Optics and Lasers in Engineering 113 (2019) 29–37

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms

Sui Liansheng [a,b,*], Zhang Xiao [a], Huang Chongtian [d], Tian Ailing [c], Anand Krishna Asundi [d]

[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] Shaanxi Province Key Lab of Thin Film Technology and Optical Test, Xi'an Technological University, Xi'an 710048, China
[d] School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore 639798, Singapore

ARTICLE INFO

Keywords:
Multiple-image encryption
Interference-based encryption
Fractional Fourier transform

ABSTRACT

An optical approach of silhouette-free multiple-image encryption based on interference is proposed, with two layers to enhance the level of security. In the first layer, a group of plain images are encoded into an amplitude distribution, called interim, using the cascaded fractional Fourier transforms. In the second layer, the interim is encrypted into two noisy ciphertext images. The two layers are compactly combined into a single whole to assure that the inherent silhouette problem is removed through the involvement of a random phase-only mask as the built-in function of cryptosystem. In addition to the phase mask keys generated in the process of encryption, the security is enhanced further by considering the fractional order as an additional key. Numerical simulations are given to demonstrate the feasibility and validity of this approach.

1. Introduction

With the rapid development of optical technology and Internet, image as an important carrier of information plays a vital role in communication due to its vivid and intuitive characteristics. To solve its security issues in the process of storage and transmission, more and more researchers have paid their attention to optical methods, which have some excellent advantages such as fast parallel processing, large key space and high robustness against various kinds of attacks [1–5]. Since the classic double random phase encoding scheme have been proposed in Fourier transform domain [6], a large number of approaches extended in different domains such as fractional Fourier domain, Fresnel domain and gyrator domain have been applied in the field of image security [7–16]. Meanwhile, various kinds of security schemes based on different optical technologies such as polarized light, photon-counting, integral imaging, diffractive imaging, holographic and others have been investigated [17–28], which have been verified to have great potential in the field of information security.

Although the interference has been applied to encode an image into two phase-only masks with an inherent silhouette problem [29–32], the interference-based optical information processing methods have gained more and more attention due to its obvious characteristics such as no iterative calculations. For instance, Wang et al. [33] combined the sparse representations of plain images into an interim based on space multiplexing, and then encrypted the interim into two ciphertext images. Zhong et al. [34] used discrete multiple-parameter fractional Fourier transform to generate three phase-only masks to avoid silhouette problem. Due to efficient and enhanced security concerns, more and more results on multiple-image encryption have emerged in recent years. Wan et al. [35] encrypted multiple images into one hologram by means of implementing the interference of multiple object beams and unique reference beam. Wu et al. [36] encoded each plain image into an intensity vector using computational ghost imaging with different diffraction distance, and considered the superposition of all vectors as ciphertext. Yi and Tan [37] constructed a basic binary-tree encryption scheme in gyrator domain, where each node is based on asymmetric double random phase encoding. Yuan et al. [38] verified two original images by using part of phase information of encrypted result, which is encrypted in non-separable fractional Fourier transform domain. Chang et al. [39] transformed plain images into noise-like digital holograms, and then decomposed them into a number of basis images, which are stored as encrypted data. Sui et al. [40] encoded each images into phase-only mask using the nonlinear iterative phase retrieval algorithm, and then synthesized all phase masks into the final ciphertext image based on phase mask multiplexing technology.

Differing from most optical multiple-image encryption schemes where an interim is encoded from one of plain images individually and then all interims are integrated into the ciphertext image using multiplexing methods such as space multiplexing and phase mask

* Corresponding author at: School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048 China.
E-mail address: liudua2010@gmail.com (S. Liansheng).

https://doi.org/10.1016/j.optlaseng.2018.10.002
Received 28 July 2018; Received in revised form 5 September 2018; Accepted 3 October 2018

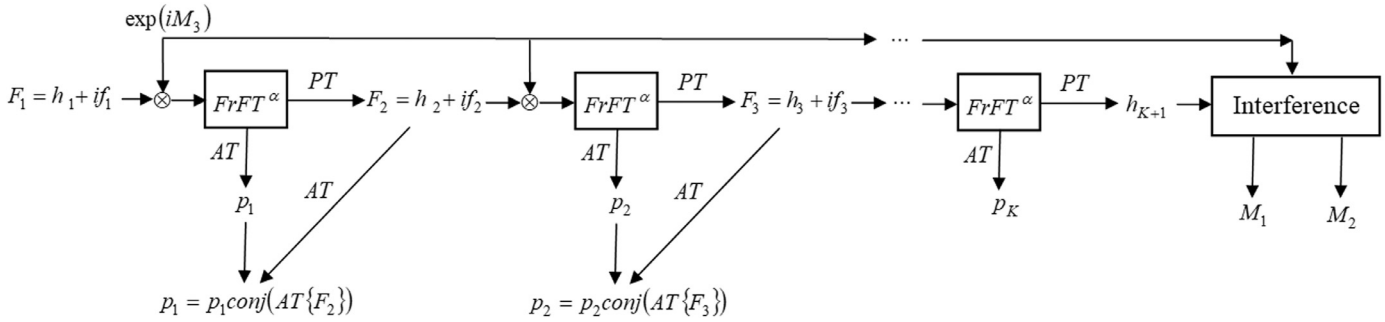

Fig. 1. Schematic diagram of the encryption process.

multiplexing and so on, the plain images are initially encoded by using the fractional Fourier transforms with the help of a random amplitude mask during the process of encryption in the proposed scheme. Then, the obtained result is encrypted into two ciphertext images using the silhouette-free interference method, where no valid information relative to original images can be discerned when only one of ciphertext images is used for decryption. Meanwhile, the corresponding phase-only mask considered as the security key is generated in the process of fractional Fourier transform according to each plain image. Furthermore, the affection of cross-talk noise existed in aforementioned multiple-image encryption schemes based on multiplexing can be avoided as well as the hierarchical decryption can be implemented, where the user with high authority can possess more security keys and access more original information.

The rest of this paper is organized as follows. In Section 2, the encryption and decryption processes of proposed optical multiple-image encryption scheme are introduced in detail. Meanwhile, the fractional Fourier transform is introduced briefly, and then the silhouette-free interference mechanism is described. In Section 3, numerical experiments and security analysis are performed. Finally, a brief conclusion is given in Section 4.

2. Scheme description

To enhance the level of security, there are two layers in the proposed multiple-image encryption scheme. In the first layer, a series of plain images are encoded into an interim amplitude distribution using the cascaded fractional Fourier transforms. In the second layer, the amplitude distribution is encrypted into two ciphertext images based on silhouette-free interference. The schematic diagram of the encryption procedure is shown in Fig. 1. Supposing that there are a series of plain images to be encrypted, represented as $f_i, i = 1, 2, \dots, K$ and K is the total number of plain images, the details of the encryption process can be depicted as follows

(1). A random image h_1 with the same size as plain images is generated, where the intensity values of pixels are randomly distributed in the range [0, 255]. A complex image $F_1 = h_1 + if_1$ is then constructed by means of taking h_1 as the real part and f_1 as the imaginary part, respectively, which is used as the input to the cascaded fractional Fourier transform procedures in the first layer.

(2). The image F_1 is multiplied by a random phase mask $\exp(iM_3)$ and modified into another complex function using the fractional Fourier transform with a fractional order α, which can be mathematically expressed as

$$\bar{F}_1 = FrFT^{\alpha}\{F_1 \exp(iM_3)\}. \tag{1}$$

Here, $FrFT^{\alpha}\{\cdot\}$ denotes the fractional Fourier transform with the order α, and M_3 is a random phase function distributed in the range $[0, 2\pi]$. For the sake of brevity, the coordinates of complex images and phase mask are omitted.

(3). The amplitude and phase distribution of the resultant $\bar{F}_1$ is obtained by using the phase-truncated and amplitude-truncated operation, respectively, which can be expressed as

$$h_2 = PT\{\bar{F}_1\}, \tag{2}$$

$$p_1 = AT\{\bar{F}_1\}. \tag{3}$$

Here, $PT\{\cdot\}$ and $AT\{\cdot\}$ denote the phase and amplitude truncation, respectively. The distribution h_2 is then used as the input of the next fractional Fourier transform procedure, and the phase distribution p_1 is considered as the security key.

(4). Similarly, a new complex image F_2 is formulated by taking the amplitude distribution h_2 as the real part and the second plain image f_2 as the imaginary part, and then modified by applying the fractional Fourier transform with the fractional order α, which is written as

$$\bar{F}_2 = FrFT^{\alpha}\{F_2 \exp(iM_3)\}. \tag{4}$$

Then, the amplitude and phase distribution, i.e. h_3 and p_2, can be calculated by using PT and AT operator, respectively. Notably, the phase p_1 obtained in the previous step is updated with the phase of the complex image F_2, which is described as

$$p_1 = p_1 \times conj(AT\{F_2\}). \tag{5}$$

Here, $conj(\cdot)$ denotes the conjugate operation and $\times$ denotes the element-by-element multiplication.

(5). After the fractional Fourier transform procedure repeats K times, the phase p_K and the amplitude h_{K+1} are calculated from the last transformed result $\bar{F}_K$, which are expressed as

$$h_{K+1} = PT\{\bar{F}_K\}, \tag{6}$$

$$p_K = AT\{\bar{F}_K\}. \tag{7}$$

The amplitude distribution h_{K+1} will be encrypted further in the process of silhouette-free interference. It should be pointed out that no update is required to modify the phase distribution p_K.

(6). In the second layer using interference, the amplitude h_{K+1} is decomposed into two phase-only masks denoted as $\exp(iM_1)$ and $\exp(iM_2)$, where the corresponding phase distributions are considered as the ciphertext images. Because the random phase-only mask $\exp(iM_3)$ will be applied in the process of interference, the annoying silhouette problem can be solved thoroughly.

(7). Finally, the security key p_i generated in each fractional Fourier transform procedure is updated with three phase-only masks, which is expressed as

$$p_i = p_i \times \exp(iM_1) \times \exp(iM_2) \times \exp(iM_3). \tag{8}$$