Optics Communications ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Optics Communications

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

Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps

Liansheng Sui [a,*], Kuaikuai Duan [a], Junli Liang [b]

[a] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[b] School of Automation and Information, Xi'an University of Technology, Xi'an 710048, China

ARTICLE INFO

Article history:
Received 6 December 2014
Received in revised form
6 January 2015
Accepted 7 January 2015

Keywords:
Discrete multiple-parameter fractional angular transform
Two-coupled logistic map
Double-image encryption

ABSTRACT

A new discrete fractional transform defined by the fractional order, periodicity and vector parameters is presented, which is named as the discrete multiple-parameter fractional angular transform. Based on this transform and two-coupled logistic map, a double-image encryption scheme is proposed. First, an enlarged image is obtained by connecting two plaintext images sequentially and scrambled by using a chaotic permutation process, in which the sequences of chaotic pairs generated by using the two-coupled logistic map. Then, the scrambled enlarged image is decomposed into two new components. Second, a chaotic random phase mask is generated based on the logistic map, with which one of two components is converted to the modulation phase mask. Another component is encoded into an interim matrix with the help of the modulation phase mask. Finally, the two-dimensional discrete multiple-parameter fractional angular transform is performed on the interim matrix to obtain the ciphertext with stationary white noise distribution. The proposed encryption scheme has an obvious advantage that no phase keys are used in the encryption and decryption process, which is convenient to key management. Moreover, the security of the cryptosystem can be enhanced by using extra parameters such as initial values of chaos functions, fractional orders and vector parameters of transform. Simulation results and security analysis verify the feasibility and effectiveness of the proposed scheme.

1. Introduction

Due to the rapid popularity of internet, issues on image encryption, authentication and communication are becoming more and more serious in order to avoid illegal access. Image encryption based on optical systems has attracted a growing attention recently, which has inherent advantages of high speed for processing multidimensional data in parallel. In the past decades, numerous kinds of optical cryptosystems have been investigated for the security of image information, in which the classical one is double random phase encoding (DRPE) scheme [1]. Most optical systems are formed by combining DRPE and different transform such as fractional Fourier transform (FrFT) [2–7], Fresnel transform (FrT) [8–11], gyrator transform (GT) [12–15], discrete cosine transform (DCT) [16–19], fractional angular transform domain [20,21] and others [22–26], which are generalization of Fourier transform (FT) with additional parameters as private keys. Generally, Chen et al. [27] provided a clear description on current development in optical cryptosystem and showed some light on future development. Additionally, Alfalou and Brosseau [28] pointed out that optical techniques can be used for compression operations simultaneously.

In order to reduce the overload of image communication on internet, the double-image encryption has attracted lots of attentions in recent years. Liu et al. [29] presented a double-image encryption scheme by using the iterative random binary encoding in gyrator transform domain, where two secret images are regarded as the real part and imaginary part of complex function and exchanged reciprocally under the control of random binary data. Chen et al. [30] proposed a double-image encryption method based on diffractive imaging with a laterally-translated phase grating which obtained several diffraction intensity patterns as ciphertext images. Wang et al. [31] defined a random orthogonal matrix to linearly recombined two secret images and encrypted the blended images into the ciphertext based on the DRPE. Zhong et al. [32] utilized two scrambled plaintext images as the phase and amplitude of a complex function which is encoded based on DRPE in fractional Fourier domain. In order to solve the problem that the cryptosystem based on phase-truncated Fourier transform is vulnerable to the specific attack proposed in [33], Zhao and Wang [34] encrypted secret images into the amplitude cyphertext and decrypted the primary images by using the DRPE system. Li

* Corresponding author.
E-mail address: liudua2010@gmail.com (L. Sui).

http://dx.doi.org/10.1016/j.optcom.2015.01.021
0030-4018/© 2015 Published by Elsevier B.V.

et al. [35] designed a double-image encryption scheme based on the chaos-based local pixel scrambling technique in GT domain, where Arnold transform is employed to scramble pixels. Wang et al. [36] mixed two primitive images to a single complex function with the help of a random binary distribution matrix, and then encrypted the complex function by using the multistage phase encoding. Xiao and Zhang [37] employed Chirikov standard map to scramble the pixels of two secret images that are considered as the amplitude and phase of the synthesized function. Wang et al. [38] recorded information of each image into two intensity interference patterns of FrFT spectra and recombined encrypted images into a synthetic ciphertext by using the random mixed encoding. Wang et al. [39] presented two security layers encryption scheme by controlling a random amplitude mask, in which the nonlinear spatial and spectral encoding technique is used to eliminate the risk of information disclosure. Sui et al. [40] designed a chaotic confusion-diffusion process to scramble images and encoded two new components into the phase and amplitude part of a complex function, which is transformed to the ciphertext by using discrete fractional random transform. Sui et al. [41] scrambled plaintext images to obtain two components by using cat map, in which one component is directly separated into two phase masks and the other component is used to derive the ciphertext image by using the cascaded discrete fractional random transforms.

Though the aforementioned double-image encryption schemes can improve efficiency of image transmission and communication, the phase masks usually are used as private keys in most cryptosystems, which is not convenient for storage, transmission and management of keys. In order to overcome this shortcoming, the multiple-parameter-based encryption scheme is proposed, in which the security is enhanced with additional keys instead of phase keys. Lang [42] reported an image encryption algorithm based on the discrete multiple-parameter fractional Fourier transform (DMPFrFT) without the use of phase key, where the security of information can be enhanced by using extra parameters of the transform. Shan et al. [43] presented a double image encryption based on the DMPFrFT, where one original image is scrambled by chaotic map and used as the amplitude of a complex function and the other image is encoded as the phase part. Zhou et al. [44] proposed an image encryption method by using the discrete multiple-parameter fractional Fourier transform, which is constructed with the fractional order, the periodicity and the vector. Generally, the aforementioned multiple-parameter fractional transforms all inherit the mathematic property of the corresponding basic transform. Wu et al. [45] proposed a four-image encryption method based on spectrum truncation, chaos and the multiple-order discrete fractional Fourier transform (MODFrFT), where the spectrum truncation is employed in discrete FT domain and the resultant performance is better than similar algorithm.

In this paper, a new discrete multiple-parameter fractional angular transform (DMPFAT) is presented. Based on the proposed transform, a double-image encryption scheme is designed where the plaintext images can be transformed to the ciphertext simply without using any phase keys. First, two plaintext images are combined into an enlarged one in the way of connecting them sequentially. Then, the enlarged image is scrambled by using a chaotic permutation process based on the two-coupled logistic map and divided into two new components, through which the statistical information of plaintext images can be destroyed thoroughly. Second, a chaotic random phase mask is generated based on the logistic map, with which one of two components is converted to the modulation phase mask. Another component is encoded into an interim image with the help of the modulation phase mask. Finally, the DMPFAT is carried out on the interim image to obtain the ciphertext and common phase function. In the encryption and decryption processes, the initial values of chaos functions, the fractional orders and vector parameter of the DMPFAT are used as keys. The proposed encryption scheme has high resistance against to the potential attacks such as chosen plaintext attack, and has inherent immunity to the specific attack that is fatal to the encryption scheme based on phase-truncated Fourier transform. Moreover, the proposed scheme has obvious advantage that no phase keys are used, which is convenient to the storage, transmission and management of private keys. Simulation results and security analysis verify the feasibility and effectiveness of the proposed scheme.

The rest of this article is organized as follows. In Section 2, the basic principles and the process of encryption and decryption are introduced in detail. In Section 3, numerical simulation results and security analysis are given. Finally, the conclusion is given in Section 4.

2. Encryption and decryption process

2.1. Discrete multiple-parameter fractional angular transform

The discrete fractional angular transform (DFAT) [21] has been widely used for image encryption due to its excellent properties such as linearity, multiplicity, index additivity and Parseval energy conservation and so on. Supposing α denotes the fractional order and β denotes the angle parameter, the DFAT of one-dimensional signal f with N points is described as

$$T_{\alpha,\beta} = A_N^{\alpha,\beta} f, \tag{1}$$

and for two-dimensional signal g, it can be defined as

$$T_{\alpha,\beta} = A_H^{\alpha,\beta} g A_W^{\alpha,\beta}, \tag{2}$$

where $A_N^{\alpha,\beta}$, $A_H^{\alpha,\beta}$ and $A_W^{\alpha,\beta}$ are the kernel matrices of the DFAT. Take the kernel matrix $A_N^{\alpha,\beta}$ as an example, which is denoted as

$$A_N^{\alpha,\beta} = V_N^{\beta} D_N^{\alpha} (V_N^{\beta})^t, \tag{3}$$

where V_N^{β} and D_N^{α} are the eigenvector matrix and eigenvalue matrix of DFAT respectively, β denotes the angle and α denotes the fractional order. The eigenvalue matrix of DFAT is expressed as

$$D_N^{\alpha} = \mathrm{diag}\left[1, \exp\left(-i\frac{2\pi\alpha}{T}\right), \exp\left(-i\frac{4\pi\alpha}{T}\right), \cdots, \exp\left(-i\frac{2(N-1)\pi\alpha}{T}\right)\right]. \tag{4}$$

where the coefficient T is a positive integer. When $N = 2$ and $N = 3$, the eigenvector matrices V_2^{β} and V_3^{β} are calculated as follows:

$$V_2^{\beta} = \begin{bmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{bmatrix}, \tag{5}$$

$$V_3^{\beta} = \begin{bmatrix} \cos\beta & \sin\beta & 0 \\ 0 & 0 & 1 \\ -\sin\beta & \cos\beta & 0 \end{bmatrix}. \tag{6}$$

For other case, the eigenvector matrix can be calculated by using a recursion process which depends on the following equations:

$$V_{2N} = \frac{1}{\sqrt{2}} \begin{bmatrix} V_N, & V_N \\ -V_N^Z, & V_N^Z \end{bmatrix}, \tag{7}$$

and