ON THE SECURITY OF IMAGE ENCRYPTION SCHEMES BASED ON MULTIPLE PARAMETERS TRANSFORMS

Esam Elsheh and Amr Youssef

Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Quebec, Canada
{e_elsh, youssef@ciise.concordia.ca}

ABSTRACT

Recent developments of generalized forms of signal processing transforms with a large number of independent parameters, such as the Multiple Parameter Fractional Fourier Transform and the Discrete Fractional Cosine Transform, have encouraged many researchers to propose image encryption algorithms based on a single or multiple applications of these transforms. In order to claim a high level of security of these parameterized transforms-based schemes, their authors usually use the argument that the encrypted image is visually indistinguishable from random noise.

In this paper, we show that these algorithms represent typical textbook examples of insecure ciphers; all the building blocks of these schemes are linear, and hence, breaking these scheme, using a known plaintext attack, is equivalent to solving a set of linear equations. We also invalidate the argument of relying on the visual quality of the encrypted image ciphertext by presenting an example for a trivially insecure system that produces ciphertext images with the same property. An agrement against the claimed efficiency of these schemes is also provided.

1. INTRODUCTION

Mathematical transforms, such as the Fourier, Cosine, and Wavelet Transforms, have long been powerful tools for signal representation, analysis and processing. The discrete forms of these transforms have been widely applied to many applications including image processing.

Motivated by the wide available spectrum of possible applications, these transforms have been generalized. For example, the Fractional Fourier Transform (FRFT) [1] has been proposed as a generalizing for the Fourier transform. The Fourier transform can be interpreted as a transform of a time domain signal into a frequency domain signal. Similarly, the interpretation of the inverse Fourier transform is as a transform of a frequency domain signal into a time domain signal. The FRFT, on the other hand, transforms a signal, either in the time domain or frequency domain, into the domain between time and frequency; it is a rotation in the time-frequency domain. The FRFT can be thought of as the Fourier transform to the n^{th} power, where it transforms a function to an intermediate domain between time and frequency. Its applications range from filter design and signal analysis to phase retrieval and pattern recognition. Unnikrishnan *et al.* [2] also proposed optical image encryption with FRFT.

With the increasing applications of FRFT, researchers have put numerous efforts on the development of its theory. Consequently, a variety of different forms of FRFTs were defined, which enriched the applications of these transforms. Zhu *et al.* [4] constructed a Multiple Fractional Fourier Transform (MFRFT) as a linear combination of the conventional FRFT. Afterward, Liu *et al.* [5] proposed the Random Fractional Fourier Transform (RFRFT) by randomizing the transform kernel function of the conventional FRFT. Later, Tao *et al.* [6] proposed the Multiple-Parameter Fractional Fourier Transform (MPFRFT) by using the fractionalized method from Shih [3]. Following ideas from the FRFT, a series of transforms, such as Fractional Cosine Transform (FCT) [7], Fractional Hadamard Transform (FRHaT) [8], and Fractional Random Transform (FRT) [9], have been proposed.

A common feature of these generalized transforms is that they have a relatively 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 exact set of parameters corresponding to the ones that were applied to the original signal. Any simple modification in these parameters would lead to the reconstruction of a completely 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. A quick review of the relevant signal processing literature would reveal a surprisingly very large number of image encryption schemes based on these transforms. For example, [10], [11] and [12] propose similar systems based on the Discrete Fractional Fourier Transform (DFRFT). To increase the number of the transform parameters, the authors in [13] introduced the Discrete Multiple Parameter Fractional Fourier Transform (DMPFRFT) and then proposed an image encryption algorithm based on it. Nu *et al.* [14] proposed an image encryption system based on the Mixed Discrete Fourier Transformation (MxDFT) in which the constructed transform matrix is represented as a linear combination of more than one DFRFT. To add more randomness to encrypted images whose energy

978-1-4244-9991-5/11/$26.00 ©2011 IEEE

concentrates around the corners or borders, the Random Discrete Fractional Fourier Transform (RDFRFT) was proposed in [15]. The eigenvectors of the kernel matrix of the RDFRFT are random DFT eigenvectors that are computed from eigenvectors of a random DFT-commuting matrix. Several discrete Fourier-related transforms have been parameterized in order to design image encryption algorithms. For example, Zhou *et al.* [16] present an image encryption system using the Discrete Parametric Cosine Transform (DPCT) and Tao *et al.* [17] present another system based on the Multiple-Parameter Discrete Fractional Hadamard Transform (MPDFrHaT).

The rest of the paper is organized as follows. In the next section, we briefly review the details of three representative samples of these image encryption schemes which are based on RDFRFT [15], Multi Orders Fractional Fourier Transforms [18] and Reciprocal-Orthogonal Parametric (ROP) Transform [19], respectively. In Section 3, we present our main observations about these schemes: all these schemes are linear and hence they can be trivially broken using a known plaintext attack. We also show that relying on the visual quality of the encrypted image does not provide any rigorous proof of security for the underlying system and we discuss the claimed efficiency of these schemes. Finally, our conclusion is presented in Section 4.

2. EXAMPLES OF IMAGE ENCRYPTION ALGORITHMS BASED ON MULTIPLE PARAMETERS TRANSFORMS

In this section, we briefly summarize three representative examples of the image encryption algorithms that are based on parameterized discrete transforms.

2.1. Image Encryption Based on RDFRFT [15]

Recall that the $N \times N$ DFT matrix is defined as

$$[\mathbf{F}]_{m,n} = \frac{1}{\sqrt{N}} e^{-j(2\pi/N)mn}, 0 \le m, n \le N-1. \tag{1}$$

The Eigen decomposition of the DFT matrix $\mathbf{F}$ is given by

$$\mathbf{F} = \sum_{k=0}^{N-1} \lambda_k \mathbf{e}_k \mathbf{e}_k^T \tag{2}$$

where $\mathbf{e}_0, \mathbf{e}_1, \cdots, \mathbf{e}_{N-1}$ form an orthonormal eigenvector basis of the DFT.

The DFRFT $\mathbf{F}^a$ with one parameter a is defined as

$$\mathbf{F}^a = \sum_{k=0}^{N-1} \lambda_k^a \mathbf{e}_k \mathbf{e}_k^T. \tag{3}$$

A generalization of DFRFT, called the Discrete Multiple Parameters Fractional Fourier Transform (DMPFRFT) [13], is defined with the corresponding matrix

$$\mathbf{F}^{\bar{a}} = \sum_{k=0}^{N-1} \lambda_k^{a_k} \mathbf{e}_k \mathbf{e}_k^T. \tag{4}$$

where $\bar{a} = [a_0, a_1, \cdots, a_{N-1}]$.

The RDFRFT [15] with $1 \times N$ parameter vector $\bar{a}$ is obtained by using the random DFT-commuting matrix $\mathbf{H}$ and the DMPFRFT, as follows

$$\mathbf{F}_{\mathbf{H}}^{\bar{a}} = \sum_{k=0}^{N-1} \lambda_k^{a_k} \mathbf{r}_k \mathbf{r}_k^T. \tag{5}$$

where $\mathbf{r}_k$ are the orthonormal random DFT eigenvectors computed from $\mathbf{H}$, λ_k is the DFT eigenvalue corresponding to $\mathbf{r}_k$ and

$$\lambda_k^{a_k} = \begin{cases} (e^{-j2\pi})^{a_k} & \text{if } \lambda_k = 1 \\ (e^{-j\pi/2})^{a_k} & \text{if } \lambda_k = -j \\ (e^{-j\pi})^{a_k} & \text{if } \lambda_k = -1 \\ (e^{-j3\pi/2})^{a_k} & \text{if } \lambda_k = j. \end{cases} \tag{6}$$

The reader is referred to [15] for the steps of obtaining matrix $\mathbf{H}$.

Finally, the 2-D RDFRFT image encryption with secret key parameters ($\bar{a}_1$, $\mathbf{H}_1$, $\bar{a}_2$, $\mathbf{H}_2$) of an $N \times M$ image $\mathbf{P}$ is defined by

$$\mathbf{Q} = \mathbf{F}_{\mathbf{H}_1}^{\bar{a}_1} \cdot \mathbf{P} \cdot \mathbf{F}_{\mathbf{H}_2}^{\bar{a}_2} \tag{7}$$

where $\mathbf{Q}$ is the encrypted image and $\mathbf{F}_{\mathbf{H}_1}^{\bar{a}_1}$, $\mathbf{F}_{\mathbf{H}_2}^{\bar{a}_2}$ are the $N \times N$ and $M \times M$ RDFRFT matrices, respectively.

2.2. Image Encryption Based on the Multi-Orders Fractional Fourier Transform [18]

The $N \times N$ of the p-th order DFRFT is defined as

$$\mathbf{F}_p^N = \mathbf{\Lambda}_{p,u}^N \cdot \mathbf{W}^N \cdot \mathbf{\Lambda}_{p,t}^N \tag{8}$$

where the matrices $\mathbf{F}_p^N, \mathbf{W}^N \in \mathbb{C}^{N\times N}$ and the diagonal matrices $\mathbf{\Lambda}_{p,u}^N, \mathbf{\Lambda}_{p,t}^N \in \mathbb{C}^{N\times N}$ are defined as

$$[\mathbf{W}^N]_{m,n} = e^{-j\frac{2\pi}{N}(m-1)(n-1)},$$

$$[\mathbf{\Lambda}_{p,t}^N]_{n,n} = e^{j\frac{1}{2}\cot(\frac{p\pi}{2})(n-1)^2\cdot\Delta t^2},$$

and

$$[\mathbf{\Lambda}_{p,u}^N]_{n,n} = e^{j\frac{1}{2}\cot(\frac{p\pi}{2})(n-1)^2\cdot\Delta u_p^2}$$

where $p \in (0, 2)$, Δt is the sampling intervals in the time domain, and $\Delta u_p = 2\pi \sin(p\pi/2)/(N\Delta t)$ is the p-th order of Fractional Fourier domain (FRFD). Correspondingly, the p-th order of the inverse DFRFT for an N-length sequence, which is equivalent to the p-th order DFRFT, can be expressed as the Hermite transposition of $\mathbf{F}_p^N$, i.e.,

$$\mathbf{F}_{-p}^N = (\mathbf{F}_p^N)^H = \mathbf{\Lambda}_{-p,t}^N \cdot (\mathbf{W}^N)^H \cdot \mathbf{\Lambda}_{-p,u}^N \tag{9}$$

The encryption is carried as follows: The $A \times B$ original image $\mathbf{P}$ is divided into $M \times N$ sub-images, $\mathbf{P}_{a,b}$, $a = 1, 2, \cdots, M$ and $b = 1, 2, \cdots, N$, with a size of $A/M \times B/N$, which are given by

$$[\mathbf{P}_{a,b}]_{m,n} = [\mathbf{P}]_{(a-1)A/M+m,(b-1)B/N+n} \tag{10}$$

If the column vectors of $\mathbf{P}_{a,b}$ are M-fold interpolated and further $p_{a,b,a}$-th order inverse discrete fractional Fourier transformed, then we can obtain the encrypted sub-images

$\mathbf{Q}_{a,b}$, based on the FRFD analysis of the interpolation [20, 21], as

$$\mathbf{Q}_{a,b} = \begin{bmatrix} \mathbf{D}_{p_{a,b,1},0} \\ \mathbf{D}_{p_{a,b,1},1} \\ \vdots \\ D_{p_{a,b,1},M-1} \end{bmatrix} \mathbf{X}_{a,b}[\mathbf{E}_{p_{a,b,2},0}\, \mathbf{E}_{p_{a,b,2},1} \cdots \mathbf{E}_{p_{a,b,2},N-1}] \tag{11}$$

where the matrix $\mathbf{X}_{a,b} \in \mathbb{C}^{(A/M)\times(B/N)}$ is the two dimensional inverse DFRFT of $\mathbf{P}_{a,b}$, which is given by

$$\mathbf{X}_{a,b} = \mathbf{F}^{A/M}_{-p_{a,b,1}} \cdot \mathbf{P}_{a,b} \cdot (\mathbf{F}^{B/N}_{-p_{a,b,2}})^T$$

The diagonal matrices $\mathbf{D}_{p_{a,b,1},l} \in \mathbb{C}^{(A/M)\times(A/M)}$, $l = 0, 1, \cdots, M-1$ and $\mathbf{E}_{p_{a,b,2},k} \in \mathbb{C}^{(B/N)\times(B/N)}$, $k = 0, 1, \cdots, N-1$ are expressed as

$$[\mathbf{D}_{p_{a,b,1},l}]_{n,n} = e^{-j\frac{1}{2}\cot(\frac{p_{a,b,l}\pi}{2})\cdot[2(n-1)l(A/M)+l^2(A/M)^2]\Delta t^2}$$

$$[\mathbf{E}_{p_{a,b,2},k}]_{n,n} = e^{-j\frac{1}{2}\cot(\frac{p_{a,b,2}\pi}{2})\cdot[2(n-1)k(B/N)+k^2(B/N)^2]\Delta t^2}$$

Then, we obtain the encrypted image $\mathbf{Q}$ by summation of $\mathbf{Q}_{a,b}$

$$\mathbf{Q} = \sum_{a=1}^{M}\sum_{b=1}^{N} \mathbf{Q}_{a,b} \tag{12}$$

2.3. Image Encryption based on the ROP Transform [19]

Any integer n can be represented by r binary digits b_i, $0 \leq i \leq r-1$. If $(-1)^{\sum_{i=0}^{r-1} b_i} = -1$, then n is called a minus integer. The rows of any $N \times N$ matrix are indexed by integer numbers $0, 1, \cdots, N-1$. A row indexed by a minus integer is called a minus-indexed row.

The Reciprocal-Orthogonal Parametric (ROP) $N \times N$ matrix is constructed using a parametric row vector $\mathbf{V}$ of length N and Hadamard matrix $\mathbf{H}$ of order N.

Throughout the rest of this section, we use a toy example with $N = 4$ to illustrate the basic principles of this scheme. The construction of the ROP transform matrix proceeds as follows.

Form a parametric row vector $\mathbf{V} = [1\ a_1\ a_1\ 1]$, with the parameter a_1 is nonzero scalar and arbitrarily chosen from the complex plane.

Construct the Hadamard matrix of order 4

$$\mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

which has four rows that can be indexed from the top to the bottom by 0, 1, 2, 3. In this case, the minus-indexed rows are those that are indexed by 1 and 2. By performing an element-by-element multiplication of each of these minus-indexed rows by the parametric vector $\mathbf{V}$ we obtain the normalized ROP matrix of order four

$$\mathbf{T}_4^{\mathbf{V}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -a_1 & a_1 & -1 \\ 1 & a_1 & -a_1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Let us denote by $\mathbf{T}_N^{\mathbf{V}_i}$ the ROP transform matrix of order N constructed using the parametric vector $\mathbf{V}_i$, which has $N/2 - 1$ independent parameters. Then, we consider four different parametric vectors $\mathbf{V}_1$, $\mathbf{V}_2$, $\mathbf{V}_3$, and $\mathbf{V}_4$ to construct the ROP transform matrices $\mathbf{T}_N^{\mathbf{V}_1}$, $\mathbf{T}_N^{\mathbf{V}_2}$, $\mathbf{T}_N^{\mathbf{V}_3}$, and $\mathbf{T}_N^{\mathbf{V}_4}$, respectively.

The output of the first round is obtained as

$$\mathbf{C} = \frac{1}{4}\ \mathbf{T}_N^{\mathbf{V}_2}(\mathbf{P} \odot [e^{j\alpha(n,m)}])\mathbf{T}_N^{\mathbf{V}_1} \tag{13}$$

whereas the encrypted image $\mathbf{Q}$ of the original image $\mathbf{P}$ of size $N \times N$ is obtained as

$$\mathbf{Q} = \frac{1}{N^2}\mathbf{T}_N^{\mathbf{V}_4}(\mathbf{C} \odot [e^{j\beta(n,m)}])\mathbf{T}_N^{\mathbf{V}_3} \tag{14}$$

where $\odot$ denotes the element-by-element multiplication operation of matrices, $[e^{j\alpha(n,m)}]$ and $[e^{j\beta(n,m)}]$ are two $N \times N$ random phase matrices, $\alpha(n,m)$ and $\beta(n,m)$, $1 \leq n, m \leq N$, are white, uniformly distributed in $[0, 2\pi]$ and independent of each other. The $(2N-4)$ independent parameters $(\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3, \mathbf{V}_4)$ of the matrices $\mathbf{T}_N^{\mathbf{V}_1}$, $\mathbf{T}_N^{\mathbf{V}_2}$, $\mathbf{T}_N^{\mathbf{V}_3}$, and $\mathbf{T}_N^{\mathbf{V}_4}$ and the random phase matrices are used as the encryption secret keys.

3. MAIN OBSERVATIONS

An introduction to different types of cryptanalytic attacks can be found in [24]. A more rigorous mathematical treatment can be found in [25]. The attack described here is a known plaintext attack, i.e., we assume that the cryptanalyst can observe some of the plaintext images and its corresponding encrypted ciphertext. One should note that, because of the large size of the key required to encrypt an image using these multiple parameter transforms, the assumption that the same encryption key will be used to encrypt several images is realistic; otherwise, the user is better off using the theoretically secure one-time pad algorithm [25].

3.1. Known plaintext attack

Despite the apparent complexity of some of the above generalized transforms, a common feature in all of them is that there is an equivalent matrix description for each one of them.

In order to avoid unnecessary mathematical notation, consider the toy example of the RDFRFT image encryption system presented in the previous section with $N = 2$.

Let $\mathbf{F}_{\mathbf{H}_1}^{\bar{\alpha}_1} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $\mathbf{F}_{\mathbf{H}_2}^{\bar{\alpha}_2} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, $\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$ and $\mathbf{Q} = \begin{bmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{bmatrix}$.

Then we have

$$\begin{bmatrix} q_{11} \\ q_{12} \\ q_{13} \\ q_{44} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{21} & a_{12}b_{11} & a_{12}b_{21} \\ a_{11}b_{12} & a_{11}b_{22} & a_{12}b_{12} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{21} & a_{22}b_{11} & a_{22}b_{21} \\ a_{21}b_{12} & a_{21}b_{22} & a_{22}b_{12} & a_{22}b_{22} \end{bmatrix} \begin{bmatrix} p_{11} \\ p_{12} \\ p_{13} \\ p_{44} \end{bmatrix}.$$

By noting that the decomposition of linear systems is linear. Similar relation follow for the two other systems presented in Section 2. Also, adding an arbitrary large number of rounds would not add any nonlinearity to these schemes. Consider an $N \times M$ image $\mathbf{P}$. Let $\mathbf{I}_{NM\times 1}$ and $\mathbf{O}_{NM\times 1}$ denote the column-vectors obtained by concatenating the elements of the input plaintext matrix, $\mathbf{P}$, and the output ciphertext matrix, $\mathbf{Q}$, respectively. Then, for all the above encryption systems, we have

$$\mathbf{O} = \mathbf{K} \times \mathbf{I}$$

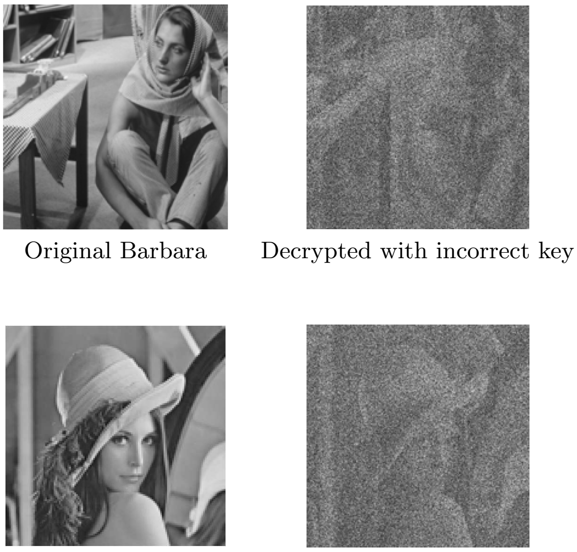
where $\mathbf{K}$ is an $NM \times NM$ equivalent key matrix whose elements can be recovered using $O(NM)$ known plaintext-ciphettext pairs. While the complexity of solving the above system of equations using Gaussian elimination is given by $O((NM)^3)$, other more advanced techniques can reduce this complexity to $O((NM)^{2.37})$. It should be noted that this complexity is much less than the usually claimed security level of these systems.

A folklore argument that is typically presented by the authors of image encryption schemes based on parameterized discrete transforms is that their proposed schemes are more secure than others because their underlying transforms utilize a larger number of transform parameters which increases the length of the corresponding secret keys. For example, the DMPFRFT-based scheme in [22] claim better security than DFRFT because it uses more parameters compared to the DFRFT.

Contrary to the above folklore argument, when considering this basic forms of known plaintext attacks, an encryption system based on a generalized transform with a huge number of parameters is equally as bad as any transform with very small number of parameters; both of them can be broken with the same complexity. Similarly, adding an arbitrary large number of transform rounds would not increase the security of these schemes.

3.2. Visual Quality of Encrypted Images

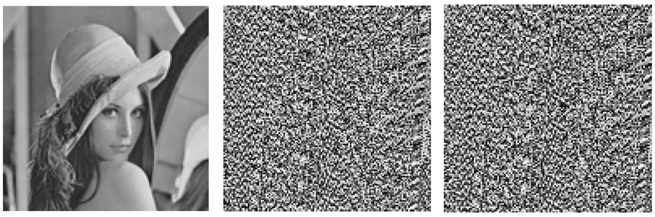
In order to claim a high level of security of these parameterized transforms-based schemes, their authors usually use the argument that the encrypted images are visually indistinguishable from random noise. While this is a necessary condition for any secure image encryption system, this condition is so loose to the extent that it can be satisfied by almost any system, even if it has a very poor security. Verifying the security of any image encryption scheme by visual observation is worthless practice; seeing a total random image as an encrypted image of the encryption scheme does not provide any assurance that the proposed algorithm is secure. As an illustration of this observation, Fig 2 shows the encrypted image using 11-bit Linear Feedback Shift register-based stream cipher (ciphertext only attack against this LFSR cipher, using the berlekamp massey algorithm [25], requires only 22 bits.) In fact, as depicted in Fig. 1, this trivially insecure 11-bit LFSR shows better key avalanche properties when compared to some published schemes. It should be noted that the existence of such a high correlation between images decrypted with slightly incorrect keys and the original images may also facilitate ciphertext only attacks using heuristic search techniques.



Original Barbara | Decrypted with incorrect key

Original Lena | Decrypted with incorrect key

Fig. 1. Examples of images decrypted with slightly incorrect keys for the ROP-based algorithm [19].



(a) (b) (c)

Fig. 2. (a) Lena (b) Lena encrypted by an LFSR (c) Lena decrypted with a slightly incorrect key (1 bit difference).

3.3. Inefficiency of the proposed Schemes

Due to the large data size and real time constrains of multimedia data, some researchers argue that algorithms that standard encryption algorithms may not be suitable for multimedia data. In fact, this reason is usually used as the main motivation for many parameterized transform based image encryption systems. However, since all the elements of the matrices corresponding to these parameterized transforms are complex numbers, the encryption process require floating point operations which are much slower than the typical operations required by modern symmetric key ciphers. Also, there is usually a large data expansion associated with the encryption process because, unlike the plaintext, the ciphertext belongs to the set of complex numbers (which typically means an expansion by a 1 : 8 factor.) Thus, current standard algorithms such as AES [23] outperform the above systems in terms of both encryption speed, bandwidth, and storage requirements.

4. CONCLUSIONS

Because of their inherent linearity, encryption algorithms based on generalized multiple parameters transforms are not secure. Careful analysis of the performance of these algorithms also reveal their inefficiency in terms of both bandwidth and throughput. For practical applications requiring block ciphers, we recommend the use of the AES algorithm. Similarly, for applications requiring stream ciphers, we recommend the use of one of the seven stream ciphers defined, by European ECRYPT stream cipher project, in the the eSTREAM Portfolio. These algorithms have undergone extensive cryptanalytic reviews by the cryptographic community and are optimized to achieve an excellent tradeoff between security and performance.

5. 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] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain, ,” Opt. Lett., vol. 25, pp. 887-889, 2000.

[3] C.C. Shih, “Fractionalization of Fourier transform,” Optics Communications. vol. 118, no. 5-6, pp. 495-498, 1995.

[4] B. Zhu, S. Liu and Q. Ran, “Optical image encryption based on multifractional Fourier transforms, ” Opt. Lett., vol. 25, pp. 1159-1161, 2000.

[5] Z. Liu and S. Liu, “Random fractional Fourier transform,” Opt. Lett., vol. 32, pp. 2088-2090, 2007.

[6] R. Tao, J. Lang and Y. Wang, “Optical image encryption based on the multiple-parameter fractional Fourier transform,” Opt. Lett., vol. 33, pp. 581-583, 2008.

[7] S.C. Pei and M.H. Yeh, “The discrete fractional cosine and sine transforms,” IEEE Transactions on Signal Processing. vol. 49, no. 6, pp. 1198-1207, 2001.

[8] R. Tao, J. Lang and Y. Wang,“ The multiple-parameter discrete fractional Hadamard transform,” Optics Communications, vol. 282, no. 8, pp. 1531-1535, 2009.

[9] Z.J. Liu, H.F. Zhao and S.T. Liu, “A discrete fractional random transform ,” Opt. Communications, vol. 255, pp. 357-365, 2005.

[10] J.M. Vilardy, J.E. Calderon, C.O. Torres and L. Mattos, “Digital images phase encryption using fractional Fourier transform,” Electronics, Robotics and Automotive Mechanics Conference CERMA, 2006.

[11] Y. Zhang and F. Zhao, “The algorithm of fractional Fourier transform and application in digital image encryption,” International Conference on Information Engineering and Computer Science ICIECS, 2009.

[12] H. Yoshimura, and R. Iwai, “New encryption method of 2D image by use of the fractional Fourier transform,” International Conference on Signal Processing ICSP, 2008.

[13] S.C. Pei and W.L. Hsue, “The multiple-parameter discrete fractional Fourier transform,” IEEE Signal Process. Lette., vol. 13, no. 6, pp. 329-332, 2006.

[14] N. Du, S. Devineni and A.M. Grigoryan, “Mixed Fourier transforms and image encryption,” IEEE International Conference on Systems, Man, and Cybernetics, 2009.

[15] S.C. Pei and W.L. Hsue, “Random discrete fractional Fourier transform,” IEEE Signal Process. Lette., vol. 16, no. 12, 2009.

[16] Y. Zhou, K. Panetta and S. Agaian, “Image encryption using discrete parametric cosine transform,” Conference on Signals, Systems and Computers, Record of the Forty-Third Asilomar 2009.

[17] R. Tao , J. Lang and Y. Wang, “The multiple-parameter discrete fractional Hadamard transform,” Journal of Optics Communications, vol. 282, no. 8, pp. 1531-1535, 2009.

[18] R. Tao, X.Y. Meng and Y. Wang, “Image encryption with multi-orders fractional Fourier transforms,” IEEE Transactions on Information Forensics and Security, vol. pp, no.99, pp. 1-, 2010.

[19] S. Bouguezel, A.M. Omair and M.N.S. Swamy, “Image encryption using the reciprocal-orthogonal parametric transform,” IEEE International Symposium on Circuits and Systems ISCAS, 2010.

[20] X.Y. Meng, R. Tao and Y. Wang, “The fractional Fourier domain analysis of decimation and interpolation,” Science in China, Ser.F, vol. 50, pp. 521-538, 2007.

[21] X.Y. Meng, R. Tao and Y. Wan, “Fractional Fourier domain analysis of cyclic multirate signal processing,” Science in China, Ser E, vol. 51, pp. 803-819, 2008.

[22] Y. Xiao, H, Zhang, Q. Ran, J. Zhang and L. Tan, “Image encryption and two dimensional discrete M-parameter fractional Fourier transform,” International Congress on Image and Signal Processing CISP, 2009.

[23] National Institute of Standards and Technology, FIPS-197: Advanced Encryption Standard, November 2001.

[24] B. Schneier, Applied Cryptography, 2nd ed. New York:Wiley, 1996.

[25] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptographic Research. Boca Raton, FL: CRC 1996.