On the Security of Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform

Esam Elsheh, Saddek Elbendago, Marwan Ali.H.Omer

Abstract— Recent developments of different forms of discrete Fourier transform, have encouraged many researchers to design image encryption algorithms based on a discrete fractional or multiple fractional Fourier transforms. One of these algorithms is proposed by Ashutosh and Sharma, (International Journal of Engineering and Advanced Technology, Vo. 2, Issue. 4, 2013). In this paper, we show that this algorithm represents a classic textbook example of insecure cipher; all the building blocks of this scheme are linear, and thus, breaking this scheme, using a known plaintext attack, is equivalent to solving a set of linear equations. We also invalidate several of the security and performance advantages claimed by the authors, namely, the efficiency, key sensitivity, and the complexity.

Index Terms—Image processing, encryption, discrete transforms, linear cipher.

I. INTRODUCTION

Mathematical Transforms, such as Fourier and Cosine are powerful tools for signal representation, processing and analysis. The discrete forms of these transforms have been extensively applied to many fields including image processing. The Discrete Fourier transform (DFT) can be defined as an invertible transform of a time domain signal into a frequency domain signal. Consequently, the interpretation of the inverse Fourier transform is as a transform of a frequency domain signal into a time domain signal. Motivated by the broad available range of possible applications, these transforms have been generalized by adding additional parameters to their original forms. For instance, the Discrete Fractional Fourier Transform (DFRFT) [1] has been proposed as a generalization for the Fourier transform. The DFRFT transforms a signal, either in the frequency domain or time domain, into the domain between frequency and time; it is a rotation in the time-frequency domain. The DFRFT can be considered as the Fourier transform to the nth power, where it transforms a function to an in-between domain that is between time and frequency. Its applications range from signal analysis and filter design to pattern recognition. With the increasing applications of DFRFT, researchers have put numerous efforts on the development of its theory, where a variety of different versions of FRFTs were developed. Zhu *et al*. [2] constructed a Multiple Fractional Fourier Transform (MFRFT) as a linear combination of the conventional DFRFT. Then, Liu *et al*. [3] proposed the Random Fractional Fourier Transform (RFRFT) by randomizing the transform kernel function of the conventional DFRFT. Later, Tao *et al*. [4] proposed the Multiple- Parameter Fractional Fourier Transform (MPFRFT).

A common characteristic of these generalized transforms is that they have a fairly larger number of independent parameters as compared to their corresponding original forms. Reconstructing the original signal from the transformed domain requires the application of the inverse transform with the same set of parameters corresponding to the ones that were applied to the original signal. Any simple alteration in these parameters would lead to the reconstruction of a distorted version of the signal. These observations have encouraged many researchers to propose image encryption algorithms based on a single or multiple steps of these transforms, where the parameters of these transforms are used as encryption keys. In this paper, we cryptanalyze the image encryption scheme based on the DFRFT that was proposed by Ashutosh *et al*. in [5].

The rest of the paper is organized as follows. In the next section, we briefly review the details of the DFT and DFRFT. In Section III, we explain the image encryption scheme proposed in [5]. In Section IV, we analyze the scheme security and show how to apply the known plaintext attack. We also invalidate several of the performance and security advantages claimed by the authors in section V. Finally, our conclusion and recommendations are presented in Section VI.

II. DISCRETE FRACTIONAL FOURIER TRANSFORM (DFRFT)

In this section, we briefly give some mathematical backgrounds on the Discrete Fourier Transform (DFT) and its extended forms.

The $N \times N$ DFT matrix is defined as

$$\mathbf{F}_{m.n} = \frac{1}{\sqrt{N}} e^{-j\left(\frac{2\pi}{N}\right)mn}, \quad 0 \le m, n \le N-1 \qquad (1)$$

The 1-D discrete Fourier transform DFT for a vector $\mathbf{x}$ is defined as follows,

$$\mathbf{X} = \mathbf{F} \cdot \mathbf{x} \qquad (2)$$

And the 2-D discrete Fourier transform DFT for a $N \times N$ matrix $\mathbf{x}$ is defined as follows,

$$\mathbf{X} = \mathbf{F} \cdot \mathbf{x} \cdot \mathbf{F}^{\mathbf{T}} \qquad (3)$$

The DFT matrix $\mathbf{F}$ has only four distinct eigenvalues $1, -1, j$, and $-j$. Let us define a nearly tridiagonal matrix $N \times N$ matrix $\mathbf{S}$ whose nonzero entries are [6].

Revised Version Manuscript Received on October 24, 2015.

Esam Elsheh, Department of Information Technology, College of Engineering Technology–Janzour, Tripoli, Libya.

Saddek Elbendago, Department of Information Technology, College of Engineering Technology–Janzour, Tripoli, Libya.

Marwan Ali.H.Omer, Department of Information Technology, College of Engineering Technology–Janzour, Tripoli, Libya.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

$$\mathbf{S}_{n,n} = 2\cos\left(\frac{2\pi}{N}\cdot n\right),\quad 0 \le n \le (N-1)$$
$$\mathbf{S}_{n,n+1} = \mathbf{S}_{n+1,n} = 1,\quad 0 \le n \le (N-2)$$
$$\mathbf{S}_{N-1,0} = \mathbf{S}_{0,N-1} = 1. \qquad (4)$$

The matrix **S** commutes with **F** as **SF = FS.** Both matrices **F** and **S** have same eigenvectors but different eigenvalues. Using the eigendecomposition of **F** the authors in [7] defined the ath-order of the $N \times N$ DFRFT matrix as follows,

$$\mathbf{F}^a = \mathbf{V}\boldsymbol{\Lambda}^a\mathbf{V}^T \qquad (5)$$

$$\mathbf{F}^a = \begin{cases} \sum_{k=0}^{N-1} e^{-j\left(\frac{\pi}{2}\right)ka}\,\mathbf{v}_k\mathbf{v}_k^T & \text{for } N \text{ odd} \\ \sum_{k=0}^{N-2} e^{-j\left(\frac{\pi}{2}\right)ka}\mathbf{v}_k\mathbf{v}_k^T + e^{-j\left(\frac{\pi}{2}\right)Na}\mathbf{v}_N\mathbf{v}_N^T & \text{for } N \text{ even} \end{cases}$$

where V is the eigenvectors of matrix F (or **S**), and Λ is a diagonal matrix with its diagonal entries corresponding to the eigenvalues for each column eigenvectors v_k in V , and v_k is the normalized k th-order discrete Hermite–Gaussian-like eigenvector of S.

The αth-order 1-D Discrete Fourier Fractional Transform DFRFT for a vector **x** is calculated as follows,

$$\mathbf{X} = \mathbf{F}^a \cdot \mathbf{x} \qquad (6)$$

And 2-D Discrete Fractional Fourier Transform DFRFT for an $N \times N$ matrix **x** is calculated as follows,

$$\mathbf{X} = \mathbf{F}^a \cdot \mathbf{x} \cdot (\mathbf{F}^a)^T \qquad (7)$$

The DFRFT inherits most of the properties of the DFT. It can be simply verified that DFRFT has the following mathematical properties:

Linearity: DFRFT is a linear transform, *i.e.* $\mathbf{F}^\alpha(a\mathbf{X} + b\mathbf{Y}) = a\mathbf{F}^\alpha\mathbf{X} + b\mathbf{F}^\alpha\mathbf{Y}$, where a and b are constants.

Unitarity: DFRFT is a unitray transform, *i.e.* $\mathbf{F}^{-a} = (\mathbf{F}^a)^*$. The inverse DFRFT is defined as $\mathbf{F}^{-a}$.

III. The Image Encryption Using DFRFT proposed in [5]

The encryption scheme proposed in [5] is an iterative cipher that composed of two rounds. Each round uses an independent random phase matrix and the DFRFT. In the first round, the $N \times N$ original image **P** is multiplied by the random phase matrix $(e^{j\beta m})$ and the resulting matrix is transformed using the DFRFT of order a. The output $N \times N$ matrix **C** is then multiplied by another random phase matrix $(e^{j\gamma n})$ and transformed using DFRFT of order $b - a$ to get the encrypted image **Y**. The two random phase matrices $(e^{j\beta m})$ and $(e^{j\gamma n})$ and the parameters a and $b - a$ are used as the encryption key.

The decryption is a reverse operation of the encryption process, in which the random phase matrices $(e^{-j\beta m})$ and $(e^{-j\gamma n})$, and the DFRFT parameters $a - b$ and $-a$ are used as the decryption key. Mathematically the encryption and decryption processes are summarized as follows,

Encryption:

$$\mathbf{C} = \mathbf{F}^a \cdot \left(\mathbf{P}\otimes e^{j\beta m}\right) \cdot (\mathbf{F}^a)^T \qquad (8)$$
$$\mathbf{Y} = \mathbf{F}^{b-a} \cdot (\mathbf{C}\otimes e^{j\gamma n}) \cdot (\mathbf{F}^{b-a})^T \qquad (9)$$

The operation ⊗ denotes element-by-element multiplication operations of the two operand matrices, and T denotes the transpose of the matrix.

Decryption:

$$\mathbf{C} = \mathbf{F}^{a-b} \cdot (\mathbf{Y}\otimes e^{-j\gamma n}) \cdot (\mathbf{F}^{a-b})^T \qquad (10)$$
$$\mathbf{P} = \mathbf{F}^{-a} \cdot (\mathbf{C}\otimes e^{-j\beta m}) \cdot (\mathbf{F}^{-a})^T \qquad (11)$$

IV. Security of the Image Encryption Scheme proposed in [5]

An introduction to the comprehensive types of cryptanalytic attacks can be found in [8]. A more rigorous mathematical treatment can be found in [9]. The attack described here is a known plaintext attack, i.e., we assume that the cryptanalyst can observe some of the plaintext messages and its corresponding encrypted ciphertext. One should note that, because of the large size of the key required to encrypt a message using the proposed encryption algorithm [5], the assumption that the same encryption key will be used to encrypt several messages is realistic; otherwise, the user is better off using the theoretically secure one-time pad algorithm [9].

The encryption scheme is proposed as an iterative cipher composed from two rounds. Each round consists from simple matrix multiplication operations. The matrix multiplication is a linear operation. For that, each round is a plain linear system. Moreover, cascading of multi linear systems gives a linear. Thus, the whole proposed cryptosystem is just a linear system. Using this fact we can easily apply the known plaintext attack on the proposed cryptosystem to find the secret key.

In the following we will give a toy example of the algorithm where $N = 2$. Let,

$$\mathbf{P} = \begin{bmatrix} p_{1,1} & p_{1,2} \\ p_{2,1} & p_{2,2} \end{bmatrix} \mathbf{F}^a = \begin{bmatrix} f_{1,1}^a & f_{1,2}^a \\ f_{2,1}^a & f_{2,2}^a \end{bmatrix} \mathbf{F}^{b-a} = \begin{bmatrix} f_{1,1}^{b-a} & f_{1,2}^{b-a} \\ f_{2,1}^{b-a} & f_{2,2}^{b-a} \end{bmatrix}$$

$$(e^{j\beta m}) = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{bmatrix} (e^{j\gamma n}) = \begin{bmatrix} \gamma_{1,1} & \gamma_{1,2} \\ \gamma_{2,1} & \gamma_{2,2} \end{bmatrix} \mathbf{C} = \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

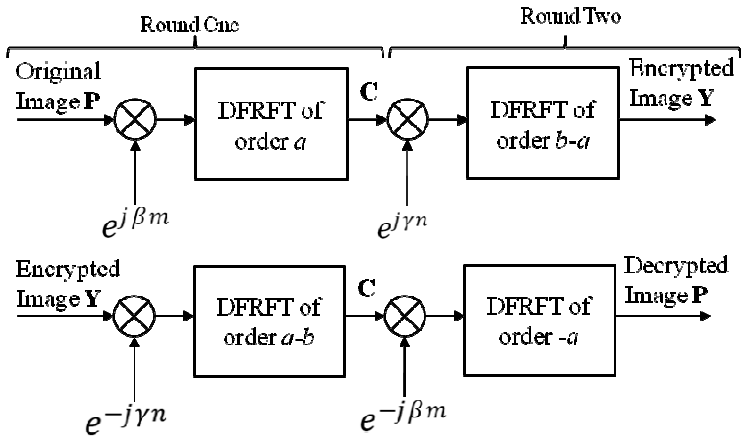


Fig. 1. The encryption and decryption processes of the scheme proposed in [5].

Let $\mathbf{P}_v$, $\mathbf{Y}_v$ and $\mathbf{C}_v$ denotes the vectors obtained by concatenating the elements of the input matrix $\mathbf{P}$, the intermediate matrix $\mathbf{C}$ and the output matrix $\mathbf{Y}$, respectively, as follows,

$$\mathbf{P}_v = \begin{bmatrix} p_{1,1} \\ p_{1,2} \\ p_{2,1} \\ p_{2,2} \end{bmatrix} \quad \mathbf{C}_v = \begin{bmatrix} c_{1,1} \\ c_{1,2} \\ c_{2,1} \\ c_{2,2} \end{bmatrix} \quad \mathbf{Y}_v = \begin{bmatrix} y_{1,1} \\ y_{1,2} \\ y_{2,1} \\ y_{2,2} \end{bmatrix}$$

We can easily retransform the first round relation between matrix $\mathbf{P}$ and the matrix $\mathbf{C}$ in equation (8) from a multiple matrices multiplications to a single matrix multiplication as follows,

$$\begin{bmatrix} c_{1,1} \\ c_{1,2} \\ c_{2,1} \\ c_{2,2} \end{bmatrix} = \begin{bmatrix} f_{1,1}^{a} f_{1,1}^{a} \beta_{1,1} & f_{1,2}^{a} f_{1,1}^{a} \beta_{1,2} & f_{1,1}^{a} f_{1,2}^{a} \beta_{2,1} & f_{1,2}^{a} f_{1,2}^{a} \beta_{2,2} \\ f_{2,1}^{a} f_{1,1}^{a} \beta_{1,1} & f_{2,2}^{a} f_{1,1}^{a} \beta_{1,2} & f_{2,1}^{a} f_{1,2}^{a} \beta_{2,1} & f_{2,2}^{a} f_{1,2}^{a} \beta_{2,2} \\ f_{2,1}^{a} f_{1,1}^{a} \beta_{1,1} & f_{1,2}^{a} f_{2,1}^{a} \beta_{1,2} & f_{1,1}^{a} f_{2,2}^{a} \beta_{2,1} & f_{2,2}^{a} f_{1,2}^{a} \beta_{2,2} \\ f_{2,1}^{a} f_{2,1}^{a} \beta_{1,1} & f_{2,2}^{a} f_{2,1}^{a} \beta_{1,2} & f_{2,1}^{a} f_{2,2}^{a} \beta_{2,1} & f_{2,2}^{a} f_{2,2}^{a} \beta_{2,2} \end{bmatrix} \cdot \begin{bmatrix} p_{1,1} \\ p_{1,2} \\ p_{2,1} \\ p_{2,2} \end{bmatrix}$$

$$\mathbf{C}_v = \mathbf{K}_1 \cdot \mathbf{P}_v \tag{12}$$

where $N^2 \times N^2$ matrix $\mathbf{K}_1$ is considered as the key matrix of the first round.

Following the analysis of the first round, we can also retransform the second round relation between matrix $\mathbf{P}$ and the matrix $\mathbf{C}$ into a simple linear equation, as follows,

$$\mathbf{Y}_v = \mathbf{K}_2 \cdot \mathbf{C}_v \tag{13}$$

$$\begin{bmatrix} y_{1,1} \\ y_{1,2} \\ y_{2,1} \\ y_{2,2} \end{bmatrix} = \begin{bmatrix} f_{1,1}^{b-a} f_{1,1}^{b-a} \gamma_{1,1} & f_{1,2}^{b-a} f_{1,1}^{b-a} \gamma_{1,2} & f_{1,1}^{b-a} f_{1,2}^{b-a} \gamma_{2,1} & f_{1,2}^{b-a} f_{1,2}^{b-a} \gamma_{2,2} \\ f_{2,1}^{b-a} f_{1,1}^{b-a} \gamma_{1,1} & f_{2,2}^{b-a} f_{1,1}^{b-a} \gamma_{1,2} & f_{2,1}^{b-a} f_{1,2}^{b-a} \gamma_{2,1} & f_{2,2}^{b-a} f_{1,2}^{b-a} \gamma_{2,2} \\ f_{2,1}^{b-a} f_{1,1}^{b-a} \gamma_{1,1} & f_{1,2}^{b-a} f_{2,1}^{b-a} \gamma_{1,2} & f_{1,1}^{b-a} f_{2,2}^{b-a} \gamma_{2,1} & f_{2,2}^{b-a} f_{1,2}^{b-a} \gamma_{2,2} \\ f_{2,1}^{b-a} f_{2,1}^{b-a} \gamma_{1,1} & f_{2,2}^{b-a} f_{2,1}^{b-a} \gamma_{1,2} & f_{2,1}^{b-a} f_{2,2}^{b-a} \gamma_{2,1} & f_{2,2}^{b-a} f_{2,2}^{b-a} \gamma_{2,2} \end{bmatrix} \cdot \begin{bmatrix} c_{1,1} \\ c_{1,2} \\ c_{2,1} \\ c_{2,2} \end{bmatrix}$$

Apparently, from the equation above the relation between the input original image and the encrypted image is a simple linear relation.

$$\mathbf{Y}_v = \mathbf{K}_2 \cdot \mathbf{K}_1 \cdot \mathbf{P}_v \tag{14}$$

$$\mathbf{Y}_v = \mathbf{K} \cdot \mathbf{P}_v \tag{15}$$

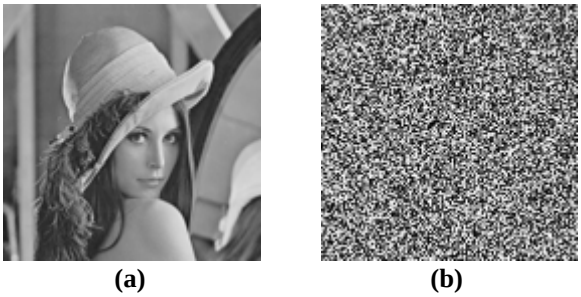
where $N^2 \times N^2$ matrix $\mathbf{K}$ is,

$$\mathbf{K} = \mathbf{K}_2 \cdot \mathbf{K}_1 \tag{16}$$

Therefore, the overall cryptosystem proposed in [5] is linear and the cryptanalyst can recover the $N^2 \times N^2$ elements of the key matrix $\mathbf{K}$ using the N^2 known plaintext-ciphertext pairs, i.e., N^2 original-encrypted image pairs. The set of the linear equations can be simply solved using Gaussian elimination with a complexity $O(N^{2^3})$, or other more advanced techniques can reduce this complexity to $O(N^{2^{2.376}})$.

V. COMMENTS ON THE IMAGE ENCRYPTION SCHEME PROPOSED IN [5]

A. For the purpose of claiming a high level of security of image encryption schemes that based on discrete transforms, their authors regularly use the argument that the encrypted images are visually indistinguishable from random noise. While this is a required condition for any secure image encryption system, this condition is so loose and can be fulfilled by almost any very weak cryptosystem. For instance, in Fig. 2 we encrypted the 128×128 Lena image by multiplying the original image with a random matrix (modular 128), and yet, the resulting image seems as total random noise.



(a) **(b)**

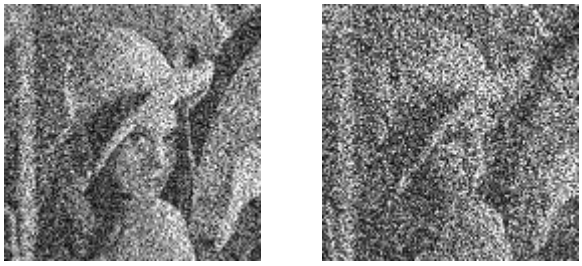
Fig. 2. (a) Lena (b) Encrypted Lena by multiplying with a random matrix.

Thus, demonstrating the security of any image encryption scheme by visual observation is useless practice; seeing a total noisy image as an encrypted image of the encryption scheme does not assure that the proposed algorithm is secure.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

B. It should be noted that the existence of such a high correlation between the images decrypted with slightly incorrect keys and the original images will make the proposed algorithm vulnerable to ciphertext-only attacks using the heuristic search techniques.

It is worth mentioning that the authors in [5] also have published these same results in [10], in which they used $a = 0.6$ and $b = 1.2$ together with with two random phase matrices as the encryption key for their example. In this paper we also invalidate their claim regarding the key sensitivity of the encryption scheme. In Fig. 3, we decrypted Lena with different values of DFRFT orders. Clearly, from the decrypted images most of the distinct features of the original Lena are noticeably visible. Therefore, the proposed algorithm does not meet the Strict Avalanche Criterion (SAC) [13], which is one of the security requirements of the modern ciphers.



(a) **(b)**

Fig. 3. Lena decrypted with (a) $a = 0.6$ $b = 1.2$ (b) $a = 0.6$ $b = 0.6$

C. Several researchers often argue that due to the large data size and real time constrains of multimedia data, the standard encryption algorithms may not be suitable for the multimedia contents. In fact, this was the main motivation for the encryption algorithms that were based on the discrete transforms and its different forms. All the elements of the matrices in these transforms are complex numbers. Thus, the encryption process requires floating point operations which are much slower than typical operations required by modern cryptosystems. Additionally, there is a large data expansion associated with encryption/decryption processes, typically by 1:8 factor. Therefore, the standard algorithms such as AES [14] perform better than the above systems in terms of speed, storage and bandwidth.

VI. CONCLUSION

We showed in this paper that the encryption algorithm proposed in [5] is a classic example of insecure cipher due to its inherent linearity. In practice, the modern encryption algorithm to be called a secure algorithm should fulfill the minimum security requirements by resisting all the basic attacks described in [8]. Accordingly, for the cryptosystems designers we recommend to test their encryption algorithms against all the modern attacks prior to claim any security advantages. Meanwhile, we recommend to the readers to use AES algorithm [14] for their applications that require block ciphers. And for the applications that require stream ciphers, we recommend to use one of the European ECRYPT stream cipher project eSTREAM Portfolio [15]. These algorithms are being examined and verified extensively by cryptographers, and also are optimized to achieve an excellent tradeoff between security and performance in both hardware and software.

REFERENCES

1. H.M. Ozaktas and D. Mendlovic, “Fractional Fourier transforms and their optical implementation,” Journal of the Optical Society of America A: Optics and Image Science, and Vision. vol. 10, no. 12, pp. 2522-2531, 1993.
2. B. Zhu, S. Liu and Q. Ran, “Optical image encryption based on multifractional Fourier transforms,” Opt. Lett., vol. 25, pp. 1159-1161, 2000.
3. Z. Liu and S. Liu, “Random fractional Fourier trans form,” Opt. Letters., vol. 32, pp. 2088-2090, 2007.
4. R. Tao, J. Lang and Y. Wang, ”Optical image encryption based on the multiple-parameter fractional Fourier transform,” Opt. Letters., vol. 33, pp. 581-583, 2008.
5. R. Ashutosh and D. Sharma, “Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform,” International Journal of Engineering and Advanced Technology, vol. 2, no. 4, 2013.
6. B. W. Dickinson and K. Steiglitz, “Eigenvectors and functions of the discrete Fourier transform,” IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP-30, no. 1, pp. 25–31, 1982.
7. S.C. Pei and W.L. Hsue “The Multiple-Parameter Discrete Fractional Fourier Transform,” IEEE Signal Processing Letters, vol. 13, no.. 6, 2006.
8. B. Schneier, Applied Cryptography, 2nd edition. New York,Wiley, 1996.
9. A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptographic Research. Boca Raton, FL: CRC, 1996.
10. R. Ashutosh and D. Sharma, “Robust Technique for Image Encryption and Decryption Using Discrete Fractional Fourier Transform with Random Phase Masking,” Procedia Technology, vol. 10, pp. 707-714, 2013.
11. A.M. Youssef, “On the Security of a Cryptosystem Based on Multiple-Parameters Discrete Fractional Fourier Transform,” Signal Processing Letters, IEEE , vol.15, no., pp.77-78, 2008.
12. E. Elsheh, and A. Youssef, “On the security of image encryption schemes based on Multiple Parameters Transforms,” Signal Processing and Information Technology (ISSPIT), 2010 IEEE International Symposium on , pp.97-101, 2010.
13. A.F.Webster and S.E. Tavares, “On the design of S-boxes”, Advances in Cryptology– CRYPTO ’85 (LNCS 218), pp. 523–534, 1986.
14. National Institute of Standards and Technology, FIPS-197: Advanced Encryption Standard, November 2001.
15. S. Babbage, C. Canniere, A. Canteaut , C. Cid, H. Gilber, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw: The eSTREAM Portfolio, 2009.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.