Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 261–268 DOI: 10.15439/2017R47
ACSIS, Vol. 10 ISSN 2300-5963

A Comparative study on Cryptographic Image Scrambling

Bhaskar Mondal
Dept. of Computer Science Engineering
National Institute of Technology
Jamshedpur, India- 831014
Email: bhaskar.cse@nitjsr.ac.in

Neel Biswas
Dept. of Computer Science Engineering
National Institute of Technology
Jamshedpur, India- 831014
Email: neelbiswas01@gmail.com

Tarni Mandal
Dept. of Mathematics
National Institute of Technology
Jamshedpur, India- 831014
Email: tmandal.math@nitjsr.ac.in

***Abstract*—In the last few decades, a numerous number of image encryption algorithm has been proposed based on scrambling. Scrambling is the most crucial part of confusion-diffusion based encryption techniques. In the current scenario, the scrambling techniques are used without knowing the cryptographic effect, quality and computational complexity. Hence, an comparative study on scrambling techniques (permutation) is required. In this paper, a comparative study has been done on different scrambling techniques like matrix transformation, bit plane scrambling, 2D mapping and key based row and columns shifting techniques. To determine the quality and efficiency of the scrambling techniques, correlation, entropy, computational complexity have been considered. From the test results it was found that matrix based image scrambling applied on Arnold Transform was the best among the considered techniques in terms of correlation.**

***Index Terms*—Arnold's map, cryptography, Fibonacci series, gray code, scrambling**

I. Introduction

In the past few decades, there has been a drastic change in the working habits, entertainment sources, modes of communication and shopping techniques. Due to this change a lot of multimedia information exchanges are done over the Internet everyday. Secure multimedia communication is increasingly becoming important as multimedia data can be easily intercepted by illegal sources. Law enforcement agents may find it very difficult to stay afloat above the ill intentions of hackers.Therefore, people should pay more attention to the security of media data. Techniques like encryption [10], [11], stanography [15], watermarking [12], secret sharing [13], [9] etc are used to secure data during the transmission over public channel.

Scrambling is widely used in encryption algorithms[16], [14], [8] for adding confusion. Scrambling refers to the permutations of pixel values or permutation of bit values in a bit plane. Transforming a plain image into a meaningless noise to eliminate the high correlation between adjacent is the aim of scrambling. Various image scrambling techniques are used in pay-TV, defense purposes, medical domain, private video conferencing and various other applications [28], [19].

This paper presents a comparative study of some popular cryptographic image scrambling methods like generalized matrix-based scrambling (transformation) [5] using Arnold's transform [1] and Fibonacci transform [27], gray code with bit plane transformation [25], 2D mapping [20], key based row and column shifting[18], [10] and Fu et. al.'s key based row and column shifting with bit-level permutation [3].

Arnold's cat map is a chaotic map named after, Vladimir Arnold who proposed the algorithm, and also applied to Fibonacci transform [28]. Fibonacci transform [27] has a unique property of uniformity. The pixels that are at equal distance from each other in original image remain at equal distances in the encrypted image as well. The adjacent pixels are also spread as far as possible. In addition to having very low correlation this method has low computational overhead.

A quantum image gray-code and bit-plane scrambling [25], [21] is presented in which bit-plane scrambling is one of the famous image scrambling techniques. It is used as one of the basic steps in many encryption algorithm [26]. The values of higher bit planes are XORed with the lower bit planes. The value of lowest bit plane be fixed.

Another image scrambling method based on 2D mapping [22] in which pseudo-randomness, aperiodicity and being sensitive to change with respect to initial conditions make chaotic maps one of the favorite techniques in scrambling. It is also used in scrambling of large amount of data such as video, audio etc [2]. The watermark information of the image is embedded in the amplitude spectrum by 2D mapping [20]. In this algorithm, a random sequence is generated using chaotic map(logistic map [23]). Then, the original image is XORed with the random sequence. Further image mirror mapping interlacing is used to scramble the image.

Key based scrambling for secure image communication is used in[18], [10], a random sequence is generated. Using this random sequence, the rows of the image is swapped. Similarly, the columns are swapped. Further, circular shifting of the rows and columns are done using using the same sequence. [24] also used a method involved row and column shifting with prediction error clustering for image encryption the compression scheme. [7], [17] also uses row and column shifting method for permutation of pixels.

A novel chaos-based bit-level permutation scheme [3] in which the image is extended to bit plane binary image. Chebyshev chaotic map is used to generate random sequences. The rows are permuted according to that random sequences.

Further, the columns are shifted according to the same random sequences. After that, the extended image is divided into 8 blocks of equal sizes and again permutation is applied on each block using generalized Arnold Cat Map. The blocks are then merged to obtain the cipher image [4]. [6] uses a pixel-level permutation and bit-level permutation for image encryption.

Correlation between the original image and the encrypted image, correlation between the current pixel and horizontal, vertical and diagonal pixels, entropy, computational complexity are used as parameters of compare the scrambling techniques.

The next section describes the overview of the schemes compared followed by comparative results in section III. And finally conclusion is presented in section IV

II. Schemes Compared

A. Generalized Matrix-based Scrambling Transformation

The equation 1 transformation is the general model:

$$\vec{V_k} = A\vec{V}_{k-1} \bmod \vec{N}, k \in Z^+ \tag{1}$$

In equation 1, A is a matrix of size $n \times n$. A is called as scrambling parameter matrix. All the entries of A are non-negative integers and $\det(A) \neq 0$, $\vec{V_k}, \vec{V}_{k-1}, \vec{N}$ are $n \times 1$ vectors and $0 < v_{i,j} \leq N_{j-1}$ for $i = k-1, k$ and $j = 1, 2, \ldots, n$ assuming $\vec{V}_{k-1} = (V_{k-1,1}V_{k-1,2}...V_{k-2,n})'$ and $\vec{V_k} = (V_{k,1}V_{k,2}...V_{k,n})'$, $\vec{N} = (N_1N_2...N_n)'$ is called the module vector in which N_j are positive integers representing the upper limit of the corresponding $v_{ij} = (i, j = 1, 2...)$. The scrambling times of the image is denoted by a positive integer k. $^+$ denotes the set of positive integers.
The case with equal module is defined as equi-modulo transformation, i.e., $\vec{N} = (NN...N)'$, then, equation 1 can be transformed into equation 2:

$$\vec{V_k} = A\vec{V}_{k-1} \bmod N, k \in Z^+ \tag{2}$$

1) Matrix based Image Scrambling applied on Arnold Transform: Cat map, also known as Arnold transform was proposed by V.I. Arnold in the research of ergodic theory. A process of splicing and clipping which realigns the digital image matrix is called transform. The 2D Arnold transform is an invertible map described by equation 3

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \tag{3}$$

where $(x_n, y_n) \in [0, 1) \times [0, 1)$

It can be applied to scramble digital images sized $N \times N$ by the discrete form in equation 4:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \tag{4}$$

where $(x_n, y_n) \in [0, N-1] \times [0, N-1]$

is the original image's pixel coordinate; N is the height or width of the image processed; (x_{n+1}, y_{n+1}) is the coordinate of the scrambled image. The transform changes the position of pixels, and if it is done several times, a disordered image can be generated.

The Scrambling process:

for each pixel $A(i, j)$ **do**
$\binom{I}{J} \leftarrow \binom{1\ 1}{1\ 2}\binom{i}{j}$
$B(I, J) \leftarrow A(i, j)$
end for

2) Matrix based Image Scrambling applied on Fibonacci Series: Fibonacci Series is a special series named after nineteenth-century mathematician Leonard Fibonacci. The following series is called Fibonacci series: $1, 1, 2, 3, 5, 8, \ldots$
Let X and Y be two adjacent Fibonacci numbers, $X = F(n), Y = F(n+1)$. Then, $F(n+2) = X + Y$.
The transformation is known as the Fibonacci Transformation which is represented by equation 5:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{5}$$

where $x, y \in \{0, 1, 2, 3 \ldots, N-1\}$

The Scrambling process:

for each pixel $A(i, j)$ **do**
$\binom{I}{J} \leftarrow \binom{1\ 1}{1\ 0}\binom{i}{j}$
$B(I, J) \leftarrow A(i, j)$
end for

B. Quantum image gray code and bit plane scrambling

NEQR, based on FRQI(Flexible Representation of Quantum Image) is a splendid representation for a quantum image. According to the NEQR model, a quantum gray scale image can be described as equation 6

$$\begin{aligned} |I\rangle &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} |f(X, Y)\rangle |XY\rangle \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \otimes_{i=0}^{q-1} \left|C^i_{i=0}\right| |XY\rangle \end{aligned} \tag{6}$$

where $|I\rangle$ stands for a $2^n \times 2^n$ image and the gray range of image is 2^q. Then, binary sequence encodes the gray value $f(X, Y)$ of corresponding pixel (X, Y), whose implication is in equation 7,

$$\begin{aligned} f(X, Y) = C^0_{XY} C^1_{XY} \ldots C^{q-2}_{XY} C^{q-1}_{XY}, C^k_{XY} \in [0, 1], \\ f(X, Y) \in [0, 2^q - 1] \end{aligned} \tag{7}$$

The Scrambling process: The first operation performed on the image is bit plane slicing. Bit plane information rule states that high bit planes contain most of the information (50.19% information of the pixel is contained in the 8th bit plane) while the lower bit planes contain less information(0.003% information of the pixel is present in the 0th bit plane). According to this rule, the elementary GB scheme adopts the Gray-code transformation in reverse order i.e 0^{th} bit plane is kept fixed.The elementary GB scrambling is denoted by the

following function 8:

$$|I\rangle = \frac{1}{2^n}\sum_{x=0}^{2^M-1}\sum_{y=0}^{2^N-1} GB(|f(X,Y)\rangle)\,|XY\rangle = \frac{1}{2^n}\sum_{x=0}^{2^M-1}\sum_{y=0}^{2^N-1} |g(X,Y)\rangle\,|XY\rangle \tag{8}$$

where $n = (M+N)/2$

The GB in the above equation stands for the elementary GB scrambling operation. The quantum circuit about this method is shown in figure 1 given below: Numbers 1 to 8 represent

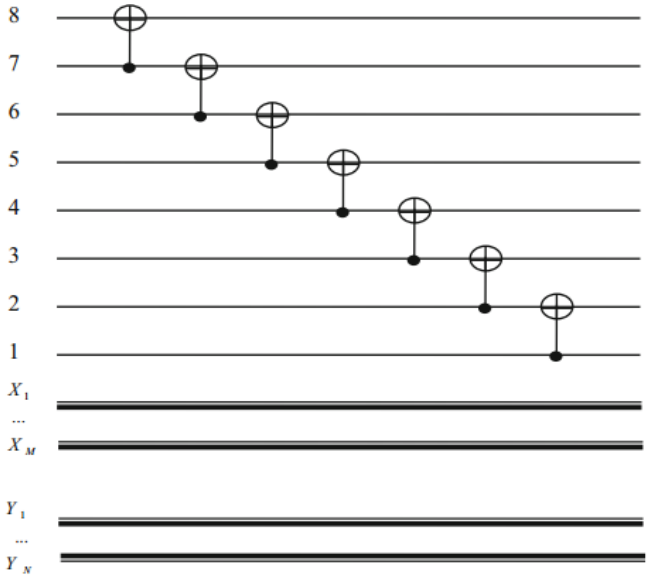


Fig. 1: The quantum circuit

the bit planes. The gates used here is CNOT gates (Controlled NOT gate).

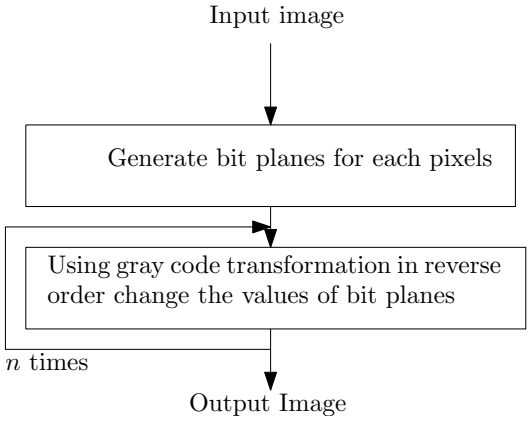


Fig. 2: Flow chart of gray Code scrambling

C. Image Scrambling based on 2D mapping

Assume the original image is $A(M \times N)$, where M represents the height and N represents the width. The pixel value of any coordinate (i, j) is expressed by $A(i, j)$ where $i = 0, 1, 2, \ldots M-1$ and $j = 0, 1, 2, \ldots N-1$. The dimension of the encryption image E is still $M \times N$.

The Scrambling process:

Step1: Generate a two dimensional random sequence R such that $R(i, j), (i = 0, 1, 2, \ldots M-1; j = 0, 1, 2, \ldots N-1)$.

Step2 Since bit-exclusive-or operations are reversible in mathematics, it may be used to realise the counter operation of the algorithm. Chaos sequence R is used to change the original image A's pixel gray level to obtain image A_1. The operation is: $A1(i, j) = A(i, j) \oplus R(i, j)$

Step3: The final encrypted image E is obtained by changing the pixels of A_1. Using image mirror mapping in mathematics reversible can realize the operation of inverse algorithm, and make the symmetrical mirror image mapping to image A_1. Image mirror maps can order around from top-bottom mirror and then left - right mirror, the opposite order can also be. In order to increase the degree of image scrambling, this article uses the image mirror mapping interlacing. First of all, take the image A's vertical median line as the symmetry axis, and then left- right mirror mapping to image A_1's even-numbered columns to obtain image A_2.This left right mirror mapping's formula can be expressed as equation 9:

$$\begin{aligned} A_2(i,j) = A_1(i, N-j+2) \ if \quad \bmod (j,2) = 0 \\ A_2(i,j) = A1(i,j) \ if \quad \bmod (j,2) = 1 \end{aligned} \tag{9}$$

Then the symmetry axis is taken to be the horizontal median line of image A_2, and then top-bottom mirror mapping to image A_2's odd-numbered rows to obtain image A_3. This topbottom mirror mapping's formula can be expressed as equation 10:

$$\begin{aligned} A_3(i,j) = A_2(M-i,j) \ if \ \bmod (i,2) = 1 \\ A_3(i,j) = A_2(i,j) \ if \ \bmod (j,2) = 0 \end{aligned} \tag{10}$$

And image A_3 is the encrypted image E.

D. Key based scrambling by row and column shifting

Key based scrambling algorithm is a very effective and simple method of image scrambling and encryption. In this method, the user specifies a key that forms a sequence of numbers. The content provider uses this sequence to generate another key sequence to scramble the image and transmit it.

Encryption in this method is key-based and subsequently a scrambled image is generated. The method is shown in figure 3.

The Scrambling process:

Step1- A secret key is used to generate a random sequence R that is of the length of the maximum dimension of the image. If an image is 256×128, then the key sequence will have a length of 256.

Step2- Now the key sequence is used to switch the Rows. If the 1^{st} value of the sequence is 66 then the 1^{st} row is swapped with 66^{th} row of the image.

Step3- Use the key sequence to switch the columns. The

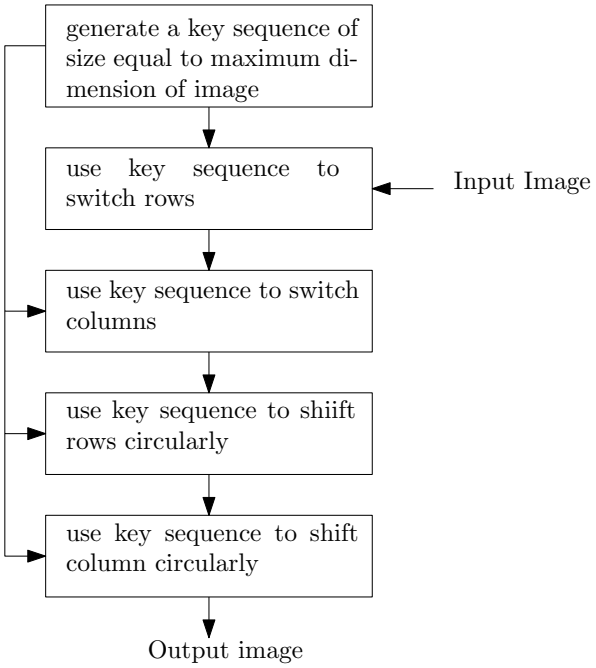


Fig. 3: Flow chart of Key based scrambling [18]

column switching process is similar to the row switching.
Step4- Now the Rows are circular shifted using the same key sequence as the scrambling achieved from row and Column switching is not acceptable.
Step5- Similarly, the columns are also circular shifted using the key sequence.
When the above 5 steps are applied to an image, the scrambled image is obtained.

E. Fu et. al.'s scrambling Scheme

This scheme is based on chaos based bit permutation. The scheme performs shuffling in two steps, first using a chaos sequence based on Chebyshev chaotic map and second using generalized Arnold transform. The scheme is successful in generating a secure image cipher. The steps are as follows:

1) Extend the image of size $M \times N$ to $M \times N \times 8$ bit plane binary image.
2) Generate the chaotic sequences S_0 and S_1 of size M and $N \times 8$ respectively using Chebyshev chaotic map in equation 11.

$$x_{(n+1)} = T_l(x_n) = \cos\left(l.\cos^{-1} x_n\right), \quad x_n \in [-1, 1], l \in [2,] \tag{11}$$

3) Permute the rows of the binary image using sequence S_0.
4) Permute the columns of binary image using sequence S_1.
5) Now, Divide the binary image into 8 blocks of equal size.
6) Permute each block with generalized Arnold cat map (in equation 4) k times.
7) marge the blocks left to right to recover the pixel plane and further generate the Cipher Image.

III. Comparative Study and Results

Four images namely test image 1 in figure 4, test image 2 in figure 5, test image 3 in figure 6, test image 4 in figure 7 were taken for experiment. Those same images were scrabbled using different methods. (b) is scrambled using scheme using Arnold's transformation, (c) is scrambled using Fibonacci transformation, (d) is scrambled using gray code with bit plane transformation, (e) is scrambled using 2D mapping, and (e) is scrambled using key based row and column shifting method and (f) is scrambled using key based row and column shifting method with bit plane permutation.

A. Entropy analysis

Entropy is the measure of randomness and unpredictability in an image. It measures the randomness in the frequency of occurence of pixels with different intensities present in the image. Low entropy anywhere, especially via repeating keys or values, produces measurable statistical correlations, which are the basis of much of cryptanalysis. By contrast, more entropy means a bigger and less predictable key search space, with fewer and more difficult to detect redundancies and correlations. The entropy in a cipher is thus a measure of how difficult it is to break the cipher via brute force.

$$H = -\sum_{i=0}^{2^N-1} p_i \log_2 p_i \tag{12}$$

A good cipher has an entropy closer to 8. The table II shows the entropy of scrambled images.

B. Comparative Computational Complexity

The Comparative numbers of operation are presented in table I. Where k stands for number of iterations of ArnoldFibonacci transformGray bit plane scrambling.

TABLE I: Comparative results of operation

Scheme	Operation
Arnold's transformation	No of mod operations $M \times N \times k$ No of swap operations $M \times N \times k$
Fibonacci transformation	No of mod operations $M \times N \times k$; No of swap operations $M \times N \times k$
gray code with bit plane transformation	No of xor operations $M \times N$; No of mod operations $M \times N \times 2$; No of copy operations $3 \times M \times N$
2D mapping	No of xor operations $7 \times M \times N \times k$
row and column shifting	No of swap operations $M \times N + N \times M = 2 \times M \times N$; Worst Case No of shift operations $\max(M, N) \times M + \max(M, N) \times N$
row and column shifting with bit plane scrambling	No of swap operations $M+N \times 8+M \times N \times 8 \times k$; No of mod operations $M \times N \times 8 \times k$

C. Correlation Coefficient

It tells us how much there is relation between the same pixels of the original and the encrypted image. It is calculated from the formula below eq. 13:

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left((A_{mn} - \overline{A})^2\right)\left((B_{mn} - \overline{B})^2\right)}} \tag{13}$$

Where A and B are the original and the encrypted image respectively. and are their means. The lower the value of the correlation coefficient, the better it is. The values were found to be as shown in table II.

IV. Conclusion

Scrambling is one of the most important part of confusion diffusion based image encryption. A huge number of scrambling techniques are available in literature. Therefor choosing the correct scrambling method for an encryption scheme becomes most crucial. The performance of a an encryption scheme largely depends on the scrambling technique used. In this paper a comparative study on different cryptographic scrambling techniques is done. The study includes matrix based, Fibonacci series based, key based scrambling techniques. Correlation coefficient, entropy and computational complexities are compared in the paper by simulating and testing them on four images.

References

[1] Nidaa AbdulMohsin Abbas. Image encryption based on independent component analysis and arnolds cat map. *Egyptian Informatics Journal*, 17(1):139 – 146, 2016.

[2] S. M. H. Alwahbani and E. B. M. Bashier. Speech scrambling based on chaotic maps and one time pad. In *Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference on*, pages 128–133, Aug 2013.

[3] Chong Fu, Bin bin Lin, Yu sheng Miao, Xiao Liu, and Jun jie Chen. A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics Communications*, 284(23):5415 – 5423, 2011.

[4] A. Jolfaei, X. W. Wu, and V. Muthukkumarasamy. On the security of permutation-only image encryption schemes. *IEEE Transactions on Information Forensics and Security*, 11(2):235–246, Feb 2016.

[5] Xiongjun Li. A generalized matrix-based scrambling transformation and its properties. In *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, pages 1429–1434, Nov 2008.

[6] Yueping Li, Chunhua Wang, and Hua Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 90:238 – 246, 2017.

[7] Wenhao Liu, Kehui Sun, and Congxu Zhu. A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84:26 – 36, 2016.

[8] Bhaskar Mondal, Anirban Bhowmick, Tanupriya Choudhury, and Tarni Mandal. A key agreement scheme for smart cards using biometrics. In *IEEE International Conference on Computing Communication and Automation (ICCCA-2016)*, volume 1, pages 1–5. Galgotias University, UP, India, 2016.

[9] Bhaskar Mondal and Tarni Mandal. A secret shearing algorithm based on lsb substitution. *International Journal of Computer Applications*, 92(4):31–35, April 2014. Full text available.

[10] Bhaskar Mondal and Tarni Mandal. A light weight secure image encryption scheme based on chaos & dna computing. *Journal of King Saud University - Computer and Information Sciences*, pages –, 2016.

[11] Bhaskar Mondal and Tarni Mandal. A nobel chaos based secure image encryption algorithm. *International Journal of Applied Engineering Research*, (5):120–3127, 2016.

[12] Bhaskar Mondal, Tarni Mandal, T. Choudhury, and D.A. Khan. Use of a light weight secure image encryption scheme based on chaos and dna computing. *Int. J. Advanced Intelligence Paradigms*, 2017.

[13] Bhaskar Mondal, Tarni Mandal, Sunil Kumar Singh, and Krishana Mohan Acharjee. A novel (k, n) secret key sharing scheme based on linear equations. *International Journal of Engineering Research Technology (IJERT)*, 2(10):1679–1682, 2013.

[14] Bhaskar Mondal, Akash Priyadarshi, and D. Hariharan. An improved cryptography scheme for secure image communication. *International Journal of Computer Applications*, 67(18):23–27, April 2013.

[15] Bhaskar Mondal and Sunil Kumar Singh. A highly secure steganography scheme for secure communication. *International Conference of Computation and Communication Advancement (IC3A)-2013*, pages 92–96, Jan 2013.

[16] Bhaskar Mondal, Nishith Sinha, and Tarni Mandal. A secure image encryption algorithm using lfsr and rc4 key stream generator. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, pages 227–237. Springer India, 2015.

[17] Zahra Parvin, Hadi Seyedarabi, and Mousa Shamsi. A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Multimedia Tools and Applications*, 75(17):10631–10648, 2016.

[18] Prashan Premaratne and Malin Premaratne. Key-based scrambling for secure image communication. In De-Shuang Huang, Phalguni Gupta, Xiang Zhang, and Prashan Premaratne, editors, *Emerging Intelligent Computing Technology and Applications*, volume 304 of *Communications in Computer and Information Science*, pages 259–263. Springer Berlin Heidelberg, 2012.

[19] B. Radu, D. A. Cristina, P. Iustin, and F. Cristina. A new fast chaos-based image scrambling algorithm. In *Communications (COMM), 2014 10th International Conference on*, pages 1–4, May 2014.

[20] Z. Wang, S. Lv, J. Feng, and Y. Sheng. A digital image watermarking algorithm based on chaos and fresnel transform. In *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2012 4th International Conference on*, volume 2, pages 144–148, Aug 2012.

[21] Jun xin Chen, Zhi liang Zhu, Chong Fu, Hai Yu, and Li bo Zhang. An efficient image encryption scheme using gray code based permutation approach. *Optics and Lasers in Engineering*, 67:191 – 204, 2015.

[22] Wang Yanling. Image scrambling method based on chaotic sequences and mapping. In *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*, volume 3, pages 453–457, March 2009.

[23] Erdem Yavuz, Rifat Yazc, Mustafa Cem Kasapba, and Ezgi Yama. A chaos-based image encryption algorithm with simple logical functions. *Computers Electrical Engineering*, 54:471 – 483, 2016.

[24] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang. Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE Transactions on Information Forensics and Security*, 9(1):39–50, Jan 2014.

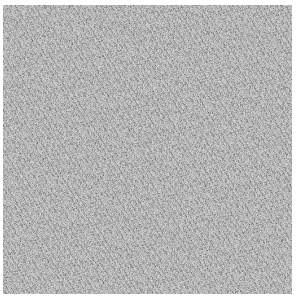
[25] Ri-Gui Zhou, Ya-Juan Sun, and Ping Fan. Quantum image gray-code and bit-plane scrambling. *Quantum Information Processing*, 14(5):1717–1734, 2015.

[26] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen. (n, k, p)-gray code for image systems. *IEEE Transactions on Cybernetics*, 43(2):515–529, April 2013.

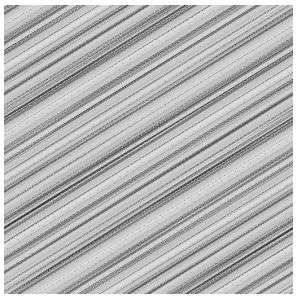
[27] Yicong Zhou, Karen Panetta, Sos Agaian, and C.L. Philip Chen. Image encryption using p-fibonacci transform and decomposition. *Optics Communications*, 285(5):594 – 608, 2012.

[28] Jiancheng Zou, R. K. Ward, and Dongxu Qi. A new digital image scrambling method based on fibonacci numbers. In *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*, volume 3, pages III–965–8 Vol.3, May 2004.

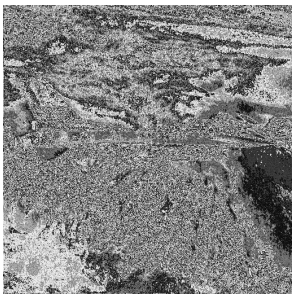
(a) Airplane: Original test image 1



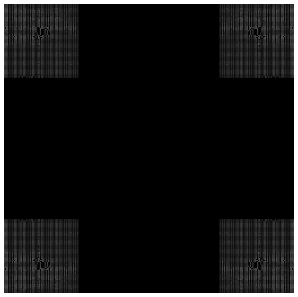
(b) Scrambled by Arnold's transformation



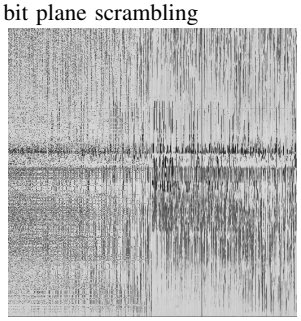
(c) Scrambled by Fibonacci transformation



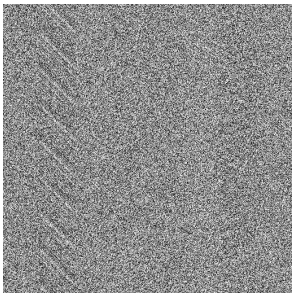
(d) Scrambled by gray code with bit plane scrambling



(e) Scrambled by 2D mapping

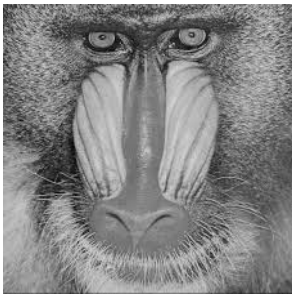


(f) Scrambled by key based row and column shifting

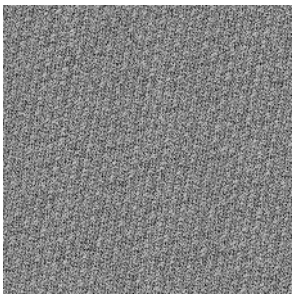


(g) Scrambled by key based row and column shifting with bit plane scrambling

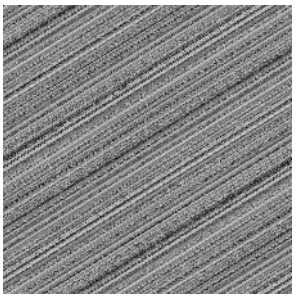
Fig. 4: Results of scrambling using different scrambling techniques on Airplane image: Original test image 1



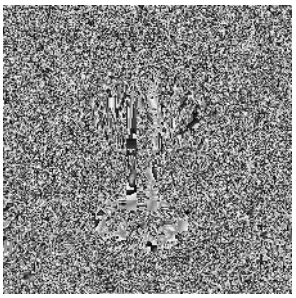
(a) Baboon: Original test image 2



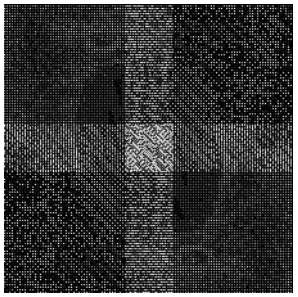
(b) Scrambled by Arnold's transformation



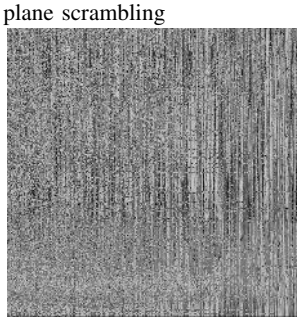
(c) Scrambled by Fibonacci transformation



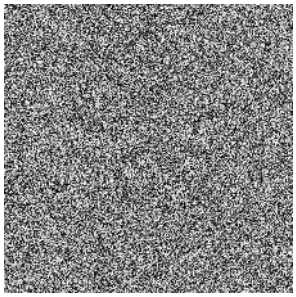
(d) Scrambled by gray code bit plane scrambling



(e) Scrambled by 2D mapping



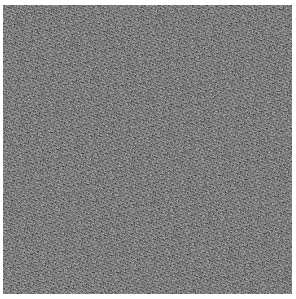
(f) Scrambled by key based row and column shifting



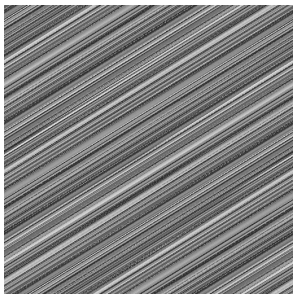
(g) Scrambled by key based row and column shifting with bit plane scrambling

Fig. 5: Results of scrambling using different scrambling techniques on Baboon image: Original test image 2

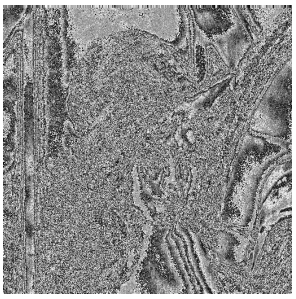
(a) Lena: Original test image 3



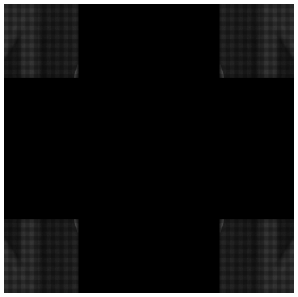
(b) Scrambled by Arnold's transformation



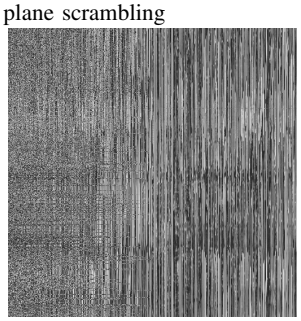
(c) Scrambled by Fibonacci transformation



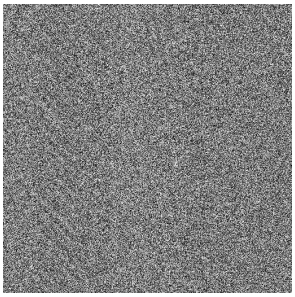
(d) Scrambled by gray code bit plane scrambling



(e) Scrambled by 2D mapping

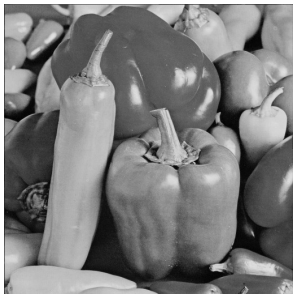


(f) Scrambled by key based row and column shifting

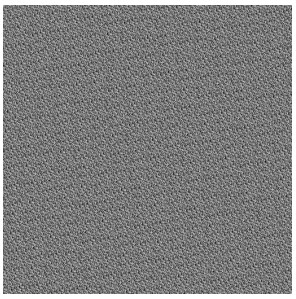


(g) Scrambled by key based row and column shifting with bit plane scrambling

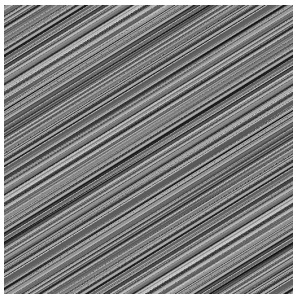
Fig. 6: Results of scrambling using different scrambling techniques on Lena image: Original test image 3



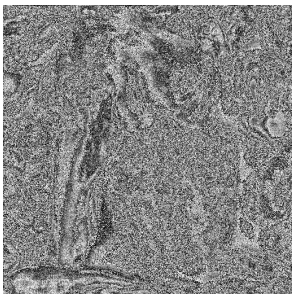
(a) Peppers: Original test image 4



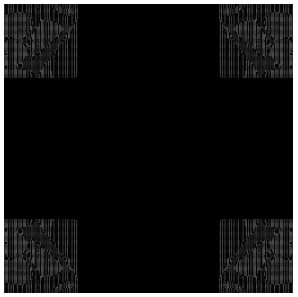
(b) Scrambled by Arnold's transformation



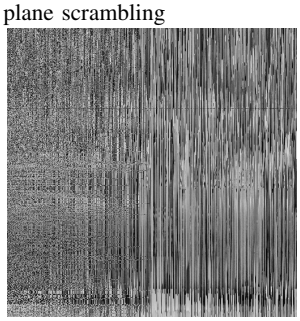
(c) Scrambled by Fibonacci transformation



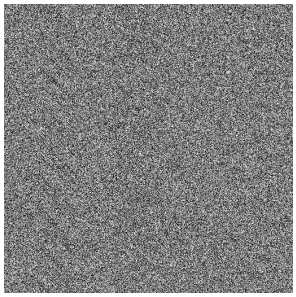
(d) Scrambled by gray code bit plane scrambling



(e) Scrambled by 2D mapping



(f) Scrambled by key based row and column shifting



(g) Scrambled by key based row and column shifting with bit plane scrambling

Fig. 7: Results of scrambling using different scrambling techniques on Pappers image: Original test image 4

TABLE II: Comparative results of correlations and entropy. (Correlation between current pixel and horizontal/diagonal/vertical pixel is found by choosing 1000 random pixels)

Test image	Parameters	Arnold's Transformation	Fibonacci Transformation	Gray code bit plane	2D mapping	row and column shifting	row and column shifting with bit plane scrambling
Airplane image	Correlation (original vs encrypted image)	0.0015	0.0117	0.0505	0.0443	0.0954	0.0016
	Horizontal Correlation	-0.1114	0.4942	0.3177	-0.0553	0.1691	0.0298
	Vertical Correlation	-0.0733	0.3451	0.3573	-0.0538	0.6425	0.0056
	Diagonal Correlation	0.0278	0.3485	0.3008	-0.0550	0.1917	0.0089
	Entropy	6.7025	6.7025	6.7025	0.8236	6.7780	7.9368
Baboon image	Correlation (original vs encrypted image)	4.5970e-04	0.0097	0.0485	0.0033	0.0569	0.0017
	Horizontal Correlation	0.0979	0.3120	0.0485	0.0446	0.0612	0.0481
	Vertical Correlation	0.1232	0.2215	0.0556	0.0722	0.3780	0.0160
	Diagonal Correlation	0.1051	0.0296	0.2883	0.0346	0.0087	0.0090
	Entropy	7.2673	7.2673	3.6133	7.2673	7.1782	7.9523
Lena image	Correlation (original vs encrypted image)	2.4868e-05	3.1170e-05	0.0091	0.0423	0.0139	0.0021
	Horizontal Correlation	0.0327	0.6513	0.1307	0.0626	0.0646	0.0199
	Vertical Correlation	-0.0875	0.4783	0.1676	0.0660	0.6749	0.0165
	Diagonal Correlation	0.1963	0.2036	0.1323	0.0667	0.0680	0.0158
	Entropy	7.4455	7.4455	7.4455	0.7.691	7.4677	7.9976
Peppers image	Correlation (original vs encrypted image)	-0.0110	0.0228	0.0022	0.0380	0.0217	0.0011
	Horizontal Correlation	0.0979	0.5906	0.1134	-0.0434	0.0252	0.0114
	Vertical Correlation	0.0175	0.3675	0.0556	-0.0405	0.6936	0.0050
	Diagonal Correlation	0.1066	0.1561	0.0834	-0.0521	0.0345	0.0398
	Entropy	7.5937	7.5937	7.5937	0.8415	7.6438	7.9966