On the Security of a Cryptosystem Based on Multiple-Parameters Discrete Fractional Fourier Transform

Amr M. Youssef, *Senior Member, IEEE*

***Abstract*—Pei and Hsue (IEEE Signal Processing Letters, Vol. 13, No. 6, pp. 329–332, June 2006) proposed an encryption scheme based on multiple-parameter discrete fractional Fourier transform. We show that all the building blocks of this scheme are linear, and hence, breaking this scheme, using a known plaintext attack, is equivalent to solving a set of linear equations.**

***Index Terms*—Discrete fractional Fourier transform, media security, multimedia signal processing, multiple-parameter discrete fractional Fourier transform.**

I. Introduction

The discrete fractional Fourier transform (DFRFT) [1], [2] is a generalization of the discrete Fourier transform (DFT) with one additional order parameter. Pei and Hsue [3] extended the DFRFT to have N order parameters, where N is the number of the input data points, and showed that the proposed multiple-parameter discrete fractional Fourier transform (MPDFRFT) has all of the desired properties for fractional transforms. They also exploited the multiple-parameter feature of the MPDFRFT and proposed the double random phase encoding in the MPDFRFT domain for encrypting digital data. Based on their experimental results, Pei and Hsue argue that their proposed scheme in the MPDFRFT domain significantly enhances data security. In particular, they claim that when this scheme is used to encrypt a 256 × 256 image, the algorithm cracking time on a PC (Pentium 4, 2.4-GHz CPU) is about 5.46×10^{134}.

In this short letter, we analyze the security of the MPDFRFT encryption scheme. Our analysis shows that all the building blocks of this scheme are linear, and hence, breaking this scheme, using a known plaintext attack, is equivalent to solving a set of linear equations.

Using the same notation as in [3], Fig. 1 shows the encryption process of the double random phase encoding in the MPDFRFT domain. The operation $\otimes$ denotes an element-by-element multiplication operations of the two operand matrices.

The 2D-MPDFRFT of a given $N \times M$ data matrix $\mathbf{P}$ with parameter vectors $(\overline{a}, \overline{b})$ is given by

$$\mathbf{P}_{(\overline{\mathbf{a}},\overline{\mathbf{b}})} = \mathbf{F}^{\overline{\mathbf{a}}} \cdot \mathbf{P} \cdot \mathbf{F}^{\overline{\mathbf{b}}}$$

where $\mathbf{F}^{\overline{a}}$ and $\mathbf{F}^{\overline{b}}$ are the N-point and M-point MPDFRFT matrices, respectively, and $\overline{a}$ and $\overline{b}$ are the parameter vectors of sizes $1 \times N$ and $1 \times M$, respectively.

$[exp(j\alpha(n,m))]$ and $[exp(j\beta(n,m))]$ denote the two $N \times M$ random phase matrices, where $\alpha(n,m)$ and $\beta(n,m)$, as well as $1 \leq n \leq N$ and $1 \leq m \leq M$ are both white and uniformly distributed in $[0, 2\pi]$.

The order parameters of the 2D-MPDFRFT, i.e., $(\overline{a}, \overline{b})$, $(\overline{c}, \overline{d})$ as well as the two random phase matrices, are used as the encryption key.

For further details about the MPDFRFT encryption, the reader is referred to [3]. Related works on optical encryption schemes and their vulnerabilities can be found in [4]–[6].

II. Security of the MPDFRFT Encoding Algorithm

Schneier [7] provides a nice introduction to different types of cryptanalytic attacks. A mathematical treatment can be found in [8].

The attack described here is a known plaintext attack, i.e., we assume that the cryptanalyst can observe some of the plaintext and its corresponding ciphertext blocks. One should note that the size of the key required to encrypt an $N \times M$ image is much larger than the size of the image itself, and hence, the assumption that the same encryption key will be used for encrypting several input images is a realistic assumption; otherwise, the user is better off using the theoretically secure one-time pad algorithm [8].

The interested reader is referred to [7] for different scenarios on how to apply this kind of attack in practice.

From Fig. 1, it is clear that we can think of the double random phase encoding algorithm as an iterative cipher with two rounds. Each round consists of simple matrix multiplication operations which are linear operation. Since the composition of linear operations is also linear, hence, the whole round function is also linear.

To avoid unnecessary complex mathematical notation, we will illustrate our observation using a toy version of the algorithm with $N = M = 2$. Consider one round of the algorithm shown in Fig. 1. Let

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}, \ [exp(j\alpha(n,m)] = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$$

$$\mathbf{F}^{\overline{a}} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \text{ and } \mathbf{F}^{\overline{b}} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Manuscript received September 12, 2006; revised November 20, 2006. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant N00930. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Zhou Wang.

The author is with Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1T7, Canada (e-mail: youssef@ciise.concordia.ca).

Digital Object Identifier 10.1109/LSP.2007.910299

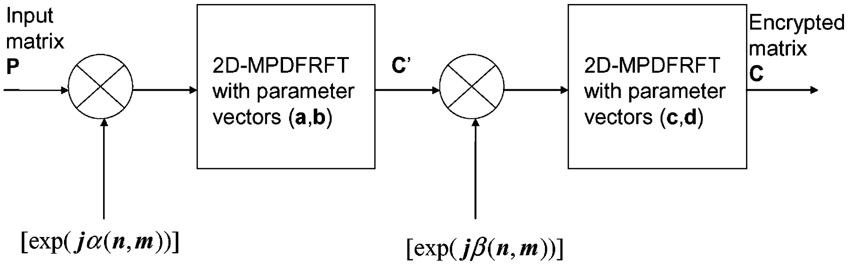

Fig. 1. Encryption process of the double random phase encoding in the MPDFRFT domain [3].

It is straightforward to show that the elements of the first round output matrix, $\mathbf{C}'$, are related to the elements of the plaintext input matrix, $\mathbf{P}$, by the following linear relation:

$$\begin{bmatrix} c'_{11} \\ c'_{12} \\ c'_{21} \\ c'_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}\alpha_{11} & a_{11}b_{21}\alpha_{12} & a_{12}b_{11}\alpha_{21} & a_{12}b_{21}\alpha_{22} \\ a_{11}b_{12}\alpha_{11} & a_{11}b_{22}\alpha_{12} & a_{12}b_{12}\alpha_{21} & a_{12}b_{22}\alpha_{22} \\ a_{21}b_{11}\alpha_{11} & a_{21}b_{21}\alpha_{12} & a_{22}b_{11}\alpha_{21} & a_{22}b_{21}\alpha_{22} \\ a_{21}b_{12}\alpha_{11} & a_{21}b_{22}\alpha_{12} & a_{22}b_{12}\alpha_{21} & a_{22}b_{22}\alpha_{22} \end{bmatrix} \times \begin{bmatrix} p_{11} \\ p_{12} \\ p_{21} \\ p_{22} \end{bmatrix}. \quad (1)$$

From the above argument, it follows that the encoding process of the random phase encoding in the MPDFRFT domain is linear irrespective of the number of rounds. Let $\mathbf{V}_o$ and $\mathbf{V}_i$ denote the vectors obtained by concatenating the elements of the input plaintext matrix $\mathbf{P}$ and the output ciphertext matrix $\mathbf{C}$, respectively, as in (1). Then, for any arbitrary number of rounds, the relation between the ciphertext vector, $\mathbf{V}_o$, and the plaintext, $\mathbf{V}_i$, can always be described by a linear relation of the form

$$\mathbf{V}_o = \mathbf{K} \cdot \mathbf{V}_i$$

where $\mathbf{K}$ is an $NM \times NM$ key-dependent 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 $O((NM)^{2.376})$ [10], [11]. For 256 × 256 images, the complexity of the Gaussian elimination is given by $O(2^{48})$ which requires much shorter time than the 5.46×10^{134} years claimed in [3].

III. Conclusion

We showed that the multiple-parameters discrete fractional Fourier transform encryptions algorithm is linear, and hence, it is insecure. We do not claim any novelty in the presented attack. In fact, as it was noted by one of the anonymous reviewers that the above system is almost a typical textbook example of an insecure cipher. On the other hand, and although a minimum requirement for any cryptosystem is that it should be secure, we still need to mention some points regarding the performance of the above class of algorithms. Since all the elements of the matrices above are complex numbers, hence, the encryption process requires floating point operations which are much slower than the typical operations required by modern symmetric key ciphers. One should also note that there is a large data expansion associated with the encryption process because, unlike the plaintext, the ciphertext belongs to the set of complex numbers. Thus, current standard algorithms such as AES [9] outperform the above system in terms of both encryption speed, bandwidth, and storage requirements. In fact, we recommend the use of standard algorithms in practical applications, including multimedia applications, since these standards have undergone extensive cryptanalytic reviews and are optimized to achieve a good tradeoff between security and performance.

Acknowledgment

The author would like to thank the anonymous referees for their valuable comments.

References

[1] S. C. Pei and M. H. Yeh, "Improved discrete fractional Fourier transform," *Opt. Lett.*, vol. 22, pp. 1047–1049, 1997.

[2] C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[3] S. Pei and W. Hsuec, "The multiple-parameter discrete fractional fourier transform," *IEEE Signal Process. Lett.*, vol. 13, no. 6, pp. 329–332, Jun. 2006.

[4] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767–769, 1995.

[5] G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.*, vol. 39, pp. 2853–2859, 2000.

[6] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, pp. 1644–1646, 2005.

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

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

[9] Federal Information Processing Standards Publication (FIPS 197), Advanced Encryption Standard (AES), Nov. 26, 2001.

[10] V. Strassen, "Gaussian elimination is not optimal," *Numerische Mathematik*, vol. 13, no. 3, pp. 354–356, 1969.

[11] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *J. Symbol. Comput.*, vol. 9, no. 251, p. 280, 1990.