Optics and Lasers in Engineering 88 (2017) 221–232

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

# Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition

Linfei Chen [a,*], Guojun Chang [a], Bingyu He [a], Haidan Mao [a], Daomu Zhao [b]

[a] The School of Science, Hangzhou Dianzi University, Hangzhou, 310018 China
[b] Department of Physics, Zhejiang University, Hangzhou, 310027 China

ARTICLE INFO

*Article history:*
Received 21 June 2016
Received in revised form
18 August 2016
Accepted 25 August 2016

*Keywords:*
Optical image encryption
Fresnel diffraction
Phase retrieval algorithm
Incoherent superposition

ABSTRACT

In this paper, an optical encryption system is proposed based on tricolor principle, Fresnel diffraction, and phase iterative algorithms. Different from the traditional encryption system, the encrypted image of this system is a color image and the plaintext of it is a gray image, which can achieve the combination of a color image and a gray image and the conversion of one image to another image. Phase masks can be generated by using the phase iterative algorithms in this paper. The six phase masks and the six diffracting distances are all essential keys in the process of decryption, which can greatly enhance the system security. Numerical simulations are shown to prove the possibility and safety of the method.



## 1. Introduction

In the optical information security field, since the double random phase encoding (DRPE) technique was proposed by Refregier and Javidi in 1995 [1], the optical image encryption technology has become an active research area and many new optical image encryption methods have been proposed by far [2–29]. To make the optical implementation more efficient, the optical encryption system based on free space Fresnel diffraction was proposed by Situ [3]. The system security is enhanced by the positions and the wavelengths which are used as additional keys to expand the key space [2–4]. In 2006, we proposed a color image encryption method using wavelength multiplexing based on Fresnel transform holograms [5], which has attracted wide attention for color image encryption technology. Recently, amplitude and phase truncation technology [6], ghost imaging [7], photon-counting polarimetric imaging [8] and so forth are applied to optical image encryption in succession, which gave a big push for the development of the optical image encryption fields. In 2010, Chen proposed an optical encryption system based on diffractive imaging [9], which has been studied by many researchers in the last few years for its simple encryption method and high security [10,11]. In 2014, Wang and Chen proposed an attack method, by which the original information could be attacked when the aperture of the system and the related parameters were given [12]. At the same time, a new method of double cross image encoding was proposed as well. Firstly, it matches the two images together and disturbs the matched ones. And then it takes them apart and codes in other ways respectively. This method could deeply damage the correlation effect of the images and enhance the system security [13,14]. In addition, phase-only technology, telescope imaging, fractional transforms, image compression-encryption and so forth were all used in optical image encryption [15–19]. In 2008, Zhang et al. proposed an optical image encryption system based on two beam interference [20]. The encryption and decryption processes were very simple, and its feasibility was proved by experiments successfully. On this basis, a large number of image coding methods based on optical interference technique have been proposed after that [21–32]. Recently, an asymmetric image encryption system based on coherent superposition and equal modulus decomposition was proposed [23], and at the same time, the image coding technique based on vector decomposition and multiple-beam interference was also proposed [24,25].

In the previous methods, the original image is modulated and encrypted into disorganized ciphertext by different kinds of phase masks and amplitude masks, so the ciphertext and the original image would have some connections. Therefore, through the ciphertext and partial information, the outline or basic information of the image can be attached by the phase retrieval algorithms when decrypting [33,34].

In this paper, we propose a novel image encryption method that encrypts an original gray image into six phase masks and a color cipher-image by using free space transmission theory and

* Corresponding author.
*E-mail address:* chenlinfei2004@163.com (L. Chen).

http://dx.doi.org/10.1016/j.optlaseng.2016.08.013
0143-8166/

phase iterative algorithms. The ciphertext is irrelevant with the original image but is essential in the decryption process, which enhance the system security. Additionally, in the decryption process, the combination of color ciphertext with the phase masks can get the gray plaintext image in the output plane by using trichromatic theory, Fresnel diffraction, and incoherent superposition. It can realize the magic effect of conversion a color image to a gray image. Finally, six transmission distances and six phase masks are all essential keys in the decryption process, and the correct information cannot be gained by only knowing some of the keys. Therefore, this paper proposes a new optical image encryption method which is interesting and has relatively high security.

The rest parts of this paper are organized as follows. In the second part, the theoretical analysis process is proposed which indicates how to produce the phase masks in the encryption process, and the optical implementation and realization of the decryption process is also presented in this part. In the third part, the numerical simulation results are presented by MATLAB in computer to prove the feasibility and safety of the proposed method. Finally, the conclusions sum up the method in the fourth part.

## 2. The encryption and decryption processes

We always have in our mind that if we can turn one thing into another like magic. In optical field, can we turn one image into another different one by using optics method? In particular, the method of realizing the conversion of a color image to a gray image by using incoherent superposition method is meaningful. Therefore, we propose this idea: taking a color image as the cipertext, using trichromatic theory to obtain its three sub images, illuminating these sub images by using the corresponding wavelengths, realizing some diffraction transforms with several phase masks, and observing another image (i.e., plaintext) by using the incoherent superposition method in the output plane. In this way, it is necessary to use iteration method to hide the color ciphertext information and the gray plaintext information in these phase masks when encrypting and this can realize the conversion of a color image to a gray image when decrypting.

### 2.1. The encryption process

To generate phase masks among the channels, Fig. 1 shows the flow chart of the encryption process. $f(x, y)$ is the original color image and its red, green, and blue sub-images $f_r(x, y)$, $f_g(x, y)$ and $f_b(x, y)$ are as each channel's ciphertext. The phase masks of the red channel are $R_r$ and $R_r'$, the phase masks of the green channel are $R_g$ and $R_g'$, and the phase masks of the blue channel are $R_b$ and $R_b'$. Among them, $R_i'(i = r, g, b)$ are the phase masks generated randomly, which remain the same in the process of iteration and

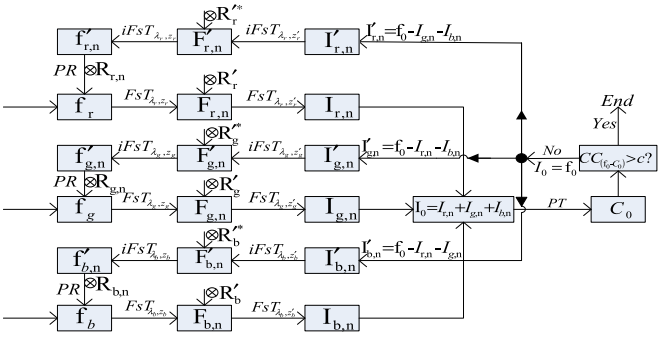


**Fig. 1.** The flow chart of the encryption process.

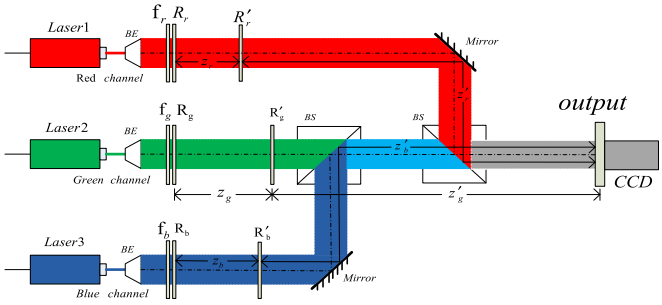


**Fig. 2.** The optical realization of the decryption process.

are placed in the Fresnel transform spaces. $R_{i,n}(i = r, g, b)$ are generated by iteration and placed in the input plane. $n$ designated under the various physical quantities in the diagram shows various intermediate variables produced in the process of n circulation. When $n=1$, $R_{i,1}(i = r, g, b)$ are generated randomly in the first cycle. At the same time, the distances of Fresnel diffractions in each channel are different and can be served as the keys, thus making the system have higher safety.

As shown in Fig. 1, the three laser beams with different wavelengths (red, green, and blue) parallel illuminate at the corresponding ciphertexts. The specific encryption process is as follows and the encryption process starts from $n=1$.

The three sub images are modulated by the phase masks $R_{i,n}(i = r, g, b)$ and Fresnel transformed for the first time, thus obtaining $F_{i,n}(u, v)$ shown in Eq. (1):

$$F_{i,n}(u, v) = FsT_{\lambda_i,z_i}\left\{f_i(x, y)\exp[j\cdot R_{i,n}(x, y)]\right\}. \tag{1}$$

where $r$, $g$, $b$ denote the red, green, and blue channels respectively, and $n$ is the cycle number. $R_{i,1}(i = r, g, b)$ are generated randomly when $n=1$, hereafter, $R_{i,n}(i = r, g, b)$ are generated by iteration. $FsT_{\lambda_i,z_i}\{\}$ represents two dimensional Fresnel transform with the incidence wavelength of $\lambda_i$ and the transmission distance of $z_i$. The two-dimensional Fresnel transform of a function $f(x, y)$ is defined by:

$$FsT_{\lambda,z}\left[f(x, y)\right] = \frac{\exp(jkz)}{j\lambda z}\iint f(x, y)\exp\left\{\frac{j\pi}{\lambda z}\left[(u - x)^2 + (v - y)^2\right]\right\}dxdy. \tag{2}$$

where $k$, $\lambda$ and $z$ are the wave number, wavelength and propagation distance, respectively. $(x, y)$ and $(u, v)$ represent the pixels' position coordinates in the input plane and transform plane, respectively. $F_{i,n}(u, v)$ is modulated by the phase masks $R_i'$ in the transform plane and Fresnel transformed for the second time, thus obtaining the complex amplitude distribution of the each channel:

$$I_{i,n}(\eta, \xi) = FsT_{\lambda_i,z_i}\left\{F_{i,n}(u, v)\exp\left[j\cdot R_i'(u, v)\right]\right\}. \tag{3}$$

After adding the complex amplitude of the three channels, $C_0$ can be obtained by phase truncation. The actual formulas are shown in Eqs. (4) and (5), in which $(\eta, \xi)$ represents the pixels' position coordinate in the output plane:

$$I_0(\eta, \xi) = I_{r,n}(\eta, \xi) + I_{g,n}(\eta, \xi) + I_{b,n}(\eta, \xi), \tag{4}$$

$$C_0(\eta, \xi) = PT[I_0(\eta, \xi)]. \tag{5}$$

So the image of the amplitude $C_0$ can be observed in the output plane.

In this paper, the correlation coefficient $(CC)$ is used to evaluate the similarity of the decryption result $C_0$ and the original image $f_0$, and to be served as the standard of controlling the number of cycles. It can be defined as: