Optics and Lasers in Engineering 51 (2013) 410–416

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Optical cryptography network topology based on 2D-to-3D conversion and phase-mask extraction

Wen Chen *, Xudong Chen

Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 14 September 2012
Received in revised form
19 October 2012
Accepted 27 November 2012
Available online 27 December 2012

Keywords:
Optical cryptography
Network topology
2D-to-3D conversion
Phase retrieval

ABSTRACT

In recent years, high-security physical architectures are desirable for data storage and transmission networks. In this paper, we propose optical cryptography network topology based on 2D-to-3D conversion and phase-mask extraction. Two different phase retrieval algorithms are applied in the designed optical cryptography network topologies. These topological architectures can be interconnected to constitute many complex optical cryptography networks, and the plaintext can be fully encrypted into phase-only masks based on any one optical encryption strategy selected from the cryptography network. The results and analyses demonstrate that the proposed optical cryptography network topologies possess high security, and a new research perspective may be opened up for optical image encryption.

1. Introduction

The scattering induced by irradiation is widely employed as a means to record specimen information in the optical imaging. Since phase distribution is directly related to the measured physical parameters [1,2], phase retrieval has become one of the most important research topics. There are two major approaches for extracting phase distributions, i.e., interferometric imaging [1–3] and noninterferometric imaging [4,5]. In the interferometric imaging object wave interferes with the reference wave under the same recording conditions [1,2], and phase distributions can be extracted from the recorded interference pattern by using some retrieval algorithms, such as phase-shifting algorithm [1]. Recently, noninterferometric imaging [4–14], such as multiple-exposure recordings [8,10–14], has become a promising alternative instead of interferometric imaging [1–3]. In the noninterferometric imaging, the phase extraction process can be stated as inverse problem, which is usually implemented by using an iterative algorithm between real and reciprocal spaces. Combined with X-ray light source, the noninterferometric imaging can achieve atomic-scale resolution [6].

In recent years, optical cryptography [15–21], such as double random phase encoding [15–17], has attracted more and more attention in the information security field, and phase retrieval algorithms [1–14,22–28] have been studied for optical cryptography. The Gerchberg–Saxton algorithm [22] is considered as an important phase retrieval technology, which has been widely applied for optical image encryption. A plaintext (such as image) can be iteratively encoded into single or multiple phase-only masks, and the phase retrieval algorithm can also be combined with phase modulation strategies for multiple-image encryption [27]. Zhang and Wang [29] further developed a non-iterative phase retrieval algorithm based on interference for optical image encryption. However, the methods aforementioned [24–29] are restricted to two-dimensional (2D) domain, and cryptosystem security could be limited. In addition, an optical cryptography network based on phase retrieval has not been established in three-dimensional (3D) space. In this paper, we propose optical cryptography network topology based on 2D-to-3D conversion and phase-mask extraction. The designed topological architectures can be interconnected to constitute many complex phase-retrieval-based optical cryptography networks, and the plaintext can be fully encrypted into phase-only masks based on any optical encryption strategy selected from the proposed optical cryptography networks.

This paper is organized as follows: in Section 2, we introduce the proposed cryptography network topology and then explain a typical encryption strategy selected from the designed optical cryptography network topologies. In Section 3, results for the selected encryption strategy are presented and high security of the developed optical encryption system is illustrated. Finally, in Section 4, we draw the conclusions for our work.

2. Theoretical analysis

Fig. 1(a–d) shows several types of the proposed cryptography topological architectures. Two different phase retrieval algorithms,

* Corresponding author. Tel.: +65 65166855; fax: +65 67791103.
E-mail address: elechenw@nus.edu.sg (W. Chen).

0143-8166/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2012.11.013

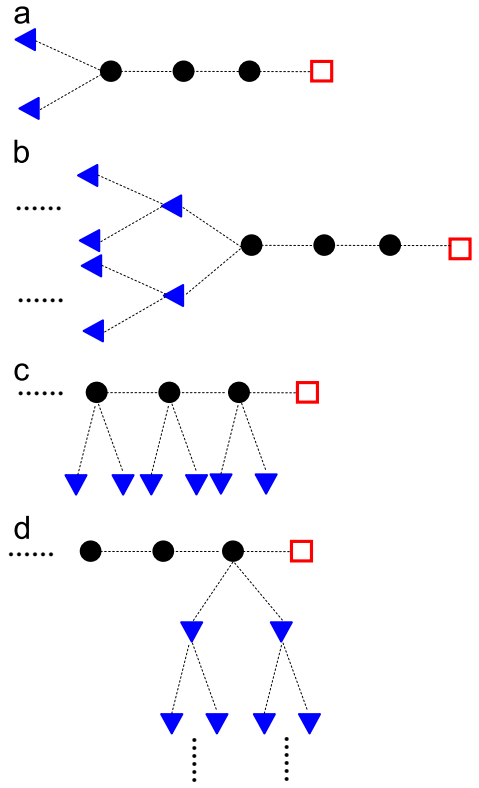

Fig. 1. (a–d) Different types of optical cryptography topological architectures. The "circular" symbols denote phase-only masks extracted at the first encryption stage. The "triangular" symbols denote phase-only masks extracted at the second encryption stage. The "rectangular" symbols denote 3D particle distributions (i.e., the plaintext).

i.e., iterative and non-iterative phase retrieval algorithms, are simultaneously applied in each optical cryptography topology. It can be seen in Fig. 1(a–d) that various encoding paths can be designed in the proposed optical cryptography topology. These topological architectures (such as star and tree structures) can be interconnected to establish many complex optical cryptography networks. An administrator with high-level authority can select any optical encryption strategy from the designed network topologies, and different ciphertexts can be generated for the different authorized receivers. Hence, the plaintext cannot be extracted from ciphertexts without knowledge about the selected optical encryption strategy and encoding path.

We analyze one typical encryption strategy selected from the proposed cryptography network topologies, and Fig. 2 shows the schematic optical experimental setup corresponding to Fig. 1(b). Two different phase retrieval algorithms are sequentially applied in the selected optical encryption strategy. At the first encryption stage, an iterative phase retrieval algorithm is developed to encrypt the plaintext into phase-only masks M1–M3. Several neighboring pixels (such as 16×16 pixels) of the 2D plaintext are combined as one particle, and the plaintext is divided into a series of particles distributed in 3D space without transverse and longitudinal superposition. It is worth noting that the 3D particle distribution (i.e., plaintext) can be encrypted into more phase-only masks rather than just masks M1–M3 at the first encryption stage. At the second encryption stage, one of the phase-only masks extracted at the first encryption stage (i.e., M1) is embedded into phase-only masks M4 and M5 based on non-iterative phase retrieval algorithm with interference principle, and similarly the extracted phase-only mask M5 is further encoded into masks M6 and M7 with interference principle (see Fig. 2).

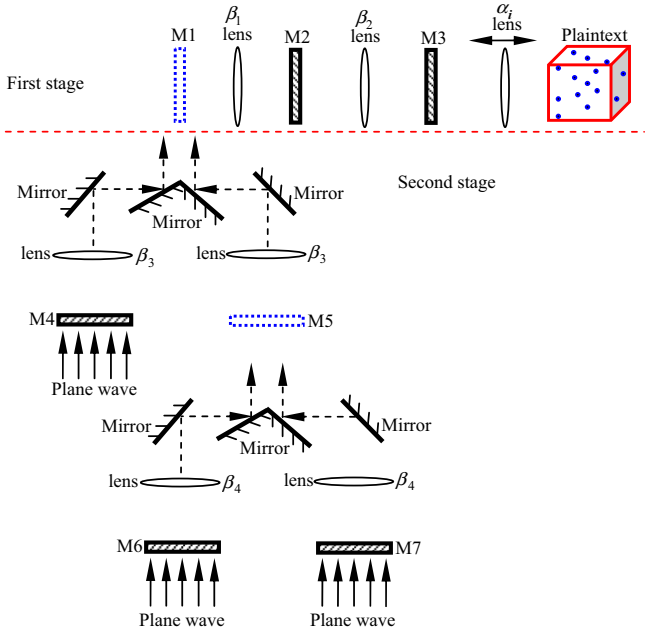

Fig. 2. A schematic experimental setup for one typical optical encryption strategy selected from the proposed optical cryptography network topologies: M, the extracted phase-only masks. A cube beam splitter can be used for combing the two waves at the second encryption stage, and lens parameters, such as lens position (indicated by double-arrow line), are sequentially adjusted to ensure that each particle is located in the specific FrFT domain.

The fractional Fourier transform (FrFT) is applied to describe wave propagation at all intervals in Fig. 2, and the wave propagation process between phase-only masks M1 and M2 can be described by [30–32]

$$\mathrm{FrFT}_{\beta_1}[\mathrm{M}_1(x_1)] = \int_{-\infty}^{+\infty} \mathrm{M}_1(x_1) Q_{\beta_1}(x_2,x_1)\,dx_1 \tag{1}$$

where

$$Q_{\beta_1}(x_2,x_1) = \begin{cases} R\exp\{j\pi[x_2^2\cot(\beta_1\pi/2) + x_1^2\cot(\beta_1\pi/2) - 2x_2x_1\csc(\beta_1\pi/2)]\} & \text{if } \beta_1 \neq 2m \\ \delta(x_2 - x_1) & \text{if } \beta_1 = 4m \\ \delta(x_2 + x_1) & \text{if } \beta_1 = 4m \pm 2 \end{cases},$$

m denotes an integer, $j=\sqrt{-1}$, $\mathrm{M}_1(x_1)$ denotes phase-only mask M1 extracted at the first encryption stage, β_1 is the FrFT function order, and $R=\sqrt{1-j\cot(\pi\beta_1/2)}$ For the sake of brevity only one-dimensional FrFT is described, and the description of 2D FrFT [30–32] is straightforward. Similarly, wave propagation processes at other intervals can also be described by Eq. (1). The lens parameters, such as lens position, are sequentially adjusted to ensure that each particle is located in the specific FrFT domain, and a series of FrFT function orders α_i (see Fig. 2) can be correspondingly generated. At the first encryption stage, the objective of the iterative phase retrieval algorithm is to extract phase-only masks M1–M3 under the given constraints, such as 3D particle distributions. The iterative phase retrieval algorithm proceeds as follows:

$$O^{(i,n)}(\mu,\nu) = \mathrm{FrFT}_{\alpha_i}\{[\mathrm{FrFT}_{\beta_2}(\{\mathrm{FrFT}_{\beta_1}[\mathrm{M}_1^{(i,n)}(x_1,y_1)]\}\mathrm{M}_2^{(i,n)}(x_2,y_2))]\mathrm{M}_3^{(i,n)}(x_3,y_3)\}, \tag{2}$$

$$\overline{O^{(i,n)}(\mu,\nu)} = \mathrm{Cons}[O^{(i,n)}(\mu,\nu)], \tag{3}$$

$$\overline{\mathrm{M}_3^{(i,n)}(x_3,y_3)} = \mathrm{USC}\left\{\frac{\mathrm{FrFT}_{-\alpha_i}[\overline{O^{(i,n)}(\mu,\nu)}]}{\mathrm{FrFT}_{\beta_2}\left(\{\mathrm{FrFT}_{\beta_1}[\mathrm{M}_1^{(i,n)}(x_1,y_1)]\}\mathrm{M}_2^{(i,n)}(x_2,y_2)\right)}\right\}, \tag{4}$$