Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 732609, 12 pages
http://dx.doi.org/10.1155/2015/732609

Research Article

Key Distribution and Changing Key Cryptosystem Based on Phase Retrieval Algorithm and RSA Public-Key Algorithm

Tieyu Zhao,[1] Qiwen Ran,[1] Lin Yuan,[1,2] Yingying Chi,[3] and Jing Ma[1]

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

Correspondence should be addressed to Tieyu Zhao; zty03y3213@163.com

Received 24 May 2015; Revised 15 June 2015; Accepted 18 June 2015

Academic Editor: Payman Jalali

The optical image encryption has attracted more and more researchers' attention, and the various encryption schemes have been proposed. In existing optical cryptosystem, the phase functions or images are usually used as the encryption keys, and it is difficult that the traditional public-key algorithm (such as RSA, ECC, etc.) is used to complete large numerical key transfer. In this paper, we propose a key distribution scheme based on the phase retrieval algorithm and the RSA public-key algorithm, which solves the problem for the key distribution in optical image encryption system. Furthermore, we also propose a novel image encryption system based on the key distribution principle. In the system, the different keys can be used in every encryption process, which greatly improves the security of the system.

1. Introduction

The characteristics of optical information processing are parallel and multidimensional, so more and more researchers have been studying the optical information security in the recent twenty years. Optical image encryption system based on double random phase encoding (DRPE) was proposed in 1995 [1] and the keys were two random phase matrices in this system. It was easy for the optical implementation and easy to combine with other encryption methods, so it attracted many researchers' attention and a lot of improved encryption systems were proposed in [2–7]. However, the security of the system in the systems without reference to the key distribution and transmission concerned researchers more. Optical asymmetric cryptosystem (OACS) was proposed based on phase-truncated Fourier transforms (PTFT) in 2010 [8], and it used nonlinear operation of the phase truncation which overcame the defects that DRPE was linear and symmetric [9–11]. Since then, the many improved systems have been proposed based on PTFT [12–20] and some researchers proposed different OACS from another perspective [21–24]. However, the existing OACS was incomplete [25], which did not meet the basic protocol of asymmetric cryptosystem (ACS). Although the security of the systems is significantly improved, only the private key sharing can establish communication in reality. Recently, Zhang et al. proposed an optical cryptosystem based on the phase-truncated Fresnel diffraction (PTFD) and transport of intensity equation (TIE) [26]. A random amplitude mask (RAM) and a random phase mask (RPM) are employed as two secret keys to encrypt the input image into a real-valued noise-like intensity distribution. Moreover, the proposed scheme is expected to against existing attacks. Wang et al. proposed a new optical information authentication system based on compressed DRPE images and quick-response (QR) codes, where the parameters of optical light wave are used as keys for optical decryption and the QR code is a key for verification [27]. Cai et al. proposed an asymmetric cryptosystem using equal modulus decomposition (EMD) to create an effective trapdoor one-way function without a silhouette problem [28].

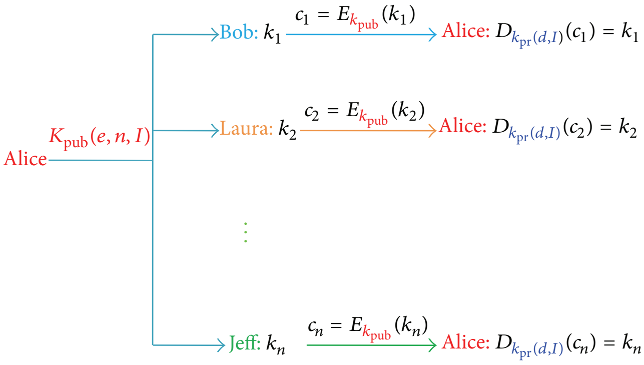

Alice
$K_{\text{pub}}(e, n, I)$
Bob: k_1
$c_1 = E_{k_{\text{pub}}}(k_1)$
Alice: $D_{k_{\text{pr}}(d,I)}(c_1) = k_1$
Laura: k_2
$c_2 = E_{k_{\text{pub}}}(k_2)$
Alice: $D_{k_{\text{pr}}(d,I)}(c_2) = k_2$
⋮
Jeff: k_n
$c_n = E_{k_{\text{pub}}}(k_n)$
Alice: $D_{k_{\text{pr}}(d,I)}(c_n) = k_n$

FIGURE 1: Key distribution scheme.

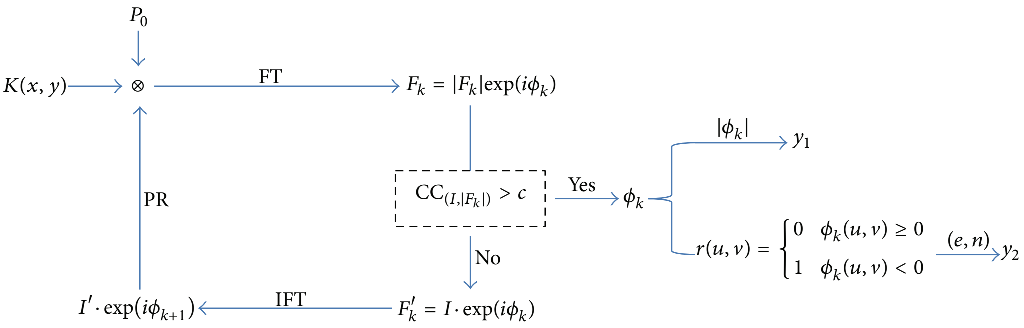

P_0
$K(x, y)$
$\otimes$
FT
$F_k = |F_k| \exp(i\phi_k)$
$\text{CC}_{(I,|F_k|)} > c$
Yes
ϕ_k
$|\phi_k|$
y_1
$r(u, v) = \begin{cases} 0 & \phi_k(u, v) \geq 0 \\ 1 & \phi_k(u, v) < 0 \end{cases}$
(e, n)
y_2
No
$F_k' = I \cdot \exp(i\phi_k)$
IFT
$I' \cdot \exp(i\phi_{k+1})$
PR

FIGURE 2: The encryption system: P_0 denotes initial phase; PR: operation of the phase reservation; $|\cdot|$: modulus; FT: Fourier transform; IFT: inverse Fourier transform.

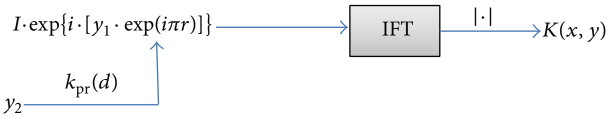


FIGURE 3: The decryption system.

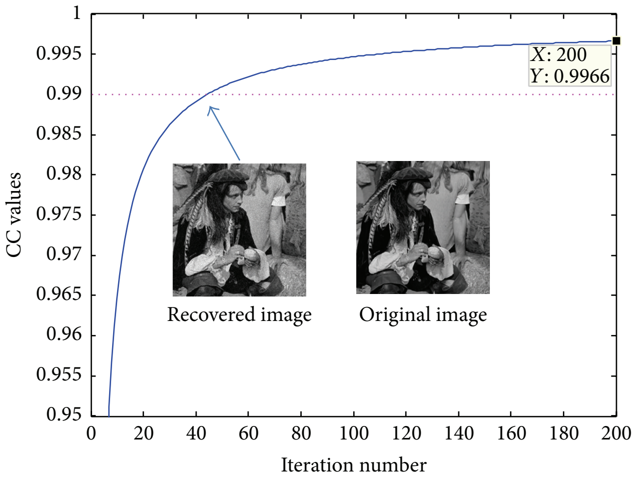


FIGURE 4: The comparison of the retrieved image and the original image.

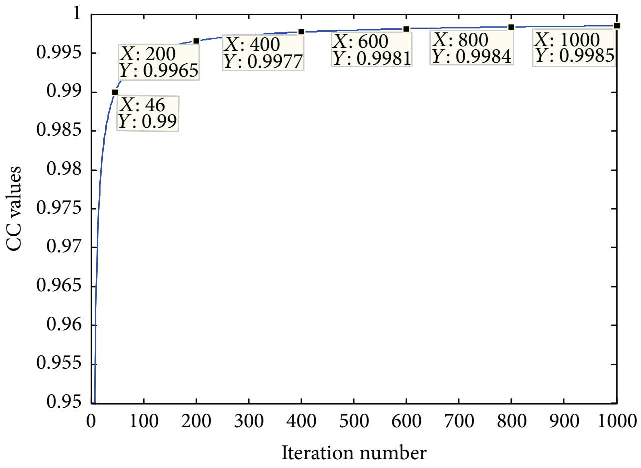
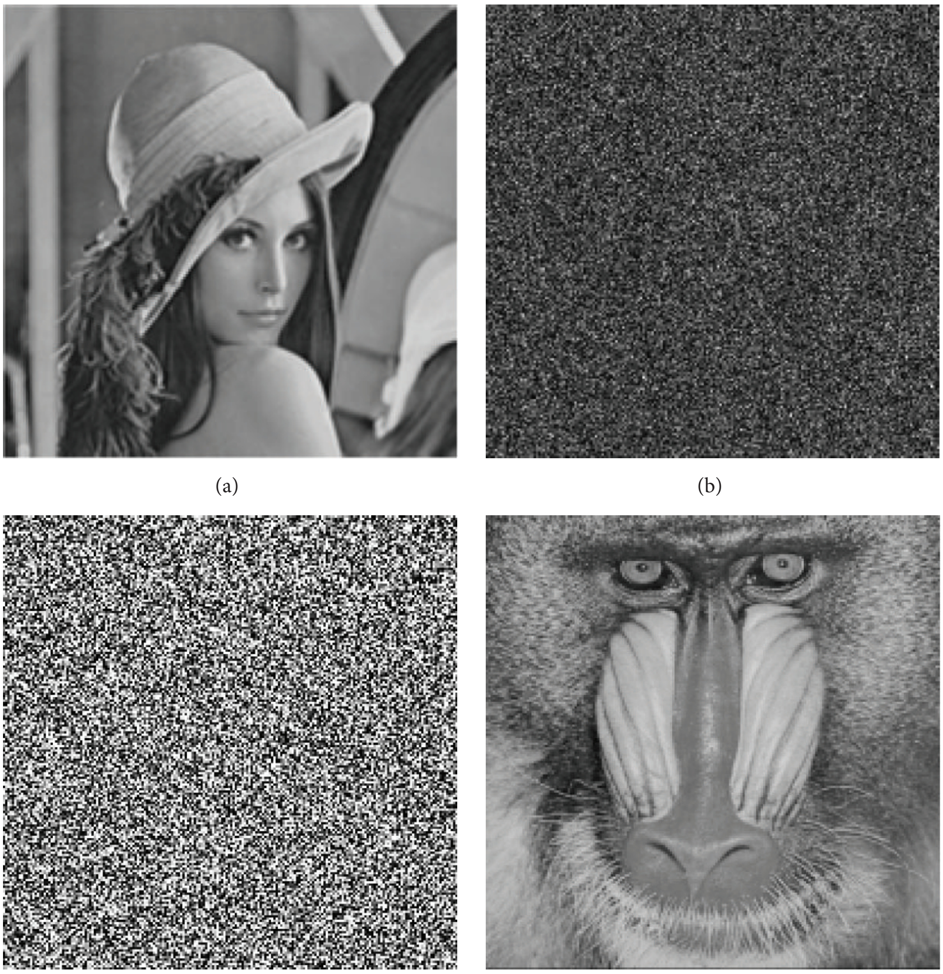


Figure 5: Correlation coefficient curve.



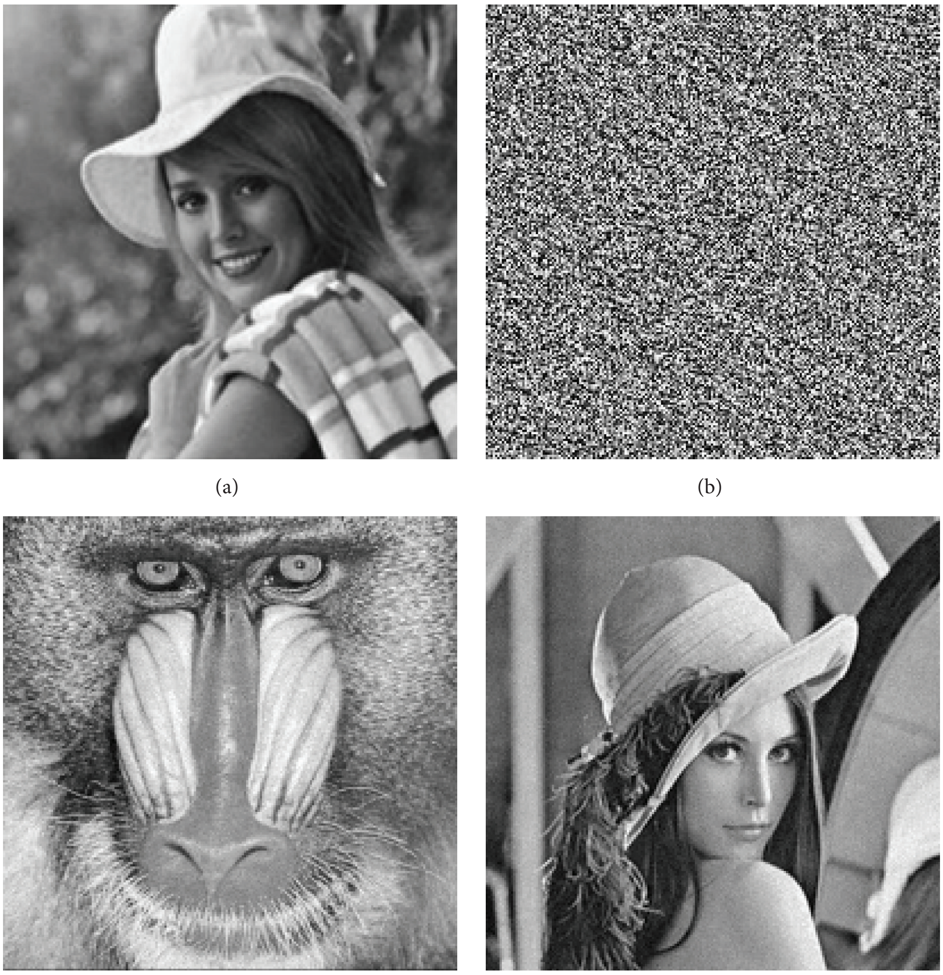
(a)

(b)

(c)

(d)

Figure 6: (a) The original image; (b) the ciphertext; (c) the first phase P_1; (d) the second phase P_2.



(a)

(b)

(c)

(d)

Figure 7: (a) Alice's public image; (b) the ciphertext; (c) Alice's retrieved phase P_2'; (d) Alice's decrypted image.

In the system the encryption key is RPM, and the decryption key is obtained by EMD.

In the existing optical cryptosystem, usually the key generally is phase functions or other optical parameters (such as wavelength, focal length, etc.), but the problem to be solved is how to distribute and transmit the keys (phase functions). In this paper, we propose a key distribution scheme, which solves the problem for the key distribution. Furthermore, we propose an image encryption system of changing key based on the key distribution principle which conforms to the basic protocol of ACS, and the greatest advantage of the system is that both sides of communication can change key constantly, which greatly improve the security of the system.

2. Key Distribution Scheme

We propose a key distribution scheme on public channel, and the process is shown in Figure 1.

The basic protocol is as follows:

(1) Alice opens the encryption keys (the public key k_{pub}) and reserves the decryption keys (the private key k_{pr}).

(2) Bob wants to send key k_1 to Alice and he uses Alice's public key to encrypt k_1.

(3) Alice receives Bob's ciphertext and uses the private key for decryption and obtains k_1.

(4) If Alice receives Laura's ciphertext and uses the private key for decryption and obtains the key k_2.

In the key distribution scheme, users do not need to establish the secret channel and the whole transmission process can be open to the public.

3. The Encryption and Decryption

3.1. RSA Public-Key Algorithm. In 1978, Rivest et al. first proposed RSA algorithm based on public-key cryptosystems of numeric theory and RSA algorithm was the best encryption algorithm in public-key cryptosystems [29]; the following steps show how the keys are generated [30]:

(1) Select two large prime numbers p and q randomly.

(2) Consider $n = p \times q$ and $\phi = (p - 1)(q - 1)$.

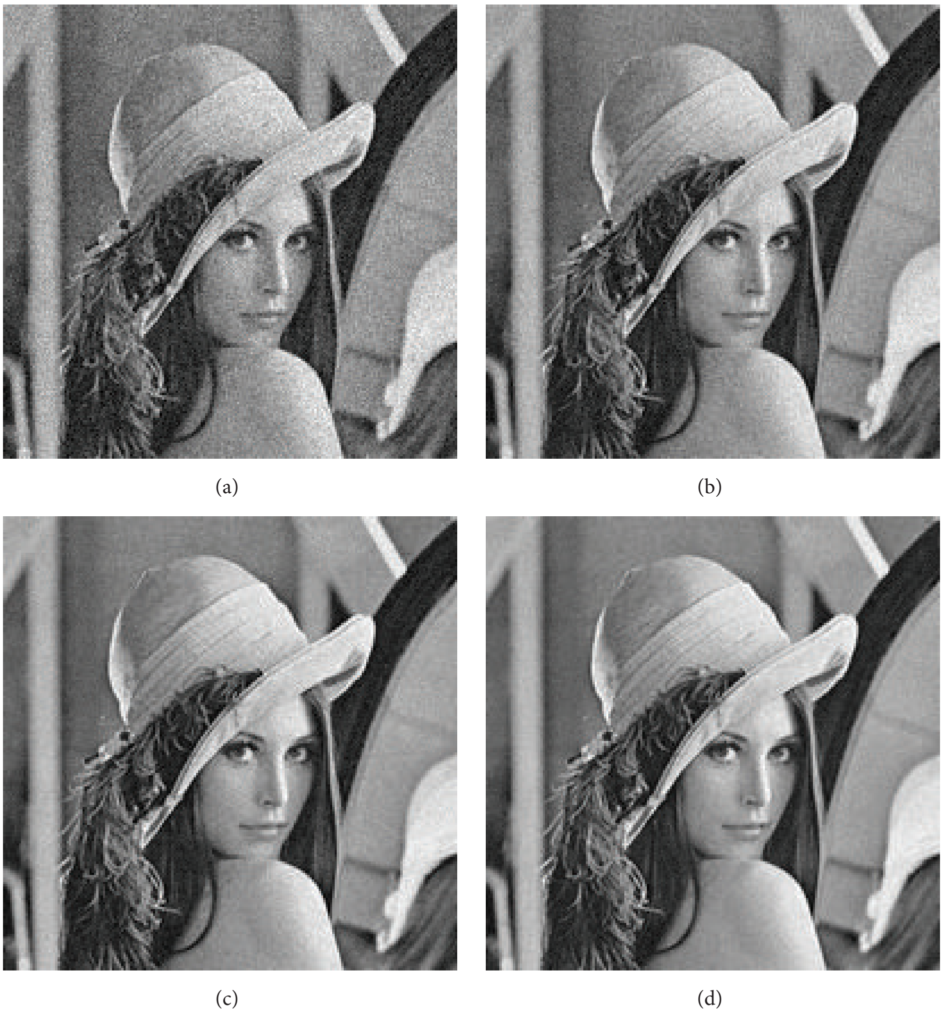


FIGURE 8: The influence of the CC on decrypted image: (a) CC = 0.95; (b) CC = 0.97; (c) CC = 0.99; (d) CC = 0.997.

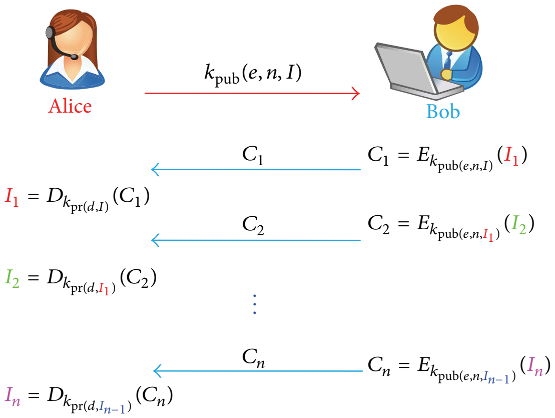

Alice
$k_{\text{pub}}(e, n, I)$
Bob
C_1
$C_1 = E_{k_{\text{pub}(e,n,I)}}(I_1)$
$I_1 = D_{k_{\text{pr}(d,I)}}(C_1)$
C_2
$C_2 = E_{k_{\text{pub}(e,n,I_1)}}(I_2)$
$I_2 = D_{k_{\text{pr}(d,I_1)}}(C_2)$
$\vdots$
C_n
$C_n = E_{k_{\text{pub}(e,n,I_{n-1})}}(I_n)$
$I_n = D_{k_{\text{pr}(d,I_{n-1})}}(C_n)$

FIGURE 9: Communication protocol.

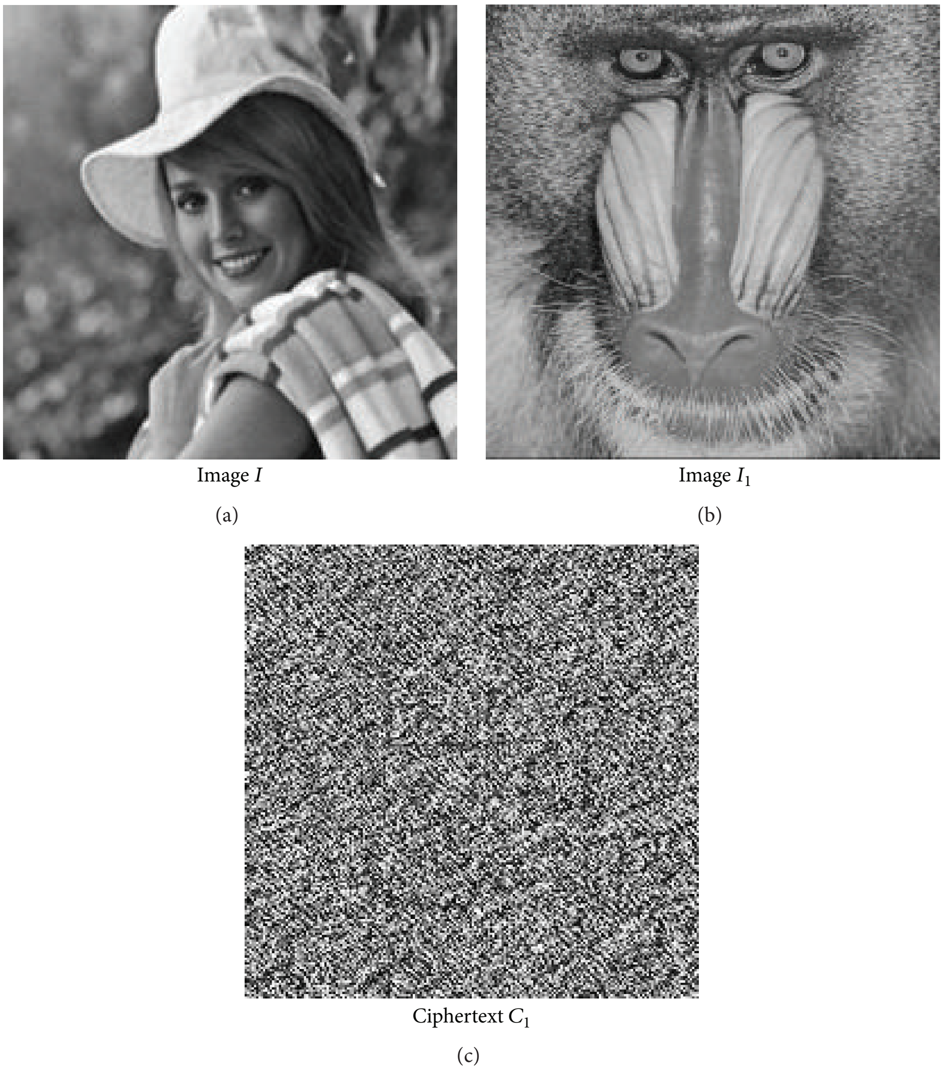


Image I

(a)

Image I_1

(b)

Ciphertext C_1

(c)

Figure 10: (a) Alice opens the image I; (b) the image I_1; (c) ciphertext C_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).

(5) (e, n) denotes the public key, and d denotes the private key.

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

$$c \equiv m^e \bmod n. \quad (1)$$

The decryption operation on each ciphertext group may be expressed as

$$m \equiv c^d \bmod n. \quad (2)$$

3.2. The Encryption Scheme. In the key distribution scheme of Figure 1 the public key is $k_{\text{pub}}(e, n, I)$. The key (e, n) is generated by RSA algorithm, and I is the public image. We present the encryption system as shown in Figure 2. The plaintext K is the key to be transferred, and P_0 is the initial random phase encoding; then

$$F_0 = \text{FT}\left(K \cdot P_0\right) = \left|F_0\right| \exp\left(i\phi_0\right), \quad (3)$$

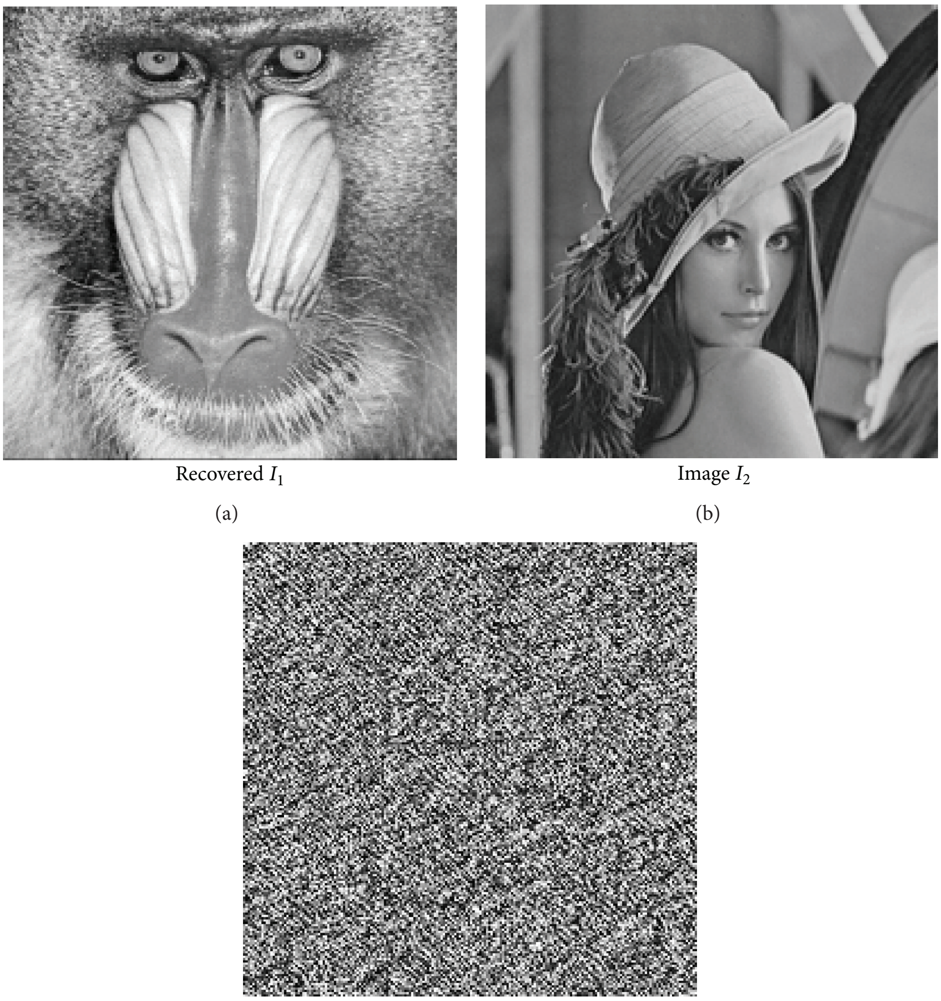
where FT denotes the Fourier transform. The correlation coefficient (CC) controls whether the iterative process continues, which is discussed in two different conditions.

First, when $\text{CC} < c$ ($c = 0.99$), iteration continues and the amplitude is limited,

$$F_0' = I \cdot \exp\left(i\phi_0\right), \quad (4)$$

where I is the target image (the public image), and the inverse Fourier transform is to be done next:

$$\text{IFT}\left(F_0'\right) = I' \cdot \exp\left(i\phi_1\right), \quad (5)$$



Recovered I_1

(a)

Image I_2

(b)

Ciphertext C_2

(c)

Figure 11: (a) Alice recovers the image "Baboon"; (b) the image I_2; (c) ciphertext C_2.

where IFT denotes the inverse Fourier transform, and phase is reserved:

$$\mathrm{PR}\left[I' \cdot \exp\left(i\phi_1\right)\right] = \exp\left(i\phi_1\right), \tag{6}$$

where PR denotes the operation of phase reservation. An iteration process is completed, and then P_0 is replaced by $\exp(i\phi_1)$ to complete the next iteration process.

Secondly, when $\mathrm{CC} \geq c$ ($c = 0.99$), the iteration is stopped and outputs ϕ_k, which is processed dividing into two parts: (a) the ciphertext $y_1 = |\phi_k|$ is obtained by modulus operation; (b) the matrix r is obtained by binary modulation

$$r = \begin{cases} 0 & \text{if } \phi_k \geq 0 \\ 1 & \text{if } \phi_k < 0. \end{cases} \tag{7}$$

The encryption key (e, n) is used to encrypt the matrix r and the ciphertext y_2 is obtained:

$$y_2 = E_{(e,n)}\left(r\right). \tag{8}$$

Then the encryption process is completed and the ciphertext (y_1, y_2) is obtained.

3.3. The Decryption Scheme. In the decryption system the private key $k_{\mathrm{pr}}(d)$ is as the decryption key, and the decryption process is shown in Figure 3. The receiver receives the ciphertext (y_1, y_2) using the private key to decrypt the ciphertext y_2 and gets the binary matrix r,

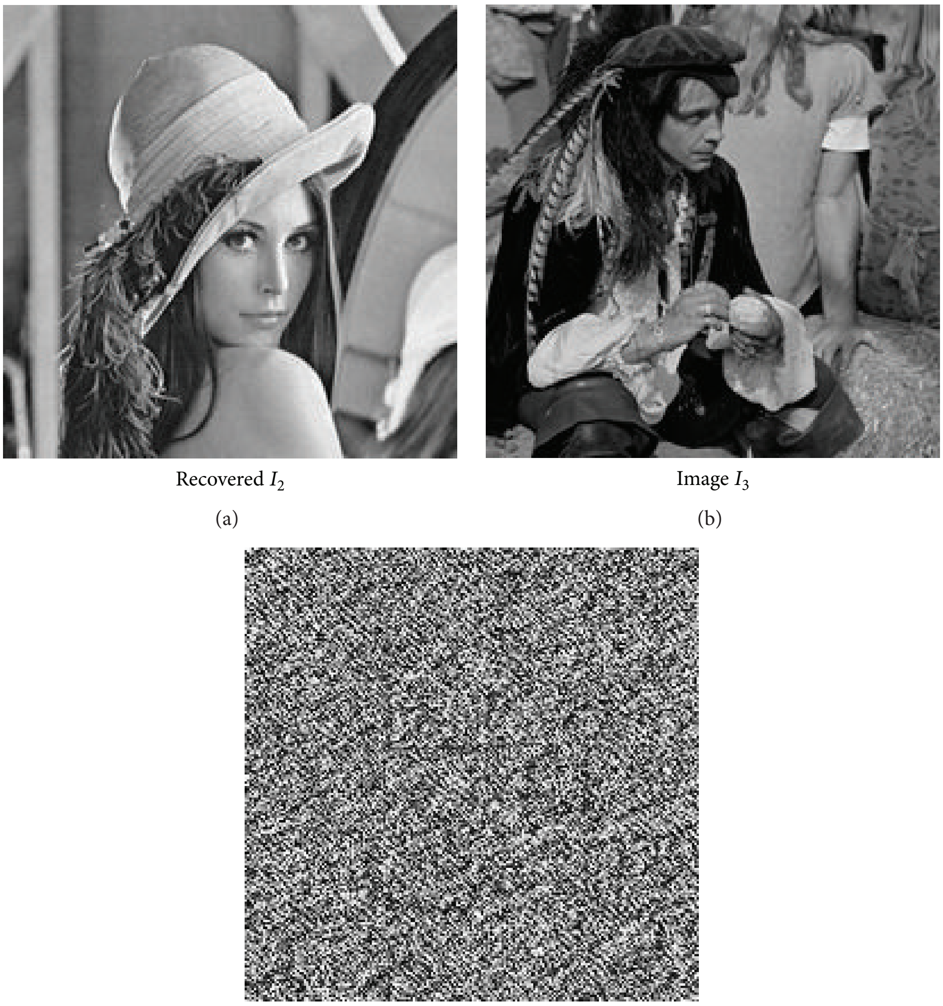
$$r = D_{k_{\mathrm{pr}}}\left(y_2\right); \tag{9}$$

then

$$\exp\left(i\pi r\right) = \begin{cases} 1 & r = 0 \\ -1 & r = 1, \end{cases} \tag{10}$$

in order to calculate phase ϕ_k,

$$\phi_k = y_1 \cdot \exp\left(i\pi r\right); \tag{11}$$



Recovered I_2

(a)

Image I_3

(b)

Ciphertext C_3

(c)

Figure 12: (a) Alice recovers the image "Lena"; (b) the image I_3; (c) ciphertext C_3.

here I is the public image, so you can get the plaintext $K(x, y)$,

$$K(x, y) = \left|\mathrm{IFT}\left\{I \otimes \exp\left(i \cdot \phi_k\right)\right\}\right|. \qquad (12)$$

In the decryption process, the receiver uses the private key to decrypt the ciphertext y_2 and gets the binary matrix r and finds the phase ϕ_k through the constraint relationship between r and the ciphertext y_1; thus it is easy to get the plaintext K.

3.4. The Performance Analysis. To evaluate the impact of iteration numbers on the retrieved image, the CC is introduced for comparing the retrieved image with the original image, which is defined as

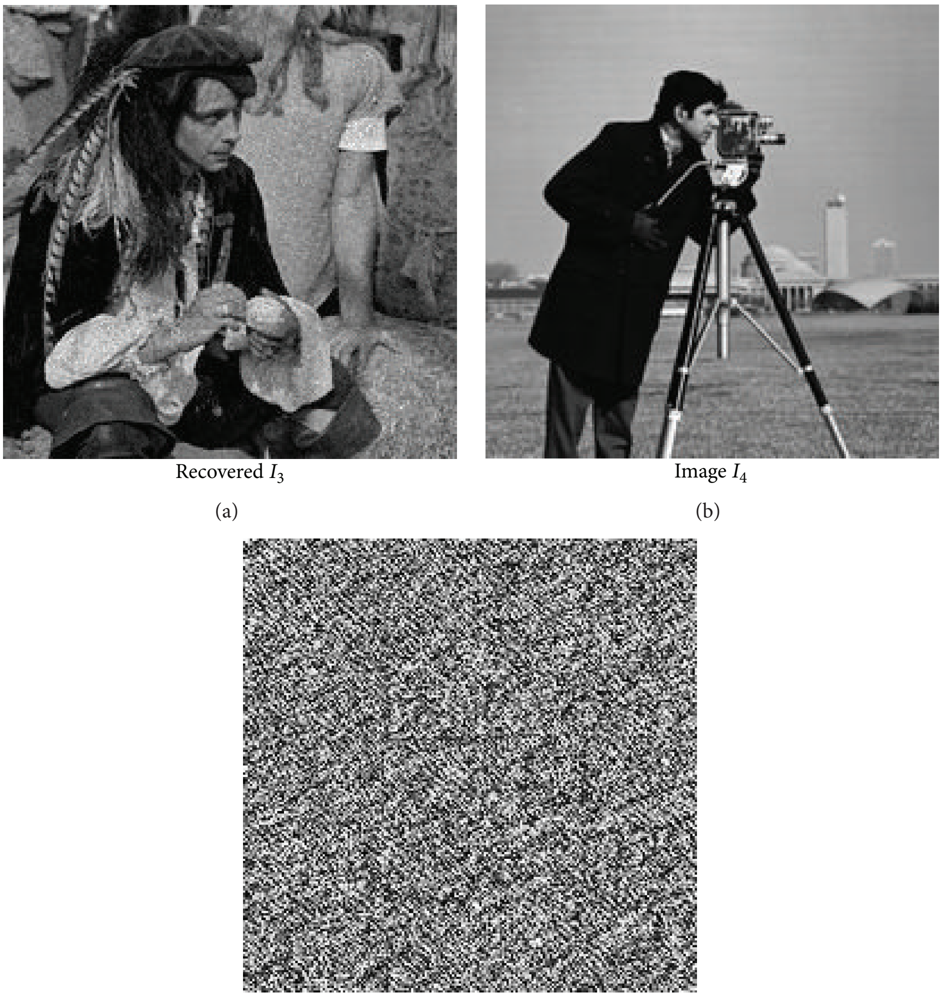
$$\mathrm{CC} = \frac{\mathrm{COV}\left[f(x, y), f'(x, y)\right]}{\sigma_f \cdot \sigma_{f'}}, \qquad (13)$$

where $f(x, y)$ and $f'(x, y)$ stand for the original image and the retrieved image, respectively, σ_f and $\sigma_{f'}$ are the standard deviations of $f(x, y)$ and $f'(x, y)$, and $\mathrm{COV}[f(x, y), f'(x, y)]$ is the covariance of the two corresponding images. The CC curves of different iteration numbers are shown in Figures 4 and 5, respectively.

In Figure 4 we present the CC curve which iteratives 200th. When the value of the CC is 0.99, the retrieved image is obtained and the original image is presented on the right. That is, the algorithm needs only a small iteration number to restore the clear image. In Figure 5, we present the CC curve which iteratives 1000th and mark the number of iterations (X) and the value of the CC (Y). Thus according to Figure 5 users can flexibly choose the value of the CC to control the iterative process in the encryption process.

4. Verification and Analysis

In this paper, we verify the key distribution scheme taking the DRPE, for example. The plaintext is real image, and just the second phase is distributed. In order to better facilitate



Recovered I_3

(a)

Image I_4

(b)

Ciphertext C_4

(c)

Figure 13: (a) Alice recovers the image “Man”; (b) the image I_4; (c) ciphertext C_4.

observation, “Baboon” image is selected as the key. The simulation of the DRPE is given in Figure 6. Figures 6(a) and 6(b) are the plaintext and the ciphertext, respectively, and Figures 6(c) and 6(d) are both the encryption keys.

The key distribution based on DRPE is shown as follows.

(1) Alice opens the public key $k_{\text{pub}}(e, n, I)$. ($e = 21746071$, $n = 37737253$) is the public keys of RSA algorithm, and I is the public image (Figure 7(a)).

(2) Bob wants to send the phase P_2 (Figure 6(d)) to Alice and uses the public key $k_{\text{pub}}(e, n, I)$ to encrypt the phase P_2 as shown in Figure 7(b).

(3) Alice receives the ciphertext and uses the private key $k_{\text{pr}}(d)$ ($d = 175771$) for decryption; then the phase P_2' is obtained in Figure 7(c).

So far the process of the key distribution is completed.

(4) Next, Bob sends the ciphertext (Figure 6(b)) to Alice who uses the phase P_2' for decryption and gets the plaintext (Figure 7(d)).

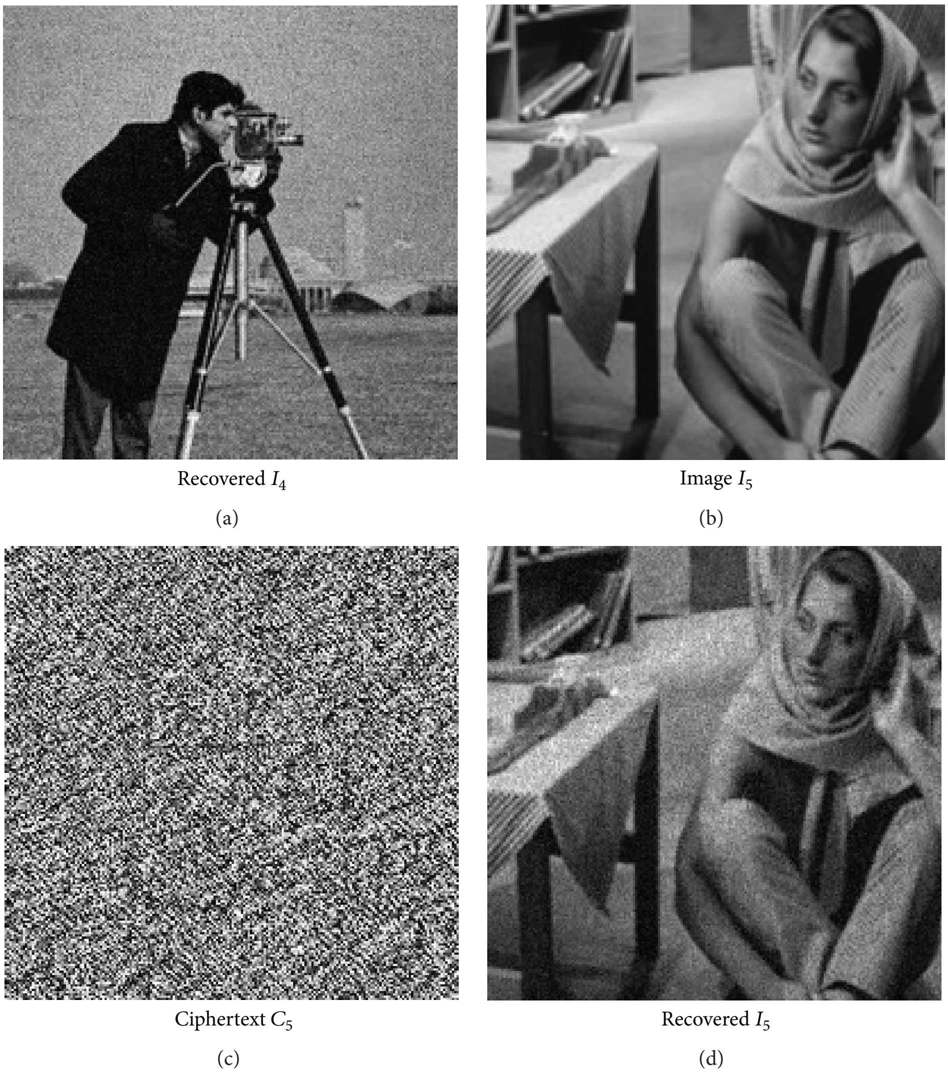
In the above simulation experiment, we have completed the key transmission for the DRPE system and can restore the original image using the obtained key P_2'.

The above step indicates the feasibility of our proposed key distribution scheme, but the quality of the decrypted image depends on the phase P_2'. Further, when the CC takes the different value, Alice will get the phase P_2' of the different quality which is used to decrypt the ciphertext (Figure 6(b)); the results are shown in Figure 8.

From the analysis of Figure 8 we can see that the closer to 1 the value of CC is, the better the quality of the key transmission is. Though it is time-consuming, it is worth spending more time to transmit a good key for the cryptosystem.

5. Changing Key Cryptosystem

We propose an asymmetric cryptosystem of changing key, and the advantage of the system is that users can change key at any time (they even can use a different key in every


Recovered I_4

(a)

Image I_5

(b)

Ciphertext C_5

(c)

Recovered I_5

(d)

FIGURE 14: (a) Alice recovers the image "Man"; (b) the image I_4; (c) ciphertext C_5; (d) Alice recovers the image "Babar."

encryption process). Thus, the security of the system is greatly improved. The communication protocol is shown in Figure 9.

The basic principle is as follows:

(1) The public key $k_{\text{pub}}(e, n, I)$ was public, while the private key $k_{\text{pr}}(d, I)$ was reserved by Alice.

(2) Bob wants to send image I_1 to Alice and can use the public key $k_{\text{pub}}(e, n, I)$ to encrypt the image I_1; the process is shown in Figure 2.

(3) Alice receives the ciphertext C_1 from Bob and then uses her private key to decrypt the ciphertext and obtains the image I_1; the process is shown in Figure 3.

(4) Next, Bob can use the key $k_{\text{pub}}(e, n, I_1)$ to encrypt image I_2.

(5) Alice receives the ciphertext C_2 and then uses the key $k_{\text{pr}}(d, I_1)$ to decrypt the ciphertext C_2 and obtains the image I_2.

The encryption scheme of changing key conforms to the basic agreement of asymmetric cryptosystem. Its characteristic is that the sender can change the key at any time and the receiver can use their existing recovery plaintext for decryption.

6. Simulation Analysis

(1) The public key ($e = 21746071, n = 68585227$) and the private key ($d = 62065831$) are obtained by RSA algorithm; at the same time an image I is opened (Figure 10(a)).

(2) Bob wants to send image I_1 to Alice and can use the opened image I and the public key (e, n) to encrypt the image I_1, as shown in Figures 10(b) and 10(c).

(3) Alice receives the ciphertext C_1 from Bob and then uses her private key (d) and the image I to decrypt the ciphertext C_1 and obtains the image "Baboon" (Figure 11(a)).

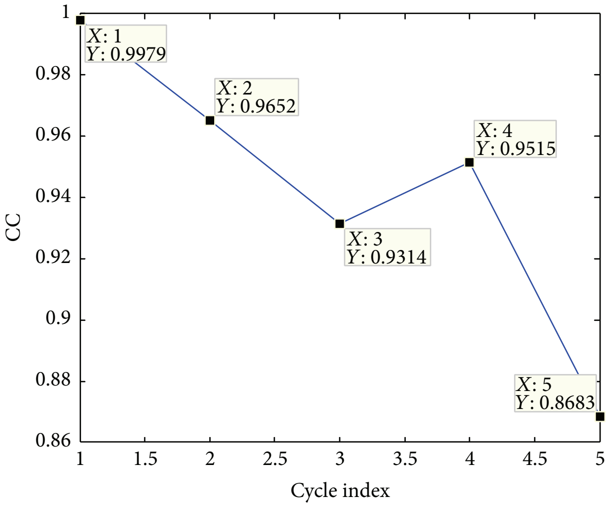


FIGURE 15: Correlation coefficient curve of cycle index.

(4) Next, Bob uses the image I_1 and the public key to encrypt the image I_2, as shown in Figures 11(b) and 11(c).

(5) Alice receives the ciphertext C_2 and then uses her private key and the recovered image I_1 for decryption and obtains the image "Lena" (Figure 12(a)).

(6) Next, Bob uses the image I_2 and the public key to encrypt the image I_3, as shown in Figures 12(b) and 12(c).

(7) Alice receives the ciphertext C_3 and then uses her private key and the recovered image I_2 for decryption and obtains the image "Man" (Figure 13(a)).

(8) Next, Bob uses the image I_3 and the public key to encrypt the image I_4, as shown in Figures 13(b) and 13(c).

(9) Alice receives the ciphertext C_4 and then uses her private key and the recovered image I_3 for decryption and obtains the image "Cameraman" (Figure 14(a)).

(10) Next, Bob uses the image I_4 and the public key to encrypt the image I_5, as shown in Figures 14(b) and 14(c).

(11) Alice receives the ciphertext C_5 and then uses her private key and the recovered image I_4 for decryption and obtains the image "Babar" (Figure 14(d)).

As cycle index increases, the correlation coefficient curve gradually declines in Figure 15. In the fifth cycle, correlation coefficient reaches its lowest point and the corresponding image contrast is shown in Figures 14(b) and 14(d). In Figure 14(d) there is the large noise in the decrypted images, so it is necessary to use the image I as the encryption key in the next encryption process, and the cycle renews.

7. Conclusion

In this paper, we propose a key distribution scheme based on phase retrieval algorithm and RSA public-key algorithm, which solves the problem that it is not easy to distribute due to overloaded key data in optical cryptosystem. Furthermore, we propose an image encryption system of changing key. The advantages are that the security of the system is guaranteed and users can change key at any time, which greatly protect users from economic loss.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the editor and reviewers for their valuable comments on the paper. Those comments are helpful and have an important guiding significance to their research.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[2] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887–889, 2000.

[3] G. H. Situ and J. J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, vol. 29, no. 14, pp. 1584–1586, 2004.

[4] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express*, vol. 15, no. 24, pp. 16067–16079, 2007.

[5] Y. Sheng, Z. Xin, M. S. Alam, L. Xi, and L. Xiao-feng, "Information hiding based on double random-phase encoding and public-key cryptography," *Optics Express*, vol. 17, no. 5, pp. 3270–3284, 2009.

[6] E. Pérez-Cabré, M. J. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Optics Letters*, vol. 36, no. 1, pp. 22–24, 2011.

[7] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Optics Letters*, vol. 38, no. 17, pp. 3198–3201, 2013.

[8] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Optics Letters*, vol. 35, no. 2, pp. 118–120, 2010.

[9] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Optics Letters*, vol. 30, no. 13, pp. 1644–1646, 2005.

[10] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Optics Express*, vol. 14, no. 8, pp. 3181–3186, 2006.

[11] G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," *Applied Optics*, vol. 46, no. 22, pp. 5257–5262, 2007.

[12] X. Wang and D. Zhao, "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in

Fourier domain," *Optics Communications*, vol. 284, no. 1, pp. 148–152, 2011.

[13] X. G. Wang and D. M. Zhao, "Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval," *Optics Communications*, vol. 284, no. 19, pp. 4441–4445, 2011.

[14] W. Chen and X. Chen, "Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain," *Optics Communications*, vol. 284, no. 16-17, pp. 3913–3917, 2011.

[15] W. Chen and X. D. Chen, "Optical asymmetric cryptography using a three-dimensional space-based model," *Journal of Optics*, vol. 13, no. 7, Article ID 079601, 2011.

[16] S. K. Rajput and N. K. Nishchal, "Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain," *Applied Optics*, vol. 52, no. 18, pp. 4343–4352, 2013.

[17] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," *Applied Optics*, vol. 51, no. 10, pp. 1446–1452, 2012.

[18] I. Mehra, S. K. Rajput, and N. K. Nishchal, "Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification," *Optical Engineering*, vol. 52, Article ID 028202, 6 pages, 2013.

[19] I. Mehra and N. K. Nishchal, "Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding," *Optics Express*, vol. 22, no. 5, pp. 5474–5482, 2014.

[20] X. G. Wang, D. M. Zhao, and Y. X. Chen, "Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask," *Applied Optics*, no. 23, pp. 5100–5108, 2014.

[21] W. Liu, Z. Liu, J. Wu, and S. Liu, "Asymmetric cryptosystem by using modular arithmetic operation based on double random phase encoding," *Optics Communications*, vol. 301-302, pp. 56–60, 2013.

[22] W. Liu, Z. J. Liu, and S. T. Liu, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm," *Optics Letters*, vol. 38, no. 10, pp. 1651–1653, 2013.

[23] S. K. Rajput and N. K. Nishchal, "Fresnel domain nonlinear optical image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm," *Applied Optics*, vol. 53, no. 3, pp. 418–425, 2014.

[24] T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography," *Optics and Lasers in Engineering*, vol. 72, pp. 12–17, 2015.

[25] W. Q. He, X. F. Meng, and X. Peng, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment," *Optics Letters*, vol. 38, no. 20, p. 4044, 2013.

[26] C. Zhang, W. He, J. Wu, and X. Peng, "Optical cryptosystem based on phase-truncated Fresnel diffraction and transport of intensity equation," *Optics Express*, vol. 23, no. 7, pp. 8845–8854, 2015.

[27] X. G. Wang, W. Chen, and X. D. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," *Optics Express*, vol. 23, no. 5, pp. 6239–6253, 2015.

[28] J. J. Cai, X. J. Shen, M. Lei, C. Lin, and S. F. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Optics Letters*, vol. 40, no. 4, pp. 475–478, 2015.

[29] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[30] T. Zhao, Q. Ran, and Y. Chi, "Image encryption based on nonlinear encryption system and public-key cryptography," *Optics Communications*, vol. 338, pp. 64–72, 2015.