Optics Communications 330 (2014) 91–98

Contents lists available at ScienceDirect

Optics Communications

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

Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain

Y. Wang, C. Quan *, C.J. Tay

Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 25 March 2014
Received in revised form
8 May 2014
Accepted 14 May 2014
Available online 27 May 2014

Keywords:
Multiple-image encryption
Mixture retrieval algorithm
Fresnel transform (FrT)

ABSTRACT

We propose a novel nonlinear multiple-image encryption based on mixture retrieval algorithm and phase mask multiplexing in Fresnel domain. The encryption process is realized by applying the Yang–Gu algorithm cascaded with a modified Gerchberg–Saxton algorithm (MGSA), which generate a private key and an intermediate phase to ensure high security. In the proposed method, all images are encoded separately into a phase only function (POF). Obtained POFs are integrated into a final POF based on phase mask multiplexing. As a result, cross-talk noise is removed resulting in a large improvement of the encryption capacity. A spatial light modulator (SLM) based optical setup has been suggested for decryption. Numerical simulations are presented to demonstrate the feasibility and effectiveness of the proposed system. Results also indicate the high robustness of the system against occlusion and noise attacks.

1. Introduction

Information security based on optical technologies is becoming increasingly important. It has attracted considerable attention in the last few decades due to high-speed and multidimensional capabilities of optical signal processing [1–6]. Among the technologies, double random phase encoding (DRPE), in which an input image can be encoded into a stationary white noise using two random phase masks located at the input and the Fourier plane, is the most widely used [7]. Different encoding domains, such as fractional Fourier transform (FrFT) [8] and Fresnel transform (FrT) [9], have been developed to increase the security. However, because of the inherent linearity of DRPE, these schemes have been found to be vulnerable to various attacks [10–14]. To overcome the linearity problem, asymmetric cryptosystems based on phase-truncated Fourier transform have been proposed [15–17]. However, a special attack would allow an attacker to reveal the encrypted information using a two-step iterative amplitude-phase retrieval algorithm [18]. Recently, Liu et al. [19] proposed a security-enhanced asymmetric cryptosystem based on the Yang–Gu mixture amplitude-phase retrieval algorithm, in which the public and private key structures are redesigned in a more complicated pattern.

Multiple-image encryptions have also received wide attention since Situ and Zhang proposed multiple-image encryption using wavelength and position multiplexing [20,21]. Further, various approaches, such as multi-channeled encryption [22], interference-based position multiplexing [23], and lateral shifting [24,25] have been proposed. These techniques normally encounter cross-talk noise problem since the encrypted image is recorded on a single medium by direct superposition. Hence the methods are limited to binary images and with limited storage capacity. To overcome the cross-talk problem, many methods based on phase retrieval algorithms have been proposed for multiple-image encryption. Hwang et al. [26] developed a multiple-image encryption with wavelength multiplexing based on modified Gerchberg–Saxton algorithm (MGSA) and phase modulation. Chang et al. [27,28] proposed wavelength and position multiplexing encryption using MGSA and two cascaded phase-only masks. In the methods, cross-talk noise is reduced significantly, but at the cost of a reduction in the size of encrypted image due to the size limitation of output plane.

In this paper, we propose a novel nonlinear multiple-image encryption based on mixture retrieval algorithm and phase mask multiplexing in Fresnel domain. The study presents a security-enhanced nonlinear cryptosystem for multiple-image encryption based on amplitude and phase modulation. With the proposed method, the cross-talk problem normally present in multiple-image encryption can be avoided. A simple optical setup for decryption has been suggested, in which two SLMs can be used to display the two decryption keys. Numerical experimental results are presented to demonstrate the feasibility and robustness of the proposed multiple-image encryption method.

* Corresponding author. Tel.: +65 65168089; fax: +65 67791459.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

http://dx.doi.org/10.1016/j.optcom.2014.05.032
0030-4018/

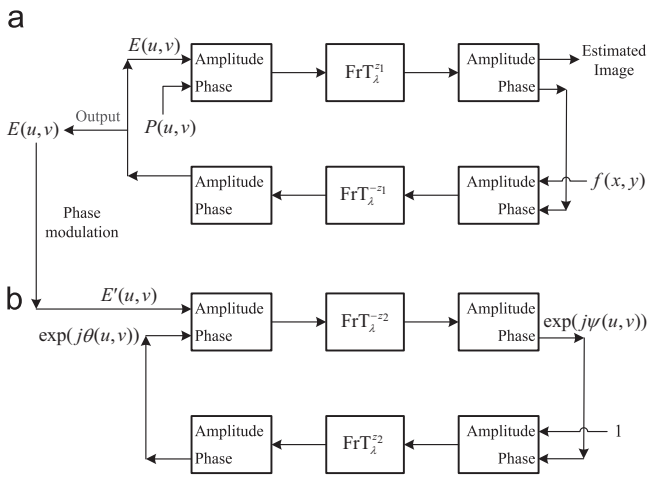

Fig. 1. (a) Yang–Gu algorithm in Fresnel domain and (b) MGSA in Fresnel domain.

2. Principle of method

In the proposed method, an image is first encrypted with the Yang–Gu amplitude-phase retrieval algorithm [19,29]. The Yang–Gu algorithm can be expressed as an iterative process shown in Fig. 1(a), in which $f(x,y)$ represents the amplitude of an image to be encrypted, $P(u,v)$ represents a public random phase key, and $E(u,v)$ represents an unknown amplitude. In the iterative process, $E(u,v)$ is first initialized to $E_0(u,v)$ by a random generation in $[0,1]$. $f(x,y)$ and $P(u,v)$ are the constraints used for updating the amplitude and phase, respectively. The following describes the procedure shown in Fig. 1(a):

1. Initial $E_0(u,v)$ is first multiplied by a public random phase key $P(u,v)$. At the mth iteration, the complex function $E'_m(u,v)$ is given by:
$$E'_m(u,v) = |E_m(u,v)| \times \exp[jP(u,v)]. \tag{1}$$

2. A Fresnel transform FrT is performed on the complex function $E'_m(u,v)$, with a free space propagation distance z_1:
$$\begin{aligned} F_m(x,y) &= \mathrm{FrT}_\lambda^{z_1}[E'_m(u,v)] \\ &= \frac{\exp\left\{\frac{j2\pi z_1}{\lambda}\right\}}{j\lambda z_1}\iint E'_m(u,v) \\ &\quad \times \exp\left[\frac{j\pi}{\lambda z_1}((x-u)^2+(y-v)^2)\right]dxdy \\ &= |F_m(x,y)| \times \exp\{j\varphi_m(x,y)\}. \end{aligned} \tag{2}$$

3. The amplitude in Eq. (2) is replaced by the amplitude of the image to be encrypted
$$F'_m(x,y) = f(x,y) \times \exp\{j\varphi_m(x,y)\}. \tag{3}$$

4. An inverse FrT is performed on $F'_m(x,y)$:
$$F''_m(u,v) = \mathrm{FrT}_\lambda^{-z_1}[F'_m(x,y)] = |F''_m(u,v)| \times \exp\{j\varphi'_m(u,v)\} \tag{4}$$

5. The phase in Eq. (4) is replaced by $P(u,v)$:
$$E'_{m+1}(u,v) = |F''_m(u,v)| \times \exp[jP(u,v)] = |E_{m+1}(u,v)| \times \exp[jP(u,v)]. \tag{5}$$

The number of iterations employed is determined by a correlation coefficient (CC) between $f(x,y)$ and $|F_m(x,y)|$. The CC value is used as a convergent criterion, which is defined as
$$\mathrm{CC} = \frac{\mathrm{cov}(f(x,y), |F_m(x,y)|)}{\sigma_{f(x,y)} \cdot \sigma_{|F_m(x,y)|}} \tag{6}$$
where $\mathrm{cov}(f(x,y), |F_m(x,y)|)$ denotes the cross-covariance and σ denotes the standard deviation.

The final retrieved amplitude $E(u,v)$ contains both positive and negative values. In order to obtain the actual amplitude, an amplitude modulator that contains -1 or 1 element should be used. However, in an actual experiment a spatial light modulator (SLM) cannot display a negative value. Hence instead of an amplitude modulation a one-way binary phase modulation $\exp[j\pi\gamma(u,v)]$ is introduced. The private modulation $\gamma(u,v)$ is generated by
$$\gamma(u,v) = \begin{cases} 1 & E(u,v) < 0 \\ 0 & E(u,v) > 0 \end{cases} \tag{7}$$
and the amplitude combined with the one-way binary phase modulation is given by
$$E'(u,v) = E(u,v)exp[j\pi\gamma(u,v)]. \tag{8}$$
The decryption key in the Yang–Gu algorithm is generated by performing the private binary modulation to the public key, as follows:
$$d(u,v) = \exp[jP(u,v)]exp[j\pi\gamma(u,v)]. \tag{9}$$

Through the Yang–Gu algorithm, an image $f(x,y)$ is encrypted into the modulated amplitude $E'(u,v)$. In order to convert $E'(u,v)$ into a POF, a MGSA process is applied [26,30]. The modulated amplitude $E'(u,v)$ obtained from the Yang–Gu algorithm is used as an input for the MGSA process (shown in Fig. 1(b)), which is described as follows:

1. Amplitude $E'(u,v)$ is multiplied by an arbitrary RPM exp $\{j\theta(u,v)\}$. At the nth iteration the complex function $G'_n(u,v)$ is given by
$$G'_n(u,v) = E'(u,v) \times \exp\{j\theta_n(u,v)\}. \tag{10}$$

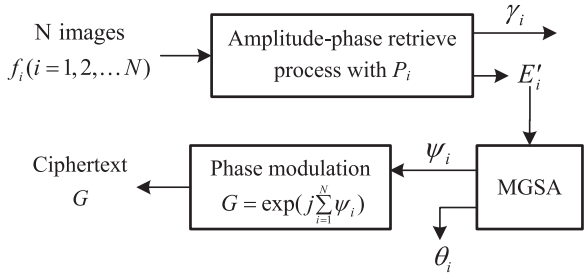

Fig. 2. Proposed multiple-image encryption processes.

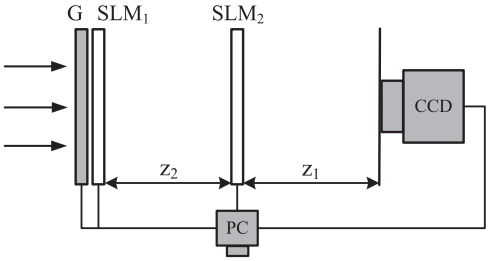

Fig. 3. Optical implementation for decryption. SLM1 and SLM2 (spatial light modulators); CCD (charge-coupled device camera); z_1 and z_2 (Fresnel propagation distances).