Optics Communications 307 (2013) 76–79

Contents lists available at SciVerse ScienceDirect

Optics Communications

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

Optical color image encryption based on computer generated hologram and chaotic theory

Jian Liu, Hongzhen Jin, Lihong Ma, Yong Li, Weimin Jin *

Institute of Information Optics, Zhejiang Normal University, Jinhua 321004, China

ARTICLE INFO

Article history:
Received 15 January 2013
Received in revised form
23 May 2013
Accepted 5 June 2013
Available online 26 June 2013

Keywords:
Encryption
Computer generated hologram
Chaotic theory
Fresnel transform

ABSTRACT

A novel technique of optical color image encryption and decryption based on computer generated hologram (CGH) and chaotic theory is proposed. The tri-color separated images of an image to be encrypted are encoded with three random phase arrays constructed by a chaotic sequence of the deterministic non-linear system, respectively. Then Burch's encoding method using the modified off-axis reference beam is adopted to fabricate the CGH as the encryption image. A clear original color image can be reconstructed as long as the correct initial value of chaotic sequence and the correct system parameters are given. The initial value of chaotic function with a very small change will lead to the generation of an entirely different chaotic sequences. As a result, the random phase array changes dramatically and the original image cannot be recovered rightly. Serving as the secret keys, the initial values of chaotic sequence and system parameters reduce the amount of the key data. And the digital encryption image is also more favorable to be stored and transmitted. The feasibility and its robustness against occlusion and noise attacks are verified by numerical simulations.

1. Introduction

Since Réfrégier and Javidi proposed a double random-phase encryption technique in 1995 [1], various improved optical image encryption methods have been proposed [2–8]. The encrypted data generated with random phase encoding is often complex numbers by traditional hologram recording and storage. It is difficult to be transmitted through the network. And if not through the digital processing or conversion, the information must be reconstructed with an optical method. The digitization of encryption information favors the preservation and transmission of information, and even real-time transmission and display through the internet. The most effective method of the digitization of encrypted information is digital holography and CGH [9–12]. Besides that the virtual object, which does not yet exist in nature, can be recorded, the CGH also permits any wavelength to be selected and system parameters to be adjusted arbitrarily.

Constructed by a chaotic sequence of the deterministic non-linear system, a random phase array has classical randomness and good confidentiality. Even through the non-linear system which has very small changes in the initial conditions, it will lead to an entirely different chaotic sequences. As a result, the random phase array changes dramatically. In recent years, random phase encoding technology based on the chaotic sequence has drawn more and more researchers' attention [13–15].

For the color image encryption, there are also some reports [16–24]. These methods are usually based on double random phase encoding, while the amount of random phase data is so large that it is not conducive to transmission. In order to reduce the amount of information and facilitate network transmission, we present the optical color image encryption method based on chaos sequence and CGH. The color image to be encrypted is decomposed into red (R), green (G), blue (B) components, and then the three components are modulated by different random phase arrays constructed by the chaotic sequences, respectively. The next is to adopt Burch's coding method using the modified off-axis reference beam to fabricate the CGH as the encryption image. A clear original color image can be reconstructed as long as the correct initial value of the chaotic function and the correct system parameters are given. The advantage of this encryption technique is that the initial value of the chaotic function is enough to generate the random phase arrays for decryption. Thus, there is no need to send the whole random phase arrays to the receiver for decryption, which dramatically reduces the amount of the key data. As the tri-color images are encoded with different chaotic sequence arrays, the number of keys are increased. Hence the security of the encrypted image is further improved. The feasibility is verified by numerical simulations.

* Corresponding author. Tel.: +86 579 8228 3030.
E-mail address: jhjinwm@163.com (W. Jin).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.06.009

2. The theory of encryption and decryption

2.1. The encryption method

The chaos function used for our study is the logistic map, which is defined as [14]

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

where μ is logistic map parameter, and $\mu \in [0,4]$, $x_n \in (0,1)$. Studies have shown that, when $3.5699456 < \mu \leq 4$, logistic mapping works in a chaotic state. The generated chaotic sequence, which has characteristics of a good random distribution and approximate zero-mean white noise and also is extremely sensitive to the initial value of chaotic function, is a rather ideal pseudo-random sequence.

The encryption method is similar to the double random phase mask encoding. The optical setup of the proposed encryption system is shown in Fig. 1. Three planes are defined as the input plane (x,y), the transform plane (x_1,y_1), and the recording plane (x_2,y_2). The distances between adjacent planes are z_1 and z_2, which satisfy the Fresnel approximation. We reconstruct six random phase arrays $\exp[j2\pi M_{1i}(x,y)]$ and $\exp[j2\pi M_{2i}(x,y)]$ $(i=1,2,3)$, which are represented in the Fig. 1 are RPM_{1i} and RPM_{2i}, respectively, to modulate the corresponding tri-color images.

The target image is expressed as $f(x,y)$, with $f_r(x,y)$, $f_g(x,y)$, and $f_b(x,y)$ corresponding to the red, green, blue (RGB) color components, respectively. In the encryption process, the three components are sequentially located in the input plane. When the system is perpendicularly illuminated with a plane wave, the encrypted wavefront, which is modulated by the random phase array, can be obtained in the recording plane. The input signal is first modulated by the first corresponding random phase arrays RPM_{1i}, through Fresnel diffraction with the distance z_1. Thus the complex-amplitude distribution obtained on the transform plane (x_1,y_1) can be expressed as follows:

$$f_r(x_1,y_1) = FrT_{Z_1}\{f_r(x,y)\exp[j2\pi M_{11}(x,y)\} \quad (2)$$

$$f_g(x_1,y_1) = FrT_{Z_1}\{f_g(x,y)\exp[j2\pi M_{12}(x,y)\} \quad (3)$$

$$f_b(x_1,y_1) = FrT_{Z_1}\{f_b(x,y)\exp[j2\pi M_{13}(x,y)\} \quad (4)$$

where FrT represents Fresnel transform. Then by the modulation of the second corresponding random phase arrays RPM_{2i} and Fresnel diffraction with the distance z_2, the complex-amplitude distribution obtained on the recording plane (x_2,y_2) can be expressed as follows:

$$f_r(x_2,y_2) = FrT_{Z_2}\{f_r(x_1,y_1)\exp[j2\pi M_{21}(x_1,y_1)]\} \quad (5)$$

$$f_g(x_2,y_2) = FrT_{Z_2}\{f_g(x_1,y_1)\exp[j2\pi M_{22}(x_1,y_1)]\} \quad (6)$$

$$f_b(x_2,y_2) = FrT_{Z_2}\{f_b(x_1,y_1)\exp[j2\pi M_{23}(x_1,y_1)]\} \quad (7)$$

The total complex-amplitude distribution obtained on the recording plane (x_2,y_2) can be expressed as follows:

$$f(x_2,y_2) = f_r(x_2,y_2) + f_g(x_2,y_2) + f_b(x_2,y_2) \quad (8)$$

As shown in Fig. 1, the reference light R illuminates directly onto the recording plane and the intensity distribution of the hologram obtained is expressed as follows:

$$I(x_2,y_2) = |R + f(x_2,y_2)|^2 \quad (9)$$

2.2. The decryption method

As shown in Fig. 2, when the encryption image (CGH) is illuminated by R^*, the complex-amplitude of obtained wave is as follows:

$$f^*(x_2,y_2) = f_r^*(x_2,y_2) + f_g^*(x_2,y_2) + f_b^*(x_2,y_2) \quad (10)$$

Through Fresnel diffraction with the distance z_2, the complex-amplitude distribution $f^*(x_1,y_1)$ on the plane (x_1,y_1) can be obtained. Then $f^*(x_1,y_1)$ is multiplied by the corresponding random phase arrays RPM_{2i} and the complex-amplitude distribution is diffracted with the Fresnel distance z_1. Then by multiplying the corresponding random phase arrays RPM_{1i}, the complex conjugate amplitude of object wave obtained can be expressed as follows:

$$f_r^*(x,y) = FrT_{Z_1}\{FrT_{Z_2}[f_r^*(x_2,y_2)]\exp[j2\pi M_{21}(x_1,y_1)]\} \times \exp[j2\pi M_{11}(x,y)] \quad (11)$$

$$f_g^*(x,y) = FrT_{Z_1}\{FrT_{Z_2}[f_g^*(x_2,y_2)]\exp[j2\pi M_{22}(x_1,y_1)]\} \times \exp[j2\pi M_{12}(x,y)] \quad (12)$$

$$f_b^*(x,y) = FrT_{Z_1}\{FrT_{Z_2}[f_b^*(x_2,y_2)]\exp[j2\pi M_{23}(x_1,y_1)]\} \times \exp[j2\pi M_{13}(x,y)] \quad (13)$$

Obviously, $|f^*(x,y)|^2 = |f(x,y)|^2$, the original color image is reconstructed.

3. Simulation experiments and analysis

The computer simulations with MATLAB programming are carried out to validate the feasibility of our novel proposal. Firstly, the random phase arrays RPM_{1i} are constructed with the initial values of logistic map $\mu_{11}=3.67$, $x_{110}=0.33$, $\mu_{12}=3.82$, $x_{120}=0.19$, and $\mu_{13}=3.94$, $x_{130}=0.85$; the random phase arrays RPM_{2i} are constructed with the initial values of logistic map $\mu_{21}=3.8$, $x_{210}=0.41$, $\mu_{22}=3.75$, $x_{220}=0.28$, and $\mu_{23}=3.72$, $x_{230}=0.68$. Burch's encoding method using the modified off-axis reference beam is used to fabricate the CGH, and the intensity distribution of Burch's encoding method is expressed as follows:

$$I(x_2,y_2) = 0.5\{1 + A(x_2,y_2)\cos[\varphi - \phi]\} \quad (14)$$

where $A(x_2,y_2)$ is normalized amplitude, ϕ and φ are the phases of the object wavefront and the reference wavefront in the recording plane, respectively.

The object to be encryption is a color image of “Flowers” with 256×256 pixels as shown in Fig. 3(1). The diffraction distances are $z_1=300$ mm, $z_2=550$ mm. The zero-order image, original image and conjugate image are existed at the same time when the CGH is reconstructed. Because the CGH is under-sampled, we expand the

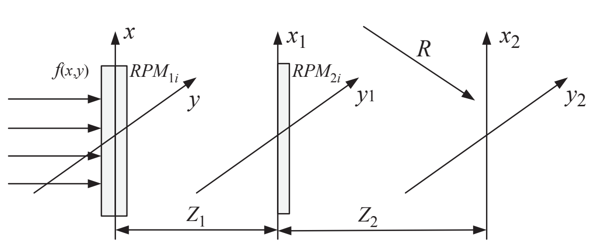

Fig. 1. Optical setup of the encryption system in Fresnel domain.

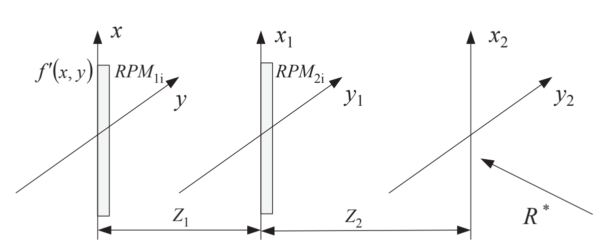

Fig. 2. Optical setup of the optical decryption system in Fresnel domain.