ARTICLE IN PRESS

Optics Communications ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Optics Communications

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

Image/video encryption using single shot digital holography

Xiaoyu Li [a], Chen Tang [a,*], Xinjun Zhu [a], Biyuan Li [a], Linlin Wang [b], Xiusheng Yan [c]

[a] Department of Applied Physics, University of Tianjin, Tianjin 300072, PR China
[b] Shenyang Institute of Aeronautical Engineering, Shenyang 110136, PR China
[c] Key Laboratory of Science and Technology on Photo-electric Information Safety Control, Yanjiao, Hebei 605201, PR China

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form
3 December 2014
Accepted 31 December 2014

Keywords:
Digital holography
Optical security and encryption
Information processing

ABSTRACT

We propose a method for image/video encryption that combines double random-phase encoding in the Fresnel domain with a single shot digital holography. In this method, a complex object field can be reconstructed with only single frame hologram based on a constrained optimization method. The system without multiple shots and Fourier lens is simple, and allows to dynamically encrypt information. We test the proposed method on a computer simulated image, a grayscale image and a video in AVI format. Also we investigate the quality of the decryption process and the performance against noise attacks. The experimental results demonstrate the performance of the method.

1. Introduction

Optical encryption and security has become an interest-raising research topic in the past few years. The main advantages of optical encryption systems over traditional security systems are that they are able to write and read in parallel complex (amplitude and phase) information, which leads to rapid transmission of information [1]. In addition, they provide a large degree of freedom to secure data with which the optical beam may be encoded, such as amplitude, phase, wavelength, and polarization [2]. Various types of optical information security have been proposed, such as optical correlations [1], computer generated holography [3], digital holography [4,5], random phase mask encoding [6,7], fractional Fourier transform [8], and polarization [9]. Among them, the double random mask encoding is widely used due to its good performance. It performs better than amplitude-based encryption in the presence of noise [10]. In Ref. [6], Javidi et al. put one random-phase mask at object plane and another at Fourier plane. Situ and Zhang extended its use from Fourier domain to Fresnel domain [11]. The method added the Fresnel propagation distance as a decryption key, so the secrecy of the systems is increased. On the other hand, digital hologram can directly record full complex information using a charge-coupled device (CCD) camera instead of photographic plates, and the 3D reconstruction of object is performed numerically by transforming the measured digital hologram, so it has an advantage of real time digital information processing.

Optical encryption and decryption need to record and reconstruct complex values, which can readily be performed using digital holography. Digital holography can be generally classified into in-line holography and off-axis holography. For a same object, an off-axis holography system must provide a space-bandwidth product that is at least a factor of four greater than that needed in an in-line arrangement. However, a CCD sensor has a limited spatial resolution. In order to take greatest use of space-bandwidth of a CCD, in-line digital holography is usually used for optical encryption. In addition, for an off-axis arrangement, since digital imaging of an object has to meet simultaneously both the need of the minimum offset angle and the limitation of the maximum interference angle, the requirement of the recording distance is stricter as compared with that of an in-line system. In an in-line system, less constraint is applied to the effective field of view, which allows a test object to be imaged with higher resolution, and hence more details can be detected [12]. As far as we know, the in-line holography is always used in dealing with optical encryption problem, for example the arrangements in Refs. [2,4,13,14]. However, in in-line digital hologram, the dc and the cross terms overlap in the Fourier domain. Some attempts to suppress zero-order and conjugate image terms were made in in-line digital hologram, such as subtracting the average intensity from the recorded hologram [15]. In addition, phase-shifting techniques are also commonly used to retrieve the original complex information. Phase shifting methods in digital holography have been studied by Yamaguchi and Zhang [16] at first. And then, several different types of phase-shifting algorithms have been proposed. Tajahuerce et al. used a 4-step phase-shifting algorithm to encrypt and decrypt data in which one random phase mask was

---

* Corresponding author.
E-mail address: tangchen@tju.edu.cn (C. Tang).

http://dx.doi.org/10.1016/j.optcom.2014.12.082
0030-4018/© 2015 Published by Elsevier B.V.

Please cite this article as: X. Li, et al., Optics Communications (2015), http://dx.doi.org/10.1016/j.optcom.2014.12.082

attached to the input plane in the object beam and another phase mask was put at a variable position in the reference beam based on a Mach–Zehnder interferometer architecture [13]. When the encrypted information is transmitted, minimizing the amount of data is important for fast data transmission. Some works have been developed to reduce the number of phase-shifting interferograms. Meng et al. proposed the two-step phase-shifting interferometry to encrypt and decrypt images based on double random-phase encoding in the Fresnel domain [14]. Recently, Jeon et al. proposed a new 2-step phase-shifting digital holographic optical encryption [17]. The system contains two random phase patterns, two spatial light modulators and two Fourier lenses. Although a 2-step phase-shifting digital holographic technique is more efficient than 4-step or multi-step phase-shifting methods, it still needs two interferograms. These methods need to take multiple records for calculating, so we need consider the stability of experimental equipments during several shots and the error which generated in phase shifter adjustment. Therefore optical encryption and decryption from a single hologram frame, if possible, are particularly expected. In this paper, motivated by the two-step phase-shifting interferometry for image encryption [14], we propose a security system that combines double random-phase encoding in the Fresnel domain with a single shot digital holography for image/video encryption. Our system is similar to the system in [14]. The difference is that our system has not phase shifting device, but theirs has. Their method needs to record two holograms, and use 2-steps phase shifting algorithm to decryption. Our method only needs one recorded hologram, and uses a constrained optimization algorithm to reconstruct decrypted image. With the system, we successfully encrypt and decrypt a video, believed to be new.

2. The proposed algorithm

Like most existing systems, the proposed system is also based on Mach–Zehnder interferometer architecture as shown in Fig. 1. Obviously, the system does not contain any Fourier lens and phase-shift device, so it is simple. A plane object wave illuminates an image/video to be encrypted in the plane (x_0, y_0), which is bonded with the first random-phase mask (RPM1), and then passes through the second random-phase mask (RPM2) in the plane (x_1, y_1). Let us assume that the complex amplitude transmittances of RPM1 and RPM2 are $\exp[i2\pi p(x, y)]$ and $\exp[i2\pi q(x, y)]$, where $p(x, y)$ and $q(x, y)$ are two independent white noises uniformly distributed in [0, 1]. The distance between the plane (x_0, y_0) and the plane (x_1, y_1) is z_1, and the distance between (x_1, y_1) and (x, y) is z_2. The complex object field in the recording plane can be written as

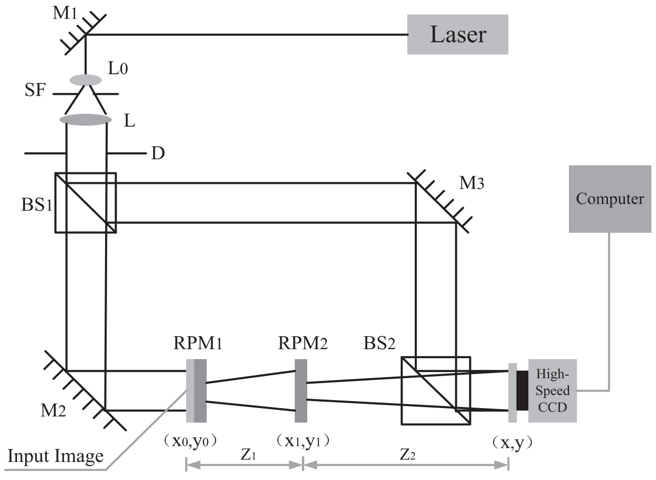

Fig. 1. Optical setup of the proposed method.

$$O_0(x, y) = FR_{z2}\left\{FR_{z1}\left\{U_0\left(x_0, y_0\right)\exp\left[i2\pi p\left(x_0, y_0\right)\right]\right\}, \exp\left[i2\pi q\left(x_1, y_1\right)\right]\right\} \quad (1)$$

where O_0 stands for object wave function at camera plane, FR_z stands for the Fresnel transform of distance z. U_0 stands for the complex value of input image.

The upper arm is the reference wave R that may be described as

$$R = |R| \exp(ikx \sin\theta), \quad (2)$$

where k is the wave number and θ is the angle between the reference beam and object beam. In the in-line hologram θ equals to zero as usual.

The object wave and reference wave intervene at the CCD plane (x, y) to form a hologram that can be expressed as

$$H = |O_0|^2 + |R|^2 + O_0R^* + O_0^*R, \quad (3)$$

here * stands for a complex conjugate.

By recording the hologram, a noise-like encrypted image can be sent to the receivers via the internet. However, in the hologram recorded by the system, the dc and the cross terms overlap seriously in the Fourier domain. Recently Khare et al. proposed a constrained optimization method for image recovery from a hologram [18]. Here we improve the method from a simple technical processing for image/video encryption. What follows is a brief synopsis of the method.

In Eq. (3), the reference beam R is known, while the complex object function O in the hologram plane is unknown. The method models the reconstruction of the complex object field in the hologram plane as a constrained optimization problem [19]. The cost function to be minimized was defined by

$$C\left(O, O^*\right) = \frac{1}{2}\|H - \left(|O|^2 + |R|^2 + OR^* + O^*R\right)\|^2 + \alpha\psi\left(O, O^*\right). \quad (4)$$

The first term on the right hand side in Eq. (4) is an L2-norm squared error data fit and the function of the second term $\psi\left(O, O^*\right)$ is a penalty function for imposing a smoothness constraint on the complex object function O. In a Fresnel zone in-line configuration as used, the smoothness constraint is justified as O is a diffracted field and is expected to have local smoothness. Further, an appropriate use of smoothness constraint guarantees the absence of any modulation due to carrier fringe frequency or its harmonics in the solution of the minimization problem for O [20]. α is a parameter that controls the relationship between the L2-norm squared error term and the constraint term.

The optimization problem can be solved iteratively by steepest descent method. The gradient of the cost function in Eq. (4) with respect to O^* is

$$\nabla_{O^*} C\left(O, O^*\right) = -\left[H - \left(|O|^2 + |R|^2 + OR^* + O^*R\right)\right] (O + R) + \alpha\nabla_{O^*}\psi(O, O^*). \quad (5)$$

hence, the iteration scheme is

$$O^{(n+1)} = O^{(n)} - t\left[\nabla_{O^*} C\right]_{O=O^{(n)}}. \quad (6)$$

t is a positive constant denoting step size. Operationally, α is set for zero. In each iteration, the averaging filter denoted as G is used to improve the results:

Please cite this article as: X. Li, et al., Optics Communications (2015), http://dx.doi.org/10.1016/j.optcom.2014.12.082