Optics and Lasers in Engineering 77 (2016) 191–202

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical color-image encryption in the diffractive-imaging scheme

Yi Qin [a,*], Zhipeng Wang [a], Qunna Pan [b], Qiong Gong [a]

[a] College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China
[b] College of Computer and Information Technology, Nanyang Normal University, Nanyang 473061, China

ARTICLE INFO

Article history:
Received 23 June 2015
Received in revised form
10 August 2015
Accepted 7 September 2015
Available online 24 September 2015

Keywords:
Optical encryption
Color image
Coherent diffractive imaging

ABSTRACT

By introducing the theta modulation technique into the diffractive-imaging-based optical scheme, we propose a novel approach for color image encryption. For encryption, a color image is divided into three channels, i.e., red, green and blue, and thereafter these components are appended by redundant data before being sent to the encryption scheme. The carefully designed optical setup, which comprises of three 4f optical architectures and a diffractive-imaging-based optical scheme, could encode the three plaintexts into a single noise-like intensity pattern. For the decryption, an iterative phase retrieval algorithm, together with a filter operation, is applied to extract the primary color images from the diffraction intensity map. Compared with previous methods, our proposal has successfully encrypted a color rather than grayscale image into a single intensity pattern, as a result of which the capacity and practicability have been remarkably enhanced. In addition, the performance and the security of it are also investigated. The validity as well as feasibility of the proposed method is supported by numerical simulations.

1. Introduction

Optically encrypting images has been a hot research topic over the past three decades [1–8]. The double random phase encoding (DRPE) has received extensive attention since it is the pioneer and representative optical method for image encryption [9]. In DRPE, the image is encoded to be complex stationary white noise picture with two random phase plates, which are placed respectively at the input plane and Fourier plane. The DRPE is proved to have huge key space and to be robust against brute force attack, and it is soon put forward to the Fresnel domain [10] and fractional Fourier domain [11]. Moreover, various multiple-image and color image encryption means based on DPRE are also developed [12–14]. However, the DRPE was puzzled by two issues that hinder its further applications. On one hand, the DRPE shows vulnerability to many attacks, such as known-plaintext [15], chosen-plaintext [16] and chosen-ciphertext [17] attacks, because of its inherent linearity. On the other hand, its ciphertext is complex field and should be always registered with holographic setups, and thus high stability of the encryption architecture is prerequisite.

In 2010, Chen et al. propose a diffractive-imaging-based encryption (DIBE) approach as an alternative to the DRPE scheme [18]. Thereafter, Chen's research group also developed other DIBE approaches by wavelength multiplexing and distance multiplexing [19,20]. Compared with DRPE, the DIBE extremely simplified the encryption architecture since only intensity patterns are needed for decryption and the phase information can be discarded. Furthermore, the system has relatively high security as the linearity of the DRPE encryption schemes is broken. It should be emphasized that the above mentioned DIBE methods request at least three intensity patterns to completely retrieve the plaintext. To simplify the encryption procedure, we further proposed some new algorithms that are able to extract the plaintext from single intensity pattern [21–23]. In particular, we have describe a phase retrieval algorithm using redundant data of the primary image as partial support constraint in the input plane [21], which enables one to completely retrieve the primary image from a single intensity.

Although the DIBE methods have obvious merits over the DRPE, the currently available contributions [18–23] show that, to our best knowledge, they can only be adopted to encrypt single image (i. e. grayscale image or binary image). In practical applications, the color information of an image is always of especial importance. In this sense, it is strongly expected that color image can be encrypted by using the DIBE scheme. Meanwhile, in many color image encryption approaches [24–26], the R, G, B channels of the plaintext are encrypted individually. Consequently, the size of the ciphertext is often three times over that of each channel. In this regard, encryption of color image in DIBE scheme will extensively

[*] Corresponding author.
E-mail address: 641858757@qq.com (Y. Qin).

http://dx.doi.org/10.1016/j.optlaseng.2015.09.002
0143-8166/© 2015 Elsevier Ltd. All rights reserved.

reduce the ciphertext size and make its storage and transmission more convenient. In other words, if we can encrypt color image in the DIBE scheme without enlarging the ciphertext size, the efficiency and practicability of it will be effectively improved. Motivated by this intention, we propose here, for the first time to our knowledge, a novel color image encryption approach in the diffractive-imaging-based scheme. This new approach is achieved by combining our preceding contribution [21] and the theta modulation [27–29]. The theta-modulation is a convenient way of encoding optical images by modulating them with gratings at different orientations or with different space frequencies, and it has been applied to speckle patterns to primarily store different images into a single record [24]. With the help of the 4f scheme, the encryption could be accomplished with pure optical manner, as a result of which the efficiency has been greatly improved. Numerical results indicate that the proposed method is effective as well as feasible, and may open up a novel perspective for optical color image encryption.

2. Description of the method

2.1. The encryption principle

A color image usually consists of red, green and blue elements with certain proportions, and is first decomposed into three channels, i.e., red, green and blue. During the encryption, each channel of the plaintext is appended with redundant data in the manner that is shown in Fig. 1. The redundant data are the dark area around the primary image and the values of them are zeros. To facilitate the discussion, a parameter ρ is introduced for quantitatively describing the redundant data, which is defined as

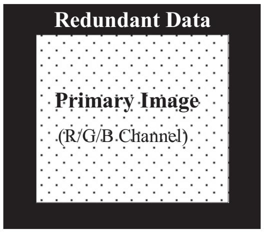

Fig. 1. The primary R/G/B channel image appended with redundant data.

$$\rho = \frac{\text{Quantity of the redundant data(Pixels)}}{\text{Quantity of the original image(Pixels)}} \tag{1}$$

Thereafter, the redundant R, G, B components are encoded with the optical setup illustrated in Fig. 2. The components, each bonded with a sinusoidal gratings $SG_i(i=1,2,3)$, are put at the input planes of three 4f schemes, of which the focal length of the lens are f. The output planes of the 4f schemes are located at the same plane, which we denote as P. When the three images are illuminated by a plane wave with a wavelength of λ, we can get a synthetic image (SI) at plane P. Then SI is successively modulated by two random phase masks, of which M1 is immediately behind SI in plane P, and the distance between M1 and M2 is d_1. The light wave emerging from M2 reach to the CCD plane after propagating a distance of d_2, and its intensity is recorded by a CCD camera. It should be emphasized that the input images, the sinusoidal gratings as well as POMs M1 and M2, are displayed with space light modulator (SLM) in practical application.

The phase values of M1 and M2 are between $[0, 2\pi]$. For convenience, symbols (x, y), (η, ξ), and (μ, ν) are used to respectively denote coordinates of plane P, M1, M2 and the CCD plane. Although the architecture seems to be complicated to some extent, it can be considered as to comprise two functional modules. The first module consists of the three 4f schemes, and each of them generates the product of the component and the sinusoidal grating, the sum of which gives rise to the SI. The second one is the DIBE scheme that includes the two phase masks M1 and M2. In particular, the second functional module can be considered as a lensless double random phase encoding scheme with an intensity ciphertext. Obviously, the SI is the output of the first module and is simultaneously the input of the second module. Let $U(x, y)$ stand for SI, we can obtain the expression of the ciphertext recorded by CCD after a simple deduction:

$$I(\mu,\nu) = |[\mathrm{FrT}\{\mathrm{FrT}[U(x,y)M_1(x,y);d_1] \times M_2(\eta,\xi);d_2\}]|^2 \tag{2}$$

where || denotes a modulus operation, FrT means the Fresnel transform with respect to λ. It is evident from Fig. 2 that the encryption process of our method can be implemented in a pure optical manner, and the speed approaches light theoretically discarding the response time of the SLMs and CCD. This is an important advantage of our proposal over the image encryption methods based on computational principles.

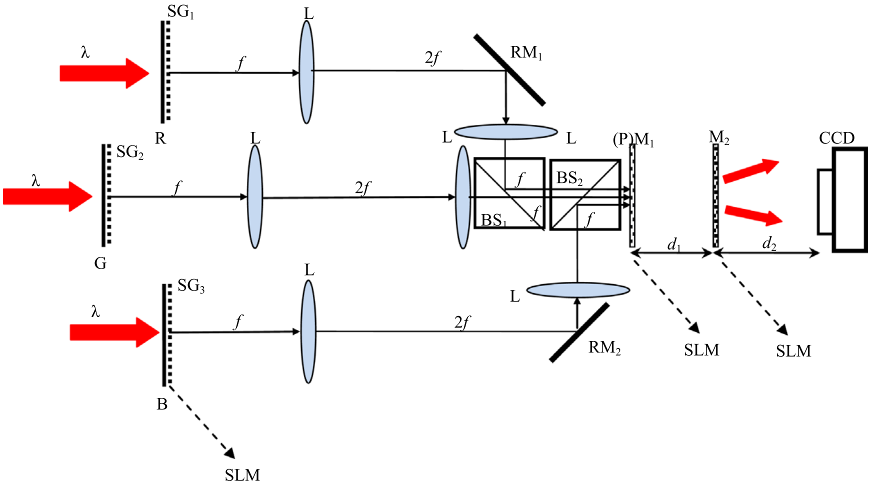

Fig. 2. Schematic optical setup for the proposed optical security system. R, G, B, the three channels of a color image; SG, the sinusoidal gratings; M, phase only mask; RM, reflective mirror; BS, beam splitter; SLM, space light modulator; L, lens; CCD, charge-coupled device.