Current Optics and Photonics
Vol. 2, No. 6, December 2018, pp. 540-546

ISSN: 2508-7266(Print) / ISSN: 2508-7274(Online)
DOI: https://doi.org/10.3807/COPP.2018.2.6.540

Optical Image Encryption Technique Based on Hybrid-pattern Phase Keys

Wenqing Sun*, Lei Wang, Jun Wang, Hua Li, and Quanying Wu

Jiangsu Key Laboratory of Micro and Nano Heat Fluid Flow Technology and Energy Application, School of Mathematics and Physics, Suzhou University of Science and Technology, Suzhou 215009, PR China

(Received July 22, 2018 : revised September 13, 2018 : accepted October 5, 2018)

We propose an implementation scheme for an optical encryption system with hybrid-pattern random keys. In the encryption process, a pair of random phase keys composed of a white-noise phase key and a structured phase key are positioned in the input plane and Fourier-spectrum plane respectively. The output image is recoverable by digital reconstruction, using the conjugate of the encryption key in the Fourier-spectrum plane. We discuss the system encryption performance when different combinations of phase-key pairs are used. To measure the effectiveness of the proposed method, we calculate the statistical indicators between original and encrypted images. The results are compared to those generated from a classical double random phase encoding. Computer simulations are presented to show the validity of the method.

Keywords : Information security, Optical encryption, Random phase key, 4f correlator
OCIS codes : (060.4785) Optical security and encryption; (100.4998) Pattern recognition, optical security and encryption; (070.4560) Data processing by optical means

I. INTRODUCTION

Optical information encryption technology has received extensive attention from researchers in recent years, because of its advantages of high-speed parallel processing and multiple degree of freedom in encoding. One of the earliest and most widely studied optical encryption methods for images was the double random phase encoding (DRPE) system proposed by Refregier and Javidi [1-5]. This architecture is based on a 4*f* imaging system together with a pair of random-phase keys, to encode image information in both spatial and Fourier-spectrum domains. There are many examples showing that optical security and encoding techniques have continued to attract the attention of researchers, and many kinds of implementations have been proposed [6-14].

A common aspect of all these classical DRPE systems, the white-noise-like random plate was utilized as a random phase key (RPK). To our knowledge, J. F. Barrera *et al.* proposed the concept of a structured phase key (SPK). They suggested that phase keys can be catalogued in two categories: random phase keys and structured phase keys [15]. In the first group, speckle patterns or white-noise-like phase keys are classical examples. In the second group, structured phase keys defined by some specific configurations are used. Although white-noise-like RPK has been widely used in image encryption, we cannot deny that this scheme is vulnerable to various types of attack [16-18]. In this regard, numerous methods have been proposed to improve robustness. The optical asymmetric encryption system (OACS) is one of the possible solutions originating from the phase-truncated Fourier transform (PT-FT) [19, 20]. The main issue is to find a more effective trapdoor one-way function, to increase system security. So far, many derivative OACSs have been proposed [21-27].

In recent years, another alternative to the classical DRPE scheme has been to use SPK in the encryption-decryption process. Several kinds of SPKs have been constructed, such as the fractal zone mask (FZM) [28], linear phase mask (LPM) [29], toroidal zone mask (TZM) [30, 31], and spiral phase mask (SPPM) [32-40]. These kinds of SPKs have shown significant simplicity and robustness, to meet the requirements of high flexibility and safety. From a broader perspective, these SPKs have been applied in

*Corresponding author: sunwenqing@mail.usts.edu.cn, ORCID 0000-0002-0861-0941
Color versions of one or more of the figures in this paper are available online.

different domains, such as the gyrator transform (GT) [41-45], Hartley transform [46], Fresnel wavelet transform [47], and gyrator wavelet transform [48]. H. Singh *et al.* proposed a scheme applied to GT, with RPK and a devil's vortex Fresnel lens (DVFL) placed in the frequency plane, for double phase-image encryption [49].

In this paper, we present the implementation scheme for an optical encryption system with hybrid-pattern random keys. Unlike the classical DRPE system, two different types of phase keys are used in this new hybrid encryption system: one is RPK, and the other is SPK. The outline of this paper is as follows: First, the principles of the encryption-decryption algorithm and the generation process for the keys are described in Section 2. Several simulated results are given as proof of concept of the proposed method in Section 3. In particular, the encryption-decryption process with different patterns of phase-key combination is analyzed: (i) SPK+RPK, (ii) RPK+SPK, (iii) SPK1+SPK2, and (iv) RPK1+RPK2 (as a reference). To evaluate the quality of the recovered images, some statistical indicators, such as the correlation coefficient (CC) and the peak signal-to-noise ratio (PSNR), between the input images and the recovered images are calculated. Next, the robustness of different phase-key combination schemes is also studied. Finally, the main conclusions of the work are provided in Section 4.

II. PRINCIPLE OF ENCRYPTION-DECRYPTION SCHEMES

In this section, we first briefly review the classical DRPE system, which is used to conduct the hybrid-phase-key approach that we propose. The schemes for the encryption and decryption processes, based on a well-known 4*f* system, are shown in Figs. 1(a) and 1(b) respectively, where KEY_1 and KEY_2 are the white-noise-like RPK or SPK, $I(x,y)$ is the input image, and $E(x,y)$ is the encrypted image. KEY_1 and KEY_2 are positioned in the input plane and the Fourier spectrum plane respectively. $FT\{\cdot\}$ and $IFT\{\cdot\}$ represent the Fourier transform and inverse Fourier transform respectively. In this case, the complex output encrypted image $E(x,y)$ can be written as

$$E(x,y) = IFT\{FT\{I(x,y)\cdot KEY_1(x,y)\}\cdot KEY_2(u,v)\}. \quad (1)$$

The decryption process is the reverse of the encryption process, where the encrypted image is Fourier transformed and then multiplied by the complex conjugate of the SPK. An $IFT\{\cdot\}$ is performed to recover the real part of $I(x,y)$. The decrypted image $I'(x,y)$ can be express as

$$I'(x,y) = IFT\{FT\{E(x,y)\}\cdot KEY_2^*(x,y)\}, \quad (2)$$

where * indicates the complex conjugate of the SPK. Note

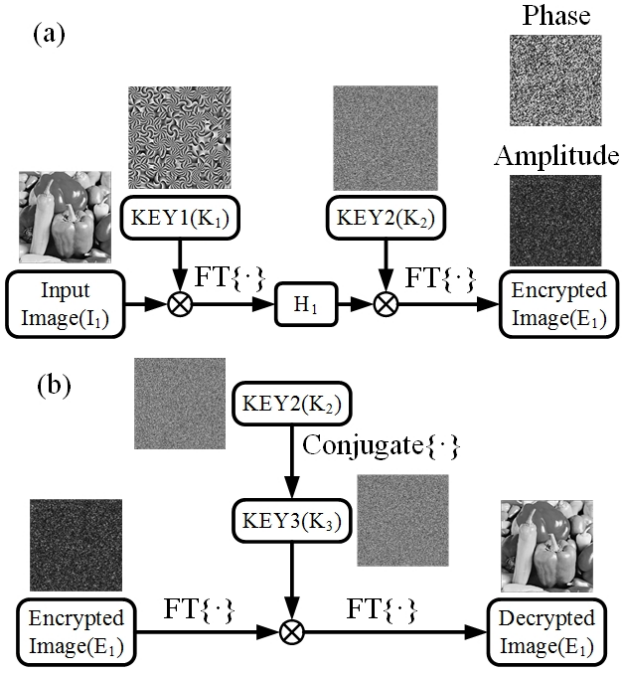

FIG. 1. Flow chart of the proposed scheme: (a) encryption process, (b) decryption process.

that if $I(x,y)$ is a complex function, multiplication by $KEY_2^*(x,y)$ is needed in the decryption process.

Next, the construction procedure for defining the subkeys in the key is introduced. By setting the value of an integer n, we split the phase key into sub-blocks of size $d = dim/n$, where dim is the pixel size of input image. For simplicity, we show an example for the case $dim = 512$ and $n = 8$. We consider that a 512×512 phase key is divided into $64 = 8\times8$ where the size of each subkey is $d\times d = 64\times64$. The SPK can be written as a linear combination of the states of the 64 subkeys M_{ij}, as shown in the following equation:

$$SPK = \sum_{i=1}^{8}\sum_{j=1}^{8} M_{ij}(d\times d). \quad (3)$$

We select some representative SPKs as cells, such as the linear phase key (LPK), quadratic phase key (QPK), spiral phase key (SPPK), and spiral quadratic phase key (SQPK). The general phase distributions of these designed cells are provided in Eqs. (4)~(7),

$$T_{LPK} = \exp[jk(a_1x + a_2y)], \quad (4)$$

$$T_{QPK} = \exp[jk(b_1x^2 + b_2y^2)], \quad (5)$$

$$T_{SPPK} = \exp[jkc_1\theta], \quad (6)$$

$$T_{SQPK} = \exp[jk(d_1\theta + d_2x^2 + d_3y^2)] \quad (7)$$

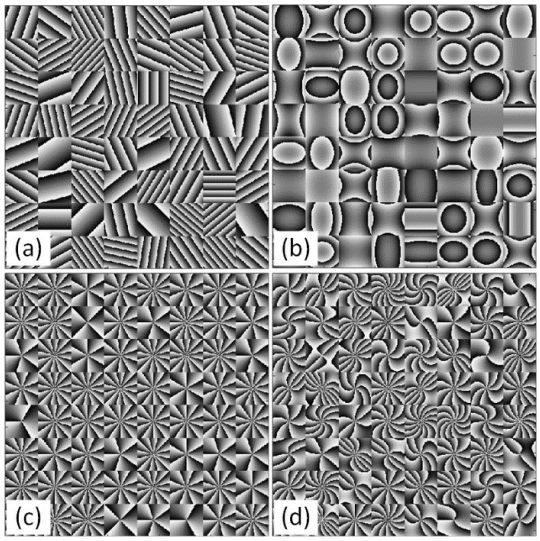

FIG. 2. Four SPK patterns: (a) LPK, (b) QPK, (c) SPPK, (d) SQPK.

in which, a_1, a_2, b_1, b_2, c_1, d_1, d_2, and d_3 are random parameters, k is the wave number, and (x, y) and (ρ, θ) are local coordinates. Each subkey will be filled with the above structured random parameter functions.

To illustrate the procedure described above, examples of SPKs generated for different function mode and number m are shown in Fig. 2. For the sake of clarity, Fig. 2 shows the phase distributions of some generated structured phase keys. For the experimental implementation of the proposed technique, a spatial light modulator (SLM) can be used to generate the SPK and RPK. In such a case, the smallest size of the subkey is limited by the number of pixels of the modulator. Theoretically, a subkey with a minimal size of 1×1 pixels can be obtained, in which case SPK and RPK are equivalent.

III. NUMERICAL SIMULATION

In this section we study the feasibility, effectiveness, and sensitivity of the hybrid-key encryption scheme, based on simulated results. The simulations are carried out on the MATLAB®2016a platform. A grayscale image (pepper image) of size 512×512 pixels is used as the original image to be encrypted, as shown in Fig. 3. We first present some simulation results to show the hybrid scheme in the classical DRPE system. In this scenario, KEY_1 is an arbitrary type of SPK positioned in the input plane, and KEY_2 is an RPK positioned in the spectrum plane. The encrypted images are shown in Figs. 4(a)~4(d), corresponding to the SPK patterns shown in Figs. 2(a)~2(d). The results show that the encrypted images have similar distributions for different types of SPKs in the SPK+RPK scheme. However, they are quite different from the image encrypted by the RPK+RPK scheme.

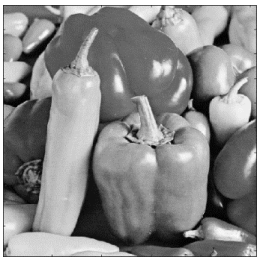

FIG. 3. Original image.

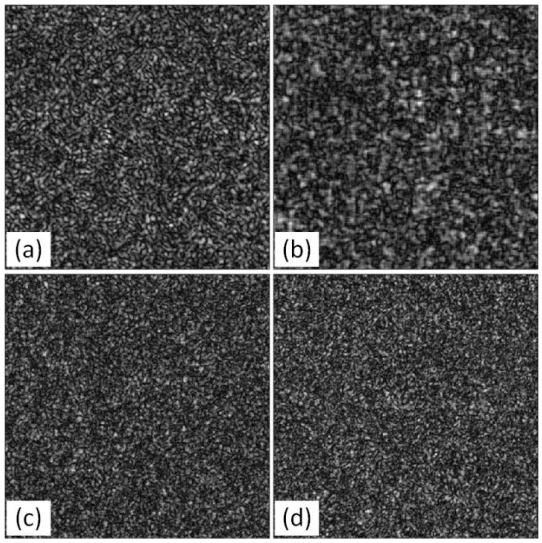

FIG. 4. Encrypted images (intensity) for different types of SPKs in the SPK+RPK scheme: (a) LPK, (b) QPK, (c) SPPK, (d) SQPK.

We quantitatively analyze the quality of the encrypted images by introducing three indices: the correlation coefficient (CC), peak signal-to-noise ratio (PSNR), and information entropy (IE), as defined respectively in Eqs. (8)~(10).

$$CC=\frac{\left|\sum_{n_x=1}^{N_x}\sum_{n_y=1}^{N_y}\left(I_p(n_x,n_y)-E[I_p]\right)\left(I_c(n_x,n_y)-E[I_c]\right)\right|}{\sqrt{\sum_{n_x=1}^{N_x}\sum_{n_y=1}^{N_y}\left(I_p(n_x,n_y)-E[I_p]\right)^2}\cdot\sqrt{\sum_{n_x=1}^{N_x}\sum_{n_y=1}^{N_y}\left(I_c(n_x,n_y)-E[I_c]\right)^2}}, \tag{8}$$

$$PSNR=10\times\lg\left(\frac{255^2}{\sqrt{\sum_{n_x}^{N_x}\sum_{n_y}^{N_y}\left|I_p(n_x,n_y)-I_c(n_x,n_y)\right|^2}}\right), \tag{9}$$

$$IE=-\sum_{l=1}^{L}P_l\log_2 P_l, \tag{10}$$

In Eqs. (8)~(10), n_x and n_y denote the pixel positions, I_p and I_c are the intensity of the original image and the encrypted image respectively, N_x and N_y are the pixel size of the image, and P_l is the probability that gray level l occurs in the encrypted image. CC and PSNR are utilized

TABLE 1. Quality evaluation of encrypted images

Indices	LPK	QPK	SPPK	SQPK	RPK
CC	0.015	0.015	0.005	0.005	0.002
PSNR	1.928	1.929	1.925	1.925	1.927
IE	7.747	7.747	7.747	7.747	7.747

to indicate the similarity between original and encrypted images. It may be noted that a smaller CC or larger PSNR means greater similarity between original and recovered images. The CC assumes values from 0 to 1, because images with negative correlations can also be recognized by the human eye. Table 1 summarizes the CC, PSNR, and IE (with a maximum value of 8) values obtained by comparing different SPKs in the hybrid-key DRPE system. The results for the above four SPK patterns are listed in Table 1. The results shown in Table 1 indicate that images encrypted by different SPKs have statistical indicators similar to those for double RPK encryption. However, the statistical indicators of the image in the SPK+RPK scheme are related to the parameter selection of the SPK.

In a hybrid encryption system, the following four key combinations can be selected:

(i) SPK + RPK,
(ii) RPK + SPK,
(iii) SPK1 + SPK2, and
(iv) RPK1 + RPK2,

where the SPK is generated by SQPK, and the double RPK scheme (iv) is selected as a reference. Figures 5(a)~5(p) are the key and the encrypted image for the above four combinations. In Fig. 5, the first column is KEY_1, the second column is KEY_2, the third column is the intensity of the encrypted image, and the fourth column is the phase of the encrypted image. From the perspective of human vision, the encryption results (including intensity and phase) of the four schemes are different. According to the principle of the DRPE system, the encrypted image can be recovered without any loss by using the fully correct conjugate key for decryption.

We conduct a decryption analysis using keys with partial error. In the first case, we introduced different percentages of error at random positions in the decryption key. The encrypted image used here comes from the results of Figs. 5(c), 5(g), 5(k). There are three groups in this Fig. 6: (a)~(d) for RPK+RPK, (e)~(h) for RPK+SPK, and (i)~(l) for SPK+RPK. In the entire phase key of both keys, in the respective columns 20%, 40%, 60%, and 80% of the pixel values at random locations are erroneous. The varying quality of the recovered image is depicted in this figure. The decrypted images are recognizable even when the fraction of erroneous key is up to 60%, for the RPK+RPK and RPK+SPK schemes. However, the decrypted image from the SPK+RPK encryption scheme has become unrecognizable at this point.

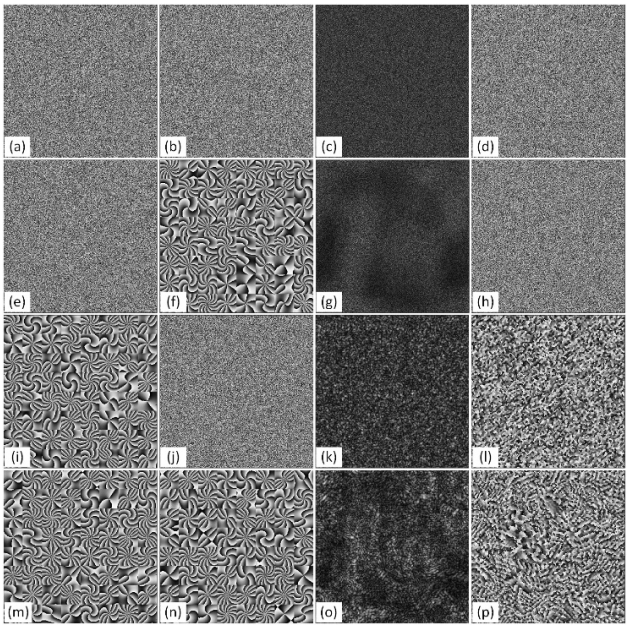

FIG. 5. The keys and encrypted image (intensity and phase) for different hybrid-key-pattern combinations: (a)~(d) RPK+RPK, (e)~(h) RPK+SPK, (i)~(l) SPK+RPK, (m)~(p) SPK+SPK. The 1st column is KEY_1, the 2nd column is KEY_2, the 3rd column is the intensity of the encrypted image, and the 4th column is the phase of the encrypted image.

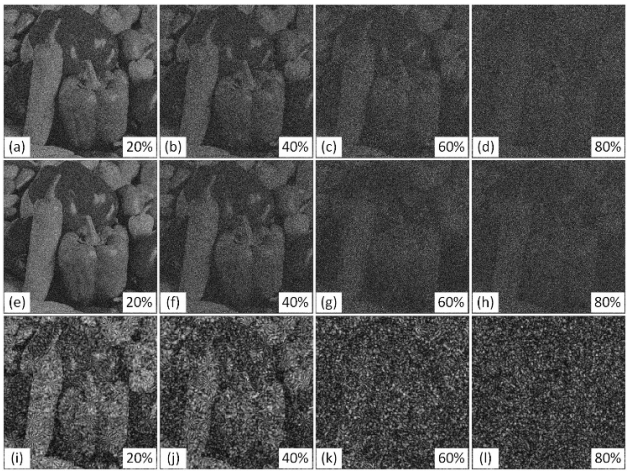

FIG. 6. Decrypted images using partial-error keys for different schemes: (a)~(d) RPK+RPK, (e)~(h) RPK+SPK, (i)~(l) SPK+RPK.

The reason for these results is obvious: The RPK+RPK scheme has the highest information entropy, while the SPK+SPK scheme presents the lowest information entropy. The information entropy of the hybrid filter scheme falls somewhere in between these two extremes.

Hypothesis testing is applied to encrypted images. According to the results, at the 95% confidence level, the encrypted amplitude image obeys the Rayleigh distribution

for all combinations. The encrypted phase image obeys the uniform distribution only for the combination RPK+RPK, and does not obey the uniform distribution for the combination SPK+SPK. For other combinations, the results are uncertain. As mentioned, the SPK+RPK and RPK+SPK are the in-between schemes.

In addition, CC results for the mean value obtained after performing 100 runs with the above four modes are shown in Fig. 7. In this figure, the percent correctness of the phase key increases from 10% to 60% with an interval of 10%. The CCs of SPK+RPK and SPK+SPK are different, but not clearly so, from the other two schemes (RPK+SPK and RPK+RPK), when the percentage of correct keys is about 10%. However, as the percent correctness of the keys gradually increases, the CCs of the four schemes become almost the same.

A quantitative result for decryption with partial parameters of keys in error is depicted in Fig. 8, using CC as the evaluation parameter. The results show that when SPK is used for decryption, if there is an error in the parameters of the SPK, the decryption quality of the image will be significantly affected. It should be noted that a hybrid key combination will not change the features of alignment sensitivity, it depends on the type of decrypted key. An RPK is very sensitive to the alignment, but an SPK is not.

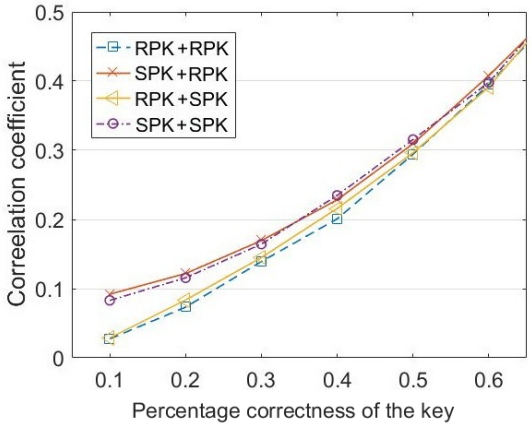

FIG. 7. Relationship between CC and percentage correctness of the key for the four schemes.

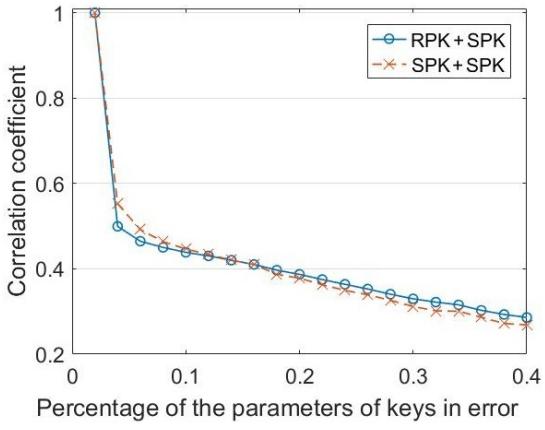

FIG. 8. Relationship between CC and percentage of key parameters in error for the RPK+SPK and SPK+SPK schemes.

IV. CONCLUSION

In this paper, a hybrid phase-key scheme for an optical encryption system is proposed. In this scheme, one of the phase keys is an RPK and the other is an SPK. The entire SPK is divided into subkeys and filled with subblocks of different parameters. The subblock is defined by various functional phase distributions. This hybrid scheme serves as an alternative for single-pattern phase keys, and shows obvious benefits and features. Numerical simulations were performed for the encryption process with the proposed hybrid-key schemes and single-pattern schemes. The output images encrypted by different key patterns show similar statistical indicators. Compared to single-pattern schemes, the hybrid-pattern method enables a more flexible key-space design with multiple degrees of freedom.

The double RPK scheme has strong randomness, but no configurability. The double SPK scheme has relatively low randomness, but high configurability. Between the remaining two options, the SPK+RPK scheme is relatively better, as the rough outline of the image cannot be recognized from the ciphertext. The SPK+SPK and RPK+SPK results show that vulnerability clearly, because the rough outline can be regarded as prior information about the plaintext image and used by attackers. However, no matter which combination of modes is selected, the defects inherent in the DRPE system cannot be changed. The hybrid keys are applied in the DRPE cryptosystem, which is based on the Fourier transforms. Therefore, the inherent linearity introduced by Fourier transforms has not been removed. It is also vulnerable to some known attacks, such as known-plaintext and chosen-ciphertext.

In this work, we also investigate the situation for reconstructing the original image when the keys are partially erroneous. The result shows that the proposed scheme is secure and robust for grayscale phase images. Undoubtedly, this hybrid-phase key encryption scheme has the potential for use in other structured encryption systems, such as Fresnel transform, Hartley transform, gyrator transform, and so on. It also can be possibly extended to encryption systems for color images, or multiple images. We hope this hybrid-key scheme can provide insights into other areas of optical information processing.

ACKNOWLEDGMENT

The work reported in this article is supported by the National Natural Science Foundation of China (NSFC) (11503017); the “Summit of the Six Top Talents” Program

of Jiangsu Province (2015-DZXX-026); Jiangsu Key Disciplines of Thirteenth Five-Year Plan (20168765); and the Suzhou Key Industry Technology Innovation Plan (SYG201646). The authors are grateful to Suzhou Key Laboratory for Precision and Efficient Processing Technology (SZS201712) for its support. We thank Shengzhi Wang for linguistic assistance during the preparation of this manuscript.

REFERENCES

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 590-636 (2009).
2. M. S. Millán, "Advanced optical correlation and digital methods for pattern matching—50th anniversary of Vander Lugt matched filter," J. Opt.-UK **14**, 103001 (2012)
3. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 121-155 (2014)
4. S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt. Laser Technol. **57**, 327-342 (2014).
5. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, and A. Markman, "Roadmap on optical security," J. Opt.-UK **18**, 083001 (2016).
6. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22-24 (2011).
7. I. Lee and M. Cho, "Optical encryption and information authentication of 3D objects considering wireless channel characteristics," J. Opt. Soc. Korea **17**, 494-499 (2013).
8. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett. **38**, 3198-3201 (2013).
9. I. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," J. Opt. Soc. Korea **18**, 201-206 (2014).
10. A. Vaish and M. Kumar, "Color image encryption using singular value decomposition in discrete cosine Stockwell transform domain," Opt. Appl. **48**, 25-38 (2018).
11. Z. Shao, Y. Shang, Q. Tong, H. Ding, X. Zhao, and X. Fu, "Multiple color image encryption and authentication based on phase retrieval and partial decryption in quaternion gyrator domain," Multimedia Tools Appl. **77**, 25821-25840 (2018).
12. X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme," Opt. Laser Eng. **102**, 106-111 (2018).
13. H. Xu, W. Xu, S. Wang, and S. Wu, "Phase-only asymmetric optical cryptosystem based on random modulus decomposition," J. Mod. Opt. **65**, 1245-1252 (2018).
14. K. Ravi, B. Basanta, and K. N. Naveen, "Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition," J. Opt.-UK **20**, 015701 (2018).
15. J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption method using toroidal zone plates," Opt. Commun. **248**, 35-40 (2005).
16. Y. Xiong, A. He, and C. Quan, "Security analysis of a double-image encryption technique based on an asymmetric algorithm," J. Opt. Soc. Am. A **35**, 320-326 (2018).
17. M. Liao, W. He, D. Lu, and X. Peng, "Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium," Sci. Rep. **7**, 41789 (2017).
18. T. Li, Z. Miao, and Y. Shi, "Ciphertext-only attack on phase-shifting interferometery-based encryption," IEEE Photon. J. **9**, 1-8 (2017).
19. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**, 118-120 (2010).
20. M. Khurana and H. Singh, "An asymmetric image encryption based on phase truncated hybrid transform," 3D Res. **8** (2017).
21. S. K. Gil, "Asymmetric public key cryptography by using logic-based optical processing," J. Opt. Soc. Korea **20**, 55-63 (2016).
22. H. Yu, J. Chang, X. Liu, C. Wu, Y. He, and Y. Zhang, "Novel asymmetric cryptosystem based on distorted wave-front beam illumination and double-random phase encoding," Opt. Express **25**, 8860 (2017).
23. H. Chen, C. Tanougast, Z. Liu, and L. Sieler, "Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains," Opt. Lasers Eng. **93**, 1-8 (2017).
24. L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, "Asymmetric color image encryption based on singular value decomposition," Opt. Lasers Eng. **89**, 80-87 (2017).
25. X. Li, M. Zhao, Y. Xing, L. Li, S. T. Kim, X. Zhou, and Q. H. Wang, "Optical encryption via monospectral integral imaging," Opt. Express **25**, 31516-31527 (2017).
26. T. Zhao, Y. Jiang, and C. Liu, "Demonstration and a practical scheme of the optical asymmetric cryptosystem," Optik **138**, 509-515 (2017).
27. L. Ma and W. Jin, "Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography," Opt. Commun. **407**, 51-56 (2018).
28. M. Tebaldi, W. D. Furlan, R. Torroba, and N. Bolognini, "Optical-data storage-readout technique based on fractal encrypting masks," Opt. Lett. **34**, 316 (2009).
29. W. Zamrani, E. Ahouzi, A. Lizana, J. Campos, and M. J. Yzuel, "Optical image encryption technique based on deterministic phase masks," Opt. Eng. **55**, 103108 (2016).
30. J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption method using toroidal zone plates," Opt. Commun. **248**, 35-40 (2005).
31. J. F. Barrera, R. Henao, and R. Torroba, "Fault tolerances using toroidal zone plate encryption," Opt. Commun. **256**, 489-494 (2005).
32. S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," Appl. Opt. **51**, 5377-5386 (2012).

33. C. Lin and X. Shen, "Design of reconfigurable and structured spiral phase mask for optical security system," Opt. Commun. **370**, 127-134 (2016).
34. C. Lin, X. Shen, and M. Lei, "Generation of plaintext-independent private key based on conditional decomposition strategy," Opt. Lasers Eng. **86**, 303-308 (2016).
35. H. Singh, "Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain," Opt. Appl. **47**, 557-578 (2017).
36. R. Kumar and B. Bhaduri, "Optical image encryption in Fresnel domain using spiral phase transform," J. Opt.-UK **19**, 095701 (2017).
37. M. R. Abuturab, "Securing multiple information using chaotic spiral phase encoding with simultaneous interference and superposition methods," Opt. Lasers Eng. **98**, 1-16 (2017).
38. Q. Chen, X. Shen, S. Dou, C. Lin, and L. Wang, "Topological charge number multiplexing for JTC multiple-image encryption," Opt. Commun. **412**, 155-160 (2018).
39. K. Ravi, B. Basanta, and K. N. Naveen, "Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition," J. Opt.-UK **20**, 015701 (2018).
40. M. Rafiq Abuturab, "Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition," Opt. Laser Technol. **98**, 298-308 (2018).
41. M. R. Abuturab, "Color image security system using double random-structured phase encoding in gyrator transform domain," Appl. Opt. **51**, 3006-3016 (2012).
42. M. R. Abuturab, "Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding," Opt. Lasers Eng. **50**, 1209-1216 (2012).
43. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," Appl. Opt. **53**, 6472 (2014).
44. A. K. Yadav, S. Vashisth, H. Singh, and K. Singh, "A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask," Opt. Commun. **344**, 172-180 (2015).
45. S. Liansheng, Z. Bei, N. Xiaojuan, and T. Ailing, "Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain," Opt. Express **24**, 499-515 (2016).
46. P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition," Opt. Lasers Eng. **91**, 187-195 (2017).
47. H. Singh, "Cryptosystem for securing image encryption using structured phase masks in fresnel wavelet transform domain," 3D Res. **7** (2016).
48. H. Singh, "Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain," Opt. Lasers Eng. **81**, 125-139 (2016).
49. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," Opt. Lasers Eng. **67**, 145-156 (2015).