Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Multiple image encryption by phase retrieval

Hong Di
Yanmei Kang
Yueqin Liu
Xin Zhang

SPIE.

Hong Di, Yanmei Kang, Yueqin Liu, Xin Zhang, “Multiple image encryption by phase retrieval,” *Opt. Eng.* **55**(7), 073103 (2016), doi: 10.1117/1.OE.55.7.073103.

Multiple image encryption by phase retrieval

Hong Di,[a] Yanmei Kang,[a] Yueqin Liu,[a] and Xin Zhang[b,c,*]
[a]University of International Relations, Department of Information Science and Technology, Beijing 100091, China
[b]Institute of Automation, Chinese Academy of Sciences, Brainnetome Center, Beijing 100190, China
[c]Institute of Automation, Chinese Academy of Sciences, National Laboratory of Pattern Recognition, Beijing 100190, China

Abstract. Multiple image encryption (MIE) was proposed to increase the efficiency of encrypting images by processing several images simultaneously. Because of the advantage of optical technology in processing two-dimensional images at high throughput, MIE has been significantly improved by use of methods originating from optics. Phase retrieval was the process of algorithmically finding solutions to the phase loss problem due to light detectors only capturing the intensity. It was to retrieve phase information for the determination of a structure from diffraction data. Error-reduction algorithm is a typical phase retrieval method. Here, we employ it to illustrate that methods in phase retrieval are able to encrypt multiple images and compress them into encrypted data simultaneously. Moreover, the decryption is also designed to handle multiple images at the same time. The whole process including both the encryption and decryption is proposed to improve MIE with respect to the compression and efficiency. The feasibility and encryption of the MIE scheme is demonstrated with encryption experiments under Gaussian white noise and unauthorized access. [DOI: 10.1117/1.OE.55.7.073103]

Keywords: image encryption; phase retrieval; error-reduction algorithm; image processing.

Paper 160764 received May 15, 2016; accepted for publication Jul. 6, 2016; published online Jul. 26, 2016.

1 Introduction

Big image data have been generated by taking advantage of both two-dimensional (2-D) information storage of an image itself and convenient devices for capturing images.[1] Sometimes image data had to be transmitted or received with an encryption because of information security.[2] It would be efficient to encrypt several images together when confronted with lots of images. Conventional image encryption working on an individual image was neither efficient nor convenient to handle multiple ones.[3] Accordingly, multiple image encryption (MIE) was proposed to process several images simultaneously so as to increase the efficiency of the encryption. Because of the high-throughput capability of optical technology to process 2-D information in parallel, methods originating from optics have been employed to perform MIE.[4]

1.1 *Multiple Image Encryption*

Methods of MIE related with the optics included various optical techniques, such as wavelength multiplexing, fractional Fourier transform (FT), and digital holography.[3,5–8] MIE based on wavelength multiplexing was to synthesize the final image by superimposing individual encrypted images together. This encryption strategy was time-consuming and sensitive to cross talk noise from adjacent images.[9] MIE based on a frequency shift was also proposed to encode images in either Fourier or fractional Fourier domain. The technique was good at encoding multiple images, but high-frequency contents of the images had to be sacrificed due to downsize cropping of the spectrum to implement the algorithm effectively.[10] MIE based on the fractional FT was to encode images by distinct fractional orders, but the method required lots of computation to generate initial phase terms by iterations. It was limited in applications because of time-consuming and complex optical setting up. Digital holography was also employed to encode four images by distinct diffraction patterns, and then compressed encrypted file by random sampling.[8] Although compressive sensing could be used in the decryption to fetch reconstructed images, these images were destructed by defocus noise. Recently, phase retrieval has been attempted to encrypt images as an intermediate step.[11,12] Though these studies have involved phase retrieval into image encryption, but did not present advantages of phase retrieval itself in MIE with respect to the compression and efficiency.

1.2 *Phase Retrieval*

Phase retrieval was the process of finding solutions algorithmically to a phase loss problem. The loss consisted in light detectors, which were just capable to capture light intensity.[13,14] Phase information, as the counterpart critical information of the light recording the information of an object, was lost in measurements. However, to reconstruct an object from the measurements, it was necessary to retrieve phase information for a determination of a structure from diffraction data.[15,16]

To retrieve phase information, various approaches have been developed attempting to solve it using both intensity measurements and a priori constraints of original objects. At the very beginning, the solution was obtained with exclusive conditions, so that the solution fitted either for the diffracted-wave field in the near-field region[17] or for a regular object such as a sphere or a cubic.[13] The kind of solutions was more limited than useful in common applications. As the computation technology progressed, iterative methods were involved to solve phase retrieval problem.

*Address all correspondence to: Xin Zhang, E-mail: xzhang@nlpr.ia.ac.cn

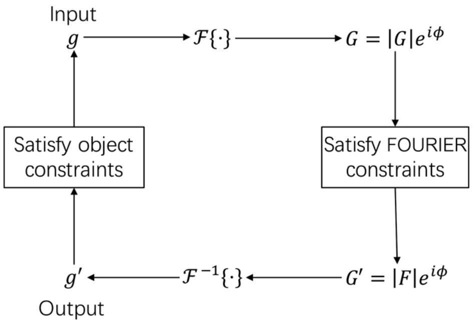
Input
g
$\mathcal{F}\{\cdot\}$
$G = |G|e^{i\phi}$
Satisfy object constraints
Satisfy FOURIER constraints
g'
$\mathcal{F}^{-1}\{\cdot\}$
$G' = |F|e^{i\phi}$
Output

Fig. 1 Block diagram of the error-reduction algorithm in one iteration.

The iterative computation methods concerning the phase retrieval started with the Gerchberg–Saxton method,[18] in which two intensity measurements in object and Fourier domains, were considered. From the Gerchberg–Saxton point of view, the next input image g_{k+1} would result from the output image in last iteration but was modified to satisfy the object-domain constraints of support and nonnegativity.

To be more general, it was to set the next input image g_{k+1} with reference to the output image g'_k in last iteration, where the output image satisfied constraints, and set it to zero, where the output image violated the constraints. This was referred to as the "error-reduction" approach. To some extent, error-reduction method could be thought as a generalization of Gerchberg–Saxton algorithm. The block diagram of the algorithm is shown in Fig. 1.

In the error-reduction algorithm, the first three steps were identical to the first three ones of Gerchberg–Saxton algorithm and the fourth step was performed as

$$g_{k+1} = g'_k \cdot \gamma, \quad \text{where } \gamma(x) = \begin{cases} 0, & x \notin \Upsilon, \\ 1, & x \in \Upsilon, \end{cases} \tag{1}$$

where Υ was the set of points at which g'_k followed the object-domain constraints and γ was a binary function. The complemental set of Υ meant that g'_k was negative or it exceeded the known diameter of the object. Here, "$\cdot$" denoted a Hadamard product as performing element-by-element multiplication.

The "input–output" approach would be to set the next input image to the previous input image, where the output image satisfies the constraints, and set it to the previous input image minus a constant times the output image, where the output image violates the constraints

$$g_{k+1} = g_k - \beta g'_k \cdot \theta, \quad \text{where } \theta(x) = \begin{cases} 0, & x \in \Theta, \\ 1, & x \notin \Theta. \end{cases} \tag{2}$$

The hybrid input–output approach was to set the next input equal to the output, where the output satisfied the constraints, and set it to the input minus a constant times the output, where the output violated the constraints. Hence, the algorithm was a hybrid between the output–output (first line) and input–output (second line) approaches. It was given as

$$g_{k+1} = \begin{cases} g'_k, & x \notin \gamma, \\ g_k - \beta g'_k, & x \in \gamma. \end{cases} \tag{3}$$

The error-reduction algorithm was shown to be closely related to the steepest-descent method. Other algorithms, including the input–output algorithm and the conjugate-gradient method, were shown to converge in practice faster than the error-reduction algorithm. But these methods shared the same strategy, and the error-reduction algorithm was more illustrative than others. Here, we employ it into MIE as an example to introduce encrypting multiple images and compressing by phase retrieval methods. Moreover, the decryption is also designed to handle multiple images at the same time. The whole process including both the encryption and decryption is proposed to improve MIE with respect to the compression and efficiency. The feasibility of the MIE scheme is demonstrated with simulated experiments.

2 Methodology

The method we proposed here can be divided into two steps, naturally. The first step is to encrypt four images by the phase retrieval. We employ the error-reduction algorithm to perform the encryption. The second step is to decrypt encoded information and fetch these four images. The two steps will be introduced in Secs. 2.1 and 2.2.

2.1 *Four Images Encryption by Phase Retrieval*

Suppose there are four images to be encrypted, i_0, i_1, i_2, and i_3. According to error-reduction algorithm, we can assign distinct object constraints to each of them. To achieve simultaneous encryption and compression, these four object constraints can be set as γ_0, γ_1, γ_2, and γ_3 as shown in Fig. 2. Here, γ_0, γ_1, γ_2, and γ_3 can be considered as sets of points as γ in Eq. (1). Referring to these four sets in Fig. 2, each of them covers a specific corner and none of them overlays with each other. The setting up will compress information to a corner after the phase retrieval. It means that

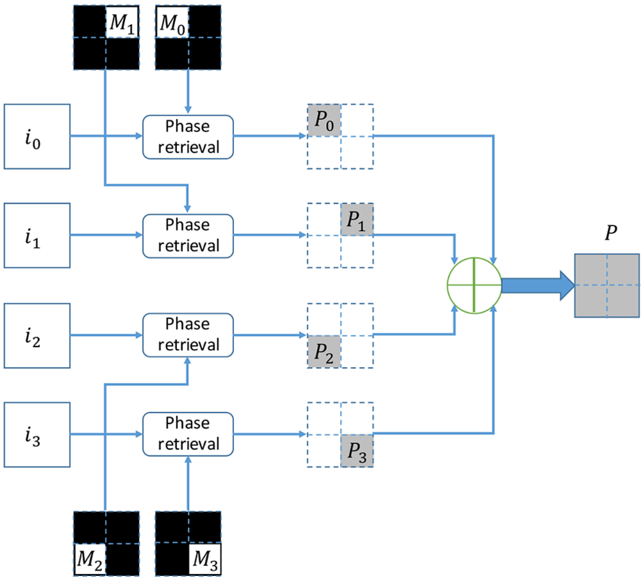

Fig. 2 Encryption process of four images.

the four images will be encrypted into a data with the quarter size of before.

Images to be encrypted, i_0, i_1, i_2, and i_3, can be set as Fourier constraints in the intensity measurements, as Fourier information includes the intensity and phase angle. To each of them, M_0, M_1, M_2, and M_3 will be their object constraints, respectively. The error-reduction algorithm works as follows. Take the first image i_0 and first object constraint M_0 as an example. Then the k'th iteration performed the following four steps:

i. transforming $g_0(x,y)_k$ to the Fourier domain to give a complex field

$$G_0(u,v)_k = |G_0(u,v)_k| \exp[j\theta_0(u,v)_k], \tag{4}$$

ii. changing the field according to the constraint in Fourier domain, i_0, as

$$G_0'(u,v)_k = i_0(u,v) \cdot \exp[j\theta_0(u,v)_k], \tag{5}$$

iii. then inverse Fourier transforming $G_0'(u,v)_k$ back to the object domain to achieve the complex image, $g_0'(x,y)_k$. The complex image can be expressed as

$$g_0'(x,y)_k = |g_0'(x,y)_k| \exp[j\phi_0'(x,y)_k], \tag{6}$$

iv. then allowing it to follow the object constraint, $\gamma_0(x,y)$ in the object domain and resulting in a new version of

$$g_0(x,y)_{k+1} = \gamma_0(x,y) \cdot g_0'(x,y)_k, \tag{7}$$

where $\gamma_0(x,y)=1$, $(x,y)\in M_0$ and $\gamma_0(x,y)=0$, $(x,y)\notin M_0$. In the $(k+1)$'th iteration, start from the first step. These four steps were repeated until no further progress was made or a fixed number of iterations reached. Finally, the image, $i_0(u,v)$, is encoded into P_0 under the object constraint, $\gamma_0(x,y)$.

After performing error-reduction algorithms as shown in Fig. 1 for every image, these four images will be encrypted into P_0, P_1, P_2, and P_3. Because the object constraints are located into distinct corners, the encrypted information will be assigned at each corner correspondingly. Combining the information together, the ultimate encrypted information will be P with the same size of one of original images. Here, P is complex. We separate it into the modulus and phase information as $P=|P|\cdot\exp[j\eta]$. The modulus, $|P|$, will be the encrypted data and the phase term, $\exp[j\eta]$, will be the key for the data.

2.2 *Decryption*

After the encryption step, four images have been encoded into complex data compressively. The compressed data can be transferred and received by wire or wireless. When data are received in a terminal, the decryption process can be started as shown in Fig. 3. The encrypted data can be defined as X_0, X_1, X_2, and X_3. The data are in the Fourier domain. However, it is not in a normal spatial-frequency distribution, but four results of Fourier transformation of four distinct images occupy each of corners. If it is to perform the inverse FT directly on the data, all reconstructed images will be blended and it will be hard to recognize each of them. Moreover, the image size is only a quarter of that of original images. Therefore, we should handle the problem of image blended and size reduced in the decryption. In addition, it is intended to perform inverse FT once, instead of four times, to obtain four images, which means that the decryption can be implemented in an optical setting and decrypt all four images simultaneously.

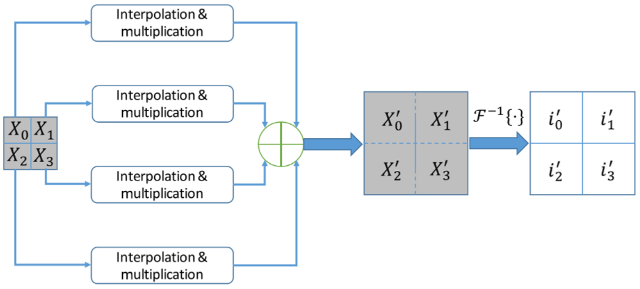
Interpolation & multiplication
Interpolation & multiplication
Interpolation & multiplication
Interpolation & multiplication
X_0 X_1
X_2 X_3
X_0' X_1'
X_2' X_3'
$\mathcal{F}^{-1}\{\cdot\}$
i_0' i_1'
i_2' i_3'

Fig. 3 Decryption process to retrieve four encrypted images.

Figure 3 shows the decryption we proposed. Once encrypted data are received, the unique and correct key data are used to open it. Then the data are distributed as X_0, X_1, X_2, and X_3. Each of them corresponds to data of original four images, but in the Fourier domain. To reconstruct images with right position and right size, we will handle the four Fourier data by ideal spectral interpolation and a multiplication. The spectral interpolation will be equivalent to zero padding in the time domain and the multiplication with a phase term is going to shift reconstructed images to each corner. After the process, these images will be reconstructed with the right size and without any overlay.

2.2.1 *Ideal spectral interpolation*

To illustrate the interpolation, we can start with a one-dimensional signal. Suppose a sampled spectrum $X(u_k)$, $k=0,1,\ldots,N-1$, typically obtained from a discrete FT. We can interpolate by taking the discrete time FT of the inverse discrete FT, which is not periodically extended, but instead zero-padded as

$$\begin{aligned} X(u_\alpha) &= \mathrm{DTFT}(\mathrm{ZeroPad}_\infty\{\mathrm{IDFT}_N[X(u_k)]\}) \\ &\triangleq \sum_{n=-\frac{N}{2}}^{\frac{N}{2}-1}\left[\frac{1}{N}\sum_{k=0}^{N-1}X(u_k)e^{ju_kn}\right]e^{-ju_kn} \\ &= \sum_{k=0}^{N-1}X(u_k)\left[\frac{1}{N}\sum_{n=-\frac{N}{2}}^{\frac{N}{2}-1}e^{j(u_k-u_\alpha)n}\right] \\ &= \sum_{k=0}^{N-1}X(u_k)\mathrm{asinc}_N(u_\alpha-u_k), \end{aligned} \tag{8}$$

where $\mathrm{asinc}_N(u)$ denotes the aliased sinc function. This is the ideal time-limited interpolation in the frequency domain using the aliased sinc function as an interpolation kernel. As we are dealing with 2-D images, Eq. (8) can be expended as

$$X(u_\alpha, u_\beta) = \sum_{k=0}^{K-1}\sum_{l=0}^{L-1} X(u_k, u_l) \cdot \mathrm{asinc}_M(u_\alpha - u_k)\mathrm{asinc}_N(u_\beta - u_l). \tag{9}$$

Fourier data X_0, X_1, X_2, and X_3 will be expended according to the above equation. After the interpolation, Fourier data have been enlarged to the same size as these original images.

2.2.2 *Multiplication by a complex exponential function*

The ideal spectral interpolation rectifies the size of reconstructed images to be equal to that of original images. However, if data produced by the interpolation are input into the inverse FT, reconstructed images would be arranged into the same position in the object domain, i.e., all images would be superimposed together. To eliminate the effect, it needs to take a step of a multiplication by a complex exponential function according to the shift theorem of FT. The direction and position of shifting every image should be well chosen to prevent images from overlapping. According to the shift theorem, the multiplication can be expressed as

$$\mathcal{F}^{-1}\left\{X(u_\alpha, u_\beta)e^{-\frac{j2\pi}{N}(u_\alpha l + u_\beta k)}\right\} = x(n-l, m-k). \tag{10}$$

As long as we set appropriate values for l and k, four reconstructed images will be shifted to different corners in the object domain.

After processing X_0, X_1, X_2, and X_3 by the ideal spectral interpolation and the multiplication, we will achieve X_0', X_1', X_2', and X_3', and they are ready to be input into an inverse FT as shown in Fig. 3. The inverse FT will reconstruct four images i_0', i_1', i_2', and i_3' simultaneously.

3 Experiments

Experiments are performed to demonstrate the effectiveness of the multiple-image encryption method. Four gray images are selected from MATLAB built-in demo images, cameraman, circles, liftingbody, and text, shown in Fig. 4. They are converted to be gray with the size of 256 × 256. The same size will be used for the masks. In these masks, the region of interest will be set as M_0, M_1, M_2, and M_3 as shown in Fig. 2 and the four regions are of the size of 128 × 128. They cover distinct corners in the mask and without overlaying on each other. We performed three experiments to demonstrate the method. The first one is to verify the effectiveness, the second is to verify the robustness against noise, and the third one is to demonstrate the encryption with respect to wrong keys.

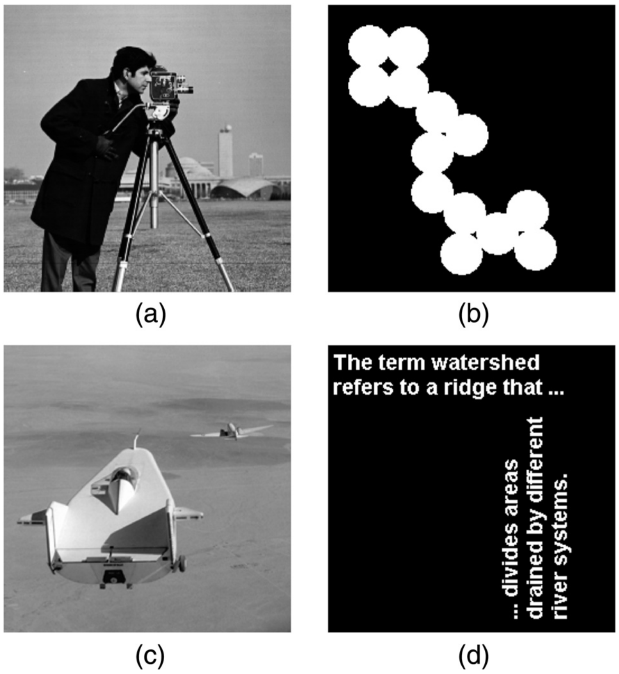

Fig. 4 Original images in experiments: (a) cameraman, (b) circles, (c) liftingbody, and (d) text.

3.1 *Normal Experiment*

In the experiment, the image i_0 and the mask M_0 are the first combination, which is input into the error-reduction phase retrieval algorithm as shown in Fig. 2. They are set as modulus constraints in the Fourier domain and in the object domain, respectively. Similarly, i_1 and M_1, i_2 and M_2, and i_3 and M_3 will be processed by the error-reduction algorithm. Ultimately, the encrypted data will be organized as P as shown in Fig. 5.

As encoded data from original images are arranged into the same corner as the region of interest for each image, the data can be extracted and combined into an encrypted data. The data will be transmitted and received by a terminal.

After the data are received, the terminal uses the key to "open" the data. Then, the decryption process is going to perform to reconstruct images. The process is the same as shown in Fig. 3. Data in each corner will be input into the ideal spectral interpolation and multiplied by a specified complex exponential function. Eventually, the inverse FT is

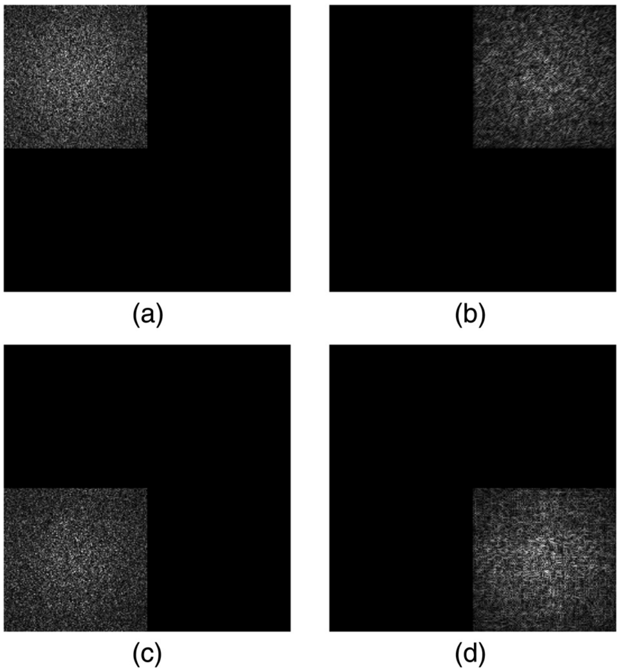

Fig. 5 Images shown in Fig. 4 are encoded by error-reduction algorithm into (a), (b), (c) and (d), respectively.

implemented on the data and the four images will be reconstructed, simultaneously.

3.2 *Experiments Against Noise*

When data are transmitted either by wire or wireless, it is inevitable that the data may be destructed owing to either communication interference or quantization error. After receiving the noisy encoded data, the decryption has to handle the data and recover images as accurately as possible. To testify the qualification of the decryption involved into the proposed method, we suppose Gaussian white noise added into the encoded data. The decryption is verified against the level of the noise.

3.3 *Experiments Against Wrong Keys*

The encryption method is proposed to protect classified images from unauthorized access. To evaluate the protection, it is necessary to quantify the performance against wrong keys. Suppose that 10%, 20%, and 50% key data are obtained by an unauthorized access. The decryption process is implemented on the data. The qualification of the decryption is evaluated in the experiment.

4 Results

4.1 *Normal Experiments*

The first experiment is to demonstrate the feasibility of the proposed method. The reconstructed images are shown in Fig. 6. Compared reconstructed images with original ones, the four images have been reconstructed completely. Textures in cameraman and texts in texts have been remained, which means that the encryption and decryption have preserved details in images effectively. The compression of data size has inevitably involved certain noise into these images, but the noise has not induced perceptible destruction to these images. As we involve an iterative algorithm to solve the error-reduction problem, we set the maximal number of iterations to be 1000 times. In a normal personal computer, 1000 iterations take 4.3 s. Hence, the encryption for four images demands around 16 s. In the encryption algorithm, we generate encoded data and corresponding key data according to original images. To protect data from unauthorized access, the encoded data and key data will be sent out by distinct ways. Once both encrypted data and key data are received, it will be able to decrypt the data.

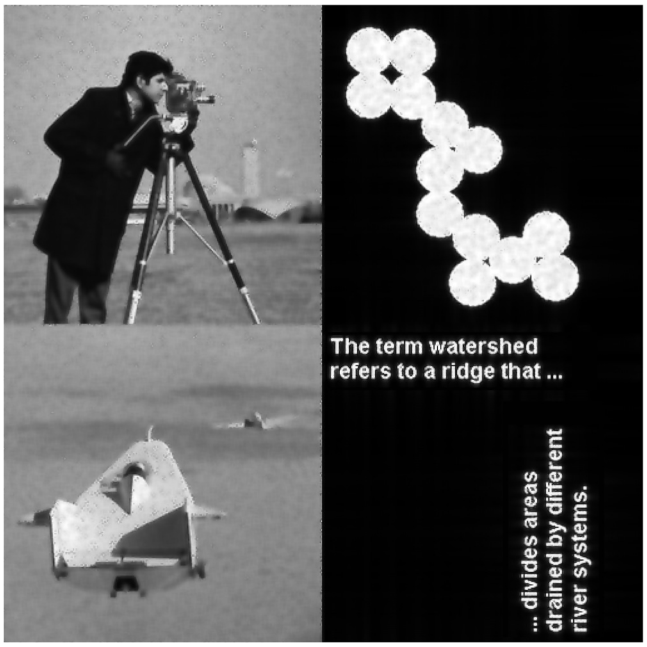

Fig. 6 Decrypted images by proposed method.

To reconstruct images simultaneously, decrypted images are achieved by the inverse FT on four images at the same time. Hence, the four reconstructed images are achieved in one figure. Here, we do not separate four images, because the figure containing four images is intuitive to demonstrate that the decryption eventually handles all four images at the same time.

To evaluate the performance quantitatively, the peak signal-to-noise ratio (PSNR) is employed to measure the quality of decrypted images after compressive encryption and transmission. The matrix is expressed as

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left(\frac{\mathrm{MAX}_x^2}{\mathrm{MSE}}\right), \tag{11}$$

where MSE is calculated as

$$\mathrm{MSE} = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[x(m,n) - x_0(m,n)]^2, \tag{12}$$

and MAX_x denotes the maximum possible pixel value of the image, x.

Take Fig. 6 as the final result in this experiment and calculate PSNR with respect to a combination of original four images. The value of PSNR is 18.19 dB. The PSNR may be lower than expected, but it is in the similar level as it is in other image processing algorithms. Actually, distorted features are also apparent in Fig. 6. One of the kind features is obvious in circles image. It is the gray flocci within these circles, which do not exist in original image, but are left in final one. These flocci textures might not be sensitive to our eyes, but they do distort images so as to make PSNR lower than expected.

Entropy is a quantitative measure of randomness that can be used to characterize the texture of the input image and reflects an expected value of information contained in an image. Here, we compare the entropy of both original images and encrypted images so as to clarify the change of the amount of the information after the encryption. Because there are four images encrypted in the experiment, an average entropy of four images is calculated. The value of the average entropy before and after the encryption is 3.65 and 1.36, respectively. It indicates that our encryption algorithm reduces the information contained in the encrypted image. We infer that the reduction resists in the encryption process, which separates original information into two parts, encrypted image and key data. So each of them shares a part of original data. The compression is quantified by the compression ratio. The ratio is equal to the size of uncompressed data divided by that of the compressed data. As we compress four images to an encrypted image at the same size of

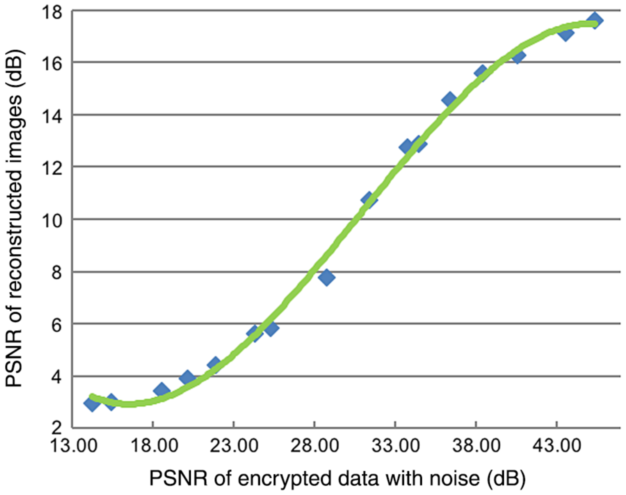

Fig. 7 PSNR of reconstructed images with respect to encrypted data destructed by Gaussian noise.

individual original image. Hence, the compression ratio is $4/1 = 4$.

4.2 *Experiments Against Noise*

When data are transmitted either by wire or wireless, it is inevitable that the data may be destructed owing to either communication interference or quantization error. After receiving the noisy encoded data, the decryption has to handle the data and recover images as accurately as possible. To testify the qualification of the decryption involved into the proposed method, we suppose Gaussian white noise destruct the encoded data. The decryption is verified against distinct level of the noise.

Referring to Fig. 7, it indicates that the decryption can tolerate the noise to some extent. When PSNR of encrypted data involving Gaussian noise is lower than 30 dB, reconstructed images are hardly to recognize important information. When PSNR of encrypted data increases from 30 dB, the quality of reconstructed images goes up dramatically. Once the data destroy the encrypted dataless and make PSNR more than 40 dB, decrypted images almost reach the same level as that without noise in normal experiment.

4.3 *Experiments Against Partial Keys*

The encryption method is proposed to protect images from unauthorized access. However, in some cases, key data may be hacked and encrypted data may be attempted to access by part of keys. To evaluate the performance of the MIE strategy against part of keys, we sample the key data randomly by different sample rate and then measure PSNRs of the decrypted images with reference to the original images.

We sample the key data randomly by the sample rate in a uniform distribution in [0, 1]. Values of key data without sampled are set to 0. Then, these key data will be used in the decryption process. Figure 8 shows the PSNRs of decrypted images under different sample rates as shown in blue square points. We embedded four decrypted texts image into Fig. 8. They are decrypted at sample rate of 0.2, 0.5, 0.8, and 0.9, respectively. When the sample rate is lower than 0.8, it is hardly to identify characters in texts figure.

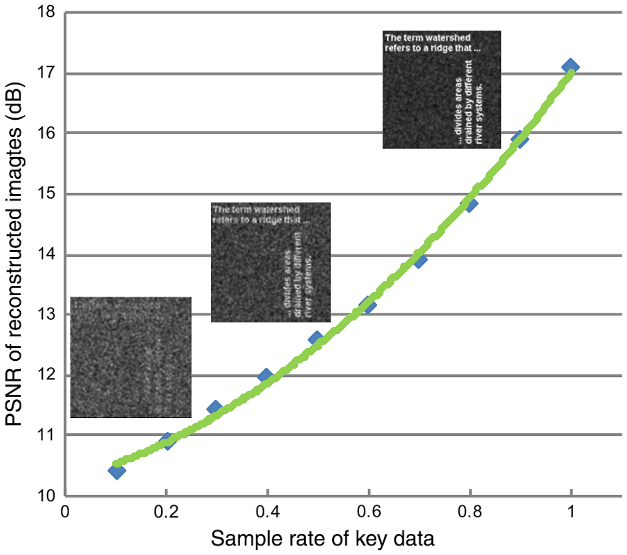

Fig. 8 PSNR of decrypted images under different sample rate of key data.

5 Conclusions

MIE was proposed to increase the efficiency of encrypting images when confronting with huge image data generated by convenient tools of capturing images. Recently, MIE has been significantly improved by methods originating from the optics. However, MIE proposed before was limited in practice because of time-consuming and complex optical setting up. Phase retrieval was the process of algorithmically finding solutions to the phase loss problem due to light detectors only capturing the intensity. It was to retrieve phase information for the determination of a structure from diffraction data. Because of its efficiency, we propose to use it into MIE to encrypt multiple images and compress them into encrypted data simultaneously. Moreover, the decryption is also designed to handle multiple images at the same time.

The encryption and decryption are proposed to improve MIE with respect to the compression and efficiency. The encryption will compress data into a quarter of size of original images. The decryption will eventually handle all four images simultaneously to increase the efficiency. We employ the PSNR to evaluate the performance of the method. In normal experiments, the PSNR of images will be around 20 dB. Referring to the decrypted images, details have been well preserved, though the compression involves certain destruction to these images. Because the transmission of encrypted data is inevitable to incur certain noise, the decryption has been evaluated with data destructed by Gaussian noise. The performance demonstrates that the decryption can tolerate data with noise to some extent. However, if noise damages images severely, the decryption will be impossible to recover images with fine details. Since encrypted data are also possible to be exposed to unauthorized access, it is worthwhile to evaluate the performance against partial key data. We attempt to access data by different sample rate of key data and then decrypt these data. The final results show that the decrypted data are highly dependent on the sample rate. If the sample rate is lower than 0.8, it is hardly to identify information from decrypted images.

Acknowledgments

This work was partially supported by the Natural Science Foundation of China (Grant No. 31571003) and by the Fundamental Research Funds for the Central Universities (Grant Nos. 3262015T70 and 3262016T49).

References

1. C. Lynch, "Big data: how do your data grow?" *Nature* **455**(7209), 28–29 (2008).
2. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier planerandom encoding," *Opt. Lett.* **20**(7), 767–769 (1995).
3. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," *Opt. Lett.* **30**(11), 1306–1308 (2005).
4. T.-C. Poon and P. P. Banerjee, *Contemporary Optical Image Processing with MATLAB*, Elsevier, Oxford (2001).
5. Q. Wang et al., "Double image encryption using phase-shifting interferometry and random mixed encoding method in fractional Fourier transform domain," *Opt. Eng.* **52**(8), 084101 (2013).
6. H. T. Chang et al., "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," *Appl. Opt.* **50**(5), 710–716 (2011).
7. R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Opt. Express* **15**(24), 16067–16079 (2007).
8. H. Di et al., "Multiple-image encryption by compressive holography," *Appl. Opt.* **51**(7), 1000–1009 (2012).
9. D.-H. Kim et al., "Crosstalk analysis for multiple-image encryption and image-quality equalization technology," *Microsyst. Technol.* **21**(12), 2717–2725 (2015).
10. Z. Liu et al., "Optical multi-image encryption based on frequency shift," *Opt. Int. J. Light Electron Opt.* **122**(11), 1010–1013 (2011).
11. L. Sui et al., "Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain," *Opt. Eng.* **53**(2), 026108 (2014).
12. N. Rawat et al., "Compressive sensing based robust multispectral double-image encryption," *Appl. Opt.* **54**(7), 1782–1793 (2015).
13. A. Walther, "The question of phase retrieval in optics," *Opt. Acta Int. J. Opt.* **10**(1), 41–49 (1963).
14. J. R. Fienup, "Phase retrieval algorithms: a comparison," *Appl. Opt.* **21**(15), 2758–2769 (1982).
15. J. R. Fienup, "Reconstruction of an object from the modulus of its Fourier transform," *Opt. Lett.* **3**(1), 27–29 (1978).
16. L. Wu, S. Tao, and S. Xiao, "Phase retrieval-based distribution detecting method for transparent objects," *Opt. Eng.* **54**(11), 113103 (2015).
17. M. R. Teague, "Deterministic phase retrieval: a Green's function solution," *J. Opt. Soc. Am.* **73**(11), 1434–1441 (1983).
18. R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of the phase from image and diffraction plane pictures," *Optik (Stuttg)* **35**, 237 (1972).

Hong Di is an assistant professor at the Department of Information Science and Technology, the University of International Relations. She received her BS and MS degrees from the same university in 2002 and 2009, respectively. She received her PhD in computer science from Beijing University of Posts and Telecommunications. Her research focuses on information security and specializes in image encryption.

Yanmei Kang is an associate professor at the Department of Information Science and Technology, the University of International Relations. She received her BS and MS degrees from Hebei Normal University in 1996 and 1999, respectively. She received her PhD from Tsinghua University in 2003. Her research focuses on information security.

Yueqin Liu: Biography is not available.

Xin Zhang is an associate professor at the Institute of Automation, Chinese Academy of Sciences. He received his BS and MS degrees in biomedical engineering from the Capital Medical University in 2002 and Tsinghua University in 2006, respectively, and received his PhD in electric and electronic engineering from the University of Hong Kong in 2010. His research interests include neurophotonics and neurohemodynamics. He is a member of SPIE.