# Image Encryption using Block Permutation and XOR Operation

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

K. Gayathri Devi
Assistant Professor
Department of Information Technology
PSG College of Technology,Tamilnadu-641004, India.

## ABSTRACT
Now a days, in every communication channel there is a necessity of transmission of messages securely from sender to the authentic receiver. In recent years, for different information transfer systems, a number of data encryption techniques has been evolved. Several encryption approaches based on permutation have been proposed by various researchers. In this paper, for encrypting images, permutation and XOR operation with a key matrix which together fulfill the purpose of cipher is proposed. First the image is divided into blocks which are then shuffled among themselves using random numbers. Lagged Fibonacci Generator (LFG) is used to generate random numbers and further the random numbers are used as key stream for XOR operation. The proposed encryption method is simple and ensures the security of the encrypted images.

## Keywords
Cryptography, image encryption, Lagged Fibonacci Generator (LFG), Random number

## 1. INTRODUCTION
Evolution of computers and Internet has made our life easy but added complexity in terms of security. Innovation in technology over past decade is a huge one [4]. Encryption is the process of information transformation for securing the data [3,4]. Most of the available encryption techniques were designed only for textual data [12]. There are various encryption algorithms such as DES, AES which comes under symmetric encryption algorithms where as RSA algorithm, which is an asymmetric encryption algorithms [1,2]. However, these algorithms are not suitable for image applications due tosome features of images such as redundancy and huge capacity of data [4].Security of digital images has attracted many in recent years and various encryption methods for images has been proposed to enhance the image security such as block based transformations [3,5] and pixel permutation techniques [4,7,8,9]. In this paper, a simple approach has been proposed that involves random permutation of blocks and performing XOR operation over the permuted image with the key generated by using Lagged Fibonacci Generator (LFG) for image encryption. The rest of the paper is organized as follows. Section 2 briefly outlines the literature review of image encryption methods. Section 3 presents the working model of proposed image encryption method. Section 4 deals with the experimental results and analysis. The paper is concluded in section 5.

## 2. LITERATURE REVIEW
Mohammad Ali BaniYounes & AmanJantan [3] proposed an block based transformation algorithm. Where the image is divided into blocks and transformed by proposed transformation algorithm followed by blowfish algorithm to encrypt the original image.

Sesha Pallavi Indrakanthi & P.S. Avadhani [4] proposed permutation based image encryption technique, which performs random pixel permutation over the image without affecting the quality of the image by making use of 64 bit key shared between the sender and the receiver.

Chinmaya Kumar Nayak *et al.* [5] proposed an index based chaotic system for image encryption. In this method, pixels of images were permutated based on the index position on chaotic sequence. Permutation process is carried on, by storing the index position of the sequence respected to their sorted real value of the sequence. Pixel of the image is rearranged and mapped with index position and thus the image is encrypted.

Panduranga H.T & Naveen Kumar S.K [6] proposed an hybrid technique for image encryption that involves scan pattern generated by scan methodology and concept of carrier image. Alphanumeric keyword is used to create carrier image. Thus carrier image is added with original image to produce encrypted image.

Mitra A et al. [7] proposed a new approach to image encryption using combinational permutation technique. The idea behind their approach is to combine different permutation techniques randomly based upon bit, block and pixel, which produces good results when combined together instead carrying it separately for encryption process.

G.A.Sathish kumar & K.BhoopathyBagan [8] proposed an encryption methodology that involves pixel shuffling, base 64 encoding based algorithm. The process involves combination of block permutation, pixel permutation and value transformation.

C.K. Huang et al. [9] proposed a methodology to encrypt gray scale image that involves pixel shuffling and gray level encryption by a single chaotic system. They performed shuffling of rows and columns combined with chaotic system followed by gray level encryption which eliminates image outlines and also changes the distribution of gray level which results in increasing key space.

Qian Mao et al. [10] proposed an image encryption scheme based upon concatenated tour automorphisms. Based upon this novel approach they proposed two application schemes

which includes scrambling matrices and iteration keys acting as secret keys.

Qiang Zhang et al. [11] proposed a novel approach for image encryption based upon DNA subsequence operation. In the methodology they proposed they made use of only simple DNA subsequence operations such as elongation, truncation, delection etc., combined with logistic chaotic map to get the location and value of the pixel points in the image.

B. Nagarajan & P.Manju [13] proposed a image encryption algorithm by making use of Genetic operators, Original image is scrambled with the help of DNA encoding by performing bit level permutation, later genetic operators such as mutation, cross over techniques were used to produce encrypted image.

T.Sivakumar and R.Venkatesan [15] proposed a framework for image encryption that uses Karhunen Loeve (KL) transform that takes input image in the form of square matrix which results in encrypted image and a decryption key. They made use of RSA algorithm to decrypt the key matrix. At receiver, on receiving encrypted image along with key matrix, the receiver multiplies the encrypted image along with transposed decrypted key matrix to get the original image.

T.Sivakumar, and R.Venkatesan [16] proposed an image encryption approach that uses matrix reordering to permute the pixel positions. In order to diffuse the pixel values they performed bitwise XOR operation using pseudo random numbers generated by linear congruential method, which resulted in encrypted image.

# 3. PROPOSED IMAGE ENTRYPTION METHOD

In this section, the proposed image encryption method using permutation and XOR operation is presented. Initially the original gray scale image is divided into blocks of NxN. Random numbers from 1 to N are generated by making use of random function which is being used to permute the divided image. The shuffled blocks of images are merged to form a single image. LFG is being used to produce another set of Random numbers which is then XORed with pixels values of the shuffled image to produce an encrypted image. Figure 1 shows the sequence of operations involving in the proposed encryption method using a block diagram

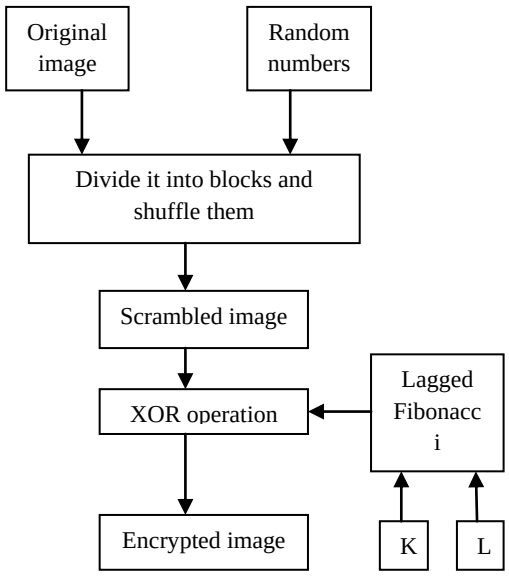



**Figure 1. Block diagram of proposed method**

## 3.1 Lagged Fibonacci Generator

Fibonacci generator is generalized to give a family of pseudo random number generators of the form as given in equation (1)

$X_n = X_{n-l} + X_{n-k} \pmod m$ where $l>k>0$ (1)

Initially, instead of two initial values, l initial values, $X_0$, ……, $X_{l-1}$, are needed inorder to compute the next sequence element. In this expression the "lags" are k and l, so that the current value of X is determined by the value of X k places ago and L places ago. Inaddition, for mostapplications of interest m is a power of two that is, $m = 2^M$.

Table1 gives the list of sample random numbers generated with initial values a=0, b=1 and key values k=2 and l=3.

**Table 1. Sample Random Numbers Generated Using LFG**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 |
| 21 | 26 | 34 | 47 | 60 | 81 | 107 | 141 |
| 188 | 248 | 74 | 181 | 67 | 0 | 248 | 67 |
| 248 | 60 | 60 | 53 | 120 | 113 | 173 | 233 |
| 31 | 151 | 9 | 182 | 160 | 191 | 87 | 96 |
| 23 | 183 | 119 | 206 | 47 | 70 | 253 | 117 |
| 68 | 115 | 185 | 183 | 45 | 113 | 228 | 158 |
| 86 | 131 | 244 | 217 | 120 | 206 | 82 | 45 |

## 3.2 Encryption algorithm

The following are the sequence of steps used to encrypt images.

Input: Original image, random numbers generated using LFG

Output: encrypted image

Step 1: Input the original image and input the block size (N).

Step 2: Original image is divided into blocks of size N*N pixels

Step 3: Generate Random numbers using LFG

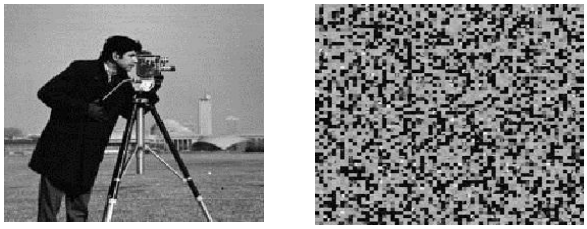
Step 4: Shuffle the block of images using Random numbers.

Step 5: Perform XOR operation between pixel data of the image in each block and the random numbers generated by using LFG.

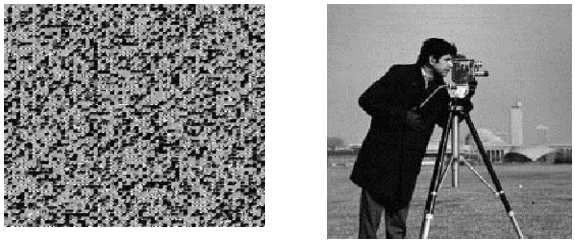
Step 6: Store the encrypted image.

# 4. EXPERIMEMTAL RESULTS AND ANALYSIS

The proposed method is implemented using java with Intel(R) core to dual processor, clock speed of 2.40GHZ, 2GB RAM, 250GB hard disk and Windows 7(32 bit) operating systems. Figure2(a) shows the original image, Figure 2(b) shows the permutated image, Figure 2(c) shows encrypted image by performing XOR operation between random numbers generated and the pixels of permutated image, Figure 2(d) shows the decrypted image.



(a) Original image (b) Permuted image



(c) Encrypted image (d) Decrypted image

**Figure 2. Results of proposed method**

## 4.1 Visual testing

There is no perceptual similarity between encrypted image and original images. The encrypted image should greatly differ from its original form. In general, two difference measures such as NPCR and UACI are used to quantify this requirement [13].

### *4.1.1 Number of Pixel Change Rate (NPCR)*

The Number of Pixels Change Rate (NPCR), which indicates the percentage of different pixels between two images. The mathematical expression for the original image $I_o(i, j)$ and its encrypted image $I_{ENC}(i, j)$ to compute NPCR value is given in the equation (2) shown below [13].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*H} * 100\% \quad (2)$$

Where, W and H are the width and height of the images

### *4.1.2 Unified Average Change Intensity (UACI)*

Even a minute change in original image must cause some major difference or change in cipher image. UACI is helpful to identify the average intensity of difference in pixels between the two images. Equation (3) gives the mathematical expression to compute UACI value for the original image $I_o(i, j)$ and encrypted image $I_{ENC}(i, j)$ is shown below [13].

$$UACI=\frac{1}{W*H}\left[\sum_{i,j} \frac{Io(i,j)-Ienc(i,j)}{255}\right] * 100\% \quad (3)$$

Where, W and H are the width and height of the images.

**Table 2. Results of NPCR measure**

| Image | Existing method | | Proposed method |
|---|---|---|---|
| | NPCR (in %) [3] | NPCR (in %) [13] | NPCR (in %) |
| Camera Man | 99.5163 | 99.4720 | 99.4385 |
| Coin | 99.5209 | 99.5802 | 99.2676 |
| Leena | 99.5524 | 99.5072 | 99.5285 |
| Peppers | 99.5204 | 99.5691 | 99.4583 |
| Baboon | 99.4497 | 99.6824 | 99.5316 |

From Table 2 it is found that, the results of NPCR of proposed method is comparable with the existing methods [3,13].

**Table 3. Results of UACI measure**

| Image | Existing method | | Proposed method |
|---|---|---|---|
| | UACI (in %) [3] | UACI (in %) [13] | UACI (in %) |
| Camera Man | 25.7913 | 30.3288 | 28.2449 |
| Coin | 26.7005 | 30.9832 | 27.5625 |
| Leena | 26.3080 | 30.2477 | 27.1301 |
| Peppers | 25.7327 | 30.1095 | 26.7484 |
| Baboon | 22.8918 | 30.3128 | 23.6760 |

From Table 3, it is found that results of UACI of proposed method is better than the existing method [3] and slightly lower than the method reported in [13]

## 4.2 Adjacent pixel correlation

It is possible to break the ciphers by statistical analysis. This is done by analyzing the correlation between the adjacent pixels in the encrypted image. In order to check whether the suggested method is secure against statistical attacks, the correlation coefficient is measured and analyzed.

From Table 4, it is found that, the result of correlation coefficient of proposed method is comparable with the existing methods [3, 14].

**Table4. Results of correlation coefficient**

| Images | Encrypted image | | |
|---|---|---|---|
| | Horizontal | Vertical | diagonal |
| Original image (Leena) | 0.9929 | 0.9936 | 0.9882 |
| Proposed method | 0.0740 | 0.0738 | 0.0631 |
| Mohammad Ali et al. | 0.0603 | 0.0593 | 0.0584 |

| | | | |
|---|---|---|---|
| [3] | | | |
| G.A Sathish kumar et al. [14] | -0.0332 | 0.0608 | 0.0567 |

## 4.3 Entropy analysis

Entropy is a measure of information content which is unpredictable. Table 5 gives shows about the entropy analysis of original versus encrypted image by the proposed encryption method.

**Table 5. Results of entropy analysis**

| Image | Original image | Encrypted image |
|---|---|---|
| Camera man | 6.7453 | 7.6404 |
| coins | 6.2371 | 7.7577 |
| leena | 7.5636 | 7.7901 |
| peppers | 6.8830 | 7.5878 |
| baboon | 6.7305 | 7.7914 |

# 5. CONCLUSION

In this paper, an image encryption method based on block permutation and XOR operation is implemented and the results were analyzed. The basic idea involves providing one of the easiest methods for encryption process. The process involves dividing the image into blocks and then shuffling them. Pixels of the blocks are XORed with the random numbers to get the encrypted image. Adjacent pixel correlation value of encrypted image is found to be less than that of the original image. From the results of NPCR and UACI values it is clearly shown that the proposed method produces good results comparable with some existing methods. In future, the work is experimented and tested with other random number generators.

# 6. REFERENCES

[1] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi, 2015.

[2] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, New York, 2010.

[3] Mohammad Ali BaniYounes and AmanJantan, "Image encryption using block-based transformation algorithm", IAENG International Journal of Computer Science, Vol 35, No.1, 2008.

[4] Sesha Pallavi Indrakanti and Avadhani P.S, "Permutation based image encryption technique", International Journal of Computer Applications, Vol. 28, No.8, 2011.

[5] Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das, "Image encryption using an enhanced block based transformation algorithm", International Journal of Research and Reviews in Computer Science, Vol. 2, No.2, 2011.

[6] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for image encryption using scan pattern and carrier images", International Journal on Computer Science and Engineering, vol. 2, No. 2, pp. 297-300, 2010.

[7] A. Mitra, Y.V. subba Rao and S.R.M. Prasanna, "A new image encryption approach using combinational permutation techniques", International Journal of Electrical and Computer Engineering, Vol.1, No.2, pp. 127-131, 2006.

[8] G. A. Sathish kumar 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, pp. 169-178, 2011.

[9] 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, No.2, pp. 563-57, 2011.

[10] Qian Mao, Chin-Chen Chang and Hsiao-Ling Wu, "An image encryption scheme based on concatenated torus automorphisms ", KSII Transactions on Internet and Information Systems, Vol. 7, No. 6,pp. 1492-1511, 2013.

[11] Qiang Zhang, Xianglian Xue and Xiaopeng Wei, "A novel image encryption algorithm based on DNA subsequence operation'', The Scientific World Journal, Vol. 2012, Article ID 286741, 2012.

[12] Manju Rani and Sudesh Kumar, "Analysis on different parameters of encryption algorithms for information security", International Journal of Advanced research in Computer Science and Software Engineering", Vol. 5, No. 8, 2015.

[13] B. Nagarajan and P.Manju, "Secure image encryption algorithm based on genetic operators", International Journal on Engineering Technology and Sciences, Vol. 3, No. 5, 2016.

[14] G.A Sathishkumar, K. Bhoopathy and R. Sriraam, "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network security and its Applications, Vol. 3, pp. 181-194, 2011.

[15] T.Sivakumar, and Dr.R.Venkatesan, "A Novel Framework for Image Encryption using Karhunen-Loeve Transform", International Journal of Computer Applications (ISSN 0975-8887), p.no 1- 6, Volume 54– No.2, September 2012.

[16] T.Sivakumar, and R.Venkatesan, "A Novel Image Encryption Approach using Matrix Reordering", wseas transactions on computers, Vol 12, Issue. 11, p.p. 407-418, November 2013.