

Multiple-image encryption by two-step phase-shifting interferometry and spatial multiplexing of smooth compressed signal

Xue Zhang(张学), Xiangfeng Meng(孟祥锋), Yurong Wang(王玉荣), Xiulun Yang(杨修伦), Yongkai Yin(殷永凯)
Citation: Chin. Phys. B . 2018, 27(7): 074205. **doi:** 10.1088/1674-1056/27/7/074205

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Optical encryption of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography

Ying Wang(王莹), Qi Liu(刘琦), Jun Wang(王君), Qiong-Hua Wang(王琼华)
Chin. Phys. B . 2018, 27(3): 034202. **doi:** 10.1088/1674-1056/27/3/034202

Image encryption using random sequence generated from generalized information domain

Xia-Yan Zhang(张夏衍), Guo-Ji Zhang(张国基), Xuan Li(李璇), Ya-Zhou Ren(任亚洲), Jie-Hua Wu(伍杰华)
Chin. Phys. B . 2016, 25(5): 054201. **doi:** 10.1088/1674-1056/25/5/054201

An iterative virtual projection method to improve the reconstruction performance for ill-posed emission tomographic problems

Liu Hua-Wei, Zheng Shu, Zhou Huai-Chun
Chin. Phys. B . 2015, 24(10): 104204. **doi:** 10.1088/1674-1056/24/10/104204

Correspondence normalized ghost imaging on compressive sensing

Zhao Sheng-Mei, Zhuang Peng
Chin. Phys. B . 2014, 23(5): 054203. **doi:** 10.1088/1674-1056/23/5/054203

Multiple-image encryption by two-step phase-shifting interferometry and spatial multiplexing of smooth compressed signal*

Xue Zhang(张学), Xiangfeng Meng(孟祥锋)†, Yurong Wang(王玉荣), Xiulun Yang(杨修伦), and Yongkai Yin(殷永凯)

Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China

(Received 12 December 2017; revised manuscript received 5 March 2018; published online 25 June 2018)

A multiple-image encryption method based on two-step phase-shifting interferometry (PSI) and spatial multiplexing of a smooth compressed signal is proposed. In the encoding and encryption process, with the help of four index matrices to store original pixel positions, all the pixels of four secret images are firstly reordered in an ascending order; then, the four reordered images are transformed by five-order Haar wavelet transform and performed sparseness operation. After Arnold transform and pixels sampling operation, one combined image can be grouped with the aid of compressive sensing (CS) and spatial multiplexing techniques. Finally, putting the combined image at the input plane of the PSI encryption scheme, only two interferograms ciphertexts can be obtained. During the decoding and decryption, utilizing all the secret key groups and index matrices keys, all the original secret images can be successfully decrypted by a wave-front retrieval algorithm of two-step PSI, spatial de-multiplexing, inverse Arnold transform, inverse discrete wavelet transform, and pixels reordering operation.

Keywords: compressive sensing, two-step phase-shifting interferometry, image encryption

PACS: 42.30.Wb, 42.25.Hz, 42.40.Kw, 07.60.Ly **DOI:** 10.1088/1674-1056/27/7/074205

1. Introduction

Information transmission and storage, especially in the age of the internet, is an inevitable part of people's lives. Meanwhile, an information security technique has emerged to prevent the unauthorized information usurpation. Since Réfrégier and Javidi proposed the double random phase encoding (DRPE) technique in 1995,[1] optical information security techniques have attracted an increasing number of researchers, because of their advantages such as high processing speed, high degree of parallelism, high encryption dimension, fast convolution, correlation operation, etc. Subsequently, some typical optical information processing techniques or transforms,[2] such as fractional Fourier transform,[3,4] digital holography,[5–7] phase retrieval,[8–10] two-beam interference,[11] fractional Mellin transform,[12] gyrator transform,[13] joint transform correlator,[14] jigsaw transform,[15] aperture movement,[16,17] and ghost imaging,[18–22] have been combined with DRPE to build more versatile security cryptosystems.

In 2000, Tajahuerce *et al.* proposed an optical encryption method of 3D information by DRPE and four-step phase-shifting interferometry (PSI),[23] in which the 3D object information was encrypted with the Fresnel diffraction pattern generated by DRPE, and then electronically recorded by four-step phase-shifting interferometry. Subsequently, three-step PSI was applied to a digital image encryption and watermarking method,[24] in which the secret image encoded by DRPE and Fresnel diffraction can be recorded into three interferograms. To raise the efficiency of encrypted information transmission, we proposed a two-step phase-shifting algorithm in 2006 and then applied it to image encryption,[25] by which an original object complex field can be recorded and reconstructed with only two interferograms.

Compressive sensing (CS) is a newly developed sampling-reconstruction technique that can complete the sampling and compressing simultaneously. This method can reduce the sampling rate, but at the expense of a complex reconstruction on the recipient.[26–30] Because of this unique advantage, CS has been successfully applied to optical information security fields. In 2014, Zhou *et al.* proposed an image compression-encryption hybrid algorithm with high security based on a key-controlled measurement matrix in CS,[31] in which the circulant matrix was utilized to construct the measurement matrix in CS and control the original row vector of the circulant matrix with a chaos system. Recently, CS has been introduced into the image encryption methods based on DRPE and PSI by Li *et al.*[32,33]

Besides the optical image encryption methods mentioned above, some pioneers have proposed multiple-image encryption methods based on wavelength multiplexing,[34] position multiplexing,[35] phase-only mask (POM) multiplexing,[36,37]

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61775121, 61307003, 61405122, and 11574311), Key R&D Program of Shandong Province, China (Grant No. 2018GGX101002), the Natural Science Foundation of Shandong Province, China (Grant No. R2016FM03), and the Fundamental Research Funds of Shandong University, China (Grant No. 2015GN031).

†Corresponding author. E-mail: xfmeng@sdu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

lateral shifting,[38] etc. In 2014, Deepan *et al.* proposed a multiple-image encryption scheme by spatial multiplexing based on CS and the DRPE,[39] in which a space multiplexing concept was used to exploit the redundant space available due to the compressive sensing process. In 2016, Sui *et al.* proposed a multiple-image encryption method based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain,[40] in which two structured phase masks were utilized to reconstruct the phase keys by nonlinear iterative phase retrieval algorithm. Based on the modified logistic map algorithm,[41,42] compressive ghost imaging and CS, we recently proposed a multiple-image encryption method,[43] in which after a random phase-only-mask generation[44] by the modified logistic map algorithms, the ciphertext can be acquired by discrete cosine transformation, random sampling and scrambling, the combined image generation, and compressive ghost imaging. At this time, we propose a multiple-image encryption method based on two-step phase-shifting interferometry and spatial multiplexing of smooth compressed signal, aiming to reduce the phase-shifting steps and the data volume of the secret images for n images encryption program, and further enhance the data usage efficiency of interferograms derived from two-step phase-shifting interferometry. The principle and procedure will be described firstly, and then a set of simulations will be given to verify the feasibility and robustness of the scheme, finally a conclusion will be drawn.

2. Analysis of fundamental principles

2.1. Brief introduction to compressive sensing

In a conventional sampling process, a massive amount of data collected can only be largely discarded at the compression stage to facilitate storage and transmission. This process of massive data acquisition followed by compression is extremely wasteful.[27] The compressive sensing (CS) theory, which combines sampling and compression into a single non-adaptive linear measurement process, can recover certain signals and images from far fewer samples than the Shannon–Nyquist sampling theorem requires, and CS consists of three steps: sparse representation, random projection, and reconstruction.[26–28]

In signal compression theory, any signal that is sparse or sparsifiable can be compressed through a measurement matrix. Taking an $N \times N$ real value matrix $\boldsymbol{X}$ as an example, it represents a natural image containing a small amount of zero values in the time domain. However, it can be sparsely represented in some arbitrary orthonormal basis $\boldsymbol{\Psi} = [\psi_1, \psi_2, \ldots, \psi_n]$ by discrete cosine transformation (DCT) or discrete wavelet transformation (DWT),[45] which can be expressed as[26–28]

$$\boldsymbol{X} = \sum_{i=1}^{n} \boldsymbol{\alpha}_i \psi_i = \boldsymbol{\Psi}\boldsymbol{\alpha}, \tag{1}$$

where $\boldsymbol{\alpha}$ is an $N \times N$ coefficient matrix of $\boldsymbol{X}$ projected on the $\boldsymbol{\Psi}$ domain, and $\boldsymbol{\Psi}$ is a normal orthonormal basis with ψ_i as columns. After setting $\boldsymbol{\alpha}$ that is less than the preselected threshold as zero, a K-sparse signal α' with K non-zero values can be obtained. It is the K-sparse signal that should be the basic requirement for the CS theorem. The projection coefficient α' offers a concise summary: most of the coefficients are small, and relatively few large coefficients capture most of the information, i.e., the knowledge of K-sparse signal α' is equivalent to the knowledge of $\boldsymbol{X}$. Thus, we are able to reconstruct the image in the time domain, as long as we have a small amount of large projection coefficients in the $\boldsymbol{\Psi}$ domain, which enables CS to reconstruct a general image from the K-sparse signal α'.

Besides the random measurement matrix $\boldsymbol{\Phi}$, a sensor satisfied restricted isometry property (RIP) with size $M \times N$, such as a Gaussian or Hadamard matrix, will exhibit a very low coherence with any sparsifying operator. It is worth mentioning here that a prerequisite should be satisfied first for $\boldsymbol{\Phi}$ prior to compressing the image[26–28]

$$Ck \log\left(\frac{N}{k}\right) \leqslant M \ll N, \tag{2}$$

where C is a small positive constant, and k is the maximum number of non-zero elements in each column of the K-sparse signal after the Arnold transform in order to make the non-zero distribution in each column uniform. The linear measurement process can be expressed as

$$\boldsymbol{Y} = \boldsymbol{\Phi}\alpha' = \boldsymbol{\Phi}\boldsymbol{\Psi}^{\mathrm{T}}\boldsymbol{X}, \tag{3}$$

where $\boldsymbol{Y}$ stands for the measurement data with size $M \times N$. If $\boldsymbol{\Phi}$ holds RIP, a steady solution can be obtained from the above underdetermined system by l_1-norm minimization

$$\tilde{\alpha} = \arg\min \left\|\alpha'\right\|_1 \quad \text{s.t.} \quad \boldsymbol{\Phi}\alpha' = \boldsymbol{Y}, \tag{4}$$

where $\|\cdot\|_1$ denotes the l_1-norm, and $\tilde{\alpha}$ is the solution to the convex optimization program. Besides the l_1-norm minimization,[46] other methods, such as orthogonal match pursuit (OMP),[47] basic pursuit (BP),[48] subspace pursuit (SP),[49] etc., are able to reconstruct the sparse solutions as well. After obtaining the estimated coefficients $\tilde{\alpha}$, then through the inverse Arnold transform and inverse basis transform (e.g., inverse DWT or inverse DCT), a recovered image without perceptual loss but data reduction will show up.

2.2. Image compression and encryption

The decay of Fourier or wavelet coefficients of smooth signals exhibits a power law, which means that for the same image, the reordered smooth image performs with a stronger sparse property than the original image in the Fourier or wavelet domain.[50] Inspired by this thought, prior to compression, we reorder the pixels in ascending/descending order

to lower the inherent frequency of the original image. For a further step, the simulated results are also presented and listed in Fig. 1. Here, we set the Haar wavelet basis as the normal orthonormal basis $\boldsymbol{\Psi}$. It is evident that the wavelet coefficients of the reordered smooth image decay faster than the original image, which implies that we will reconstruct higher fidelity images with fewer measurements.

For simplicity, as depicted in the encryption part shown in Fig. 2, taking four secret images for instance, all the pixels of each image are reordered in ascending order, and four relative index matrices recoding every pixel's original location can be simply represented as SK_1, SK_2, SK_3, and SK_4, followed by five-order Haar wavelet transform and sparseness operation, i.e., any element less than the preset threshold is set as zero. Then, Arnold transform and sample operation could be implemented as Eq. (3), where $M = N/4$. According to spatial multiplexing, a combined image C with the size of $N \times N$, consisting four $M \times N$ sample results: Y_1, Y_2, Y_3, and Y_4 from top to bottom, can be grouped, which will be located at the input plane of the two-step PSI encryption system, and then encoded into two interferograms ciphertexts.

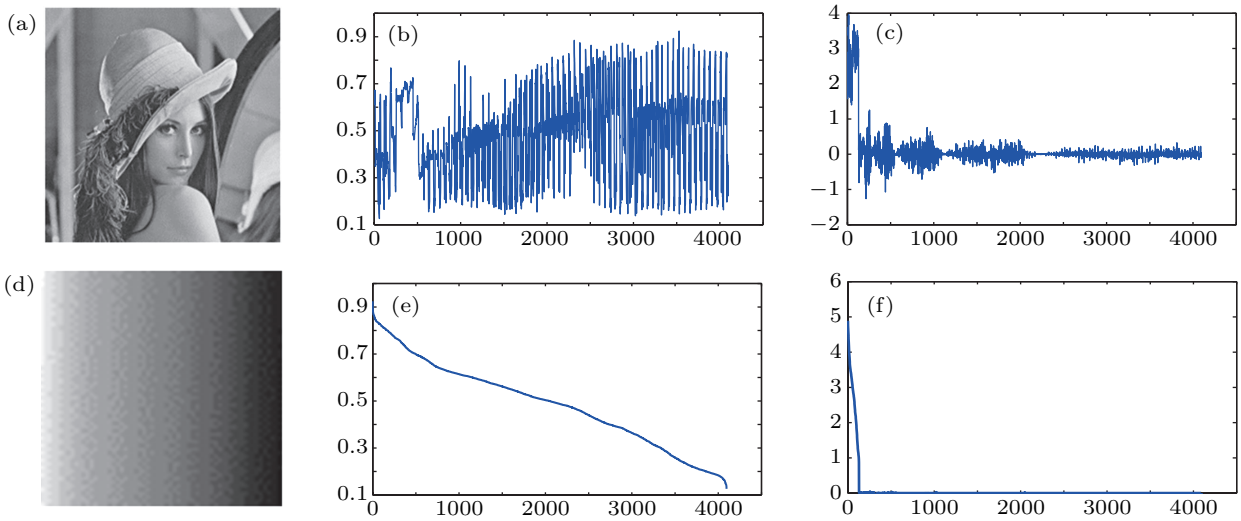


Fig. 1. (color online) (a) Original 'Lena' with 64×64 pixels; (b) pixels distribution of (a); (c) the wavelet coefficients distribution of (a) after five-order Haar DWT; (d) the reordered smooth image in descending order of (a); (e) pixels distribution of (d); (f) the wavelet coefficients distribution of (d) after five-order Haar DWT.

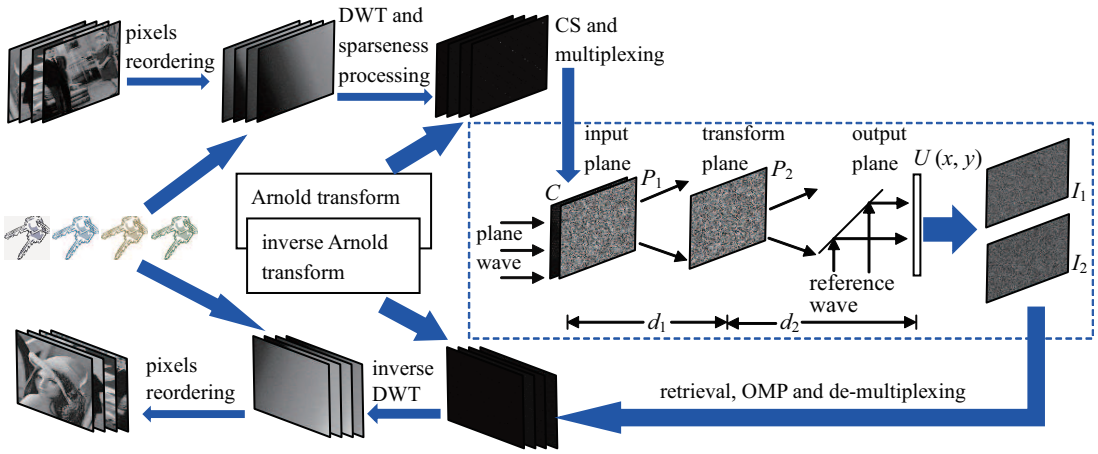


Fig. 2. (color online) Schematic diagram of the multiple image encryption and decryption process.

In the two-step PSI encryption system shown in Fig. 2, a linearly polarized light is collimated, and then divided into two arms (object wave arm, and reference wave arm) by the beam splitter (BS). On the object wave arm, both the combined image $C(x_1, y_1)$ and the first random phase mask (RPM) P_1 are located at the input plane, while the second RPM P_2 is located at the transform plane. The distances between the input plane and the transform plane, and between the transform plane and the output plane are denoted by d_1 and d_2, respectively. When the object wave with wave length λ illuminates the combined image C, at the output plane, a complex wave field can be mathematically represented as[24,25]

$$U(x,y) = \mathrm{FrT}_{d_2}\{\mathrm{FrT}_{d_1}\{C(x_1,y_1)\exp[\mathrm{i}2\pi P_1(x_1,y_1)]\} \times \exp[\mathrm{i}2\pi P_2(x_2,y_2)]\}, \quad (5)$$

where FrT_d stands for the Fresnel transform of distance d, while $P_1(x_1,\ y_1)$ and $P_2(x_2,\ y_2)$ are two independent white noises uniformly distributed in [0,1].

On the reference wave arm, the phase δ of the reference wave is monitored by a piezoelectric transducer mirror (PZT). After interfering with the object wave at the CCD plane, two interferograms will be obtained by the two-step PSI algorithm[25]

$$I_1(x,y) = A_0^2(x,y) + A_r^2 + 2A_0(x,y)A_r\cos[\varphi(x,y)], \quad (6)$$

$$I_2(x,y) = A_0^2(x,y) + A_r^2 + 2A_0(x,y)A_r\cos[\varphi(x,y) - \delta], \quad (7)$$

where $A_0(x,y)$ and $\varphi(x,y)$ are amplitude and phase of $U(x,y)$, respectively. A_r, the constant amplitude of the on-axis reference plane wave, is larger than the maximum of $A_0(x,y)$. Therefore, the combined image C has been encoded into two interferograms ciphertexts. Afterwards, four secret key groups SG_i consisting of each index matrix SK_i and RPM: P_2 will be distributed to four different users: User_i $(i = 1,2,3,4)$. All the ciphertexts and secret keys except four secret key groups are kept by the cryptosystem, anyone who would like to get the decrypted image has to go to the cryptosystem with his/her own secret key group (example: SG_1 consists of SK_1 and P_2).

2.3. Image reconstruction and decryption

The decryption process will occur when the User_i enters the cryptosystem with his/her secret key group SG_i. As the decryption part illustrates in Fig. 2, after the two interferograms ciphertexts I_1 and I_2 are loaded into the decryption system, the reconstructed complex wave field U' can be mathematically expressed as[25]

$$U'(x,y) = \frac{I_1 - a}{2A_r} + \mathrm{i}\frac{I_2 - I_1\cos\delta - (1-\cos\delta)a}{2A_r\sin\delta}, \quad (8)$$

where

$$a = \frac{-v - \sqrt{v^2 - 4uw}}{2u}, \quad (9)$$

$$u = 2(1-\cos\delta), \quad (10)$$

$$v = -2(1-\cos\delta)(I_1 + I_2) - 4A_r^2\sin^2\delta, \quad (11)$$

$$w = (I_1 - I_2\cos\delta)^2 + I_2^2\sin^2\delta + 4A_r^4\sin^2\delta. \quad (12)$$

In case the User_i has the complex information and with the help of RPM P_2 in the secret key group SG_i, the recovered combined image C' at the input plane will be reconstructed with corresponding auxiliary keys

$$C'(x_1,y_1) = \mathrm{abs}\big(\mathrm{IFrT}_{d_1}\big\{\mathrm{IFrT}_{d_2}\left[U'(x,y)\right] \times \exp\left[-\mathrm{i}2\pi P_2(x_2,y_2)\right]\big\}\big), \quad (13)$$

where abs and IFrT denote the real amplitude extraction operation and inverse Fresnel transform, respectively.

It is not until the authorized User_i is able to get the exclusive module Y_i $(i = 1, 2, 3, 4)$ consisting in C' from top to bottom that he/she can obtain correct decrypted images through the next decryption work. After the OMP reconstruction algorithm and inverse Arnold transform, four K-sparse images are recovered; then taking the inverse DWT operator followed by reordering in the index matrix (SK_1, SK_2, SK_3, and SK_4) order, all the original secret images can be decrypted.

Correlation coefficient (CC),[51,52] normalized cross correlation (NCC),[53] structural similarity index metric (SSIM), and mean square error (MSE) are adopted as objective criterions to evaluate the image quality between the recovered and the original secret image.

3. Simulations

A series of simulations have been carried out using MATLAB R2014a to verify the feasibility and validity of the proposed method. All resolutions of the digital images are 15 μm, the parameters: $\lambda = 532$ nm, $d_1 = d_2 = 0.01$ m, and $\delta = \pi/2$. The sizes of the measurement key and the sampled results are 64×256, and the sizes of other images are 256×256.

Four plaintext images with 256×256 pixels to be encrypted are shown in Figs. 3(a)–3(d), and the corresponding reordered images in ascending order are shown in Figs. 3(e)–3(h). After taking 5-order Haar DWT and making sparse operation, four sparsely represented figures are shown in Figs. 4(a)–4(d), and figures 4(e)–4(h) show the corresponding transformed images after Arnold.

A preselected Gaussian random matrix, acting as a measurement matrix, is shown in Fig. 5, and the four compressive images are displayed in Figs. 6(a)–6(d). The final combined image C as an input image in the encryption system is shown in Fig. 7. The two RPMs (P_1 and P_2) are shown in Figs. 8(a) and 8(b), respectively, while figures 9(a) and 9(b) depict the two interferograms (I_1 and I_2).

During decryption, figures 10(a)–10(d) show the four decrypted images with all the corrected keys, and the corresponding CCs, NCCs, MSEs, and SSIMs are listed in Table 1. Obviously, these final decrypted images of good quality are very similar to the corresponding individual secret images.

Table 1. Four quality evaluation metrics for the decrypted images.

	Lena	Cameraman	Flower	Couple
CC	0.9983	0.9989	0.9985	0.9981
NCC	0.9991	0.9992	0.9990	0.9987
SSIM	0.9851	0.9816	0.9851	0.9752
MSE	4.2×10^{-5}	4.9×10^{-5}	5.2×10^{-5}	8.7×10^{-5}

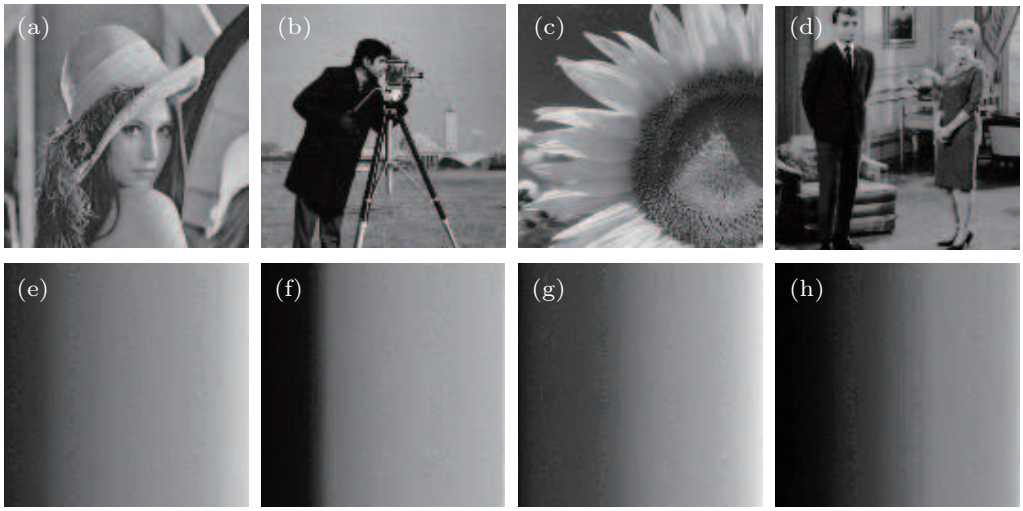


Fig. 3. (a)–(d) Four secret images to be encrypted; (e)-(h) the corresponding reordered images after pixels ascending order for (a)–(d).

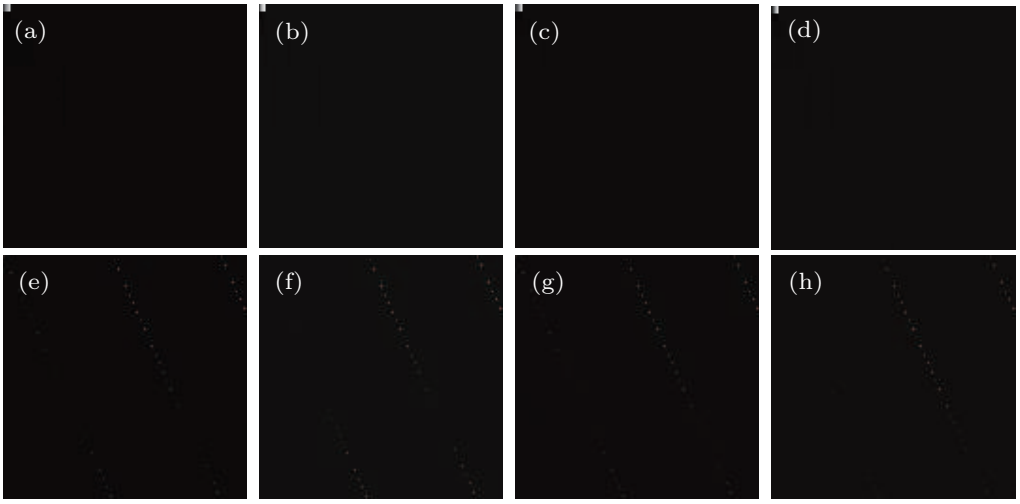


Fig. 4. (a)–(d) Four sparse images after 5-order Haar DWT; (e)–(h) the corresponding images after Arnold transform for (a)–(d).



Fig. 5. The measurement matrix $\boldsymbol{\Phi}$.

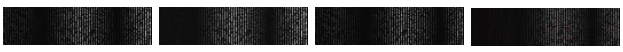


Fig. 6. (a)–(d) Four compressive images by CS.



Fig. 7. The combined image grouped by spatial multiplexing.

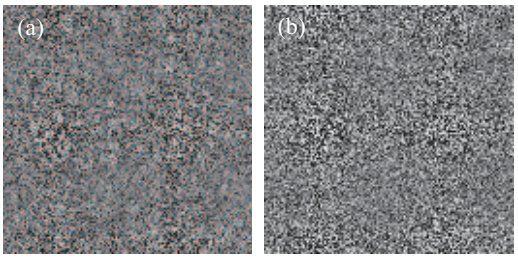


Fig. 8. Two RPMs: (a) P_1, (b) P_2.

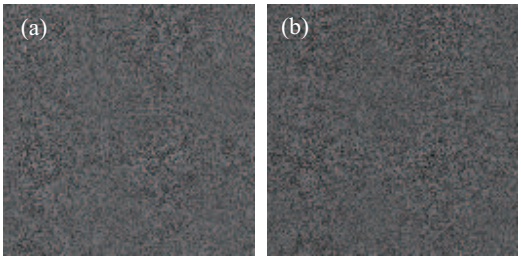


Fig. 9. Two interferograms ciphertexts: (a) I_1, (b) I_2.

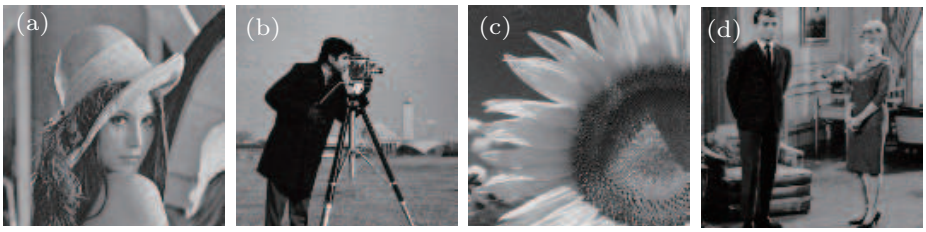


Fig. 10. (a)–(d) Four decrypted images by all the correct keys.

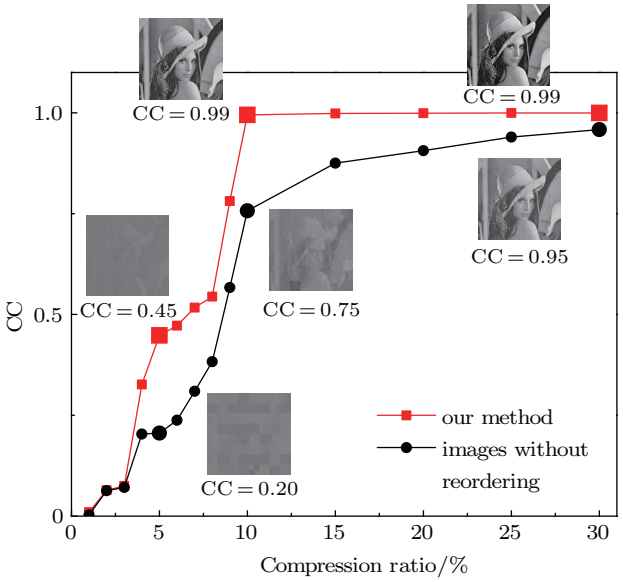


Fig. 11. (color online) The variation curve between the CCs of the decrypted image and compression ratio.

Next, as shown in Fig. 11, we take 'Lena' for instance and compare the encryption performance of our method with the method without reordering in prior to compression. Six large points denote six different reconstructed images under respective compression ratios. The three images above the red curve are recovered by our method. Obviously, our method performs better under the same compression ratio (M/N), and it is not until the compression ratio is less than 10% that CC is less than 0.9, which implies that our method is capable of encoding more than 10 images with the perfectly recovered image quality. However, image quality recovering without reordering falls seriously with the reduction of the compression ratio. Therefore, our method sharply improves data usage efficiency and lessens the storage space.

Taking 'Lena' as an example, the time complexity of the proposed encryption method is plotted in Fig. 12, where the row coordinate denotes the compression ratio, while the column coordinate is the total time cost of encryption and decryption for 'Lena' (Intel(R) Core(TM) i5-4590CPU @ 3.30 GHz; RAM: 8.00GB; No GPU). From the results, we can see that the

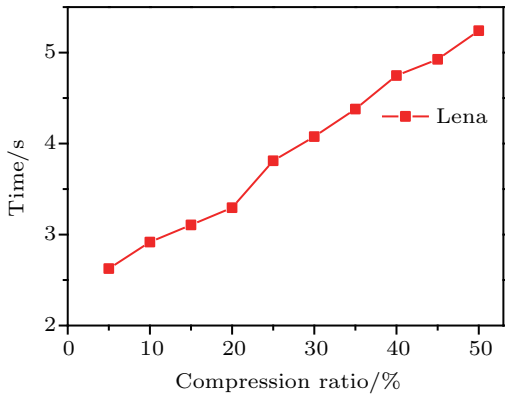


Fig. 12. (color online) The variation curve between the time for encryption and decryption and the compression ratio.

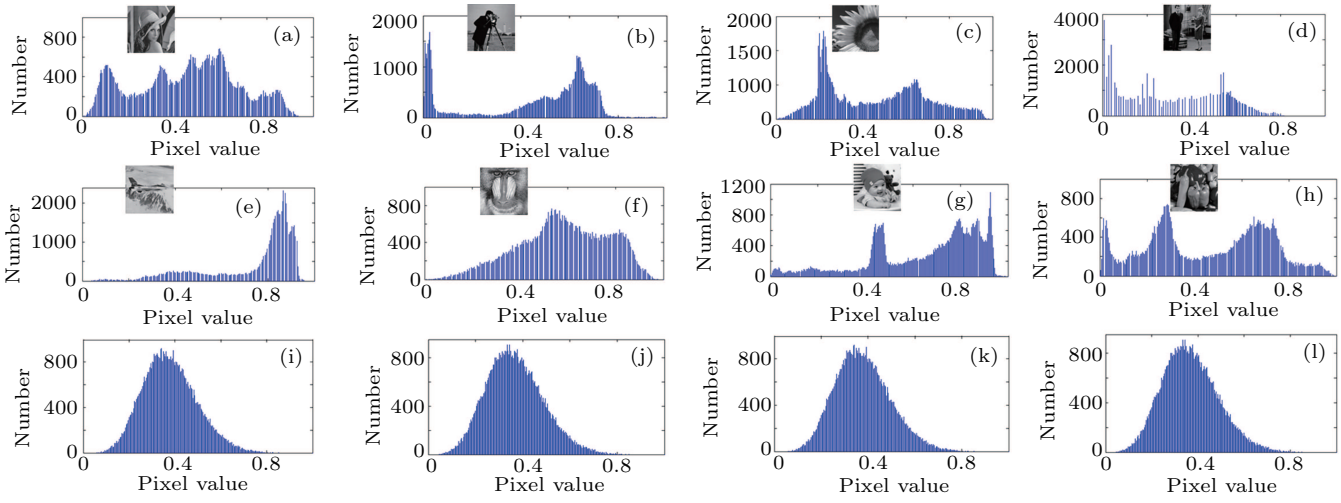


Fig. 13. (color online) Two sets of histograms of original images and interferograms. Set1: (a)–(d) original images; (i)–(j) two interferograms I_1 and I_2; Set2: (e)–(h) original images; (k)–(l) two interferograms I_1 and I_2.

time cost of our method accelerates linearly with the growth of the compression ratio. Because a high fidelity image with CC greater than 0.9 is going to be decrypted when the compression ratio is larger than 10%, a 'Lena' can be encrypted and decrypted for only 3 seconds using our method, and the time complexity of other different original images performs the similar result as Fig. 12.

To reveal that our proposed method is resistant to statistical attack,[54–57] we encrypt two sets of plain images, each of which consists of four images. Fig. 13 shows the histograms of original images and interferograms, where original images have obvious characteristics and differ from each other seriously, but the distribution of each interferogram is quite similar and obeys the Gaussian distribution. Besides, for different sets of images, the distributions of interferograms remain, which implies that the image encryption performance of the proposed method is good enough.

Table 2. Adjacent pixels correlation of original images and interferograms.

	Horizontal	Vertical	Diagonal
Lena	0.9222	0.9603	0.9030
Cameraman	0.9368	0.9585	0.9082
Flower	0.9376	0.9263	0.9050
Couple	0.9530	0.9654	0.9283
I_1	0.0043	0.0145	0.0005
I_2	0.0020	0.0087	0.0029

To further illustrate the performance, the correlation of adjacent pixels is analyzed. We randomly select adjacent pixels from original images and interferograms on the horizontal (vertical, diagonal) direction, and calculate the adjacent pixels correlation.[54–57] All results are shown in Table 2, from which we can see that the adjacent pixels correlation of original images is high, close to 1.0, while the adjacent pixels correlation of interferograms is low, close to 0, which means that the pixels scrambling of our proposed method works very well.

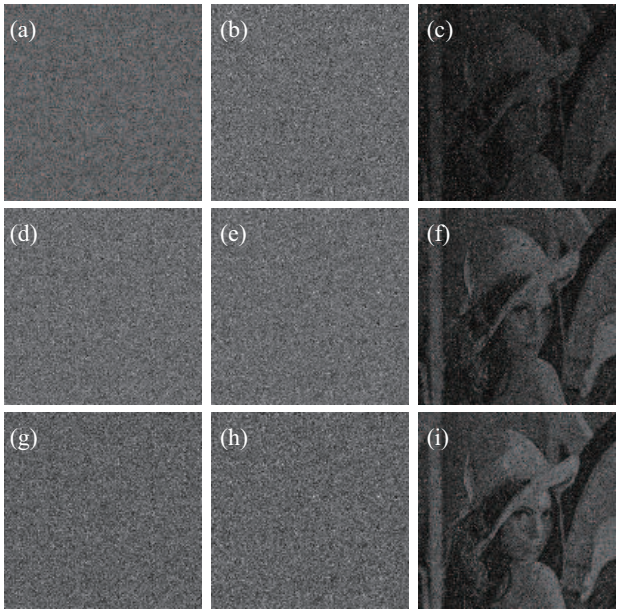


Fig. 14. (a) and (b) Two interferograms distorted by Gaussian white noise; (c) the retrieved image by (a) and (b); (d) and (e) two interferograms distorted by salt and pepper noise; (f) the retrieved image by (d) and (e); (g) and (h) two interferograms distorted by speckle noise; (i) the retrieved image by (g) and (h).

Then, a set of robustness tests against possible attacks are investigated. Two interferograms are contaminated by three different noise attacks: Gaussian white noise of mean 0 and variance 0.01 (as shown in Figs. 14(a) and 14(b)), salt and pepper noise of density 0.01 (as shown in Figs. 14(d) and 14(e)), speckle noise of mean 0 and variance 0.01 (as shown in Figs. 14(g) and 14(h)), and the corresponding reconstructed images for the 'Lena' image are shown in Figs. 14(c), 14(f), and 14(i). From these pictures we can see that all the retrieved images can be recognized without doubt.

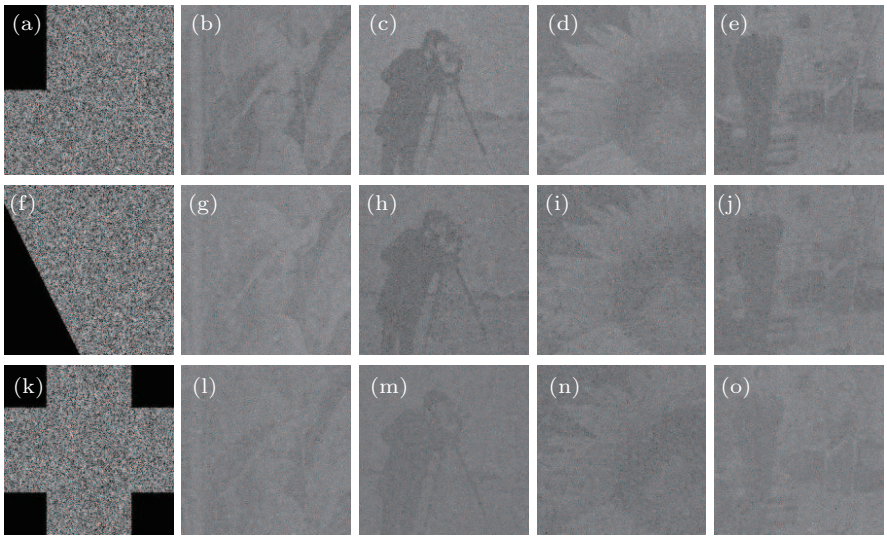


Fig. 15. Three different types of cropping attack: (a) 12.5% occlusion; (f) 20% occlusion; (k) 25% occlusion; the corresponding decrypted images follow with them at the same rows.

The cropping attack on P_2 is tested here. Figure 15 shows three different cropping ways and their decrypted images. From the results, we can see that with the rise of cropping ratio, the fidelity or visibility of decrypted images is declining. But we can still distinguish our interested part from the results when P_2 suffers from the cropping attack ratio. Therefore, our proposed method is capable of resisting the cropping attack.

Different from our previous encryption works based on two-steps of phase-shifting interferometry,[25] in this paper, we introduce an advanced image acquisition and reconstruction technique termed compressive sensing theorem and encrypt n images with only two interferograms. The proposed method can enhance the data usage efficiency of interferograms and lessen the storage of ciphertexts. Compared with the reported optical cryptosystems based on compressive sensing and DRPE,[39] the main advantage of our proposed scheme can be summarized as follows. (i) Prior to compression, we first reorder the original images, which results in smaller nonzeros wavelet coefficients of original images and a lower compression ratio with higher decrypted quality. (ii) The two-step phase-shifting interferometry is easily capable of recording the phase information of complex amplitude which is difficult for DRPE.

4. Conclusion

In conclusion, we proposed a multiple-image encryption method based on two-step phase-shifting interferometry and spatial multiplexing of the smooth compressed signal. Followed by pixels ascending reordering, DWT, sparseness operation, Arnold transform and pixels sampling for four different secret images, one combined image can be grouped with the aid of CS and spatial multiplexing techniques. Then the combined image can be encoded into only two interferograms ciphertexts by the two-step PSI and DRPE, by which the efficiency of ciphertexts data transmission has been greatly raised. The use of the CS theory decreases the data volume of the secret images, thus, with this approach, it is possible to realize multiple image encoding and encryption. Both theoretical analysis and numerical simulations confirm the feasibility of the proposed method.

References

[1] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[2] Xie Z L, Qi B and Ma H T 2016 *Chin. Phys. Lett.* **33** 044206
[3] Unnikrishnan G, Joseph J and Singh K 2000 *Opt. Lett.* **25** 887
[4] Liu S T, Mi Q L and Zhu B H 2001 *Opt. Lett.* **26** 1242
[5] Wang X G, Zhao D M, Jing F and Wei X F 2006 *Opt. Express* **14** 1476
[6] Wan Y H, Man T L, Chen H, Jiang Z Q and Wang D Y 2014 *Chin. Phys. Lett.* **31** 044203
[7] Li J C 2012 *Acta Phys. Sin.* **61** 134203 (in Chinese)
[8] Wang R K, Watson I A and Chatwin C 1996 *Opt. Eng.* **35** 2464
[9] Situ G and Zhang J 2005 *Opt. Commun.* **245** 55
[10] Liu H Q, Ren Y Q, Zhou G Z, He Y, Xue Y L and Xiao T Q 2012 *Acta Phys. Sin.* **61** 078701 (in Chinese)
[11] Zhang Y and Wang B 2008 *Opt. Lett.* **33** 2443
[12] Zhou N R, Wang Y X and Gong L H 2011 *Opt. Commun.* **284** 3234
[13] Liu Z J, Guo Q, Xu L, Ahmad M A and Liu S T 2010 *Opt. Express* **18** 12033
[14] Nomura T, Mikan S, Morimoto Y and Javidi B 2003 *Appl. Opt.* **42** 1508
[15] Kumar P, Joseph J and Singh K 2011 *Appl. Opt.* **50** 1805
[16] Chen W, Situ G and Chen X 2013 *Opt. Express* **21** 24680
[17] Xie Z L, Ma H T, Qi B, Ren G, T A N Y F, He B, Zeng H L and Jiang C 2015 *Chin. Phys. Lett.* **32** 124203
[18] Chen W and Chen X 2013 *Appl. Phys. Lett.* **103** 221106
[19] Si Y, Kong L J and Li Y N 2016 *Chin. Phys. Lett.* **33** 034203
[20] Gao L, Tian J and Lin H L 2015 *Chin. Phys. Lett.* **32** 014202
[21] Zhang Y D and Zhao S M 2017 *Chin. Phys. B* **26** 054205
[22] Pang B Q, Wang S, Cheng T, Kong Q F, Wen L H and Yang P 2017 *Chin. Phys. B* **26** 054204
[23] Tajahuerce E and Javidi B 2000 *Appl. Opt.* **39** 6595
[24] Cai L Z, He M Z, Liu Q and Yang X L 2004 *Appl. Opt.* **43** 3078
[25] Meng X F, Cai L Z, Xu X F, Yang X L, Shen X X, Dong G Y and Wang Y R 2006 *Opt. Lett.* **31** 1414
[26] Donoho D L 2006 *IEEE Trans. Inf. Theory* **52** 1289
[27] Candes E J and Wakin M B 2008 *IEEE Signal Process. Mag.* **25** 21
[28] Zhang Y S, Zhou J T, Chen F, Zhang L Y, Wong K W, He X and Xiao D 2016 *Neurocomputing* **205** 472
[29] Zhang Y S, Zhang L Y, Zhou J T, Liu L C, Chen F and He X 2016 *IEEE Access* **4** 2507
[30] Hao C Q, Wang J, Deng B and Wei X L 2012 *Acta Phys. Sin.* **61** 148901 (in Chinese)
[31] Zhou N R, Zhang A D, Zheng F and Gong L H 2014 *Opt. Laser Technol.* **62** 152
[32] Li J, Li H B, Li J S, Pan Y Y and Li R 2015 *Opt. Commun.* **344** 166
[33] Li J, Li J S, Pan Y Y and Li R 2015 *Sci. Rep.-UK.* **5** 10374
[34] Situ G and Zhang J 2005 *Opt. Lett.* **30** 1306
[35] Situ G and Zhang J 2006 *J. Opt. A: Pure Appl. Opt.* **8** 391
[36] Wang Q, Guo Q, Lei L and Zhou J Y 2013 *Appl. Opt.* **52** 6849
[37] Chen W 2016 *IEEE Photon J.* **8** 1
[38] Barrera J F, Henao R, Tebaldi M, Torroba R and Bolognini N 2006 *Opt. Commun.* **259** 532
[39] Deepan B, Quan C, Wang Y and Tay C J 2014 *Appl. Opt.* **53** 4539
[40] Sui L S, Zhou B, Ning X J and Tian A L 2016 *Opt. Express* **24** 499
[41] Chai X L, Gan Z H, Ke Yuan K, Lu Y and Chen Y R 2017 *Chin. Phys. B* **26** 020504
[42] Ye G D, Huang X L, Zhang Y L and Wang Z X 2017 *Chin. Phys. B* **26** 010501
[43] Li X Y, Meng X F, Yang X L, Yin Y K, Wang Y R, Peng X, He W Q, Dong G Y and Chen H Y 2016 *IEEE Photon J.* **8** 4
[44] Zhu C X and Sun K H 2012 *Acta Phys. Sin.* **61** 120503 (in Chinese)
[45] Gan T, Feng S T, Nie S P and Qing Z Z 2012 *Acta Phys. Sin.* **61** 084203 (in Chinese)
[46] Ji D J, Qu G R, Hu C H, Liu B D, Jian J B and Guo X K 2017 *Chin. Phys. B* **26** 060701
[47] Theis F J, Jung A, Puntonet C G and Lang E W 1969 *IEEE T. Inform. Theory* **15** 419
[48] Chen S S, Donoho D L and Saunders M A 2001 *SIAM Rev.* **43** 33
[49] Wei D and Milenkovic O 2009 *IEEE T. Inform. Theory* **55** 2230
[50] Candes E J and Tao T 2006 *IEEE T. Inform. Theory* **52** 5406
[51] Meng X F, Cai L Z, Wang Y R, Yang X L, Xu X F, Dong G Y, Shen X X, Zhang H and Cheng X C 2006 *Appl. Opt.* **45** 3289
[52] Fan D S, Meng X F, Wang Y R, Yang X L, Peng X, He W Q, Dong G Y and Chen H Y 2013 *Appl. Opt.* **52** 5645
[53] Wu J H, Liao X F and Yang B 2017 *Signal Process.* **141** 109
[54] Zhang D, Liao X F, Yang B and Zhang Y S 2018 *Multimed. Tools Appl.* **77** 2191
[55] Wu J H, Liao X F and Yang B 2018 *Signal Process.* **142** 292
[56] Li B, Liao X F and Jiang Y 2017 *Multimed. Tools Appl.* **77** 8911
[57] Hua W and Liao X F 2017 *Multimed. Tools Appl.* **76** 7087