Optica Applicata, Vol. XLVII, No. 2, 2017
DOI: 10.5277/oa170206

Fully-phase optical image encryption in diffractive-imaging scheme with QR-code-based random illumination

ZHIPENG WANG[1*], YINGYING ZHANG[1], QIONG GONG[2], SHUYI LI[2], YI QIN[2]

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

[2]College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China

[*]Corresponding author: wzpnynu@163.com

Based on a fully phase encoding and phase retrieval algorithm, a diffractive-imaging-based optical encryption scheme with random illumination is proposed. In the encryption process, a QR code image is placed in the optic path to modulate the incident light and thus generate a random illumination, which has been demonstrated to enable the proposed scheme to resist the multi-slice ptychographic phase retrieval algorithm attack. The plaintext is phase-encoded, and then encrypted by two random phase masks. The diffraction pattern in the output plane is recorded as ciphertext by a CCD camera. For decryption, an iterative phase retrieval algorithm with median filtering operation is implemented. Simulation results demonstrate the effectiveness, security, and robustness of the proposal.

Keywords: optical encryption, diffractive imaging, fully phase, phase retrieval algorithm.

1. Introduction

Optical information security is a relatively new field formed by introducing the optical technology into the traditional cryptography, and thus optical cryptosystem always has some particular advantages, such as inherent parallelism, multiple degrees of freedom (wavelength, polarization, three-dimensional topology, *etc*.), to name a few. The double random phase encoding (DRPE) system [1] is the most well-known optical cryptosystem invented by REFREGIER and JAVIDI in 1995. Unfortunately, the DRPE and its derivatives [2–4], together with many existing approaches [5–9], have to register and process complex data, and this drawback becomes an obstacle to their real applications.

Most of the existing optical encryption systems are amplitude-based encryptions, in which the plaintexts are intensity representations. On the other hand, fully phase image encryptions have also gained much attention [10–13]. The plaintext in the fully

phase encryption is phase encoded, making the encryption scheme to be a nonlinear system. As a result, fully phase encryption is more secure than amplitude-based encryption. It has also been stated that the fully phase encryption performs better than amplitude-based encryption in the presence of additive noise [10]. In recent years, the quick response (QR) code, as a two-dimensional bar code with certain error correction capability, has been merged into optical encryption systems [8, 14–16].

In 2010, an alternative approach for optical image encryption based on diffractive imaging [17] was proposed by WEN CHEN *et al*. Different from the above mentioned methods, the diffractive-imaging-based encryption (DIBE) is able to recover the plaintext from several intensity patterns by using phase retrieval algorithms, which means that one no longer need to record the complex values of the diffractive filed. Consequently, the DIBE raises many researchers' interest in the past five years and has been extensively studied in the past several years. For instance, WEN CHEN *et al*. proposed an optical encryption using multiple intensity samplings with axial translation of the image sensor [18]. YI QIN *et al*. proposed a simplified optical image encryption in the diffractive-imaging-based scheme [19]. XIAOGANG WANG *et al*. proposed an optical binary image encryption in which the secret binary image can be recovered based on phase retrieval with an aperture-key and wavelength keys [20]. Recently, SHENLU ZHONG *et al*. proposed a novel optical information verification and encryption method based on interference principle and phase retrieval with sparsity constraints [21], in which two phase retrieval algorithms are used in the encryption process.

The DIBE has been considered to have high security until TUO LI and YISHI SHI demonstrated its vulnerability to multi-slice ptychographic phase retrieval algorithm (MPPRA) [22]. Nevertheless, the DIBE is still regarded as one of the most secure cryptosystems since it can only be breached by the MPPRA up to now. So it is strongly expected that the DIBE can be protected from this attack. Motivated by this target, we propose here, to our best knowledge, a novel extension of the DIBE scheme that employs a random illumination and full-phase encoding. In the proposed scheme, a QR code is placed in the optic path to generate a random illumination, which makes the proposed encryption scheme invulnerable to MPPRA attack. Then the phase-encoded plaintext is encrypted by two statistically independent random phase masks (RPM). The diffraction intensity pattern is recorded as ciphertext by a charge coupled device (CCD). For decryption, an iterative phase retrieval algorithm is applied. We shall show the proposal not only retains the merits of DIBE but also possesses greater security.

2. Theoretical analysis

The real-value plaintext $f(x, y)$, whose values are restricted to [0, 1], is first phase encoded. The phase-only version of the plaintext is denoted by P_{R}, which can be described by

$$P_{\mathrm{R}}(x, y) = \exp\left[j2\pi f(x, y)\right] \tag{1}$$

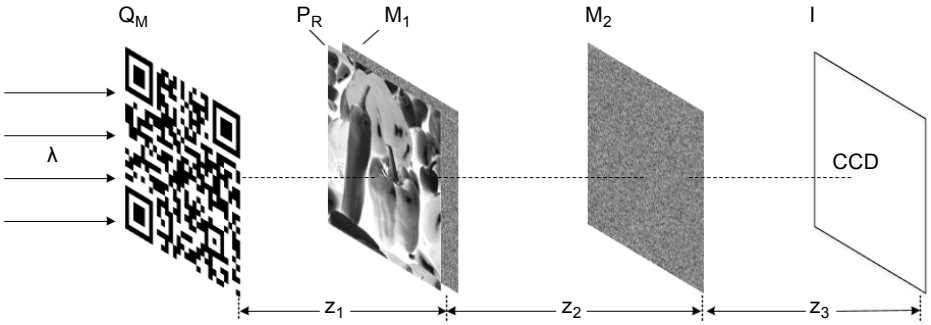

Fig. 1. Optical encryption scheme.

The phase-encoded image of the plaintext is then put in the optical path for encryption. The encryption process can be carried out either optically or digitally. Figure 1 illustrates the schematic diagram for encryption. QR code image Q_M is generated from an assistant key. The assistant key can be a string of alphanumeric data, whether it is relevant to the plaintext or not. Note that, since the QR code can be generated from a string of alphanumeric data, it is more convenient to be stored and distributed compared to the random amplitude mask. The QR code image has two different values (0 and 1), where 0 indicates that the incident light is totally blocked and 1 means that the incident light is totally transmitted. M_1 and M_2 are two statistically independent random phase masks, which are randomly distributed in $[0, 2\pi]$. The whole encryption system is illuminated by a collimated plane wave with a wavelength of λ. Taking advantage of a CCD camera, the diffraction intensity pattern is recorded as ciphertext, which can be expressed as

$$I(\mu, v) = \left| \mathrm{FrT}_{\lambda, z_3}\left\{ \mathrm{FrT}_{\lambda, z_2}\left[\mathrm{FrT}_{\lambda, z_1}(Q_M(m, n)) P_R(x, y) M_1(x, y) \right] M_2(\eta, \xi) \right\} \right|^2 \qquad (2)$$

where (m, n), (x, y), (η, ξ) and (μ, v) are used to denote the coordinates of the QR code image, the plaintext image, the random phase mask M_2, and the CCD plane, respectively. Symbol FrT$[\cdot]$ denotes the free-space wave propagation under the Fresnel approximation [20], and $|\cdot|$ denotes the modulus operation.

Obviously, the encryption process is very simple, since no interferometric setup is necessary, and only one diffraction intensity pattern needs to be recorded. Besides, the plaintext is phase-encoded in the first place. It has been stated that the fully phase encryption is more secure than amplitude-based encryption and the decrypted image obtained from the fully phase encryption is more robust to additive noise than that obtained from the amplitude-based encryption. Moreover, a QR code generated from an assistant key is used to scramble the incident collimated plane wave light. As a result, the light field in front of the plaintext's plane is randomly distributed, rather than uniformly distributed as in ordinary optical encryption systems. The proposed random

-illumination-based optical image encryption scheme can resist the MPPRA attack, which makes the proposed encryption scheme even more secure.

In order to decrypt the phase-encoded plaintext, an iterative phase retrieval algorithm is implemented. It had been stated that if two or less diffraction patterns are recorded as ciphertexts, the iterative phase retrieval algorithm will encounter the stagnation problem [19]. As described before, only a single diffraction pattern is recorded as ciphertext in the proposed method. Consequently, in order to solve the stagnation problem, a median filter is introduced to each cycle of the iterative phase retrieval algorithm. The median filter is very important for the convergence of the phase retrieval algorithm. The iterative decryption process will diverge without this median filtering operation. The iterative decryption process can be described as follows.

1. Assume an initial random distribution f_n, $n = 1$ for the plaintext, and the phase -encoded version of the plaintext can be calculated by

$$P_{\mathrm{R}} = \exp\left[j2\pi f_n\right] \tag{3}$$

2. Calculate the light field in front of the plaintext's plane

$$L_{\mathrm{F}} = \mathrm{FrT}_{\lambda, z_1}(Q_{\mathrm{M}}) \tag{4}$$

3. Propagate forward to the CCD plane, and the wave front in the output plane is calculated by

$$O_n = \mathrm{FrT}_{\lambda, z_3}\left[\mathrm{FrT}_{\lambda, z_2}(L_{\mathrm{F}} P_{\mathrm{R}} M_1) M_2\right] \tag{5}$$

4. Apply a support constraint in the output plane with the square root of the ciphertext

$$\hat{O}_n = \sqrt{I}\left[O_n / |O_n|\right] \tag{6}$$

5. Propagate back to the plaintext's plane, and calculate the modified phase-encoded version of the plaintext

$$\hat{P}_{\mathrm{R}} = \mathrm{FrT}_{\lambda, -z_2}\left[\mathrm{FrT}_{\lambda, -z_3}(\hat{O}_n) M_2^*\right] M_1^* L_{\mathrm{F}}^* \tag{7}$$

where symbol * indicates the complex conjugation operation.

6. Apply a median filtering operation to the phase part of $\hat{P}_{\mathrm{R}}$, and obtain the revised version of the plaintext f_{n+1}

$$f_{n+1} = \mathrm{medfilter}\{\mathrm{angle}[\hat{P}_{\mathrm{R}}]\} \tag{8}$$

where "angle" indicates the phase extraction operation, and "medfilter" indicates the median filtering operation, the window size is 3 × 3 pixels.

7. Calculate the iterative error between f_{n+1} and f_n, and the iterative error can be expressed by

$$\text{Error} = \sum_{x,\,y}\left[\left|f_{n+1}(x,y)\right| - \left|f_n(x,y)\right|\right]^2 \tag{9}$$

Replace f_{n+1} for f_n, and repeat the above steps 1 to 7 until the calculated iterative error is smaller than the preset threshold value δ. For instance, δ can be set to 0.0001 in the iterative decryption algorithm. After this iterative decryption process, the plaintext can be retrieved.

3. Numerical simulations and discussion

3.1. The effectiveness of the proposal

Numerical simulations are performed to verify the proposed fully phase optical image encryption system under MATLAB R2014a environment. A collimated plane wave (λ = 633 nm) is used in the simulation. The pixel size of CCD camera is 2.5 μm. Axial distances are set as $z_1 = z_2 = z_3 = 50$ mm. The threshold δ in the iterative retrieval algorithm is predefined as 0.0001. Figure 2**a** shows the plaintext ("peppers.bmp", 512 × 512 pixels). The plaintext is phase-encoded (converting the amplitude-based

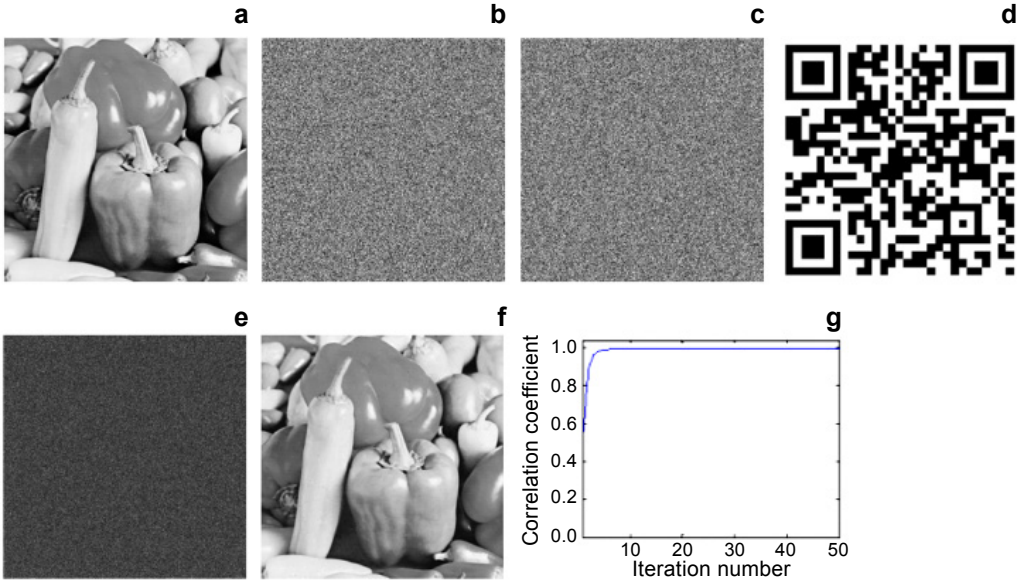

Fig. 2. The plaintext (**a**), M_1 (**b**), M_2 (**c**), the QR code image generated from the assistant key (**d**), the ciphertext (**e**), the decrypted image (**f**), and correlation coefficient (CC) value between plaintext and decrypted image (**g**).

plaintext into a phase-only image), and then encrypted by two RPMs. Figures 2**b** and 2**c** are two statistically independent random phase masks M_1 and M_2, respectively. Figure 2**d** is the QR code image that is used in the encryption scheme. The assistant key corresponding to the QR code in this simulation is a string of words ("Pic Name: Peppers"). Note that, the assistant keys keep changing for encrypting different plaintexts, which makes the encryption scheme more difficult to crack. After the optical encryption process, the intensity diffraction pattern (*i.e.*, ciphertext) captured by CCD camera is shown in Fig. 2**e**. With the help of the proposed decryption algorithm, the original image can be retrieved, which is shown in Fig. 2**f**. It can be seen that the retrieved image is almost the same as plaintext, which indicates the validity of the proposed encryption scheme. In order to quantitatively describe the similarity between the retrieved image and the plaintext, the correlation coefficient (CC) value [16] between them is calculated. The curve of CC values between the retrieved image and the plaintext is shown in Fig. 2**g**, and the eventual CC value after 50 iterations is close to 1 (CC = 0.9954). It can be concluded from the curve that the proposed method has a rapid convergence rate.

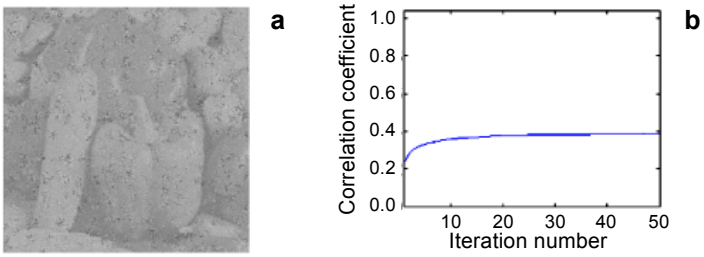

Fig. 3. The retrieved image without median filtering operation (**a**), and correlation coefficient (CC) value between plaintext and the retrieved image (**b**).

In the iterative decryption algorithm, the median filtering operation in each iteration cycle is very important for the convergence of the decryption algorithm. As a comparison, the iterative decryption algorithm without the median filtering operation is also executed. The simulation results are shown in Fig. 3. Figure 3**a** shows the decrypted image after 50 iterations, by utilizing the iterative decryption algorithm without the median filtering operation. The curve of CC values is shown in Fig. 3**b**, and the eventual CC value after 50 iterations is 0.3865. It can be observed that the quality of the decrypted image is degraded greatly (compared with Fig. 2**f**), and only the rough sketch of the plaintext can be retrieved.

The light wavelength λ, the axial distances z_1, z_2 and z_3, the two RPMs, and the QR code image are essential for decrypting the plaintext. For the sake of brevity, only the simulation results with the incorrect QR code image are presented here. Figure 4**a** is the incorrect QR code image that is used for decryption. This QR code is generated from a different assistant key (a string of words "incorrect assistant key"). With this incorrect QR code, the decrypted image is shown in Fig. 4**b**, and it is seen that no information about the plaintext can be observed from it. Figure 4**c** shows the curve of CC value

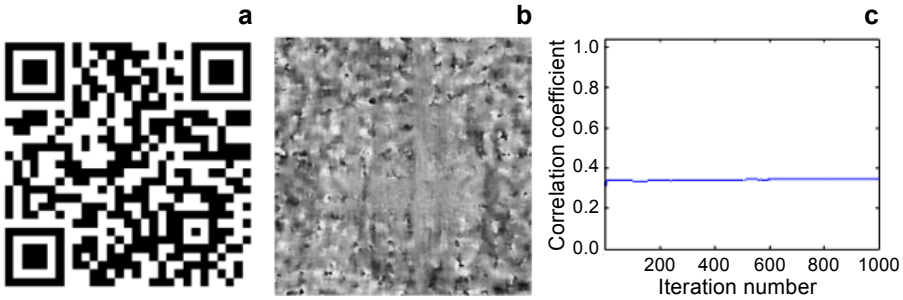

Fig. 4. The incorrect QR code image that is used for decryption (**a**), the decrypted image (**b**), and correlation coefficient (CC) value between plaintext and decrypted image (**c**).

between the retrieved image and the plaintext. After 1000 iterations, the eventual CC value is 0.3490. The simulation results indicate that only those who have the assistant key can correctly retrieve the plaintext. Meanwhile, different plaintexts correspond to different assistant keys, as a result of which the attackers cannot break through the proposed encryption scheme without knowing the correct assistant key.

Since the ciphertext could be contaminated during transmission, robustness against the contaminations is also investigated. Figure 5**a** shows a noise contaminated ciphertext, in which the additive noise is randomly distributed in [–0.1, 0.1]. If this noise con-

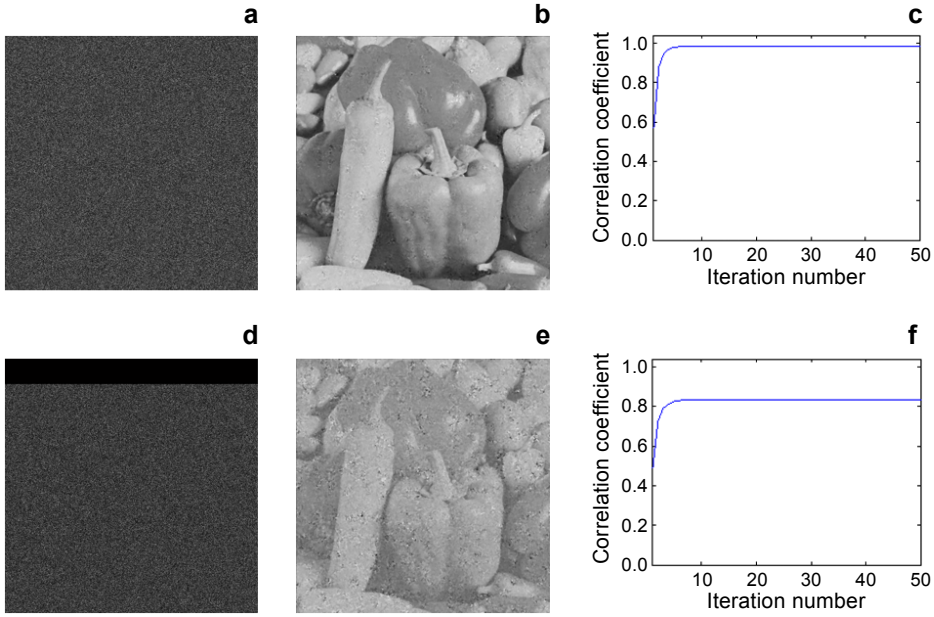

Fig. 5. The noise contaminated ciphertext (**a**), the decrypted image under noise contamination (**b**), correlation coefficient (CC) value between plaintext and decrypted image under noise contamination (**c**), the 10% occlusion contaminated ciphertext (**d**), the decrypted image under occlusion contamination (**e**), and CC value between plaintext and decrypted image under occlusion contamination (**f**).

taminated ciphertext is used for decryption, the decrypted image is shown in Fig. 5**b**. The curve of CC values between the decrypted image and the plaintext is shown in Fig. 5**c**, and the eventual CC value reaches 0.9829. Figure 5**d** shows an occlusion contaminated ciphertext, in which 10% of the ciphertext is occluded. Figure 5**e** shows the decrypted image by using this 10% occluded ciphertext. The curve of CC values between the decrypted image and the plaintext is shown in Fig. 5**f**, and the eventual CC value reaches 0.8341. In order to better evaluate the robustness against noise and occlusion contaminations of the proposed scheme, we compare the simulation results with the previously proposed DIBE scheme (in [19]). According to the description in [19], the eventual CC value between decrypted image and the plaintext is only 0.8732, when the ciphertext is noise contaminated, and when the ciphertext is 10% occluded, the eventual CC value is only 0.3724. Through the comparison, it can be found that, under same contamination conditions, the quality of the decrypted image in the proposed scheme is much higher than that of the previous scheme. The improvement of the quality of the decrypted image under contamination conditions mainly benefits from the introduction of the fully phase technique. It has been verified that fully phase encryption is more robust to additive noise than amplitude-based encryption [10]. The simulation results demonstrate the robustness of the proposed scheme against noise and occlusion contaminations.

3.2. The security of the proposal

It has been claimed that the DIBE schemes can well resist conventional cryptographic attacks (for instance, known-plaintext attack, chosen-plaintext attack, chosen-ciphertext attack, *etc*.) because of the nonlinearity characteristics of the encryption schemes [19]. Similarly, the proposed encryption scheme, as a typical DIBE, has high resistance against conventional attacks as well. Most recently, the DIBE has been cracked by the MPPRA

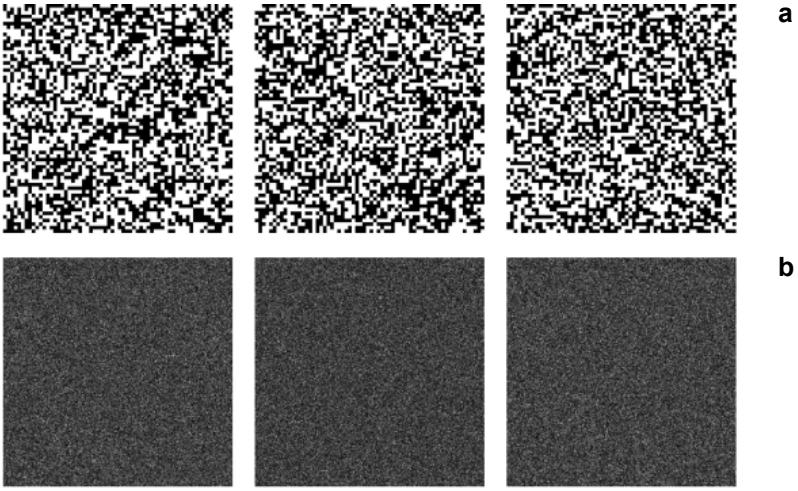

Fig. 6. Three different plaintexts (**a**), and three ciphertexts (**b**).

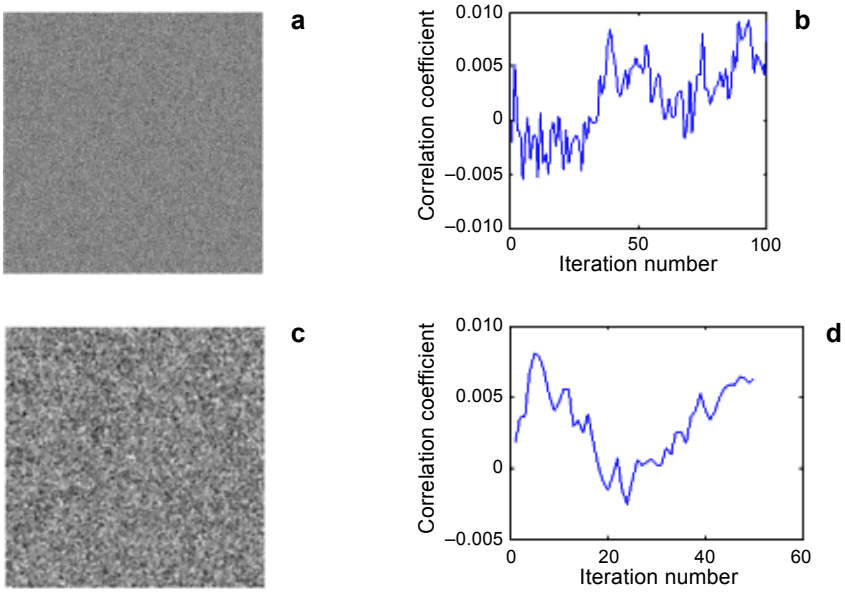

Fig. 7. The retrieved M_2 by using the MPPRA attack (**a**), correlation coefficient (CC) value between the retrieved M_2 and the correct M_2 (**b**), attack result by using the retrieved RPMs (**c**), and CC value between the attack result and the correct plaintext (**d**).

method [22]. In order to investigate the proposal's robustness against the MPPRA attack, the MPPRA method is utilized to attack the proposed encryption scheme. Assume that an attacker has obtained 50 pairs of plaintexts and ciphertexts. The plaintexts are 50 randomly distributed binary images which are different from each other. For the sake of brevity, only three pairs of plaintexts and ciphertexts are shown in Fig. 6. With the help of these plaintext-ciphertext pairs, the random phase mask M_2 can be retrieved by using the MPPRA attack, which is shown in Fig. 7**a**. The curve of CC value between the retrieved RPM and the correct RPM is shown in Fig. 7**b**. The obtained CC value is within the range of [–0.0055, 0.0092]. The retrieved RPMs are utilized to further decrypt the intercepted ciphertext (see Fig. 2**e**), and the attack result is shown in Fig. 7**c**. The curve of CC value between the attack result and the correct plaintext is shown in Fig. 7**d**. The obtained CC value is within the range of [–0.0025, 0.0081]. Apparently, the correct plaintext cannot be cracked by the MPPRA attack, which means the proposed scheme can well resist the MPPRA attack, and has a higher level of security than ordinary DIBE schemes.

3.3. Discussion

From the theoretical analysis and the simulation results, the advantages of the proposal can be concluded as follows.

Through the security simulation results, we can see that the most prominent advantage of the proposal is that it can well resist the MPPRA attack (not to mention the

conventional cryptographic attacks). As a result, the proposed scheme is much more secure compared to DIBE schemes.

Only a single diffraction intensity pattern needs recording in the proposed encryption scheme. Therefore, neither interferometric setup nor movement of the optical elements is necessary for encryption, which greatly simplifies the encryption and decryption procedures.

The QR code image used for encryption is generated from the assistant key, which is a string of alphanumeric data, so compared to the large RPM, the assistant key is more convenient to store and transmit.

The proposed encryption scheme is a fully phase-based optical encryption, in which the plaintext is phase-encoded in the first place. It has been stated that the fully phase -based encryption is much more robust to additive noise than amplitude-based encryption [11]. The simulation result also verifies that the proposed scheme is more robust against noise and occlusion contaminations than other DIBE schemes.

4. Conclusion

In summary, a fully phase diffractive-imaging-based optical encryption scheme is proposed in this paper. In the optical encryption process, a QR code image generated from an assistant key is placed in the optic path to produce a random illumination, which helps make the proposed scheme immune to MPPRA attack. For decryption, an iterative phase retrieval algorithm with a median filtering operation in each iteration is implemented. Also, relative numerical simulations have been performed to verify the effectiveness, the security, and the robustness against contaminations.

Acknowledgements – This study was supported by the National Natural Science Foundation of China (Grant No. 61505091), the College Key Scientific Research Programs of Henan Province (Grant No. 16B510005), and the Excellent Young Teacher Fund of Nanyang Normal University (QN2016010 and QN2016011).

References

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

[4] LINFEI CHEN, DAOMU ZHAO, *Optical image encryption based on fractional wavelet transform*, Optics Communications **254**(4–6), 2005, pp. 361–367.

[5] KUMAR NISHCHAL N., JOSEPH J., SINGH K., *Securing information using fractional Fourier transform in digital holography*, Optics Communications **235**(4–6), 2004, pp. 253–259.

[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] 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.

[8] CHAO LIN, XUEJU SHEN, BAOCHEN LI, *Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code*, Optics Express **22**(17), 2014, pp. 20727–20739.
[9] JUN LI, JIAOSHENG LI, LINA SHEN, YANGYANG PAN, RONG LI, *Optical image encryption and hiding based on a modified Mach–Zehnder interferometer*, Optics Express **22**(4), 2014, pp. 4849–4860.
[10] TOWGHI N., JAVIDI B., LUO Z., *Fully phase encrypted image processor*, Journal of the Optical Society of America A **16**(8), 1999, pp. 1915–1927.
[11] KUMAR NISHCHAL N., JOSEPH J., SINGH K., *Fully phase encryption using fractional Fourier transform*, Optical Engineering **42**(6), 2003, pp. 1583–1588.
[12] XIAOGANG WANG, DAOMU ZHAO, *Fully phase multiple-image encryption based on superposition principle and the digital holographic technique*, Optics Communications **285**(21–22), 2012, pp. 4280–4284.
[13] MARKMAN A., JAVIDI B., *Full-phase photon-counting double-random-phase encryption*, Journal of the Optical Society of America A **31**(2), 2014, pp. 394–403.
[14] BARRERA J.F., MIRA-AGUDELO A., TORROBA R., *Experimental QR code optical encryption: noise-free data recovering*, Optics Letters **39**(10), 2014, pp. 3074–3077.
[15] BARRERA J.F., MIRA A., TORROBA R., *Optical encryption and QR codes: secure and noise-free information retrieval*, Optics Express **21**(5), 2013, pp. 5373–5378.
[16] 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.
[17] WEN CHEN, XUDONG CHEN, SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010, pp. 3817–3819.
[18] 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.
[19] 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.
[20] XIAOGANG WANG, WEN CHEN, XUDONG CHEN, *Optical binary image encryption using aperture-key and dual wavelengths*, Optics Express **22**(23), 2014, pp. 28077–28085.
[21] SHENLU ZHONG, MENGJIAO LI, XIAJIE TANG, WEIQING HE, XIAOGANG WANG, *Information verification and encryption based on phase retrieval with sparsity constraints and optical inference*, Optics and Lasers in Engineering **88**, 2017, pp. 214–220.
[22] TUO LI, YISHI SHI, *Security risk of diffractive-imaging-based optical cryptosystem*, Optics Express **23**(16), 2015, pp. 21384–21391.

Received September 13, 2016
in revised form January 3, 2017