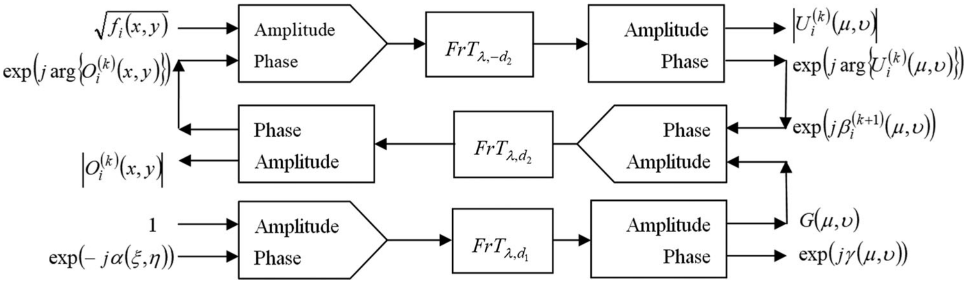
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Multiple-Image Hiding Based on Cascaded Free-Space Wave Propagation Using the Structured Phase Mask for Lensless Optical Security System

Volume 9, Number 5, October 2017

Liansheng Sui
Xiao Zhang
Ailing Tian



DOI: 10.1109/JPHOT.2017.2754290
1943-0655 © 2017 IEEE

Multiple-Image Hiding Based on Cascaded Free-Space Wave Propagation Using the Structured Phase Mask for Lensless Optical Security System

Liansheng Sui,[1,2] Xiao Zhang,[1] and Ailing Tian[3]

[1] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an
710048, China
[2] Shaanxi Key Laboratory of Network computing and Security Technology, Xi'an 710048,
China
[3] Shannxi Province Key Laboratory of Thin Film Technology and Optical Test, Xi'an
Technological University, Xi'an 710048, China

DOI:10.1109/JPHOT.2017.2754290

Manuscript received August 31, 2017; revised September 13, 2017; accepted September 15, 2017. Date of publication September 19, 2017; date of current version October 4, 2017. This work was supported in part by Xi'an Science and Technology Bureau under Grant CXY1509(3), and in part by the Key Laboratory Science Research Plan of Education Department of Shaanxi Province under Grant 16 JS079. Corresponding author: Liansheng Sui (e-mail: liudua2010@gmail.com).

Abstract: A novel optical multiple-image hiding method is proposed based on two cascaded free-space propagation transforms in this paper. With the use of the structured phase mask in the phase retrieval algorithm, a plain image is encoded to only one statistically independent phase-only mask. All retrieved phase masks are integrated into the noise-like ciphertext by using the phase mask multiplexing technique. When reconstructing an original plain image, the architecture of double random phase encoding system is directly adopted, where the structured phase mask and the corresponding decryption key mask are located at determined positions along the axis of propagation. Besides the propagation distances, the optical parameters such as wavelength, focal length, and topological charge of the structured mask are considered as the security keys to expand the key space. To the best of our knowledge, it is the first report on employing the structured phase mask in the process of phase retrieval algorithm, which can enhance the level of security greatly. Simulation results have been given to verify the feasibility and robustness of the proposed scheme.

Index Terms: Multiple-image hiding, phase retrieval algorithm, free-space propagation.

1. Introduction

Due to its marked physical characteristics such as parallel processing, multi-dimensional capabilities and multiple parameters, optical information security technology has attracted extensive attention in the past decades [1]–[3]. One of the classical techniques is double random phase encoding (DRPE) based on the architecture of $4f$ optical system, with which the plain image can be encrypted into the ciphertext with stationary white noise distribution [4]. Now, it has been extended into different optical domains such as fractional Fourier transform domain [5], Fresnel transform domain [6], gyrator transform domain [7], [8] and other domains [9], [10], where additional optical parameters can be considered as the security keys to eliminate threats caused by the intrinsic linearity of DRPE [11]–[13]. Other than DRPE and its extension, many other kinds of optical image encryption and hiding techniques such as integral imaging [14], diffractive imaging [15], photon-counting imaging [16]–[18], ghost imaging [19]–[21], polarized light encoding [22], joint transform correlator [23], interferometer [24], compressive sensing [25], [26], ptychography [27] and quick response codes [28] also have been widely investigated. Additionally, sparse representation and constraints have been employed to implement optical image encryption and authentication [29], [30].

Recently, due to efficient and enhanced security concerns, more and more researchers have paid their attentions to the multiple-image encryption and hiding schemes based on different multiplexing techniques such as wavelength multiplexing [31], position multiplexing [32], phase only mask multiplexing [33], space multiplexing [34], [35], theta modulation [36], lateral shifting [37], frequency shift [38] and spectral cropping [39] and so on. With the help of DRPE, Niu *et al.* [40] proposed a multiple-image hiding method based on interference and frequency spectrum center shift technique, where two plain images are encrypted into interference distribution. However, it should be pointed out that the interference-based method has inherent silhouette problem. The optical multiple-image processing schemes also have been investigated in different domains such as cascaded fractional Fourier transform domain [41], [42]. Wan *et al.* [43] presented a multiple-image encryption scheme based on compressive holography, which can record all information into one hologram via interference between multiple object beams and unique reference beam. Chen [44] proposed a three-dimensional space strategy for optical multiple-image encryption, which decomposed each plain image into a series of particle-like points. It is worth mentioning that Alfalou and Brosseau [45] reported an algorithm that can simultaneously compress and encrypt multiple images. Wu *et al.* [46] suggested a multiple-image encryption scheme based on computational ghost imaging, where each plain image is initially encoded into an intensity vector with different diffraction distance. This scheme has obvious disadvantage that a series of reference intensity patterns should be considered as the private keys, which makes the storage space large and transmission bandwidth tedious. To reduce storage space, Li *et al.* [47] proposed a multiple-image encryption approach based on compressive ghost imaging and coordinate sampling, in which random phase-only masks are generated with the modified logistic map algorithm. In addition, the iterative phase retrieval technique such as the modified Gerchberg-Saxton algorithm usually is employed to encrypt multiple-image, where the affection of cross-talk noise could be eliminated as soon as possible [48], [49].

In this paper, a novel multiple-image hiding method based on two cascaded free-space wave propagation transforms is proposed, which has enhanced security due to the use of the structured phase mask. Initially, a phase retrieval algorithm is suggested to encode each plain image to only one phase-only mask, where the optical parameters such as focal length, illuminating wavelength and topological charge of the structured phase mask can be considered as the security keys, which results in the significant enlargement of the key space. Subsequently, all retrieved phase-only masks are synthesized into the ciphertext with the noise-like distribution by directly adopting the phase mask multiplexing, where the corresponding decryption key for each plain image is simultaneously generated. There are two advantages: one is the hiding scheme can avoid the affection of cross-talk noise to some degree; another is the number of plain images to be encrypted can be enlarged. Because only one decryption key is generated for one plain image, the amount of phase mask key is reduced greatly. Therefore, the management of decryption key such as storage and transmission becomes very expedient. The plain image can be easily reconstructed with high quality by using the optical setup similar to the architecture of double random phase encoding system. Via two cascaded free-space wave propagation transforms, the reconstructed image that resemble closely to the original one can be recorded in the output image plane. Notably, an enhanced level of security can be obtained due to high sensitivity of the security keys. Compared with the previous work in Ref. [50], where three phase masks planes are employed in the process of iterative algorithm, the mechanism of the proposed scheme is simple, which is similar to the double random phase encoding system.

The rest of this paper is organized as follows. In Section 2, the proposed algorithm including the encryption and decryption process is introduced in detail, in which the phase retrieval algorithm using the structured phase mask is described. Meanwhile, the synthesis process of ciphertext

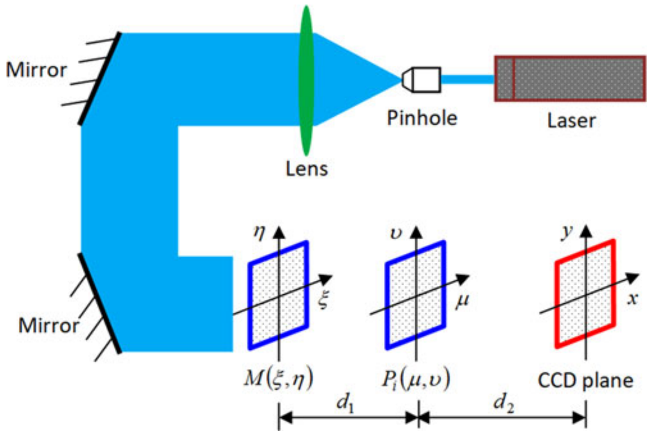


Fig. 1. Schematic setup for hiding a plain image into only one phase-only mask through the phase-only optical system: $M(\xi,\eta)$ is the structured phase mask and $P_i(\mu,\upsilon)$ is the phase-only mask; CCD, charge-coupled device, is used to record the plain image; d_1 and d_2 are propagation distances.

based on the phase mask multiplexing technique is discussed. In Section 3, numerical simulation results and security analysis are carried out. Finally, a brief conclusion is given in Section 4.

2. Proposed Algorithm

Let $f_i(x,y),\ i=1,2,\ldots,K$ denotes a series of different plain images and K denotes the maximum number of these images. Initially, each plain image $f_i(x,y)$ is optically hidden into only one phase-only mask $P_i(\mu,\upsilon)$ by using an iterative phase retrieval algorithm. Subsequently, the noise-like ciphertext $C(\mu,\upsilon)$ is synthesized with these statistically independent phase-only masks by adopting the phase mask multiplexing technique. Simultaneously, the decryption key $D_i(\mu,\upsilon)$ is engendered for the corresponding plain image $f_i(x,y)$.

Fig. 1. depicts a schematic setup for a phase-only optical system, with which the approximated phase-only mask $P_i(\mu,\upsilon)$ can be retrieved under the constraints such as the intensity of plain image and optical parameters. The laser beam collimated by the combination of a pinhole and a lens is incident vertically on the structured phase mask $M(\xi,\eta)$ with complex transmittance of $exp(-j\alpha(\zeta,\eta))$, where $j=\sqrt{-1}$ and $\alpha(\xi,\eta)$ is the phase distribution. The complex transmittance in the phase-only mask plane $P_i(\mu,\upsilon)$ is denoted as $\exp(j\beta_i(\mu,\upsilon))$, where the phase distribution $\beta_i(\mu,\upsilon)$ is statistically independent white sequence in $[0,2\pi]$. Symbols (ξ,η), (μ,υ) and (x,y) denote coordinates of the structured phase mask plane, the phase-only mask plane and the image plane, respectively. Just like similar optical setup in other schemes [51], it can minimize the hardware requirement such as expensive transformative lenses, which makes it not only has high efficiency but also is easy to be implemented optically.

To illustrate the adopted iterative phase retrieval algorithm, the iteration process for hiding the plain image $f_i(x,y)$ into only one phase-only mask $P_i(\mu,\upsilon)$ is described as follows

1) The complex-valued wavefront $O_i^{(k)}(x,y)$ obtained in the image plane can be expressed as

$$O_i^{(k)}(x,y) = FrT_{\lambda,d_2}\left(\left|\left\{FrT_{\lambda,d_1}\left(\exp\left(-j\alpha\left(\xi,\eta\right)\right)\right)\right\}\right|\exp\left(j\beta_i^{(k)}\left(\mu,\upsilon\right)\right)\right), \tag{1}$$

where FrT denotes the free-space wave propagation transform [29], [30], $|\cdot|$ denotes a modulus operation, λ denotes light wavelength, the parameters d_1 and d_2 denote propagation distances, the subscript k represents the approximated functions at the kth iteration of the retrieval process. In the initial stage, the phase distribution $\beta_i^{(1)}(\mu,\upsilon)$ is generated by using random phase function.

2) The constraint with the known plain image $f_i(x, y)$ is applied to update the amplitude part of the above-obtained complex wavefront, which satisfies

$$\hat{O}_i^{(k)}(x, y) = \sqrt{f_i(x, y)}O_i^{(k)}(x, y) \,/\, \left|O_i^{(k)}(x, y)\right|, \tag{2}$$

where $\hat{O}_i^{(k)}(x, y)$ denotes the modified wavefront in the image plane.

3) The modified wavefront in the image plane is inversely Fresnel-transformed back to the phase-only mask plane to obtain a new diffraction space wave function, which can be mathematically described as

$$U_i^{(k)}(\mu, \upsilon) = FrT_{\lambda,-d_2}\left(\hat{O}_i^{(k)}(x, y)\right), \tag{3}$$

where $FrT_{\lambda,-d_2}$ denotes the free-space wave back-propagation operation with the axis distance d_2.

4) The phase part of the complex wavefront $U_i^{(k)}(\mu, \upsilon)$ is retained by truncating its amplitude, with which a new complex transmittance in the phase-only mask plane can be obtained as

$$\beta_i^{(k+1)}(\mu, \upsilon) = \arg\left\{U_i^{(k)}(\mu, \upsilon)/\left|U_i^{(k)}(\mu, \upsilon)\right|\right\}, \tag{4}$$

$$P_i^{(k+1)}(\mu, \upsilon) = \exp\left(j\beta_i^{(k+1)}(\mu, \upsilon)\right). \tag{5}$$

where $\arg\{\cdot\}$ is used to calculate the phase distribution of the argument.

5) Together with $M(\xi, \eta) = \exp(-j\alpha(\xi, \eta))$, the updated phase mask $P_i^{(k+1)}(\mu, \upsilon)$ is used to calculate the estimated plain image denoted as $\hat{f}_i^{(k+1)}(x, y)$. First, the complex wavefront in the image plane is modified as follows

$$O_i^{(k+1)}(x, y) = FrT_{\lambda,d_2}\left(\left|\left\{FrT_{\lambda,d_1}\left(\exp\left(-j\alpha(\xi, \eta)\right)\right)\right\}\right| \exp\left(j\beta_i^{(k+1)}(\mu, \upsilon)\right)\right), \tag{6}$$

Then, the estimated plain image can be constructed as

$$\hat{f}_i^{(k+1)}(x, y) = \left|O_i^{(k+1)}(x, y)\right|^2. \tag{7}$$

6) To monitor when the iterative process will stop, the correlation coefficient (CC) between the plain image $f_i(x, y)$ and the estimated one $\hat{f}_i^{(k+1)}(x, y)$ is calculated as the convergent criterion, which is defined as

$$\mathrm{CC} = \frac{E\left[\left[f_i - E[f_i]\right]\left[\hat{f}_i^{(k+1)} - E\left[\hat{f}_i^{(k+1)}\right]\right]\right]}{\sqrt{E\left[\left[f_i - E[f_i]\right]^2\right]}\sqrt{E\left[\left[\hat{f}_i^{(k+1)} - E\left[\hat{f}_i^{(k+1)}\right]\right]^2\right]}}, \tag{8}$$

where $E[\cdot]$ represents the expected value operator of the argument. For brevity, the coordinates of images are omitted.

7) Usually, a threshold value very close to 1 is defined to guarantee high quality of the estimated image. Repeat above steps until the calculated result reaches the defined threshold or maximum iterations.

Once the convergent criterion is satisfied, the estimated plain image will be eventually reconstructed. Suppose the iterative process stop right after the Nth iteration, the relationship between the estimated plain image $\hat{f}_i^{(N+1)}(x, y)$, phase masks $\exp(-j\alpha(\xi, \eta))$ and $\exp(j\beta_i^{(N+1)}(\mu, \upsilon))$ can be deduced as

$$\hat{f}_i^{(N+1)}(x, y) = \left|FrT_{\lambda,d_2}\left(\left|\left\{FrT_{\lambda,d_1}\left(\exp\left(-j\alpha(\xi, \eta)\right)\right)\right\}\right| \exp\left(j\beta_i^{(N+1)}(\mu, \upsilon)\right)\right)\right|^2. \tag{9}$$

Defining the phase-only mask $P_i(\mu, \upsilon)$ as

$$P_i(\mu, \upsilon) = \exp\left(-j\gamma(\mu, \upsilon)\right)\exp\left(j\beta_i^{(N+1)}(\mu, \upsilon)\right), \tag{10}$$

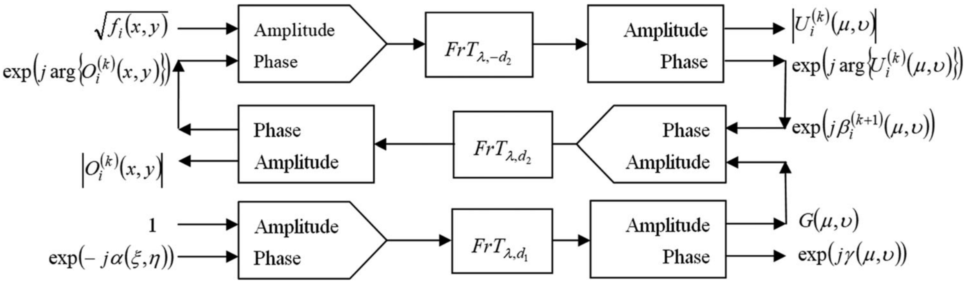


Fig. 2. Diagram of the phase retrieval process using the structured phase mask. Notably, the structured phase mask is first Fresnel-transformed in each cycle. The amplitude of the resultant, denoted as $G(\mu,\upsilon) = |\{FrT_{\lambda,d_1}(\exp(-j\alpha(\xi,\eta)))\}|$, is used as the constraint to update the complex-valued wavefront in the phase-only mask plane.

where the phase distribution $\gamma(\mu,\upsilon)$ is obtained as

$$\gamma(\mu,\upsilon) = \arg\left\{FrT_{\lambda,d_1}(\exp(-j\alpha(\xi,\eta)))/\left|FrT_{\lambda,d_1}(\exp(-j\alpha(\xi,\eta)))\right|\right\}, \tag{11}$$

Thus, the estimated plain image can be reconstructed via two cascaded free-space wave propagation transforms with the help of the architecture of double random phase encoding system, which is mathematically expressed as

$$\hat{f}_i^{(N+1)}(x,y) = \left|FrT_{\lambda,d_2}\left(\left\{FrT_{\lambda,d_1}(M(\xi,\eta))\right\}P_i(\mu,\upsilon)\right)\right|^2. \tag{12}$$

In order to further illustrate the aforementioned phase retrieval process, a diagram of hiding a plain image into only one phase-only mask is shown in Fig. 2, where the phase distribution $\alpha(\xi,\eta)$ is deduced from the structured phase mask $M(\xi,\eta)$ and keeps unchanged in the entire iteration process. Obviously, different from the conventional phase retrieval algorithm where a plain image is encoded into two statistically independent phase-only masks, only one mask $\exp(j\beta_i^{(N+1)}(\mu,\upsilon))$ is engendered from the iterative process in the proposed algorithm.

It should be pointed out that the structured phase mask $M(\xi,\eta)$ shown in Fig. 1 is generated based on the combination of Fresnel zone plate and radial Hilbert mask in the aforementioned phase retrieval algorithm, which can be described as

$$M(\xi,\eta) = \exp\{-j\{\arg\{F(r)\} + \arg\{H(\rho,\theta)\}\}\}, \tag{13}$$

So, its phase distribution $\alpha(\xi,\eta)$ satisfies

$$\alpha(\xi,\eta) = \arg\{F(r)\} + \arg\{H(\rho,\theta)\}, \tag{14}$$

The function $F(r)$ is the complex field amplitude of Fresnel zone plate, which can be expressed as

$$F(r) = \exp\left\{-j\frac{\pi}{\lambda f}r^2\right\}, \tag{15}$$

where the parameter r is the radius and f is the focal length of the diffractive optical element. The function $H(\rho,\theta)$ is the phase function in log-polar coordinates (ρ,θ) of radial Hilbert mask, which can be given as

$$H(\rho,\theta) = \exp\{jP\theta\}, \tag{16}$$

where the parameter P called as topological charge denotes the order of transformation. Recently, the structured phase mask has attracted increasing attention in the field of optical information security. Muhammad [52] proposed a color image encryption system in gyrator transform domain based on the double random phase encoding, where two random phase masks respectively located in the spatial plane and frequency plane are substituted with the structured ones. These structured phase masks are generated based on the Fresnel zone plate, where the optical parameters such as focal length and wavelength can be considered as encryption keys to enhance the level of security. Further, Singh *et al.* [53] proposed a double phase-images encryption scheme using gyrator transforms, where the approximate double random phase encoding are applied. After two cascaded transforms, the intermediate images are bonded with the structured phase mask to improve the security. This structured phase mask is generated based on devil's vortex Fresnel lens and possesses characteristics of various keys in a single mask. Due to its enhanced security, Yadav *et al.* [54] proposed a phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask, in which the problem of axis alignment in optical setup can be overcome. Obviously, the structured phase masks have great potential for information security. Different from aforementioned schemes, the structured phase mask is not only used to guarantee the security but also used in the phase retrieval process to encode the plain image into only one phase-only mask.

When all plain images are encoded into the respective phase-only masks $P_i(\mu, \upsilon)$, the ciphertext $C(\mu, \upsilon)$ with noise-like distribution can be synthesized by integrating these statistically independent masks directly with the use of the phase mask multiplexing technique, which can be mathematically expressed as

$$C(\mu, \upsilon) = \exp\left(j\sum_{i=1}^{K} \arg\{P_i(\mu, \upsilon)\}\right). \tag{17}$$

The corresponding decryption key $D_k(\mu, \upsilon)$ for each plain image $f_k(x, y)$ is obtained as

$$D_k(\mu, \upsilon) = \exp\left(j\sum_{i=1, i\neq k}^{K} \arg\{P_i(\mu, \upsilon)\}\right). \tag{18}$$

When an authorized user wants to reconstruct the plain image $\hat{f}_i(x, y)$ using (12), the necessary phase-only mask $P_i(u, v)$ can be calculated by the following way as

$$P_i(\mu, \upsilon) = C(\mu, \upsilon) \times conj\{D_i(\mu, \upsilon)\}, \tag{19}$$

where $conj\{\cdot\}$ is used to compute the conjugation of the argument. Because the formation of ciphertext is implemented based on the phase mask multiplexing technique, the decryption process can be carried out efficiently without any affection of cross-talk noise. Most importantly, the encrypted capacity of the multiple-image encryption scheme is expanded considerably, which indicates that the number of encrypted plain images can be enlarged. In the construction process using the double random phase encoding system, the structured phase mask is placed into the spatial plane while the phase-only mask generated with (19) is placed into the frequency plane.

Different from the phase retrieval algorithm based on the architecture of double random phase encoding system, only one phase-only mask is retrieved in the proposed scheme. No matter this phase mask is used as the secret key or the ciphertext, it is easily distributed, stored and memorized. Besides the propagation distances d_1 and d_2, the optical parameters such as light wavelength λ and topological charge P included in the structured phase mask can be used as the security keys, which indicates that the security of the encryption scheme can be enhanced greatly. It also should be pointed out that the vexing information disclosure problem usually caused by the phase truncation and preservation operations, which make the security keys and the ciphertext useless as described in [55], can be thoroughly avoided because the retrieved phase-only mask $P_i(\mu, \upsilon)$ is formulated by the multiplication of two masks, i.e., $\exp(j\beta_i^{(N+1)}(\mu, \upsilon))$ and $\exp(-j\gamma(\mu, \upsilon))$. In addition, it is worth noting that the structured phase mask is subtly applied in the phase retrieval process in the proposed scheme, which is different from the modified Gerchberg-Saxton algorithm described in [48], [49] where the constant image placed in the output plane is used as the constraint condition.

3. Results and Security Analysis

To confirm the feasibility and robustness of the proposed multiple-image encryption scheme, a set of numerical simulations have been carried out. First, four images with the size of 256 × 256

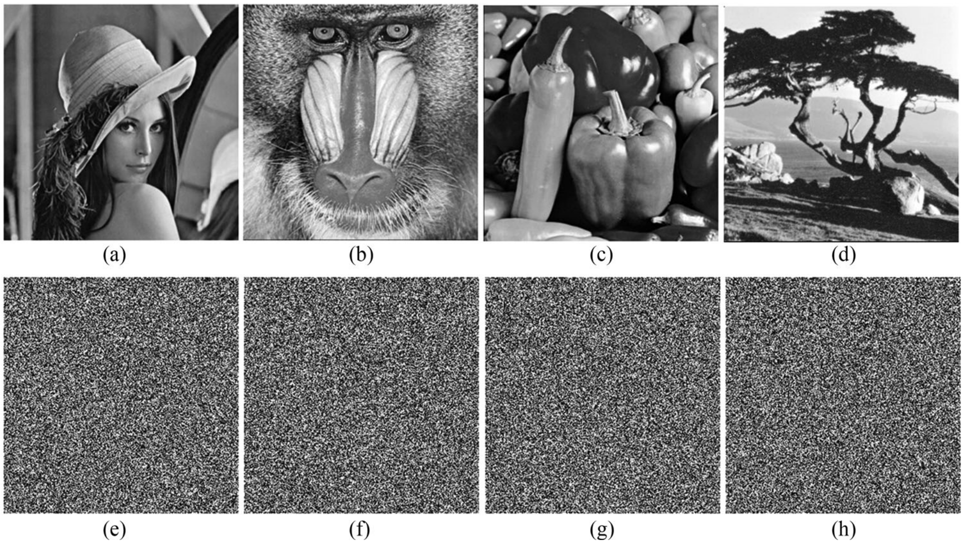


Fig. 3. (a)–(d) Original plain images and (e)–(h) phase-only masks respectively corresponding to (a)–(d).

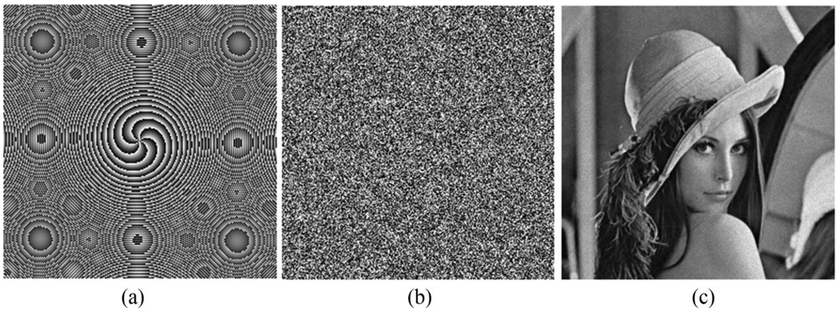


Fig. 4. (a) The phase distribution of structured phase mask, (b) ciphertext and (c) decrypted image "Lena".

pixels shown in Fig. 3(a)–(d) are used as the plain images to be encrypted, which are chosen from the USC-SIPI image databases [56]. The illumination wavelength λ of the incident unity plane wave is 632 nm, two propagation distances are 30 mm and 50 mm, respectively, and the pixelsize in the image plane is 8 um. The focal length in the structured phase mask $M(\xi, \eta)$ is 40 mm, and the topological charge is 6. The retrieved phase-only masks obtained by using the phase retrieval algorithm expressed with (1)–(8) are respectively shown in Fig. 3(e)–(h), from which any original structured information cannot be discerned with the naked eyes. The phase distribution of the structured phase mask generated based on the Fresnel zone plate and radial Hilbert mask is shown in Fig. 4(a), while the ciphertext with the noise-like distribution is displayed in Fig. 4(b). For simplicity, only one reconstructed image called as "Lena" is depicted in Fig. 4(c), which is decrypted with all correct secret keys such as the decryption key expressed in (18) and other security keys. Obviously, the reconstructed result has high quality without any noise and distortion. Similar results are obtained for other plain images "Baboon", "Peppers" and "Tree".

To analyze the sensitivity of security keys such as focal length f, illumination wavelength λ and topological charge P of the structured phase mask besides the axial distances in two free-space wave propagation operations, the ciphertext is decrypted with at least one wrong key as well as other correct keys. Fig. 5(a)–(e) show the reconstructed results about the plain image "Lena" when one of the security keys is wrong. Fig. 5(a) and (b) show the decrypted images when two axial distances respectively have tiny change as 0.4 mm and 3 mm, from which it is obvious that the first propagation distance has higher sensitivity. Fig. 5(c) shows the decrypted image when the focal

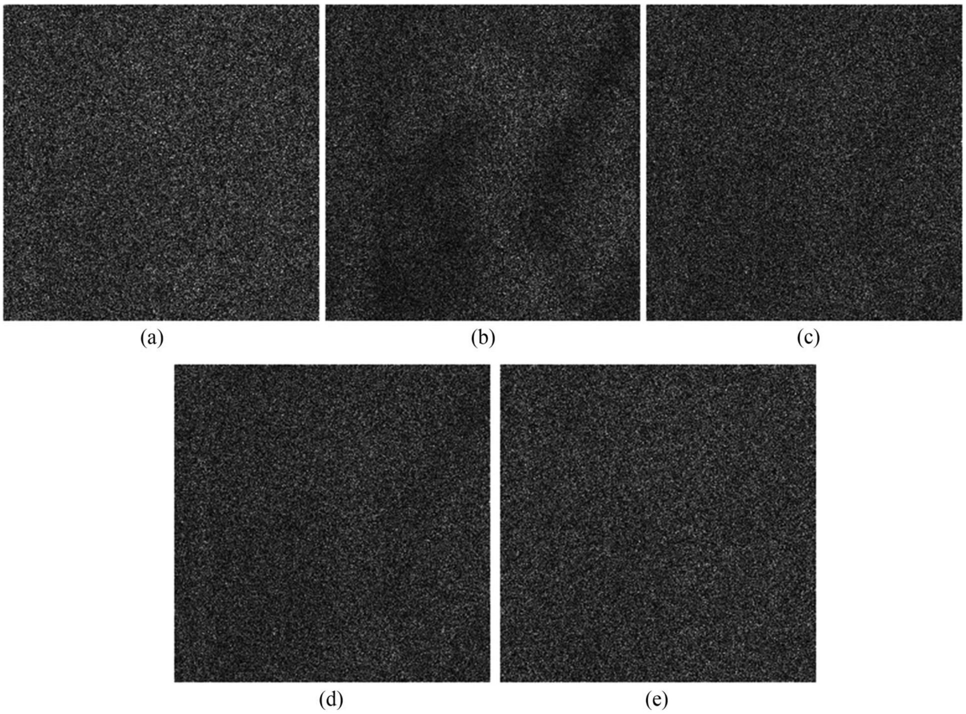


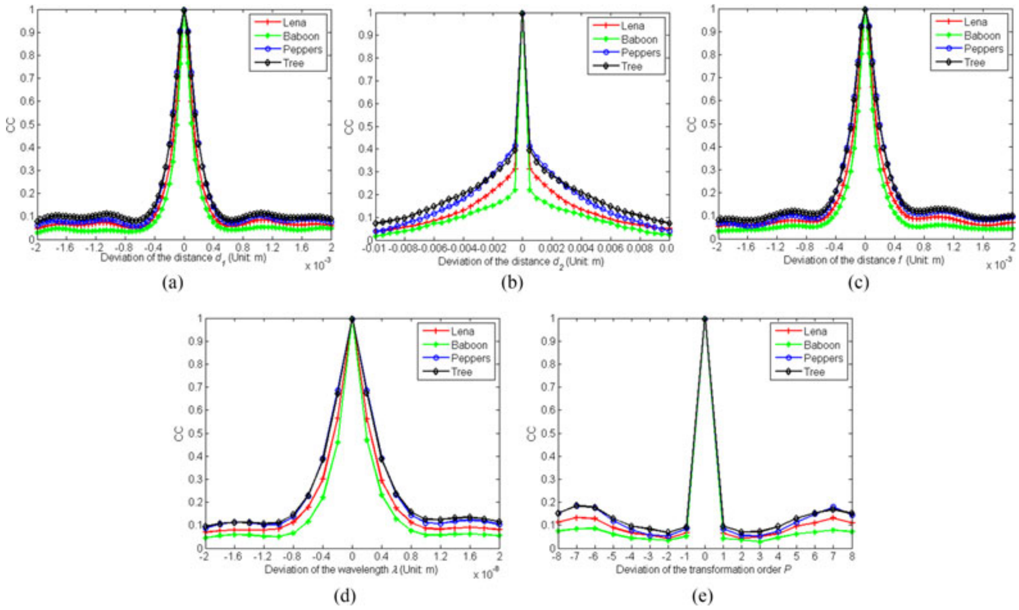
Fig. 5. Decrypted “Lena” with (a) wrong d_1, (b) wrong d_2, (c) wrong f, (d) wrong $\lambda$and (e) wrong P.

length has the tiny change as 0.5 mm. Fig. 5(d) displays the decrypted one when the illuminating wavelength has the tiny change as 8 nm. Fig. 5(e) displays the decrypted one when the topological charge of the radial Hilbert mask is 7. It can be seen from Fig. 5. that it is hardly to distinguish any valid information from these noise images when one of the security keys has the slight deviation. For other plain images, similar conclusion can be verified. The relationship curves between the CC values and the deviation of the security keys are depicted in Fig. 6(a)–(e). For any of security keys, the CC value is very close to 1 if its deviation approaches to 0. Otherwise, the CC value decreases sharply. Consequently, it is sure that the proposed scheme can actually enhance the security in the process of decryption.

Because there is a great possibility to alter the ciphertext during the storage and transmission, for example, the ciphertext image usually can be interfered by some noise as well as the information may be partially lost, the robustness against noise and occlusion attack should be checked. Suppose the ciphertext image is contaminated with the Gaussian random noise. In order to test the degree of noise immunity, the strength of noise varies from the lowest to the highest. The detailed mode can be mathematically expressed as

$$C'(\mu, \upsilon) = C(\mu, \upsilon) \times (1 + kG(\mu, \upsilon)), \tag{20}$$

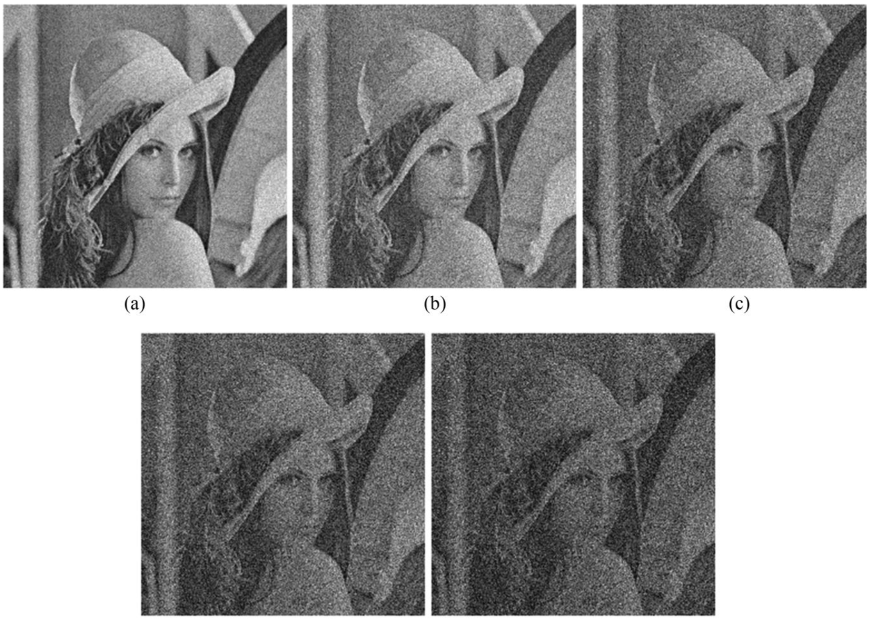
where $C'(\mu, \upsilon)$ is the contaminated image and $G(\mu, \upsilon)$ is the Gaussian noise with zero-mean and 0.2 standard deviation, the coefficient k is the nose strength. Fig. 7(a)–(e) respectively show the noise-affected decrypted images “Lena” when the noise strength varies from 0.2 to 1.0. It can be seen that most of the information in the plain image is easily recognized from the decrypted result with naked eyes, even the noise strength achieves the maximum value. In the process of analyzing occlusion attack, the ciphertext image is destroyed by cropping the pixels to some extent. Fig. 8(a) and (b) show the ciphertext images with 12.5% and 25% occlusion, respectively, which means that there are a large amount of pixels in the ciphertext image from the left side to be discarded. Fig. 8(c) and (d) display the corresponding decrypted images. Although the quality of decrypted image drastically drops with the increase of occluded area, the main information of original plain



(a) (b) (c)

(d) (e)

Fig. 6. Relationship curves between CC with (a) deviation of d_1, (b) deviation of d_2, (c) deviation of f, (d) deviation of λ and (e) deviation of P.



(a) (b) (c)

(d) (e)

Fig. 7. Decrypted "Lena" with (a) $k = 0.2$, (b) $k = 0.4$, (c) $k = 0.6$, (d) $k = 0.8$ and (e) $k = 1.0$.

image can be recognized visually. Similar results can be verified for other plain images. Evidently, it can be concluded that the proposed scheme has high robustness against some common attacks such as noise and occlusion attack.

As we all know, a secure image encryption scheme should be immune to the statistical attacks. To prove the security of the proposed scheme, two aspects of statistical attack on histogram and correlation analyses are carried out. As an important statistical evaluation index, the histogram of image usually leaks distributed information of the intensity of pixels. For an image encryption,

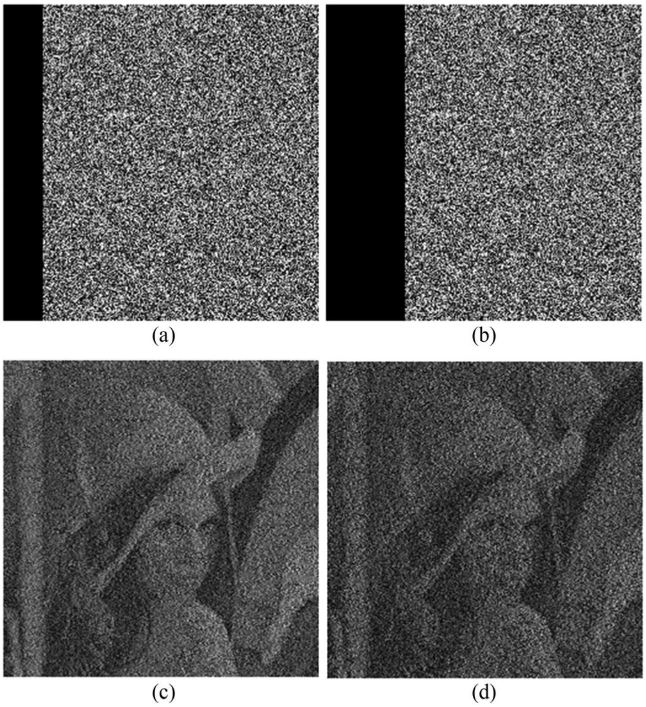


Fig. 8. Ciphertext with (a) 12.5% occlusion, (b) 25% occlusion, (c) decrypted image from (a) and (d) decrypted image from (b).

it is best that the histogram of ciphertext is uniformly distributed and the histograms of different ciphertext images are similar to each other. Fig. 9(a) is the histogram of the ciphertext shown in Fig. 4(b), while Fig. 9(b) is the histogram of the decryption key about the plain image “Lena”. Obviously, the histogram is uniformly distributed regardless of ciphertext or decryption key. Similar results are obtained for other decryption keys. Additionally, a different ciphertext is obtained by encrypting other four plain images called as “Zelda”, “Elaine”, “House” and “Man”, which also are selected from USC-SIPI image databases. The corresponding histograms about this ciphertext and the decryption keys of “Zelda” are shown in Fig. 9(c) and (d), respectively, which also have the uniform distributions. Hence, it is concluded that the proposed scheme can efficiently resist against the histogram attack.

Correlation analysis is usually used to reflect the degree of closed relation between two variables. According to an image, the adjacent pixels can be correlated in three directions, i.e., horizontal, vertical and diagonal directions. Practically, if the correlation of adjacent pixels in the ciphertext image is lower, the performance of the encryption scheme is higher. To evaluate the degree of correlation, the 3000 pairs of adjacent pixels in three different directions are randomly selected from the plain image “Lena” and the ciphertext shown in Fig. 4(b), where the correlation coefficients on a group of adjacent pixels (x_i, y_i) are calculated as

$$Cor = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}}, \tag{21}$$

where $\bar{x} = 1/N \sum_{i=1}^{N} x_i$ and $\bar{y} = 1/N \sum_{i=1}^{N} y_i$. Fig. 10(a)–(c) respectively show the horizontal, vertical and diagonal correlation of adjacent pixels in the plain image “Lena”, while Fig. 10(d)–(f) show the corresponding results of the ciphertext. From Fig. 10, it is easily deduced that the correlation of the plain image is strong in all directions, while the correlation of the ciphertext has uniform distribution in three directions. The detailed results about correlation coefficients for all plain images shown in

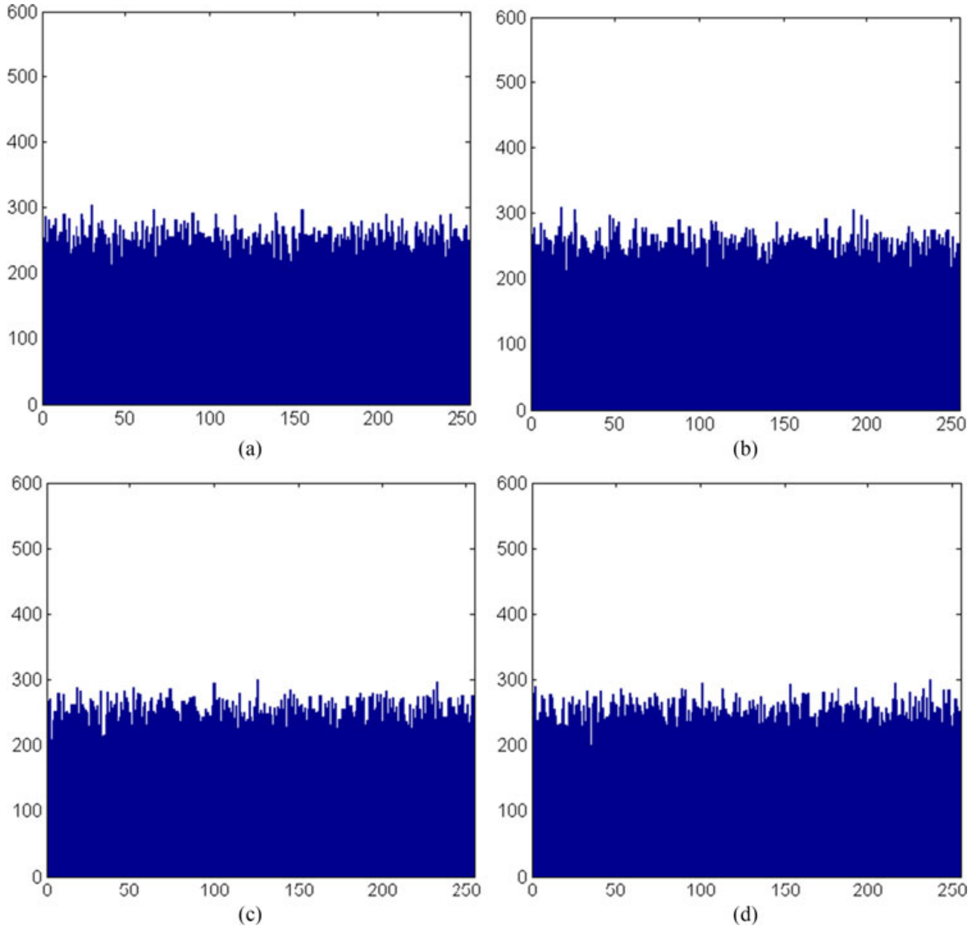


Fig. 9. Histogram of (a) ciphertext shown in Fig. 4(b), (b) decryption key of "Lena", (c) ciphertext of other four plain images "Zelda", "Elaine", "House" and "Man" and (d) decryption key of "Zelda".

Table 1

Correlation Coefficients of Plain Images Shown in Fig. 3(a)–(d) and the Ciphertext

Correlation coefficients	Plain image				Ciphertext
	Lena	Baboon	Peppers	Tree	
Horizontal	0.9465	0.8643	0.9683	0.9690	-0.0268
Vertical	0.9690	0.8325	0.9751	0.9511	0.0135
Diagonal	0.9170	0.7929	0.9448	0.9385	0.0103

Fig. 3(a)–(d) and ciphertext are given in Table 1, from which it is safe to say that the correlation of adjacent pixels in the plain images has been successfully removed via the process of encryption. So, the proposed scheme has excellent capability to resist against correlation analysis.

In a nutshell, there are two obvious characteristics in the proposed scheme. One is that security of the encryption system can be enhanced greatly because the optical parameters in one structured

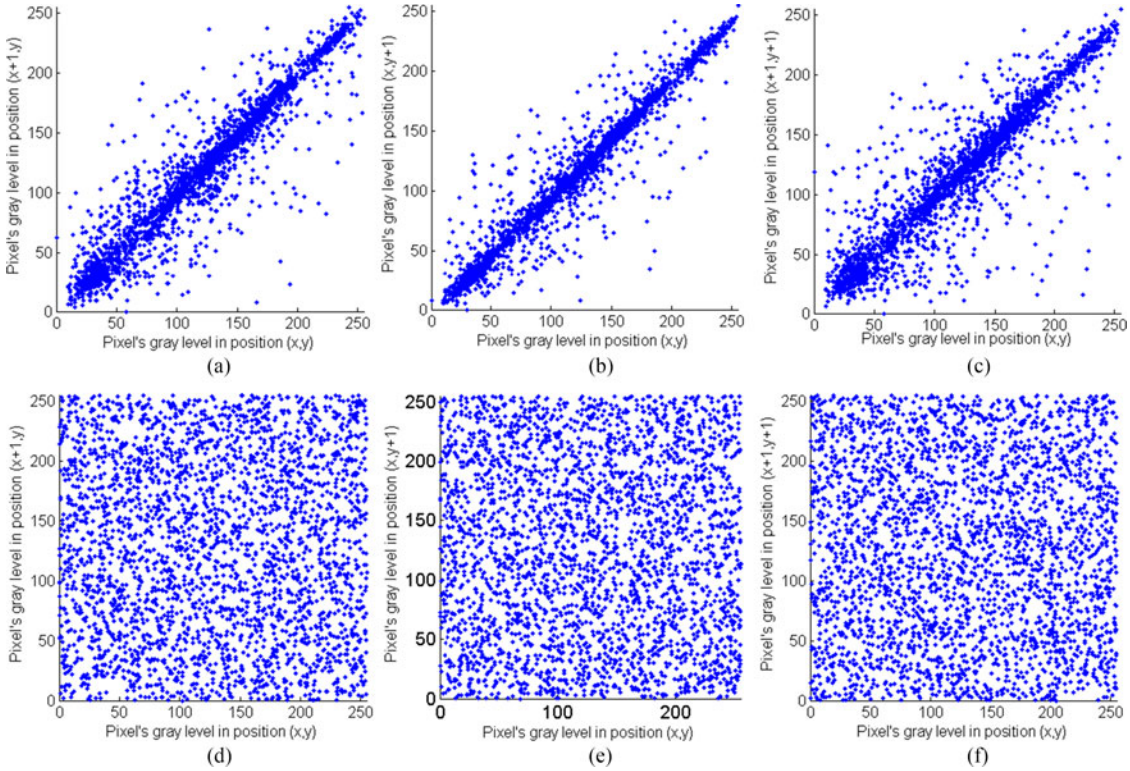


Fig. 10. Correlation distribution of (a) horizontal direction in "Lena", (b) vertical direction in "Lena", (c) diagonal direction in "Lena", (d) horizontal direction in the ciphertext, (e) vertical direction in the ciphertext and (f) diagonal direction in the ciphertext.

phase mask can be considered as security keys, which have high sensitivity demonstrated in aforementioned analyses. Another is that the phase retrieval process is simple, which can be performed in the conventional architecture of double random phase encoding. In Ref. [50], there are three phase mask planes in the iterative process, and the beam is modulated into the optical vortex beam with the structured phase plane. The structured phase plane is generated based on the spiral phase plate, where only the topological charge is used as security key. Compared with the mechanism of the proposed scheme, the related optical setup in this scheme is somewhat complicated.

4. Conclusion

In summary, an optical multiple-image hiding scheme based on two cascaded free-space wave propagation is proposed. It is featured of only one phase-only mask retrieved from a plain image by using the proposed phase retrieval algorithm, where the structured phase mask generated based on the Fresnel zone plate and radial Hilbert mask has played an important role. The use of the parameters such as focal length, illuminating wavelength and topological charge of the structured phase mask as security keys can improve the security level of the cryptosystem consequently. Adopting the phase mask multiplexing technique, all retrieved phase-only masks are encrypted to the noise-like ciphertext, which can avoid the affection of cross-talk noise in the previous multiple-image encryption schemes. Due to the expanded image hiding capacity, the number of plain images to be encrypted nearly has no any limitation. In the decryption process, the approximated image can be reconstructed using the architecture of double random phase encoding, where the structured phase mask is placed into the spatial plane and the corresponding phase-only mask placed into the frequency plane. Simulation results show that the proposed scheme works very well and has high feasibility and robustness in different aspects such as key sensitivity, noise attack, occlusion attack, and histogram attack and correlation analysis and so on.

References

[1] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photon.*, vol. 1, no. 3, pp. 589–636, Nov. 2009.
[2] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, Jun. 2014.
[3] A. Alfalou and C. Brosseau, "Recent advances in optical image processing," *Prog. Opt.*, vol. 60, pp. 119–262, 2015.
[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] J. Lang and Z. G. Zhang, "Blind digital watermarking method in the fractional Fourier transform domain," *Opt. Laser Eng.*, vol. 53, pp. 112–121, Feb. 2014.
[6] Z. Liu *et al.*, "Securing color image by using phase-only encoding in Fresnel domains," *Opt. Lasers Eng.*, vol. 68, pp. 87–92, May 2015.
[7] J. X. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and H. Yu, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains," *Opt. Lasers Eng.*, vol. 66, pp. 1–9, Mar. 2015.
[8] L. Sui, B. Zhou, X. Ning, and A. Tian, "Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain," *Opt. Exp.*, vol. 24, no. 1, pp. 499–515, Jan. 2016.
[9] L. Sui, K. Duan, J. Liang, and X. Hei, "Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps," *Opt. Exp.*, vol. 22, no. 9, pp. 10605–10621, May 2014.
[10] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional mellin transform," *Opt. Commun.*, vol. 343, pp. 10–21, May 2015.
[11] A. Carnicer, M. Monters-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, no.13, pp. 1644–1647, Jul. 2005.
[12] 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, no. 8, pp. 1044–1047, Apr. 2006.
[13] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 31, no. 22, pp. 3261–3263, Nov. 2006.
[14] X. W. Li and I. K. Lee, "Robust copyright protection using multiple ownership watermarks," *Opt. Exp.*, vol. 23, no. 3, pp. 3035–3046, Feb. 2015.
[15] I. Mehra and N. K. Nishchal, "Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging," *Opt. Lasers Eng.*, vol. 68, pp. 74–82, May 2015.
[16] D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, and B. Javidi, "Optical encryption using photon-counting polarimetric imaging," *Opt. Exp.*, vol. 23, no. 2, pp. 655–666, Jan. 2015.
[17] E. Perez-Cabre, E. A. Mohammed, M. S. Millan, and H. L. Saadon, "Photon-counting multifactor optical encryption and authentication," *J. Opt.*, vol. 17, no. 2, Feb. 2015, Art. no. 025706.
[18] S. K. Rajput, D. Kumar, and N. K. Nishchal, "Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking," *J. Opt.*, vol. 16, no. 12, Dec. 2014, Art. no. 125406.
[19] M. Zafari, R. kheradmand, and S. Ahmadi-Kandjani, "Optical encryption with selective computational ghost imaging," *J. Opt.*, vol. 16, no. 10, Oct. 2014, Art. no. 105405.
[20] L. Wang, S. Zhao, W. Cheng, L. Gong, and H. Chen, "Optical image hiding based on computational ghost imaging," *Opt. Commun.*, vol. 366, pp. 314–320, May 2016.
[21] W. Chen, "Optical data security system using phase extraction scheme via single-pixel detection," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7801507.
[22] A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona, Y. Huang, and B. Javidi, "Security authentication using phase-encoded nanoparticle structures and polarized light," *Opt. Lett.*, vol. 40, no. 2, pp. 135–138, Jan. 2015.
[23] I. Mehra, S. K. Rajput, and N. K. Nishchal, "Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase- truncation approach," *Opt. Lasers Eng.*, vol. 52, pp. 167–173, Jan. 2014.
[24] J. Li, J. Li, Y. Pan, and R. Li, "Optical image hiding with a modified Mach-Zehnder interferometer," *Opt. Lasers Eng.*, vol. 55, pp. 258–261, Apr. 2014.
[25] S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique," *Opt. Commun.*, vol. 353, pp. 90–95, Oct. 2015.
[26] N. Rawat, I. C. Hwang, Y. Shi, and B. G. Lee, "Optical image encryption via photon-counting imaging and compressive sensing based ptychography," *J. Opt.*, vol. 17, no. 6, Jun. 2015, Art. no. 065704.
[27] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, May 2013.
[28] 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.
[29] W. Chen, X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. no. 6900113.
[30] 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.

[31] G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” *Opt. Lett.*, vol. 30, no. 11, pp. 1306–1309, Jun. 2005.

[32] G. Situ and J. Zhang, “Position multiplexing for multiple-image encryption,” *J. Opt. A, Pure Appl. Opt.*, vol. 8, no. 5, pp. 391–397, Mar. 2006.

[33] Q. Wang, Q. Guo, L. Lei, and J. Y. Zhou, “Multiple-image encryption based on interference principle and phase only mask multiplexing in Fresnel transform domain,” *Appl. Opt.*, vol. 52, no. 28, pp. 6849–6857, Oct. 2013.

[34] Q. Gong, X. Liu, G. Li, and Y Qin, “Multiple-image encryption and authentication with sparse representation by space multiplexing,” *Appl. Opt.*, vol. 52, no. 31, pp. 7486–7493, Nov. 2013.

[35] 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.

[36] Z. Zhong, Y. Zhang, M. Shan, Y. Wang, Y. Zhang, and H. Xie, “Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform,” *J. Opt.*, vol. 16, no. 12, Dec. 2014, Art. no.125404.

[37] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encryption–decryption via lateral shifting of a random phase mask,” *Opt. Commun.*, vol. 259, no. 2, pp. 532–536, Mar. 2006.

[38] Z. Liu, Y. Zhang, H. Zhao, M. A. Ahmad, and S. Liu, “Optical multi-image encryption based on frequency shift,” *Optik*, vol. 122, no. 11, pp. 1010–1013, 2011.

[39] P. Deng, M. Dian, M. Shan, Z. Zhong, and Y. Zhang, “Multiple-image encryption using spectral cropping and spatial multiplexing,” *Opt. Commun.*, vol. 359, pp. 234–239, Jan. 2016.

[40] C. Niu, X. Wang, and X. Mao, “Multiple-image hiding based on interference principle,” *Opt. Quantum Electron.*, vol. 43, nos. 6–10, pp. 91–99, Mar. 2012.

[41] D. Kong, X. Shen, Q. Xu, W. Xin, and H. Guo, “Multiple-image encryption scheme based on cascaded fractional Fourier transform,” *Appl. Opt.*, vol. 52, no. 12, pp. 2619–2625, Apr. 2013.

[42] Y. Li, F. Zhang, Y. Li, and R. Tao, “Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform,” *Opt. Lasers Eng.*, vol. 72, pp. 18–25, Sep. 2015.

[43] Y. Wan, F. Wu, J. Yang, and T. Man, “Multiple-image encryption based on compressive holography using a multiple-beam interferometer,” *Opt. Commun.*, vol. 342, pp. 95–101, May 2015.

[44] W. Chen, “Optical multiple-image encryption using three-dimensional space,” *IEEE Photon. J.*, vol. 8, no. 2, Apr. 2016, Art. no. 6900608.

[45] A. Alfalou and C. Brosseau, “Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption,” *Opt. Lett.*, vol. 35, no. 11, pp. 1914–1916, Jun. 2010.

[46] J. Wu, Z. Xie, Z. Liu, W. Liu, Y. Zhang, and S. Liu, “Multiple-image encryption based on computational ghost imaging,” *Opt. Commun.*, vol. 359, pp. 38–43, Jan. 2016.

[47] X. Li *et al.*, “Multiple-image encryption based on compressive ghost imaging and coordinate sampling,” *IEEE Photon. J.*, vol. 8, no. 4, Aug. 2016, Art. no. 3900511.

[48] 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, no. 24, pp. 3917–3919, Dec. 2009.

[49] J. J. Huang, H. E. Hwang, C. Y. Chen, and C. M. Chen, “Lensless multiple-image optical encryption based on improved phase retrieval algorithm,” *Appl. Opt.*, vol. 51, no. 13, pp. 2388–2394, May 2012.

[50] X. Wang, W. Chen, and X. Chen, “Optical image hiding using double-phase retrieval algorithm based on nonlinear cryptosystem under vortex beam illumination,” *J. Opt.*, vol. 17, no. 3, Mar. 2015, Art. no. 035704.

[51] W. Chen, X. Wang, and X. Chen, “Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase,” *J. Opt.* vol. 17, no. 3, Mar. 2015, Art. no. 035702.

[52] R. A. Muhammad, “Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain,” *Opt. Laser Technol.*, vol. 45, pp. 525–532, Feb. 2013.

[53] 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.*, vol. 67, pp. 145–156, Apr. 2015.

[54] 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.*, vol. 344, pp. 172–180, Jun. 2015.

[55] X. Wang, W. Chen, and X. Chen, “Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding,” *Opt. Exp.*, vol. 22, no. 19, pp. 22981–22995, Sep. 2014.

[56] Original images. [Online]. Available. http://sipi.usc.edu/database/database.php