Asian Journal of Information Technology 15 (22): 4635-4647, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

A New Image Encryption Method Using Scan Pattern and Random Key Stream

[1]T. Sivakuma and [2]T. Anusha
[1]Department of Information Technology,
[2]Department of Computer Science and Engineering, PSG College of Technology,
Coimbatore, 641004 Tamil Nadu, India

Abstract: The amount of digital data transmitted across the network has been increased due to the advancement in internet technologies. The exchange of sensitive and confidential multimedia data via internet necessitates a demand for secure transmission. The conventional encryption algorithms used to encrypt text data are not desirable to encrypt multimedia data. This study proposes a new image encryption method using scan pattern based pixel permutation and bitwise XOR operation using random key stream. The new scan pattern for pixel permutation is derived from the concept of rat-in-a-maze. The proposed random key stream to perform bitwise XOR operation is generated by adapting the randomized bit pattern generation method used for the SHA-512 hash function. The proposed method resists statistical, differential, ciphertext-only and known plaintext attacks. It has sufficient key space to resist exhaustive key search attack and attains optimal entropy value. The NIST randomness test assured that the proposed random key stream contains random bits for effective encryption.

Key words: Image encryption, scan pattern, Rat-in-a-maze, random key stream, hash functio

INTRODUCTION

Internet provides an essential communication for people in the world to share all kinds of information and security becomes an important issue during transmit. Data security is the way of protecting the information from unresearcherized disclosure and usage (Stallings, 2013; Menezes *et al*., 2010). The number of images uploaded and downloaded per day in social networks for education, business, advertisements and entertainment purposes is approximately several millions (Aggarwal, 2011). A broad availability of digital devices like digital cameras, scanners, mobile phones, notebooks at reasonable prices accelerate the growth of multimedia content production (Zare *et al*., 2013). Encryption of images is different from text data due to the large size of images and it takes more time to encrypt digital images. The conventional algorithms used to encrypt text messages are not compatible to encrypt digital images (Chang *et al*., 2001; Chen *et al*., 2004).The correlation among the bits, pixels and blocks in a given arrangement provides the intelligible information present in the image (Francois *et al*., 2012). Thus, image encryption methods should reduce the correlation among the bit, pixel and block level to protect the encrypted image from statistical and differential attacks. Image encryption methods based on permutation are classified as bit permutation (Fu *et al*., 2011; Zhao *et al*., 2012), pixel permutation (Sathishkumar *et al*., 2011; Loukhaoukha *et al*., 2012; Huang *et al*., 2013; Panduranga and Naveenkumar, 2010; Usman *et al*., 2007; Bourbakis and Alexopoulos, 1992; Alexopoulos *et al*., 1995; Maniccam and Bourbakis, 2001, 2004) and block permutation (Patidar *et al*., 2011). In bit permutation, the bits of each pixel of the image are permuted with the key generated by using pseudorandom index generator In pixel permutation, the pixel position of the image is permuted using key of size same as the length of the image. In block permutation, the image is divided into blocks and these blocks are permuted based on random key. In this study, a new image encryption method using pixel permutation and bitwise XOR operation is introduced.

Literature review: Chen *et al*. (2004) generalized the two-dimensional chaotic cat map to 3D for designing a real-time secure symmetric encryption scheme. The method employs the 3D cat map to shuffle the pixel position and uses another chaotic map to confuse the relationship between the original and encrypted images. Francois *et al*. (2012) presented an image encryption scheme by coupling the chaotic function and XOR operator. This method has large key space and satisfying

Corresponding Author: T. Sivakuma, Department of Information Technology, PSG College of Technology, Coimbatore, 641004 Tamil Nadu, India

the confusion and diffusion properties. Fu *et al.* (2011) presented a chaos-based bit permutation scheme for image ciphering through two-stage bit-level shuffling algorithm using chaotic sequence sorting algorithm and Arnold Cat map. Usman *et al.* (2007) described the utilization of pixel arrangement and random permutation to encrypt medical images with high speed computation. The pixel permutation method particularly does not require any mathematical manipulation and this is especially useful for medical image where the image is very big (Usman *et al.*, 2007).Bourbakis and Alexopoulos (1992) developed an image encryption method based on the principles of scan language to encrypt 2D digital images. Alexopoulos *et al.* (1995) presented a cryptographic scheme for encrypting 2D gray-scale images by using fractals. This scheme is based on a transposition of the image elements implemented by a generator of 2D hierarchical scanning patterns. Patidar *et al.* (2011) presented a robust chaos-based pseudorandom permutation substitution scheme for image encryption. The permutation process depends on the input image and controlled by pseudo random numbers.

Sathyanarayana *et al.* (2011) introduced an image encryption scheme with key sequence derived from the random sequence of elliptic curve points. This scheme utilized the properties of Finite Fields and elliptic curves to design a stream cipher. Hung *et al.* (2013) presented a cryptographic system for enhancing medical image security by using chaotic amplitude phase frequency model nonlinear adaptive filter. Bouslimi *et al.* (2012) introduced a joint encryption/water-marking system to protect medical images by using the combination of substitutive watermarking algorithm and the stream cipher or a block cipher. The increasing need for telemedicine in healthcare industry created a necessity to secure the transmitted data among medical centers (Mahmood and Dong, 2011). Mahmood and Dony, (2011) applied the information theory to identify the Region of Interest (ROI) and the Region of Background (ROB) of a medical image to develop a hybrid image encryption method. The Advanced Encryption Standard is applied for ROI and the Gold Code (GC) coding method is applied for the ROB to protect medical images.

Cheddad *et al.* (2010) described a new way of encrypting digital images with password protection using SHA-2 hash algorithm coupled with Fourier Transform and XOR operation. Seyedzade *et al.* (2010) introduced an image encryption algorithm based on SHA-512 hash function. The entropy of the encrypted image is increased and both security and performance aspects are satisfactory with two iterations. Pandey *et al.* (2012) presented an image encryption method using diffusion and confusion operations. The encryption method employed block based image transformation using shuffle exchange operation to shuffle the pixels of image and M box for chaotic confusion. Ye (2011) proposed a chaos-based image encryption scheme using permutation-diffusion mechanism. The generalized Arnold map is use to generate one chaotic orbit to get two index order sequences for pixel permutation. In the diffusion process, a generalized Arnold map and a generalized Bernoulli shift map are employed.The main features of chaotic systems are sensitivity to initial conditions, ergodicity, mixing property, simple analytic description and high complex behavior. Cryptography works with integer values on finite fields but chaos works with continuous values using fixed or floating point representation. In digital chaos based cryptography the encryption procedure is performed in discrete time and discrete space but the underlying chaotic system is defined in continuous domain. So, it is necessary to apply some numerical methods to obtain the chaotic orbits and this leads to increases the computation time (Arroyo *et al.*, 2009; Ozkaynak *et al.*, 2012; Alvarez *et al.*, 2011). The spatial domain schemes are generally faster but security level is little low, however the frequency domain schemes maintain good security performance.

Image encryption methods based on bit permutation, pixel permutation, block permutation and chaotic systems were studied extensively. From the literature review, it is found that there is a scope and demand to develop new image encryption methods. In this study, a new image encryption method using pixel permutation and bitwise XOR operation is introduced. The scan pattern for pixel permutation is derived from the concept of Rat-in-a-maze. The random key stream for bitwise XOR operation is generated by adapting the randomized bit pattern generation method as used for the SHA-512 hash function.

Preliminaries: This study will serve as a background and introduction of the basic concepts used in the proposed pixel permutation and random key stream generator.

Scan patterns: Image scanning is a formal language based 2D spatial accessing methodology which can represent and generate large number of scanning paths. Scanning of a two dimensional array is an order in which each element of the array is accessed exactly once (Bourbakis and Alexopoulos, 1992; Alexopoulos *et al.*, 1995; Maniccam and Bourbakis, 2001). The continuous raster, diagonal, orthogonal and spiral models shown Fig. 1a-d are the basic and widely used scan patterns for pixel permutation.

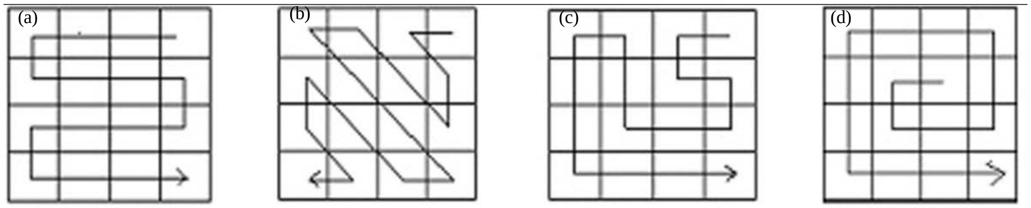
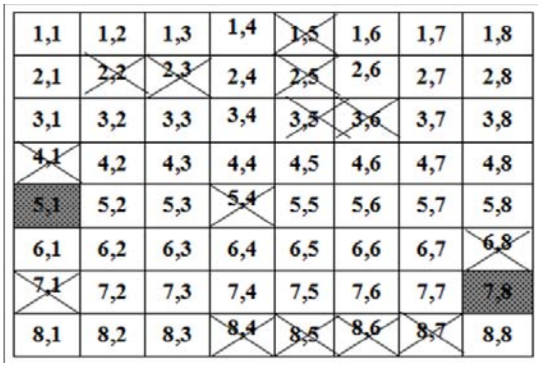


Fig. 1: Basic scan patterns: a) Raster; b) Diagonal; c) Orthogonal and d) Spiral



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

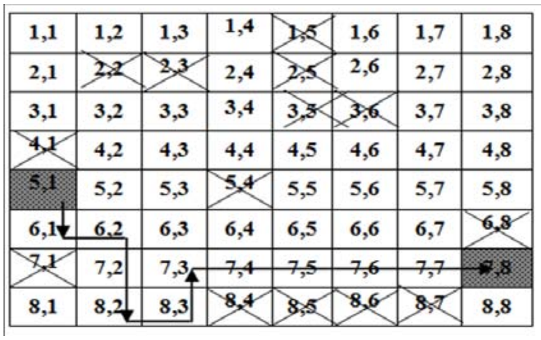
Fig. 2: Initial state of the maze

Proposed scan pattern generation: The key idea of the proposed image encryption method is to introduce new and simple scan patterns for pixel permutation. The scan patterns are generated from the notion of rat-in-a-maze which is a well-known backtracking problem in algorithm design. A maze is a rectangular area with single entry and exit points. The interior of the maze contains walls or obstacles that the rat cannot walk through. The traditional Rat-in-a-maze problem is used to find the travel path of the Rat from the entry point towards the exit point with least travel distance. In the proposed method, the problem is modulated such that the rat should visit maximum number of cells between the source and destination points to generate complex travel paths. This helps to create a pool of rat's travel path that visit many cells between the entry and exist points of the maze. From the pool of travel paths, one path is chosen to generate scan pattern.

To describe the scan pattern generation, consider a maze of order 8 which is represented as 8×8 matrix as shown in Fig. 2 with an assumed set of blocked cells (1,5), (2, 2), (2, 3), (2, 5), (3, 5), (3, 6), (4, 1), (5, 4), (6, 8), (7, 1), (8, 4), (8, 5), (8, 6) and (8,7). The chosen entry and exit points of the maze are at cells (5, 1) and (7, 8).

	3 (h-1, i)	
4 (h, i-1)	(h, i)	2 (h, i+1)
	1 (h+1, i)	

Fig. 3: Traversal priority initial state of the maze



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

Fig. 4: Travel path - I (cells visited: 10)

Priorities such as Bottom (1), Right (2), Top (3) and Left (4) are considered to visit the next cell from the current position as shown in Fig. 3. If the Rat is at (h, i) of the maze and the cells around (h, i) are not blocked, then there are four possible moves as per the principle. The first priority is given to the cell (h+1, i). If it is blocked or already visited, then the cell (h, i+1) is visited next. If both (h+1, i) and (h,i+1) are blocked/visited, then the cell (h-1, i) is visited next. The cell (h, i-1) is visited, only if the other three cells are visited or blocked. By adapting the specified priorities, the simple travel path between the entry and exit points of the maze is shown in Fig. 4. The following are the sequences of steps needed to generate scan pattern from the travelpath.

- Traverse the co-ordinate of the cells visited by the rat
- Traverse the co-ordinate of the cells not visited by the rat column wise
- Traverse the co-ordinate of the blocked cells column wise

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

Fig. 5: Scan pattern derived from travel path-I

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

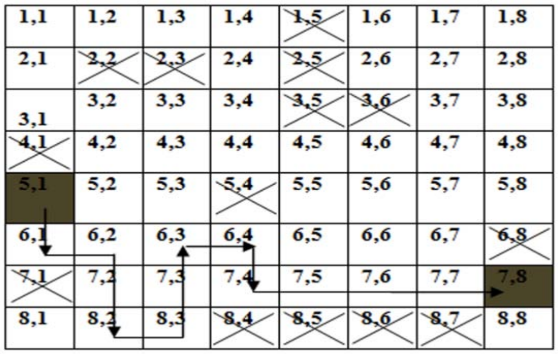


Fig. 6: a) Travel path-II (Cells Visited: 12) and b) Scan pattern derived from travel path-II

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

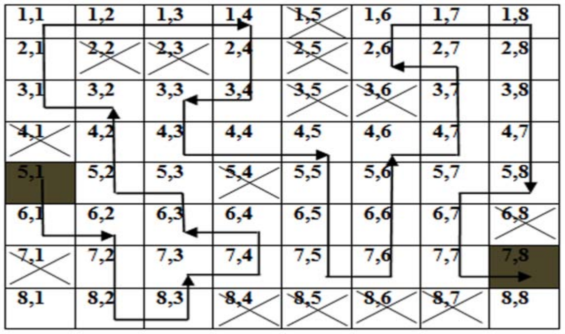


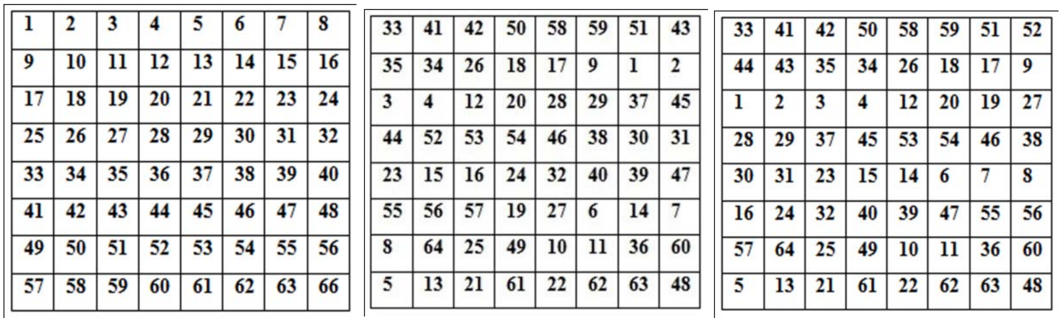
Fig. 7: Complex travel paths: a) Travel path - III (Cells Visited: 40) and b) Travel path- IV (Cells Visited: 46)

By following the sequence of steps the scan pattern, denoted as coordinates, derived from the travel path-I is shown in Fig. 5.

The next travel path of the Rat is found by backtracking the first travel path from the destination cell up to (7, 3). From this cell, as per the priority, the next move to the cell (6, 3) leads to obtain another travel path between the entry and exit points of the maze. The second travel path and the corresponding generated scan pattern are shown in Fig. 6ab.

Likewise, a pool of travel paths can be obtained for the same maze order, blocked cells, entry and exit points by backtracking and considering the priority for traversing the cells. Two more complex travel paths which can visit many cells between the entry and exit points are shown in Fig. 7ab

From the pool of travel paths, the paths which can visits maximum number of cells between the entry and exit points of the maze can be chosen to generate the scan patterns. This selection is based on the user specific



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	66

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

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

Fig. 8: Illustrative example of proposed pixel permutation: a) Original matrix, permuted matrix using; b) Travel path-III; c) Travel path-IV

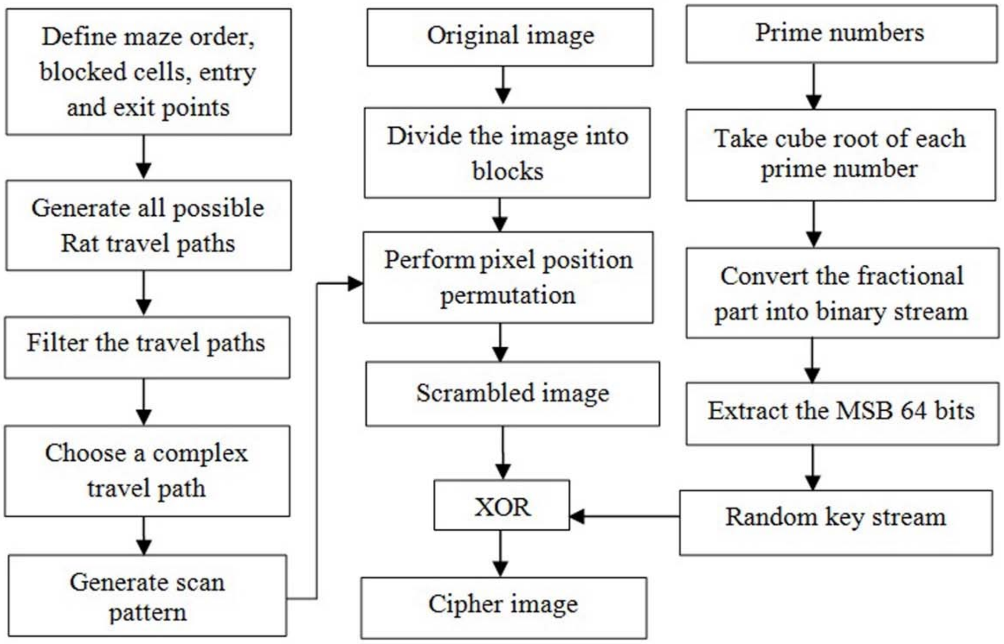

Define maze order, blocked cells, entry and exit points
Generate all possible Rat travel paths
Filter the travel paths
Choose a complex travel path
Generate scan pattern
Original image
Divide the image into blocks
Perform pixel position permutation
Scrambled image
XOR
Cipher image
Prime numbers
Take cube root of each prime number
Convert the fractional part into binary stream
Extract the MSB 64 bits
Random key stream

Fig. 9: Proposed image encryption method

Threshold (T) value. If the chosen threshold value is '48', then the number of cells visited by the Rat between the entry and exit points of the maze should be greater than or equal to '48'. The filtered travel paths should be securely shared to generate scan pattern by the communicating persons.

Proposed pixel position permutation: The scan pattern generated by using the rat's travel path is used to permute the pixel positions of the image. To demonstrate the proposed pixel permutation, let us consider an original 8×8 matrix as shown in Fig. 8a-c are the scrambled matrices by using the scan pattern generated from the travel paths shown in the Figure 7a and b, respectively. The proposed procedure is simple and supports large number of scan patterns when compared with the basic scan models.

Role of random numbers in cryptography: Pseudo Random Number Generators (PRNGs) and True Random Number Generators (TRNGs) are the two main approaches to generate random numbers (Hu *et al*., 2013). The PRNGs are deterministic and periodic but TRNGs are non deterministic and aperiodic. 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 (www.random.org).

In the proposed method, the generation of additive constants used as for the SHA-512 hash function is adapted to generate random numbers. The SHA-512 hash function has 80 rounds and each round uses a 64-bit additive constant K_t, where $0 = t = 79$ which is derived from the fractional parts of the cube roots of the first 80 prime numbers. These constants are used to provide a randomized set of 64-bit patterns which should eliminate any regularity in the input data (Stallings, 2013). Due to its randomness, this is adapted by the proposed method to generate random key stream to enforce the security.

MATERIALS AND METHODS

The proposed image encryption method: The proposed image encryption method uses pixel permutation to scramble the original image and random key stream to change the pixel values of the scrambled image. The notion of rat-in-a-maze is used to generate scan patterns for pixel permutation. The random key stream to change the pixel values is generated by adapting the randomized bit pattern generation method used in the SHA-512 hash function. The block diagram to outlines the various operations involved in the proposed method is shown in Fig. 9.

The method consists of three parts, namely, construction of scan pattern, random key stream generation and converting the original image into cipher image. In the first part, the maze order, blocked cells, the entry and exit points of the Rat are fixed to create a pool of rat's travel paths. Next, filter the travel paths based on the Threshold (T) value and choose a travel path to generate scan pattern. In part two, random key stream is generated by converting the fractional parts of the cube roots of the prime numbers into binary stream and by considering the most significant 64 bits. In the third part, the original image is divided into blocks of size b×b pixels such that the block size and maze order are equal. For simulation and analysis the value of b is chosen as 8 and 16. The pixels of each block are permuted by using the scan pattern to scramble the image. The scrambled image is XORed with the random key stream to obtain the cipher image.

Algorithm to generate rat travel paths: In this study the algorithm to generate the travel path of the rat is presented. In the algorithm, P_1 and P_2 represent the entry and exit points and T is the threshold value. The value of T is user specific and is used to filter the generated Rat's travel path.

```
Function: Maze_enc(Maze_order)
Input: Entry co-ordinate ($P_1$), Exit co-ordinate ($P_2$), Threshold (T)
Output: Rat travel paths, Total number of travel paths
Step 1: Set the maze order and Threshold (T).
Step 2: Initialize the maze with blocked and non-blocked cells represented as 1's and 0's respectively.
Step 3: Input the entry co-ordinate ($P_1$) and exit co-ordinate ($P_2$).
Step 4: Generate the Rat's travel paths and store it in the array Solution[ ][ ].
Step 5: Store the number of cells visited during each travel in the variable Cell_count.
Step 6: Assign the total number of possible travel paths in the variable Total_path.
Step 7: Filter the travel paths (Cell_count = T) which meet the threshold (T) value and store the resultant travel paths in the array Rat_path[][].
Step 8: Return the array Rat_path and Total_path.
```

Generation of random key stream: In this study the algorithm to construct random key stream from the prime numbers is presented. To generate 256×256 amount of random numbers, a range of prime numbers is considered such that 64 bits are derived from each prime to construct four random numbers. The algorithm to generate random key stream is given below.

```
Algorithm: Random_Prime ()
Step 1: Generate and store the prime number in the array Prime[r][c], where r is the row value and c is the column value.
Step 2: Let Random[n][n] be the array to store the random numbers, where n is order of the matrix.
Step 3: Take the cube root of the first prime number.
Step 4: Convert fractional part into binary stream.
Step 5: Use the most significant 64 bits of the binary stream to create four random numbers as follows:
        5.1 $B_1$←bits 63 - 56, $B_2$←bits 55 - 48, $B_3$←bits 47 - 40, $B_4$←bits 39 - 32
        5.2 $B_5$←bits 31 - 24, $B_6$←bits 23 - 16, $B_7$←bits 15 - 8, $B_8$←bits 7 - 0
        5.3 $R_1$ = $B_1$ XOR$B_2$, $R_2$ = $B_3$ XOR$B_4$, $R_3$ = $B_5$ XOR$B_6$, $R_4$ = $B_7$ XOR$B_8$
Step 6: Eliminate the bit stream which contains only '0' bits.
Step 7: Convert the remaining bit stream(s) as integer and store in the array Random[][].
Step 8: Repeat steps 3-7 until sufficient numbers are generated.
Step 9: Return the content of the array Random[][].
```

The test images taken for experimental purpose contains 256×256 pixels and hence the chosen value of n is 256.

Encryption algorithm: The encryption algorithm to convert the plain image into cipher image is presented in this section. The following are the sequence of steps:

```
Input: Plain image and maze_order (b)
Output: Cipher image
Step 1:Let P[m][m] be the plain image, where m is the order of the image matrix.
Step 2:Let Scan←pattern[][] be the array to store the scan coordinates.
Step 3:Let Scramble[][] be the array to store the scrambled image.
Step 4:Input the maze order (b).
//Generate Rat's travel path
Step 5:Rat_path[][]_Maze_enc(b)
Step 6:Choose a travel path and generate scan pattern as follows:
        6.1Traverse the cells visited by the Rat and store the corresponding coordinates row-wise in the array Scan←pattern.
        6.2Traverse the cells not visited by the Rat column- wise and place corresponding coordinates row-wise in the array Scan_pattern.
        6.3Traverse the blocked cells column-wise and store the coordinates
```

```
row-wise in the array Scan_pattern.
Step 7:Divide the plain image into blocks of size b×b pixels and apply the scan pattern to each block to scramble the plain image.
Step 8:Combine all the blocks and store the scrambled image in the array Scramble[][].
Step 9:Generate random key stream by using sequence of steps given in Section 4.2.
Random_key[][]_Random_Prime()
Step 10: Perform bitwise XOR operation between the scrambled image and random key stream.
Cipher_Image_bitxor(Scramble, Random_key)
Step 11: Store the Cipher_Image.
```

RESULTS AND DISCUSSION

The proposed method is simulated and tested with various standard gray-scale images like Lena, Baboon, Cameraman and Peppers. The implementation is done in Matlab R2010a with Intel(R) Core 2 Duo, 2 GB RAM, 2.80 GHz and 160 GB HDD. The result obtained with the Lena image is presented for comparison and visual observations. The original Lena image taken as input is shown in Fig. 10a. The scrambled version of the Lena image with maze order 8 and 16 are shown in Fig. 10b and c. From the result, it is observed that increase in maze order to generate scan pattern improves the effect of pixel permutation.

The sample random key stream generated by using the proposed method is shown in Fig. 11a. The scrambled Lena images are XORed with the random key stream and the ciphered images are shown in Fig. 11b and c.

Result shows that the encrypted Lena image is completely different from its original version and confirms the effectiveness of the proposed random key stream generator and image encryption method.

Performance and security analysis: In performance and security analysis, the evaluation metrics which are necessary to assure the security of the proposed method is measured. A single iteration of execution is done for comparing the obtained result with the standard value and the existing methods. To confirm the efficiency of the proposed method, the evaluation metrics such as histogram, correlation, entropy, number of pixel change rate and unified average changing intensity are measured and analyzed.

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. 12a-d.

The horizontal axis of the graph represents the gray-level variations while the vertical axis represents the number of pixels in that particular gray-level. From result, it is seen that the histogram of the encrypted image is flat and hence the gray-level values are uniformly distributed in the encrypted image.

Correlation analysis: Both in natural and computer-graphical images averagely 8-16 adjacent pixels are correlative in all the directions (Chang *et al*., 2001). The correlation 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 to confirm the resistance level of the proposed method against statistical attacks. The correlation can be mathematically calculated by using the Eq. 1-4.

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

Where:

γ_{xy} = The correlation coefficient
Cov(x, y) = The covariance of x and y

and is represented as:

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{2}$$

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3}$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{4}$$

Where:

E(x) and D(x) = The mean and standard deviation of the corresponding gray-scale values
N = The number of pixel data pairs

The obtained correlation between the adjacent pixels of the original and encrypted images is given in Table 1. The obtained correlation value is optimal and significant improvement is observed with maze order 16. The adjacent pixel correlation value reported in the existing methods is given in Table 2. From Table 1 and Table 2, it is found that the result attained by the proposed method is better than the methods in (Loukhaoukha *et al*., 2012; Panduranga and Kumar, 2010; Saraswathi and Venkatesulu, 2012 and comparable with those methods in (Sathyanarayana *et al*., 2011; Seyedzade *et al*., 2010). Thus, the proposed method

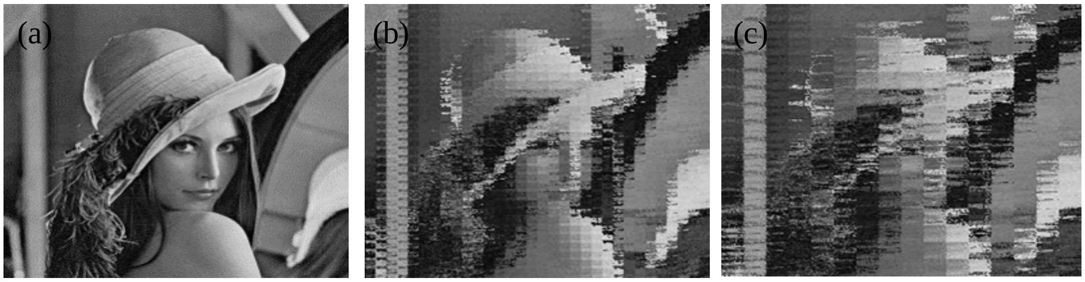


Fig.10: Result of proposed pixel permutation: a) Original lena image; b) Scrambled image (b =8); c) Scrambled image (b=16)

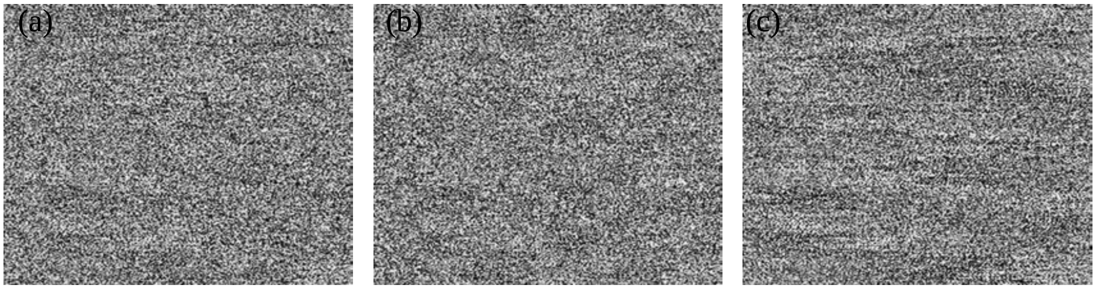


Fig. 11: Result of proposed image encryption method: a) Random key stream; b) Encrypted image (b = 8) and c) Encrypted Image (b = 16)

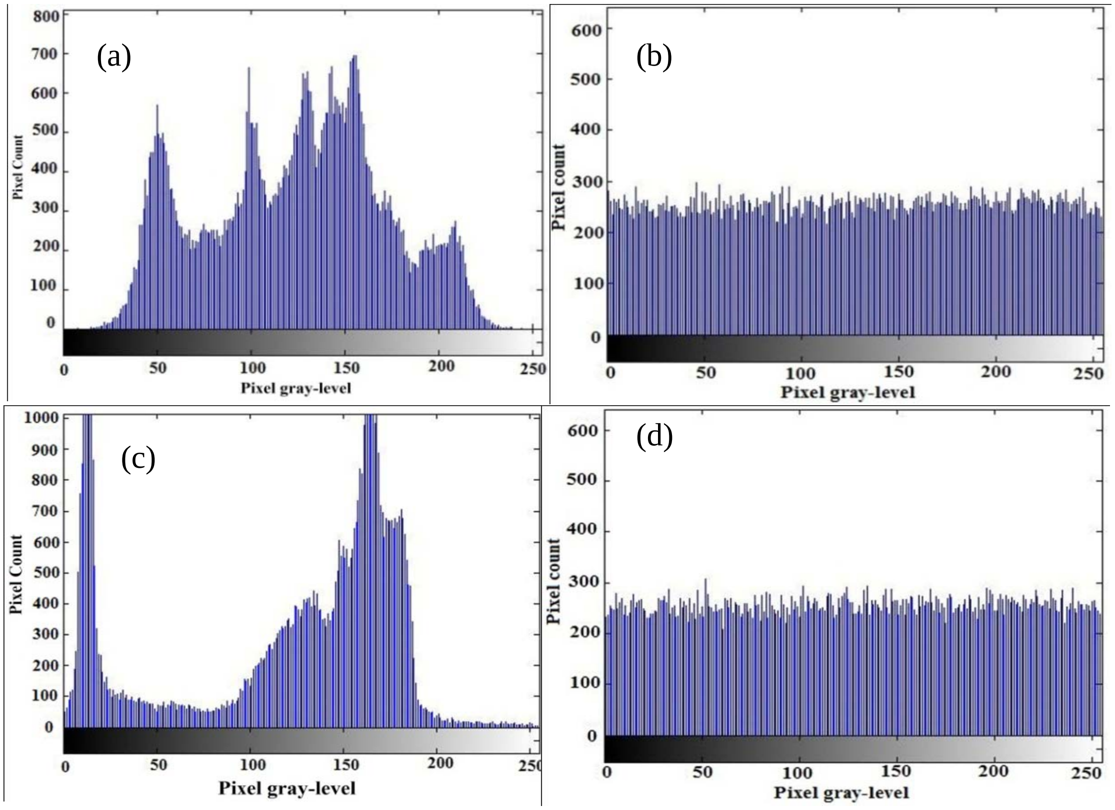


Fig. 12: Histogram of original and encrypted images: a) Original lena image; b) Encrypted lena image; c) Original cameraman image and d) Encrypted cameraman image

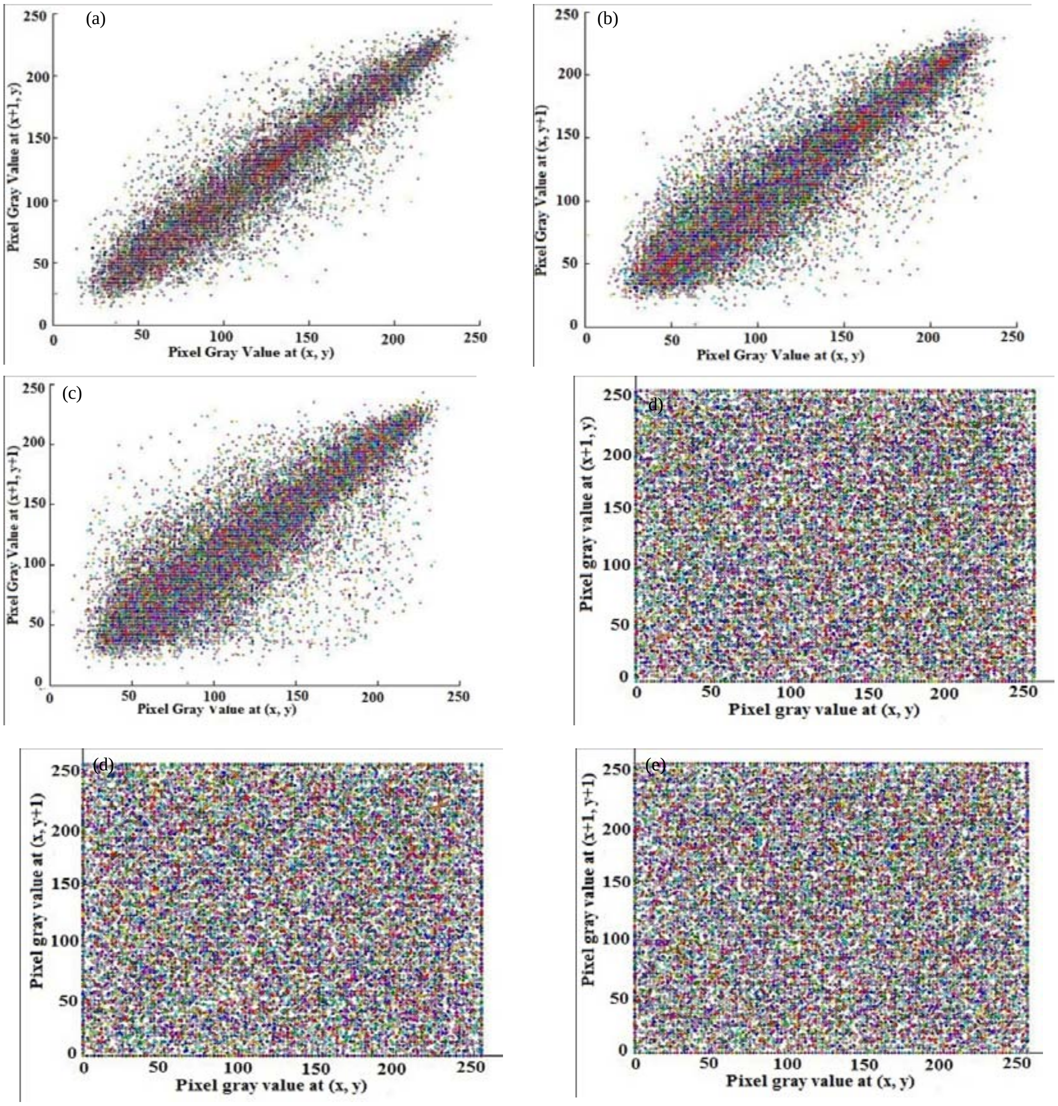


Fig. 13: Distribution of adjacent pixel correlation: a) Horizontal direction-original image; b) Vertical direction-original Image; c) Diagonal direction-original image; d) Horizontal direction-encrypted image; e) Vertical direction-encrypted image and f) Diagonal direction-encrypted image

Table 1: Adjacent pixel correlation value of proposed method

Image	Original image			Encrypted image (b = 8)			Encrypted image (b = 16)		
	Hor.	Ver.	Dia.	Hor.	Ver.	Dia.	Hor.	Ver.	Dia.
Lena	0.9344	0.9321	0.9280	0.0035	0.0104	0.0101	0.0014	0.0165	0.0025
Peppers	0.9624	0.9673	0.9519	0.0019	0.0115	0.0188	0.0070	0.0246	0.0228
Baboon	0.6965	0.8184	0.6520	0.0047	0.0127	0.0196	0.0041	0.0146	0.0086

Hor. = Horizontal; Ver. = Vertical; Dia. = Diagonal

resists the statistical attacks based on analysis of correlation between adjacent pixels. 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. 13a-f.

The cross correlation is used to find the similarity between the original and the corresponding encrypted images. The cross correlation value of proposed method and the existing methods are given in Table 3. Result shows that the encrypted image is completely different

Table 2: Adjacent pixel correlation value of existing methods

	Encrypted image		
Encryption method	Horizontal	Vertical	Diagonal
Loukhaoukha *et al.* (2011)	0.0068	0.0091	0.0063
Panduranga *et al.* (2013)	0.0263	0.0163	0.0114
Vidhyasaraswathi *et al.* (2004)	0.01776	0.04912	0.00348
Sathyanarayana *et al.* (2011)	-0.0027	-0.0028	0.0026
Seyedzade *et al.* (2010)	-0.0006	-0.0030	0.0061

Table 3: Comparison of cross correlation

Encryption method	Correlation value
Proposed	-0.0046 (b = 8) 0.0019 (b = 16)
Panduranga *et al.* (2013)	-0.0073
Sathishkumar *et al.* (2011)/A-I	-0.0535
Sathishkumar *et al.* (2011)/A-I and A-II	0.0074

Table 4: Comparison of entropy value

Encryption method	Encrypted image (Sh)
Proposed	7.9966 (b = 8) 7.9972 (b = 16)
Sathishkumar GA *et al.* (2012)	7.8101
Loukhaoukha K *et al.* (2011)	7.9968
Huang CK *et al.* (2012)	7.9967
Sathyanarayana SV *et al.* (2011)	7.9996
Bouslimi D *et al.* (2013)	7.9995

Table 5: Comparison of NPCR and UACI values

Encryption Method	NPCR value (in %)	UACI value (in %)
Proposed	99.6201 (b = 8) 99.6262 (b = 16)	28.6526 (b = 8) 30.8069 (b = 16)
Sathishkumar *et al.* (2011)	98.4754	32.2128
Loukhaoukha *et al.* (2012)	99.5850	28.6210
Huang *et al.* (2012)	99.5400	28.2700
Vidhyasaraswathi *et al.* (2004)	99.8500	33.5800

from its corresponding original version and the obtained result is better than the existing methods in (Panduranga and Kumar, 2010; Sathishkumar and Bagan, 2011).

Entropy analysis: 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 (Menezes *et al*., 2010; Shannon, 1949). In image encryption, the encrypted image should provide an equiprobable gray level. If the entropy value of the encrypted image is close to the ideal value of 8 Sh (Shannon), then the encryption algorithm is robust against entropy attacks. The entropy, H(S), of any message can be calculated by using Eq. 5:

$$H(S) = \sum_{i=0}^{m-1} p(Si)\log(1/p_{(Si)}) \qquad (5)$$

Where:

S = The message

$P(S_i)$ = Represent the probability of occurrence of the symbolS_i in the message

The entropy value attained by the proposed method and the existing methods are given in Table 4. From the result, it is found that the result obtained by the proposed method is near to 8 Sh and optimal. Also, the result is better than the method in (Sathishkumar *et al*., 2011) and comparable to the methods in (Loukhaoukha *et al*., 2012; Huang *et al*., 2013; Sathyanarayana *et al*., 2011; Bouslimi *et al*., 2012).

Visual testing: The encrypted image should be significantly different from the original image to avoid differential and ciphertext attacks. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two metrics 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 (Mahmood and Dong, 2011; Shannon, 1949; Jawad and Fawad, 2013)

Number of Pixel Change Rate (NPCR): The 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) = 0, if $I_1(i,j)$ is equal to $I_2(i, j)$, 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% (Ye, 2011). The NPCR value is calculated by using the mathematical formula given in the Eq. 6:

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

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 5. It is clearly seen that the obtained NPCR values are greater than 99.5% and optimal. The NPCR value of proposed method is better than those methods in (Sathishkuma and Dony, 2011; Huang *et al*., 2013) and comparable with (Vidhyasaraswathi and Venkatesulu, 201).

Unified Average Changing Intensity (UACI): The UACI determines the average intensity differences 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%. The UACI is computed by using the formula given in the Eq. 7:

$$\text{UACI}=\frac{1}{W\times H}\left[\sum_{i,j}\frac{I_1(i,j)-I_2(i,j)}{255}\right]\times 100\% \quad (7)$$

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 is given in Table 5. It is observed that the values are close to the 31% and significantly match with the optimal value. Also, the result is better than those methods by Loukhaoukha *et al.* (2012) and Huang *et al.* (2012) and comparable to the methods by Sathishkumar *et al.* (2011).

The values of NPCR and UACI signify that the proposed method resists differential attacks significantly and can provide better result when higher dimension maze is considered to generate scan pattern.

Key space analysis: A key is typically a compact way to specify the encryption transformation to convert the plaintext into ciphertext. The number of encryption/decryption key pairs that are supported by a cipher system is referred as the key space. A necessary but usually not sufficient, condition for an encryption scheme to be secure is that the supported key space should be large enough to prohibit exhaustive key search attack (Menezes *et al*., 2010).

The example presented in proposed scane papattern generation has a total of 29, 087 possible travel paths and there are 22 travel paths satisfy the threshold (T) value 48 with the mentioned blocked cells, entry and exit points. For the same specifications with entry point (2, 1) and exist point (8, 8), there are 28, 170 travel paths exists and 13 paths satisfies the threshold T = 48. Furthermore, the proposed method utilized the first 16,384 prime number to generate 65,536 random numbers. Thus, the proposed method has sufficient amount of scan patterns and large range of random numbers to resist the exhaustive key search attack. For real time implementation, higher dimension maze and any range of primes can be used to safe from the security attacks.

Cryptanalysis: Cryptanalysis is performed based on the amount of information known to the cryptanalyst and the purpose is to deduce the secret key used for encryption. In cryptanalysis, it is assumed that the adversary knows everything about the cryptosystem except the secret key. In the ciphertext-only attack, the adversary tries to deduce the key or plaintext by only observing the ciphertext. In known-plaintext attack, the adversary has a quantity of plaintext-ciphertext pairs. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. In chosen-plaintext attack, the adversary chooses a plain image and somehow obtains the corresponding ciphered image. By analyzing the plain/ciphered image pair, the attacker tries to reveal the secret keys. In the chosen-ciphertext attack, the adversary selects the ciphertext and study the plaintext by decrypting them. To mount the latest two attacks, the adversary gains access to the equipment used for encryption/decryption but not the secret key (Stallings, 2013; Menezes *et al.*, 2010; Ozkaynak *et al.*, 2012)

The efficiency of the proposed image encryption method primarily depends on the chosen scan pattern and the randomness of the key stream. The scan pattern generated by using the concept of rat-in-a-maze is depends on the factors such as maze order, the blocked cells, entry and exit points. The basic scan patterns such as raster, diagonal, orthogonal and spiral are based on well-defined moves for image scanning whereas the proposed scan model is random and unpredictable when higher dimensional maze is considered. Also, the secret key includes the random key stream generated from the subset of a large prime number series.

The NIST randomness test such as frequency and runs tests are conducted to assess the randomness of the random key stream and the encrypted image. The obtained probability value (p-value) of frequency test is 0.6420 for the random key stream and 0.6281 for the encrypted Lena image. The obtained P-value of runs test is 0.4604 for the random key stream and 0.3477 for the encrypted Lena image. The p-values are greater than 0.01 and assures that the generated random key stream and the encrypted Lena image are highly random. Thus, if the adversary chooses a sample plaintext sequence p_1, p_2, ... p_n and the corresponding ciphertext sequence c_1, c_2 ... c_n to search for the repetition in the ciphertext then the probability of occurring such ciphertext is low and hence the adversary may not be able to predict the secret keys.

Also, a change in encryption key should cause significant change in the encrypted image. To test this, the Lena image is encrypted by using slightly different random key stream to obtain two ciphered version of the original Lena image. The NPCR and UACI between the ciphered images is 77.7695 and 26.1842%, confirms that a change in random key stream significantly affects the cipher image.

Thus, the proposed method has considerable amount of resistance against the ciphertext-only and known plaintext attacks and has a significant resistance to other attacks. The overall security attained by the proposed method is significantly sufficient to resist possible attacks due to the unconventional scan pattern generation procedure and random key stream generator. The security of the proposed method against cryptanalysis can be further investigated and enhanced by increasing the number of iterations for encryption with distinct scan pattern and random key stream.

CONCLUSION

In this study, a new image encryption method based on pixel permutation and bitwise XOR operation is developed. The new scan pattern for pixel permutation is generated from the notion of Rat-in-a-maze. The proposed random key stream for XOR operation is constructed by adapting the randomize bit pattern generation method used for the SHA-512 hash function. The result of histogram and correlation coefficient proves the resistance of security attacks based on statistical analysis. The NPCR and UACI values are greater than 99.6 and around 31%, respectively and confirm the resistance of differential, ciphertext-only and known plaintext attacks. The obtained entropy value is optimal and near to the standard value 8 Sh. The supported key space is sufficient to make the exhaustive key search attack as infeasible. The NIST randomness test assured that the proposed key stream generator produces random bits.

REFERENCES

Aggarwal, C.C., 2011. Social Network Data Analytics. Springer, Berlin, Germany, ISBN: 978-1-4419-8461-6, Pages: 501.

Alexopoulos, C., N.G. Bourbakis and N. Ioannou, 1995. Image encryption method using a class of fractals. J. Electron. Imaging, 4: 251-259.

Alvarez, G., J.M. Amigo, D. Arroyo and S. Li, 2011. Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers. In: Chaos-Based Cryptography, Ljupco, K. and S. Lian (Eds.). Springer, Berlin, Germany, ISBN: 978-3-642-20541-5, pp: 257-295.

Arroyo, D., C. Li, S. Li, G. Alvarez and W.A. Halang, 2009. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos Solitons Fractals, 41: 2613-2616.

Bourbakis, N. and C. Alexopoulos, 1992. Picture data encryption using SCAN patterns. Pattern Recognition, 25: 567-581.

Bouslimi, D., G. Coatrieux, M. Cozic and C. Roux, 2012. A joint encryption-watermarking system for verifying the reliability of medical images. IEEE. Trans. Inf. Technol. Biomed., 16: 891-899.

Chang, C.C., M.S. Hwang and T.S. Chen, 2001. A new encryption algorithm for image cryptosystems. J. Syst. Software, 58: 83-91.

Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. A hash-based image encryption algorithm. Opt. Commun., 283: 879-893.

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals, 21: 749-761.

Francois, M., T. Grosges, D. Barchiesi and R. Erra, 2012. A new image encryption scheme based on a chaotic function. Signal Process. Image Commun., 27: 249-259.

Fu, C., B.B. Lin, Y.S. Miao, X. Liu and J.J. Chen, 2011. A novel chaos-based bit-level permutation scheme for digital image encryption. Optics Commun., 284: 5415-5423.

Hu, H., L. Liu and N. Ding, 2013. Pseudorandom sequence generator based on the Chen chaotic system. Comput. Phys. Commun., 184: 765-768.

Huang, C.K., C.W. Liao, S.L. Hsu and Y.C. Jeng, 2013. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommun. Syst., 52: 563-571.

Jawad, A. and A. Fawad, 2013. Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Network Secur., 12: 18-31.

Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A secure image encryption algorithm based on Rubik's cube principle. J. Electr. Comput. Eng. 10.1155/2012/173931

Mahmood, A.B. and R.D. Dony, 2011. Segmentation based encryption method for medical images. Proceedings of the2011 International Conference on Internet Technology and Secured Transactions (ICITST), December 11-14, 2011, IEEE, New York, USA., ISBN: 978-1-4577-0884-8, pp: 596-601.

Maniccam, S.S. and N.G. Bourbakis, 2001. Lossless image compression and encryption using SCAN. Pattern Recognit., 34: 1229-1245.

Maniccam, S.S. and N.G. Bourbakis, 2004. Image and video encryption using SCAN patterns. Pattern Recognit., 37: 725-737.

Menezes, A.J., P.C.V. Oorschot and S.A. Vanstone, 2010. Handbook of Applied Cryptography. CRC Press, New York, USA.,.

Ozkaynak, F., A.B. Ozer and S. Yavuz, 2012. Cryptanalysis of Bigdeli algorithm using Cokal's attack. Int. J. Inf. Security Sci., 1: 79-81.

Pandey, U., M. Manoria and J. Jain, 2012. A novel approach for image encryption by new M box encryption algorithm using block based transformation along with shuffle operation. Int. J. Comput. Appl., 42: 9-15.

Panduranga, H.T. and S.K.N. Kumar, 2010. Hybrid approach for image encryption using SCAN patterns and Carrier Images. Int. J. Comput. Sci. Eng., 2: 297-300.

Patidar, V., N.K. Pareek, G. Purohit and K.K. Sud, 2011. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Opt. Commun., 284: 4331-4339.

Saraswathi, P.V. and M. Venkatesulu, 2012. A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal. J. Comput. Sci., 8: 1541-1546.

Sathishkumar, G.A. and K.B. Bagan, 2011. A novel image encryption algorithm using pixel shuffling and base 64 encoding based chaotic block cipher (IMPSBEC). WSEAS. Trans. Comput., 10: 169-178.

Sathishkumar, G.A., K.B. Bagan and N. Sriraam, 2011. Image encryption based on diffusion and multiple chaotic maps. Int. J. Network Secur. Applic., 3: 181-194.

Sathyanarayana, S.V., M.A. Kumar and K.H. Bhat, 2011. Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points. Int. J. Network Secur., 12: 137-150.

Seyedzade, S.M., S. Mirzakuchaki and R.E. Atani, 2010. A novel image encryption algorithm based on hash function. Proceedings of the 6th Iranian Machine Vision and Image Processing, October 27-28, 2010, Isfahan, Iran, pp: 1-6.

Shannon, C.E., 1949. Communication theory of secrecy systems. Bell Syst. Tech. J., 28: 656-715.

Stallings, W., 2013. Cryptography and Network Security-Principles and Practice. 5th Edn., Pearson Education, New Delhi, India,.

Usman, K., H. Juzoji, I. Nakajima, S. Soegidjoko and M. Ramdhani et al., 2007. Medical image encryption based on pixel arrangement and random permutation for transmission security. Proceedings of the 2007 9th International Conference on E-Health Networking Application and Services, June 19-22, 2007, IEEE, New York, USA., pp: 244-247.

Ye, R., 2011. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Commun., 284: 5290-5298.

Zare, M.R., A. Mueen and W.C. Seng, 2013. Automatic classification of medical X-ray images using a bag of visual words. IET Comput. Vision, 7: 105-114.

Zhao, L., A. Adhikari, D. Xiao and K. Sakurai, 2012. On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption. Commun. Nonlinear Sci. Numer. Simul., 17: 3303-3327.