Optics Communications 418 (2018) 106–114

Contents lists available at ScienceDirect

Optics Communications

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

Security enhancement of double random phase encryption with a hidden key against ciphertext only attack

Shuming Jiao, Zhaoyong Zhuang, Changyuan Zhou, Wenbin Zou *, Xia Li

Shenzhen Key Lab of Advanced Telecommunication and Information Processing, College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China

ARTICLE INFO

Keywords:
Optical encryption
Double random phase encoding
Ciphertext only attack
Security enhancement

ABSTRACT

In this paper, we propose a security enhanced double random phase encoding (DRPE) encryption system against common ciphertext only attacks (COA). We point out one common weakness of COA schemes that the cracked plaintext image is usually in wrong circularly shifting positions and flipping status. Regarding to this weakness, an extra security layer (either optical or digital) cascaded with the DRPE system is constructed using a hidden key in our work. Simulation results demonstrate that our proposed system has significantly better security strength against COA than conventional DRPE system.

1. Introduction

The research of optical information security has attracted increasingly more attention in the past decade. Optical systems are extensively employed in information encryption [1–33], information authentication [34–38] and information hiding [39–43]. In optical security, the information is processed optically rather than digitally, with advantages of multiple dimensions, high parallelity and high processing speed. Double random phase encoding (DRPE) system [1] is the first attempt of using optical systems for information encryption, proposed by in 1995. DRPE can be implemented in the object image domain and Fourier transformed domain of a $4f$ optical lens system. The concept of DRPE has been extended to fractional Fourier domain [2], Fresnel domain [3], and photo counting technology area [35] as well. In addition to DRPE, optical encryption systems with other configurations are extensively investigated such as joint transform correlator [5], ghost imaging [6] and ptychography [7]. Despite the success, some common difficulties and challenges remain to be tackled in optical encryption such as the noise contamination problem in decrypted results, which can be possibly eliminated by phase coding [8], error correction coding [9–11] and spatial pixel separation [12,13]. Another fundamental and challenging issue in optical encryption research is the difficulty of real optical implementation as many early works only provide computer simulation results. In recent years, numerous real optical encryption experiments are conducted such as encryption by interference [14], joint transform correlator systems [15–17], computer-generated hologram [18,19], spatially incoherent illumination systems [20,21], spiral phase mask [22], optical scanning holography [23] and microscopic integral imaging [24]. It is an emerging trend that optical encryption systems are gradually evolving from theoretical models to practical implementations.

For any information encryption system (either based on digital algorithm or based on optical system), its security strength is always the foremost concern. To enhance the security strength, possible security flaws of a given optical encryption system are investigated and attacking algorithms are proposed to crack the system. Then the optical encryption system can be improved regarding to the weakness revealed by the attacking schemes. The improved system can be possibly further cracked by new attacking methods. It is an iterative cycle between new attacking methods and new security enhancement schemes in the development of security systems. For DRPE system, attacking methods including known plaintext attack [44–46], chosen plaintext attack [47,48], chosen ciphertext attack [28,48] and ciphertext-only attack (COA) schemes [49–53] have been proposed in the past. Among these attacking methods [44–54], COA reveals the most severe security flaw of a DRPE system since it can illegally recover the plaintext from the ciphertext information alone. The security strength of DRPE has to be enhanced against these COA schemes. However, up to now, very little anti-COA work has been conducted.

In this paper, we notice that the phase retrieval step in common COA algorithms [49–53] has a limitation that only the plaintext content can be disclosed but the circularly shifting position and flipping status are usually incorrect. In our proposed security enhanced DRPE system, the circularly translational shift and flipping status of DRPE input is employed to generate a hidden key and one extra encryption layer based on this hidden key is constructed between the original plaintext and the

* Corresponding author.
E-mail address: wzouszu@sina.com (W. Zou).

https://doi.org/10.1016/j.optcom.2018.02.064
Received 23 December 2017; Received in revised form 22 February 2018; Accepted 26 February 2018

DRPE system. In this way, the existing COA methods will fail to crack our system and the security strength of original DRPE system is significantly enhanced.

In previous works, the security enhancement of DRPE systems has been investigated from different perspectives. A common approach to enhance the system security is to incorporate more dimensions and parameters in the key space including Fractional Fourier transform orders [3], propagation distance in Fresnel domain [4], amplitude modulation [25], permutation key [26], polarization [27], shifting of random phase mask [28], modular arithmetic [29] and combination of multiple keys [30]. Asymmetric phase truncation operation [31,32] is another possible way of enhancing the security of a DRPE system. In addition, a security enhancement strategy in DRPE is recently proposed by multiplexing the ciphertext with another 'salt' ciphertext [33]. These existing works all can enhance the DRPE system security to certain extent and some of them are supported by both simulation and experiment results [3,27–29,33]. However, our proposed scheme in this paper differs from previous works with two features: (1) our security enhancement scheme is designed specifically addressing the flaws of recently proposed COA attack schemes [49–53]; and (2) the security enhancement is achieved using a hidden key without introducing any additional explicit key in this paper while extra keys in addition to the two random phase masks are generally required in previous works.

This paper is organized as follows. In Section 2, the DRPE optical encryption system and corresponding COA schemes are briefly reviewed. The weakness and limitation of common COA methods are analyzed. In Section 3, our proposed security enhanced DRPE system model is presented and one example of system implementation with XOR encryption is reported. In Section 4, simulation results demonstrate the outperformance of our proposed system over conventional DRPE systems in terms of security strength against COA attacks. In Section 5, a brief conclusion is provided.

2. DRPE system and ciphertext only attack (COA) methods

The optical setup of a DRPE system [1] is illustrated in Fig. 1. In DRPE, the plaintext image $f(x, y)$ is multiplied with the first random phase only mask $\exp(j2\pi\Psi(x, y))$ and then Fourier transformed by the first lens optically. After that, the light field is multiplied with the second random phase mask $\exp(j2\pi\Phi(x, y))$, described by Eq. (1). Then the light field is inversely Fourier transformed by the second lens and an encrypted light field can be obtained as the ciphertext $q(x, y)$. By knowing the two random phase mask keys (at least the second random phase mask key), the plaintext image can be decrypted from the ciphertext as $f'(x, y)$ with a decryption optical setup similar to the encryption one, shown in Fig. 1(b) and Eq. (2).

$$q(x, y) = IFT\left\{FT\left[f(x, y)\exp(j2\pi\Psi(x, y))\right] exp(j2\pi\Phi(u, v))\right\} \quad (1)$$

$$f'(x, y) = |IFT\{FT[q(x, y)] exp(-j2\pi\Phi(u, v))\} exp(-j2\pi\Psi(x, y))|. \quad (2)$$

The DRPE optical system can convert a plaintext image into a ciphertext. An incorrect noisy decrypted result will be obtained if the ciphertext is decrypted with wrong keys. However, attacking methods [44–54] can possibly recover the plaintext without knowing correct keys thus the security of DRPE encryption system is challenged. Among these attacking methods, COA methods [49–53] can crack the system by recovering the plaintext image from only the ciphertext. For DRPE system, a Fourier spectrum magnitude relationship between plaintext image and ciphertext is often employed for designing COA algorithms. In DRPE, the Fourier spectrum magnitude of the ciphertext $q(x, y)$ is equal to the Fourier spectrum magnitude of the random phase mask modulated plaintext (i.e. $f(x, y)\exp(j2\pi p(x, y))$). This relationship (denoted by Eq. (3)) can be derived from Eqs. (1) and (2).

$$Q(u, v) = |FT[q(x, y)]| = |FT\left[f(x, y)\exp(j2\pi\Psi(x, y))\right]|. \quad (3)$$

Based on this relationship plus other constraint conditions, the plaintext image $f(x, y)$ can be possibly retrieved from $q(x, y)$ (or equivalently $Q(u, v)$) by iterative phase retrieval algorithms [49–53]. Additional assumptions such as tight and sharp object shape support [49] or small number of non-zero pixels [50] are imposed on the plaintext image to ensure the phase retrieval process can converge and find correct plaintext image $f(x, y)$ and random phase mask $\Psi(x, y)$. Alternatively in [51], speckle correlation is performed first to acquire the Fourier spectrum magnitude $F(u, v)$ (Eq. (4)) of original plaintext image (without multiplication of the random phase mask) from $Q(u, v)$. Then phase retrieval is performed in the second stage to extract plaintext image $f(x, y)$ from the acquired $F(u, v)$.

$$F(u, v) = |FT[f(x, y)]|. \quad (4)$$

Despite the success, the existing COA schemes [49–53] usually can only work when certain constraints on the plaintext image are valid. For example, the method [49] requires the plaintext object to be in regular geometric shape, the method [50] requires the majority part of the plaintext image is zero intensity and the method [51] requires the image size (number of pixels) of plaintext image is sufficiently large.

If these conditions are not satisfied, the attacking algorithms may fail to work. Furthermore, another inherent drawback of these methods lies in the shifting and flipping property of Fourier transform, shown in Eqs. (5) and (6).

$$|FT[f(x, y)]| = |FT\left[f\left(x - x_0, y - y_0\right)\right]| \quad (5)$$

$$|FT[f(x, y)]| = |FT[f(-x, -y)]|. \quad (6)$$

For an arbitrary intensity image $f(x, y)$, if it is circularly shifted in horizontal and (or) vertical directions with a random distance (denoted by (x_0, y_0) in Eq. (5)), and (or) flipped (Eq. (6)), the frequency spectrum magnitude after Fourier transform remains the same as that of original. For example, in Fig. 2, the Fourier spectrum magnitudes of the three images are equal. As a consequence, it is impossible to derive the circularly shifting position and flipping status of true plaintext image from only $F(u, v)$ or $Q(u, v)$ by any phase retrieval algorithms. The COA schemes are not capable of disclosing the correct circularly shifting position and flipping status of plaintext from only the ciphertext. This common weakness can be utilized to enhance the security of a DRPE system against COA. In this paper, a security enhancement scheme for DRPE system using a hidden key is proposed.

3. Proposed security enhancement scheme for DRPE system with a hidden key

3.1. Model and structure of proposed security enhanced DRPE system

The general model and structure of our proposed security enhanced DRPE system is presented in Fig. 3.

In our proposed scheme, one extra symmetrical encryption system is cascaded with the DRPE system. The original plaintext is first encrypted by this extra encryption layer before DRPE encryption. It shall be noted that there is no special requirement on this extra encryption system and it can be an arbitrary symmetrical optical or digital encryption system. In this paper, a simple XOR (Exclusive OR) digital encryption system is adopted.

The encrypted result from this extra system (primary ciphertext) is circularly translationally shifted by certain distance (x_0, y_0) and possibly flipped and then employed as the input intensity image (plaintext) to a DRPE system. The shifting distance (x_0, y_0) and flipping status ($fp = 0$ or 1; 0: not flipped; 1: flipped) information are pre-defined as random values by users and each set of these parameters corresponds to a different hidden key. The hidden key serves as the encryption and decryption key of the extra encryption system. Here the hidden key is defined to be a key that is used in the encryption and decryption steps but not required to be sent to the information receiver through a secret channel. As a comparison, the actual encryption and decryption keys (two random phase masks) have to be known by the decryption side.