Optics and Lasers in Engineering 98 (2017) 46–55

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical encryption scheme for multiple color images using complete trinary tree structure

Yonggang Su[a], Chen Tang[a,*], Guannan Gao[a], Fan Gu[a], Zhenkun Lei[b], Shuwei Tang[c]

[a] *School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China*
[b] *State Key Laboratory of Structural Analysis for Industrial Equipment, Dalian University of Technology, Dalian 116024, China*
[c] *Science and Technology on Electro-Optical Information Security Control Laboratory, Tianjin 300308, China*

ARTICLE INFO

Keywords:
Multiple color image encryption
Complete trinary tree
Phase truncated Fresnel transform
Random amplitude-phase mask

ABSTRACT

We propose an optical encryption scheme for multiple color images based on the complete trinary tree structure. In the proposed encryption scheme, the encryption modules (EMs) are taken as branch nodes, and the color components of plain images are input as leaf nodes. In each EM which consists of phase truncated Fresnel transforms and random amplitude-phase masks, three input images are subsequently encoded into a complex function and finally encrypted to a real-value image. The proposed encryption scheme can encrypt multiple color images into a real-value grayscale cipher image, and make different color images have different encryption and decryption paths. By the proposed encryption scheme, we can realize an authority management with high security among multiple users. In addition, the proposed scheme possesses the advantages such as high robustness against various attacks and high encryption efficiency. Moreover, as the number of plain color images increases, high quality of the decrypted color images can still be maintained. Extensive simulation results have shown the performance of the proposed scheme. The proposed scheme can also be directly extended to encrypt multiple gray images.

1. Introduction

With the rapid development of network and communication technologies, both the information security and the secure communication have become one of the most challenging issues. Recently, optical information security techniques, especially optical image encryption techniques, have attracted significant interest as they possess superior advantages, such as high-speed parallel processing of information and arbitrary parameter selection [1]. Among the various techniques proposed for optical image encryption, the double random phase encoding (DRPE) is the most well-known technique [2]. This technique uses two random phase masks respectively placed on the input plane and the Fourier plane to encrypt the input image into a stationary white noise. During the past decades, a number of DRPE-based optical encryption schemes have been presented, such as the Fresnel transform encryption scheme [3,4], the fractional Fourier transform encryption scheme [5,6], and the Gyrator transform encryption scheme [7,8], etc. However, due to the inherent linear property, the DRPE-based encryption schemes have been proved to be vulnerable to different types of attacks [9–11]. To break the linearity of the DRPE, Cheng et al. [12] added an undercover amplitude-modulating operation in the Fourier transform based DRPE encryption scheme, which can ensure the encryption scheme against the known-plaintext attack. In addition, Qin et al. proposed a phase-truncated Fourier transform (PTFT) based encryption scheme to overcome the linear property of the DRPE [13]. In this PTFT-based encryption scheme, the input image can be encoded into a real-value cipher image with two public keys, and the authorized user is able to retrieve the input image using two private keys. Subsequently, optical encryption schemes based on nonlinear phase truncation techniques have been further developed [14–16].

The optical image encryption schemes proposed in the above mentioned papers are designed for a gray or binary image. Since the color information of an image sometimes plays an important role in many applications. Therefore, more and more attention has been paid to the optical methods for color image encryption recently. Chen et al. proposed a color image encryption scheme using wavelength multiplexing based on lensless Fresnel transform holograms [17]. Sui et al. proposed a color image encryption scheme using two-coupled logistic map and phase retrieve algorithm in fractional Fourier domain [18]. After that, they also proposed a color image encryption scheme based on the Yang–Gu mixture amplitude–phase retrieval algorithm in the gyrator domain [19]. Liu et al. proposed a color image encryption system by using the Arnold transform and discrete cosine transform [20]. Chen et al. proposed a method for color image encryption and synthesis using coherent diffractive imaging in the Fresnel domain [21]. In addition, some

[*] Corresponding author.
E-mail address: tangchen@tju.edu.cn (C. Tang).

http://dx.doi.org/10.1016/j.optlaseng.2017.05.019
Received 5 February 2017; Received in revised form 10 May 2017; Accepted 29 May 2017
Available online 9 June 2017
0143-8166/© 2017 Elsevier Ltd. All rights reserved.

asymmetric color image encryption schemes based on phase truncation operation have also been proposed [22–25]. However, the above mentioned encryption schemes are all designed for single color image.

To increase the efficiency of image encryption in large quantities, researchers have recently developed some optical multiple-image encryption schemes. For the aspect of optical multiple gray image encryption, Situ et al. proposed two encryption schemes by using the wavelength multiplexing technique and position multiplexing technique, respectively [26,27]. Gone et al. proposed a multiple-image encryption and authentication scheme using space multiplexing technique [28]. Wang et al. proposed a multiple-image encryption scheme based on polarized light encoding and optical interference principle in Fresnel transform domain [29]. By using the compressive sensing and the double random phase encoding technique, Deepan et al. proposed a multiple image encryption scheme in which the space multiplexing method was employed for integrating multiple-image data [30]. In addition, the multiple gray image encryption schemes using the vector composition [31] and the phase retrieval algorithm [32,33] were also proposed and investigated by researchers. For the aspect of optical multiple color image encryption, Aburab proposed two encryption schemes by using gyrator transform [34,35]. In Ref. [34], each normalized color image is independently phase-only encoded, and then all the phase-only images are combined together to produce a single-phase-only image. The single-phase-only image is bounded with a random phase mask to form a complex image, and then two phase-only masks are analytically obtained from the inverse Fourier transformation of the complex image. The two phase-only masks are illuminated by the spherical wave, and then Gyrator transformed. By executing the phase and amplitude truncation operation on the transformed image, the encrypted image and decryption keys can be obtained, respectively. In Ref. [35], each channel of a color image is separately permutated with generalized Arnold map, and then Gyrator transformed. Each transformed channel is multiplied together to produce a single-channel encrypted image. In the same way, single-channel encrypted images obtained from different color images are directly multiplied together to produce a single encrypted image. The single encrypted image is multiplied by a random phase mask, and then phase- and amplitude-truncated to obtain the first encrypted image and first decryption key, respectively. The first encrypted image is gyrator transformed and then phase- and amplitude-truncated to get the final encrypted image and second decryption key, respectively. In the above two encryption schemes, the original color images can be retrieved by executing the inverse process of encryption with the help of decryption keys.

Among most of the existing optical multiple image encryption schemes, different images have almost the same or similar encryption or decryption processes. Therefore, if an illegal user can manage to correctly decrypt some images, the decryption processes of other images are also leaked. To overcome this shortcoming, Yi et al. proposed a binary-tree encryption strategy for multiple images, in which different images have different encryption or decryption paths [36]. However, this binary-tree encryption strategy is designed for multiple gray images, and is not suitable for encrypting multiple color images.

In this paper, an optical encryption scheme for multiple color images based on complete trinary tree structure is proposed. In the proposed encryption scheme, the EMs are taken as branch nodes, while the color components of plain color images are taken as leaf nodes. Each EM in the proposed encryption scheme consists of phase truncated Fresnel transforms and random amplitude-phase masks, which can be implemented optically or digitally. In each EM, three input images are subsequently encoded into a complex function, and finally encrypted to a real-value image. The proposed encryption scheme can encrypt multiple color images into a real-value grayscale cipher image, which can be recorded, stored and transmitted conveniently. Similar with the binary-tree encryption strategy, the proposed encryption scheme can also make different color images have different encryption and decryption paths. So even if an illegal user can manage to decrypt some color images correctly, it is still difficult for him to illegally decrypt other color images. The security of the proposed encryption scheme is therefore strengthened efficiently. In addition, when adopting the proposed encryption scheme to encrypt multiple color images, we can realize an authority management with high security among multiple users. The main secret keys generated in the encryption processes of EMs are depended on the plain color images, i.e., different color images have different main secret keys. Therefore, the proposed encryption scheme can resist the chosen-plaintext attack. The random amplitude-phase mask, the wavelength, and the Fresnel transform distance in each EM are introduced as additional keys, which provide additional difficulties for the attacker of the proposed encryption scheme. The proposed encryption scheme also possesses high encryption efficiency and high robustness against statistical attack, occlusion attack and noise attack. Furthermore, as the number of color images to be encrypted increases, decrypted color images with high quality can still be obtained by the proposed encryption scheme. The performance of the proposed encryption scheme have been demonstrated by extensive numerical simulations, including the visual and quantitative test, the sensitivity of secret keys, the authority management test, the robustness against various attacks, and the encryption efficiency test. It is worth noting that the proposed encryption scheme can also be directly applied to encrypt multiple gray images.

The rest of this paper is organized as follows. In Section 2, the proposed encryption scheme for multiple color images based on complete trinary tree structure is described in detail. In Section 3, extensive simulation results and security analysis are given. In Section 4, performance comparison of the proposed encryption scheme and the other encryption scheme is discussed. Finally, the conclusion is given in Section 5.

2. The proposed multiple color image encryption scheme

The proposed multiple color image encryption scheme is based on complete trinary tree structure. In the proposed encryption scheme, the *R, G* and *B* components of color images are taken as leaf nodes, and the EMs are taken as branch nodes. The EMs consist of phase truncated Fresnel transforms and random amplitude-phase masks. Before we go in the details of the complete trinary tree encryption scheme, we will give detailed descriptions of the encryption and decryption process in EMs.

2.1. Encryption and decryption process in EMs

The flowchart of the encryption process is shown in Fig. 1(a), where the phase truncated Fresnel transforms and random amplitude-phase masks are used. The encryption process involves the following steps:

Step 1: A color image f is firstly decomposed into red, green and blue components represented as f_r, f_g and f_b, respectively. Then, the red and blue components f_r, f_b are encoded into a complex function as the real part and the imaginary part. The complex function is then multiplied by the first pair of random amplitude-phase masks (RAM$_1$ and RPM$_1$) represented as R_1 and $\exp(j \cdot 2\pi \cdot \varphi)$, respectively.

$$f_{rb} = \left(f_r + j \cdot f_b\right) \cdot R_1 \cdot \exp(j \cdot 2\pi \cdot \varphi), \tag{1}$$

where R_1 and φ are independent white noise uniformly distributed in an interval (0, 1).

Step 2: The encoded image f_{rb} is firstly Fresnel transformed. Then, through the nonlinear operation of amplitude- and phase-truncation, the private secret key p' and the preliminary encrypted image c_{rb} can be achieved as follows:

$$p' = AT\left[FrT_{\lambda,z_1}\left(f_{rb}\right)\right], \tag{2}$$

$$c_{rb} = PT\left[FrT_{\lambda,z_1}\left(f_{rb}\right)\right], \tag{3}$$

where $AT[\cdot]$ and $PT[\cdot]$ represent the amplitude- and phase-truncation, respectively; $FrT_{\lambda,z_1}(\cdot)$ represents the Fresnel transform with wavelength λ and distance z_1.