Optics & Laser Technology 49 (2013) 108–117

Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

Cryptographic analysis on the key space of optical phase encryption algorithm based on the design of discrete random phase mask

Chao Lin*, Xueju Shen, Zengyan Li

Department of Opto-electronic Engineering, Shijiazhuang Mechanical Engineering College, Heping West Road No 97, Shijiazhuang 050003, PR China

ARTICLE INFO

Article history:
Received 1 October 2012
Received in revised form
14 December 2012
Accepted 15 December 2012
Available online 24 January 2013

Keywords:
Random phase encoding
Block cipher
Key space

ABSTRACT

The key space of phase encryption algorithm using discrete random phase mask is investigated by numerical simulation in this paper. Random phase mask with finite and discrete phase levels is considered as the core component in most practical optical encryption architectures. The key space analysis is based on the design criteria of discrete random phase mask. The role of random amplitude mask and random phase mask in optical encryption system is identified from the perspective of confusion and diffusion. The properties of discrete random phase mask in a practical double random phase encoding scheme working in both amplitude encoding (AE) and phase encoding (PE) modes are comparably analyzed. The key space of random phase encryption algorithm is evaluated considering both the encryption quality and the brute-force attack resistibility. A method for enlarging the key space of phase encryption algorithm is also proposed to enhance the security of optical phase encryption techniques.

1. Introduction

Optical encryption has become candidate as a promising technique for coping with increasingly complicated information security environment due to its intrinsic high-speed parallel processing and multiple encryption freedom properties. Though various optical encryption architectures have been constructed and claimed to be of high security level [1–10], the classical double random phase encoding (DRPE) approach [1] is still attractive to researchers. The resistances of double random phase encryption technique under chosen-cyphertext [11], known-plaintext attacks [12,13], and chosen-plaintext [14] have been investigated in recent years. These remarkable researches reveal the security flaw of DRPE technique originated from the linearity of 4-f system. Dedicating to enhance the attack immunity of optical encryption scheme, many efforts have been taken by introducing nonlinear property into optical encryption system to construct nonlinear and asymmetric optical encryption architecture [15].

Besides the attack free performance, a practical cryptosystem must endure the statistical analysis and brute-force attack efficiently [16]. In conventional cryptography, it has been recognized that attackers can analyze the cyphertext to obtain certain system properties by statistical analysis in principle. The high-performance computing devices are also widely accessible for an attacker with which one can make acceptable time-consuming trials on probing the key space of any cryptosystem to obtain exact or approximate decryption keys within tolerant decryption errors. So, the encryption quality and key space of a cryptosystem should also be reasonably evaluated to claim the statistical analysis free and brute-force attack free performances.

DRPE technique has gained wide interests in analyzing the system behaviors in encryption and decryption process [17–21]. The influence of perturbation [22], shift-tolerance property [23] and statistical performance [24] has all been investigated to show the substantial properties of DRPE system. The error analysis of decryption random phase mask is also presented by performing perfect encryption and imperfect decryption [25]. Monaghan el al. investigated the robustness of DRPE technique to brute-force attack assuming that insights gained by fully mapping small key-space can be extrapolated to large key-spaces [26]. But the performance of encryption process in DRPE technique is not fully considered in their work, so the conclusions about the key-space of DRPE technique are not comprehensive enough. Compared with these works discussing the decryption error, encryption process, statistical property and key space, this paper focuses on the brute-force attack resistibility considering both the quality of encrypted image and blind searching resistibility which can provide an all-sided evaluation on optical phase encryption algorithm. Under a practical environment, the discrete and finite phase values that the spatial light modulator (SLM) can control or display may limits the randomization level of cypher image and

* Corresponding author. Tel.: +8613603392084; fax: +86031187994222.
E-mail address: vestigelinchao@163.com (C. Lin).

0030-3992/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2012.12.022

the key-space of the cryptosystem [27–29]. What is more, we believe that optical encryption system requires a larger key space than conventional mathematical and electronic based encryption system because the attacker can perform a blind searching for the right decryption key using optical processors with high speed too. In this practical environment, if the key space of an optical encryption system is smaller than digital encryption system, the resistibility of optical encryption system under brute force attack may become a big security flaw. The intrinsic high speed of light is beneficial for not only the authorized users but also the unauthorized attackers. So, the key space of optical encryption algorithms must be thoroughly analyzed to claim the brute force attack resistibility. In this paper, from the cryptography point of view, the relationship between the quality of encrypted image and brute-force attack property utilizing discrete random phase mask is first demonstrated to exhibit the comprehensive performance of phase encryption technique. The confusion and diffusion property of optical phase encryption technique is also presented which clarifies the statistical characteristic of phase encryption algorithm. The key space and confusion–diffusion analysis on optical phase encryption algorithm can be combined together to become a useful tool when designing new optical encryption system.

This paper is organized as follows. In Section 2, some basic theory about classical double random phase encryption (DRPE) technique under amplitude encoding and phase encoding modes and the error metric are presented. In Section 3, we introduce the block cypher design criteria in conventional cryptography theory to evaluate the optical random phase encryption technique by performing a qualitative analysis. The numerical simulation results of key space utilizing discrete random phase masks in amplitude encoding and phase encoding modes are shown in Sections 4 and 5. Concluding remark is outlined in the final section.

2. Basic theory and evaluation criterion

2.1. Review of amplitude-based and phase-based DRPE techniques

As depicted in Fig. 1, the encryption procedure can be described as follows when performing amplitude encoding double random phase encryption technique [1]. Input image is sampled to have $N \times N$ pixels. Let x and y denote the spatial coordinates, u and v denote the coordinates in the Fourier plane. Let $f(x,y)$ denotes the plaintext to be encrypted normalized into [0, 1]. The input random phase key and Fourier plane random phase key are generated independently by two white noise sequences $a(x,y)$ and $b(u,v)$ uniformly distributed in the interval of [0, 1]. Then following the DRPE architecture, the cypher image can be deduced as follows in Eq. (1):

$$\varphi_A(x,y) = \Im^{-1}\{\Im\{f(x,y)\exp[i2\pi a(x,y)]\}\exp[i2\pi b(u,v)]\} \quad (1)$$

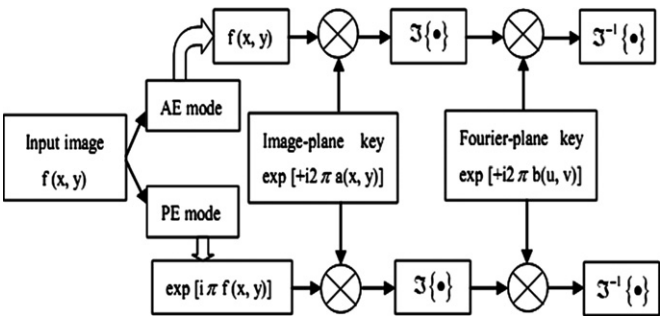

Fig. 1. Block diagram of amplitude-based and phase-only DRPE technique.

where $\Im$ and $\Im^{-1}$ are the Fourier and inverse Fourier transforms, respectively, $\varphi_A(x,y)$ denotes the cypher image for amplitude encoding. The decryption procedure is the inverse operation of the encryption process in which the phase conjugation of the encryption phase mask is utilized to compensate the random phase modulation in the Fourier and spatial planes.

The block diagram in Fig. 1 simultaneously demonstrates the encryption procedure when performing phase encoding DRPE technique. The only difference with amplitude-based DRPE technique is that the original image is encoded to be as a phase-only function [30]. The encrypted result is given by:

$$\varphi_P(x,y) = \Im^{-1}\{\Im\{\exp[i\pi f(x,y)]\exp[i2\pi a(x,y)]\}\exp[i2\pi b(u,v)]\} \quad (2)$$

In the decryption process of phase-only DRPE technique, the spatial random phase mask is essential to recover the original image. Extracting the phase of $\exp[i\pi f(x,y)]$, and dividing by π is necessary to completely recover the plaintext. The range of phase encoded image is assumed as [0, π] in Eq. (2), so that no ambiguity will occur when deciding what angle the phase would be.

2.2. Error metric

The metric we introduce in order to quantify both the difference between plaintext and cyphertext and the error between the decrypted plaintext and original plaintext is the correlation coefficient (CC). The correlation coefficient in the integral form is defined as:

$$cc = \frac{\iint |f(x,y)||\varphi(x,y)|dxdy}{\sqrt{\iint |f(x,y)|^2 dxdy}\sqrt{\iint |\varphi(x,y)|^2 dxdy}}. \quad (3)$$

In which $f(x,y)$ denotes the original image and $\varphi(x,y)$ denotes the decrypted image or the encrypted image. When the encryption quality is poor, the correlation coefficient value is relatively high.

In the whole numerical simulation procedure, the physical model issues are neglected. The fill factor and high diffraction order of spatial light modulator, the resolution and imaging size of CCD camera are also unconsidered. Although the ignorance of the above factors, simulation results can be claimed to be convincing because this study reveals the nature of DRPE technique which is not dependent on these practical physical limiting factors.

3. Block cipher analysis on DRPE technique

In this section, the modern block cipher theory is introduced to present a qualitative analysis on the DRPE technique in order to identify the role of random phase mask in optical encryption scheme.

3.1. Block cipher theory

The product cipher is a complex cipher combining substitution, permutation, and other components. Two important properties are accompanied with this concept: diffusion and confusion. The diffusion operation aims to hide the relationship between the cyphertext and plaintext. This will frustrate the adversary who exercises cyphertext statistics to find the plaintext. Diffusion implies that each symbol in the cyphertext is dependent on some or all symbols in the plaintext. The goal of confusion is to hide the relationship between cyphertext and the encryption key. This will defeat an attacker who tries to analyze the cyphertext to find the key [16].