Optics Communications 376 (2016) 47–51

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Security of image encryption scheme based on multi-parameter fractional Fourier transform

Tieyu Zhao [a,*], Qiwen Ran [a], Lin Yuan [a,b], Yingying Chi [c], Jing Ma [a]

[a] State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin 150001, China
[b] College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China
[c] School of Psychology, Northeast Normal University, Changchun 130024, China

ARTICLE INFO

Article history:
Received 22 October 2015
Received in revised form
4 May 2016
Accepted 8 May 2016
Available online 12 May 2016

Keywords:
Multi-parameter fractional Fourier transform
Image encryption
Information security

ABSTRACT

Recently, multi-parameter fractional Fourier transform (MPFRFT) has been widely applied in the optics cryptosystem, which has attracted more and more researchers' attention. However, in further study we find a serious security problem on the MPFRFT which is the multi-choice of decryption key corresponding to an encryption key. The existence of multi-decryption-key hinders the application of this algorithm. We present a new generalized fractional Fourier transform, which can overcome the problem and enlarge the key space. The simulation results show that the proposed algorithm has higher security and key sensitivity.

1. Introduction

The application of the Fourier transform (FT) well solved the problems of optical signal processing. FRFT greatly expanded the application of the FT in optics and with the development of the study, its optical implementation methods were proposed. The FRFT was a generalized FT, and it had more flexibility and research value. In 1980, the FRFT was first proposed by Namias in the quantum mechanics and used to explain the Schrödinger equation under various conditions [1]. However, it as a new mathematical method has no physical meaning. In 1987, McBride and Kerr presented the integral form of the FRFT, which perfected and promoted the concept of Namias [2]. Since 1993, Mendlovic and Ozaktas published a series of articles [3–5] in which optical FRFT was defined in a gradient refractive index (GRIN) and can be implemented by using simple lens. As Lohmann said: "FT is such an important for optics and optical information processing, so that its each event in mathematics can have important impact on the optical field [6]. "In 1995, Refregier and Javidi proposed optical image encryption scheme based on 4f system [7]. Whereafter, the scheme was extended to the FRFT domain by Unnikrishnan [8]. The transform order also can be used as the encryption key in addition to the random phase matrix so that the security of the system was improved. In 2000, Zhu et al. proposed an optical image encryption method based on multi-fractional Fourier transforms (MFRFT) [9] which was a generalized FRFT, so the transform cycle can also be used as a key. In 2005, Ran et al. proposed general MFRFT method based on the generalized permutation matrix group [10]. Pei et al. proposed an image encryption method based on multiple-parameter discrete fractional Fourier transform (MPDFRFT) [11] that significantly enhanced data security because the order parameters of the MPDFRFT can be exploited as extra keys for decryption. In 2007, Liu et al. proposed a random fractional Fourier transform (RFRFT) by using random phase modulations and the optical implementation was also presented based on the Lohmann's type FRFT configuration [12]. In 2008, Tao et al. proposed multi-parameter fractional Fourier transform (MPFRFT) that is applied to optics image encryption [13]. Whereafter, Ran et al. analyzed the security and the reliability of the encryption schemes based on the FRFT and MPFRFT. The results shown that the image encryption methods had deficiencies, and modified MPFRFT proposed can avoid all the deficiencies [14]. Hence, the image encryption schemes [15–24] were proposed based on MPFRFT, which greatly enriched the research of this field.

In this paper, we analyze the MPFRFT and its application in image encryption, and the results show that this algorithm has great potential safety risk which hinders its application in signal processing. We present a new generalized FRFT which not only overcomes the deficiency but also enlarges the key space. So it has higher security in the image encryption. In theory, it is an

* Corresponding author.
E-mail address: zty03y3213@163.com (T. Zhao).

http://dx.doi.org/10.1016/j.optcom.2016.05.016
0030-4018/

extension of FRFT so that it has further research value.

2. Weighted fractional Fourier transform

In 1995, Shih proposed a new FRFT by using a superposition method of state function [25]. This FRFT can be defined as a linear combination of the four state functions, namely primitive function and its once, twice, triple order Fourier transform. Logically, such defined FRFT was independent of the previous various definitions. The definition was as follows:

$$F^{\alpha}[f(t)] = \sum_{l=0}^{3} A_l(\alpha) f_l(t) \tag{1}$$

here $f_0(t) = f(t)$, $f_1(t) = (Ff_0)(t)$, $f_2(t) = (Ff_1)(t)$, $f_3(t) = (Ff_2)(t)$.

$$A_l(\alpha) = \cos\left(\frac{(\alpha - l)\pi}{4}\right)\cos\left(\frac{2(\alpha - l)\pi}{4}\right)\exp\left(\frac{-3(\alpha - l)i\pi}{4}\right) \tag{2}$$

In 2000, Zhu et al. proposed a generalized fractional Fourier transform (Multi-fractional Fourier transforms) [9] which was mainly used in image encryption. The MFRFT is defined as follows:

$$F_M^{\alpha}[f(t)] = \sum_{l=0}^{M-1} A_l(\alpha) f_l(t), \tag{3}$$

Here $f_l(t) = F^{4l/M}[f(t)]$, the weighting coefficient is

$$A_l = \frac{1}{M}\sum_{n=0}^{M-1} \exp\left[-\frac{2\pi i(\alpha - l)}{M}\right], \tag{4}$$

so MFRFT can be represented as

$$F_M^{\alpha}[f(t)] = \frac{1}{M}\sum_{n=0}^{M-1}\sum_{l=0}^{M-1} \exp\left[-\frac{2\pi i(\alpha - l)}{M}\right] f_l(t). \tag{5}$$

Comparing with the previous FRFT, the image encryption based on MFRFT was more secure due to the introduce of key M.

In 2008, Tao et al. proposed the MPFRFT based on the MFRFT, and it was applied to the optical image encryption with even higher security [13]. It was defined as follows:

$$F_M^{\alpha}(\mathfrak{M}, \mathfrak{N})[f(t)] = \sum_{l=0}^{M-1} A_l(\alpha, \mathfrak{M}, \mathfrak{N}) f_l(t) \tag{6}$$

Here basis function $f_l(t) = F^{4l/M}[f(t)]$, $l = 0, 1, 2, \cdots, M-1$. The weighted coefficient was:

$$A_l(\alpha, \mathfrak{M}, \mathfrak{N}) = \frac{1}{M}\sum_{k=0}^{M-1} \exp(-2\pi i/M)\left[(m_k M + 1)\alpha(k + n_k M) - lk\right] \tag{7}$$

$\mathfrak{M} = (m_0, m_1, \cdots, m_{(M-1)}) \in \mathbb{Z}^M$. $\mathfrak{N} = (n_0, n_1, \cdots, n_{(M-1)}) \in \mathbb{Z}^M$.

So vector parameters $(\mathfrak{M}, \mathfrak{N})$ can be used as the encryption key.

Whereafter, Ran et al. proposed the modified MPFRFT, and the parameter range was extended to real number field [14]. The method was widely used in image encryption, and its definition was as follows:

$$F_M^{\alpha}(\mathfrak{N})[f(t)] = \frac{1}{M}\sum_{l=0}^{M-1}\sum_{k=0}^{M-1} \exp(-2\pi i/M)\left[\alpha(k + n_k M) - lk\right] f_l(t). \tag{8}$$

The same basis function $f_l(t) = F^{4l/M}[f(t)]$, $\mathfrak{N} = (n_0, n_1, \cdots, n_{(M-1)}) \in \mathbb{R}^M$.

The modified MPFRFT overcame the defect of periodicity and the parameter range was extended to real number field which led to higher security.

3. Analysis and discussion

3.1. Security analysis

The modified MPFRFT on one hand overcame the periodicity-deficiency of FRFT. On the other hand the parameters' range extended to the real number field which greatly enlarged the key space, enhanced the security level and further widened its application in image encryption [15–24].

However with the develop of research, it shows that the image encryption methods based on the modified MPFRFT have deficiency of multi-solution corresponding to one encryption key and thus decrease the security level of the encryption method. Here we unify MFRFT, MPFRFT and the modified MFRFT as

$$F_M^{\alpha}(\mathfrak{N})[f(t)] = \sum_{l=0}^{M-1} A_l(\alpha, \mathfrak{N}) f_l(t), \tag{9}$$

here basis function $f_l(t) = F^{4l/M}[f(t)]$ and the parameter $\mathfrak{N} = (n_0, n_1, \cdots, n_{(M-1)}) \in \mathbb{R}^M$.

$$A_l(\alpha, \mathfrak{N}) = \frac{1}{M}\sum_{k=0}^{M-1} \exp\left\{\frac{-2\pi i}{M}\left[\alpha(k + n_k M) - lk\right]\right\}. \tag{10}$$

We define the new FRFT as MFRFT here and after.

In the encryption process the encryption keys are $[M, \alpha, \mathfrak{N}]$. Here M is the expansion cycle, α is transform order, and $\mathfrak{N}$ is the vector parameter. The keys $[M, -\alpha, \mathfrak{N}]$, $[M, -\alpha, \mathfrak{N} + b]$, and $b \in \mathbb{R}$ can decrypt correctly. Such deficiency greatly weakens the security of cryptosystems and also hinders the application of the transformation in other areas.

3.2. The simulation verification

In the simulation experiments, we use the software Matlab (2011b) based on the computer and image "Lena" with 200*200 pixels as example.

The encryption keys:

$$K = (M, \alpha, \mathfrak{N}) = \left[4, \sqrt{6}, (\sqrt{23}, 5.2, \sqrt{3.4}, \sqrt{71})\right],$$

The decryption keys:

$$K' = (M, -\alpha, \mathfrak{N}) = \left[5, -\sqrt{6}, (\sqrt{23}, 5.2, \sqrt{3.4}, \sqrt{71})\right], \text{ and}$$

$$K'(b) = (M, -\alpha, \mathfrak{N} + b) = \left[5, -\sqrt{6}, (\sqrt{23} + b, 5.2 + b, \sqrt{3.4} + b, \sqrt{71} + b)\right], b \in \mathbb{R}.$$

Let $b = \sqrt{5}$, the simulation results are shown in Fig. 1. Fig. 1 (a) and (b) are the original image and the encrypted image respectively. Fig. 1(c) and (d) are the decrypted image by keys K' and $K'(b)$ respectively. The smallest error is acceptable between two decrypted images as shown in Fig. 2.

3.3. The theoretical analysis

Here by means of theoretical analysis we analyze the defect of multi-solution. The weighting coefficient of the MPFRFT is:

$$A_l(\alpha, \mathfrak{N}) = \frac{1}{M}\sum_{k=0}^{M-1} \exp\left\{\frac{-2\pi i}{M}\left[\alpha(k + n_k M) - lk\right]\right\}, \tag{11}$$

therefore,