Optics Communications 402 (2017) 302–310

Contents lists available at ScienceDirect

Optics Communications

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

Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain

Hongfeng Xu [a,c], Wenhui Xu [b], Shuaihua Wang [a], Shaofan Wu [a,*]

[a] Fujian Institute of Research on the Structure of Matter, Chinese Academy of Sciences, Fuzhou 350108, China
[b] College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[c] University of Chinese Academy of Sciences, Beijing 100049, China

ARTICLE INFO

Keywords:
Optical cryptosystem
Asymmetric
Attacking
Modulus decomposition

ABSTRACT

We propose a scheme of attacking the pure phase asymmetric optical cryptosystem based on equal modulus decomposition (EMD) method. The cryptosystem is proven to be vulnerable to our modified iterative algorithm, even though the applying of phase encoding can reduce the constrain conditions. Furthermore, since that the improvement of system space asymmetry and key variety is an effective way to further enhance the security, we have proposed an asymmetric cryptosystem based on modulus decomposition in Fresnel domain. Compared with traditional asymmetric cryptosystem in Fourier domain, the combination with Fresnel transform cannot only simplify the system, but also improve the space asymmetry and introduce the geometric parameters as security keys. Numerical simulations are performed to demonstrate the feasibility and security of the proposed cryptosystem. In addition, several exemplary schemes for security-enhanced asymmetric cryptosystems are presented, which may bring profound illumination to many deeper researches in asymmetric optical cryptosystem.

1. Introduction

Optical encryption has attracted extensive interest since the double random phase encoding (DRPE) method was proposed in 1995 [1]. Recently, many novel methods based on Fourier transform [1–3], Fresnel transform [4–9], fractional Fourier transform [10–13], and gyrator transform [14–16] have been further developed for optical encryption. Most of the above methods belong to the category of symmetric cryptosystem, in which the decryption keys are the same as the encryption keys. However, the symmetric cryptosystem will be insufficiently valid for key distribution and management when multiple legal users constitute a large network [17]. Asymmetric cryptosystem using phase-truncated Fourier transforms has been proposed for solving the problems [18–20], while several studies have demonstrated that it is vulnerable to some attacks [21–23]. Inspired by PTFT-based asymmetric cryptosystem, the combination of coherent superposition and modulus decomposition has been applied into asymmetric cryptosystem [24,25]. It has been found that amplitude-only cryptosystem based on equal modulus decomposition (EMD) can be easily breached by iterative transform (IRT) [26], and other attack methods [27]. To enhance the security, phase-only EMD method was applied into asymmetric cryptosystem, of which the robustness against attacks has been verified by the studies [28].

In this paper, we firstly present a cryptanalysis of the EMD-based pure phase asymmetric cryptosystem and show that the cryptosystem is vulnerable to our modified IRT. Furthermore, we propose an asymmetric cryptosystem based on coherent superposition and modulus decomposition in Fresnel domain, which can enhance the security and simplify the system structure simultaneously. On the one hand, the introduction of Fresnel transform cannot only defend the attack of IRT by getting rid of the constraint of Fourier lens, but also introduce the geometrical parameters (wavelength and axial distances) as security keys, both of the space asymmetry and key variety are significantly improved; On the other hand, no lens is required in our system, which makes the decryption system simple and flexible. Numerical simulation has been performed to demonstrate the feasibility and robustness of our proposed system. To further improve the space asymmetry and key variety, several exemplary schemes are proposed, which may open up many novel opportunities in asymmetric optical cryptosystem.

[*] Corresponding author.
E-mail address: wsf@fjirsm.ac.cn (S. Wu).

http://dx.doi.org/10.1016/j.optcom.2017.05.035
Received 11 April 2017; Received in revised form 15 May 2017; Accepted 16 May 2017
0030-4018/© 2017 Elsevier B.V. All rights reserved.

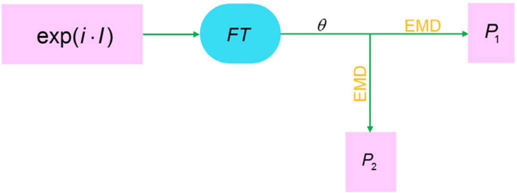

Fig. 1. Flowchart of the encryption process of EMD-based pure phase cryptosystem.

2. Cryptanalysis of "EMD-based pure phase asymmetric optical cryptosystem"

2.1. Theory of EMD-based pure phase cryptosystem

Fig. 1 shows the flowchart of the EMD-based pure phase cryptosystem proposed by Cai et al. [28]. Compared with traditional asymmetric cryptosystem [24], the EMD-based pure phase cryptosystem combines with phase encoding [29,30], in which the original image is preprocessed by phase encoding. The phase-encoded image is mathematically presented by $\exp[i \cdot \sqrt{I_k(x)}]$, where $\sqrt{I(x)}$ denotes the intensity distribution of the original image. The rest encryption processes of the EMD-based pure phase cryptosystem are the same as the traditional asymmetric cryptosystem, which can be expressed as follows:

$$I'(u) = A(u) \cdot \exp[i \cdot \varphi(u)] = FT\left[\exp(i \cdot \sqrt{I(x)})\right], \tag{1}$$

$$P_1(u) = \frac{A(u)/2}{\cos[\varphi(u) - \theta(u)]} \exp[i \cdot \theta(u)], \tag{2}$$

$$P_2(u) = \frac{A(u)/2}{\cos[\varphi(u) - \theta(u)]} \exp[i \cdot (2\varphi(u) - \theta(u))], \tag{3}$$

where $FT[\cdot]$ is Fourier transform, $\theta(u)$ is a random uniform distribution in the interval $[0, 2\pi]$. $P_1(u)$ and $P_2(u)$ are ciphertext and private key, respectively. With $P_1(u)$ and $P_2(u)$ the original image can be retrieved by the following equation:

$$I(x) = \left|FT^{-1}[P_1(u) \cdot PCF + P_2(u) \cdot PCF]\right|^2, \tag{4}$$

where $FT^{-1}[\cdot]$ is an inverse Fourier transform, PCF represents phase contrast filter, which is used for the realization of Zernike's phase contrast. Zernike's phase contrast is a technique for the visualization of phase perturbations [31], with which the decryption image can be recorded by the intensity detectors (like CCD) directly.

2.2. Security analysis and attack process

In Ref. [28], the authors have tested the robustness of the EMD-based pure phase cryptosystem against IRT proposed by Deng in Ref. [26]. They have indicated that no valuable information about the plaintext can be recovered, and the EMD-based pure phase cryptosystem can guarantee high-level security to the attack based on iterative Fourier transform. We have made some changes of IRT, and performed the numerical simulation to demonstrate that the EMD-based pure phase cryptosystem [28] is vulnerable to our modified IRT. Suppose that the ciphertext $P_1(u)$ is known. The attack algorithm can be described as below:

(1) Guess the complex value of the private key $P_2^0(u)$, and then begin the following iterative process.

(2) For the $kth(k = 0, 1, 2, 3, \dots)$ iteration, the private key is $P_2^k(u)$, the decrypted image is acquired as:

$$I_k(x) = \left|\arg\left\{FT^{-1}[P_1(u) + P_2^0(u)]\right\}\right|^2. \tag{5}$$

(3) Perform Fourier transform of $\exp[i \cdot \sqrt{I_k(x)}]$:

$$I'_k(u) = A_k(u) \cdot \exp[i \cdot \varphi_k(u)] = FT\left|\exp[i \cdot \sqrt{I_k(x)}]\right|^2. \tag{6}$$

(4) $P_2^{k+1}(u)$ Can be obtained with the constraint of the ciphertext $P_1(u)$:

$$P_2^{k+1}(u) = I'_k(u) - P_1(u). \tag{7}$$

(5) Substitute the amplitude of $P_2^{k+1}(u)$ with $P_1(u)$, while preserving the phase, as the moduli of the ciphertext and private key are identical in EMD method.

$$P_2^{k+1}(u) = |P_1(u)| \cdot \left[P_2^{k+1}(u) / \left|P_2^{k+1}(u)\right|\right]. \tag{8}$$

(6) Update $P_2^{k+1}(u)$ with $P_1(u)$ to make further use of the constraint:

$$P_2^{k+1}(u) = P_2^{k+1}(u) + \alpha \cdot \mathrm{conj}(P_1(u)) \max\left(|P_1(u)|^2\right), \tag{9}$$

where α is the adjustment factor, $\mathrm{conj}(\cdot)$ denotes the complex conjugate of a function, $\max(\cdot)$ represents the maximum of a matrix.

(7) Calculate the correlation coefficient (CC) [32] between the decrypted and original images, as well as the decrypted private key $P_2^{k+1}(u)$ and original private key $P_2(u)$.

$$\mathrm{CC} = \mathrm{cov}(f, f_0) \cdot (\sigma_f, \sigma_{f_0})^{-1}, \tag{10}$$

where $\mathrm{cov}(f, f_0)$ denotes the cross-covariance between f and f_0, σ_f is the standard deviation. The value of ranges from 0 to 1, $\mathrm{cov}(f, f_0) = 1$ means that watermark is extracted perfectly.

(8) Repeat steps (1)–(6) until the number of iterations reaches the preset threshold value.

2.3. Attack results

Numerical simulation has been performed to verify the feasibility of the proposed attack algorithm. A gray-scale image and a binary image are served as the original images, as shown in Fig. 2(a) and (e), respectively. Fig. 2(b) and (f) show the decrypted results, which are pretty recognizable. These decrypted images are obtained by 200 times of iteration. The CC values between original and decrypted gray-scale images, as well as the binary images change are nearly close to 0.6 and 0.65, respectively. Since that the CC values change with iterative numbers, the variation curves of the gray-scale images and the binary images are shown in Fig. 2(c) and (g), respectively. Both the CC values are about 0.6 after 50 times of iteration. We also calculate the CC between Original and decrypted private key $P_2(u)$ corresponding to gray-scale image and binary image displayed in Fig. 2(d) and (h), respectively. Both of the CC values are more than 0.3 after 50 times of iteration. The simulation results demonstrate that the EMD-based pure phase asymmetric cryptosystem is vulnerable to our improved IRT algorithm.

These attack results are selected from several computational results, as each entire iterative computational result is different, which is caused by the decrease of constraints. In the traditional EMD-based asymmetric cryptosystem, since that the moduli of the private key $P_2(u)$ and ciphertext $P_1(u)$ are identical according to the EMD theory, there are two constraints: a ciphertext and a known random phase mask. With the two constraints, the cryptosystem is extremely vulnerable to IRT attack, the attack results in Ref. [26] are pretty good. However, in the EMD-based pure asymmetric cryptosystem, the only constraint is the ciphertext $P_1(u)$. Even though it requires several computational running processes to obtain a set of relatively preferable results, it can still indicate that the EMD-based pure asymmetric cryptosystem can be breached by our modified IRT method.

3. Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain

In this section we propose an asymmetric optical cryptosystem combined modulus decomposition with Fresnel transform. The encryption and decryption processes are shown in Fig. 3(a) and (b), respectively.