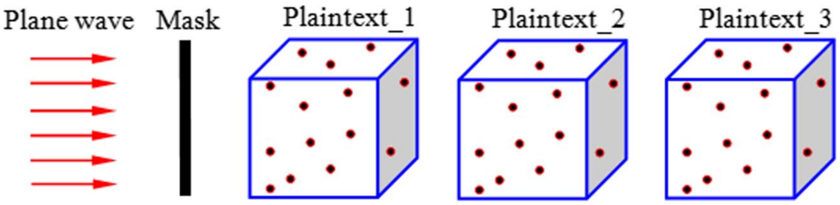
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Optical Multiple-Image Encryption Using Three-Dimensional Space

Volume 8, Number 2, April 2016

Wen Chen



DOI: 10.1109/JPHOT.2016.2550322
1943-0655 © 2016 IEEE

Optical Multiple-Image Encryption Using Three-Dimensional Space

Wen Chen

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University,
Hong Kong, China

DOI: 10.1109/JPHOT.2016.2550322

Manuscript received March 8, 2016; revised March 28, 2016; accepted March 30, 2016. Date of publication April 4, 2016; date of current version April 15, 2016. This work was supported by The Hong Kong Polytechnic University through a startup grant (1-ZE5F). Corresponding author: W. Chen (e-mail: owen.chen@polyu.edu.hk)

Abstract: A novel method using 3-D space is proposed for optical multiple-image encryption. Each input image is divided into a series of particle-like points distributed in 3-D space, and all generated particle-like points are simultaneously encrypted into a phase-only mask. The proposed method may open up a novel research perspective for optical multiple-image encryption, since a 3-D-space processing strategy is developed and successfully applied.

Index Terms: Optical multiple-image decryption, optical multiple-image encryption, 3-D space.

1. Introduction

Since double random phase encoding was developed [1], various optical infrastructures [2]–[10], such as digital holography [2], have been developed. In optical encoding, the objective is to convert the input image into stationary white noise by using random phase-only masks placed in the optical path [1].

In recent years, optical multiple-image encryption [11] has attracted much attention, since several images are simultaneously encoded to enhance system capacity. Among the developed multiplexing approaches, phase-mask extraction algorithms [12], [13] have been widely applied, since the decoding process can be implemented by using either a digital or optical approach. For instance, Hwang *et al.*, [13] proposed to use Gerchberg-Saxton algorithm [12] and phase modulation scheme for optical multiple-image encryption. However, system security [13] may be limited due to only 2-D processing. Gerchberg-Saxton algorithm has been modified and applied for optical multiple-image authentication [14], however it is still conducted in 2-D space. The Gerchberg-Saxton algorithm is further extended to three-dimensional (3-D) space [8], [15] for optical security, however only single-image encryption strategy has been studied.

In this paper, a novel method using 3-D space is proposed for optical multiple-image encryption. Each input image is divided into a series of particle-like points distributed in 3-D space, and all generated particle-like points are simultaneously encoded into a phase-only mask. It is numerically illustrated that significant advantage, i.e., high security, can be obtained in the proposed method for optical multiple-image encryption, since 3-D-space processing strategy is further applied.

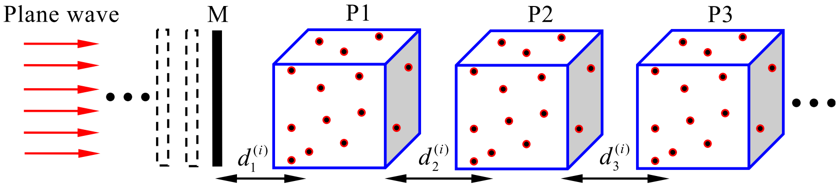


Fig. 1. Schematic illustration of optical multiple-image encryption in 3-D space: M—phase-only mask extracted during encoding; P—plaintext; i—particle-like point index (i.e., $i = 1, 2, 3, \ldots$). In practice, it is straightforward to encode the plaintexts into multiple cascaded phase-only masks.

2. Principles

Fig. 1 shows a schematic layout for the proposed optical multiple-image encryption in 3-D space. For simplicity three input images are encoded, and each input image is divided into a series of particle-like points distributed in a 3-D space (see Fig. 1). A digital approach should be applied to encode all particle-like points into a phase-only mask (M), and here a phase retrieval algorithm is studied for the phase-mask extraction. During the encryption, coordinates (μ_1, v_1), (μ_2, v_2), and (μ_3, v_3), respectively, denote transverse areas inside the plaintext P1, P2, and P3 planes, and three input images are applied as plaintexts and respectively denoted as $O_1(\mu_1, \nu_1)$, $O_2(\mu_2, \nu_2)$, and $O_3(\mu_3, \nu_3)$. The phase-mask extraction process consists of the following steps.

1) The particle-like points are sequentially processed, and at the initial stage a random phase-only distribution is assumed to $M^{(i,n)}(x, y)$, where i denotes particle-like point index (integer $i = 1, 2, 3, \ldots$) and n denotes iteration number (integer $n = 1, 2, 3, \ldots$). Wave propagation from phase-mask plane to the first 3-D space is described by

$$O\left(\mu_1^{(i)}, v_1^{(i)}\right) = \mathrm{FWP}_{d_1^{(i)}}\left[M^{(i,n)}(x, y)\right] \tag{1}$$

where $d_1^{(i)}$ denotes a series of axial distances (plane to particle-like point) between phase-only mask (M) plane and plaintext (P1) plane, and FWP represents free-space wave propagation implemented by diffraction theory [2], [4], [16].

2) A constraint is applied to update the complex-valued wavefront $O(\mu_1^{(i)}, v_1^{(i)})$

$$\overline{O\left(\mu_1^{(i)}, v_1^{(i)}\right)} = \mathrm{PSC}\left[O\left(\mu_1^{(i)}, v_1^{(i)}\right)\right] \tag{2}$$

where PSC denotes plaintext-plane constraint described by [8], [15], [17]

$$\mathrm{PSC}\left[O\left(\mu_1^{(i)}, v_1^{(i)}\right)\right] = \begin{cases} \left[2\omega O_1(\mu_1, v_1) - \left|O\left(\mu_1^{(i)}, v_1^{(i)}\right)\right|\right] O\left(\mu_1^{(i)}, v_1^{(i)}\right) \Big/ \left|O\left(\mu_1^{(i)}, v_1^{(i)}\right)\right|, & \text{if } (\mu_1, v_1) \in i \\ O\left(\mu_1^{(i)}, v_1^{(i)}\right), & \text{if } (\mu_1, v_1) \notin i \end{cases} \tag{3}$$

where $O_1(\mu_1, \nu_1)$ denotes the plaintext P1 (i.e., the first desired input image), and ω denotes a ratio between the summation of calculated output and the summation of the desired input image (i.e., amplitude map) within a signal window (i.e., particle-like point i).

3) Subsequently, wave propagation from the first 3-D space to the second 3-D space is conducted

$$O\left(\mu_2^{(i)}, v_2^{(i)}\right) = \mathrm{FWP}_{d_2^{(i)}}\left[\overline{O\left(\mu_1^{(i)}, v_1^{(i)}\right)}\right] \tag{4}$$

where $d_2^{(i)}$ denotes a series of axial distances (particle-like point to particle-like point) between the plaintext (P1) plane and plaintext (P2) plane.

4) A constraint is applied to update the complex-valued wavefront $O(\mu_2^{(i)}, v_2^{(i)})$

$$\overline{O\left(\mu_2^{(i)}, v_2^{(i)}\right)} = \mathrm{PSC}'\left[O\left(\mu_2^{(i)}, v_2^{(i)}\right)\right] \tag{5}$$

where PSC′ denotes plaintext-plane constraint described by [8], [15], [17]

$$\mathrm{PSC}'\left[O\left(\mu_2^{(i)}, v_2^{(i)}\right)\right] = \begin{cases} \left[2\omega O_2(\mu_2, v_2) - \left|O\left(\mu_2^{(i)}, v_2^{(i)}\right)\right|\right] O\left(\mu_2^{(i)}, v_2^{(i)}\right) \Big/ \left|O\left(\mu_2^{(i)}, v_2^{(i)}\right)\right|, & \text{if } (\mu_2, v_2) \in i \\ O\left(\mu_2^{(i)}, v_2^{(i)}\right), & \text{if } (\mu_2, v_2) \notin i \end{cases} \tag{6}$$

where $O_2(\mu_2, \nu_2)$ denotes the plaintext P2 (i.e., the second desired input image).

5) Subsequently, wave propagation from the second 3-D space to the third 3-D space is conducted

$$O\left(\mu_3^{(i)}, v_3^{(i)}\right) = \mathrm{FWP}_{d_3^{(i)}}\left[\overline{O\left(\mu_2^{(i)}, v_2^{(i)}\right)}\right] \tag{7}$$

where $d_3^{(i)}$ denotes a series of axial distances (particle-like point to particle-like point) between the plaintext (P2) plane and plaintext (P3) plane.

6) A constraint is applied to update the complex-valued wavefront $O(\mu_3^{(i)}, v_3^{(i)})$

$$\overline{O\left(\mu_3^{(i)}, v_3^{(i)}\right)} = \mathrm{PSC}''\left[O\left(\mu_3^{(i)}, v_3^{(i)}\right)\right] \tag{8}$$

where PSC″ denotes plaintext-plane constraint described by [8], [15], [17]

$$\mathrm{PSC}''\left[O\left(\mu_3^{(i)}, v_3^{(i)}\right)\right] = \begin{cases} \left[2\omega O_3(\mu_3, v_3) - \left|O\left(\mu_3^{(i)}, v_3^{(i)}\right)\right|\right] O\left(\mu_3^{(i)}, v_3^{(i)}\right) \Big/ \left|O\left(\mu_3^{(i)}, v_3^{(i)}\right)\right|, & \text{if } (\mu_3, v_3) \in i \\ O\left(\mu_3^{(i)}, v_3^{(i)}\right), & \text{if } (\mu_3, v_3) \notin i \end{cases} \tag{9}$$

where $O_3(\mu_3, \nu_3)$ denotes the plaintext P3 (i.e., the third desired input image).

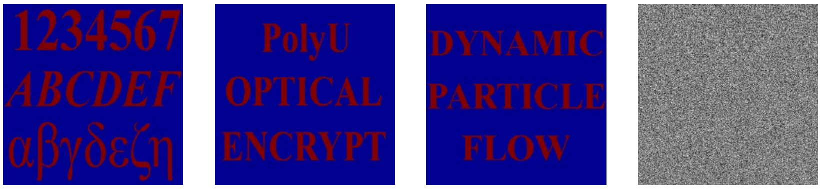
7) Wave back-propagation is conducted, and an updated phase-only mask $\overline{M^{(i,n)}(x, y)}$ is obtained

$$O\left(x^{(i)}, y^{(i)}\right) = \mathrm{FWP}_{-\left[d_1^{(i)} + d_2^{(i)} + d_3^{(i)}\right]}\left[\overline{O\left(\mu_3^{(i)}, v_3^{(i)}\right)}\right] \tag{10}$$

$$\overline{M^{(i,n)}(x, y)} = \frac{O(x^{(i)}, y^{(i)})}{|O(x^{(i)}, y^{(i)})|} \tag{11}$$

where $|\,|$ denotes modulus operation, and $\mathrm{FWP}_{-(\ldots)}$ denotes back propagation [2], [4], [16]. It is worth noting that the particle-like point index i in (1)–(11) is used to sequentially represent three particles that are placed on the same longitudinal axis, and the three particles are selected from the plaintexts P1, P2, and P3, respectively.

Equations (1)–(11) are iteratively implemented for the three particles each time until the symbol i reaches the maximum number of particle-like points, and phase-only mask (M) is sequentially updated. For instance, when the first three particles on the same longitudinal axis are processed based on (1)–(11), the updated phase-only mask (M) [see (11)] is further used for the next three particles (located on the another same longitudinal axis) starting from (1) with $i = i + 1$. After all particles are processed, the updated phase-only mask (M) will be further used for the next iteration (i.e., $n = n + 1$). After a preset threshold is satisfied, the updated phase-only mask is considered as ciphertext. For simplicity, only one phase-only mask (M) is used here, and it is straightforward to encode the plaintexts into multiple cascaded phase-only masks



(a) (b) (c) (d)

Fig. 2. (a)–(c) Three input images and (d) phase-only mask (M) extracted by using the phase retrieval algorithm during encryption. The color is used in (a)–(c) only for display purposes, and it does not mean the use of a color-image encryption strategy. Each input image in (a)–(c) contains pixel values of 1 (i.e., background pixels) and 2. Similarly, the color has also been used in Figs. 3–6 only for result display purposes.

(see Fig. 1). Different initialized phase-only masks or different thresholds can be applied to generate a varied phase-only mask (M).

During the decryption, a collimated plane wave can be generated to illuminate the extracted phase-only mask (M), and the series of axial distances is used as principal key. For instance, when the first plaintext P1 should be extracted during the decoding, security key $d_1^{(i)}$ will be required. Each particle-like point can be sequentially extracted at an axial position with a known transverse area, and a decoded input image is obtained by incorporating all decoded particles in the transverse domain. Similarly, the plaintexts P2 and P3 can be respectively decoded by using the series of axial distances $(d_1^{(i)} + d_2^{(i)})$ and $(d_1^{(i)} + d_2^{(i)} + d_3^{(i)})$. For the decryption, an optical approach can be applied by sequentially translating a CCD camera. Correlation coefficient (CC) [5] is calculated to evaluate similarity between the original input images $O_h(\mu_h, \nu_h)$ and the decrypted images $O_h{}'(\mu_h, \nu_h)$

$$\mathrm{CC}_h = \frac{\mathrm{cov}(O_h, O_h{}')}{\sigma_{O_h} \times \sigma_{O_h{}'}} \tag{12}$$

where $h = 1, 2, 3$, cov denotes cross-covariance, and σ denotes standard deviation. For the sake of brevity, coordinate (μ_h, ν_h) is omitted in (12).

3. Results and Discussion

In Fig. 1, a collimated plane wave is simulated for the illumination in the optical path, and light wavelength is 600.0 nm. Particle-like point position distributions are randomly generated, and the series of axial distances $d_1^{(i)}$, $d_2^{(i)}$, and $d_3^{(i)}$ is randomly distributed in a range of [1.0 mm, 6.0 mm], [7.0 mm, 12.0 mm] and [6.0 mm, 10.0 mm], respectively. Pixel size of 4.65 μm and 512 × 512 pixels are used in the proposed method. The 16 × 16 neighboring pixels of each plaintext are combined and generated as a particle-like point. The 1024 particle-like points are generated for each input image, and the maximum particle-like point index i is 1024. Each series of particle-like points is distributed in a specific 3-D space (see Fig. 1), and for the sake of brevity three input images (i.e., plaintexts) are investigated. It is worth noting that a digital method should be applied for the encoding, and either a digital or optical approach can be used for the decoding. During optical decryption, the generated phase-only mask M (i.e., ciphertext) can be embedded into phase-only spatial light modulator, and a series of 2-D transverse regions can be recorded via axial translation of CCD camera (i.e., through axial scanning). When 3-D particle-like point distribution is available, a decoded input image is obtained by incorporating all decoded particle-like points in the transverse domain.

Fig. 2(a)–(c) show three input images with 512 × 512 pixels which contain pixel values of 1 and 2. When the phase retrieval algorithm is applied for the encoding, after 30 iterations phase-only mask M (i.e., ciphertext) is generated and shown in Fig. 2(d). It can be seen in Fig. 2(d) that all particle-like points are encoded into phase-only mask (M), and no information about the input

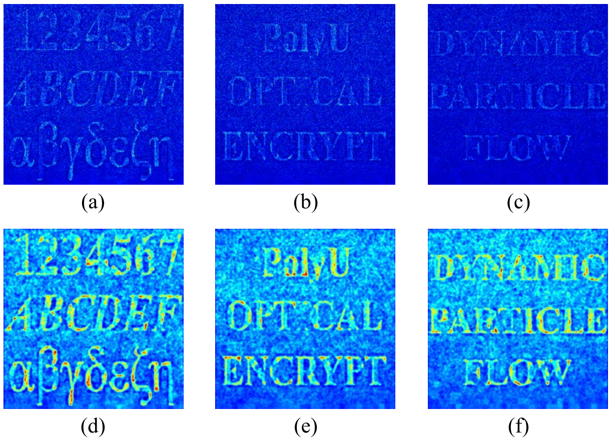


Fig. 3. (a)–(c) Decoded input images corresponding to three plaintexts P1–P3 by using correct security keys and correct phase-only mask. (d)–(f) Decoded images obtained after a Gaussian low-pass filter corresponding to (a)–(c), respectively. The color is used only for display purposes.

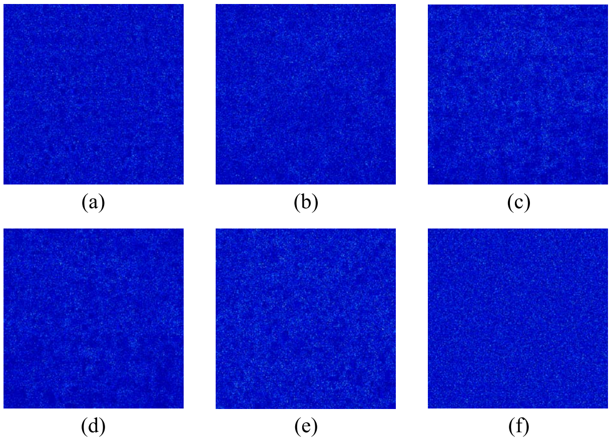
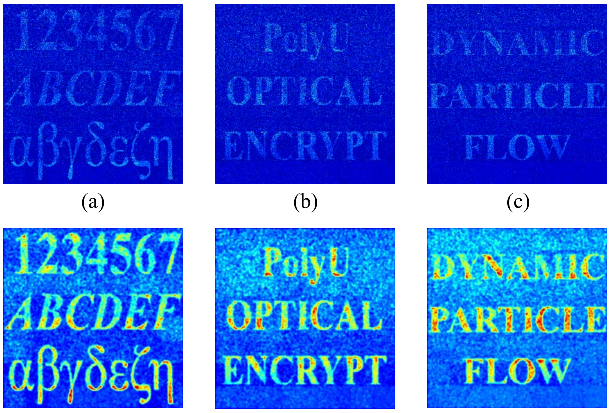


Fig. 4. Decoded input images are obtained at one section of the plaintext plane, when only one axial distance of (a) 1.0 mm, (b) 9.0 mm, (c) 20.0 mm, or (d) 22.0 mm is used. The decoded input image is obtained by using (e) a series of wrong distances and (f) a wrong phase-only mask. The color is used only for display purposes.

images can be observed after the encoding. When all security keys and the extracted phase-only mask (M) are correct, the decoded input images are obtained and shown in Fig. 3(a)–(c). The CC values for Fig. 3(a)–(c) are 0.33, 0.28, and 0.30, respectively. It can be seen that the input images are affected by noise. The noise can be suppressed by using a filter algorithm, and Fig. 3(d)–(f) show the decoded input images when Gaussian low-pass filter is used to respectively process those in Fig. 3(a)–(c). The CC values for Fig. 3(d)–(f) are 0.69, 0.63, and 0.65, respectively. It can be seen in Fig. 3(d)–(f) that quality of decoded input images is acceptable, and most information about the input images can be observed. Since 3-D particle-like points are generated and applied, system security is dramatically enhanced and any one sectional decoding cannot render information about the input images. Fig. 4(a)–(d) show the decoded input images obtained at one section of the plaintext plane, when only an axial distance of 1.0 mm, 9.0 mm, 20.0 mm, or 22.0 mm is used between phase-only mask (M) plane and the plaintext plane, respectively. The CC values for Fig. 4(a)–(d) are 0.026, 0.022, 0.048, and 0.041, respectively. It can be seen in Fig. 4(a)–(d) that the decoded input images obtained at one arbitrary section do not render the information. Performance of principal security keys and the extracted phase-only mask (M) is also analyzed,



(a) (b) (c)

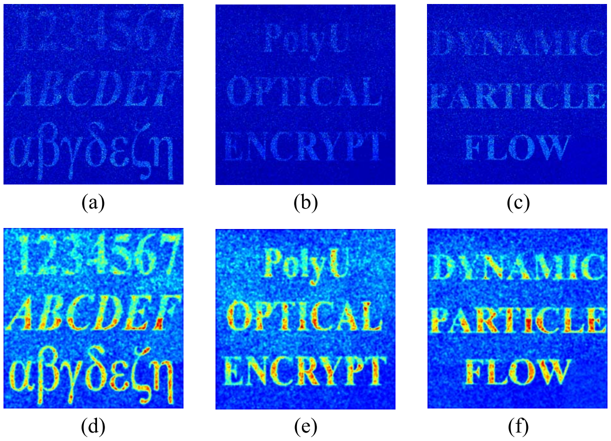
(d) (e) (f)

Fig. 5. The 64 × 64 neighboring pixels of each input image are combined as a particle-like point. (a)–(c) Decoded input images corresponding to the three plaintexts P1–P3 by using correct security keys and correct phase-only mask. (d)–(f) Decoded images obtained after a Gaussian low-pass filter corresponding to (a)–(c), respectively. The color is used only for display purposes.

and for the sake of brevity only the decoded input images corresponding to the plaintext P1 are presented here. Fig. 4(e) and (f) show the decoded input images obtained by using a series of wrong distances (within a range of [0.5 mm, 6.5 mm]) and an incorrect phase-only mask, respectively. The CC values for Fig. 4(e) and (f) are 0.037 and -0.00058, respectively. It can be seen in Fig. 4(e) and (f) that the decoded input images are noisy, when the keys or phase-only mask are incorrectly used for the decoding.

For a comparison, the different number of neighboring pixels is also combined as a particle-like point. The 64 × 64 neighboring pixels of each input image are combined and generated as a particle-like point, and other parameters are the same as those used for Fig. 3(a)–(c). When all security keys and the extracted phase-only mask (M) are correct, the decoded input images are obtained in Fig. 5(a)–(c). The CC values for Fig. 5(a)–(c) are 0.44, 0.38, and 0.41, respectively. In this case, the 64 particle-like points are generated for each input image, and the maximum particle-like point index i is 64. The noise can be further suppressed, and Fig. 5(d)–(f) show the decoded input images after Gaussian low-pass filter respectively corresponding to Fig. 5(a)–(c). The CC values for Fig. 5(d)–(f) are 0.83, 0.80, and 0.82, respectively. When the 128 × 128 neighboring pixels of each input image are combined and generated as a particle-like point, using correct keys the decoded input images are obtained in Fig. 6(a)–(c). The CC values for Fig. 6(a)–(c) are 0.39, 0.40, and 0.44, respectively. In this case, other parameters are the same as those used for Fig. 3(a)–(c). The 16 particle-like points are generated for each input image, and the maximum particle-like point index i is 16. The noise can also be suppressed, and Fig. 6(d)–(f) show the decoded input images after Gaussian low-pass filter respectively corresponding to Fig. 6(a)–(c). The CC values for Fig. 6(d)–(f) are 0.81, 0.83, and 0.84, respectively. It can be seen in Figs. 5 and 6 that when more neighboring pixels of each input image are combined as a particle-like point, the decoded input images are of higher quality [i.e., compared with those in Fig. 3(a)–(f)]. However, when more neighboring pixels are combined to generate a particle-like point, the less number of points are generated and the security could be compromised for optical multiple-image encryption.

The advantages of the proposed method and its comparison to previous work are briefly described as follows: 1) Since any one sectional decoding cannot render information about the plaintexts, attack algorithm [18], [19] cannot be applied to extract system keys. 2) All particle-like points (i.e., plaintexts) are simultaneously encoded into phase-only mask, and it is straightforward to encode the plaintexts into multiple cascaded phase-only masks for security enhancement. 3) Different from previous work [11], [13], [14], the proposed method effectively applies 3-D-space processing strategy for optical multiple-image encryption. The proposed



(a) (b) (c)

(d) (e) (f)

Fig. 6. The 128 × 128 neighboring pixels of each input image are combined as a particle-like point. (a)–(c) Decoded input images corresponding to the three plaintexts P1–P3 by using correct security keys and correct phase-only mask. (d)–(f) Decoded images obtained after a Gaussian low-pass filter corresponding to (a)–(c), respectively. The color is used only for display purposes.

method achieves the higher security than conventional approaches [11], [13] for optical multiple-image encryption, since 3-D-space processing method is applied and any sectional decryption cannot render original input information. It is also demonstrated that the proposed method provides a novel alternative for optical security [1], [3], [5], [20], [21].

4. Conclusion

A novel method using 3-D space has been proposed for optical multiple-image encryption. Each input image is divided into a series of particle-like points distributed in 3-D space, and all generated particle-like points are simultaneously encoded into a phase-only mask. The simulation results illustrate that the higher security is achieved in the proposed method for optical multiple-image encryption compared with previous work, since 3-D-space processing strategy is successfully applied.

References

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, pp. 767–769, 1995.

[2] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” *Opt. Lett.*, vol. 24, pp. 762–764, 1999.

[3] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” *Opt. Lett.*, vol. 36, pp. 22–24, 2011.

[4] W. Chen and X. Chen, “Space-based optical image encryption,” *Opt. Exp.*, vol. 18, pp. 27095–27104, 2010.

[5] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.*, vol. 6, pp. 120–155, 2014.

[6] X. F. Meng *et al.*, “Two-step phase-shifting interferometry and its application in image encryption,” *Opt. Lett.*, vol. 31, pp. 1414–1416, 2006.

[7] 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, pp. 12033–12043, 2010.

[8] W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution,” *J. Opt.*, vol. 14, 2012, Art. no. 075402.

[9] W. Chen and X. Chen, “Marked ghost imaging,” *Appl. Phys. Lett.*, vol. 104, 2014, Art. no. 251109.

[10] W. Chen and X. Chen, “Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit,” *Opt. Lett.*, vol. 38, pp. 546–548, 2013.

[11] G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” *Opt. Lett.*, vol. 30, pp. 1306–1308, 2005.

[12] R. W. Gerchberg and W. O. Saxton, “A practical algorithm for the determination of phase from image and diffraction plane pictures,” *Optik (Stuttgart)*, vol. 35, pp. 237–246, 1972.

[13] H. E. Hwang, H. T. Chang, and W. N. Lie, “Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain,” *Opt. Lett.*, vol. 34, pp. 3917–3919, 2009.

[14] W. Chen and X. Chen, “Optical multiple-image authentication based on modified Gerchberg–Saxton algorithm with random sampling,” *Opt. Commun.*, vol. 318, pp. 128–132, 2014.

[15] W. Chen and X. Chen, “Interference-based optical image encryption using three-dimensional phase retrieval,” *Appl. Opt.*, vol. 51, no. 25, pp. 6076–6083, Sep. 2012.

[16] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York, NY, USA: McGraw-Hill, 1996.

[17] C. F. Ying, H. Pang, C. J. Fan, and W. D. Zhou, “New method for the design of a phase-only computer hologram for multiplane reconstruction,” *Opt. Eng.*, vol. 50, 2011, Art. no. 055802.

[18] X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” *Opt. Lett.*, vol. 31, pp. 1044–1046, 2006.

[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, 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, 2015, Art. no. 7800310.

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