Optics and Lasers in Engineering 62 (2014) 139–152

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain

Liansheng Sui [a,b,*], Kuaikuai Duan [a], Junli Liang [c], Zhiqiang Zhang [a], Haining Meng [a]

[a] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[b] Shaanxi Key Laboratory for Network Computing and Security Technology, Xi'an 710048, China
[c] School of Automation and Information, Xi'an University of Technology, Xi'an 710048, China

ARTICLE INFO

Article history:
Received 19 March 2014
Received in revised form
2 June 2014
Accepted 2 June 2014

Keywords:
Multiple-image encryption
Phase-only function
Asymmetric cryptosystem

ABSTRACT

A multiple-image encryption scheme is proposed based on the asymmetric technique, in which the encryption keys are not identical to the decryption ones. First, each plain image is scrambled based on a sequence of chaotic pairs generated with a system of two symmetrically coupled identical logistic maps. Then, the phase-only function of each scrambled image is retrieved with an iterative phase retrieval process in the fractional Fourier transform domain. Second, all phase-only functions are modulated into an interim, which is encrypted into the ciphertext with stationary white noise distribution by using the fractional Fourier transform and chaotic diffusion. In the encryption process, three random phase functions are used as encryption keys to retrieve the phase-only functions of plain images. Simultaneously, three decryption keys are generated in the encryption process, which make the proposed encryption scheme has high security against various attacks, such as chosen plaintext attack. The peak signal-to-noise is used to evaluate the quality of the decrypted image, which shows that the encryption capacity of the proposed scheme is enhanced considerably. Numerical simulations demonstrate the validity and efficiency of the proposed method.

1. Introduction

With the rapid popularity of computer and internet, the exchange of information plays an important role in modern society. Images as an effective carrier of information have been widely used in various fields. The acquisition, transmission and processing of image have been seen at every corner of the digital age, and so image security issues have become increasingly serious and aroused a lot of attention. Since Refregier and Javidi proposed the optical image encryption based on input plane and Fourier plane random encoding [1], lots of schemes on optical image encryption have been put forward in other domains such as fractional Fourier transform (FrFT) [2–8], gyrator transform (GT) [9–12], Fresnel transform (FrT) [13–15], and fractional Mellin transform [16–18]. Alfalou and Brosseau [19] analyzed the performance on different methods and pointed out many schemes can be used for compression simultaneously. Though most optical schemes have excellent properties such as parallel and multi-dimensional capability of signal processing, it should be pointed out that these schemes belong to the category of symmetric cryptosystems, where the keys are identical in the encryption and decryption processes. Due to the inherently linear property of mathematical or optical transformation, these schemes are vulnerable to the conventional attacks such as chosen plaintext attack. Additionally, most schemes mainly discuss the single image encryption, which reduce the efficiency when encrypting, storing and transmitting multiple images.

In order to relieve the network load, the double-image encryption has attracted lots of attentions. Li and Wang [20] proposed a double-image encryption based on iterative GT, where two plain images are encrypted into a single one as the amplitude of GT with different groups of angles simultaneously. Liu et al. [21,22] suggested the double-image encryption schemes in the GT domain not only by using iterative random binary encoding but also by using random phase encoding and pixel exchanging. Additionally, Liu et al. [23] encrypted two plain images into the amplitude and phase of a complex function, respectively, in which the discrete fractional angular transform is used. Zhang and Xiao [24] designed a double optical image encryption by using the discrete Chirikov standard map which is utilized to scramble the pixel positions and intensity values, respectively. Li and Wang [25] proposed a double-image encryption based on discrete fractional random transform and chaotic maps, which can raise the efficiency when encrypting, storing or transmitting. Sui et al. [26] proposed a double-image encryption based on discrete fractional random transform, where

* Corresponding author at: School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China. Tel.: +86 2982312231; fax: +86 29 82312220.
E-mail address: liudua2010@gmail.com (L. Sui).

http://dx.doi.org/10.1016/j.optlaseng.2014.06.003
0143-8166/

a chaotic confusion-diffusion process is used to break the correlations between adjacent bit planes efficiently. Moreover, Wang and Zhao [27] suggested an asymmetric double-image encryption which has a high level of robustness against the specific attack.

With the development of double-image encryption techniques, more and more researchers pay their attentions to multiple-image encryption. Situ and Zhang [28,29] proposed the multiple-image encryption schemes based on wavelength multiplexing and position multiplexing. Alfalou and Mansour [30] proposed a multiple images encryption scheme based on double random phase encoding, in which target images are multiplexed and encoded by using the iterative Fourier transform (FT). Subsequently, Alfalou and Brosseau [31] reported an algorithm to compress and encrypt multiple target images simultaneously based on a specific spectral multiplexing operation, where a fingerprint image is used as the first encryption key and a random phase key as the second key in order to achieve good security level. Similarly, Alfalou et al. [32] suggested a multiple-image encryption scheme based on the discrete cosine transform (DCT) and the specific spectral filtering technique, which implemented simultaneous fusion, compression and encryption of multiple images. Liu et al. [33] proposed an optical multi-image encryption based on frequency shift technique, where the lower frequency parts of the plain images are selected, shifted and encrypted by using double phase encoding in FrFT domain. Compared with other schemes, its optical implementation is efficient. Wang and Zhao [34] designed a multiple-image encryption based on the nonlinear phase truncation operations in FT domain, which can avoid the disadvantages of the classical double random phase encoding scheme and is vulnerable to conventional attacks such as chosen plaintext attack. Additionally, Wang and Zhao [35] proposed a fully phase multiple-image encryption based on superposition principle and digital holographic technique, where a real-valued plain image is encoded into a phase-only function (POF). Hwang et al. [36] proposed a multiple images encryption in FrT domain based on modified Gerchberg-Saxton algorithm (MGSA), which reduces the cross-talks of the decrypted images significantly. Based on MGSA, Chang et al. [37,38] suggested the position multiplexing encryption schemes by using cascaded phase-only masks and Huang et al. [39] designed the scheme with architecture of two adjacent phase-only functions in FrT domain to increase capacity of the cryptosystem. Deng and Zhao [40] proposed a multiple-image encryption algorithm using phase retrieve algorithm and intermodulation in Fourier domain, which can avoid the cross-talk noise completely, but the convergent speed of iterative process should be further improved.

Recently, due to the excellent properties such as ergodicity, pseudo-randomness, sensitivity to initial conditions and control parameters, the chaotic maps are used to encrypt image in different transform domains, which can strengthen the nonlinearity of plain image in spatial and transform domains. Singh and Sinha [41,42] proposed an optical image encryption schemes based on chaos not only in FrFT domain but also in GT domain. Liu and Wang [43] suggested a color image encryption based on spatial bit-level permutation, in which three channels of color image are confused and diffused by the high-dimensional chaotic map. Li et al. [44] designed a double-image encryption based on the chaos-based local pixel scrambling technique in GT domain, where two images are regards as the amplitude and phase of a complex function and then Arnold transform is used to scramble pixels at the local area. 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. Singh and Sinha [46] proposed a multiple images encryption based on chaos and multiple canonical transforms, where three linear canonical transforms such as FrFT, extended FrFT and FrT are utilized.

In this paper, an asymmetric multiple-image encryption scheme is proposed based on the coupled logistic maps in FrFT domain, in which the encryption keys are not identical to the decryption ones. First, a sequence of chaotic pairs is generated by using a system of two symmetrically coupled identical logistic maps and used to scramble the plain images. The POF of each scrambled image is retrieved by using an iterative process in the FrFT domain. Second, all POFs are modulated into an interim, which is transformed to the real-value ciphertext with stationary white noise distribution by using the FrFT and chaotic diffusion. Three random phase functions are used as encryption keys to retrieve the phase-only functions of plain images and three decryption keys are generated in the encryption process. Comprehensive application of the iterative process and chaos map makes the convergent speed faster when retrieving the POFs of plain images. Additionally, the cryptosystem enlarges the key space and achieves good encryption. Numerical simulations demonstrate the validity and efficiency of the proposed method.

The rest of this article is organized as follows. In Section 2, the basic principles and the processes 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. Logistic map and two-coupled logistic map

Chaos theory is a famous theory on the study of nonlinear dynamics, in which seemingly random events are actually predictable from simple deterministic equations. The dynamical systems are established based on various chaos functions such as logistic map, Lorenz attractors and so on. A chaos function has three properties: (1) it is sensitive to initial conditions; (2) it is topologically mixing; (3) its periodic orbits are dense. With a chaotic map, a large number of random iterative values with the desirable properties of non-correlation, pseudo-randomness and ergodicity are generated. These random iterative values are limited between bounds, and their convergence after any value of iterations is never seen. The chaotic maps have demonstrated great potential for information security, especially for image encryption.

The logistic map is a one-dimensional nonlinear chaos function and defined as

$$f(x) = p \times x \times (1-x). \tag{1}$$

The function is bound for $0 \le p \le 4$, which is the system parameter known as bifurcation parameter. The iterative form of the logistic map is denoted as

$$x_{n+1} = p \times x_n \times (1-x_n). \tag{2}$$

where $x_n \in (0,1)$ is the iterative value and x_0 is the initial value. The dynamical systems in chaotic state at the time $p \in [3.5699456, 4]$ and slight variations of the initial parameter can yield a totally different random iterative value which is a non-periodic and non-converging sequence over time.

However, some drawbacks exit in the cryptosystem using one-dimensional chaotic map to permute image, such as small key space, poor efficiency and weak security. To overcome these limitations, the chaos function is usually composed of two coupled one-dimensional nonlinear maps which control corresponding parameters. In accordance with such a principle, a system of two symmetrically coupled identical logistic maps [47] which is