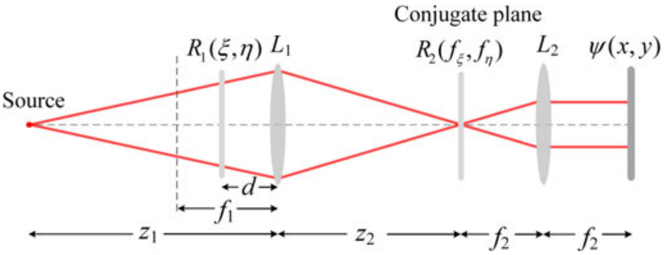
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Optical Image Encryption With Divergent Illumination and Asymmetric Keys

Volume 9, Number 2, April 2017

Xiaogang Wang
Guoquan Zhou
Chaoqing Dai
Junlang Chen



DOI: 10.1109/JPHOT.2017.2684179
1943-0655 © 2016 IEEE

Optical Image Encryption With Divergent Illumination and Asymmetric Keys

Xiaogang Wang, Guoquan Zhou, Chaoqing Dai, and Junlang Chen

School of Sciences, Zhejiang A&F University, Hangzhou 311300, China

DOI:10.1109/JPHOT.2017.2684179

Manuscript received January 4, 2017; revised March 13, 2017; accepted March 15, 2017. Date of publication March 17, 2017; date of current version April 10, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61575178, Grant 61205006, and Grant 11574272 and in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY16A040014. Corresponding author: X. Wang (e-mail: wxg1201@163.com).

Abstract: A flexible optical encryption system based on divergent illumination and asymmetric encoding is proposed. The input image is encrypted by use of two random phase masks (RPMs) located at the input and the conjugate plane in a diverging spherical wave field. Compared with the counterparts using planar illumination and symmetric keys, a significant difference is that continuous change of positions of optical elements applied for encryption is allowed, resulting in decryption keys that are different from the encryption keys (or their conjugates) and variable size display of encrypted/decrypted images. A detailed mathematical description and calculation results with different bandwidths of the system support our proposal.

Index Terms: Optical encryption, optical image reconstruction, image analysis.

1. Introduction

Optical information processing systems have emerged as a very promising means of encryption, securing, and authentication of data [1]–[3]. They can provide a better and safe method for image communication. To retrieve the original optical information at the receiver side, the encryption method and keys are usually required. The double random phase encoding (DRPE) proposed by Refregier and Javidi [4], [5], by far, is one of the most widely used and studied optical encryption techniques, which uses a classical 4-f correlator and two random phase masks (RPMs). In the past decades, it has been combined with the Fresnel transform [6–8], the fractional Fourier transform [9], gyrator transform [10], and phase truncation operations [11]–[14]. To improve security, DRPE has been integrated with other digital or optical imaging techniques such as photon-counting imaging [15]–[17], iterative computational algorithms [18]–[20], and compressive sensing [21], [22].

It can be noticed that the majority of existing schemes of optical image encryption based on random phase encoding at present are under planar illumination. Convergent spherical light has recently been applied for optical encryption [23]; however, the classical coherent 4f imaging system itself didn't have any change except the replacement of the plane wavefront with convergent illumination, where the encryption/decryption key must be fixed in the back focal plane (BFP) of the first lens in the scheme. Another noticeable feature common to those DRPE-based proposals is the use of an identical phase key for both encryption and decryption (or one is for encryption but its conjugate for decryption), which makes the DRPE not secure in some cases [24]. Generally speaking,

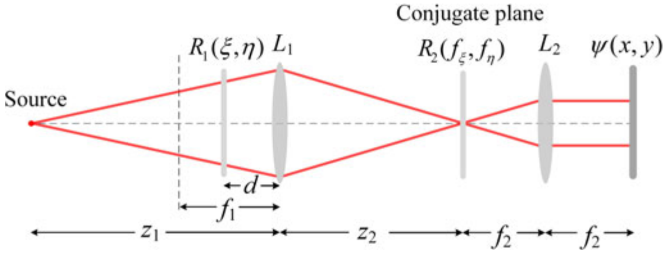


Fig. 1. Schematic setup for asymmetric encryption with divergent illumination. L_1 and L_2 are two lenses. R_1 and R_2 are random phase masks. ψ is the encrypted image.

optical symmetric encryption that uses identical key to encrypt and decrypt image is much faster and less complicated but not as secure as optical asymmetric encryption where the encryption and decryption keys differ [25]. To improve security level, the difference between encryption key and decryption key has been accomplished in phase-truncation Fourier transform based system. However, some of these schemes are found to be vulnerable and crypt analyses is performed on those schemes [26], [27]. The problem of information disclosure has also been proved to be a serious security risk [28]. In addition, a shortcoming of those phase-truncated Fourier-based approaches isthat the nonlinear operations of phase truncation during encryption and decryption processes may make them lose the inherent nature of parallelism of optical security techniques.

In this paper, we describe an optical image encryption based on input plane and conjugate plane random encoding. The optical security system uses divergent illumination and asymmetric keys. Compared with the counterparts with planar illumination, a significant difference is that continuous change of positions of optical elements applied for encryption is allowed, with variable size display of encrypted/decrypted images. It is more flexible, and the additional degrees of freedom makes it more secure. Another remarkable feature of the optical security system is that the decryption key is not identical to encryption key. In addition, we avoid reusing the identical key for decrypting by changing the locations of optical elements, as in a one-time pad approach.

2. Description of Encryption Scheme

The optical system used for coherent optical image encryption is depicted in Fig. 1. In the encryption process, the positive image to be encrypted is placed in the input plane located at a distance d to the left of lens L_1 and illuminated from the left with a spherical wave field of monochromatic light. The source plane and its conjugate are located at distances z_1 and z_2 to the left and right of lens L_1, respectively. We shall assume the setup to be as depicted in the figure: the lens is positive, the source is located to the left of the front focal plane (FFP) of L_1 and its conjugate to the right of the back focal plane (BFP), and the conjugate plane coincides with the FFP of the second lens L_2.

Let $f(\xi,\eta)$ be the primary image to be encrypted, where (ξ,η) are the coordinates of the input plane. The input is modulated by a random phase function $R_1(\xi,\eta)=\exp[j2\pi a(\xi,\eta)]$ where $a(\xi,\eta)$ denotes a white sequences uniformly distributed in $[0,1]$. The analysis required to find the properties of light propagation from source to its conjugate is relatively complex. For more details on these analysis, (see [29]). When only paraxial conditions are considered, the relationship between in the input field $U_0(\xi,\eta)=f(\xi,\eta)R_1(\xi,\eta)$ and the complex amplitude distribution $U(u,v)$ in the conjugate plane is [29]

$$U(u,v)=\frac{z_1\exp\left[jk\frac{(z_1+z_2)d-z_1z_2}{2z_2^2(d-z_1)}\left(u^2+v^2\right)\right]}{j\lambda z_2(z_1-d)} \times\int\int_{-\infty}^{\infty}U_0(\xi,\eta)\exp\left[-j\frac{2\pi z_1(u\xi+v\eta)}{\lambda z_2(z_1-d)}\right]d\xi d\eta. \tag{1}$$

Since z_1, z_2, and the focal length f_1 of the first lens L_1 satisfy the usual lens law, i.e., $z_1^{-1}+z_2^{-1}+f_1^{-1}=0$, the quantity z_1 in (1) can be found in terms of z_2 and f_1. To simplify the expressions, let

$a(u, v) = \frac{(f_1-d)(u^2+v^2)}{2\lambda[(f_1-d)z_2+f_1 d]}$ and $l = \frac{z_2(f_1-d)+f_1 d}{f_1}$, and with these definitions, (1) is rewritten as

$$U(u, v) = \frac{\exp[\,j2\pi a(u, v)]}{j\lambda l} \times \int\int_{-\infty}^{\infty} U_0(\xi, \eta) \exp\left[-j\frac{2\pi}{\lambda l}(u\xi + v\eta)\right] d\xi d\eta \tag{2}$$

where (u, v) are the coordinates of the conjugate plane. Aside from the front exponential term in (2), the field is a Fourier transform of the input complex-amplitude distribution where the frequency variables substitution used for the transform are $f_\xi = u/\lambda l$ and $f_\eta = v/\lambda l$. To encode the spectrum of the input image, another RPM represented by $R_2(f_\xi, f_\eta) = \exp[j2\pi b(f_\xi, f_\eta)]$ is placed in the conjugate plane. Note that $b(f_\xi, f_\eta)$ is a white sequences independent of $a(\xi, \eta)$.

Since the output spectrum $U(u, v)$ of the first part of the security system is located in the FFP of the lens L_2, an exact Fourier transform of the product of the field $U(u, v)$ and the second RPM is performed, whereas the finite extent of the lens aperture is neglected.

$$\psi(x, y) = \frac{\exp(j2kf_2)}{j\lambda f_2} \int\int_{-\infty}^{\infty} U(u, v) R_2\left(\frac{u}{\lambda l}, \frac{v}{\lambda l}\right) \times \exp\left[-j\frac{2\pi}{\lambda f_2}(ux + vy)\right] du dv \tag{3}$$

where the amplitude and phase of the light at the coordinates of the output plane x and y are again related to the amplitude and phase of the input spectrum at frequency $x/\lambda f_2$ and $y/\lambda f_2$, respectively. The constant phase term in the front of integral can be omitted because it doesn't affect the transverse spatial structure of the output distribution. In order to simplify the expressions, all constant phase terms are omitted in the following derivation of integral equations.

We substitute (2) into (3) and perform some necessary algebra. To depict $\psi(x, y)$ as an explicit function of (x, y), we introduce a function $h(u, v)$ by its Fourier transform $\hat{h}(f_\xi, f_\eta) = \exp\{j2\pi[a(\lambda l f_\xi, \lambda l f_\eta) + b(f_\xi, f_\eta)]\}$; therefore, it may be shown that

$$\psi(x, y) = \frac{-l}{f_2} \int\int\int\int_{-\infty}^{\infty} U_0(\xi, \eta)\hat{h}(f_\xi, f_\eta) \times \exp\left\{j2\pi\left[f_\xi\left(\frac{x}{-f_2/l} - \xi\right) + f_\eta\left(\frac{y}{-f_2/l} - \eta\right)\right]\right\} df_\xi df_\eta d\xi d\eta. \tag{4}$$

We now set $m = -\frac{f_2}{l} = -\frac{f_1 f_2}{[z_2(f_1-d)+df_1]}$. Thus, the encrypted image can be given by

$$\begin{aligned}\psi(x, y) &= \frac{1}{m} \int\int\int\int_{-\infty}^{\infty} U_0(\xi, \eta)\hat{h}(f_\xi, f_\eta) \times \exp\left\{j2\pi\left[f_\xi\left(\frac{x}{m} - \xi\right) + f_\eta\left(\frac{y}{m} - \eta\right)\right]\right\} df_\xi df_\eta d\xi d\eta \\ &= \frac{1}{m} \int\int_{-\infty}^{\infty} U_0(\xi, \eta) h\left(\frac{x}{m} - \xi, \frac{y}{m} - \eta\right) d\xi d\eta.\end{aligned} \tag{5}$$

By applying the convolution theorem to (5), the output can also be expressed as a convolution of a function $h'(x, y)$ and a scaled version of the input field $U_0'(x, y)$.

$$\psi(x, y) = h'(x, y) \otimes U_0'(x, y) \tag{6}$$

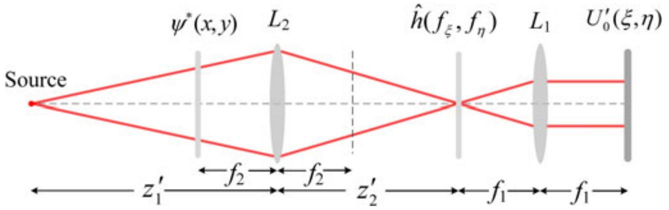


Fig. 2. Optical scheme used for decoding using an asymmetric key.

where the two functions of the right-hand side are given by

$$h'(x, y) = \frac{1}{m^2} h\left(\frac{x}{m}, \frac{y}{m}\right) \tag{7}$$

$$U'_0(x, y) = \frac{1}{m} U_0\left(\frac{x}{m}, \frac{y}{m}\right). \tag{8}$$

It can be found from (8) that $U'_0(x, y)$ is simply the geometrical image field of $U_0(x, y)$ formed by both lenses. The more shorter the focal length of L_2, the more smaller in size the encrypted image. This may be convenient for a size-limited intensity detector to display and record the optically secure data. It can also be found that the resulting encrypted image appears inverted relative to the input image.

3. Decryption of the Encoded Image With an Asymmetric Key

For the illumination, both planar and spherical waves can be used for decryption in the proposed proposal. In this letter, however, we put more emphasize on optical decoding with divergent illumination. To perform the decryption, positions of the two lenses in the encryption scheme should first be interchanged. As shown in Fig. 2, a complex conjugate of the encoded image $\psi^*(x, y)$ is placed in the FFP of L_2 and is illuminated by the spherical wave field emanating from the point source located at a distance z'_1 to the left of the lens L_2. Here, the asterisk denotes a complex conjugate. Note that both the encoded image and its conjugate can be used for decryption, which will be explained in the last paragraph in this section.

Likewise, we assume that the source is located to the left of the FFP of L_2 and its conjugate to the right of the BFP of L_2, and the conjugate plane coincides with the FFP of L_1. For this time, the conjugate plane of the source now locates at z'_2, which satisfies $z'^{-1}_1 + z'^{-1}_2 + f^{-1}_2 = 0$.

As indicated in (2), the quadratic-phase factor preceding the Fourier transform operation $\exp[j2\pi a(u, v)]$ has now vanished when $\psi^*(x, y)$ is placed in the FFP of the lens; therefore, the amplitude distribution in the conjugate plane is given by

$$U'(u, v) = \frac{1}{j\lambda f_2} \int\int_{-\infty}^{\infty} \psi^*(x, y) \exp\left[\frac{-j2\pi(ux + vy)}{\lambda f_2}\right] dxdy. \tag{9}$$

Note that for convenience, coordinates of the input plane, the conjugate plane and the output plane in decryption scheme are now denoted by (x, y), (u, v) and (ξ, η), respectively. Substitute (5) into (9) and perform algebra necessary to find

$$U'(u, v) = \frac{1}{j\lambda l} \int\int_{-\infty}^{\infty} U^*_0(\xi, \eta) \times \exp\left[\frac{j2\pi(ux + vy)}{\lambda l}\right] \hat{h}(f_\xi, f_\eta) dxdy \tag{10}$$

from which we find that the phase function $\hat{h}(f_\xi, f_\eta)$ can be used as key to decode the Fourier spectrum of $U^*_0(\xi, \eta)$ by being placed in the conjugate plane. Compared with the security systems with planar illumination, a significant difference is that the decryption key in this system is no longer just the encryption key $R_2(f_\xi, f_\eta)$ or its conjugate. The decrypted complex amplitude in the output plane may be written as

$$U'_0(\xi, \eta) = \frac{1}{j\lambda f_1} \int\int_{-\infty}^{\infty} U'(u, v)\hat{h}^*(f_\xi, f_\eta) \times \exp\left[-\frac{j2\pi(ux + vy)}{\lambda f_1}\right] dudv. \tag{11}$$

Substituting (10) into (11) and letting $m' = f_1/l$, the decrypted result can be given by

$$U'_0(\xi, \eta) = \frac{1}{m'} U_0^*\left(\frac{\xi}{m'}, \frac{\eta}{m'}\right) \tag{12}$$

which shows that the output field of the decryption scheme is just a scaled copy of the conjugate of the input field in encryption. Likewise, the output field can also be expressed as a convolution of a scaled decryption key function and a scaled copy of the encrypted field. This will not be discussed further. Since the input image is positive, a scale version denoted by function $\frac{1}{m'} f(\frac{\xi}{m'}, \frac{\eta}{m'})$ can be obtained from the intensity data captured by a CCD.

In classical DRPE system, the cypher and the conjugation of encrypting key are used for decryption. However, the conjugation of cypher text and the encrypting key can also be used for decryption [30]. In fact, applying the conjugation of cypher text and using the conjugation of phase key in frequency domain are essentially the same. The only difference is the decrypted image in the former is inverted. Likewise, either of them can be used in our proposal. What should be noted is that the conjugation of the phase key shown in Fig. 2 must be used when the cypher text but not the conjugate of cypher text is applied for decrypting. The proof is left to the reader.

4. Results and Discussion

Some calculations were carried out to demonstrate how the system works under the situation of limitedresources. The basic calculation conditions are as follows: A He-Ne laser with 632.8 nm is used as the coherent light source. The lenses L_1 has a focal length of 250 mm, and L_2 has a focal length of 300 mm. The image to be encrypted has a size of 512 × 512 pixels, which is shown in Fig. 3(a). The sampling interval in the input plane is $8\mu m$. Theoretically, an input image can be encrypted into complex-amplitude stationary white noise with the help of the two RPMs respectively located at the input plane and the Fourier plane [4]. The white noise has an infinite bandwidth. In practice, however, architectures under the framework of DRPE are diffraction-limited security systems, yielding limited-bandwidth encrypted images. The phase masks used for encryption and decrypting with finite size can be made by bleaching gray-scale photographic films of uniformly distributed white sequences or just digitalized and displayed using a spatial light modulator. In the following, we assume that the lens elements are sufficiently large to pass all of the light transmitted by the encryption and decryption keys. In other words, $R_2(u, v)$ and $\hat{h}(f_\xi, f_\eta)$ are the limiting elements of the proposed security system.

The distance parameters of the first half of this security system chosen for encryption of Fig. 3(a) are $z_1 = 700$ mm, $d = 60$ mm and $z_2 = 280$ mm. The output image resulting from a system with bandwidth of 50 × 50 pixels (corresponding to the stop size of 2.0 mm × 2.0 mm) is shown in Fig. 3(b). The decrypted image without using any decryption key is illustrated in Fig. 3(c), which has correlation coefficient (CC) value of −0.009. The correctly decrypted image corresponding to Fig. 3(b) is shown in Fig. 3(d) with CC value of 0.653, where that the outcome is polluted by the speckle noise due to the limited space–bandwidth product of the system resulting from the finite size and limited number of pixels of the RPMs.

To improve the quality of the recovered image, we then encrypted the original with larger cutoff frequencies. The encrypted image with a system bandwidth of 100 × 100 pixels is demonstrated in Fig. 4(a) and the corresponding decrypted image is shown in Fig. 4(b) with the corresponding CC value of 0.676. Fig. 4(c) and (d) are the resultant encrypted and decrypted images of Fig. 3(a)

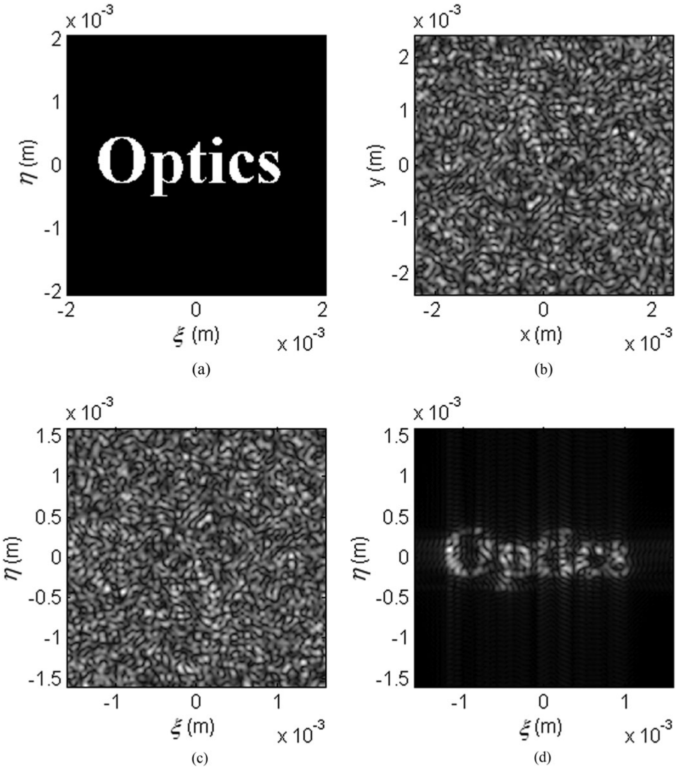


Fig. 3. Calculation results with limited-bandwidth systems. (a) Original image of Optics. (b) Encrypted image with a system bandwidth of 50 × 50 pixels. (c) Decrypted image of Optics without using phase key. (d) Decrypted image with correct key.

with a system bandwidth of 150 × 150 pixels, respectively. The CC value for Fig. 4(d) is 0.682. The encrypted results with different system bandwidths seem not quite white noise but are obviously irrecognizable. As can be seen from Fig. 4, a better quality of decrypted image can be obtained by an increase in the system bandwidth. The coherent cutoff frequencies in those experiments are all much lower than one half of the maximum frequency (the Nyquist frequency) presented in $U_0'(x, y)$, assuring the reasonableness of the sizes of the phase masks used in the conjugate plane in the calculations.

Security analysis showed that if possible, it should be avoided to re-use the same keys for different images in DRPE systems, as in a one-time pad approach [24], which implies using different encryption keys for each image to be encrypted is one of the best way to avoid various attacks at present. In this proposed security system with divergent illumination, re-using the same keys for different images can be easily avoided by changing the locations of optical elements since the corresponding key used for decryption is not identical to the encryption code. The decryption key denoted by function $\hat{h}(f_\xi, f_\eta)$ is decided by two independent parts: function $\exp[j2\pi a(u, v)]$ that involves the distances parameters of the first part of the system, and the code for encryption, i.e., $R_2(f_\xi, f_\eta)$. Changing the locations of optical elements even when using the same encryption key results in different decryption keys makes the system perform as in a one-time pad approach.

When the phase key used in the decryption with a system bandwidth of 150 × 150 pixels was replaced by an invalid key produced by a different set of parameters, i.e., $z_1 = 600$ mm, $d_0 = 90$ mm and $z_2 = 300$ mm, the decrypted result is a noisy image, as can be shown in Fig. 5(a). Additional simulations were carried out to test the performance of the two phase functions composing the decryption key. Fig. 5(b) shows the resulting image decrypted with phase mask $\exp[j2\pi a(u, v)]$. When the encryption key is just used for decryption, the resultant image is presented in Fig. 5(c). No valuable information can be observed.

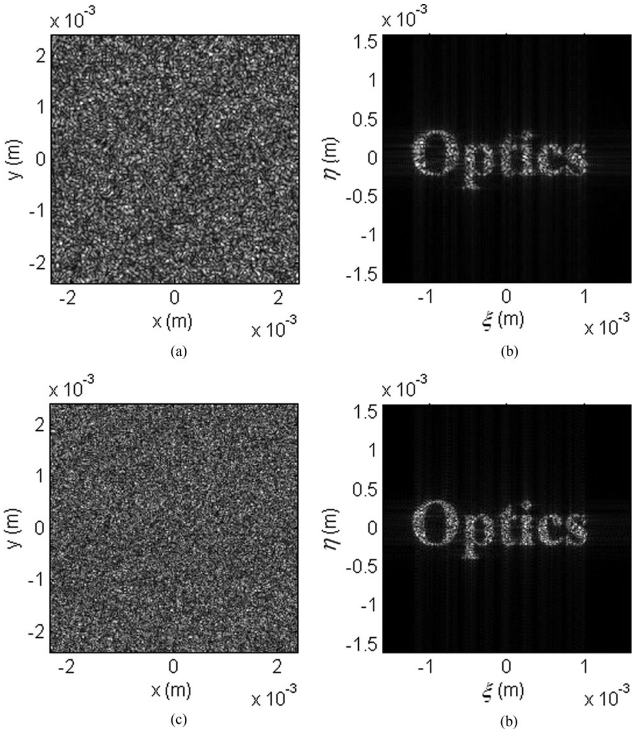


Fig. 4. Calculation results of encryption and decryption. (a) and (b) Encrypted and decrypted image with a system bandwidth of 100 × 100 pixels, respectively. (c) and (d) With a system bandwidth of 150 × 150 pixels.

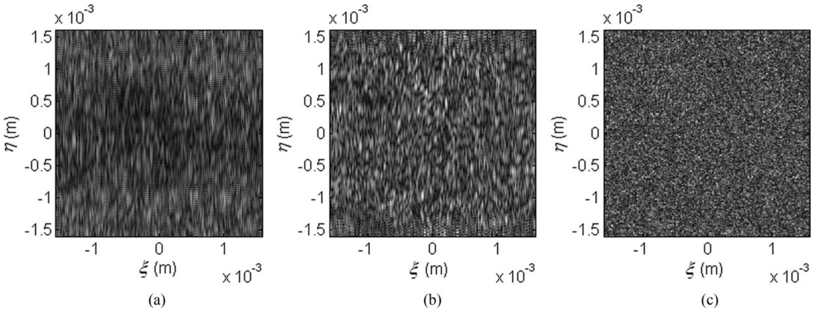


Fig. 5. Decrypted images of Optics using invalid keys. (a) Decrypted image with a code produced by incorrect distance parameters. Decrypted results when using part of the phase keys. (b) $\exp[j2\pi a(u, v)]$. (c) R_2 (f_ξ, f_η).

5. Conclusion

In this paper, we have theoretically proved the feasibility of a free space optical encryption mode based on input plane and conjugate plane random phase encoding with divergent illumination. Different from the classical DRPE system, a continuous change of position of optical elements applied for encryption is allowed. The security of the system can also be effectively enhanced by the fact that the decryption key is different from the encryption code, avoiding re-using the same key (or the conjugate of it) for decrypting different images by changing the locations of optical elements.

Besides, simulation experiments with different bandwidths of the system have been carried out to support our proposal. The encrypted images with different system bandwidths seem not quite white noise but were still irrecognizable and satisfactory decrypted results have been achieved by using asymmetric decryption keys. It is believed that this approach can effectively enlarge application domain of double random phase encoding for optical security, and a different research perspective may be opened up for double-random-phase based optical information verification.

Acknowledgment

The authors would like to thank the anonymous referees for their valuable comments and suggestions that have improved this paper.

References

[1] B. Javidi *et al.*, “Roadmap on optical security,” *J. Opt.*, vol. 18, no. 8, Jul. 2016, Art. no. 083001.

[2] A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” *Adv. Opt. Photon.*, vol. 1, no. 3, pp. 589–636, Nov. 2009.

[3] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, Apr. 2014.

[4] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.

[5] B. Javidi, G. S. Zhang, and J. A. Li, “Encrypted optical memory using double-random phase encoding,” *Appl. Opt.*, vol. 36, no. 5, pp. 1054–1058, Feb. 1997.

[6] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” *Opt. Lett.*, vol. 24, no. 11, pp. 762–764, Jun. 1999.

[7] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, Jul. 2004.

[8] X. Wang, W. Chen, S. Mei, and X. Chen, “Optically secured information retrieval using two authenticated phase-only masks,” *Sci. Rep.*, vol. 5, Oct. 2015, Art. no. 15668.

[9] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, Jun. 2000.

[10] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, “Double image encryption by using iterative random binary encoding in gyrator domains,” *Opt. Exp.*, vol. 18, no. 11, pp. 12033–12043, May 2010.

[11] W. Qin and X. Peng, “Asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, Jan. 2010.

[12] X. Wang and D. Zhao, “Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask,” *Opt. Lett.*, vol. 38, no. 18, pp. 3684–3686, Sep. 2013.

[13] S. K. Rajput and N. K. Nishchal, “Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask,” *Appl. Opt.*, vol. 51, no. 22, pp. 5377–5386, Aug. 2012.

[14] X. Deng and D. Zhao, “Single-channel color image encryption based on asymmetric cryptosystem,” *Opt. Laser Technol.*, vol. 44, no. 1, pp. 136–140, Feb. 2012.

[15] E. Perez-Cabre, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” *Opt. Lett.*, vol. 36, no. 1, pp. 22–24, Jan. 2011.

[16] A. Markman, B. Javidi, and M. Tehranipoor, “Photon-counting security tagging and verification using optically encoded QR codes,” *IEEE. Photon. J.*, vol. 6, no. 1, Feb. 2014, Art. no. 6800609.

[17] W. Chen, “Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation,” *IEEE. Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 6900209.

[18] H. Hwang, H. Chang, and W. Lie, “Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems,” *Opt. Exp.*, vol. 17, no. 16, pp. 13700–13710, Aug. 2009.

[19] Z. Liu, C. Shen, J. Tan, and S. Liu, “A recovery method of double random phase encoding system with a parallel phase retrieval,” *IEEE. Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7801807.

[20] X. Wang, W. Chen, and X. Chen, “Optical encryption and authentication based on phase retrieval and sparsity constraints,” *IEEE. Photon. J.*, vol. 7, no. 2, Apr. 2015, Art. no. 7800310.

[21] Y. Rivenson, A. Stern, and B. Javidi, “Single exposure super-resolution compressive imaging by double phase encoding,” *Opt. Exp.*, vol. 18, no. 14, pp. 15094–15103, Jul. 2010.

[22] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, “Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique,” *Appl. Opt.*, vol. 53, no. 20, pp. 4539–4547, Jul. 2014.

[23] T. Sanpei *et al.*, “Optical encryption for large-sized images,” *Opt. Commun.*, vol. 361, pp. 138–142, Feb. 2016.

[24] X. Peng, P. Zhang, H. Z. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, Apr. 2006.

[25] X. Wang and D. Zhao, “A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Commun.*, vol. 285, no. 6, pp. 1078–1081, Mar. 2012.

[26] Y. Wang, C. Quan, and C. Tay, “Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform,” *Appl. Opt.*, vol. 54, no. 22, pp. 6874–6881, Aug. 2015.

[27] Y. Wang, C. Quan, and C. Tay, “New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition,” *Appl. Opt.*, vol. 55, no. 4, pp. 679–686, Feb. 2016.

[28] X. Wang, D. Zhao, and Y. Chen, “Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask,” *Appl. Opt.*, vol. 53, no. 23, pp. 5100–5108, Aug. 2014.

[29] J. W.Goodman, *Introduction to Fourier Optics*, 3rd ed. Englewood, CO, USA: Roberts & Company, 2005.

[30] J. Fredy Barrera, A. Mira, and R. Torroba, “Optical encryption and QR codes: Secure and noise-free information retrieval,” *Opt. Exp.*, vol. 21, no. 5, pp. 5373–5378, Mar. 2013.