Optics and Lasers in Engineering 88 (2017) 214–220

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Information verification and encryption based on phase retrieval with sparsity constraints and optical inference

Shenlu Zhong, Mengjiao Li, Xiajie Tang, Weiqing He, Xiaogang Wang *

School of Sciences, Zhejiang A&F University, Lin'an, Zhejiang Province, 311300 China

ARTICLE INFO

Article history:
Received 26 January 2016
Received in revised form
1 July 2016
Accepted 25 August 2016

Keywords:
Optical encryption
Information authentication
Phase retrieval
Phase encoding

ABSTRACT

A novel optical information verification and encryption method is proposed based on inference principle and phase retrieval with sparsity constraints. In this method, a target image is encrypted into two phase-only masks (POMs), which comprise sparse phase data used for verification. Both of the two POMs need to be authenticated before being applied for decrypting. The target image can be optically reconstructed when the two authenticated POMs are Fourier transformed and convolved by the correct decryption key, which is also generated in encryption process. No holographic scheme is involved in the proposed optical verification and encryption system and there is also no problem of information disclosure in the two authenticable POMs. Numerical simulation results demonstrate the validity and good performance of this new proposed method.

1. Introduction

Information security has already become a vital element in contemporary society, particularly as information collection and distribution become ever more connected through electronic information delivery systems and commerce. In past decades, various researches on digital and optical security systems have been conducted [1–3]. One of the most attractive optical image encryption techniques is the double random phase encoding (DRPE) in Fourier domain proposed by Refregier and Javidi in 1995 [4]. It has spawned many variation infrastructures and methods, such as DRPE based on fractional Fourier transform [5–8], Fresnel transform [9–11] and gyrator transform [12–14]. In order to remove the linearity of the classical DRPE systems that may results in vulnerability to several attacks [15–19], a nonlinear DRPE scheme based on phase-truncated Fourier transforms was proposed in 2010 [20], where the decryption phase keys were generated during encryption. However, it was found to be vulnerable to the attacks based on iterative amplitude-phase retrieval algorithms [21,22]. Nevertheless, it's important to note that attacks on the security of a cryptosystem can also be used for encryption and security enhancement. Based on the idea of the specific attack [21], nonlinear optical cryptosystems in Fourier domain [23] and Fresnel domain [24] have also been proposed by employing a cascaded Yang–Gu (or Gerchberg-Saxton) algorithm. Furthermore, a target image can be encoded into a preselected fake image by reverse-engineering the modified amplitude-phase retrieval-based attack under the framework of nonlinear DRPE [25].

Recently, the classical DRPE has been integrated with photon-counting imaging for information authentication [26–31]. To make the decrypted images contain sufficient information for verification, photon-counting imaging technique has been applied to the double-random-phase encoded image [26], optically encoded quick response (QR) codes [27], full phase version of the primary image [28], and so on [29–31]. Alternative information authentication methods with sparse representation have also been proposed by extracting sparse data randomly from double-random-phase encoded images [32–36]. Complex holographic schemes, however, are always required in those verification methods with sparse representations [26–34]. A simplified verification can be achieved by integrating the classical optical DRPE with an iterative phase retrieval algorithm using 2D median filtering [35], where only sparse phase data retrieved from the optically encoded intensity patterns are used for information verification. Optical authentication with sparse representation allows us to identify the encrypted images without information disclosure of primary image. Actually, it can also provide us a way to design authenticable diffractive optical elements for secure information recovery [36].

In this paper, we propose a novel optical verification and encryption method based on interference principle and iterative phase retrieval algorithm with sparsity constraints. Two sparse phase-only masks (POMs) are first obtained by using DRPE-based optical information authentication scheme and the modified iterative phase retrieval algorithm with 2D median filtering. No complex holographic scheme is used during the production of sparse POMs. To encrypt the target image into two POMs that are

* Corresponding author.
E-mail address: wxg1201@163.com (X. Wang).

http://dx.doi.org/10.1016/j.optlaseng.2016.08.015
0143-8166/

different from the sparse POMs, a fast phase retrieval algorithm under the framework of nonlinear DRPE is applied, where one of the sparse POMs is used as a sparsity constraint and the other is a fixed constraint after being modified by a random phase mask (PRM). In the decryption process, the encrypted results, i.e., the two POMs obtained using iterative phase retrieval algorithm with sparsity constraints need to be identified in the classical optical DRPE scheme. The target image can be optically reconstructed when the two authenticated POMs are Fourier transformed and convolved by the correct decryption key, which is also generated in encryption. No unintended information disclosure can be found in the proposed method. The rest of this paper is organized as follows. In Section 2, we describe the principle of the proposed algorithm. In Section 3, the feasibility and security of this method is verified by numerical simulations. Some conclusions are finally presented in Section 4.

2. Proposed algorithm

The Proposed algorithm consists of the following steps: (1) Producing two sparse POMs $S_1(x)$ and $S_2(x)$ from two secrete images by integrating iterative phase retrieval algorithm and optical DRPE; (2) Numerical calculation of the two authenticable POMs $M_1(x)$ and $M_2(x)$ and the decryption phase key $K(\mu)$ based on phase retrieval with sparsity constraint and optical inference.

2.1. Producing sparse data by integrating iterative phase retrieval algorithm and optical DRPE

To generate parse POMs $S_1(x)$ and $S_2(x)$, two secret images $g_1(x)$ and $g_2(x)$ are individually encoded into white noise in optical DRPE system shown in Fig. 1, where two RPMs, $R_1(x) = \exp[i\alpha(x)]$ and $R_2(\mu) = \exp[i\beta(\mu)]$ with $\alpha(x)$ and $\beta(\mu)$ uniformly distributed over $[0, 2\pi]$, are respectively placed at the input plane and the spatial frequency domain. When function $g_1(x)$ is used as the input signal, the amplitude part of the complex-valued wave function recorded at the CCD plane can be given by

$$\psi(x) = \left|\left[g_1(x)R_1(x)\right] \otimes h_1(x)\right| \tag{1}$$

where $h_1(x) = \mathrm{IFT}\{R_2(\mu)\}$ and the symbols $\otimes$, $|\,|$ and IFT[] stand for convolution, modulus and the inverse Fourier transform, respectively. A sparse phase distribution $S_1(x)$ can be obtained from the function $\phi(x)$ by using a modified iterative phase retrieval algorithm with 2D median filtering [35], which is presented in the following.

(i) Start with a guess at the object function $g_1^{(j)}(x)$, where the subscript j represents the jth iteration. The phase part of the outcome of DRPE can be respectively given by

$$p^{(j)}(x) = \mathrm{PR}\left[\left(g_1^{(j)}(x)R_1(x)\right) \otimes h_1(x)\right] \tag{2}$$

where the operator PR[] denotes phase reservation, retaining the phase part of the complex function but removing its amplitude part. Note that $g_1(x)$ is an array of all ones in the initial stage.

(ii) Function $p^{(j)}(x)$ is multiplied by the known value $\psi(x)$ and then convolved by function $h_2(x)$ which is given by $h_2(x) = \mathrm{IFT}[R_2^*(\mu)]$, where superscript $*$ denotes complex conjugation. The amplitude part of the resultant complex distribution can be represented by

$$\phi^{(j)}(x) = \left|\left[\psi(x)p^{(j)}(x)\right] \otimes h_2(x)\right| \tag{3}$$

(iii) Update the guessed object function by smoothing $\varphi^{(j)}(x)$ with a digital low-pass filter.

$$g_1^{(j+1)}(x) = \mathrm{MFilt}\left[\left|\phi^{(j)}(x)\right|\right] \tag{4}$$

where MFilt[] denotes nonlinear operation of 2D median filtering [35].

(iv) Repeat (i)–(iii) until the number of iterations or the correlation coefficient (CC) value between function $g_1^{(j+1)}(x)$ and $g_1(x)$ reaches the preset threshold value. The CC applied to evaluate the similarity between two images $g_1^{(j+1)}(x)$ and $g_1(x)$ is introduced as

$$CC = \frac{E\left\{\left[g_1 - E[g_1]\right]\left[g_1^{(j+1)} - E\left[g_1^{(j+1)}\right]\right]\right\}}{\sqrt{E\left\{\left[g_1 - E[g_1]\right]^2\right\}E\left\{\left[g_1^{(j+1)} - E\left[g_1^{(j+1)}\right]\right]^2\right\}}} \tag{5}$$

where $E[\,]$ denotes the expected value operator.

(v) Suppose the iteration process stop at the Jth iteration. We obtain phase function $p^{(J)}(x)$ from Eq. (2) and then extract sparse encrypted data $S_1(x)$ from $p^{(J)}(x)$ randomly [32–36].

Likewise, another sparse POM $S_2(x)$ can be obtained from the secret image $g_2(x)$, using the same process.

2.2. Image encryption based on optical inference and phase retrieval with sparsity constraint

After obtaining the sparse data using optical DRPE and phase retrieval algorithm with 2D median filtering, we proceed to encode the target image $f(x)$ into authenticable POMs $M_1(x)$ and $M_2(x)$ using optical inference and phase retrieval algorithm with sparsity constraint. For clarity, we first explain the verification and decryption process that can be performed by using the optical setup of linear DRPE shown in Fig. 1 with only minor adjustments. Before being applied for image decryption, the two POMs $M_1(x)$ and $M_2(x)$ should be authenticated in the DRPE scheme. The output images obtained at the CCD plane are respectively given by

$$\psi_1(x) = \left|M_1(x) \otimes h_2(x)\right| \tag{6}$$

$$\psi_2(x) = \left|M_2(x) \otimes h_2(x)\right| \tag{7}$$

which indicate that the conjugate of $R_2(\mu)$ is applied as a decryption key in authentication. The two images $\psi_1(x)$ and $\psi_2(x)$ are respectively compared with their original images, $g_1(x)$ and $g_2(x)$, by nonlinear correlation that is describes as [26–28,32–36]

$$NC(x) = \left|\mathrm{IFT}\left[c(\mu)|c(\mu)|^{\omega-1}\right]\right|^2 \tag{8}$$

where $c(\mu) = \mathrm{FT}[\psi_1(x)]\cdot\left\{\mathrm{FT}[g_1(x)]\right\}^*$ and ω denotes the strength of applied nonlinearity.

Once the two POMs $M_1(x)$ and $M_2(x)$ pass authentication, they are separately placed in the input plane and each is illuminated by a light beam. The two coherent beams are interfered by a beam splitter and then modulated by a decryption phase key $K(\mu)$, which

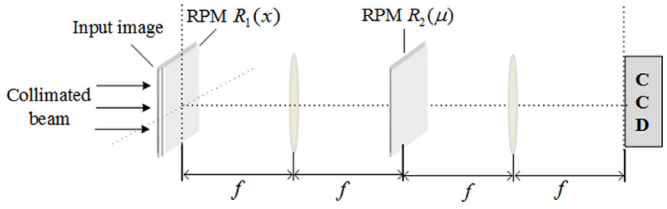

Fig. 1. Schematic setup for information verification without reference beam illuminating at the CCD plane.