Optics Communications 309 (2013) 231–235

Contents lists available at ScienceDirect

Optics Communications

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

Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem

Sudheesh K. Rajput, Naveen K. Nishchal *

Department of Physics, Indian Institute of Technology Patna, Patliputra Colony, Patna 800013, India

ARTICLE INFO

Article history:
Received 9 May 2013
Received in revised form
13 June 2013
Accepted 17 June 2013
Available online 17 July 2013

Keywords:
Image processing
Image encryption
Phase retrieval
Fractional Fourier transform

ABSTRACT

In this paper, we show that amplitude- and phase-truncation-based optical asymmetric cryptosystem is vulnerable to known-plaintext attack. The decryption keys are generated with the help of modified Gerchberg–Saxton phase retrieval algorithm from known-plaintext and ciphertext. With the help of the generated keys, the encrypted image, which is encrypted using encryption keys placed in either of the domains (Fourier, Fresnel, or fractional Fourier domain) is decrypted successfully. The vulnerability is proved through the results of computer simulation.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

With the pioneering publication of double random phase encoding (DRPE) technique proposed by Refregier and Javidi [1], a large number of contributions have appeared in the literature. Various optical domains have been exploited for safely spacing the secured keys; the random phase masks (RPM) [2,3]. Recently, it has been shown that the *DRPE* is vulnerable to the chosen-ciphertext attack, chosen plaintext attack, and known-plaintext attack [4–7]. These techniques have been reported to be vulnerable because of the inherent linearity in the encryption process. Also most of the reported techniques in literature belong to the category of symmetric cryptosystems in which the keys used for encryption, is identical to the decryption keys. For practical uses a symmetric cryptosystem would suffer from problems in key distribution, management, and delivery under an environment of network security. To overcome these problems, asymmetric cryptosystem has been introduced [8–21]. Peng et al. [8] proposed asymmetric cryptography based on wavefront sensing. In this method, the encryption key was derived from optical parameters, such as the wavelength, the focal length, or their combination and the decryption key was obtained from a regular point array formed by microlenslet array. Chen et al. [9] proposed an asymmetric cryptsystem using three-dimensional space based model, in which *RPM* and plaintext are combined as a series of particles. Qin and Peng [10] proposed an asymmetric cryptosystem based on phase-truncation approach in which asymmetric keys are generated during encryption. Further this scheme has been extended by adopting several architectures [11–17]. It was believed that asymmetric cryptosystem based on phase-truncation will have immunity against existing attacks. However, encrypted information of this scheme is revealed if encryption keys are considered as public keys [18]. To overcome this problem some asymmetric cryptosystems have been proposed which has immunity against special attack [19,20]. Recently, Liu et al. [21] proposed an asymmetric cryptosystem based on mixture retrieval type of Yang-Gu algorithm.

In the analysis of encryption scheme, it is assumed that attackers already know the encryption algorithm as well as encryption domain and other resources. For example in known-plaintext attack, a pair of plaintext and cipher text is known to the attackers [6]. If known plaintext attack can be used to break an encryption algorithm, then chosen plaintext attacks and chosen cipher text attacks can also do the same thing. It is because chosen plaintext attack and chosen cipher text attack provide more resources to the attackers than does known plaintext attack [22]. Recently, Nakano et al. [23] defined a singular key, different from the encryption key as a singular key that can decrypt only a given encrypted image in a known-plaintext attack but cannot decrypt other images that are encrypted with the same encryption key.

So far most of the studies on attacks on the various encryption schemes have been based on phase retrieval algorithms [24–26]. In this paper, we show that (1) asymmetric cryptosystem [10] is vulnerable to known plaintext- and ciphertext attack, and (2) data encrypted in one domain, e.g., Fourier domain can be decrypted in Fresnel domain or vice versa. In other words, for decryption, the information of corresponding domain parameters is not required. The keys can be generated in any domain with the help of known pair of ciphertext–plaintext using modified Gerchberg–Saxton (G–S) algorithm. With the help of the generated keys, encrypted image based on phase truncation approach in one domain is

* Corresponding author. Tel.: +91 612 2552027; fax: +91 612 2277383.
E-mail address: nkn@iitp.ac.in (N.K. Nishchal).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.06.036

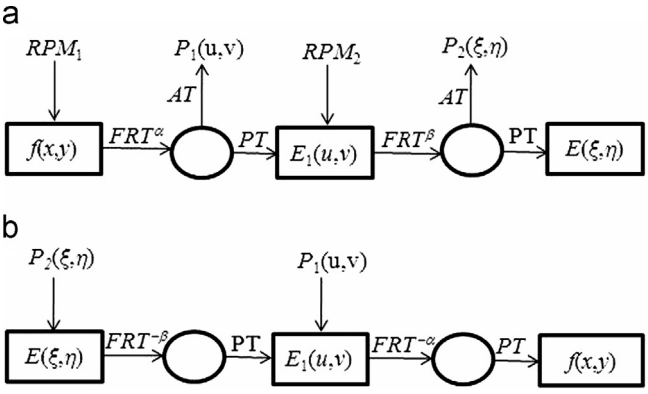

Fig. 1. Block diagram for (a) encryption and (b) decryption.

retrieved in another domain. To the best of our knowledge, this is the first report, which discusses known-plaintext attack on phase-truncation based asymmetric cryptosystem independent of encryption domain. Computer simulation results are presented in support of the proposed idea.

2. Principle

First we give brief introduction of asymmetric cryptosystem using fractional Fourier transform (FRT). But it is possible to encrypt data after placing *RPMs* in one optical domain, e.g., Fourier, Fresnel, or *FRT*, and decrypt data in any of those domains. The block diagrams for encryption and decryption processes are shown in Fig. 1(a) and (b), respectively. In phase truncation based image encryption scheme, two statistically independent *RPMs*; RPM_1 and RPM_2 are employed to encode an image $f(x,y)$ into an asymmetric ciphertext $E(\xi,\eta)$ as real-valued and stationary white noise [10,11]. Firstly, the image bonded with RPM_1 is fractional Fourier transformed and phase-truncated [15].

$$E_1(u,v) = PT\left\{K\iint f(x,y)\exp\{i2\pi R_1(x,y)\}\exp\left[j\pi\frac{x^2+y^2+u^2+v^2}{\tan\alpha}-2j\pi\frac{xyuv}{\sin\alpha}\right]dx\,dy\right\} \tag{1}$$

here $PT\{\cdot\}$ represents phase-truncation and α denotes the order of *FRT*, whose value lies between 0 and 1. Now this phase-truncated value bonded with RPM_2 is again fractional Fourier transformed and phase-truncated, which gives the encrypted image, $E(\xi,\eta)$.

$$E(\xi,\eta) = PT\{\Im^{\beta}[E_1(u,v)\exp\{i2\pi R_2(u,v)\}]\} \tag{2}$$

here $\Im^{\beta}$ represents the *FRT* of order β. For complete retrieval of an image, the decryption keys (DKs) are generated as

$$P_1(u,v) = AT\{\Im^{\alpha}[f(x,y)\exp\{i2\pi R_1(x,y)\}]\} \tag{3}$$

$$P_2(\xi,\eta) = AT\{\Im^{\beta}[E_1(u,v)\exp\{i2\pi R_2(u,v)\}]\} \tag{4}$$

here $AT[\cdot]$ denotes the amplitude truncation. Owing to the non-linear operation of phase truncation approach, which leads to one way function, the asymmetric cryptosystem offers immunity against existing attacks. Therefore, to an attacker, the chief task is to reproduce *DKs*; $P_1(u,v)$ and $P_2(\xi,\eta)$, because original image can be retrieved only if correct *DKs* are used. However, it is possible to retrieve amplitude-truncated values with the help of phase retrieval algorithm, which help generate *DKs* [24–26].

For generating the first *DK*, G–S algorithm is applied between input plane and the fractional Fourier plane using known-plaintext and arbitrarily chosen *RPM*. Suppose $|f(x,y)|$ represents the amplitude of the input image to be encrypted and $\exp\{i2\pi r(x,y)\}$ denotes the arbitrary *RPM*. The block diagram of modified G–S phase retrieval algorithm is shown in Fig. 2. It is defined by the following steps [25,26]:

1. Any complex function $f'_n(x,y)$ after nth iteration can be written as
$$f'_n(x,y) = |f(x,y)|\exp\{i2\pi r_n(x,y)\} \tag{5}$$

2. Now the complex function $f'_n(x,y)$ is fractional Fourier transformed with some arbitrary fractional order α' as
$$F_{n+1}(u,v) = \Im^{\alpha'}[f'_n(x,y)] = |F_{n+1}(u,v)|\exp\{i\varphi_n(u,v)\} \tag{6}$$

3. Replace amplitude of Eq. (6) with unity
$$F'_{n+1}(u,v) = 1\exp\{i\varphi_n(u,v)\} \tag{7}$$

4. Now perform *FRT* to $F'_{n+1}(u,v)$ of order α' as
$$F''_{n+1}(x,y) = \Im^{-\alpha'}\left[F'_{n+1}(u,v)\right] = \left|F''_{n+1}(x,y)\right|\exp\left\{i\varphi'_n(x,y)\right\} \tag{8}$$

5. Replace amplitude of Eq. (8) with input intensity
$$f'_{n+1}(x,y) = \left|f(x,y)\right|\exp(i\varphi'_n(x,y) = \left|f(x,y)\right|\exp\left\{ir_{n+1}(x,y)\right\} \tag{9}$$

The convergence of the iteration process is completed with the computation of the mean square error (MSE) reaching the minimum value. The *MSE* defined by the following equation is calculated between $abs[f(x,y)]$ and $abs[F''_{n+1}(x,y)]$,

$$MSE = \frac{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\{|f(x,y)|-|F''_{n+1}(x,y)|\}^2}{N\,N} \tag{10}$$

For generating the second *DK*, G–S algorithm is applied between *FRT* plane and the output plane using known-ciphertext and arbitrarily chosen *RPM*, $\exp\{i2\pi r'(\xi,\eta)\}$. The basic steps for phase retrieval algorithm remains same but with the change that in this case $|f(x,y)|$ is replaced with $|E(\xi,\eta)|$. The arbitrarily chosen *FRT* order is β'. Now similar to Eqs. (6) and (8), we can obtain the phase, $\psi_n(u,v)$, and $E''_{n+1}(\xi,\eta)$. In this case, the convergence of the iteration process is completed when the *MSE* value between $abs[E(\xi,\eta)]$ and $abs[E''_{n+1}(\xi,\eta)]$ reaches minimum.

Now both the *DKs* are generated with the help of the retrieved phase functions; $\varphi_n(u,v)$ and $\psi_n(u,v)$, in *FRT* plane and the output plane, as follows:

$$k_1(u,v) = \exp\{i\arg[\exp\{i\varphi_n(u,v)\}]\} \tag{11}$$

$$k_2(\xi,\eta) = \exp\{i\arg[\Im^{-\beta'}\{\exp\{i\psi_n(u,v)\}\}]\} \tag{12}$$

We can see from Eqs. (5) to (12) that the key generation procedure depends on plaintext, ciphertext, and the domain used in the G–S algorithm. Hence, one can generate *DKs* in arbitrary

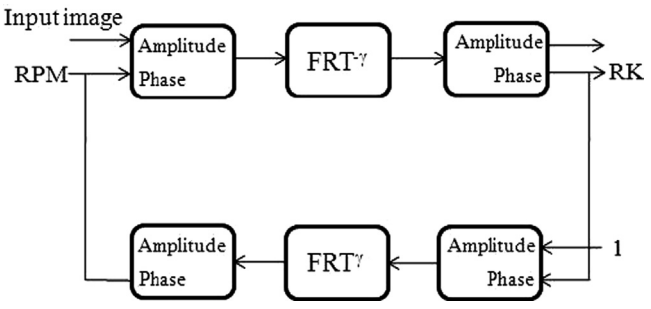

Fig. 2. Block diagram of modified G–S algorithm. RPM: random phase mask; RK: retrieved key.

Download English Version:

https://daneshyari.com/en/article/7932373

Download Persian Version:

https://daneshyari.com/article/7932373

Daneshyari.com