Optics Communications 335 (2015) 205–211

Contents lists available at ScienceDirect

Optics Communications

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

Multiple-image encryption based on optical asymmetric key cryptosystem

Wei Liu [a], Zhenwei Xie [a], Zhengjun Liu [b], Yan Zhang [c], Shutian Liu [a,*]

[a] Department of Physics, Harbin Institute of Technology, Harbin 150001, China
[b] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China
[c] Department of Physics, Capital Normal University, Beijing 100048, China

ARTICLE INFO

Article history:
Received 10 July 2014
Received in revised form
29 August 2014
Accepted 16 September 2014
Available online 26 September 2014

Keywords:
Multiplexing encryption
Optical asymmetric key cryptosystem
Optical experiments demonstration

ABSTRACT

We propose a multiple-image encryption scheme with asymmetric keys and demonstrate it by optical experiments. The original secret images are multiplexed and encoded into a real-valued ciphertext using only one public encryption key. In the decryption process, each secret image can only be de-multiplexed by its corresponding private decryption key. The multiplexing capacity is analyzed through examining the distribution of cross-talk noise and the key space of private decryption key. Numerical simulations and optical experiments have been carried out to demonstrate the validity, high security, and large multiplexing capacity of the proposed method.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Optical information security has attracted much attention owing to its power of high-speed and parallelism [1], especially in the area of high-density information security [2]. During the past decade, many optical or digital multiplexing operations have been proposed for multiple-image encryption [3–13], which also stimulate the generation of a new research area, i.e., optical movie encryption [10,11]. Basically, the reported multiplexing encryption methods belong to the symmetric key cryptosystems, which use the same keys for encryption and decryption. However, if potential attackers have access to the encryption implementations, such symmetric encoding strategies could provide additional useful resources for attacks. That can result in security vulnerabilities. A simple example to demonstrate the fact can be easily given; that is, if attackers can generate several pairs of plaintext and ciphertext through the encryption implementations, the traditional double random phase encoding (DRPE) [14] could be easily deciphered by chosen and known plaintext attacks [15–17].

Recently, several exploited security systems using optical asymmetric key cryptosystem (OAKCS) have been reported [18–24] and examined [25,26]. These novel encryption methods greatly enhance the security against the existing chosen and known plaintext attacks, mainly for the reason that the decryption keys can be different in each encoding. In addition, nonlinear encryption is achieved by OAKCS [27], which makes the security system more reliable. Despite the above advantages, as we know, it is argued now that 'asymmetric' is not properly used to describe such optical encryption schemes [28]. Since it is hard to optically implement the general mathematical-puzzles-based asymmetric cryptography, the definition and implementation of asymmetric cryptosystem cannot be the same as those in electronic area. A short discussion to refute the argument of just follow exactly the terminology structures, and algorithms of general cryptography is given in [29], and a more detailed discussion to support the view can be seen in [30]. These discussions make a sense that true asymmetric cryptography comes from electronic code but basic concepts can be borrowed from cryptography for optical security.

In fact, as the decryption key differs from the encryption key, the feature of OAKCS is just opposite to the symmetric key cryptosystems. According to the key structures of encryption and decryption, the asymmetric concept is absolutely suitable for describing such optical encryption schemes, and accordingly 'asymmetric key cryptosystem' is used for emphasizing such kind of key structure herein. Due to the special key structure of OAKCS, through constructing an appropriate algorithm, the raised multiplexing encryption can be achieved using only one public key, while de-multiplexing is able to be implemented by different private keys.

In this paper, we propose, analyze and demonstrate an OAKCS algorithm for multiple-image encryption application. In our scheme, the secret images are encoded and multiplexed by the same public key with employing summation and normalization operations, and the final multiplexing encryption result is obtained in real-valued distribution. After the multiplexing encoding, each secret image corresponds to a unique private decryption key. The decryption

* Corresponding author. Tel.: +86 451 86418042.
E-mail address: stliu@hit.edu.cn (S. Liu).

http://dx.doi.org/10.1016/j.optcom.2014.09.046
0030-4018/© 2014 Elsevier B.V. All rights reserved.

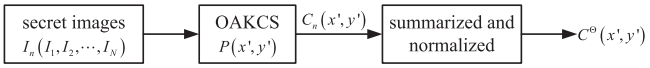

Fig. 1. The block diagram of the encryption process.

process can be simply implemented by two spatial liquid modulators (SLMs) and optical experiments are carried out to demonstrate it. Necessary simulations are carried out to analyze the multiplexing capacity.

2. Principle of the proposed multiple image encryption method

The diffraction-based OAKCS is taken as an example to describe the principle, and accordingly derivative schemes based on other optical transforms can be directly derived. The encryption process is illustrated in Fig. 1. Let $I_n(x,y)$ $(n=1,2,\ldots,N)$ denote the amplitude of one secret image to be encrypted, and N is the total number of secret images. The secret image $I_n(x,y)$ is first encoded by the public random phase key $P(x',y')$ based on OAKCS [23] using the modified Yang–Gu amplitude–phase retrieval algorithm [31], and the relationship between the ciphertext and the plaintext is described by the following equation:

$$C_n(x',y')P(x',y') = \mathrm{IFrT}^z\{I_n(x,y)\exp[\mathrm{i}\phi_n(x,y)]\}, \tag{1}$$

where z indicates the diffraction distance, $C_n(x',y')$ denotes the first-step real-valued encoding result, and $\phi_n(x,y)$ represents the unknown random phase which serves as an intermediate arithmetic variable. $C_n(x',y')$ and $\phi_n(x,y)$ need to be retrieved. The diffraction process is computed by Fresnel transform (FrT^z), and IFrT^z denotes its inversion.

To solve the above phase retrieval problem, it is mandatory to ensure that the energy conservation law is satisfied between the two transform planes. Therefore, before introducing the iterative calculation process, the detailed definitions of the unitary operator pairs FrT and IFrT are discussed first. Let unitarity is assumed to be satisfied, then Eq. (1) can be rewritten as

$$\mathrm{FrT}^z\{C_n(x',y')P(x',y')\} = I_n(x,y)\exp[\mathrm{i}\phi_n(x,y)]. \tag{2}$$

The left side of Eq. (2) points out the Fresnel transform (FrT^z) which is defined as [32]

$$\begin{aligned}\mathrm{FrT}^z\{C_n(x',y')P(x',y')\} &= [C_n(x',y')P(x',y')] \otimes h(x',y',z)\\ &= \mathrm{IFT}[\mathrm{FT}\{C_n(x',y')P(x',y')\}\mathrm{FT}\{h(x',y',z)\}],\end{aligned} \tag{3}$$

where '$\otimes$' indicates convolution, FT and IFT indicate Fourier transform and inverse Fourier transform, respectively, and $h(x',y',z)$ denotes the point pulse function given by

$$h(x',y',z) = \frac{\exp(2\mathrm{i}\pi z/\lambda)}{\mathrm{i}\lambda z}\exp\left\{\frac{\mathrm{i}\pi}{\lambda z}(x'^2+y'^2)\right\}, \tag{4}$$

where λ is the wavelength. According to Eqs. (2) and (3), the complex output of Eq. (1) is obtained by performing the following computing:

$$C_n(x',y')P(x',y') = \mathrm{IFT}\left\{\frac{\mathrm{FT}\{I_n(x,y)\exp[\mathrm{i}\phi_n(x,y)]\}}{\mathrm{FT}\{h(x',y',z)\}}\right\}. \tag{5}$$

Consequently, the inverse Fresnel transform (IFrT) is defined as

$$\mathrm{IFrT}^z\{I_n(x,y)\exp[\mathrm{i}\phi_n(x,y)]\} = \mathrm{IFT}\left\{\frac{\mathrm{FT}\{I_n(x,y)\exp[\mathrm{i}\phi_n(x,y)]\}}{\mathrm{FT}\{h(x',y',z)\}}\right\}. \tag{6}$$

Thus we get a pair of unitary operators which are indicated by Eqs. (3) and (6), respectively.

The digital iterative calculation process of encoding each secret image is shown in Fig. 2, which employs a modified Yang–Gu amplitude–phase retrieval algorithm in Fresnel domain [31]. In the initialization, the unknown first-step encoding result $C_n^{(0)}(x',y')$ is set

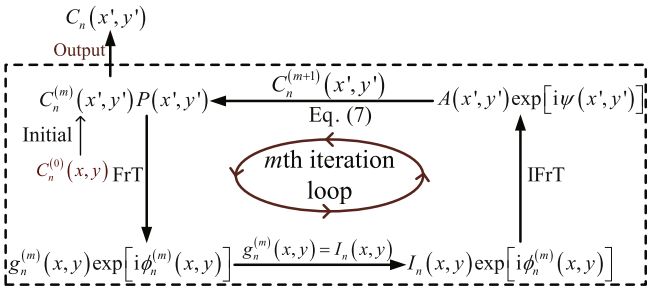

Fig. 2. The mth iterative process of the modified Yang–Gu algorithm.

to be randomly generated in the interval [0,1]. The iterative process can be summarized in the following five steps: (1) compute the diffraction output distribution using the public phase $P(x',y')$ and the estimated $C_n(x',y')$; (2) substitute the obtained amplitude $g_n^{(m)}(x,y)$ with $I_n(x,y)$ as the new diffraction output; (3) obtain the inverse complex diffraction input $A(x',y')\exp[\mathrm{i}\psi(x',y')]$; (4) update the first-step real-valued encoding result $C_n(x',y')$ by

$$C_n^{(m+1)}(x',y') = \mathrm{Re}\{A(x',y')\exp[\mathrm{i}\psi(x',y')]P^*(x',y')\}, \tag{7}$$

where 'Re' represents the operation of computing the real part and $P^*(x',y')$ is the complex conjugate of $P(x',y')$; (5) repeat the above three steps until the predefined precision is achieved. Here we use the correlation coefficient (CC) as a convergence criteria, which is given by

$$CC = \frac{\mathrm{cov}\{g_n^{(m)}(x,y), I_n(x,y)\}}{\sigma_{g_n^{(m)}}\sigma_{I_n}}, \tag{8}$$

where $\mathrm{cov}\{g_n^{(m)}(x,y), I_n(x,y)\}$ indicates the covariance between $g_n^{(m)}(x,y)$ and $I_n(x,y)$, $\sigma_{g_n^{(m)}}$ and σ_{I_n} are their standard deviations. Generally, $CC=0.99$ is large enough to ensure the quality of the recovery images. The iteration stops for the final $C_n(x',y')$ when CC or iterative number reaches the pre-set threshold value.

According to the above described encryption method, each secret image is encoded using the same public phase key. The corresponding unique private key (PK) is simultaneously generated by

$$\mathrm{PK}_n(x',y') = \begin{cases}\pi & \text{if } C_n(x',y') \le 0\\ 0 & \text{if } C_n(x',y') > 0.\end{cases} \tag{9}$$

The PK will be used for generating the private decryption key through employing a binary phase modulation [23]. The final multiplexing encryption result is obtained by summation as

$$C(x',y') = \sum_{n=1}^{N} |C_n(x',y')|. \tag{10}$$

The ciphertext $C(x',y')$ must be normalized into the grayscale interval [0,255], for the reason that it can be displayed by an amplitude-type SLM in an optical implementation. We define the final ciphertext $C^{\Theta}(x',y')$ as

$$C^{\Theta}(x',y') = \frac{255C(x',y')}{\max\{C(x',y')\}}, \tag{11}$$

where $\max\{C(x',y')\}$ indicates the maximum matrix element in $C(x',y')$.

The private decryption keys (DKs) are obtained by performing binary phase modulations to the public key. They are given by

$$\mathrm{DK}_n(x',y') = P(x',y')\exp[\mathrm{i}\ \mathrm{PK}_n(x',y')]. \tag{12}$$

Fig. 3 illustrates the simple decryption process, which can be implemented digitally or optically. The operator 'PT' denotes phase truncation, and '$\times$' is the symbol of multiplication. As shown in Fig. 3, each secret image can be retrieved by its correct decryption

key, and the corresponding decryption result is represented as

$$I_n(x,y) = |\mathrm{FrT}^z\{C^{\Theta}(x',y')\mathrm{DK}_n(x',y')\}|, \tag{13}$$

which implicatively tells a fact that the key space of the private key (PK) can determine the ultimate multiplexing capacity.

Through examining Eqs. (10)–(13), the cross-talk noise (CTN) generated in the decryption process is calculated by

$$\mathrm{CTN} = \sum_{k \neq n}^{N} \mathrm{FrT}^z\{|C_k|P \exp[\mathrm{i}\ \mathrm{PK}_n]\}, \tag{14}$$

where the coordinates are omitted for simplicity. Since $|C_k|$ is mainly dependent on the corresponding individual secret image and randomized by ϕ_k [see Eq. (1)], in a certain extent, Eq. (14) can be approximately equal to the convolution of the sums of mutually independent random variables [see Eq. (3)]. In probability theory, the Central Limit Theorem tells that the sum of a large number of independent random variables will tend to be distributed according to the Gaussian distribution [33]. From this point of view, the generated CTN will appear as Gaussian-like distributed noise and thus has no meaningful information, especially when number N is very large. By considering the fact that statistically randomly distributed noise can be suppressed by employing some linear filtering methods, the quality of the decrypted images can be ensured after filtering, which implies that the multiplexing capacity is expected to be very huge. Simulations and optical experiments will give a convincing demonstration in the following section.

Fig. 3. The block diagram of the decryption process.

Fig. 4. The original grayscale images to be encoded and multiplexed.

3. Numerical simulations and optical experiments

3.1. Numerical simulations

In this subsection, numerical results are presented to show the feasibility of our proposal. The standard grayscale test images [34] chosen for numerical simulations are shown in Fig. 4, each has a size of 256 × 256 pixels. Nine images are taken in the simulations for a comparison with the previous reports in terms of multiplexing capacity. Unlike the wavelength or position multiplexing in Fresnel domain, the wavelength λ and the diffraction distance z here are fixed and opened. Hence the optical implementation will be simpler for decryption. The distance z is set as z=0.30 m, and the wavelength is fixed as λ=632.8 nm.

The public random phase key $P(x',y')$ is generated by $P(x',y') = \exp[\mathrm{i}2\pi a(x',y')]$. $a(x',y')$ denotes an independent white sequence uniformly distributed in [0,1], and its angle distribution is illustrated in Fig. 5(a). The final real-valued multiplexing encryption result obtained by Eq. (11) is shown in Fig. 5(b), and it appears in the form of random white noise. In the simulations, the threshold value of CC is set as CC=0.99, and the corresponding iteration numbers for the secret images are given as 60 ('Lena'), 82 ('Cameraman'), 81 ('Plane'), 69 ('Boat'), 67 ('Baboon'), 62 ('Barbara'), 62 ('Elaine'), 64 ('Peppers'), and 57 ('Rice'). Here in, the iterative number is chosen as 300 for each secret image to obtain a higher precision. Taking 'Lena' as an example, the curve of CC versus the iterative number is plotted in Fig. 6. It can be seen that the recovery quality of the secret image is quite good by employing the iterative encoding algorithm.

The decrypted images using correct private decryption keys are shown in Fig. 7(a), which are retrieved with cross-talk noise and thus look blurred. The mean correlation coefficient is obtained as

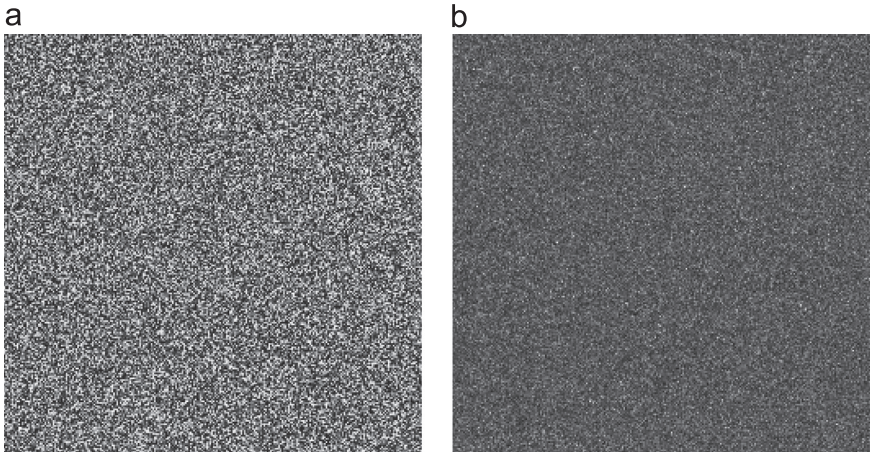

Fig. 5. Numerical simulation results of (a) public phase key and (b) multiplexing encryption image.

$\overline{CC} = 0.526$. As we have discussed in Section 2, a large N will tend to a Gaussian-like CTN. Therefore, Gaussian low-pass filtering is employed to improve the image quality. The filtering kernel function is given by

$$K(x,y) = \frac{1}{2\pi\delta^2}\exp\left(-\frac{x^2+y^2}{2\delta^2}\right), \tag{15}$$

where δ is the width parameter. The filtered decrypted images are shown in Fig. 7(b). The quality ($\overline{CC_f} = 0.91$) of the decrypted images is much improved and can be clearly recognized even though there are still some noise. To see the influence of the key space for the multiplexing capacity, the retrieval accuracy is analyzed using different key sizes, as shown in Table 1. For an image with $M \times N$ pixels, the theoretical key space can be given by $2^{M\times N-1}$, for the reason that each binary modulation leads to a new comprise of decryption key. Table 1 clearly shows that a larger key space will result in a larger multiplexing capacity.

In addition, the sensitivity of the decryption keys is checked by a test which uses different percentages of the correct key for decryption. We calculate the recovery image quality of each adopted percentage to show the result. The numerical values are presented in Table 2. Note that the recovery image is unrecognizable while $CC = 0.113$, the exploited security system can be stable even if 50% of the correct decryption key is known by unauthorized attackers. However, a blurry outline of the secret image can be recognized when 75% is known for decryption. This result does not mean that the security level is low, because it is extremely difficult for any attacker to get 75% of the correct decryption key due to the large key space. Consequently, a high sensitivity of the decryption keys is obtained.

The correlation coefficient versus the number of encrypted images N is plotted in Fig. 8, which can tell the true multiplexing capacity. It can be seen that the decreasing of CC, in both cases of with and without Gaussian low-pass filtering, tends to stagnate with the increasing of the number of encrypted images, especially in the case of $N \geq 7$. The results can be attributed to the fact that the generated CTN is close to a statistical random distribution in a large multiplexing number. To our knowledge, if an image is polluted by statistically randomly distributed noise, its quality would only reduce about 50% and much useful information could still be recognized. In other words, the generated CTN has an impact cap for image quality despite the multiplexing number, which is just demonstrated by the two curves. We also perform another numerical simulation to check the theory using a movie which includes 92 grayscale frames (126×194 pixels). The mean

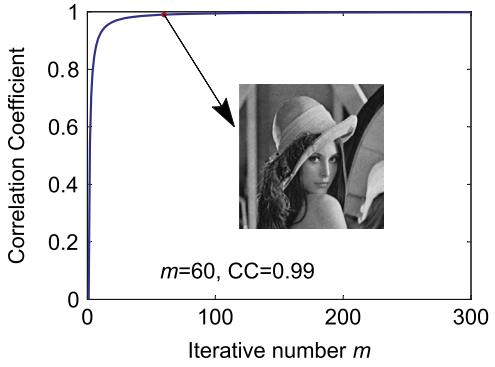

Fig. 6. The curve of CC versus the iterative number.

Table 1
Recovery accuracy versus the key space.

Key size	256×256	128×128	64×64	32×32
$\overline{CC}$	0.526	0.511	0.498	0.481
$\overline{CC_f}$	0.910	0.877	0.816	0.751

Table 2
Recovery accuracy versus the adopted percentage of the decryption key.

Percentage (%)	0	25	50	75	100
$\overline{CC}$	0.003	0.031	0.113	0.248	0.526

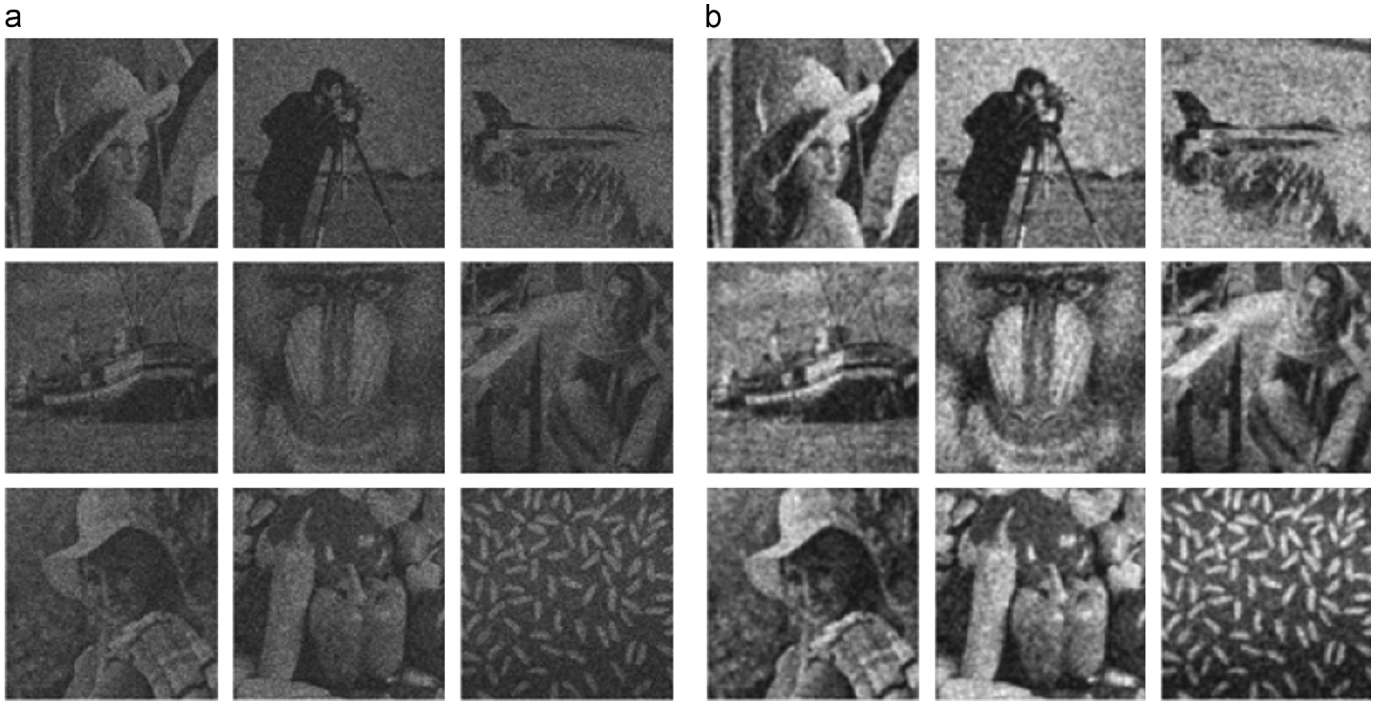

Fig. 7. Numerical simulation results of (a) decrypted images without filtering and (b) decrypted images after filtering.

correlation coefficient of the filtered decryption images ($N=92$) is obtained as $\overline{CC_f}=0.92$. All the above results just tell that a very large multiplexing capacity is obtained by our method.

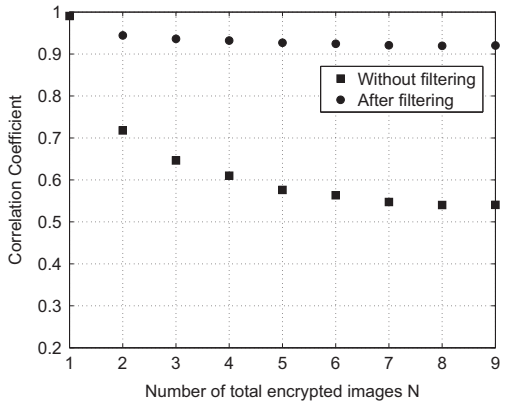

Fig. 8. The curve of correlation coefficient versus the number N of encrypted images.

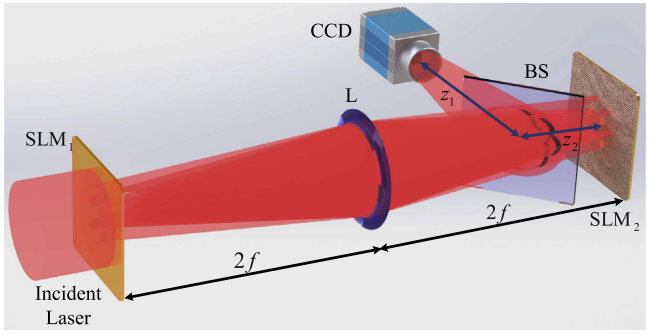

Fig. 9. Optical experimental setup for decryption. SLM, spatial light modulator; BS, beam splitter; L, lens; CCD, CCD camera. The ciphertext is displayed by the amplitude-only SLM_1, and the decryption phase keys are displayed by the phase-only SLM_2.

3.2. Optical experiments

Optical experiments are also carried out to make the proposal more convincing. The optical setup for decryption is illustrated in Fig. 9. In the experiments, the system is illuminated by a parallel coherent beam generated by He–Ne laser ($\lambda=632.8$ nm). Two computer-controlled SLMs are used to display the ciphertext (encryption result) and the decryption keys, respectively. Since the display of an SLM is always packed in a large frame to protect the fragile surface, it is not easy to make two SLMs closely attached [see Eq. (13)]. Therefore, the 4f lens imaging system is employed to solve this technical problem by projecting the ciphertext onto the decryption key. The focal length of the lens is $f=10$ cm. The ciphertext C^{Θ} is displayed by a transmissive amplitude-only SLM_1 (Holyeye LC2002) with 800×600 pixels and 32 μm pixel pitch, and the reflective phase-only SLM_2 (Holyeye Pluto1080P) with 1920×1080 pixels and 8 μm pixel pitch is used for displaying the decryption phase keys. The distances of the center of the beam splitter (BS) between the CCD camera and SLM_2 are z_1 and z_2, respectively. In the decryption process, each decrypted image is detected by a CCD camera (PCO Pixelfly, 12bit) with 1392×1024 pixels and 6.45 μm × 6.45 μm pixel area in the predefined diffraction distance z ($z=z_1+z_2=30$ cm).

Though the optical process of the decryption is very clear, additional noise will be introduced in experiments by technical problems, e.g., the problem of coherent noise, the alignment between elements, and the grating and aperture effects of the SLMs. Despite these difficulties, we successfully demonstrate the proposal in experimental work. In experiments, the nine original images to be multiplexed are designed as binary alphabet images for simplicity. They are shown in Fig. 10(a), each image has a size of 300×300 pixels. The corresponding detected decryption results using correct DKs are shown in Fig. 10(b), which can be clearly recognized without any filtering.

The security is also examined by experiments using different trial keys for decryption. The decoded image using the public phase key (public key attack) is illustrated in Fig. 11(a), which is nothing but random white noise. This result tells that original

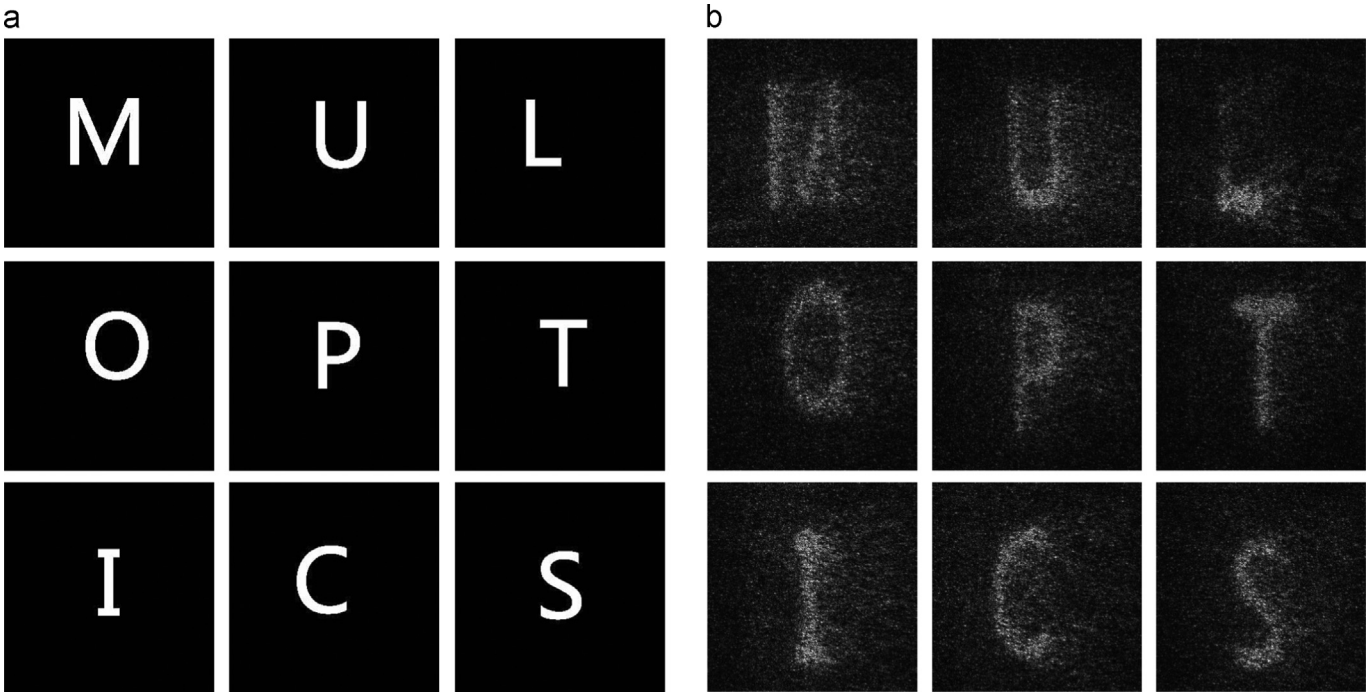

Fig. 10. The simulation results of (a) the designed original images used for experiments and (b) the corresponding experimental decrypted images using correct private decryption keys.

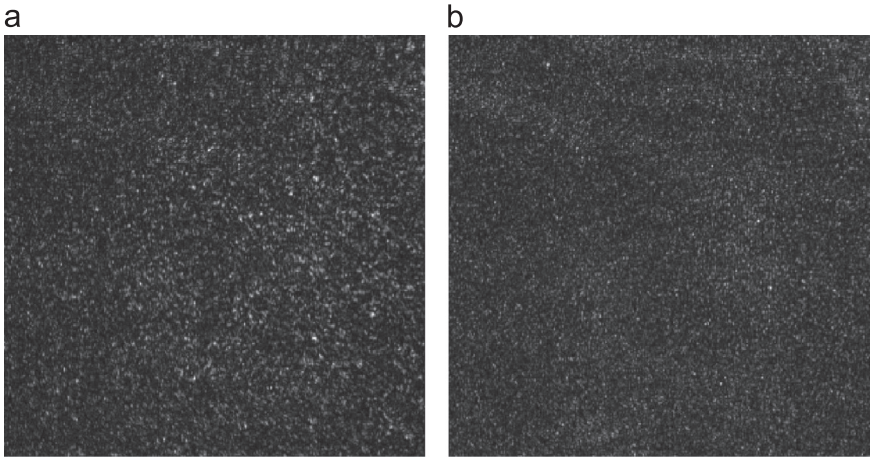

Fig. 11. Experimental results of the decryption using (a) public phase key and (b) random phase key.

secret images cannot be deciphered even the encryption key is known by attackers. Furthermore, suppose that the binary modulation (0 and π) is known by attackers, naturally one can perform brute-force attack using some random binary matrices as private keys to decipher the system. In this test, the corresponding decoded result is shown in Fig. 11(b). Obviously, the brute-force attack also failed to decipher the original information. In addition, since each secret image corresponds to a unique private decryption key, attackers cannot construct any effective retrieval algorithm to reproduce the random phase code [23], as a result, the existing reported attacks are also invalid to our cryptosystem [15–17,35].

3.3. Discussion

Compared with our previous work [23], experimental demonstration and multiplexing encryption are performed. To our knowledge, although there have been some other reported schemes for OAKCS [18–24], most of them concern encrypting a single image and have no experimental demonstration. We successfully carry out the optical experiments by solving the technical problems, though some speckle noise is still introduced in the experimental results. Compared with some existing multiple image encryption schemes [2,5,8–10], the quality of the decrypted images here may be not so perfect, however, a larger multiplexing capacity and a simpler optical realization are achieved simultaneously. Therefore, the presented security system can be more suitable for some real applications, such as multi-identity authentication.

To improve the quality of the decryption images, Gaussian low-pass filtering method is employed to reduce the Gaussian-like CTN. Although that is not the major task of our research, a little more discussion in the area of noise filtering is presented. To our knowledge, other linear filtering methods [36], e.g., smooth filtering and Wiener filtering, can also be useful to suppress such statistically distributed noise, but a similar retrieval accuracy is obtained. Therefore, modified or new filtering methods are required. That issue can be real complex, however, further investigations will be carried on in the future.

4. Conclusion

To summarize, we have introduced an optical multiple-image encryption method with asymmetric keys based on OAKCS. The proposed multiplexing encryption scheme obtains a real-valued ciphertext using only one public key and designs asymmetric keys for decryption. In the decryption process, each original image can only be de-multiplexed by its corresponding private decryption key. Gaussian low-pass filtering is employed to suppress the cross-talk noise to improve the recovery image quality. Simulations and optical experiments have successfully demonstrated the validity, high security, and the large multiplexing capacity. The presented security system is also suggested for optical verification due to its simple optical implementation.

Acknowledgments

This work was supported by the National Basic Research Program of China under Grant no. 2013CBA01702, the National Natural Science Foundation of China under Grant nos. 61377016, 10974039 and 11104049, Specialized Research Fund for the Doctoral Program of Higher education (Grant 20102302120009) and the Program for New Century Excellent Talents in University (NCET-12-0148).

References

[1] B. Javidi, Phys. Today 50 (1997) 27.
[2] A. Alfalou, C. Brosseau, Adv. Opt. Photonics 1 (2009) 589.
[3] G. Situ, J. Zhang, Opt. Lett. 30 (2005) 1306.
[4] G. Situ, J. Zhang, J. Opt. A: Pure Appl. Opt. 8 (2006) 391.
[5] H. Hwang, H. Chang, W. Lie, Opt. Lett. 34 (2009) 3917.
[6] B. Hennelly, T. Naughton, J. McDonald, J. Sheridan, G. Unnikrishnan, D. Kelly, B. Javidi, Opt. Lett. 32 (2007) 1060.
[7] Z. Liu, S. Liu, Opt. Commun. 275 (2007) 324.
[8] S. Soualmi, A. Alfalou, H. Hamam, J. Opt. A: Pure Appl. Opt. 9 (2007) 73.
[9] A. Alfalou, C. Brosseau, Opt. Lett. 35 (2010) 1914.
[10] R. Henao, E. Rueda, J. Barrera, R. Torroba, Opt. Lett. 35 (2010) 333.
[11] F. Mosso, J. Barrera, M. Tebaldi, N. Bolognini, Opt. Express 19 (2011) 5706.
[12] J. Barrera, M. Tebaldi, C. Rios, E. Rueda, N. Bolognini, R. Torroba, Opt. Express 20 (2012) 3388.
[13] J. Barrera, M. Tebaldi, D. Amaya, W. Furlan, J. Monsoriu, N. Bolognini, R. Torroba, Opt. Lett. 37 (2012) 2895.
[14] P. Refrégiér, B. Javidi, Opt. Lett. 20 (1995) 767.
[15] X. Peng, H. Wei, P. Zhang, Opt. Lett. 31 (2006) 3261.
[16] U. Gopinathan, D. Monaghan, T. Naughton, J. Sheridan, Opt. Express 14 (2006) 3181.
[17] P. Kumar, A. Kumar, J. Joseph, K. Singh, Opt. Lasers Eng. 50 (2012) 1196.
[18] W. Qin, X. Peng, Opt. Lett. 35 (2010) 118.
[19] W. Chen, X. Chen, J. Opt. 13 (2011) 075404.
[20] S. Rajput, N. Nishchal, Appl. Opt. 51 (2012) 5377.
[21] S. Rajput, N. Nishchal, Appl. Opt. 52 (2013) 871.
[22] W. Liu, Z. Liu, J. Wu, S. Liu, Opt. Commun. 301–302 (2013) 56.
[23] W. Liu, Z. Liu, S. Liu, Opt. Lett. 38 (2013) 1651.
[24] X. Wang, D. Zhao, Opt. Lett. 38 (2013) 3684.
[25] X. Wang, D. Zhao, Opt. Commun. 285 (2012) 1078.
[26] I. Mehra, S. Rajput, N. Nishchal, Opt. Laser Eng. 52 (2014) 167.
[27] S. Rajput, N. Nishchal, Appl. Opt. 53 (2014) 418.
[28] W. He, X. Meng, X. Peng, Opt. Lett. 38 (2013) 4044.

[29] W. Liu, Z. Liu, S. Liu, Opt. Lett. 38 (2013) 4045.
[30] X. Wang, Y. Chen, C. Dai, D. Zhao, Appl. Opt. 53 (2014) 208.
[31] G. Yang, B. Gu, B. Dong, Theory of the amplitude–phase retrieval in any linear transform system and its applications, in: M.A. Fiddy (Ed.), Inverse Problems in Scattering and Imaging, Proceedings of the Society of Photo-Optical Instrumentation Engineers, vol. 1767, 1992, pp. 457–479.
[32] J. Goodman, Introduction to Fourier Optics, 3rd ed., Roberts & Company, Towson, MD, USA, 2005 (Chapter 4).
[33] From Wikipedia ⟨http://en.wikipedia.org/wiki/Central_limit_theorem⟩.
[34] The USC-SIPI Image Database ⟨http://sipi.usc.edu/database/⟩.
[35] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.
[36] T. Acharya, A. Ray, Image Processing: Principles and Applications, John Wiley & Sons, Hoboken, NJ, USA, 2007 (Chapter 6).