Compressive optical image encryption using phase-shifting interferometry on a joint transform correlator

Jun Li[*], Bangwen Jia, Xiaofang Dai, Miao Lei, Chanxia Yang,
Jiaosheng Li, Hongbing Li, Rong Li

[1]Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials,
 School of Physics and Telecommunication Engineering, South China Normal University,
 Guangzhou 510006, China

[2]Guangdong Provincial Engineering Research Center for Optoelectronic Instrument,
 School of Physics and Telecommunication Engineering, South China Normal University,
 Guangzhou 510006, China

[*]Corresponding author: lijunc@126.com

A compressive optical image encryption method, which combines compressive sensing with phase-shifting interferometry on a joint transform correlator, is proposed in the fully optical domain. The object image is first permutated using a binary scrambling method. Next, the permutated object field is encrypted and registered as the holograms by phase-shifting interferometry on the joint transform correlator setup. Then, the encrypted images and the key are compressed to the compressed data using single-pixel compressive imaging. The original image can be reconstructed and decrypted using the specified algorithm. The simulations demonstrate that the method is effective and suitable for image security transmission.

Keywords: fully optical system, holographic interferometry, joint transform correlator (JTC), binary scrambling method, inverse problems.

1. Introduction

With the rapid development of computer technology and the Internet, more and more attention has been paid to the information security [1–3]. For the security of image data, many optical image encryption methods have been proposed successively, for instance, multidimensional random phase encoding, coherent diffractive imaging for optical encryption, phase-retrieval algorithms for optical encryption, phase-truncated strategy for optical encryption, sparsity-driven optical information authentication [4–9]. Among these methods, they are mostly based on the Mach–Zehnder interferometer (MZI) architecture, and generally require accurate alignment due to the use of the

random phase masks. Even one pixel error in the alignment would result in failed reconstruction [10–12]. But the encryption methods based on a joint transform correlator (JTC) architecture can overcome the alignment drawbacks perfectly [13–18].

The large volume of data required for storing or transmitting holograms has been a main limiting factor of the above optical image security. For solving the problem, many hologram compression schemes have been reported in recent years [19, 20]. But their effectiveness is limited by the introduction of laser speckle, and the realization of hologram compression is typically performed using electronic means. The newly developed theory of compressive sensing (CS) [21, 22] provides a new technical approach for hologram compression in the fully optical domain [23–27]. Some optical image encryption methods based on CS have been proposed recently [28–36]. However, these methods are mostly related to the image compression with CS via electronic means, and all relate to image encryption methods based on compressive sensing using the MZI architecture, but the optical image encryption based on compressive sensing using a JTC architecture has not been discussed.

This paper first proposes a compressive optical image encryption method on a JTC architecture, which combines the single-pixel compressive imaging with phase-shifting interferometry on a JTC architecture. First, the original image is permutated using the binary scrambling method. Next, the permutated object field and the decrypting key are registered as holograms using three-step phase-shifting interferometry (PSI) on a JTC architecture. Then, the encrypted image and the key are compressed to a much less volume signal utilizing the sparsity of the signal using single-pixel compressive imaging. At the receiving terminal, the encrypted image and the decrypted key are achieved from small amounts of data record by a photodiode using an optimization process, and the original image can be decrypted with the reconstructed holograms and the correct keys. This method not only has the advantage of the high accuracy for spatial arrangement of the optics elements, but also can perform optical image encryption and optical image compression in the fully optical domain. Therefore, it is effective and suitable for secure optical image transmission in future all-optical networks. Moreover, our method utilizes the sparsity of a signal to reconstruct a complete signal from a small sample to overcome the limitation of the large hologram data volumes of 3D images or 3D television, and real-time transmission of encrypted information. The principles and numerical simulations are described below.

2. Fundamental principles

The compressive optical image encryption system is illustrated in Fig. 1, where a linearly polarized laser beam is expended and collimated, and then illuminates a spatial light modulator (SLM). The object image $f(x, y)$ is permutated using the binary scrambling method firstly. The steps of permutation are as follows. Make the logic operation of XOR between the scrambling keys (key_1 and key_2) and coordinates of each pixel address of
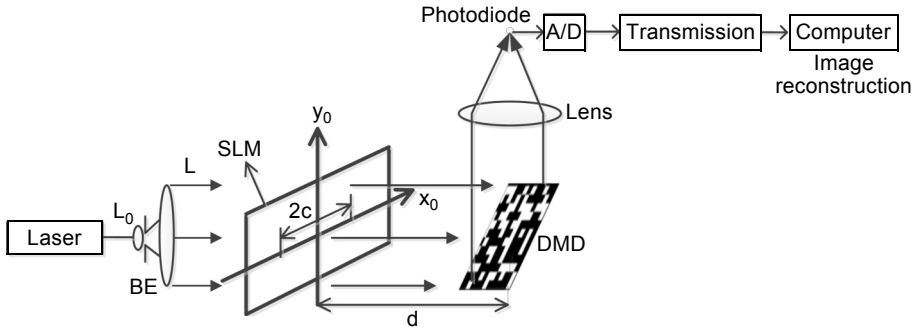
Fig. 1. Setup of compressive optical image encryption system; DMD – digital micro-mirror device, SLM – spatial light modulator, BE – beam expander, L – light.

the image, that is $f(x, y) \rightarrow f_0(x \oplus \text{key}_1, y \oplus \text{key}_2) \rightarrow f_0(x_0, y_0)$, where $\oplus$ denotes the operation of XOR; (x, y) and (x_0, y_0) denote location coordinates of the object image and permutated image, respectively.

Under the control of the computer, the SLM displays the permutated image $f_0(x_0, y_0)$ and the random phase mask (RPM) $n_1(x_0, y_0)$ on its right half and the other RPM $n_2(x_0, y_0)$ on its left half. So the right and the left half waves passing through the SLM respectively correspond to the object wave and the reference wave in the PSI. Then the two waves overlap to form the interferogram on a digital micro-mirror device (DMD) plane. The compressive sampling data are obtained by computing random linear measurements of the interferogram I_H and the measurement matrix Φ on the DMD plane and then collected by a highly sensitive photodiode. Finally we can acquire the compressed hologram image by a traditional communication channel and then retrieve it via the specific algorithm. And the object image can be decrypted via an inverse Fresnel transformation with six reconstructed holograms and the correct keys.

Suppose that the permutated image $f_0(x_0, y_0)$ has been normalized into the range of [0, 1/2], and $n_1(x_0, y_0)$ and $n_2(x_0, y_0)$ are two independent and random white noises uniformly distributed in [0, 1]. The distance between the centers of the object scene and the reference scene is $2c$, the wavelength of the input plane wave is λ, and the diffraction distance is d. In combination with the adequate state of light polarization, the SLM can reach a phase modulation 2π. The object wave and the reference wave on the back side of SLM can be described respectively as

$$o(x_0 - c, y_0) = \exp\left[i2\pi f_0(x_0 - c, y_0)\right]\exp\left[i2\pi n_1(x_0 - c, y_0)\right] \tag{1}$$

$$r(x_0 + c, y_0) = \exp\left[i2\pi n_2(x_0 + c, y_0)\right] \tag{2}$$

where $o(x_0 - c, y_0)$ denotes the object wave, and $r(x_0 + c, y_0)$ denotes the reference wave on the input plane.

After being Fresnel diffraction, the two complex waves on the DMD plane become

$$O(x, y) = \mathrm{FR}_d\left[o(x_0 - c, y_0)\right] = A_0 \exp\left[i\varphi_0(x, y)\right] \tag{3}$$

$$R(x, y) = \mathrm{FR}_d\left[r(x_0 + c, y_0)\right] = A_r \exp\left[i\varphi_r(x, y)\right] \tag{4}$$

where FR_d represents Fresnel diffraction of the distance d; $O(x, y)$ and $R(x, y)$ respectively represent the diffracted fields of the object wave $o(x_0 - c, y_0)$ and the reference wave $r(x_0 + c, y_0)$ on the DMD; A_0, A_r, φ_0, φ_r denote amplitude and phase of the object wave and the reference wave on the DMD plane, respectively.

Using standard three-step PSI on the JTC with phase shifting angles of 0, $\pi/2$ and π, then the three interferograms I_{H1}, I_{H2}, and I_{H3} on the DMD plane are sampled sequentially and expressed as

$$I_{H1}(x, y) = A_0^2 + A_r^2 + 2A_0 A_r \cos\left[\varphi_0(x, y) - \varphi_r(x, y) + 2cx\right] \tag{5}$$

$$I_{H2}(x, y) = A_0^2 + A_r^2 + 2A_0 A_r \cos\left[\varphi_0(x, y) - \varphi_r(x, y) + 2cx + \frac{\pi}{2}\right] \tag{6}$$

$$I_{H3}(x, y) = A_0^2 + A_r^2 + 2A_0 A_r \cos\left[\varphi_0(x, y) - \varphi_r(x, y) + 2cx + \pi\right] \tag{7}$$

A DMD consists of millions of micro-mirrors and works by controlling the reflection of each individual pixel on the display. The mirrors on the DMD were in a certain pseudo-random condition according to the restricted isometry property (RIP) [37] in CS theory. With the help of pseudo-random number generator (RNG), randomly selected mirrors of DMD are oriented in a direction towards the lens (a "1"), while the rest are oriented in a different direction (a "0"). Then the light reflected by the mirrors in direction towards the lens is summed at the photodiode to compute the measurement as its output voltage

$$Y(m) = \{y_{1m}, y_{2m}, y_{3m}\} = \varphi_m\left[I_{H1}, I_{H2}, I_{H3}\right] \tag{8}$$

here φ_m is the m-th pseudo-random matrix on the DMD plane $m \in \{1, 2, \ldots, M\}$. Once we repeat the process M times, we can obtain the full measurements Y of the compressive sampling

$$Y = [y_1, y_2, y_3] = \psi\left[I_{H1}, I_{H2}, I_{H3}\right] \tag{9}$$

where

$$\left[I_{H1}, I_{H2}, I_{H3}\right] = \begin{bmatrix} I_{H11} & I_{H21} & I_{H31} \\ I_{H12} & I_{H22} & I_{H32} \\ \vdots & \vdots & \vdots \\ I_{H1M} & I_{H2M} & I_{H3M} \end{bmatrix}$$

and I_{H1M} represents the hologram I_{H1} in the *M*-th measurement; $\psi \in R^{M \times \sqrt{N} \times \sqrt{N}}$ is the measurement matrixes uploaded into the DMD device; $Y \in R^{M \times 3}$ is the measurement data on the photodiode; and $y_k \in R^{M \times 1}$, $I_{Hk} \in R^{\sqrt{N} \times \sqrt{N} \times 1}$, where $k = 1, 2, 3$.

We convert the optical signal to digital signal using a photodiode and transmit it using a conventional channel to the computer where the image reconstruction and decryption will be performed. We first adopt a two-step iterative shrinkage (TwIST) [38] algorithm to reconstruct the interference wave intensity $\hat{I}_{Hk}$ by solving the optimal problem below:

$$\min_{I_{Hk}} \frac{\mu}{2} \left\| Y_k - \Psi \hat{I}_{Hk} \right\|_2^2 + \mathrm{TV}(\hat{I}_{Hk}), \quad \text{s.t. } Y_k = \Psi I_{Hk} \tag{10}$$

where $\left\| Y_k - \Psi \hat{I}_{Hk} \right\|_2^2$ is the l_2 norm of $Y_k - \Psi \hat{I}_{Hk}$, and μ is a constant. The first penalty is a least-squares term that is small when $\hat{I}_{Hk}$ is consistent with the correlation vector Y_k. The second penalty $\mathrm{TV}(\hat{I}_{Hk})$ is the signal's total variation,

$$\mathrm{TV}(\hat{I}_{Hk}) = \sum_{i,j} \sqrt{(\hat{I}_{Hk_{i+1,j}} - \hat{I}_{Hk_{i,j}})^2 + (\hat{I}_{Hk_{i,j+1}} - \hat{I}_{Hk_{i,j}})^2} \tag{11}$$

where the indices *i* and *j* run over all pairs of the adjacent pixels in $\hat{I}_{Hk}$. Due to the non-differentiability of the Euclidean norm at the origin, we will take an approximated TV as:

$$\mathrm{TV}(\hat{I}_{Hk}) = \sum_{i,j} \sqrt{(\hat{I}_{Hk_{i+1,j}} - \hat{I}_{Hk_{i,j}})^2 + (\hat{I}_{Hk_{i,j+1}} - \hat{I}_{Hk_{i,j}})^2 + \xi^2} \tag{12}$$

where ξ is a small positive parameter. Apart from the consideration of sparsity and fidelity for a given reconstruction, TV regularization preserves edges of the recovered image while suppressing any spurious high-frequency components. After setting up the cost function, fixed-point iteration is employed to extract a solution for the problem.

When the intensity patterns $\hat{I}_{H1}$, $\hat{I}_{H2}$, $\hat{I}_{H3}$ are reconstructed with the TwIST algorithm, we can calculate the complex amplitude on the DMD plane

$$O_e(x, y) = \frac{\hat{I}_{H1} - \hat{I}_{H3} + i(2\hat{I}_{H2} - \hat{I}_{H1} - \hat{I}_{H3})}{4} \tag{13}$$

In order to decrypt $O(x, y)$, we must obtain the principle key $R'(x, y)$ which is taken from the diffracted field $R(x, y)$ with a phase deviation. The method of the principle key encryption is basically same as the method of the permutated image. So we carry out three-step PSI process again, but now the RPM $n_2(x, y)$ is displayed on the left half of the SLM, zero on its right half. Next, the wave diffracted by the object, on the DMD plane, becomes a plane wave represented as $C(x, y) = \exp(i\varphi_c)$, where φ_c is constant. Then, through the CS, we can get the intensity patterns $\hat{I}'_{Hk}$ ($k = 1, 2, 3$). So we can calculate the complex amplitude on the DMD plane

$$R'(x, y) = A_r \exp\left[i(\varphi_c - \varphi_r + 2cx) \right] = \frac{\hat{I}'_{H1} - \hat{I}'_{H3} + i(2\hat{I}'_{H2} - \hat{I}'_{H1} - \hat{I}'_{H3})}{4} \tag{14}$$

Further we obtain $O'(x, y)$, which represents the product of the object wave $O_e(x, y)$ and a constant phase term, by

$$O'(x, y) = \frac{O_e(x, y)}{R'(x, y)} = A_0 \exp\left[i(\varphi_0(x, y) - \varphi_c)\right] \tag{15}$$

Then, the object wave $o(x_0 - c, y_0)$ can be reconstructed from

$$o(x_0 - c, y_0) = \text{IFR}_d\left[O'(x, y)\right] \tag{16}$$

where IFR_d stands for the inverse Fresnel transform of the distance d. Finally, after multiplying $o(x_0 - c, y_0)$ by $\exp[-i2\pi n_1(x_0, y_0)]$ and extracting the phase of the result and dividing it by π, we can obtain the permutated image $f_0(x_0, y_0)$. Finally, we can get the original image $f(x, y)$ by using the binary scrambling method again.

Once $\hat{I}_{Hk}$ and $\hat{I}'_{Hk}$ are known, in addition to the scrambling keys of decryption (key$_1$ and key$_2$), λ, d and random mask $n_1(x_0, y_0)$, we can digitally or optically retrieve the original object image from the encrypted image.

3. Computer simulations and analysis

A series of simulations have been carried out to investigate the effectiveness of our proposed method. This section presents a series of results based on the following conditions. The original object image used in the simulation is shown in Fig. 2**a**. The pa-
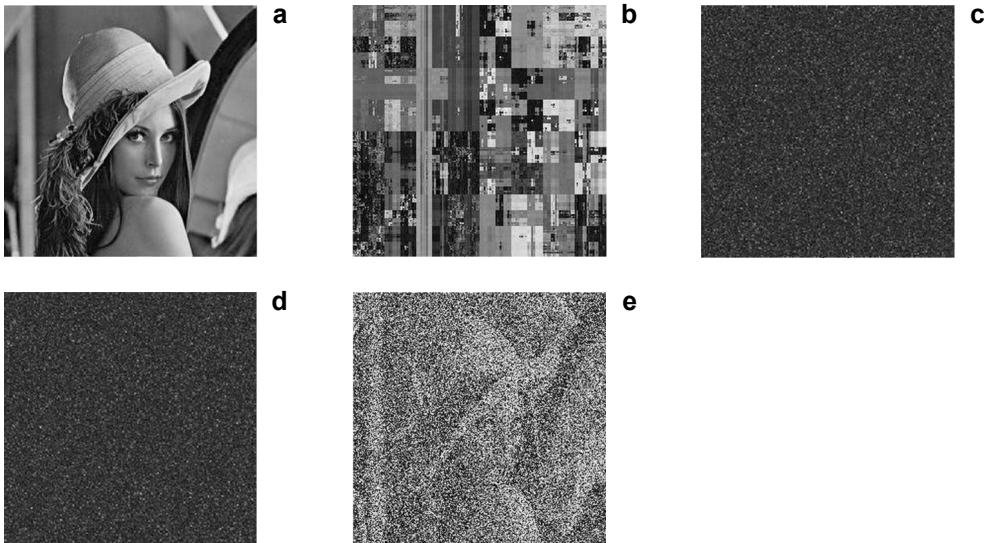

Fig. 2. Computer simulation results with a grayscale image. Grayscale image (**a**), the permutated image (**b**), one of the encrypted holograms of the object on DMD plane (**c**), one of the holograms of the key on DMD plane (**d**), and retrieved image from $256 \times 256 \times 51.8\%$ measurements using our method (**e**).

rameters used in these simulations are $\lambda = 632.8$ nm and $d = 0.5$ m. All the frames are digitized to 256 gray levels with the size of 256×256 pixels, $key_1 = key_2 = 85$. We took $256 \times 256 \times 51.8\%$ measurements from the encrypted image in our compressive optical image encryption system. The intensity values of the complex amplitude field containing encrypted object information are first modulated by the DMD. Then, once we received the compressed data of the encrypted image in the photodiode detector, we can reconstruct the original image from the compressed and encrypted image using the correct keys and the parameters of the optical system. The simulation results for the compressive optical image encryption on a JTC interferometer are shown in Fig. 2. After performing compressive optical image encryption on the object image, the three encrypted interferograms containing the secret image information on the DMD plane will be sampled with compressive sensing theory. Figure 2**a** is the original image, Fig. 2**b** is the permutated image, one of these interferograms of the object image and the key are shown in Figs. 2**c** and 2**d**, respectively, Fig. 2**e** shows the recovered object image from $256 \times 256 \times 51.8\%$ measurements using our method. The computer simulations show that this compressive optical image encryption method is performed using optical scheme in the Fresnel domain.

An excellent encryption system should be robust to block all forms of cryptanalysis, statistic, and unlawful attacks. In order to demonstrate that the proposed encryption system is secured against a variety of illegal attacks, we will make detailed security analyses such as key space analysis and sensitivity analysis, statistical analysis with respect to the key and original image [25, 39].

3.1. Key space analysis and sensitivity analysis

Key space is one way of measuring encryption algorithm safety. We has used the principal key $n_2(x_0, y_0)$, the scrambling key and additional keys, such as wavelength λ, diffraction distance d, measurement matrix Φ and so on. Due to the sensitivity of control parameters and initial conditions of the system, even though the secret-key has a tiny change, it should result in very different scrambling index matrix.

To further investigate the security of this compressive optical image encryption method, we reconstruct the original grayscale image with $256 \times 256 \times 51.8\%$ measurements when one of the keys is incorrect as shown in Fig. 3. Once one of the keys is incorrect, the retrieved image will be greatly affected. Among these keys, the principal key $n_2(x_0, y_0)$ plays a critical role in the security system, as was shown in Fig. 3**a**, in which the retrieved image is the same as the noise and fully unrecognizable when the principal key is not used; when the scrambling keys are not used or the scrambling keys are incorrect, the reconstruction images are as shown in Figs. 3**b** and 3**c**; when the diffraction distance of the object image and the wavelength of the He-Ne laser exhibit a relative error, there are no correct reconstruction images as shown in Figs. 3**d** and 3**e**; when $n_1(x_0, y_0)$ is not eliminated, the reconstruction image is as shown in Fig. 3**f**; when the measurement matrix Φ is incorrect, the reconstruction image is as shown in Fig. 3**g**.

Moreover, we introduced compressive sensing in the encryption system, the encrypted images and the keys are compressed to the compressed data using single-pixel com-
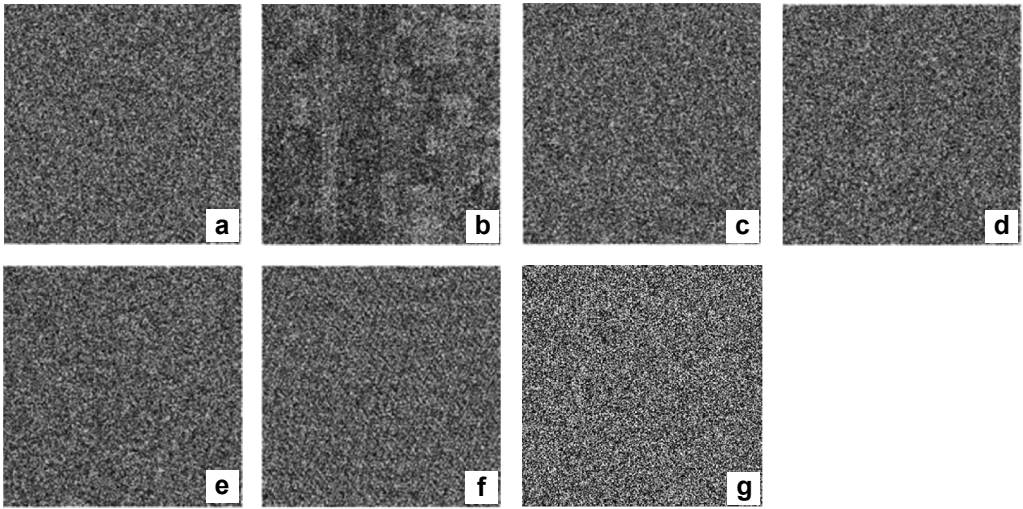
Fig. 3. Retrieved images with one incorrect key in the decryption process: when the principal key $n_2(x_0, y_0)$ is not used (**a**), when the scrambling key is not used (**b**), when the scrambling keys are incorrect (**c**), when d is erroneous (**d**), when λ is erroneous (**e**), when $n_1(x_0, y_0)$ is not eliminated (**f**), and when the measurement matrix Φ is incorrect (**g**).
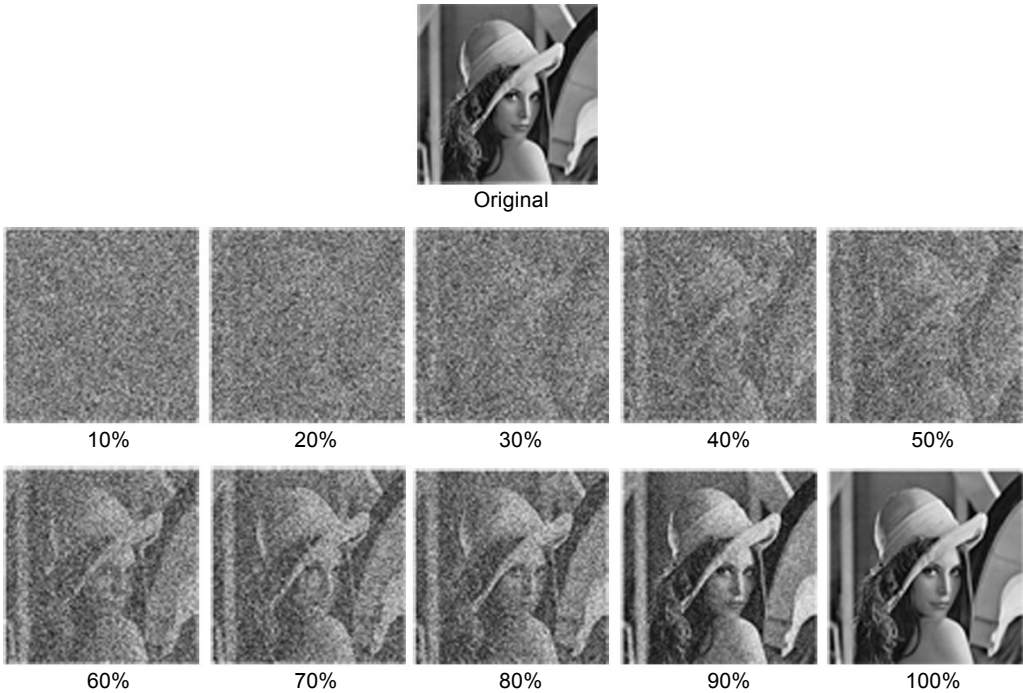

Original

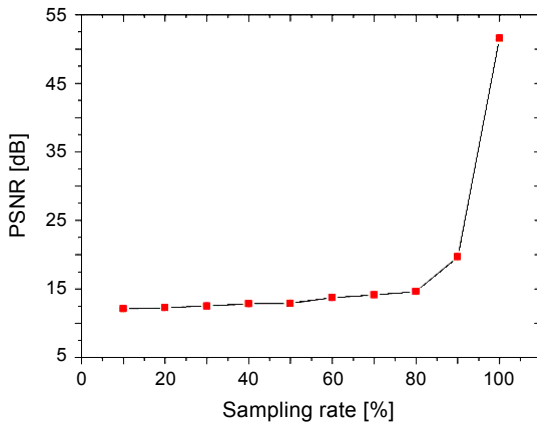Fig. 4. Reconstructed images from partially recovered keys.

Fig. 5. PSNR between the original image and reconstructions *versus* the sampling rate.

pressive imaging, which converted two-dimensional data into one-dimensional data. We first adopt a two-step iterative shrinkage (TwIST) algorithm to reconstruct the interference wave intensity by solving the optimal problem under additive white Gaussian noise in the system. If we use different sampling rates, the retrieved image will be greatly affected. Once the measuring matrix is incorrect, we will never acquire the correct retrieved image. This proves that the system's security is improved with the addition key space of the measurement matrix.

We compared the reconstructed images at different sampling rates from 10% to 100% with an increase rate of 10%. The detailed reconstructed results in the simulation are shown in Fig. 4. As can be seen from the figure, we can clearly see contents of the image when the sampling rate is greater than 50%. The simulation results show that our proposed JTC-based compressive optical image encryption is feasible. The relations of the sampling rate in the compressive sampling process and the peak signal-to-noise ratio (PSNR) between the original image and the reconstructions are shown in Fig. 5. The PSNRs increase with the increase of a sampling rate. When the sampling rate reaches 51.8%, the PSNR is close to or greater than 13 dB.

3.2. Statistical analysis

A histogram test is carried out and shown to demonstrate the effectiveness of the system. Since the image histogram shows how pixels of the image are distributed along a gray-intensity scale, the difference between the histogram of the original image and the ciphered image is that the original image is distributed unevenly, as it is shown in Fig. 6. However, the histogram of the ciphered image is nearly uniformly distributed and is significantly different from the original image. In addition, when we use another image, the distribution of the encrypted image will also be changed. So, the system can protect the information of the image to withstand the statistical attack well.
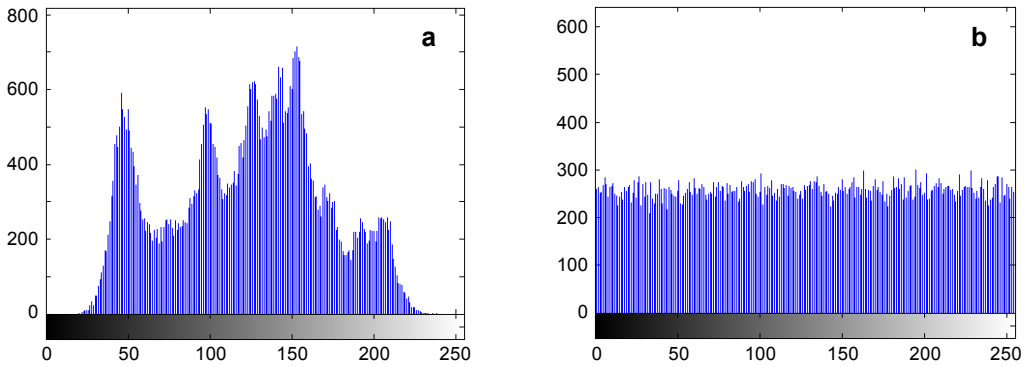
Fig. 6. Histogram of the original image (**a**) and of the encrypted image (**b**).

We have also made some simulations with other images and obtained satisfactory retrieval results, which are similar to those obtained with the use of grayscale images. So they are ignored here.

4. Conclusions

In the fully optical domain, a compressive optical image encryption method combining compressive sensing with phase-shifting interferometry on a JTC architecture has been proposed. The simulations show that the method can be used to reconstruct the original image well with fewer measurement data and can be applied to grayscale images and binary images to perform image encryption and compression in an all-optical system. So the method presents an effective scheme to overcome the limitations of the large holograms data volume for current optical image encryption systems and its simple JTC architecture overcomes the alignments drawbacks existing in the systems based on MZI architecture. In addition, the DMD used in the setup of the compressive optical image encryption can perform high-speed measurements, and the measurement patterns are loaded into the DMD at speeds up to 31.5 kHz. Therefore, it is expected to be widely used for 3D object encryption, video secure transmission, real-time video encryption technology and future all-optical networks, such as real-time video security transmissions and naked-eye 3D television.

References

[1] MATOBA O., NOMURA T., PEREZ-CABRE E., MILLAN M.S., JAVIDI B., *Optical techniques for information security*, Proceedings of the IEEE **97**(6), 2009, pp. 1128–1148.
[2] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.

[3] Cox I.J., Kilian J., Leighton F.T., Shamoon T., *Secure spread spectrum watermarking for multimedia*, IEEE Transactions on Image Processing **6**(12), 1997, pp. 1673–1687.

[4] Wen Chen, Javidi B., Xudong Chen, *Advances in optical security systems*, Advances in Optics and Photonics **6**(2), 2014, pp. 120–155.

[5] Wen Chen, Xudong Chen, Sheppard C.J.R., *Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain*, Optics Express **20**(4), 2012, pp. 3853–3865.

[6] Wenqi He, Xiang Peng, Xiangfeng Meng, Xiaoli Liu, *Optical hierarchical authentication based on interference and hash function*, Applied Optics **51**(32), 2012, pp. 7750–7757.

[7] Jun Li, Jiaosheng Li, Yangyang Pan, Rong Li, *Optical image hiding with a modified Mach–Zehnder interferometer*, Optics and Lasers in Engineering **55**, 2014, pp. 258–261.

[8] Wen Chen, Xudong Chen, *Security-enhanced interference-based optical image encryption*, Optics Communications **286**, 2013, pp. 123–129.

[9] Rajput S.K., Nishchal N.K., *Image encryption based on interference that uses fractional Fourier domain asymmetric keys*, Applied Optics **51**(10), 2012, pp. 1446–1452.

[10] Jun Li, Jiaosheng Li, Lina Shen, Yangyang Pan, Rong Li, *Optical image encryption and hiding based on a modified Mach–Zehnder interferometer*, Optics Express **22**(4), 2014, pp. 4849–4860.

[11] Chao Lin, Xueju Shen, Qinzu Xu, *Optical image encoding based on digital holographic recording on polarization state of vector wave*, Applied Optics **52**(28), 2013, pp. 6931–6939.

[12] Seok-Hee Jeon, Sang-Keun Gil, *2-step phase-shifting digital holographic optical encryption and error analysis*, Journal of the Optical Society of Korea **15**(3), 2011, pp. 244–251.

[13] Nomura T., Javidi B., *Optical encryption using a joint transform correlator architecture*, Optical Engineering **39**(8), 2000, pp. 2031–2035.

[14] La Mela C., Iemmi C., *Optical encryption using phase-shifting interferometry in a joint transform correlator*, Optics Letters **31**(17), 2006, pp. 2562–2564.

[15] Barrera J.F., Vargas C., Tebaldi M., Torroba R., Bolognini N., *Known-plaintext attack on a joint transform correlator encrypting system*, Optics Letters **35**(21), 2010, pp. 3553–3555.

[16] Jun Li, Tao Zheng, Qing-zhi Liu, Rong Li, *Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography*, Optics Communications **285**(7), 2012, pp. 1704–1709.

[17] Lina Shen, Jun Li, Hongsen Chang, *Double-image encryption based on joint transform correlation and phase-shifting interferometry*, Chinese Optics Letters **5**(12), 2007, pp. 687–689.

[18] Rueda E., Ríos C., Barrera J.F., Torroba R., *Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture*, Applied Optics **51**(11), 2012, pp. 1822–1827.

[19] Patten R.F., Hennelly B.M., Kelly D.P., O'Neill F.T., Ying Liu, Sheridan J.T., *Speckle photography: mixed domain fractional Fourier motion detection*, Optics Letters **31**(1), 2006, pp. 32–34.

[20] Frauel Y., Naughton T.J., Matoba O., Tajahuerce E., Javidi B., *Three-dimensional imaging and processing using computational holographic imaging*, Proceedings of the IEEE **94**(3), 2006, pp. 636–653.

[21] Donoho D.L., *Compressed sensing*, IEEE Transactions on Information Theory **52**(4), 2006, pp. 1289–1306.

[22] Rivenson Y., Stern A., Javidi B., *Overview of compressive sensing techniques applied in holography*, Applied Optics **52**(1), 2013, pp. A423–A432.

[23] Clemente P., Durán V., Tajahuerce E., Andrés P., Climent V., Lancis J., *Compressive holography with a single-pixel detector*, Optics Letters **38**(14), 2013, pp. 2524–2527.

[24] Jun Li, Yaqing Li, Yuping Wang, Ke Li, Rong Li, Jiaosheng Li, Yangyang Pan, *Two-step holographic imaging method based on single-pixel compressive imaging*, Journal of the Optical Society of Korea **18**(2), 2014, pp. 146–150.

[25] Jun Li, Jiao Sheng Li, Yang Yang Pan, Rong Li, *Compressive optical image encryption*, Scientific Reports **5**, 2015, p. 10374.

[26] Takhar D., Laska J.N., Wakin M.B., Duarte M.E., Baron D., Sarvotham S., Kelly K.F., Baraniuk R.G., *A new compressive imaging camera architecture using optical-domain compression*, Proceedings of SPIE **6065**, 2006, article ID 606509.

[27] Alfalou A., Brosseau C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009, pp. 589–636.

[28] 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.

[29] Huang R., Rhee K.H., Uchida S., *A parallel image encryption method based on compressive sensing*, Multimedia Tools and Applications **72**(1), 2014, pp. 71–93.

[30] Xingbin Liu, Wenbo Mei, Huiqian Du, *Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain*, Journal of Modern Optics **61**(19), 2014, pp. 1570–1577.

[31] Xiaoyong Liu, Yiping Cao, Pei Lu, Xi Lu, Yang Li, *Optical image encryption technique based on compressed sensing and Arnold transformation*, Optik – International Journal for Light and Electron Optics **124**(24), 2013, pp. 6590–6593.

[32] Jun Li, Hongbing Li, Jiaosheng Li, Yangyang Pan, Rong Li, *Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography*, Optics Communications **344**, 2015, pp. 166–171.

[33] Alfalou A., Brosseau C., Abdallah N., Jridi M., *Simultaneous fusion, compression, and encryption of multiple images*, Optics Express **19**(24), 2011, pp. 24023–24029.

[34] Alfalou A., Brosseau C., *Implementing compression and encryption of phase-shifting digital holograms for three-dimensional object reconstruction*, Optics Communications **307**, 2013, pp. 67–72.

[35] 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.

[36] Alfalou A., Brosseau C., *Dual encryption scheme of images using polarized light*, Optics Letters **35**(13), 2010, pp. 2185–2187.

[37] Candès E. J., *The restricted isometry property and its implications for compressed sensing*, Comptes Rendus Mathematique **346**(9–10), 2008, pp. 589–592.

[38] Bioucas-Dias J.M., Figueiredo M.A.T., *A new TwIST: two-step iterative shrinkage/thresholding algorithms for image restoration*, IEEE Transactions on Image Processing **16**(12), 2007, pp. 2992–3004.

[39] Jun Li, Ting Zhong, Meixia Jiang, Bo Dai, Rong Li, *Digital camera with image encryption*, Optik – International Journal for Light and Electron Optics **127**(3), 2016, pp. 1391–1394.