Optics Communications 344 (2015) 147–155

Contents lists available at ScienceDirect

Optics Communications

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

Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask

Y. Wang, C. Quan *, C.J. Tay

Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 31 October 2014
Received in revised form
13 January 2015
Accepted 14 January 2015
Available online 16 January 2015

Keywords:
Color image encryption
Optical image encryption
Information disclosure

ABSTRACT

Many phase-truncation-based cryptosystems encounter an information disclosure problem. In this paper, a novel color image encryption using a phase-truncated Fresnel transform and random amplitude mask (RAM) without the risk of information disclosure is proposed. An image is first separated into three channels (red, green, and blue) and using an additional RAM channel the risk of information disclosure encountered in previous encryption methods is eliminated. Moreover unlike previous methods where each channel is encrypted independently, the four channels employed in the proposed method are encrypted using a cascading technique. Robustness of the proposed scheme against attacks is analyzed. Numerical simulations are presented to demonstrate the feasibility and effectiveness of the proposed system.

1. Introduction

Since the pioneering work in optical image encryption based on double random phase encoding was proposed by Refregier and Javidi [1], optical encryption techniques for information security have received wide attention. In a double random phase encoding system, an image is encoded into an image with stationary white noise through two random phase masks located at the input and Fourier planes. Since Refergier's work many optical encryption algorithms, such as Fresnel [2,3], fractional Fourier [4,5], and gyrator transforms [6,7] have been further developed. However, these methods are applicable only to a gray or binary image, where the image is illuminated by a monochromatic light and no color information can be retrieved. Color information in an image, such as human security facial features and detailed military maps, is useful in many practical applications. In this regards, optical methods [8–13] for color image encryption have been studied. In 1999, Zhang and Karim [8] proposed a method for color image encryption based on an indexed image and double random phase masks. Subsequently, color image encryption based on wavelength multiplexing using lensless Fresnel domain holograms [9], cascaded phase-only masks [10], double random-structured phase encoding [11], and interference [12,13] have also been proposed. These color image encryption techniques however employed a linear symmetric cryptosystem, which is prone to attacks [14–17].

To overcome the limitations of a linear symmetric cryptosystem, Qin and Peng proposed an asymmetric cryptosystem based on a phase-truncated Fourier transform (PTFT) [18]. In the technique, the image is encoded into a real-value ciphertext with two public keys and a user is able to retrieve the original image using two private keys. Subsequently, optical color image encryption techniques based on phase-truncated cryptosystem were further developed [19–22]. Chen et al. [19] proposed a color image encryption system based on multiple wavelength and phase-truncated Fresnel transform. Rajput et al. [20] proposed a color cryptosystem using polarization selective diffractive optical element and structured phase mask. Single-channel color image encryption techniques based on phase truncation operation were also proposed [21,22]. In addition, Joshi et al. [23] proposed a color image encryption using fractional Fourier transform, and Mehra et al. [24] proposed a color image fusion technique using wavelet transform. Recently, Wang et al. [25] presented a study on the risk of information disclosure in a PTFT-based cryptosystem. It was reported that using a decryption key the main information of the original image can be revealed [25]. A risk of information disclosure also exists in the aforementioned encryption systems [19–22]. This does not imply that the PTFT-based cryptosystems do not work; however the risk of information disclosure has to be eliminated.

In this paper, we propose a novel cascading color image encryption scheme using a RAM in Fresnel domain without the risk of information disclosure. Compared with existing PTFT-based cryptosystems, the risk of information disclosure has been

* Corresponding author. Fax: +65 67791459.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

http://dx.doi.org/10.1016/j.optcom.2015.01.045
0030-4018/

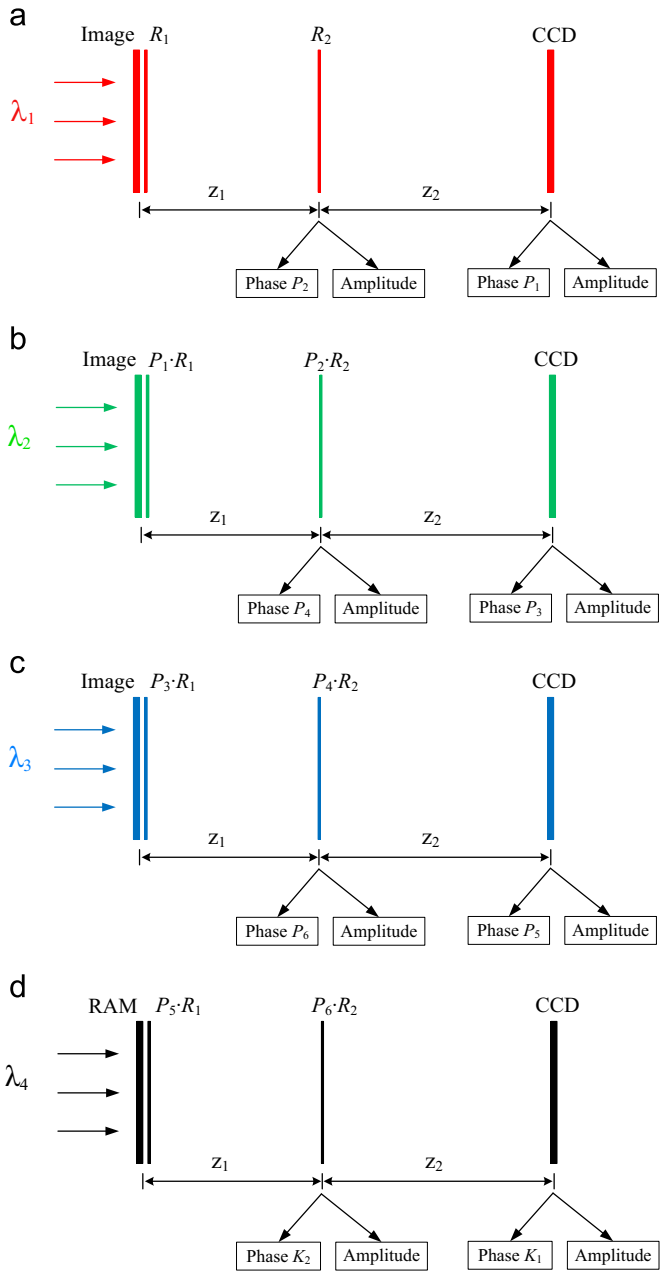

Fig. 1. Schematic arrangement of optical color image encryption based on four-channel cryptosystem using multiple wavelengths. (a) Red channel; (b) green channel; (c) blued channel; (d) RAM channel. CCD, charge-coupled device. z_1 and z_2, Fresnel propagation distances. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

eliminated in the proposed system and strategies for avoiding existing attacks are suggested. The proposed method can be applied on a gray or color image in other domains such as Fourier, fractional Fourier and gyrator transform domains. Numerical simulations are presented to demonstrate the feasibility and effectiveness of the proposed cryptosystem.

2. Theory of method

A color image consisting of red, green and blue colors is decomposed into three channels (red, green and blue channels). Let $f(x, y)$ represents the original image to be encrypted and $f_R(x, y)$, $f_G(x, y)$ and $f_B(x, y)$ represent the functions in the corresponding red, green and blue channels. With an additional RAM channel, the four channels are encrypted in sequence based on a phase-truncated Fresnel transform (PTFrT). Fig. 1(a)–(d) show the optical setup for the encryption of red, green, blue and RAM channels using multiple wavelengths. The wavelengths in the red, green, blue and RAM channels are denoted by λ_1, λ_2, λ_3 and λ_4 respectively. For simplicity, only one channel (red channel) analyzed is shown here.

As shown in Fig. 1(a), an image is illuminated by a collimated plane wave of wavelength λ_1, and functions $R_1(x, y)$ and $R_2(u, v)$ denote two statistically independent random phase masks (RPMs) located at the input and Fresnel planes respectively. With a free space propagation distance of z_1, the Fresnel spectrum is phase truncated and the amplitude obtained before R_2 is described by:

$$g_R(u, v) = \mathrm{PT}\{FrT_{\lambda_1}^{z_1}[f_R(x, y)R_1(x, y)]\}, \tag{1}$$

where PT{} denotes the operator of a phase truncation. $\mathrm{FrT}_{\lambda_1}^{z_1}$ denotes a Fresnel transform with free space propagation distance z_1 and is defined as [26]:

$$\mathrm{FrT}_{\lambda_1}^{z_1}[f(x, y)](u, v) = \frac{\exp\{j2\pi z_1/\lambda_1\}}{j\lambda_1 z_1} \iint f(x, y) \times \exp\left[\frac{j\pi}{\lambda_1 z_1}((x-u)^2 + (y-v)^2)\right] dxdy \tag{2}$$

After a second free space propagation distance of z_2, an encrypted ciphertext $C_R(\xi, \eta)$ is recorded at the CCD plane and is expressed as:

$$C_R(\xi, \eta) = \mathrm{PT}\{FrT_{\lambda_1}^{z_2}[g_R(u, v)R_2(u, v)]\}. \tag{3}$$

The decryption keys for the red channel (red keys) are given by $P_2(u, v)$ and $P_1(\xi, \eta)$:

$$P_2(u, v) = \mathrm{PR}\{FrT_{\lambda_1}^{z_1}[f_R(x, y)R_1(x, y)]\}, \tag{4}$$

$$P_1(\xi, \eta) = \mathrm{PR}\{FrT_{\lambda_1}^{z_2}[g_R(u, v)R_2(u, v)]\}. \tag{5}$$

where PR{} denotes an operator of the phase reservation. It is seen that the decryption keys $P_1(\xi, \eta)$ and $P_2(u, v)$ are different from encryption keys $R_1(x, y)$ and $R_2(u, v)$. The decrypted image at the red channel is given by:

$$g_R'(u, v) = \mathrm{PT}\{FrT_{\lambda_1}^{-z_2}[C_R(\xi, \eta)P_1(\xi, \eta)]\}, \tag{6}$$

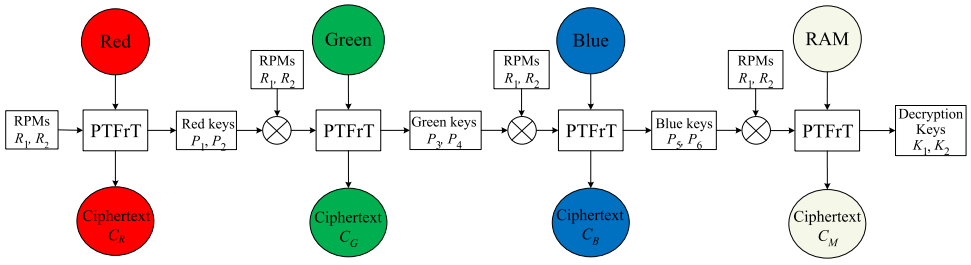

Fig. 2. Flowchart of the proposed four-channel encryption process.