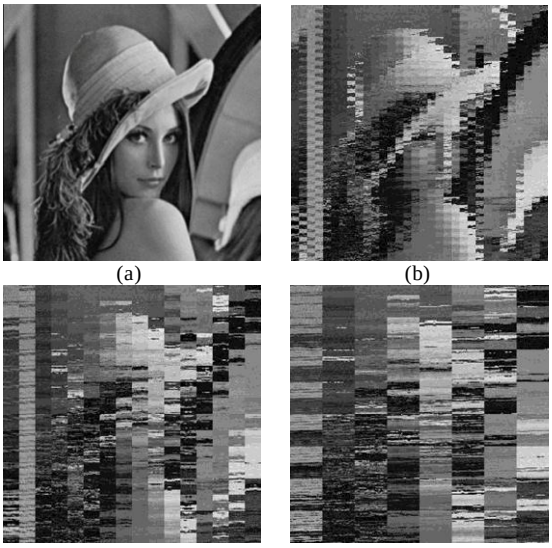
Step 1: Input the random number range (n x n), where 'n' is the order of the plain image.
Step 2: Input the initial input (seed) value.
Step 3: Let Random[n][n] be the array to store the random numbers.
Step 4: Temp ← abs(sin(seed)); and Increment seed;
Step 5: Convert the fractional part of the value of Temp into binary stream.
Step 6: Use the 64 most significant bits of the binary stream to create eight stream each of size 8 bits as follows:
6.1 B_1←bits 63 - 56, B_2←bits 55 - 48,
6.2 B_3←bits 47 - 40, B_4←bits 39 - 32
6.3 B_5←bits 31 - 24, B_6←bits 23 - 16,
6.4 B_7 ←bits 15 - 8, B_8←bits 7 - 0
Step 7: Eliminate the bit stream which contains all zeroes.
Step 8: Convert each 8 bit stream as integer and store the numbers in the array Random[][].

Step 9: Repeat steps 4 to 8 until sufficient random numbers are generated.
Step 10: Return the content of the array Random[][].

The test images considered for experimental analysis are of size 256 x 256 pixels, and hence the chosen value of 'n' is 256.

IV. Implementation And Visual Results

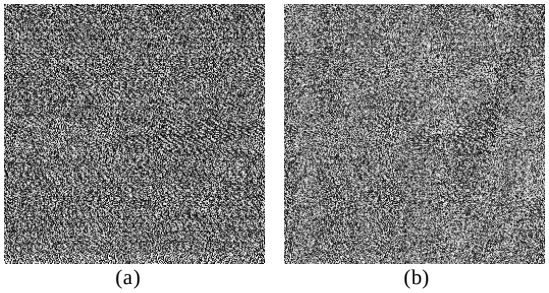
The proposed method is implemented using Matlab 2010a with P-IV Processor, 2.80 GHz, 2 GB RAM, 160 GB HDD, and Windows (32 bit) operating system. The experimentation is done with standard gray-scale test images Lena, Baboon, Cameraman, and Peppers. The assumed Hilbert Curve (HC) dimensions considered for implementation are 8, 16, and 32. The implementation result of proposed image encryption method is presented by using the Lena image for visual observations in Fig. 5. From the result, it is seen that increasing the dimension of HC leads to better shuffling (permutation) result.



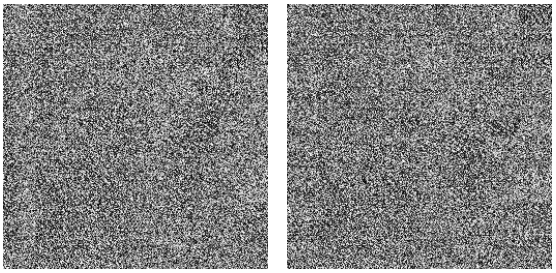
(a) (b) (c) (d)

Figure 5. Result of proposed pixel permutation: (a) Original image, Pixel permuted images of (b) Order 8 x 8, (c) Order 16 x 16 (d) Order 32 x 32

The sample constructed random key stream is shown in Fig. 6(a) and the encrypted images corresponding to HC order 8, 16, and 32 are shown in Fig. 6(b) – (d). The chosen seed value of random number generator is 0.01 with the seed is incremented by 0.3 after each iteration. The encrypted images confirm the effectiveness of the proposed random key stream generation method.



(a) (b)



(c) (d)

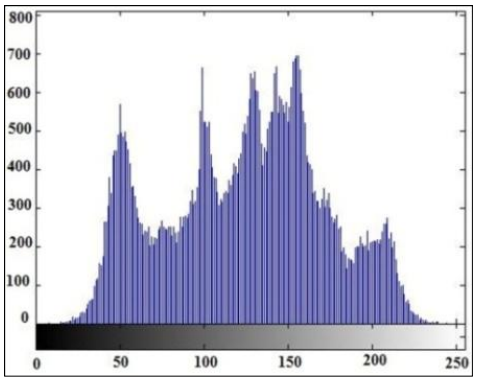
Figure 6. Results of proposed method: (a) Random key stream, Encrypted images of (b) Order 8 x 8, (c) Order 16 x 16, (d) Order 32 x 32

V. Performance And Security Analysis

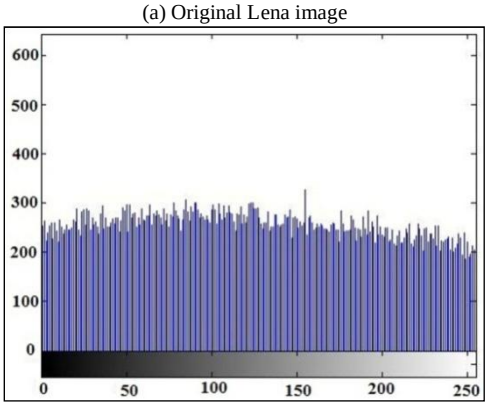
In order to quantify the security level of the proposed method, the image encryption algorithm evaluation parameters like histogram, correlation coefficient, entropy, NPCR, and UACI are computed, compared with few existing image encryption methods and analyzed.

A. Histogram Analysis

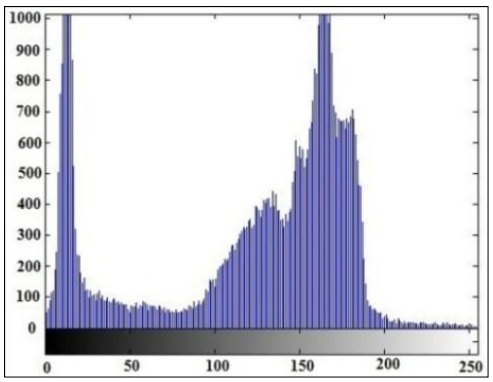
An image histogram is a graphical representation of the number of pixels in an image as a function of their intensity values. Image histogram is a measure for inspecting the difference between the original and encrypted images visually at pixel level. The histogram of the original images and the corresponding encrypted images are shown in Fig. 7.



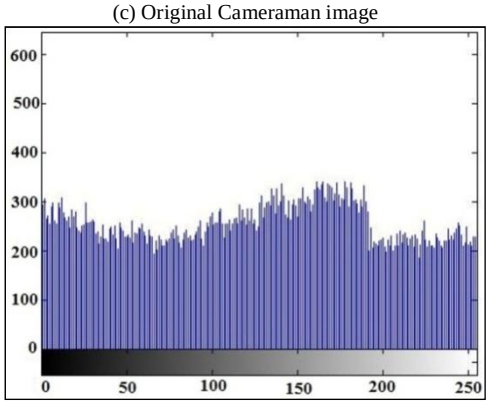
(a) Original Lena image



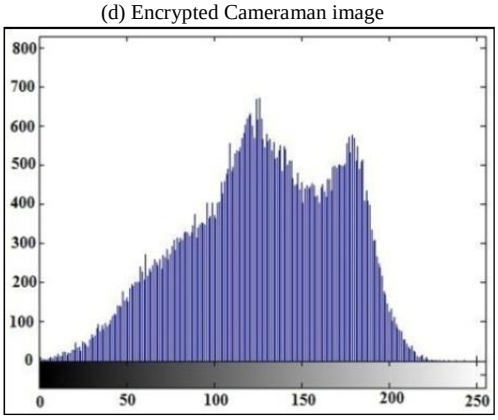
(b) Encrypted Lena image



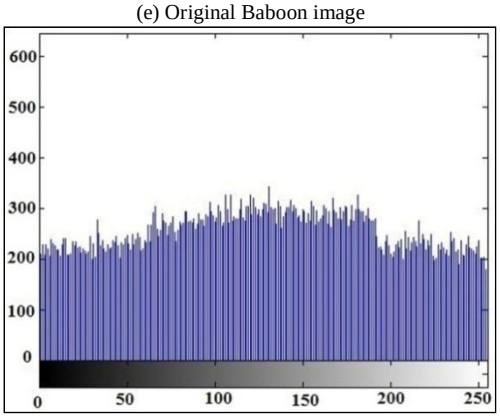
(c) Original Cameraman image



(d) Encrypted Cameraman image



(e) Original Baboon image



(f) Encrypted Baboon image

Figure 7. Histogram of original and encrypted images

From result, it is seen that the histogram of the encrypted image is flat and this demonstrates the effectiveness of the proposed image encryption method. Thus, the proposed method resists statistical attacks based on analysis of histogram.

B. Correlation Analysis

The correlation coefficient is a useful measure to determine the degree of relationship between the original and cipher images and also between the adjacent pixels of the encrypted image. The correlation is measured and analyzed to confirm the resistance level of the proposed method against statistical attacks. The correlation coefficient can be mathematically calculated by using the equation (1).

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

Where, γ_{xy} is the correlation coefficient and Cov(x, y) is the covariance of x and y and is represented as,

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

$$\mathbf{E(x)} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (3)$$

$$\mathbf{D(x)} = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2 \qquad (4)$$

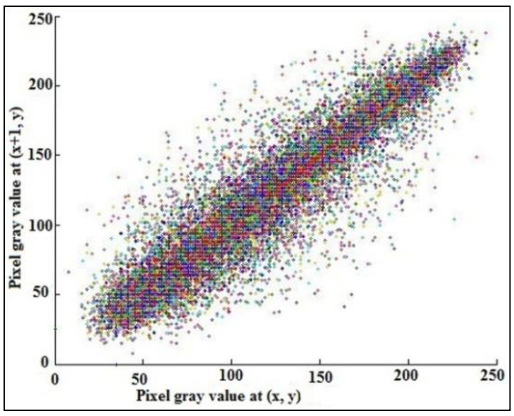
Where, E(x) and D(x) are the mean and standard deviation of the corresponding gray-scale values and N is the number of pixel pairs. The result attained by proposed method and few existing methods are given in Table I.

Table I. COMPARISON OF ADJACENT PIXEL CORRELATION

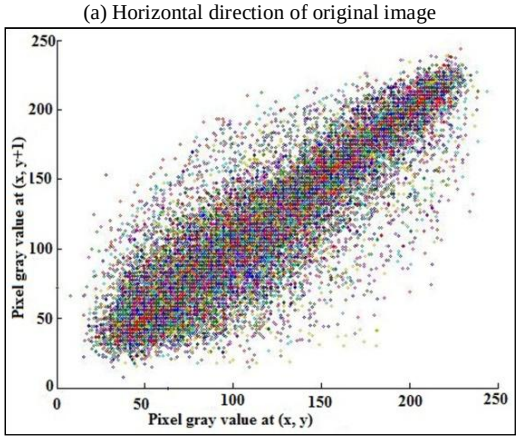
Encryption Method	Directions		
	Horizontal	Vertical	Diagonal
Proposed	0.0045	0.0073	0.0241
Khaled Loukhaoukha et. al. [6]	0.0068	0.0091	0.0063
C.K. Huang et. al. [8]	−0.0025	−0.0006	−0.0050
H.T Panduranga et. al. [9]	0.0263	0.0163	0.0114
P. Vidhya Saraswathi et. al. [14]	0.01776	0.04912	0.00348
S. V. Sathyanarayana et. al. [16]	-0.0027	-0.0028	0.0026
Abbas Cheddad et. al. [17]	-0.0028	-0.0068	-0.0044
Seyedzade S.M et. al. [18] (R=2)	-0.0006	-0.0030	-0.0061
M. Zeghid et. al. [22]	0.036	0.035	Not reported
Narendra K Pareek et. al [24]	0.0083	-0.0162	0.0078

The obtained correlation value between the adjacent pixels of the encrypted image is close to zero and is optimal. It is observed that the result of the proposed method is better than the methods in [6, 9, 14, 22, 24] and comparable to those methods in [8, 16, 17, 18].

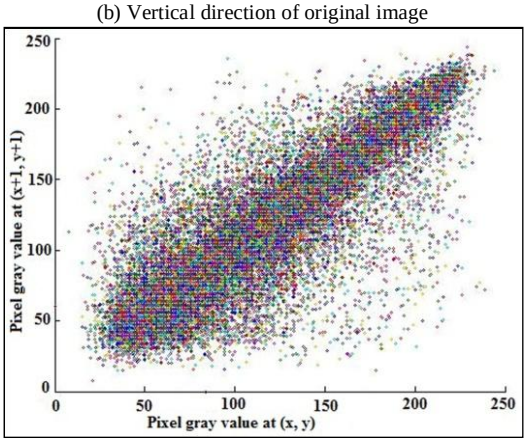
The graphical view of correlation between adjacent pixels of the original and encrypted Lena images in the horizontal, vertical, and diagonal directions are shown in Fig. 8(a) - 8(f).



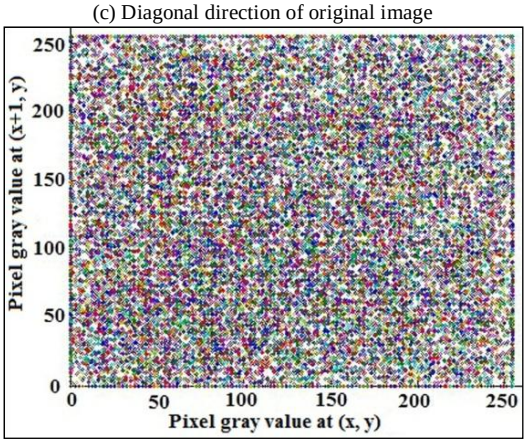
(a) Horizontal direction of original image



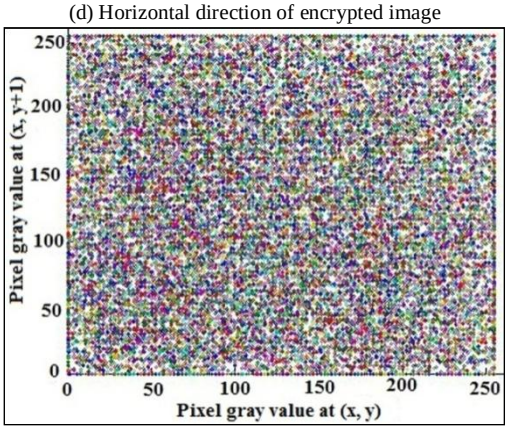
(b) Vertical direction of original image



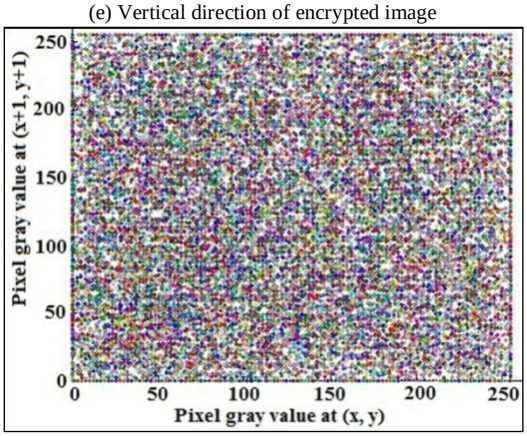
(c) Diagonal direction of original image



(d) Horizontal direction of encrypted image



(e) Vertical direction of encrypted image



(f) Diagonal direction of encrypted image

Fig. 8. Adjacent pixel correlation distribution

The result shows that the relationship between adjacent pixels of the encrypted image is reduced and hence the proposed method resists the statistical attacks based on analysis of correlation between adjacent pixels.

The cross correlation is measured to find the relationship between the original and the encrypted images. The cross correlation value obtained by the proposed method and some of the existing methods are presented in Table II. Result shows that the relationship between the original image and the corresponding encrypted image is very low and significantly matches with the existing methods.

Table II. COMPARISON OF CROSS CORRELATION

Encryption Method	Correlation value
Proposed	0.0366
H.T Panduranga et. al. [9]	-0.0073
G.A Sathishkumar et. al. [21]/A-I	-0.0535
G.A Sathishkumar et. al. [21]/A-I & A-II	0.0074
Narendra K Pareek et. al. [24]	0.0211

C. Information Entropy

Information entropy measurement is an important parameter to analyze image encryption methods. The entropy of a source gives the information provided by a random

process about itself. Entropy is a measure of the uncertainty in a random variable and it shows the degree of uncertainties in any communication system. Thus, entropy is used to quantify the expected amount of the information contained in a message [29, 30]. The entropy, H(m), of any message can be calculated by using the equation (5).

$$\boldsymbol{H(m) = \sum_{i=0}^{m-1} p(mi) log\ (1/p(mi))} \quad (5)$$

Where, $p(m_i)$ represent the probability of occurrence of the symbol m_i in the message. The entropy value obtained by the proposed method and few existing methods are compared and given in Table III.

TABLE III. COMPARISON OF INFORMATION ENTROPY

Encryption Method	Encrypted Image (Sh)
Proposed	7.9924
G.A Sathishkumar et al. [5]	7.8101
Khaled Loukhaoukha et al. [6]	7.9968
C.K. Huang et. al. [8]	7.9967
S. V. Sathyanarayana et. al. [16]	7.9996
D. Bouslimi et. al. [19]	7.9995
M. Zeghid et. al. [22]	7.9100
Narendra K Pareek et. al [24]	7.9996
Rakesh S et. al. [25]	7.9993

It is found that the result obtained by the proposed method is near to 8 Sh and acceptable. The obtained result is better than those methods in [5, 22] and comparable to the methods in [6, 8, 16, 19, 24, 25].

D. Visual Testing

The visual testing is employed to confirm the security level against the differential attacks. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two measures used to quantify the visual difference between two 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 [6, 26, 27].

1) Number of Pixel Change Rate (NPCR)

The Number of Pixel Change Rate (NPCR) is defined as the variance rate of pixels between two images. By considering two images $I_1(i, j)$ and $I_2(i, j)$, an array D(i, j) is defined as follows. D(i, j) is equal to 0, if $I_1(i, j) = I_2(i, j)$, else D(i, j) = 1. If both images are same then the output is equal to zero else equal to one. The result is optimal when it is beyond 99.5% [27]. The NPCR value is calculated by using the mathematical formula given in the equation (6).

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

Where, W and H are the width and height of the images. The obtained NPCR value between the original and encrypted images is given in Table IV.

TABLE IV. COMPARISON OF NPCR VALUE

Encryption Method	NPCR Value (%)
Proposed	99.5468
G.A Sathishkumar et. al. [5]	98.4754
Khaled Loukhaoukha et. al. [6]	99.5850
C. K. Huang et. al. [8]	99.5400
P. Vidhya Saraswathi et. al. [14]	99.8500
Abbas Cheddad et. al. [17]	99.6113
A. Umamageswari et. al. [20]	99.8500
Narendra K Pareek et. al. [24]	99.4600

It is clearly seen that the obtained NPCR values are greater than 99.5% and optimal. It is observed that the proposed method provides better NPCR value when compared with those methods in [5, 8, 24], comparable with the methods in [6, 17], and slightly lower than the methods in [14, 20].

2) Unified Average Changing Intensity (UACI)

The Unified Average Changing Intensity (UACI) determines the average intensity difference between two images. NPCR concentrates on the absolute number of pixels which changes value in differential attacks, while the UACI focuses on the averaged difference between two images. The value is optimal when it is around 33% [27]. The UACI is computed by using the formula given in the equation (7).

$$\mathbf{UACI} = \frac{1}{\boldsymbol{W*H}} \left[\sum_{i,j} \frac{\mathbf{I1}(i,j) - \mathbf{I2}(i,j)}{255} \right] \mathbf{* 100\%} \quad (7)$$

Where, $I_1(i,j)$ and $I_2(i,j)$ are two images, W and H are the width and height of the images. The calculated UACI value between the original image and cipher image and a comparison with existing methods is given in Table V. It is found that the values are close to 29% and significantly match with the optimal value.

TABLE V. COMPARISON OF UACI VALUE

Encryption Method	UACI Value (in %)
Proposed	28.8065
G.A Sathishkumar et. al. [5]	32.2128
Khaled Loukhaoukha et. al. [6]	28.6210
C. K. Huang et. al. [8]	28.2700
P. Vidhya Saraswathi et. al. [14]	33.5800

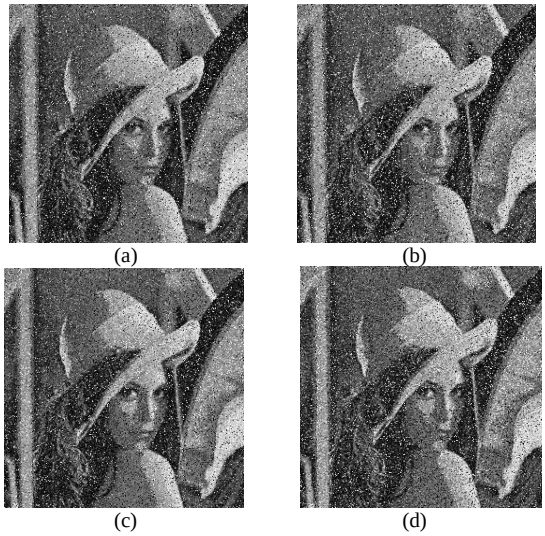
It is observed that the UACI value attained by the proposed method is better than the methods in [6, 8] and lower than those methods in [5, 14]. The results of NPCR and UACI signify that the proposed method significantly resists the differential attacks.

E. Noise Attack Analysis

The attackers or intruders may introduce cropping and additive noise 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. Thus, the proposed method is tested with additive noise and cropping attacks.

1) Additive Noise Attack

An additive noise attack consists in adding random noise to the intercepted encrypted image [7]. The additive noise attack is tested by using salt and pepper noise and speckle noise to confirm the security against this attack. The decrypted Lena image with additive noise attack is shown in Fig. 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.



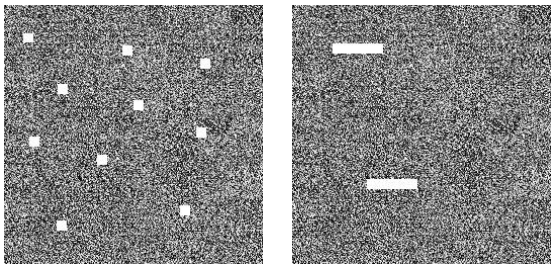
(a) (b) (c) (d)

Figure 9. Decrypted Lena Images after Additive Noise Attack

From the results, it is found that the proposed method has good resistance against additive noise attacks. Also, better result is obtained when compared with the result reported in [7] for high density and variance of salt and pepper and speckle noises and comparable with the method in [23].

2)Cropping Attacks

The cropping attacks consist of modifying the intercepted cipher image by destroying few regions [7]. The cropping attack is tested with the encrypted Lena image after removing 10 regions each of size 10x10 pixels and two region of 50x10 pixels as shown in Fig. 10(a) and 10(b). The corresponding decrypted images are shown in Fig. 10(c) and 10(d). The decrypted images are significantly distorted and could be recognized as a Lena image.



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

Figure 10. Decrypted Lena image after cropping attack

From the results, it is observed that the proposed method assures acceptable resistance against cropping attack, result is better than the method suggested in [7] and comparable with the result reported in [23].

6. Conclusion

In this paper, a new image encryption method is introduced based on pixels position permutation and random key stream. The pixels position permutation is done based on the novel implementation of Hilbert Curve. The constants generation method used in the MD5 hash function is adopted to generate random key stream. The result of histogram and correlation coefficient proves the resistance of statistical attacks. The NPCR value is greater than 99.5% and the UACI value is near to 29% respectively, and confirms the resistance of proposed method against differential attacks. The obtained entropy value is acceptable and near to the standard value 8 Sh. The proposed encryption method is very sensitive for the encryption key and is secure against additive noise and cropping attacks.

References

[1] Han Shuihua and Yang Shuangyuan, "An asymmetric image encryption based on matrix transformation", *ECTI Transactions on Computer and Information Technology*, Vol. 1, No. 2, pp126-133, 2005.

[2] M. Francois, T. Grosges, D. Barchiesi and R. Erra, "A new image encryption scheme based on a chaotic function", *Signal Processing: Image Communication*, Vol.27, No. 3, pp249-259, 2012.

[3] Fu Chong, Lin Bin-Bin, Miao Yu-Sheng, Liu Xiao, and Chen Jun-Jie, "A novel chaos-based bit-level permutation scheme for digital image encryption", *Optics Communications*, Vol. 284, No. 23, pp5415-5423, 2011.

[4] 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, pp3303-3327, 2012.

[5] 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, pp169-178, 2011.

[6] 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*, Vol. 20, No. 12, pp1-13, 2011.

[7] 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*, Vol. 2013, pp1-10, 2013.

[8] 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*, Vol. 52, pp563–571, 2013.

[9] H.T Panduranga and S.K Naveen Kumar, "Hybrid approach for image encryption using SCAN patterns and carrier images", *International Journal on Computer Science and Engineering*, Vol. 2, No. 2, pp297-300, 2010.

[10] K. Usman, H. Juzoji, I. Nakajima, S. Soegidjoko, M. Ramdhani, T. Hori and S. Igi, "Medical image encryption based on pixel arrangement and random permutation for transmission security", *IEEE Conf. on e-Health Networking, Application and Services*, Taipei, 19-22 June 2007, pp244-247.

[11] N. G Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns", *Pattern Recognition*, Vol. 25, No. 6, pp567-581, 1992.

[12] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou, "Image encryption method using a class of fractals", *Journal of Electronic Imaging*, Vol. 4, No. 3, pp251-259, 1995.

[13] S.S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns", *Pattern Recognition*, Vol. 37, No. 4, pp725-737, 2004.

[14] 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, pp.1541-1546, 2012.

[15] Patidar Vinod, N. K Pareek, G Purohit, and K.K Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", *Optics Communications*, Vol. 284, No. 19, pp.4331-4339, 2011.

[16] S. V. Sathyanarayana, M. Aswatha Kumar and K. N. Hari Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points", *International Journal of Network Security & its Applications*, Vol.12, No.3, pp.137-150, 2011.

[17] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "A hash-based image encryption algorithm", *Journal of Optics Communications*, Vol. 283, No. 6, pp.879-893, 2010.

[18] Seyedzade S.M, Mirzakuchaki S and Atani R.E, "A novel image encryption algorithm based on hash function", *Machine Vision and Image Processing*, 27-28 Oct. 2010, Iranian - Isfahan, pp.1-6.

[19] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 5, pp.891-899, 2012.

[20] A.Umamageswari and G.R.Suresh, "Security in medical image communication with Arnolds cat map method and reversible watermarking", *IEEE Int. Con. on Circuits, Power and Computing Technologies*, 20-21 March 2013, India, pp.1116–1121.

[21] 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, pp.181-194, 2011.

[22] M. Zeghid, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption", *International Journal of Computer, Information, Systems and Control Engineering*, Vol. 1, No. 3, pp.526-531, 2007.

[23] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, "Image encryption using fibonacci-lucas transformation", *International Journal on Cryptography and Information Security*, Vol.2, No.3, pp.131-141, 2012.

[24] Narendra K Pareek, Vinod Patidar and Krishan K Sud, "Substitution-diffusion based Image Cipher", *International Journal of Network Security & its Applications*, Vol.3, No.2, pp.149-160, 2011.

[25] 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*,Vol.2, No.1, pp.49-57, 2012.

[26] 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. 4, pp.18-31, 2012.

[27] 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, pp.31-38, 2011.

[28] William Stallings, "*Cryptography and Network Security"*, Prentice Hall, 2005.

[29] Alfred J.Menezes, Paul C.van Oorschot, and Scott A.Vanstone, "*Handbook of applied cryptography"*, CRC Press, 2010.