Optics and Lasers in Engineering 100 (2018) 118–123

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Two-level image authentication by two-step phase-shifting interferometry and compressive sensing

Xue Zhang [a], Xiangfeng Meng [a,*], Yongkai Yin [a], Xiulun Yang [a], Yurong Wang [a], Xianye Li [a], Xiang Peng [b], Wenqi He [a], Guoyan Dong [c], Hongyi Chen [d]

[a] Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China
[b] College of Optoelectronics Engineering, Shenzhen University, Shenzhen 518060, China
[c] College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[d] College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China

ARTICLE INFO

Keywords:
Compressive sensing
Two-step phase-shifting interferometry
Image encryption
Image authentication

ABSTRACT

A two-level image authentication method is proposed; the method is based on two-step phase-shifting interferometry, double random phase encoding, and compressive sensing (CS) theory, by which the certification image can be encoded into two interferograms. Through discrete wavelet transform (DWT), sparseness processing, Arnold transform, and data compression, two compressed signals can be generated and delivered to two different participants of the authentication system. Only the participant who possesses the first compressed signal attempts to pass the low-level authentication. The application of Orthogonal Match Pursuit CS algorithm reconstruction, inverse Arnold transform, inverse DWT, two-step phase-shifting wavefront reconstruction, and inverse Fresnel transform can result in the output of a remarkable peak in the central location of the nonlinear correlation coefficient distributions of the recovered image and the standard certification image. Then, the other participant, who possesses the second compressed signal, is authorized to carry out the high-level authentication. Therefore, both compressed signals are collected to reconstruct the original meaningful certification image with a high correlation coefficient. Theoretical analysis and numerical simulations verify the feasibility of the proposed method.

1. Introduction

Since Réfrégier and Javidi proposed the double random phase encoding (DRPE) technique in 1995 [1], optical information security has attracted much attention due to its significant advantages, such as parallel computing and multiple encoding dimensions, and it has been successfully combined with other optical information processing techniques or transforms, such as fractional Fourier transform [2,3], Fresnel transform [4,5], digital holography [6], phase retrieval [7–9], gyrator transform [10], fractional Mellin transform [11], two-beam interference [12], joint transform correlator [13], diffractive imaging [14], polarization encoding [15], jigsaw transform [16], aperture movement [17], phase reservation and compression [18], and ghost imaging [19,20].

In 2000, Tajahuerce et al. proposed a three-dimensional information encryption method based on random phase encoding and four-step phase-shifting digital holography [21], by which the phase and amplitude information generated by a 3D object at a plane located in the Fresnel diffraction region can be recorded. Subsequently, Cai et al. proposed a digital image encryption and watermarking method based on DRPE and three-step phase-shifting interferometry (PSI), in which the image to be hidden is stored in three interferograms and then can be reconstructed using one random phase mask, geometric parameters keys, and a specific decryption algorithm [22]. To raise the efficiency of encrypted information transmission, in 2006, we proposed the two-step phase-shifting algorithm [23], by which an original complex field can be retrieved with only two interferograms, and then applied it to an image encryption system based on DRPE in the Fresnel domain.

Compressive sensing (CS) is a newly developed signal processing technique for efficiently acquiring and reconstructing a signal by finding solutions to underdetermined linear systems. It is based on the principle that, through optimization, the sparsity of a signal can be exploited to recover it from far fewer samples than required by the Shannon-Nyquist sampling theorem [24–27]. Based on CS and DRPE, Deepan et al. proposed a multiple-image encryption method [28] in 2014. Subsequently, Zhou et al. proposed an image compression-encryption hybrid algorithm based on a key-controlled measurement matrix in CS [29]. Recently, Li

* Corresponding author at: Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China.
E-mail address: xfmeng@sdu.edu.cn (X. Meng).

http://dx.doi.org/10.1016/j.optlaseng.2017.08.002
Received 19 May 2017; Received in revised form 1 August 2017; Accepted 1 August 2017
0143-8166/

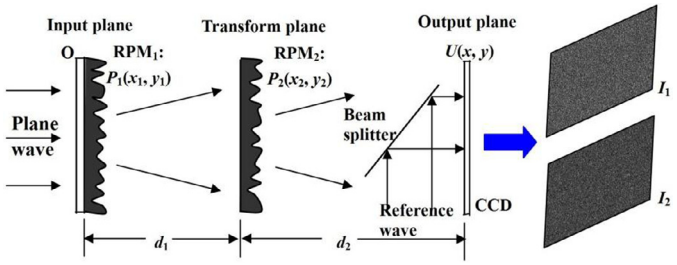

Fig. 1. Schematic diagram of the image encoding.

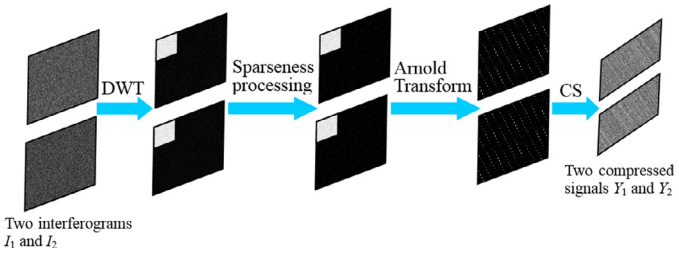

Fig. 2. Schematic diagram of the interferogram data compression.

et al. conducted a series of explorations in optical information encryption using phase-shifting digital holography and CS [30,31]. To decrease the data volume required for storing or transmitting encrypted interferograms and further increase the authority levels, here we present a two-level image authentication method based on two-step PSI, DRPE and CS, which can accomplish both low-level and high-level authentication for the certification image. We first present the theoretical analysis, description, and procedure of the method, then provide its simulation verification, and finally draw the conclusion.

2. Theoretical analysis and description of the authentication system

2.1. Image encoding by two-step PSI and DRPE

The schematic diagram of image encoding is shown in Fig. 1. In the authentication center, a certification image O that is to be hidden is in contact with a random phase mask (RPM_1) P_1 and placed at the input plane; the other RPM_2: P_2 is placed at the transform plane, where P_1 and P_2 are two independent white noises that are uniformly distributed in the interval [0, 1]. The distances between the input plane, the transform plane and the output plane are denoted by d_1 and d_2, respectively. When an on-axis plane wave of wavelength λ is inputted into the input plane, the complex wave $U(x, y)$ at the output plane can be mathematically represented by [22,23,32]

$$U(x,y) = \mathrm{FrT}_{d1}\left\{O(x_1,y_1)\exp\left[i2\pi P_1(x_1,y_1)\right]\right\}\exp\left[i2\pi P_2(x_2,y_2)\right], \quad (1)$$

where FrT_d stands for the Fresnel transform of distance d.

We can simplify Eq. (1) to $U(x,y) = A_0(x,y)\exp[i\varphi(x,y)]$, where $A_0(x, y)$ and $\varphi(x, y)$ denote the amplitude and phase of the complex wave $U(x, y)$, respectively. Then, A_r is the constant amplitude of the on-axis reference plane wave, and it is larger than the maximum pixel value of $A_0(x, y)$. The phase shifts or phase steps that are introduced in the first and second exposures are 0 and δ, respectively. By the two-step PSI algorithm [23], we can obtain two interferograms (I_1, I_2), whose intensity distributions are

$$I_1(x,y) = {A_0}^2(x,y) + {A_r}^2 + 2A_0(x,y)A_r\cos\varphi(x,y), \quad (2)$$

$$I_2(x,y) = {A_0}^2(x,y) + {A_r}^2 + 2A_0(x,y)A_r\cos[\varphi(x,y)-\delta]. \quad (3)$$

In this way, the information of certification image O is encoded into the two interferograms.

2.2. Interferogram data compression by CS

Compressive sensing (CS) theory asserts that one can recover certain signals and images from far fewer samples or measurements than traditional methods use. Compressive sensing combines sampling and compression into a single non-adaptive linear measurement process. It mainly consists of three steps: sparse representation, random projection and reconstruction [25,30,31].

First, a brief overview of CS is given. In signal compression theory, any signal that is sparse or sparsifiable can be compressed through a measurement matrix. Taking as an example a one-dimensional signal of size $n\times1$ that is redundant and can be sparsified in other domains through an orthogonal basis transform such as the discrete cosine transform or discrete wavelet transform, the procedure can be expressed as

$$s = \Psi\alpha, \quad (4)$$

where α is the sparse representation of the initial signal s in the transform domain and Ψ is the corresponding orthogonal basis. Then, the sparse signal α can be easily compressed through an $m\times n$ measurement matrix Φ whose dimensions satisfy

$$ck\log\left(\frac{n}{k}\right) \le m << n, \quad (5)$$

where k is the sparsity of the signal in the transform domain, which denotes the number of non-zero elements in this signal, and c is a constant. Then, the sparse signal can be easily compressed into a small measurement signal of size $m\times1$ and the mathematical description can be expressed as

$$y = \Phi\alpha = \Phi\Psi^T s. \quad (6)$$

In the signal reconstruction procedure, orthogonal basis Ψ is a known basis, and knowledge of α is equivalent to knowledge of s. Therefore, the reconstruction involves solving for the sparse signal α from the measurement signal y and measurement matrix Φ, which is a convex optimization problem and can be written as

$$\tilde{\alpha} = \arg\min||\alpha||_1 \quad s.t.\ \Phi\alpha = y, \quad (7)$$

where $||\bullet||_1$ denotes the L_1-norm. To recover the sparse signal α, there are many alternative reconstruction algorithms, such as Orthogonal Match Pursuit (OMP) [33], Basic Pursuit (BP) [34], and Subspace Pursuit (SP) [35]. Subsequently, it is easy to acquire the initial signal s from α through the corresponding inverse transform.

The schematic diagram of interferogram data compression in our scheme is shown in Fig. 2, in which two interferograms (I_1, I_2) of size $N\times N$, which are acquired from two-step PSI, are sparsified through the third-order Haar wavelet transform, and a threshold value is selected beforehand to control the sparsity K; the pixel values that are smaller than the threshold value are set to zero. To realize a smaller but safe key space, we control the two intensity distributions with similar sparsity, so that they can be compressed by the same measurement matrix Φ. Then, the Arnold transform is applied to the two sparse images to obtain more uniform sparseness distributions for every column. The measurement matrix Φ, which is a standard Gaussian distribution matrix, is randomly selected and is of size $M\times N$, where M and N satisfy the equation $cK\log(N/K) \le M << N$, which was described above, but the sparsity K is the maximum column sparsity in the two scrambled images. Then, the two scrambled images can be compressed by measurement matrix Φ and we obtain two compressed signals (Y_1, Y_2) of size $M\times N$; the mathematical description can be expressed as

$$Y_i = \Phi\times {I^s}_i \quad (i = 1, 2), \quad (8)$$

where Y_i denotes the compressed signal result of the ith interferogram. ${I^s}_i$ is the ith intensity distribution after sparsification and application of the scramble transform, and Φ is the measurement matrix.