Optica Applicata, Vol. LII, No. 1, 2022
DOI: 10.37190/oa220104

Compressed optical image encryption in the diffractive-imaging-based scheme by input plane and output plane random sampling

Shujia Wan, Qiong Gong, Hongjuan Wang, Shibang Ma, Yi Qin*

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

*Corresponding author: 641858757@qq.com

The successful recovery of the plaintext in the simplified diffractive-imaging-based encryption (S-DIBE) scheme needs to record one intact axial intensity map as the ciphertext. By aid of compressive sensing, we propose here a new image encryption approach, referred to as compressed DIBE (C-DIBE), which allows further compression of the intensity map. The plaintext is sampled before being sent to DIBE. Afterwards, the intensity map recorded by the CCD camera is also processed by such sampling operation to generate the ciphertext. For decryption, we first obtain the sparse plaintext using the proposed phase retrieval algorithm, and then reobtain the primary plaintext from it via compressive sensing. Numerical results show that a proper proportion of the intensity map (*e.g.* 50%) is enough to totally recover a grayscale image. We achieve multiple-image encryption by space multiplexing without enlarging the size of the ciphertext. The robustness of C-DIBE against brute-force attack evidently outperforms S-DIBE due to the extended key space. Numerical simulation has been presented to confirm the proposal.

Keywords: diffractive-imaging-based encryption, compressive sensing, random sampling.

1. Introduction

Optical encryption has been a very promising research field during the past two decades [1–5]. There are at least two advantages of the optical encryption methods over the traditional ones. First, the optical elements are able to process two-dimensional information in parallel, and they operate, ideally, at the speed of light. Second, the light wave is naturally accompanied by multiple freedom degrees, including wavelength, polarization, and so on. These degrees of freedom can effectively extend the key space and hence strengthen the optical cryptosystem. The representative work, known as the double random phase encoding (DRPE), was proposed in 1995 [6]. By placing two random phase masks (RPMs) in the input and Fourier planes of the optical 4*f* system, it can translate the input image into stationary white noise [6]. The DRPE is then extensively explored, including mainly modifying its architecture [7, 8], analyzing its security [9, 10], enhanc-

ing its robustness against cryptographic attacks [11]. In addition, the invention of DRPE also prompts people to explore more and more new optical cryptosystems [12–17]. Among them, the diffractive-imaging-based scheme (DIBE) [12], which was put forward by CHEN *et al*. in 2010, can be regarded as a revolutionary improvement of DRPE. First, it records the intensity rather than the complex amplitude of the diffraction field as the ciphertext, circumventing the holographic layout. On the other hand, unlike DRPE, the relationship between its plaintext and ciphertext is nonlinear, which reinforces the security to some extent.

Recently, there is an increasing demand on exchanging data via the Internet. It is desirable to simultaneously encrypt and compress the image to facilitate its storage or transmission [18]. Direct compression of the ciphertext using lossless techniques is unpractical due to its white-noise appearance [19]. Instead, people explore to first compress image in some transform domain, such as discrete cosine transform (DCT) domain, and then to conduct the encryption. For instance, ALFALOU *et al*. proposed to realize simultaneous compression and encryption of color video images using DCT spectral multiplexing [20], and they also developed several other methods for this purpose [21–23]. Another commonly used technique for data compression is the well-known compressive sensing (CS), which offers the solution to reconstruct the primary image from a relative small number of measurements [24]. Based on CS and the chaotic system, GONG *et al*. demonstrated an image compression and encryption approach [25]. RAWAT *et al*. demonstrated a double-image encryption method by introducing the CS into a modified DRPE scheme [26]. In particular, DEEPAN *et al*. succeed in encrypting and compressing four images by aid of CS and space multiplexing [27].

In the first several years of the invention of DIBE, it was believed that at least three [28] or more [12] intensity maps along the axis should be captured to fully recover the plaintext. However, in 2014, we proposed the simplified DIBE (S-DIBE) and demonstrated that one such intensity map was enough if a median-filter based phase retrieval algorithm is adopted [29]. In this paper, by aid of CS, we propose for the first time, to our best knowledge, a compressed DIBE (C-DIBE) that allows further compression of the intensity map. In other words, the proposal permits one to totally retrieve the plaintext with far less information than an intact intensity map without altering the optical configuration of the DIBE. The key strategy of the proposal is to perform both input plane and output plane sampling on DIBE. In case of properly sampling, we can first obtain the sampled plaintext from the likewise sampled intensity map, and then recover the whole plaintext via CS. Through space multiplexing, multiple ciphertexts of C-DIBE can be integrated into one synthesized ciphertext to achieve compressed encryption. In addition, the proposal outperforms the S-DIBE in security due to both the newly introduced secret keys and its higher sensitivity to axial distance and wavelength. In particular, the post-processing involved in the encryption procedure is rather time-saving, making the encryption speed of the proposal comparable to S-DIBE. We present numerical results to support the proposal.

2. Methods

2.1. Compressive sensing

Let the image of interest, denoted by f, be a K-dimensional vector. Its observation can be acquired by using a sensing matrix with a size of $J \times K$ ($J \ll K$)

$$y = \Phi f \tag{1}$$

Generally, the reconstruction of f from y is an ill-posed problem. However, it is demonstrated that one can obtain an accurate estimation of f if two premises, sparsity and incoherence, are satisfied [30]. The sparsity requires f to be represented by a k-sparse vector α

$$f = \Psi\alpha \tag{2}$$

where k-sparse means at most k of the total K components of α are nonzero, and Ψ is a $K \times K$ matrix referred to as the sparse operator. The incoherence requires the sensing matrix and the sparse operator are dissimilar as much as possible. More detailed discussion on sparsity and incoherence can be found in [30]. Once these conditions are met, one can recover the f by solving the convex program

$$\min \|\alpha\|_1 \quad \text{subject to} \quad y = \Phi\Psi\alpha \tag{3}$$

Where $\|\alpha\|_1$ stands for the ℓ_1 norm that expressing the number of nonzero entries of α. In applications, we can also reconstruct f by minimizing the total variation (TV) of it

$$\min [\mathrm{TV}(f)] \quad \text{subject to} \quad y = \Phi f \tag{4}$$

with $\mathrm{TV}(f) = \sum_{i,j} \sqrt{(f_{i+1,j} - f_{i,j})^2 + (f_{i,j+1} - f_{i,j})^2}$.

In fact, the TV can be regarded as the ℓ_1 norm of the gradient. Although programs (4) and (3) share the same spirit, the former performs better in practice [31].

2.2. Encryption

Figure 1 illustrates the encryption process of the proposed C-DIBE. The optical configuration marked with the red dashed rectangle is used to realize the DIBE. The monochromatic light from the laser is first expanded by the expander and then collimated by the lens. The spatial light modulator (SLM) is employed to display the input image. The emergent light from the SLM is successively modulated by three RPMs M1, M2, and M3, and is ultimately recorded by the CCD camera. The axis distances between Mi (i = 1, 2, 3) and their right side neighbor devices are denoted by d_1. The original image (*i.e.* plaintext) $U(x, y)$ undergoes the sampling before it is sent to the DIBE scheme.

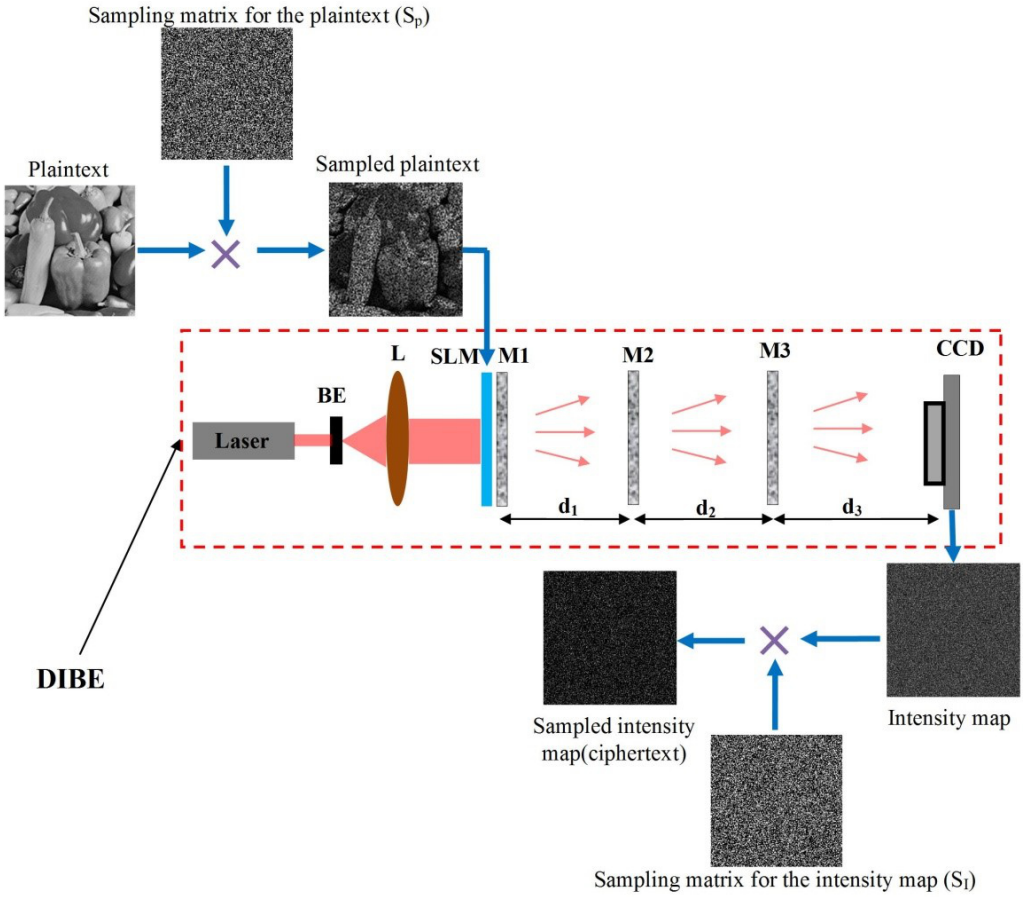

Fig. 1. The encryption process of the proposed C-DIBE. M1, M2, M3, random phase masks; BE, beam expander; CCD, charged-coupled device; SLM, spatial light modulator.

The random sampling of the plaintext is realized by directly multiplying it with a binary sampling matrix $S_P(x, y)$ (*i.e.* the value of each element is "1" or "0"),

$$U_S(x, y) = U(x, y)\, S_P(x, y) \tag{5}$$

Suppose $S_P(x, y)$ is with a size of $M \times N$, we define the sampling ratio (SR) of it as

$$\eta_P = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} S_P(x, y) \times 100\% \tag{6}$$

As the sampling matrix is binary, the SR essentially indicates the ratio that the pixels of "1" account for. In other words, the SR means that, after sampling, η_P percent

information of the target image is preserved while the rest is lost. In fact, Eq. (5) can be regarded as a special form of Eq. (1). Thus, the CS theory implies that, if η_{P} is not too small, we can reobtain a natural image from its sparse representation in the space domain [31].

The sampled plaintext $U_{\mathrm{S}}(x, y)$ is taken as the input image of DIBE and displayed in the SLM for encryption. Let the symbols (x, y), (η, ξ), (p, q) and (μ, v) represent the coordinates of the planes where the SLM/M1, M2, M3, and the CCD locate. In this paper, the free space diffraction of the wavefront is calculated with the angular spectrum method [32], and the complex field immediately before M2 can be mathematically expressed as

$$U(\eta, \xi) = \mathrm{FT}^{-1}\left\{\mathrm{FT}\left[U_{\mathrm{S}}(x, y) M_1(x, y)\right] H(f_x, f_y)\right\} \tag{7}$$

where FT stands for the Fourier transform and FT^{-1} denotes the inverse Fourier transform, and

$$H(f_x, f_y) = \exp\left[j \frac{2\pi d_1}{\lambda} \sqrt{1 - (\lambda f_x)^2 - (\lambda f_y)^2}\right] \tag{8}$$

is the transfer function of the free space propagation. Here j is the imaginary unit, f_x and f_y denote the spatial frequencies, and λ denotes the wavelength of the illumination light. For the sake of brevity, Eq. (8) is rewritten as

$$U(\eta, \xi) = \mathrm{FSP}_{\lambda}\left[U_{\mathrm{S}}(x, y) M_1(x, y);\, d_1\right] \tag{9}$$

Following this symbol, the intensity map captured by the CCD camera is expressed by

$$I(\mu, v) = \left|\mathrm{FSP}_{\lambda}\left\{\mathrm{FSP}_{\lambda}\left[\mathrm{FSP}_{\lambda}\left(U_{\mathrm{SF}}(x, y) M_1(x, y);\, d_1\right) M_2(\eta, \xi);\, d_2\right] M_3(p, q);\, d_3\right\}\right|^2 \tag{10}$$

Instead of being directly saved as the ciphertext, like some previous methods [28, 29], $I(\mu, v)$ is also sampled in the same manner that we deal with the plaintext. The sampling of it can be described by

$$I_{\mathrm{S}}(\mu, v) = I(\mu, v)\, S_{\mathrm{I}}(\mu, v) \tag{11}$$

where $S_{\mathrm{I}}(\mu, v)$ is the sampling matrix for the intensity map with a SR of η_{I}; $I_{\mathrm{S}}(\mu, v)$ is taken as the final ciphertext. The RPMs, wavelength, axial distances, and the sampling matrixes serve as the secret keys. Note that the DIBE operates optically and the digital sampling procedure takes little time under a common PC, the encryption procedure can achieve a rather high speed.

2.3. Decryption

As an inversion of the encryption, the decryption consists mainly of two steps. The first step aims to obtain the sampled plaintext from the ciphertext using the proposed phase retrieval algorithm (PRA), and the second step further recovers the intact plaintext by use of CS. The PRA starts from assigning an initial estimation, $E^{(n)}(x, y)$, $n = 1$, to the plaintext. The estimation then propagates numerically from the input plane to the output plane, where the wavefront can be described by the complex amplitude of

$$C^{(n)}(\mu, v) = \mathrm{FSP}_{\lambda}\left\{\mathrm{FSP}_{\lambda}\left[\mathrm{FSP}_{\lambda}\left(E^{(n)}(x, y)M_1(x, y);\, d_1\right)M_2(\eta, \xi);\, d_2\right]M_3(p, q);\, d_3\right\} \tag{12}$$

Thereafter, the phase of $C^{(n)}(\mu, v)$ is retained while the amplitude of it is replaced by

$$\overline{I(\mu, v)} = I_{\mathrm{S}}(\mu, v)S_{\mathrm{I}}(\mu, v) + \left[1 - S_{\mathrm{I}}(\mu, v)\right]I^{(n)}(\mu, v) \tag{13}$$

where $I^{(n)}(\mu, v)$ denotes the intensity of $C^{(n)}(\mu, v)$. Then, we obtain a new complex amplitude at the output plane:

$$\overline{C^{(n)}(\mu, v)} = \overline{I(\mu, v)}\,\frac{C^{(n)}(\mu, v)}{\left|C^{(n)}(\mu, v)\right|} \tag{14}$$

Then, $\overline{C^{(n)}(\mu, v)}$ numerically propagates from the CCD plane to the input plane, where a renewed intensity map is generated:

$$\overline{E^{(n)}(x, y)} = \left|\mathrm{FSP}_{\lambda}\left\{\mathrm{FSP}_{\lambda}\left[\mathrm{FSP}_{\lambda}\left(\overline{C^{(n)}(\mu, v)};\, -d_3\right)M_3^{*}(p, q);\, -d_2\right]M_2^{*}(\eta, \xi);\, -d_1\right\}\right|^2 \tag{15}$$

where $|\cdot|$ and the superscript asterisk indicate the modulus and conjugation operations, respectively. In addition, the negative distances imply the inverse diffraction of the complex amplitude. Afterwards, a new estimation of the input image can be obtained by using the known $S_{\mathrm{P}}(x, y)$

$$\overline{\overline{E^{(n)}(x, y)}} = \overline{E^{(n)}(x, y)}\,S_{\mathrm{P}}(x, y) \tag{16}$$

The first iteration completes when $\overline{\overline{E^{(n)}(x, y)}}$ is derived, and it is then sent to Eq. (12) to substitute $E^{(n)}(x, y)$ to launch the next iteration. So we have

$$E^{(n+1)}(x, y) = \overline{\overline{E^{(n)}(x, y)}} \tag{17}$$

The iteration described by Eqs. (12)–(17) will continue unless the error between two adjacent estimations of the input image, defined by

$$\text{Error} = \sum \left[\left| E^{(n)}(x, y) \right| - \left| E^{(n-1)}(x, y) \right| \right]^2 \tag{18}$$

drops down to a predefined threshold value δ. Assuming the iteration repeats totally N times before its termination, the estimation in the last iteration is considered as the recovered sampled plaintext, and thus we have

$$U_{\mathrm{S}}(x, y) = \overline{\overline{E^{(N)}}}(x, y) \tag{19}$$

Referring to the CS theory specified in Subsection 2.1, the original image $U(x, y)$ can be recovered by solving the following convex optimization problem

$$\min \left[\mathrm{TV}(U(x, y)) \right] \quad \text{subject to} \quad U_{\mathrm{S}}(x, y) = U(x, y) S_{\mathrm{P}}(x, y) \tag{20}$$

The flowchart for illustrating the decryption is shown in Fig. 2.

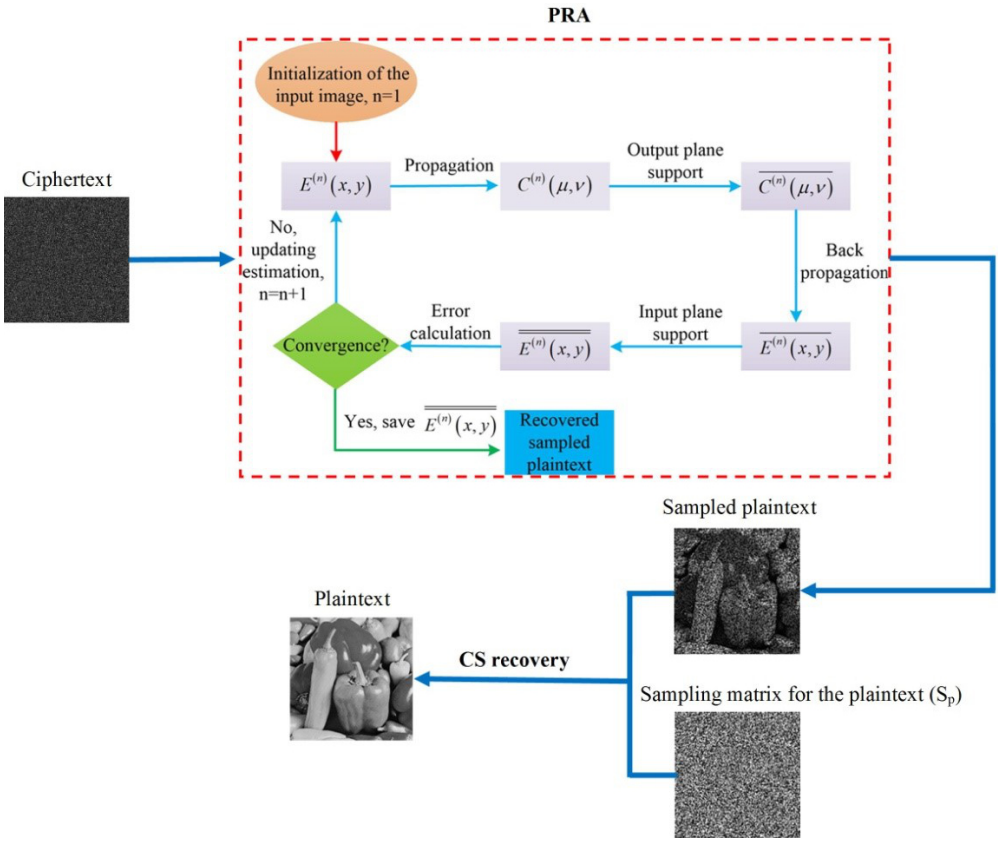

Fig. 2. The flowchart for illustrating the decryption process of the proposal.

3. Simulations and discussions

3.1. Validity test

Numerical simulations are carried out on the platform of MATLAB R2011a to validate the effectivity of the proposal. The wavelength of the illumination light is 632.8 nm, and the axial distances are all set to 100 mm. The threshold for terminating the iteration is empirically set to 0.00001. The SRs η_P and η_I are set respectively as 45% and 50%. The image "peppers" with a size of 256×256 pixels, as shown in Fig. 3**a**, is chosen as the plaintext, and the sampling matrix for it is shown in Fig. 3**b**. Figure 3**c** is the mag-

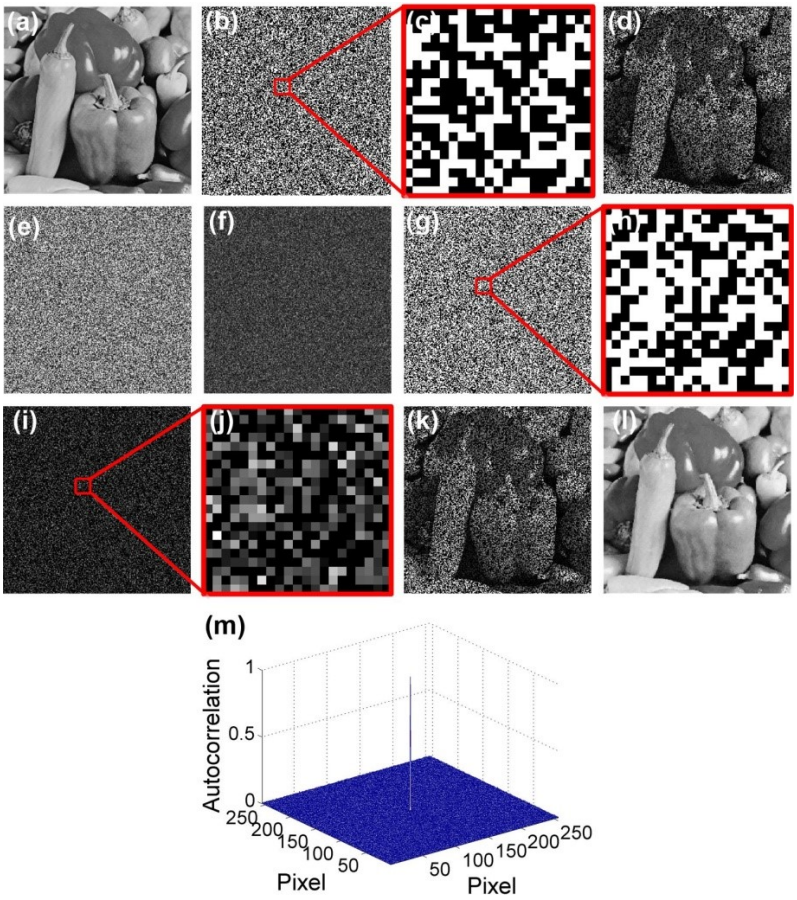

Fig. 3. Validity test of the proposal. (**a**) The plaintext; (**b**) the sampling matrix for the plaintext; (**c**) magnification of the area in (**b**) marked by red square; (**d**) the sampled plaintext; (**e**) the phase distribution of M1; (**f**) the intensity map captured by the CCD camera; (**g**) the sampling matrix for the intensity map; (**h**) magnification of the area in (**g**) marked by red square; (**i**) the sampled intensity map; (**j**) magnification of the area in (**i**) marked by red square; (**k**) the recovered sampled plaintext; (**l**) the recovered plaintext; (**m**) the autocorrelation function of the intensity map.

nification of the area marked by red square in Fig. 3**b**. It is seen there are randomly distributed black ("0") and white ("1") pixels. The sampled plaintext shown in Fig. 3**d** is sent to DIBE for encryption. Figure 3**e** shows the phase distribution of one of the three RPMs (*i.e.* M1), and the other two are not displayed here for brevity. By multiplying the intensity map (Fig. 3**f**) captured by the CCD camera and the corresponding sampling matrix (Fig. 3**g**), we get the sampled intensity map shown in Fig. 3**i**. The magnification of a patch of it is shown in Fig. 3**j**, in which the pure black pixels indicate where the information of the intensity map has been lost. Figure 3**k** shows the recovered sampled plaintext with the proposed PRA. After solving the program described by Eq. (20), we obtain the recovered plaintext (Fig. 3**l**). The correlation coefficient (CC) [29] between it and the original plaintext is 0.9841, indicating a high quality retrieval. It should be pointed out that the intensity map (Fig. 3**f**) is a stationary white noise distribution, as its autocorrelation function is a Dirac function (Fig. 3**m**). In addition, the autocorrelation function remains unchanged in spite of the change of the plaintext.

3.2. Secrete key analysis

In practice, the RPMs, sampling matrixes, axial distances, as well as the wavelength act as the secret keys, and it is important to figure out how they affect the decrypted result. In this investigation, the test of a certain key implies that only this key is changed while all the other keys are kept correct. Figures 4**a**–4**c** show the recovered plaintexts when M1, M2, and M3 are respectively wrong. These results are noise-like patterns and the CC values for them, respectively –0.0102, 0.0134, and 0.0059, also verify their independence of the original image. The decrypted results using incorrect $S_P(x, y)$ and $S_I(x, y)$ are shown in Figs. 4**d** and 4**e**. Although the CCs for them (*i.e.* 0.2203 and

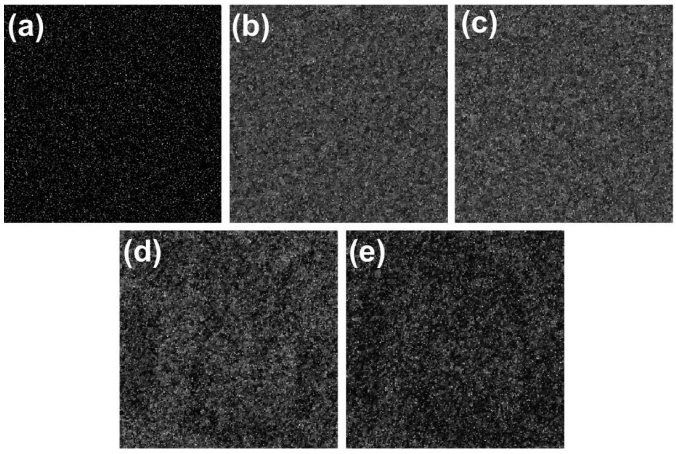

Fig. 4. Decrypted images with incorrect secret keys. (**a**) Incorrect M1; (**b**) incorrect M2; (**c**) incorrect M3; (**d**) incorrect sampling matrix for the plaintext; (**e**) incorrect sampling matrix for the intensity map.

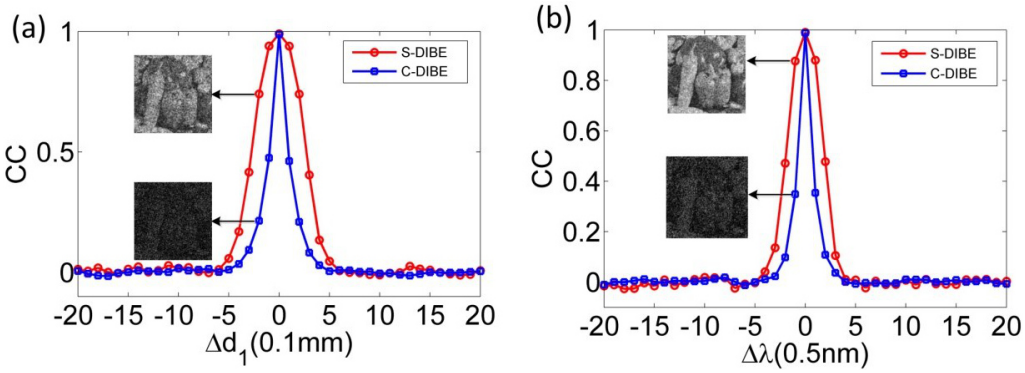

Fig. 5. Axial distance and wavelength sensitivity test. (**a**) The dependence of the CC value upon the distance error; (**b**) the dependence of the CC value upon the wavelength error.

0.1560) are not enough low, still no information about the plaintext can be perceived. Compared with S-DIBE, the three new added secreted keys in our proposal markedly enlarge the key space and hence reinforce the security.

The response of the decrypted images against the changes of axial distances and wavelength is also investigated. Suppose an incorrect axial distance d_1' rather than the actual value d_1 is employed for decryption. We change the distance error, defined as $\Delta d_1 = d_1' - d_1$, from –2 mm to 2 mm with an interval of 0.1 mm, and calculate the CC value for each decrypted image. For comparison, the CC-Δd_1 curves obtained by using this proposal and the S-DIBE are simultaneously displayed in Fig. 5**a**. As can be seen, our curve (*i.e.* blue curve with hollow square marker) has a more sharp shape in the middle, indicating its higher sensitivity to the distance error. In particular, the sub-images in Fig. 5**a** show that a small deviation of 0.2 mm from the correct value in our method will lead to totally unrecognizable decrypted result (CC = 0.2001); by contrast, the same distance error in S-DIBE results in a relatively legible one (CC = 0.7806). Similar results can be obtained when d_2 or d_3 are tested, and they are not illustrated here for brevity. We also study the impact of the wavelength error upon the decrypted image, and the corresponding results using the proposal and S-DIBE are shown in Fig. 5**b**. It is seen that the proposal is also more sensitive to the wavelength error. The sub-images manifest that, when the wavelength error reaches to 0.5 nm, the decrypted image in this proposal is indiscernible while that in S-DIBE is still highly related to the original image.

3.3. Robustness against noise

The ciphertext may be contaminated during transmission, so we examine the robustness of the proposal against noise. We pollute the ciphertext by adding the multiplicative noise to it and then have

$$P_S(\mu, v) = I_S(\mu, v)\left[1 + \beta(\mu, v)\right] \tag{21}$$

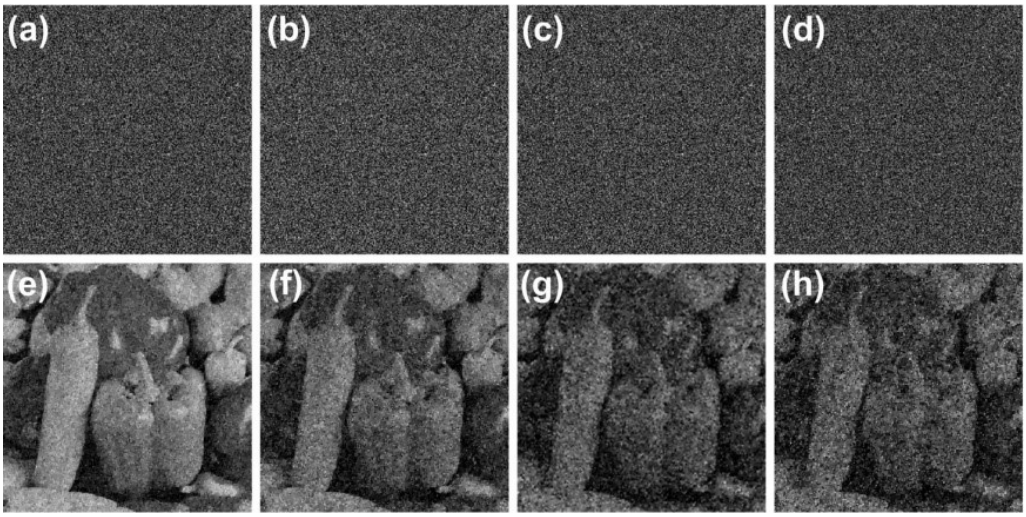

Fig. 6. Noise robustness test. (**a**)–(**d**) The polluted ciphertexts with β = 0.1, 0.2, 0.3, and 0.4; (**e**)–(**h**) the corresponding decrypted images from these ciphertexts.

Where $P_S(\mu, v)$ is the polluted ciphertext, $\beta(\mu, v)$ is a white noise that is uniformly distributed within $[0, \beta]$. For test, we increase the value of β from 0.1 to 0.4 with an interval of 0.1, and the polluted ciphertexts are displayed in Figs. 6**a**–6**d**. The corresponding decrypted images are shown in Figs. 6**e**–6**h**, for which the CC values are 0.9011, 0.7874, 0.6853, and 0.6071, respectively. It is seen that, as expected, the decrypted image degrades as the noise level grows; nevertheless, it can still be recognized when β rises to 0.4.

3.4. The sampling ratio (SR) analysis

The appropriate choice of SR for the plaintext (*i.e.* η_P) and that for the intensity map (*i.e.* η_I) are important for decryption. It has been shown in Subsection 3.1 that the configuration of $\eta_P = 0.45$ and $\eta_I = 0.5$ can produce a high quality decrypted image. In practical applications, η_I is anticipated to be as small as possible such that the intensity map can be fully compressed. The dependence of the CC values of the decrypted image on the SRs is therefore investigated and presented in Fig. 7**a**. Figure 7**b** is the top view of Fig. 7**a**, and the white dashed line denotes where $\eta_P = \eta_I$. Suppose 0.9600 is the minimum acceptable CC value of the decrypted image, the eligible coordinates of (η_P, η_I) constitute approximately a triangular region in the η_P-η_I plane, as indicted by the green lines in Fig. 7**b**. Within this region, the red dot with the coordinate (22%, 25%) of indicates where η_I takes its minimum value. The CC value related to this point is 0.9645, and the corresponding decrypted image is depicted in Fig. 7**c**. Figure 7**c** means that 25% of the area of the intensity map is adequate to produce a high quality decrypted image, which is quadruple that of the S-DIBE. In addition, the green dot represents the point (100%, 100%), and the corresponding decrypted image is

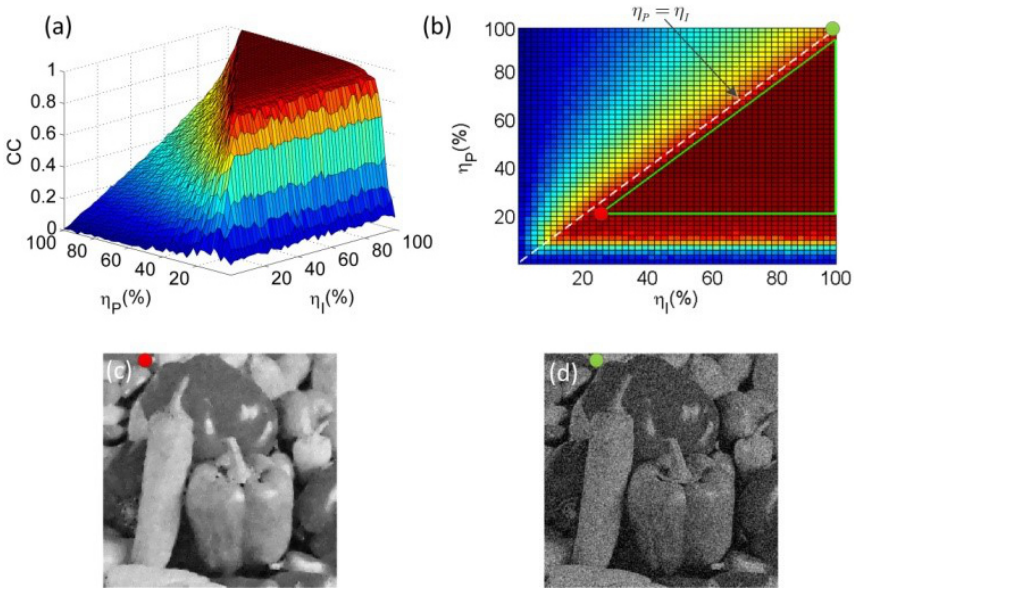

Fig. 7. (**a**) The relationship between the CC values and the sampling ratios; (**b**) the top view of (**a**); (**c**) the decrypted image corresponding to the red dot in (**b**); (**d**) the decrypted image corresponding to the green dot in (**b**).

shown in Fig. 7**d**. As can be seen, the quality of Fig. 7**d** is inferior to that of Fig. 7**c**, and this means a higher SR for the intensity map results, not always in a better decryption. Therefore, the SR for the plaintext and the intensity map should be taken simultaneously into account in real applications. In fact, the triangular region can also be approximately described by

$$\eta_P > 22\%, \quad \eta_P < \eta_I \tag{22}$$

The first inequality in Eq. (22) means that the random sampling operation on the plaintext should reserve sufficient information of it. This can be explained that, in the CS theory, there is a lower limit on the sampling ratio for successful recovery of the original signal. The second inequality in Eq. (22) manifests that the sampling quantity of the intensity map should surpass that of the plaintext.

3.5. Multiple-image encryption

Note that the ciphertext of C-DIBE does not really reduce the amount of transferred image data in digital channels, as the ciphertext is still a 256×256-sized image. However, the sparse form of it allows multiple such ciphertexts to be synthesized into one identical-sized image via space multiplexing [33]. In other words, we can realize multiple-image encryption and decryption based on C-DIBE without increasing the ciphertext size. To illustrate this, three grayscale images, shown in Figs. 8**a**–8**c**, are chosen as the plaintexts for test. They are individually encrypted by C-DIBE and the

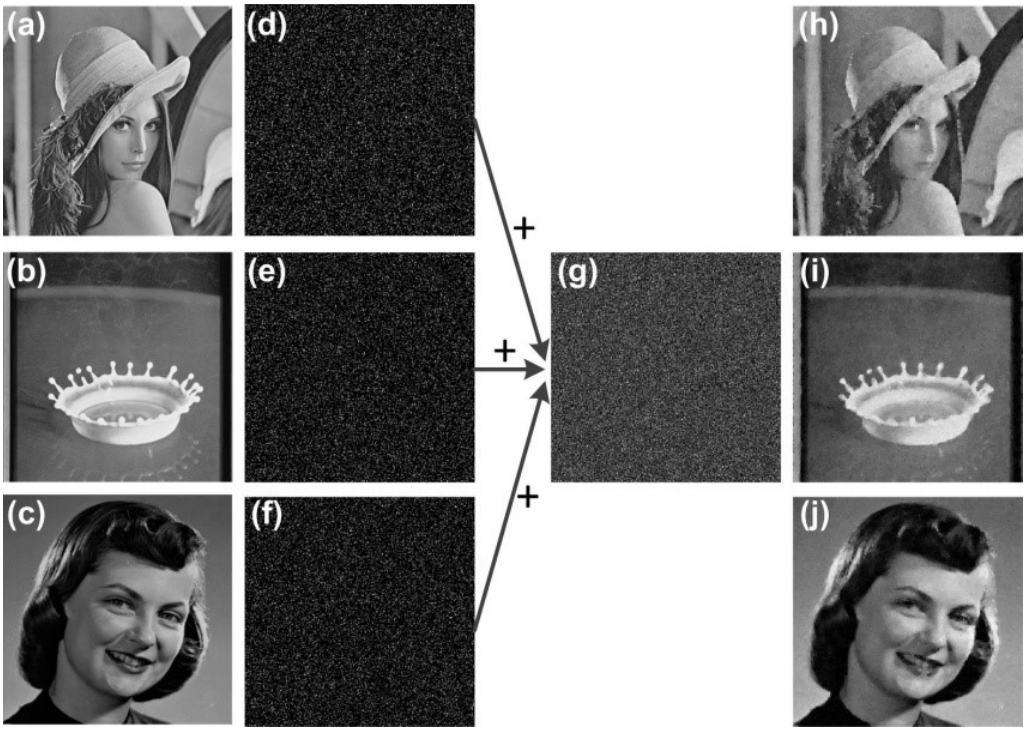

Fig. 8. Multiple-image encryption based on C-DIBE. (**a**)–(**c**) The plaintexts; (**d**)–(**f**) the ciphertexts corresponding respectively to (**a**)–(**c**); (**g**) the synthesized ciphertext; (**h**)–(**j**) the decrypted plaintexts.

SRs for them all equal 0.3 (*i.e.* $\eta_P = 30\%$). The sampling matrixes for the intensity maps have the same SR (*i.e.* $\eta_I = 33\%$), and they are yielded to be complementary to each other, as described in the method suggested in [33]. The C-DBIE ciphertexts of these plaintexts are shown respectively in Figs. 8**d**–8**f**, and their direct superposition forms the synthesized ciphertext (Fig. 8**g**). By aid of the sampling matrix, the ciphertext corresponding to each primary image included in the synthesized ciphertext can be isolated without cross-talk. The final decrypted results are shown in Figs. 8**h**–8**j**, for which the CC values are 0.9554, 0.9760, and 0.9826. It is seen that the plaintexts have been recovered with high quality.

3.6. Some discussions

Cryptography attacks are potential threats to optical cryptosystems. The C-DIBE can be regarded as a variation of S-DIBE, thus it is probable to be vulnerable to chosen-plaintext attack that has breached the S-DIBE [34]. Therefore, the C-DIBE should be cautiously protected from such attack. Recently, there are increasingly interesting on compressing the ciphertexts of optical cryptosystems [18–23]. Most of these methods choose to firstly compress the plaintexts in a certain transform domain (*e.g.* Fourier domain) via multiplexing, and then perform the encryption procedure. By contrast, our method

achieves compression by directly abandoning partial information of the ciphertext, and this may provide new insight into ciphertext compression.

4. Conclusions

In summary, we have reported the C-DIBE, a new image encryption approach, by introducing the CS to the conventional DIBE. The proposal permits one to recover a high quality plaintext in DIBE by using far less information than traditionally needed. In our test, as low as 50% information of an intact intensity map of the conventional DIBE is enough to totally recover the plaintext, and this value can be further relaxed in case of lowering the anticipation of the decrypted result. It is also found that, for successful recovery, the SR for the intensity map must surpass that for the plaintext. Compared with S-DIBE, the proposal has a larger key space due to its higher sensitivity to axial distance and wavelength, as well as the three additional secret keys. Also, the C-DIBE is robust against noise attack. The proposal explores new insight to the DIBE and its feasibility and validity have been confirmed by numerical results.

Acknowledgements
This work is supported by the National Natural Science Foundation of China (61505091), Science and Technology Department of Henan Province (192102110200), and Nanyang Normal University (2020QN031, 2020QN032).

References

[1] JAVIDI B., CARNICER A., YAMAGUCHI M., NOMURA T., PÉREZ-CABRÉ E., MILLÁN M.S., NISHCHAL N.K., TORROBA R., BARRERA J.F., HE W., PENG X., STERN A., RIVENSON Y., ALFALOU A., BROSSEAU C., GUO C., SHERIDAN J.T., SITU G., NARUSE M., MATSUMOTO T., JUVELLS I., TAJAHUERCE E., LANCIS J., CHEN W., CHEN X., PINKSE P.W.H., MOSK A.P., MARKMAN A., *Roadmap on optical security*, Journal of Optics **18**(8), 2016, article 083001, DOI: 10.1088/2040-8978/18/8/083001.

[2] CHEN W., JAVIDI B., CHEN X., *Advances in optical security systems*, Advances in Optics and Photonics **6**(2), 2014, pp. 120–155, DOI: 10.1364/AOP.6.000120.

[3] LIU S., GUO C., SHERIDAN J.T., *A review of optical image encryption techniques*, Optics & Laser Technology **57**, 2014, pp. 327–342, DOI: 10.1016/j.optlastec.2013.05.023.

[4] GONG Q., WANG H., QIN Y., WANG Z., *Modified diffractive-imaging-based image encryption*, Optics and Lasers in Engineering **121**, 2019, pp. 66–73, DOI: 10.1016/j.optlaseng.2019.03.013.

[5] QIN Y., WANG Z., WANG H., GONG Q., ZHOU N., *Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container*, Optics and Lasers in Engineering **105**, 2018, pp. 118–124, DOI: 10.1016/j.optlaseng.2018.01.014.

[6] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[7] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586, DOI: 10.1364/OL.29.001584.

[8] 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, DOI: 10.1364/OL.25.000887.

[9] 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, DOI: 10.1364/OL.30.001644.

[10] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006, pp. 1044–1046, DOI: 10.1364/OL.31.001044.
[11] CHENG X.C., CAI L.Z., WANG Y.R., MENG X.F., ZHANG H., XU X.F., SHEN X.X., DONG G.Y., *Security enhancement of double-random phase encryption by amplitude modulation*, Optics Letters **33**(14), 2008, pp. 1575–1577, DOI: 10.1364/OL.33.001575.
[12] CHEN W., CHEN X., SHEPPARD C.J.R., *Optical image encryption based on diffractive imaging*, Optics Letters **35**(22), 2010, pp. 3817–3819, DOI: 10.1364/OL.35.003817.
[13] NOMURA T., JAVIDI B., *Optical encryption using a joint transform correlator architecture*, Optical Engineering **39**(8), 2000, pp. 2031–2035, DOI: 10.1117/1.1304844.
[14] ZHANG Y., WANG B., *Optical image encryption based on interference*, Optics Letters **33**(21), 2008, pp. 2443–2445, DOI: 10.1364/OL.33.002443.
[15] SUI L., ZHAO X., HUANG C., TIAN A., ANAND A., *An optical multiple-image authentication based on transport of intensity equation*, Optics and Lasers in Engineering **116**, 2019, pp. 116–124, DOI: 10.1016/j.optlaseng.2019.01.006.
[16] SUI L., YIN C., WANG Z., TIAN A., ASUNDI A.K., *Single-pixel correlated imaging with high-quality reconstruction using iterative phase retrieval algorithm*, Optics and Lasers in Engineering **111**, 2018, pp. 108–113, DOI: 10.1016/j.optlaseng.2018.08.001.
[17] CLEMENTE P., DURÁN V., TORRES-COMPANY V., TAJAHUERCE E., LANCIS J., *Optical encryption based on computational ghost imaging*, Optics Letters **35**(14), 2010, pp. 2391–2393, DOI: 10.1364/OL.35.002391.
[18] ALFALOU A., BROSSEAU C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009, pp. 589–636, DOI: 10.1364/AOP.1.000589.
[19] NAUGHTON T.J., MCDONALD J.B., JAVIDI B., *Efficient compression of Fresnel fields for Internet transmission of three-dimensional images*, Applied Optics **42**(23), 2003, pp. 4758–4764, DOI: 10.1364/AO.42.004758.
[20] ALFALOU A., BROSSEAU C., ABDALLAH N., *Simultaneous compression and encryption of color video images*, Optics Communications **338**, 2015, pp. 371–379, DOI: 10.1016/j.optcom.2014.10.020.
[21] ALFALOU A., BROSSEAU C., ABDALLAH N., JRIDI M., *Simultaneous fusion, compression, and encryption of multiple images*, Optics Express **19**(24), 2011, pp. 24023–24029, DOI: 10.1364/OE.19.024023.
[22] ALFALOU A., BROSSEAU C., ABDALLAH N., JRIDI M., *Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks*, Optics Express **21**(7), 2013, pp. 8025–8043, DOI: 10.1364/OE.21.008025.
[23] ALFALOU A., BROSSEAU C., *Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption*, Optics Letters **35**(11), 2010, pp. 1914–1916, DOI: 10.1364/OL.35.001914.
[24] CANDÈS E.J., WAKIN M.B., *An introduction to compressive sampling*, IEEE Signal Processing Magazine **25**(2), 2008, pp. 21–30, DOI: 10.1109/MSP.2007.914731.
[25] GONG L., QIU K., DENG C., ZHOU N., *An image compression and encryption algorithm based on chaotic system and compressive sensing*, Optics & Laser Technology **115**, 2019, pp. 257–267, DOI: 10.1016/j.optlastec.2019.01.039.
[26] RAWAT N., KIM B., MUNIRAJ I., SITU G., LEE B.-G., *Compressive sensing based robust multispectral double-image encryption*, Applied Optics **54**(7), 2015, pp. 1782–1793, DOI: 10.1364/AO.54.001782.
[27] DEEPAN B., QUAN C., WANG Y., TAY C.J., *Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique*, Applied Optics **53**(20), 2014, pp. 4539–4547, DOI: 10.1364/AO.53.004539.
[28] CHEN W., CHEN X., 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, DOI: 10.1364/JOSAA.30.000806.
[29] QIN Y., GONG Q., WANG Z., *Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme*, Optics Express **22**(18), 2014, pp. 21790–21799, DOI: 10.1364/OE.22.021790.

[30] CANDÈS E., ROMBERG J., *Sparsity and incoherence in compressive sampling*, Inverse Problems **23**, 2007, pp. 969–985, DOI: 10.1088/0266-5611/23/3/008.
[31] LUSTIG M., DONOHO D.L., SANTOS J.M., PAULY J.M., *Compressed sensing MRI*, IEEE Signal Processing Magazine **25**(2), 2008, pp. 72–82, DOI: 10.1109/MSP.2007.914728.
[32] GOODMAN J.W., *Introduction to Fourier Optics*, 2nd Ed., McGraw-Hill, New York, 1996.
[33] GONG Q., LIU X., LI G., QIN Y., *Multiple-image encryption and authentication with sparse representation by space multiplexing*, Applied Optics **52**(31), 2013, pp. 7486–7493, DOI: 10.1364/AO.52.007486.
[34] LI T., SHI Y., *Security risk of diffractive-imaging-based optical cryptosystem*, Optics Express **23**(16), 2015, pp. 21384–21391, DOI: 10.1364/OE.23.021384.

Received December 7, 2020
in revised form February 20, 2021