Optics and Lasers in Engineering 83 (2016) 48–58

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Information verification cryptosystem using one-time keys based on double random phase encoding and public-key cryptography

Tieyu Zhao [a,*], Qiwen Ran [a], Lin Yuan [a,b], Yingying Chi [c], Jing Ma [a]

[a] State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin 150001, China
[b] College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China
[c] School of Psychology, Northeast Normal University, Changchun 130024, China

ARTICLE INFO

Article history:
Received 19 May 2015
Received in revised form
3 March 2016
Accepted 3 March 2016

Keywords:
Image encryption
Information verification
Asymmetric cryptosystem

ABSTRACT

A novel image encryption system based on double random phase encoding (DRPE) and RSA public-key algorithm is proposed. The main characteristic of the system is that each encryption process produces a new decryption key (even for the same plaintext), thus the encryption system conforms to the feature of the one-time pad (OTP) cryptography. The other characteristic of the system is the use of fingerprint key. Only with the rightful authorization will the true decryption be obtained, otherwise the decryption will result in noisy images. So the proposed system can be used to determine whether the ciphertext is falsified by attackers. In addition, the system conforms to the basic agreement of asymmetric cryptosystem (ACS) due to the combination with the RSA public-key algorithm. The simulation results show that the encryption scheme has high robustness against the existing attacks.

1. Introduction

In the past 20 years, the optical image encryption has attracted more and more researchers' attention. DRPE [1] was one of the most widely used optical encryption schemes due to its easy implementation and combination with other encryption schemes. The encryption schemes based on DRPE combined with fractional Fourier transform were proposed respectively in [2,3]. Recently, DRPE combined with double image encryption, RSA public-key algorithm, and the photon counting imaging technique are used to image encryption [4–7]. Many chaos-based encryption algorithms [8–18] have been proposed. Due to relying on dynamicity, chaos-based encryption algorithms were regarded as a promising research for image encryptions. At the same time, the encryption method based on the generalized fractional Fourier transform has been further improved [19,20]. Optical asymmetric cryptosystem (OACS) was been proposed [21–24], which can overcome the disadvantages that the conventional optical cryptosystem is linear symmetric system and vulnerable to attacks [25–27]. However, He et al proposed that the existing OACS is untenable because of the misunderstanding of the basic principles of ACS [28]. In this paper, we propose a novel optical image encryption system which conforms to the basic agreement of ACS. Each time the encryption is performed, a new decryption key will be generated simultaneously. Therefore, the system has the feature of OTP cryptosystem [29]. The proposed system can resist the attacks [25–27,30,31] owing to the use of the phase modulation technique. Besides, the system uses the fingerprint key so that the receiver, through decryption with the private key and the fingerprint, can determine whether the ciphertext is maliciously tampered with. Moreover, the authenticity and integrity of the information can be both ensured. In the end of this paper, we verify the robustness of the system against the known plaintext attack (KPA) and special attack and demonstrate the reliability of the system in the aspect of the information verification.

The reminder of this paper is organized as follows. In Section 2, the basic agreement of asymmetric cryptosystem and the importance of phase are presented. The proposed image cryptosystem is described in Section 3. Simulation results and performance analyses are shown in Section 4. The security and reliability of the proposed system are given in Section 5. Finally, a conclusion is drawn in Section 6.

2. The basic principle

2.1. Basic agreement of asymmetric cryptosystem

In 1976, Diffie and Hellman first proposed the historic idea of public key cryptography [32] in which Alice makes the encryption key public and keeps the decryption key private.

* Corresponding author.
E-mail address: zty03y3213@163.com (T. Zhao).

http://dx.doi.org/10.1016/j.optlaseng.2016.03.001
0143-8166/

The working principle of ACS

(1) Alice uses the cryptosystem to produce a pair of keys—an encryption key (public key) and a decryption key (private key). The encryption key is public, while the decryption key is reserved privately by Alice.
(2) If Bob wants to send information to Alice, he may use the public key to encrypt the information.
(3) Alice uses her private key to decrypt the ciphertext received from Bob and obtains the plaintext (even though others receive the ciphertext, they cannot decrypt it due to the lack of the private key).

2.2. RSA public-key algorithm

In 1978, Rivest et al. first proposed RSA algorithm based on the public key cryptosystem of numeric theory which is the best encryption algorithm in all the public key cryptosystems [33]. So far, only short RSA key can be cracked down by the brute force attack [34]. As long as RSA key is long enough, RSA encryption algorithm is quite safe in practice.

The secret keys are generated through the following steps [5,35]:

(1) select two large prime numbers p and q randomly,
(2) calculate $n = p \times q$ and $\phi = (p-1)(q-1)$,
(3) select an integer e, such that $1 < e < \phi$ and gcd $(e, \phi) = 1$ (gcd-relatively prime),
(4) the decryption key d is calculated by $d \cdot e \equiv 1 \bmod \phi$ (mod-modulo operators), and
(5) (e, n) denotes the public key, and d denotes the private key.

In the encryption process, the bit string of plaintext is first divide into many groups. Then the corresponding decimal number to each group is set less than n. Finally perform the encryption operation on each plaintext group m such that

$$c \equiv m^e \bmod n. \tag{1}$$

The decryption operation on each ciphertext group is expressed as

$$m \equiv c^d \bmod n. \tag{2}$$

2.3. The importance of phase

Phase is very important in signal processing for its capability of reconstructing a signal completely [36,37]. Similarly, the phase is also very important in image processing as shown in Fig. 1. Firstly, the phase and the amplitude are extracted by the Fourier transform on the images "Lena" and "Baboon" respectively. Secondly, the new image is obtained by the inverse Fourier transform, and we can clearly see the contour of the image "Lena". This shows the importance of phase in image processing. Here *PT* and *PR* denote the operation of phase truncation and phase reservation respectively. The definition is as follows:

For any complex amplitude $F = |F| \exp(i \cdot \phi)$, then

$$PT(F) = |F|, \tag{3}$$

$$PR(F) = \exp(i \cdot \phi). \tag{4}$$

Our encryption scheme mainly focuses on the phase processing.

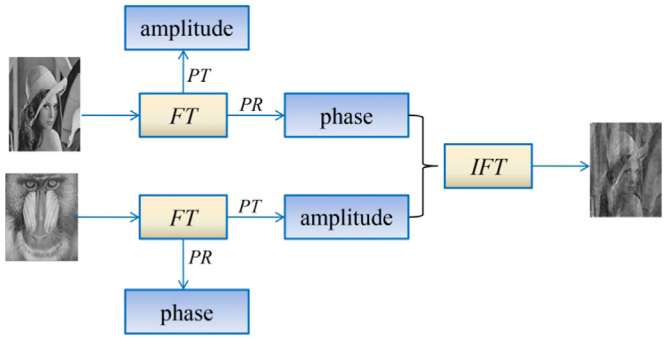

Fig. 1. The importance of phase. *PT* denotes the operation of phase truncation; *PR* – the operation of phase reservation; *FT* – Fourier transform; and *IFT* – inverse Fourier transform.

3. A new image encryption system

The working flowchart of the proposed cryptosystem is shown in Fig. 2.

The working procedure of the system is

(1) If Bob wants to send information to Alice, he first needs to register an authentication image (referring to his fingerprint image in this paper) in Alice's information database.
(2) Bob encrypts the information into the ciphertext using the public key and his fingerprint.

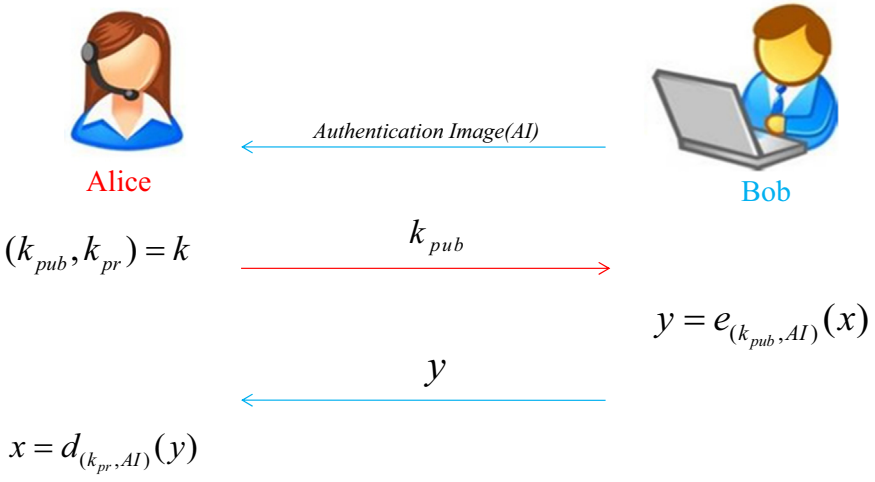

Fig. 2. The flowchart of the proposed cryptosystem.