Optics Communications 407 (2018) 51–56

Contents lists available at ScienceDirect

Optics Communications

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

Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography

Lihong Ma, Weimin Jin *

Zhejiang Normal University, Institute of Information Optics, Jinhua, Zhejiang, 321004, China
Key Laboratory of Optical Information Detecting and Display Technology in Zhejiang Province, Jinhua, Zhejiang, 321004, China

ARTICLE INFO

Keywords:
Optical image encryption
Symmetric and asymmetric cryptosystem
Compressive sensing
Computer generated holography

ABSTRACT

A novel symmetric and asymmetric hybrid optical cryptosystem is proposed based on compressive sensing combined with computer generated holography. In this method there are six encryption keys, among which two decryption phase masks are different from the two random phase masks used in the encryption process. Therefore, the encryption system has the feature of both symmetric and asymmetric cryptography. On the other hand, because computer generated holography can flexibly digitalize the encrypted information and compressive sensing can significantly reduce data volume, what is more, the final encryption image is real function by phase truncation, the method favors the storage and transmission of the encryption data. The experimental results demonstrate that the proposed encryption scheme boosts the security and has high robustness against noise and occlusion attacks.

1. Introduction

Optical encryption technique was first introduced by Réfrégier and Javidi in 1995 [1]. This method is based on double random phase encoding method (DRPE), which uses two statistically independent random phase masks at the input plane and the Fourier plane to encrypt the primary image into stationary white noise. Owing to the inherent advantages of parallel processing and more encryption freedoms compared with electronic encryption counterparts, optical encryption techniques have been extensively studied in the recent 20 years [2–12]. However, most of these proposed methods stem from DRPE. And the encrypted images are often recorded and stored by traditional optical holograms with silver halide plates. It is very difficult to transmit such analog encrypted holograms through the internet. The digitization of the encrypted images favors the information storage and transmission, and even real-time transmission and display through the internet. The most effective method to digitalize the encrypted images is digital holography (DH) or computer generated holography (CGH) [13–16]. Especially by CGH, besides any wavelength to be selected and system parameters to be adjusted arbitrarily, the virtual object, which does not yet exist in nature, can also be encrypted.

However, all the encryption methods mentioned above belong to the category of symmetric cryptosystems, in which the encryption keys are identical to the decryption keys. From the cryptography point of view, it is difficult for symmetric cryptosystems to safely manage, distribution and transmit the secret keys under network environment. That is to say, the symmetric cryptosystems easily suffer from the key attacks and the security is relatively low. In this regard, it is necessary to develop asymmetric cryptosystems to solve those problems encountered in the symmetric cryptosystems. Peng and Qin proposed an asymmetric cryptosystem based on a phase-truncated Fourier transform [17,18], in which two decryption keys are different from the encryption keys. Owing to the nonlinear operation of phase truncation, high robustness against existing attacks could be achieved. Other asymmetric cryptographic systems have also been proposed [19].

Instead of taking samples at the Shannon–Nyquist rate, Candes and Donoho proposed a new signal processing theory called compressive sensing (CS) [20–22], which can fulfill the compressive sampling at a significantly lower rate than that of the Shannon–Nyquist sampling theorem. Due to significantly reducing data volume, CS has attracted many researchers who studied in image and signal processing [23,24]. Subsequently, many image encryption schemes by combining CS have been proposed [25–28]. CS-based image encryption algorithms greatly benefit the information storage and transmission. However, the encryption scheme only based on CS technique cannot achieve perfect security. On the other hand, as the compressed encryption image is complex signal, the holography is usually adopted to record the signal.

* Corresponding author at: Zhejiang Normal University, Institute of Information Optics, Jinhua, Zhejiang, 321004, China.
E-mail address: jhjinwm@163.com (W.M. Jin).

http://dx.doi.org/10.1016/j.optcom.2017.08.047
Received 6 April 2017; Received in revised form 17 August 2017; Accepted 20 August 2017
0030-4018/

Factually, the method of reality-preserving more favors the signal recording [29,30].

In this paper, to the best of our knowledge, a novel symmetric and asymmetric hybrid cryptosystem, based on a skillfully combination of CGH, CS and phase truncation techniques, is proposed, which can more effectively keep information secret with low data volume. In the encryption process, there are six secret keys, two random phase masks, a random measurement matrix, two Fresnel diffraction distances and the recording wavelength. In the decryption process, the random measurement matrix, the two Fresnel diffraction distances and the recording wavelength are still served as the symmetric secret keys, which are identical to the counterparts in the encryption process. However, the two phase masks obtained by phase preserving in the encryption process are served as asymmetric secret keys, which are different from the random phase masks used as the encryption keys. Therefore, the proposed method is a symmetric and asymmetric hybrid cryptosystem. The method not only inherits the advantages from CGH and CS but the nonlinear operation of phase truncation boosts the security. Hopefully it will provide a novel scheme for optical image encryption.

2. Fundamental theory

2.1. Compressive sensing

CS theory [20–24] relies mainly on two guiding principles, sparsity and incoherence. The sparsity is that any natural signal can be compressible or be sparse in certain basis and thus the compressed small numbers of measurements reserve adequate information of the primary image to ensure perfect recovery of it. Nature signal in time domain or in space domain is not usually sparse. However, nature signal in certain transform domain, such as in discrete Fourier transform domain (DFT), discrete wavelet transform domain (DWT), discrete cosine transform domain (DCT), is usually sparse. Here, take one-dimension (1-D) signal for example, suppose x is a signal with length N and in R^N space can be represented in an orthonormal basis $\psi := [\psi_1, \psi_2, \dots, \psi_N]$ as follows:

$$x = \sum_{i=1}^{N} \alpha_i \psi_i = \psi\alpha \tag{1}$$

where α is the coefficient sequence of signal x. The signal is compressible if the coefficient vector α satisfies $\|\alpha\|_0 \ll N$ where $\|\alpha\|_0$ is the number of the nonzero coefficient. That is to say, coefficient vector α is sparse. In CS process, an $M \times N$ $(M < N)$ measurement matrix Φ incoherent with ψ is used to obtain a measurement vector. The measurement process is:

$$y = \Phi x = \Phi\psi\alpha = \Theta\alpha \tag{2}$$

where y is an $M \times 1$ measurement vector, the sensor matrix Θ is the product of Φ and ψ. To reconstruct the signal correctly, the sensor matrix Θ should meet restricted isometry property (RIP). And the length M of the measurement vector y satisfies:

$$M \geq cK \log(N/K) \tag{3}$$

where c is a constant which is very small and $k = \|\alpha\|_0$ is the number of the nonzero coefficient. The input signal x can be recovered with probability from measurement vector y by solving an on-convex problem:

$$\min \|\alpha\|_0 \; s.t. y = \Theta\alpha. \tag{4}$$

To solve the above problem, some reconstruction schemes have been developed, such as Basis Pursuit algorithm (BP), Total Variation Minimization algorithm (TV), Orthogonal Matching Pursuit algorithm (OMP), Compressive Sampling Matching Pursuit algorithm (CoSaMP), and Smooth l_0 algorithm (SL0). OMP algorithm is adopted in this proposed method.

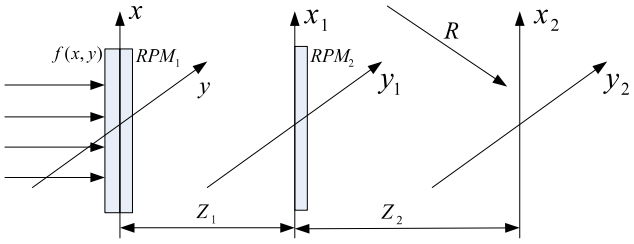

Fig. 1. Schematic of the CGH encryption system in Fresnel domain.

2.2. Image encryption technique by computer generated holography

2.2.1. The CGH encryption method

As is known to all, CGH stems from optical holography but the hologram is generated by programming and computing, which is numerical simulation of optical holography. Therefore, it is flexible for CGH to set the system parameters and it is available to obtain the digitalized encryption hologram.

The CGH encryption system is schematically shown in Fig. 1. Three parallel planes are defined as the input plane (x, y), the transform plane (x_1, y_1), and the output plane (x_2, y_2). The distances between adjacent planes are z_1 and z_2, respectively, which satisfy the Fresnel approximation. The input image is expressed as $f(x, y)$. Two random phase-only masks RPM1 and RPM2 are used to encode the input image at the input plane and the transform plane, where RPM1 $= \exp[j2\pi M_1(x, y)]$ and RPM2 $= \exp[j2\pi M_2(x_1, y_1)]$. Therefore, the encryption method is still based on the DRPE but the transform plane is at the Fresnel plane. The digitalized reference light beam R is introduced. Thus two complex fields interfere at the output plane and a computer generated hologram is generated.

The input image is perpendicularly illuminated by a plane wave. Assume that the wavelength of the illuminating light is λ. And in CGH any wavelength can be selected. In the encryption process, the input digital image $f(x, y)$ is first modulated by the first random phase mask RPM1, then the transmitted light field propagates to the transform plane by Fresnel diffraction with the distance z_1. Thus, the complex amplitude distribution obtained at the transform plane (x_1, y_1) can be expressed as follows:

$$f(x_1, y_1) = FrT_{Z1}\{f(x, y)\exp[j2\pi M_1(x, y)]\} \tag{5}$$

where FrT denotes the Fresnel diffraction. Then $f(x_1, y_1)$ is modulated by the second random phase mask RPM2 and the transmitted light field propagates to the output plane by Fresnel diffraction with the distance z_2. The complex amplitude field at the output plane can be expressed as follows:

$$f(x_2, y_2) = FrT_{Z2}\{f(x_1, y_1)\exp[j2\pi M_2(x_1, y_1)]\}. \tag{6}$$

As shown in Fig. 1, the digitalized reference light R illuminates directly onto the output plane and the encrypted digital hologram obtained is expressed as follows:

$$I(x_2, y_2) = \left|R(x_2, y_2) + f(x_2, y_2)\right|^2. \tag{7}$$

2.2.2. The CGH decryption method

For a digitalized hologram, it can be reconstructed by numerical calculation which is the numerical simulation of optical hologram reconstruction. As shown in Fig. 2, we generate a numerical plane wave R^*, which is the conjugate wave of the reference wave, to illuminate the encrypted hologram. After filtering the zero term and the virtual image, the complex amplitude of transmitted wave $f^*(x_2, y_2)$, which is the conjugate wave of the object wave, can be obtained. Through Fresnel diffraction with the distance z_2, the complex amplitude distribution