Optik 125 (2014) 2365–2368

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Multi-image encryption based on interference of computer generated hologram

Dezhao Kong [a,*], Xueju Shen [a], Yaqin Shen [b], Xin Wang [a]

[a] Department of Electronic and Optics, Mechanical Engineering College, Shijiazhuang 050003, China
[b] Telecommunications Research Institute, The Ministry of Industry and Information Technology, Beijing 100191, China

ARTICLE INFO

Article history:
Received 19 May 2013
Accepted 14 October 2013

Keywords:
Image processing
Optical security and encryption
Computer holography

ABSTRACT

A multi-image encryption scheme based on interference of computer generated holograms (CGH) is proposed. The encrypted information can be divided into several parts and recorded by corresponding CGHs that distribute randomly. With interference of all CGHs, the original information can be reconstructed. So the multi-image encryption is achieved, and every hologram can be regarded as the key to the corresponding image. Multi-user authentication and storage of information is implemented by applying unique CGH to interfere the common CGH. Furthermore, the CGHs can be cascaded to implement classification of images. When images of different level are assigned to corresponding user, hierarchical encryption is completed successfully. Numerical simulation verifies the feasibility of the method, and demonstrates the security of the algorithm and the decryption characteristics. Flexibility and variability of scheme can be higher than the existing methods. There are a lot of scheme's details still to consider and fulfill in the future.

1. Introduction

The accelerated growth of science and technology has produced an enormous proliferation of data, which demands high transfer rates with secure and reliable data storage for internet, defense, commerce, banking, and other day-to-day applications. Optical information processing, owing to its inherent parallelism and complex 2D data processing, is receiving increased attention. The optical methods can offer the excellent freedom of keys, and the corresponding encryption schemes cover the methods based on phase [1], amplitude [2], polarization [3] and wavelength [4]. The methods proposed can be classified by the application of different optical systems, and the various optical systems mainly contain the implementation of Fourier transform [5], Fresnel transform [6], joint correlator transform [7], fractional Fourier transform [8], phase-shifting interference [9], hologram [10], and the various alterations on basis of the methods mentioned [11–15]. Different schemes have different characteristics and virtues, while better simplicity, higher security and better application are the common goal of the method.

CGH is a hologram encoded by computer which comprehensively records the light's amplitude and phase. With low noise, high repeatability and the ability of free encoding, CGH has more advantages than optical hologram in digital storage of information and photoelectric reconstruction. CGH has been applied widely, for instance hologram display [13,14], optical correlation [15,16], testing of aspherics [17]. With these virtues in mind, we propose the novel method that based on interferences of CGH to implement the optical image encryption. Several holograms distributing randomly interfere together to reconstruct the information protected, so every hologram can be regarded as a partial keys to the image. Furthermore, multi-user authentication can be implemented by assigning different keys to different users, and multi-image encryption and hierarchical encryption can be completed by cascading holograms. This method is verified to have better simplicity, higher security and better applicability than other methods.

2. Principle of the scheme

2.1. Basic theory of computer generated hologram

To begin with, given a discrete, planar image $I(u, v; z_i)$ located at a depth z_i from a holographic recording plane, a complex Fresnel hologram $H_F(m, n)$ can be generated numerically as the product of the object wave $O(m, n; z_i)$ and a planar reference $R(m, n)$ wave according to Eq. (1). If the hologram is to be printed on a film, or displayed on an amplitude spatial light modulator (SLM), only the real part of the complex Fresnel hologram is retained, as shown in Eq. (2):

$$H_F(m, n) = O(m, n; z_i)R*(m, n) \quad (1)$$

* Corresponding author. Tel.: +86 15027404833; fax: +86 031187994222.
E-mail address: xiaowu89511@126.com (D. Kong).

0030-4026/$ – see front matter © 2014 Published by Elsevier GmbH.
http://dx.doi.org/10.1016/j.ijleo.2013.10.066

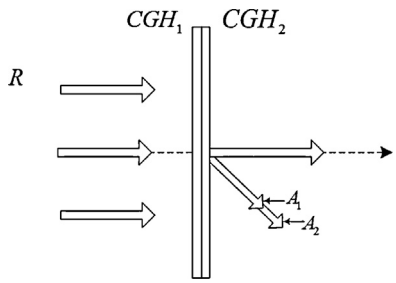

Fig. 1. Single image encryption schematic.

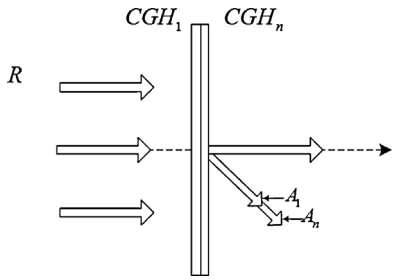

Fig. 2. Multi-image encryption schematic.

$$H(m,n) = Re\{O(m,n;z_i)R*(m,n)\} \tag{2}$$

where $Re\{\}$ represents the real part of a complex number. The object wave is given by

$$O(m,n;z_i) = \sum_{u=0}^{X-1}\sum_{v=0}^{Y-1} I(u,v;z_i)\frac{\exp[ik(m-u,n-v;z_i)]}{r(m-u,n-v;z_i)} \tag{3}$$

where m, u and n, v are the discrete coordinate points along the vertical and horizontal directions, respectively. The $r(m-u,n-v;z_i) = \sqrt{(m-u)^2+(n-v)^2+z_i^2}$ represents the Euclidean distance between an object point at $(u,v;z_i)$ and the location (m,n) on the plane of the hologram. X and Y are the vertical and horizontal extents of the image, $k = 2\pi/\lambda$ is the wave number, and λ is the wavelength of the optical beam. All pixels in the image are assumed to be self-illuminating with intensity $I(u,v;z_i)$. The reference wave $R(m,n)$ is assumed to be a plane wave incident at an angle θ with respect to the normal of the hologram and hence can be represented by $R(m)$ for simpler optical geometry.

Eq. (3) can be encapsulated as the two-dimensional (2D) convolution of the source image with the Fresnel zone plate $F(m,n;z_i)$ as

$$O(m,n;z_i) = I(m,n;z_i) * F(m,n;z_i) \tag{4}$$

where $F(m,n;z_i) = \exp[ikr(m,n;z_i)/r(m,n;z_i)]$ and denotes a 2D convolution operation involving m and n.

Adopting the convolution operation in Eq. (4) in place of Eq. (3), the source image is expressed as a function of m and n (i.e., $I(m,n;z_i)$). The hologram generation process in Eq. (3) can be easily extended to represent a 3D object. The latter is first partitioned into a sequence of evenly spaced planar images positioned at distances $[z_0, z_1, \ldots, z_{N-1}]$ from the hologram. Subsequently, the latter is generated by summing the contribution from each image plane.

2.2. The encryption and decryption algorithm

Encryption scheme based on the interference of CGH (Fig. 1) is described as follows CGH_1 and CGH_2 are computer generated holograms of two pure phase (amplitude constant), and they are exactly same in the number of sampling points and the size, with recording of the same size phase information $\varphi_{O1}(x,y)$ and $\varphi_{O2}(x,y)$, respectively. CGH_1 and CGH_2 are appressed together with their centers aligned. When illuminated with collimated parallel light R, diffraction of two holograms will occur, respectively. Because the pure phase CGH can be very thin, diffracted lights will be overlapping to interfere. Based on pure phase holographic principle, diffracted light contains two components, A_1 and A_2, shown in Eqs. (5) and (6).

$$A_1 = T_O \exp[i\varphi_{O1}(x,y)] \tag{5}$$

$$A_2 = T_O \exp[i\varphi_{O2}(x,y)] \tag{6}$$

where T_O is a constant. A_1 and A_2 propagate in same in the direction of amplitude, and phase difference of them is constant. Then the interference of A_1 and A_2 will happen. With complex amplitude of the interference field $A = A_1 + A_2$, intensity distribution of interference field I can be known.

$$\begin{aligned} I &= \left|A_1 + A_2\right|^2 \\ &= 2T_O^2[1+\cos(\varphi_{O2}-\varphi_{O1})] \\ &= 2T_O^2[1+\cos(\Delta\varphi_1)] \end{aligned} \tag{7}$$

where $\Delta\varphi_1$ is the phase difference of A_1 and A_2. According to the principle described above, if the intensity distribution of interference field is expected to be the certain value I, corresponding two beams of interfered light must have the phase difference $\Delta\varphi_1$. So the amplitude of image to be encrypted M_1 can be expressed as

$$M_1 = k[1+\cos(\Delta\varphi_1)] \tag{8}$$

where k is a constant. The value of M_1 is only decided by phase difference $\Delta\varphi_1$.

$$\Delta\varphi_1 = ar\cos\left(\frac{M_1}{k} - 1\right) \tag{9}$$

The $\Delta\varphi_1$ can be set to be the error of two random phase masks $\varphi_{O1} - \varphi_{O2}$. When they are stored in two CGHs, respectively, the encryption is completed. Both CGHs can be regarded as the keys and encrypted images. In the reconstruction, the two holograms are aligned together. With collimated parallel light illuminated, the diffraction light from two holograms interferes. The interference intensity distribution of the light field is modulated by error of diffraction light's phase, shown as Eq. (9). Finally, the original image is reconstructed and recorded by CCD.

From the introduction and verification above, it can be seen that the scheme is simple and stable, as encryption and decryption are completed by just two CGHs. With information protected by a random distribution of CGHs, the scheme still reconstructs a high quality copy of original image. Compared with the scheme proposed already, the scheme has virtues of the simplicity, low requirement of encryption environment, flexibility. Also, the keys are easy to carry and copy.

From the single image encryption, the basic principle of encryption is introduction. When we use CGH_1 to encrypted multi-image, multi-image encryption is obtained, shown as in Fig. 2. The first computer generated hologram CGH_1 can be regarded as a common key, and different image M_{n-1} can get their own unique encryption by applying personal keys CGH_n in decryption. The information cannot be obtained in the absence of either common key or personal key. Thus, multi-user encryption can be achieved and it can ensure the security and independence of the user.

On the other hand, it also means to achieve a system to store multi-user's information successfully. The storage of information can be completed just by combining a common hologram with the user's own information. The scheme is not only simple and convenient, but also has a large capacity. The scheme can also be applied