Optica Applicata, Vol. XLVI, No. 1, 2016
DOI: 10.5277/oa160105

Optical image encryption by using diffractive imaging with special constraint in the input plane

ZHIPENG WANG, HONGJUAN WANG, XINGQIANG YANG, PING ZHANG, CHENXIA HOU, YI QIN*

College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China

*Corresponding author: 641858757@qq.com

In order to simplify the optical setup and the encryption process, a diffractive-imaging-based optical encryption system using a single diffraction pattern is proposed. A predesigned binary mask is placed before the plaintext in the encryption process, and three randomly distributed phase only masks are placed in the optical path. Only one diffraction pattern needs to be recorded as ciphertext by CCD. In the decryption process, an iterative phase retrieval algorithm is applied, in which the predesigned binary mask acts as a support constraint in the input plane. After the iterative process, an interpolation operation for the zero-valued pixels is also implemented. The effectiveness and robustness of the proposal are demonstrated by numerical simulation results.

Keywords: optical encryption, diffractive imaging, bilinear interpolation.

1. Introduction

Over the past decade, there has been a steadily growing interest in the development of cryptosystems based on optical techniques. The most famous one is the double random phase encoding (DRPE) invented by RÉFRÉGIER and JAVIDI [1], in which a primary image can be converted into stationary white noise by two random phase masks (RPMs), one placed in the input plane and the other in the Fourier plane. In addition to DRPE, many algorithms and infrastructures [2–18], such as fractional Fourier transform [2, 3], Fresnel transform [4], and gyrator transform [5, 6], have been further developed. Although these methods have been proved to be effective and feasible, encryption results of them are complex values and should always be recorded by interferometric equipments, which require strictly stable environment. Moreover, since many of these approaches are linear, they have been demonstrated to be vulnerable to cryptographic attacks [19–22].

To deal with these problems, people proposed to employ diffractive imaging schemes based on a single wave-propagation path to substitute DRPE and its derivatives. The first

optical cryptosystem based on diffractive imaging is proposed by WEN CHEN *et al*. [23] and afterwards some derivative architectures are further invented [24–27]. These methods enable one to retrieve the primary image from several intensity patterns, as a result of which the interferometric optical path is avoided and the stability of the encryption environment has been exceedingly undemanding. Nevertheless, in order to exactly recover the plaintext, at least three diffraction patterns should be recorded as ciphertexts in these methods; therefore both the encryption and decryption procedures become rather complicated. So more convenient and effective approaches are developed and presented.

Lately, we have proposed several diffractive-imaging-based optical encryption systems that only need to record one diffraction pattern in the encryption process [28–30]. In the encryption system proposed in [28], redundant data is digitally appended to the primary image before a standard encryption procedure, as a result of which the encryption efficiency is reduced. We have proposed a single-intensity-recording optical encryption technique with the help of QR code [29]. In this encryption technique, the information to be encrypted is first transformed into a QR code by means of worldwide free available software, and then encrypted by a 4-f system. The diffraction pattern is recorded by a charge-coupled device (CCD). Unfortunately, the information to be encrypted can only be four standardized kinds of data (numeric, alphanumeric, byte/binary, *etc*.), and the data size is limited by the QR code. We have also proposed a simplified optical encryption approach using a single diffraction pattern in a diffractive-imaging-based scheme in [30]. The plaintext can be recovered using a single diffraction pattern in this approach. However, the decryption process, formed of two iterative cycles, is rather complicated.

In this paper, we propose a novel method that is able to retrieve the primary image from a single diffraction pattern. In the proposed method, the plaintext is attached to a predesigned binary mask, and three random phase masks are used in the optical path. Only one diffraction pattern is captured as ciphertext by CCD. During decryption, a phase retrieval algorithm is executed, in which the predesigned binary mask serves as a support constraint in the input plane. The simulation results demonstrate the effectiveness and robustness of the proposal.

2. Theoretical analysis

2.1. Encryption process

Figure 1 shows a schematic experimental setup for the proposed diffractive-imaging -based optical encryption method. A collimated plane wave with a wavelength of λ is first generated and is used to illuminate the plaintext image. A predesigned binary mask P, which only has two values 0 and 1, is placed just before the plaintext. Since the plaintext image is multiplied by the predesigned binary mask, parts of the pixels in the plaintext are restricted to zero. It is worth noting that the predesigned binary

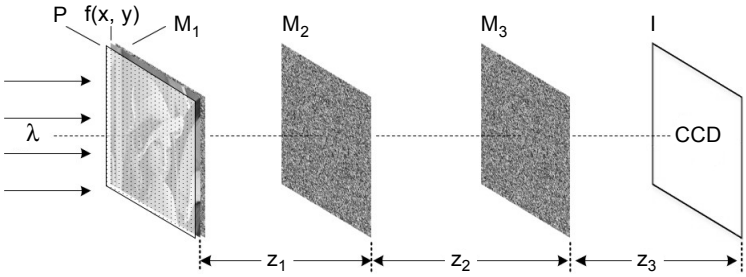

Fig. 1. A schematic experimental setup for the proposed diffractive-imaging-based optical encryption method.

mask can be embedded in a spatial light modulator (SLM). Thereafter, the diffractive field emerging from the primary image is modulated by three statistically independent phase-only masks M_1, M_2, and M_3, which are randomly distributed in $[0, 2\pi]$. The diffractive intensity pattern in the output plane is captured by a CCD. For convenience, symbols (x, y), (η, ξ), (p, q) and (μ, ν) are used to denote coordinates of the plaintext image, M_2, M_3, and the CCD plane, respectively.

In the Fresnel approximation, wave propagation between the input plane and the phase-only mask (M_2) plane can be described by [4, 31]

$$g(\eta, \xi) = \frac{\exp(jkz_1)}{j\lambda z_1} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} P(x, y) f(x, y) M_1(x, y) \times \\ \times \exp\left\{ j\frac{k}{2z_1}\left[(x-\eta)^2 + (y-\xi)^2 \right] \right\} \mathrm{d}x\,\mathrm{d}y \tag{1}$$

where $P(x, y)$ denotes the binary mask, $f(x, y)$ denotes the plaintext, $M_1(x, y)$ denotes the first phase-only mask, $g(\eta, \xi)$ denotes the wave front just before the second phase -only mask M_2, $j = \sqrt{-1}$, λ is light wavelength, wave number $k = 2\pi/\lambda$, z_1 denotes axial distance. For the sake of simplicity, Eq. (1) can be rewritten as [28]

$$g(\eta, \xi) = FrT_\lambda[P(x, y) f(x, y) M_1(x, y);\ z_1] \tag{2}$$

Therefore, the diffraction intensity pattern recorded by CCD can be described as

$$I(\mu, \nu) = \left| FrT_\lambda\{FrT_\lambda[g(\eta, \xi) M_2(\eta, \xi);\ z_2] M_3(p, q);\ z_3\} \right|^2 \tag{3}$$

where symbol | | denotes the modulus operation. The recorded intensity pattern $I(\mu, \nu)$ is saved as ciphertext. The encryption process can be implemented optically. An optical setup for encryption is shown in Fig. 2. SLM_1 displays the predesigned binary mask, and the plaintext is displayed in SLM_2. SLM_3, SLM_4 and SLM_5 display the three random phase masks M_1, M_2 and M_3, respectively. The optical setup is illuminated by

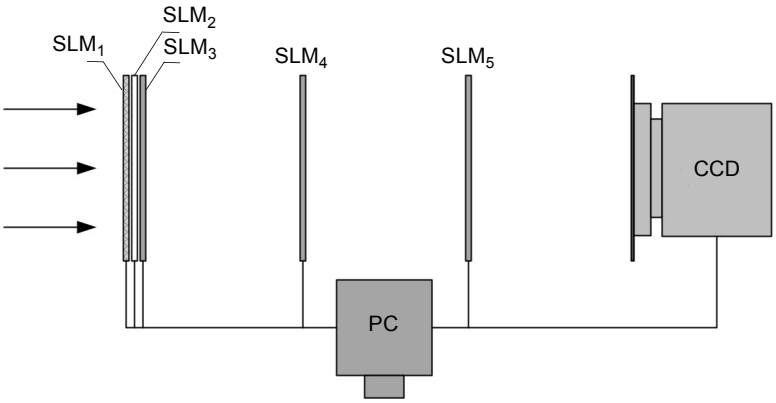

Fig. 2. An optical setup for encryption; SLM – spatial light modulator, CCD – charge-coupled device, PC – personal computer.

a uniform plane wave, and the diffraction intensity pattern (*i.e.*, ciphertext) can be captured by CCD camera in the output plane.

For only one diffraction intensity pattern is recorded in the encryption process, the interferometric optical path is unnecessary. Consequently, the optical setup is simplified. Moreover, due to the linearity characteristic, the DRPE-based optical encryption scheme is vulnerable to cryptographic attacks, such as known-plaintext-attack (KPA) and chosen-plaintext-attack (CPA). On the contrary, the proposed method only needs to record the amplitude component of the diffraction light field, and the phase component is discarded, as a result of which the linearity characteristic of the proposal is broken. Therefore, the proposed scheme can well resist conventional cryptographic attacks.

2.2. Decryption process

Because only the diffraction intensity pattern without phase distribution is recorded as the ciphertext, the plaintext cannot be recovered by using the inverse of the encryption process. As a result, an iterative phase retrieval algorithm is usually applied between real and reciprocal spaces to recover the plaintext. However, it has been stated that phase retrieval algorithm will encounter the stagnation problem when two or less intensity patterns are used [25]. In the proposed method, the predesigned binary mask serves as a support constraint in the input plane, which helps overcome the stagnation problem.

The iterative decryption process can be described as follows:

– First, assume an initial random or constant real-valued distribution $f_n(x, y)$, $n = 1$ for the plaintext, and a support constraint in the input plane is applied by using the predesigned binary mask $P(x, y)$

$$\hat{f}_n(x, y) = P(x, y)\, f_n(x, y) \tag{4}$$

– Propagate forward to the CCD plane [28], and the wave front in the output plane is calculated by

$$O_n(\mu, \nu) = FrT_\lambda\left\{FrT_\lambda\left\{FrT_\lambda\left[\hat{f}_n(x, y)M_1(x, y);\ z_1\right]M_2(\eta, \xi);\ z_2\right\}M_3(p, q);\ z_3\right\} \tag{5}$$

– Apply a support constraint in the output plane with the square root of the intensity pattern:

$$\hat{O}_n(\mu, \nu) = [I(\mu, \nu)]^{1/2}\frac{O_n(\mu, \nu)}{|O_n(\mu, \nu)|} \tag{6}$$

– Propagate back to the input plane:

$$f_{n+1}(x, y) = \left|FrT_\lambda\left\{FrT_\lambda\left\{FrT_\lambda\left[\hat{O}_n(\mu, \nu);\ -z_3\right]M_3^*(p, q);\ -z_2\right\}M_2^*(\eta, \xi);\ -z_1\right\}\right| \tag{7}$$

– The iterative error between $f_{n+1}(x, y)$ and $\hat{f}_n(x, y)$ is calculated to judge whether the iterative process should be stopped

$$\text{Error} = \sum_{x, y}\left[|f_{n+1}(x, y)| - |\hat{f}_n(x, y)|\right]^2 \tag{8}$$

The decryption process is a gradual process of convergence. The iterative error decreases at each iteration cycle. The iterative process continues until the iterative error is smaller than a preset threshold δ (for example, δ can be set to be 0.0001).

– After the above iterative process, we can obtain a retrieved image which is similar to the plaintext. However, the retrieved image is different from the plaintext, for parts of the pixels in the retrieved image are restricted to zero because of the binary mask that is attached to the plaintext. In order to recover the exact original image, an interpolation operation for the zero values is also implemented. Image interpolation is widely used and studied in digital image processing [32–34]. There are many types of interpolation methods, such as traditional interpolation [32] and edge-based interpolation [33, 34]. For the simplicity of the algorithm, we apply the bilinear interpolation method, one of the most commonly used image interpolation method, to modify the zero-valued pixels in the retrieved image. In the bilinear interpolation method that is applied in our proposal, the zero-valued pixel can be substituted by its adjacent pixels as

$$f(x, y) = \frac{1}{4}[f(x-1, y) + f(x, y-1) + f(x, y+1) + f(x+1, y)] \tag{9}$$

It is well-known that adjacent pixels have strong correlation. As a result, the zero values can be modified after the bilinear interpolation operation. It can be seen from

the simulation results in Section 3 that the correlation coefficient (CC) [29] between the decrypted image and the plaintext is close to 1. Note that, if a more complicated interpolation method is applied, the CC value between the decrypted image and the plaintext will be closer to 1.

2.3. Design of the binary mask

From the description of the encryption and decryption processes, it can be seen that the predesigned binary mask plays an important role in recovering the plaintext. The predesigned binary mask serves as a support constraint in the input plane, which helps solve the stagnation problem. Meanwhile, the binary mask attached to the plaintext causes parts of the iteratively retrieved image be zero, which need to be substituted by its adjacent pixels. Therefore, the design of the binary mask needs to meet the following two restrictions: *i*) the values of edge pixels must be 1; *ii*) in the binary mask, the pixels valued 0 are surrounded by the pixels valued 1. Only when the above two restrictions are met, can all the zero valued pixels in the retrieved image be modified by the interpolation method. Therefore, the best decryption quality can be achieved.

3. Numerical simulations

Numerical experiments are performed under MATLAB 7.1 environment to verify the validity of the proposed method. A collimated plane wave ($\lambda = 633$ nm) is used in the simulation. The pixel size of CCD camera is 2.5 μm. Axial distances between phase only masks are set as $z_1 = z_2 = z_3 = 50$ mm. The threshold δ in the iterative retrieval algorithm is predefined as 0.0001. The plaintext (*Lena*) with 512×512 pixels is shown in Fig. 3**a**. The predesigned binary mask is shown in Fig. 3**b**, where the black pixels represent zero while the white pixels represent one. The enlarged view of the dashed box in Fig. 3**b** is shown in Fig. 3**c**. It is clear that the predesigned binary mask satisfies the two restrictions that are described in Section 2.3. The real part of a phase only mask (M_1) is shown in Fig. 3**d**. The diffraction intensity pattern captured by CCD (*i.e.*, ciphertext) is shown in Fig. 3**e**. It can be seen that the plaintext is fully hidden after the encryption process, and no information about the plaintext can be observed. Figure 3**f** shows the retrieved image after the phase retrieval algorithm, part pixels of which are restricted to 0. After the interpolation operation, we can get the final decrypted image, which is shown in Fig. 3**g**. Figure 3**h** shows the curve of CC value between the plaintext and the decrypted image. The final CC value reaches 0.9994. It is very close to 1, which means the plaintext has been exactly retrieved. As a comparison, the CC value between the plaintext (Fig. 3**a**) and the retrieved image without interpolation operation (Fig. 3**f**) is also calculated, and the value is 0.7774. It can be seen from the two CC values that the interpolation operation is essential for improving the quality of the recovered image.

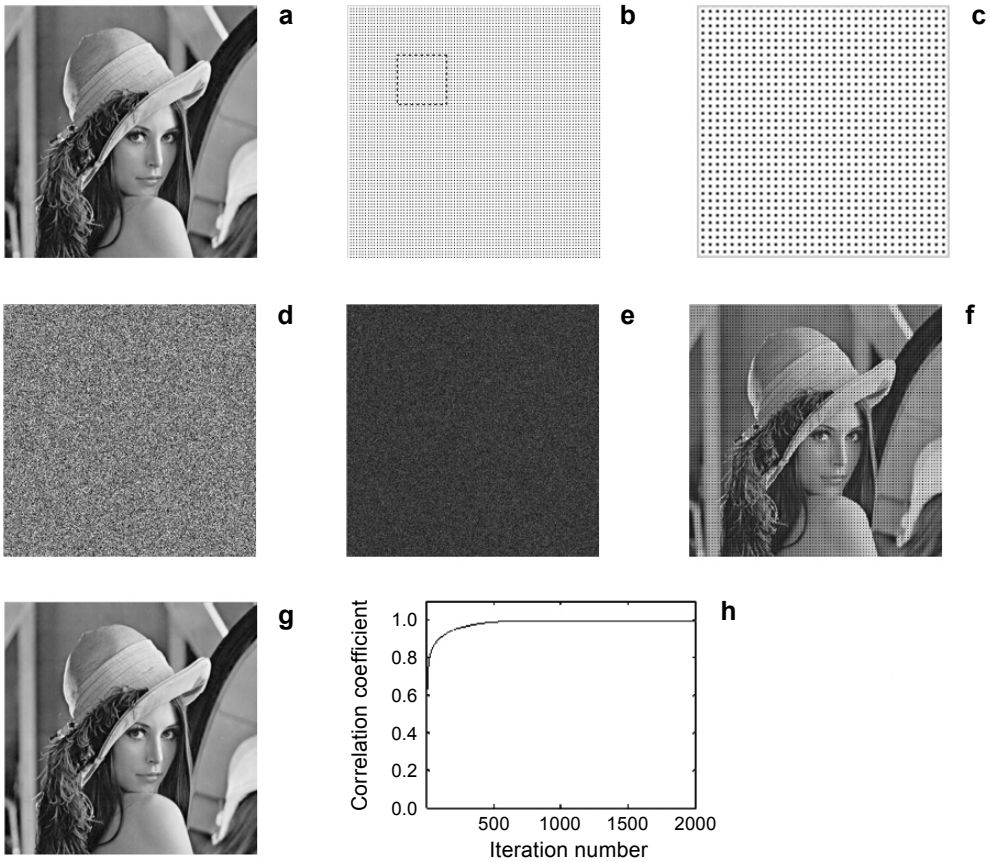

Fig. 3. The plaintext (**a**), the predesigned binary mask (**b**), the enlarged view of the dashed box in **b** (**c**), a phase only mask (M_1) (**d**), the ciphertext (**e**), retrieved image before interpolation operation (**f**), the decrypted image (**g**), and CC value between plaintext and decrypted image (**h**).

We also investigate the mean square error (MSE) [9] and peak signal-to-noise ratio (PSNR) of the decrypted image, and

$$\mathrm{PSNR} = 20\log\left(\frac{L}{\sqrt{\mathrm{MSE}}}\right) \tag{10}$$

where L is the maximum possible pixel value of the image. After 2000 iterations, the eventual MSE and PSNR are 4.1602×10^{-5} and 91.9397, respectively. All these parameters show that the difference between the plaintext and the decrypted image is very small, and high decryption quality is obtained.

The number of the pixels valued zero in the predesigned binary mask affects the convergence rate of a phase retrieval algorithm. In order to facilitate the description,

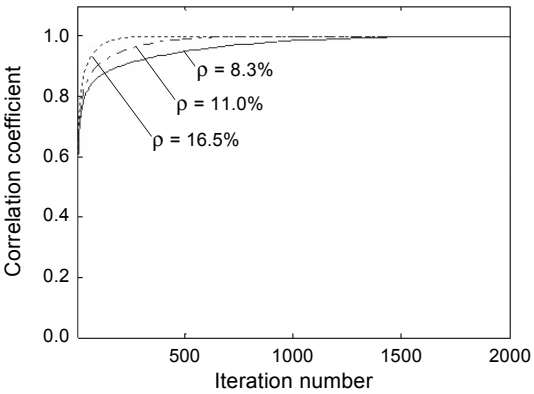

Fig. 4. The curves of CC value between plaintext and decrypted image when ρ takes different values.

a parameter ρ is introduced for quantitatively describing the zero values in the binary mask, which is defined as

$$\rho = \frac{\text{Number of pixels valued zero}}{\text{Number of total pixels}} \times 100\% \tag{11}$$

Figure 4 shows the curves of CC value between the plaintext and the decrypted image when ρ takes the values of 16.5%, 11.0% and 8.3%. The eventual CC values after 2000 iterations are 0.9991, 0.9994 and 0.9995, respectively. Obviously, the bigger the parameter ρ is, the faster the convergence rate is. This is because a bigger ρ means more pixels in the plaintext are restricted to zero to act as the support constraint in the input plane, thus consequently the convergence rate can be enhanced. However, the eventual CC value decreases slightly along with the increase of ρ, because more pixels need to be modified by the interpolation operation.

We can infer from the description of the decryption process that the predesigned binary mask plays an important role in solving the stagnation problem. Therefore, the performance of the binary mask is also investigated. Figure 5**a** is the binary mask

Fig. 5. Performance of the binary mask. The binary mask used for decryption (different from the binary mask used for encryption, shown in Fig. 3**b**) (**a**), decrypted image after 2000 iterations (**b**), and the curves of CC value (**c**).

that is used for decryption, which is different from the one used for encryption. Figure 5**b** shows the decryption result obtained after 2000 iterations, when the binary mask used for decryption is different from the correct one, for which the CC value is 0.5720. The curve of CC value between the plaintext and the decrypted image is shown in Fig. 5**c**. Based on this phenomenon, the proposed scheme can act as a hierarchical image encryption system, where the users with different levels can decrypt the images with different resolutions. Only those with this binary mask can obtain the explicit plaintext (see Fig. 3**g**). On the contrary, the low level users can only obtain the rough image of the plaintext (see Fig. 5**b**).

Performance of security keys, such as three phase only masks, is further analyzed during image decryption. The decryption result is shown in Fig. 6**a**, when one phase only mask (M_1) is incorrect. The obtained CC value is within the range of [–0.0011, 0.0047],

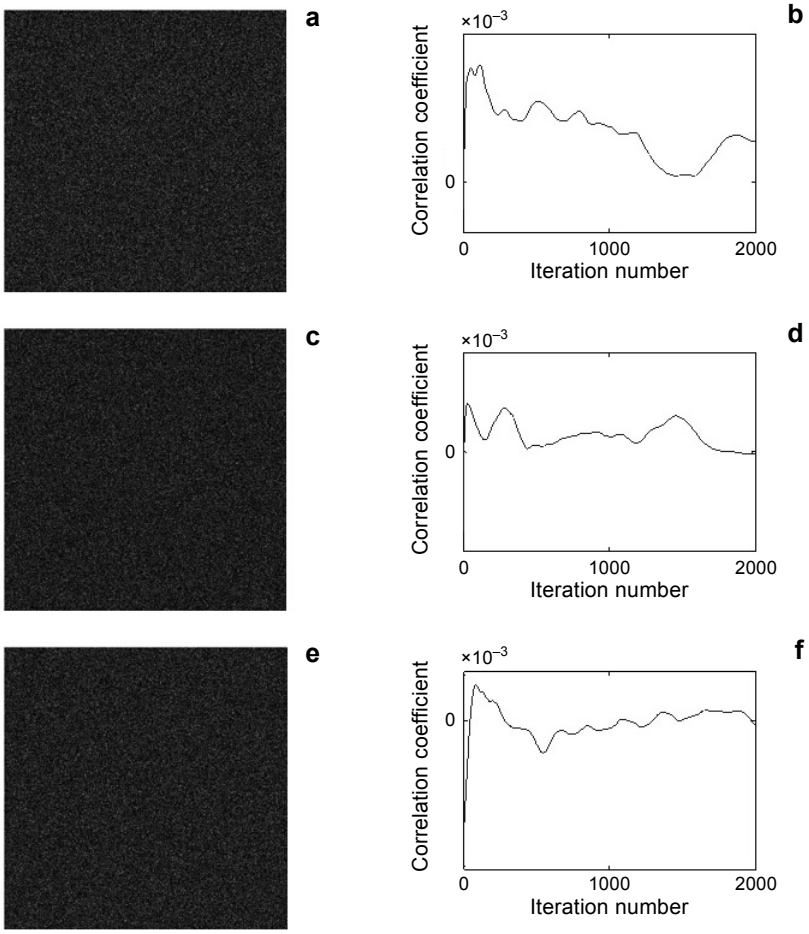

Fig. 6. Decrypted image after 2000 iterations by using wrong phase only mask M_1 (**a**), wrong axial distance z_1 (**c**), and wrong wavelength λ (**e**); **b**, **d** and **f** – the curves of CC value corresponding to **a**, **c** and **e**, respectively.

as shown in Fig. 6**b**. Simulation results for incorrect M_2 and M_3 are similar with that for incorrect M_1, which are not present here for the sake of brevity. Furthermore, the decryption results are sensitive to the encryption parameters, such as axial distances and light wavelength. Therefore, the performance of encryption parameters is also demonstrated. Figure 6**c** shows the decryption result obtained after 2000 iterations, when there is an error of 0.5 mm in the axial distance z_1. In this case, the obtained CC value is within the range of [–0.0040, 0.0024], as shown in Fig. 6**d**. Figure 6**e** shows the decryption result obtained after 2000 iterations, when there is an error of 10 nm in wavelength during image decryption process. In this case, the obtained CC value is within the range of [–0.0041, 0.0015], as shown in Fig. 6**f**.

The ciphertext may be contaminated in the transmission path. Therefore, the robustness of the proposed method against noise and occlusion attacks is also investigated. A noise contaminated ciphertext is shown in Fig. 7**a**. The addictive noise [29] is generated by $\{\text{Mean}[I(\mu, \nu)]\text{SNR}^{-1}\text{VA}\}$, where Mean – a mean value of the ciphertext,

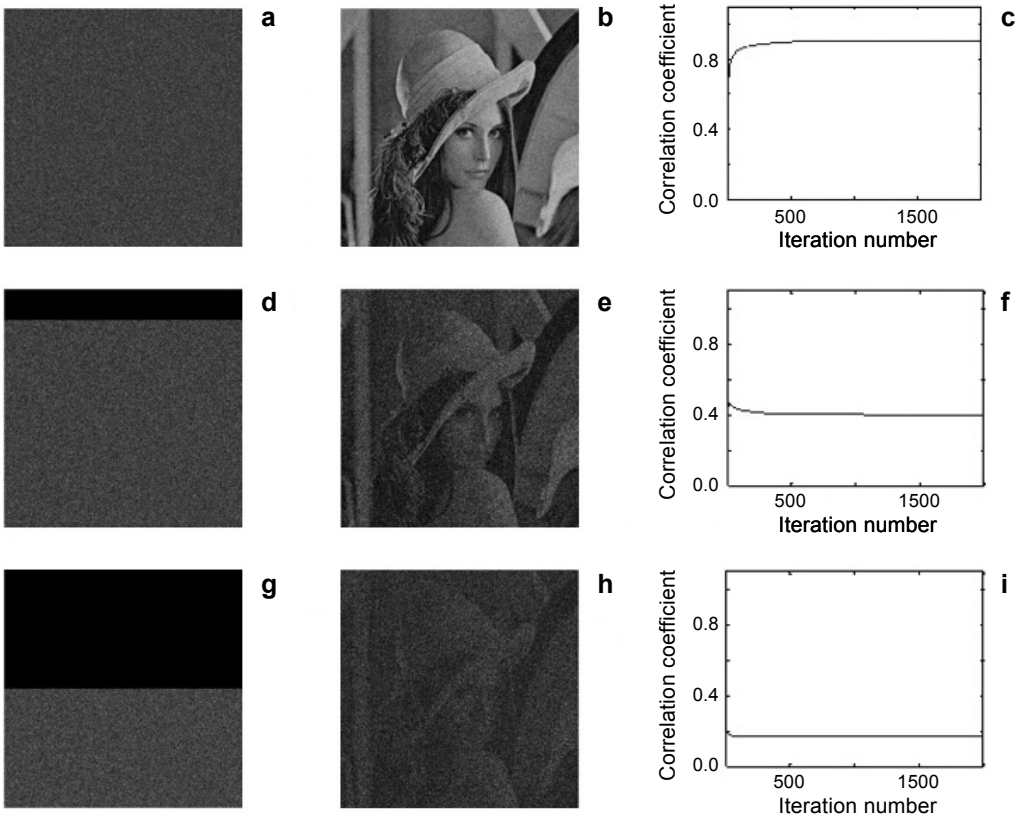

Fig. 7. The simulation results under noise attack (**a**–**c**), and the simulation results under occlusion attack (**d**–**i**). The contaminated ciphertexts (**a**, **d**, **g**), the decrypted images (**b**, **e**, **h**), and the curves of CC value between plaintext and decrypted image (**c**, **f**, **i**).

VA – a 2D variable randomly distributed in a range of [–0.5, 0.5], and SNR – signal -to-noise ratio, which is set to be 4 in this simulation. The decrypted image under noise attack is shown in Fig. 7**b**. The relationship between the iteration number and the CC value is shown in Fig. 7**c**. The maximum of the CC value is 0.9029. Figure 7**d** shows a ciphertext with 13% occlusion. The decrypted image using this occluded ciphertext is shown in Fig. 7**e**. The relationship between the iteration number and the CC value is shown in Fig. 7**f**, in which the maximum of the CC value is 0.4677 during the iteration process. We also increase the occlusion percentage to 50% in order to further show the performance of the method. The corresponding simulation result is shown in Figs. 7**g**–7**i**. We can infer from the simulation result that even though half of the ciphertext is missing, slight information of the plaintext can be obtained, and the maximum of the CC value is 0.1944 during the iteration process. It can be seen from the simulation results that most information about the plaintext can be obtained when the proposed method suffers from noise and occlusion attacks.

Compared with the previously proposed encryption methods based on diffraction imaging, our proposal has three advantages:

1) Compared with the schemes in [24–27], only one diffraction pattern needs recording in the encryption process, which simplifies the encryption and decryption procedures. Moreover, the optical setup is simplified, since no movements of the elements are required in the encryption process.

2) Unlike the diffractive-imaging-based encryption method that we proposed in [28], the proposed method does not require appending data to the plaintext. Thus, the encryption efficiency is improved.

3) The proposed method can act as a two-level image encryption approach, where those with and without the predesigned binary mask can decrypt different resolution images. On the contrary, there are also some disadvantages in the proposed method: *i*) Since parts of the pixels in the retrieved image are established using the image interpolation method, the retrieved image is not exactly the same as the input image. It can be seen from the above simulation that the CC value between the plaintext and the decrypted image is close to 1, but not equal to 1. *ii*) Compared with the schemes that record multiple diffraction intensity patterns as ciphertexts, the convergence rate of the iterative decryption process in the proposed method is very slow because less support constraint is utilized. As a result, more researches are needed in the future to further improve the performance of the optical encryption approach.

4. Conclusion

In this paper, we propose a novel diffractive-imaging-based optical encryption method, in which only single diffraction pattern needs to be recorded as ciphertext. The encryption process can be implemented either optically or digitally. Neither interferometric structure nor movement of the elements is required. As a result, the optical setup is greatly simplified. The simulation results show that the proposal can realize gray-

scale image encryption and decryption. Meanwhile, the robustness of the proposal against noise and occlusion attacks is also demonstrated.

Acknowledgments – This study was supported by the National Natural Science Foundation of China (grant No. 61505091) and the Fundamental and Cutting-edge Technology Research Programs of Henan Province (grant Nos. 142300410184 and 142300410454).

References

[1] RÉFRÉGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.

[2] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000, pp. 887–889.

[3] NAVEEN KUMAR NISHCHAL, JOBY JOSEPH, KEHAR SINGH, *Securing information using fractional Fourier transform in digital holography*, Optics Communications **235**(4–6), 2004, pp. 253–259.

[4] GUOHAI SITU, JINGJUAN ZHANG, *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586.

[5] HUIJUAN LI, *Image encryption based on gyrator transform and two-step phase-shifting interferometry*, Optics and Lasers in Engineering **47**(1), 2009, pp. 45–50.

[6] ZHENGJUN LIU, LIE XU, CHUANG LIN, SHUTIAN LIU, *Image encryption by encoding with a nonuniform optical beam in gyrator transform domains*, Applied Optics **49**(29), 2010, pp. 5632–5637.

[7] YAN ZHANG, BO WANG, *Optical image encryption based on interference*, Optics Letters **33**(21), 2008, pp. 2443–2445.

[8] PÉREZ-CABRÉ E., MYUNGJIN CHO, JAVIDI B., *Information authentication using photon-counting double-random-phase encrypted images*, Optics Letters **36**(1), 2011, pp. 22–24.

[9] WAN QIN, XIANG PENG, *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010, pp. 118–120.

[10] ZHENGJUN LIU, CHENG GUO, JIUBIN TAN, WEI LIU, JINGJING WU, QUN WU, LIQIANG PAN, SHUTIAN LIU, *Securing color image by using phase-only encoding in Fresnel domains*, Optics and Lasers in Engineering **68**, 2015, pp. 87–92.

[11] NANRUN ZHOU, YIXIAN WANG, LIHUA GONG, *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242.

[12] WEI LIU, ZHENGJUN LIU, SHUTIAN LIU, *Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm*, Optics Letters **38**(10), 2013, pp. 1651–1653.

[13] ZHENGJUN LIU, QING GUO, LIE XU, AHMAD M.A., SHUTIAN LIU, *Double image encryption by using iterative random binary encoding in gyrator domains*, Optics Express **18**(11), 2010, pp. 12033–12043.

[14] WEN CHEN, XUDONG CHEN, *Arbitrarily modulated beam for phase-only optical encryption*, Journal of Optics **16**(10), 2014, article 105402.

[15] WEN CHEN, JAVIDI B., XUDONG CHEN, *Advances in optical security systems*, Advances in Optics and Photonics **6**(2), 2014, pp. 120–155.

[16] NANRUN ZHOU, AIDI ZHANG, FEN ZHENG, LIHUA GONG, *Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing*, Optics and Laser Technology **62**, 2014, pp. 152–160.

[17] TIANXIANG HUA, JIAMIN CHEN, DONGJU PEI, WENQUAN ZHANG, NANRUN ZHOU, *Quantum image encryption algorithm based on image correlation decomposition*, International Journal of Theoretical Physics **54**(2), 2015, pp. 526–537.

[18] XIAOLING HUANG, GUODONG YE, *An image encryption algorithm based on hyper-chaos and DNA sequence*, Multimedia Tools and Applications **72**(1), 2014, pp. 57–70.

[19] CARNICER A., MONTES-USATEGUI M., ARCOS S., JUVELLS I., *Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005, pp. 1644–1646.

[20] WAN QIN, XIANG PENG, *Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys*, Journal of Optics A: Pure and Applied Optics **11**(7), 2009, article 075402.

[21] WAN QIN, XIANG PENG, XIANGFENG MENG, GAO B.Z., *Vulnerability to chosen-plaintext attack of optoelectronic information encryption with phase-shifting interferometry*, Optical Engineering **50**(6), 2011, article 065601.

[22] WAN QIN, XIANG PENG, XIANGFENG MENG, *Cryptanalysis of optical encryption schemes based on joint transform correlator architecture*, Optical Engineering **50**(2), 2011, article 028201.

[23] WEN CHEN, XUDONG CHEN, SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010, pp. 3817–3819.

[24] WEN CHEN, XUDONG CHEN, SHEPPARD C.J.R., *Optical double-image cryptography based on diffractive imaging with a laterally translated phase grating*, Applied Optics **50**(29), 2011, pp. 5750–5757.

[25] WEN CHEN, XUDONG CHEN, ANAND A., JAVIDI B., *Optical encryption using multiple intensity samplings in the axial domain*, Journal of the Optical Society of America A **30**(5), 2013, pp. 806–812.

[26] WEN CHEN, GUOHAI SITU, XUDONG CHEN, *High-flexibility optical encryption via aperture movement*, Optics Express **21**(21), 2013, pp. 24680–24691.

[27] WEN CHEN, XUDONG CHEN, *Optical image encryption using multilevel Arnold transform and noninterferometric imaging*, Optical Engineering **50**(11), 2011, article 117001.

[28] YI QIN, ZHIPENG WANG, QIONG GONG, *Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern*, Applied Optics **53**(19), 2014, pp. 4094–4099.

[29] ZHI-PENG WANG, SHUAI ZHANG, HONG-ZHAO LIU, YI QIN, *Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code*, Optics Communications **332**, 2014, pp. 36–41.

[30] YI QIN, QIONG GONG, ZHIPENG WANG, *Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme*, Optics Express **22**(18), 2014, pp. 21790–21799.

[31] GOODMAN J.W., *Introduction to Fourier Optics*, 2nd Ed., McGraw-Hill, New York, 1996.

[32] KEYS R., *Cubic convolution interpolation for digital image processing*, IEEE Transactions on Acoustics, Speech and Signal Processing **29**(6), 1981, pp. 1153–1160.

[33] JENSEN K., DIMITRIS A., *Subpixel edge localization and the interpolation of still images*, IEEE Transactions on Image Processing **4**(3), 1995, pp. 285–295.

[34] XIN LI, ORCHARD M.T., *New edge-directed interpolation*, IEEE Transactions on Image Processing **10**(10), 2001, pp. 1521–1527.

Received July 16, 2015
in revised form August 24, 2015