SCIENTIFIC REPORTS

OPEN

Compressive Optical Image Encryption

Jun Li, Jiao Sheng Li, Yang Yang Pan & Rong Li

Received: 29 October 2014
Accepted: 10 April 2015
Published: 20 May 2015

An optical image encryption technique based on compressive sensing using fully optical means has been proposed. An object image is first encrypted to a white-sense stationary noise pattern using a double random phase encoding (DRPE) method in a Mach-Zehnder interferometer. Then, the encrypted image is highly compressed to a signal using single-pixel compressive holographic imaging in the optical domain. At the receiving terminal, the encrypted image is reconstructed well via compressive sensing theory, and the original image can be decrypted with three reconstructed holograms and the correct keys. The numerical simulations show that the method is effective and suitable for optical image security transmission in future all-optical networks because of the ability of completely optical implementation and substantially smaller hologram data volume.

With the increased importance of information security, image security has become increasingly important in many current application areas[1]. The study of image security includes image encryption, image hiding and image watermarking[2–5]. Image encryption technology has been widely applied to many application areas, such as 3D image encryption, data monitoring, data tracking and confidential data transmission in the military and medical fields[6], quantum-secured imaging[7], and quantum-secured surveillance[8]. In recent years, image security that fully utilises optical parallel features has become an important research topic[9–11]; we also have demonstrated the feasibility of optical image hiding and optical image encryption and hiding[12,13] These methods may be effective solutions to the future implementation of all-optical systems[14].

However, the large volume of data required for storing or transmitting holograms has been a main limiting factor of optical image security. Many hologram compression schemes have been reported in recent years to solve this problem[15,16]; however, their effectiveness is limited by the introduction of hologram laser speckling[17], and the realisation of hologram compression is typically performed using electronic means. The newly developed theory of compressive sensing (CS)[18–21] provides a new technical approach for hologram compression in the optical domain[22–24] and captures the non-adaptive linear projections of compressible signals at a rate that is significantly below the Nyquist rate. These signals are then reconstructed from these projections using an optimisation process. Simultaneously, CS is combined with other special imaging methods to obtain wider application, such as in quantum imaging[25,26], photon counting imaging[27], the coherent imaging of different wavelengths[28], and the measurement of electric fields[29,30]. These features may also be effective solutions for the massive data processing and information security requirements of the Internet of Things (IoT)[31]. Recently, various image encryption methods based on compressive sensing, such as parallel image encryption[32], image encryption with an Arnold transform[33–35] and colour image encryption[36], have been proposed. However, these methods relate to digital image encryption; completely optical schemes for image encryption based on compressive sensing have not been discussed.

This paper proposes a completely optical image encryption method based on compressive sensing. Using a Mach-Zehnder interferometer, an object image is first encrypted to a white-sense stationary noise pattern using a DRPE[37] method in the object beam path. Then, the encrypted image is highly compressed to a signal utilising the sparsity of the signal in a sparse domain. At the receiving terminal, the encrypted image reconstruction is achieved from small amounts of data by an optimisation

Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou 510006, China. Correspondence and requests for materials should be addressed to J.L. (email: lijunc @126.com)

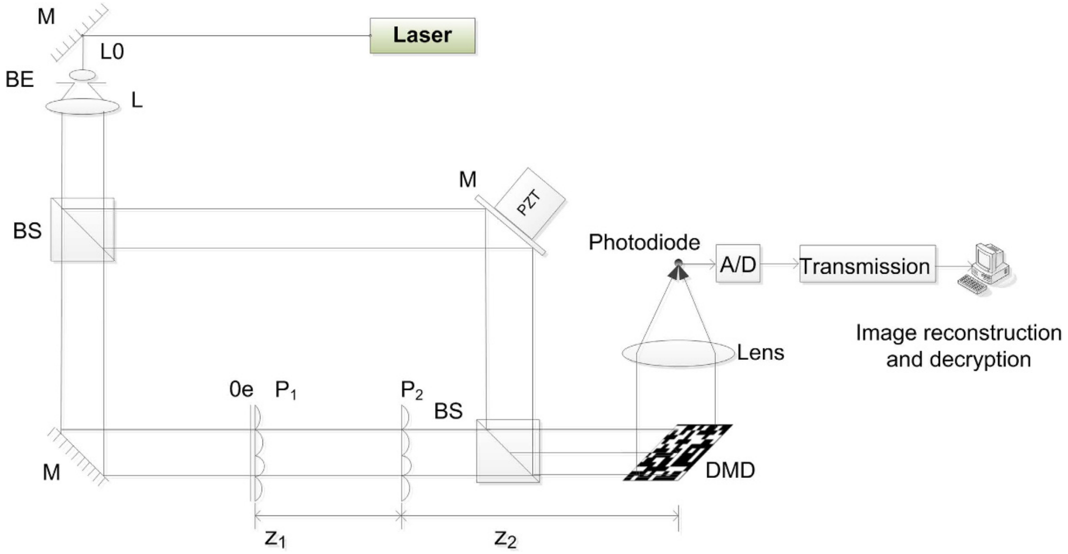

Figure 1. Setup of compressive optical image encryption. BE, beam expander; L, lens; BS, beam splitter; M, mirror; P, random phase plate; PZT, piezoelectric transducer mirror; Oe, object image.

process, and the original image can be decrypted with three reconstructed holograms and the correct keys. The method can be used to perform compressive optical image encryption in a purely optical system; therefore, it is effective and suitable for secure optical image transmission in future all-optical networks. Moreover, our method utilises 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 3DTV. In addition, our method can overcome the limitations of the precision and costs of traditional sensors, wavelengths and resolution for array imaging based on CS. The principles and numerical simulations are described below.

Methods

The compressive optical image encryption system is shown in Fig. 1. A laser beam is split into an object beam and a reference beam. The object beam first illuminates an object image that is used for encryption and subsequently passes through two random phase masks P_1 and P_2 to perform the encryption using the DRPE method. In the other arm, the reference beam illuminates the piezoelectric transducer mirror (PZT), which is capable of phase shifting. Then, the two waves overlap to form an interference pattern in the plane of a Digital Micromirror Device (DMD). The DMD, a semiconductor-based "light switch" array of millions of individually addressable, tiltable mirror-pixels, is a reflective spatial light modulator. Each tiltable mirror-pixel can be rotated $+12$ or -12 degrees from the horizontal to reflect light to or away from an intended target. When the mirror-pixel is in the $+12$ degree state, more than 88% of the reflected energy can be coupled to the target[38]. Then, the compressive sampling data are obtained by the photodiode detector with the modulation of the encrypted complex light field by the DMD device. Finally, we can acquire the compressed hologram image by a traditional communication channel and subsequently reconstruct it via the specific algorithm. In addition, the original object can be decrypted via an inverse Fresnel transformation with three reconstructed holograms and the correct keys.

Let us assume that the reference wave is simply given by the real amplitude R, and a complex object field in the plane P_1 is $U_0(x_0, y_0)$. The complex amplitude transmittances of the random phase plates P_1 and P_2 are $\exp\left[i2\pi \cdot p\left(x_0, y_0\right)\right]$ and $\exp\left[i2\pi \cdot q\left(x_0, y_0\right)\right]$, respectively, where $p\left(x_0, y_0\right)$ and $q\left(x_0, y_0\right)$ are two independent white noises uniformly distributed in[0, 1]. The distance between plates P_1 and P_2 is z_1 , and that between P_2 and DMD is z_2. The complex object field $U\left(x, y\right)$ on the DMD plane can be described as

$$U\left(x, y\right) = FR_{Z_2}\left\{FR_{Z_1}\left\{U_0(x_0, y_0)\exp\left[i2\pi \cdot p\left(x_0, y_0\right)\right]\right\} \times \exp\left[i2\pi \cdot q\left(x_0, x_0\right)\right]\right\}, \tag{1}$$

where FR_Z denotes the Fresnel transform of the distance z. Based on traditional three-step, phase-shifting holography, the phases of the reference wave can be modulated by PZT to 0, $\frac{\pi}{2}$ and π. Then, the three interference intensities of the complex amplitude field on the DMD plane are expressed as

$$I_1(x, y; 0) = \left|R + U\left(x, y\right)\right|^2 = I_0(x, y) + 2\,\mathrm{Re}\left[U\left(x, y\right)\right] \cdot R, \tag{2}$$

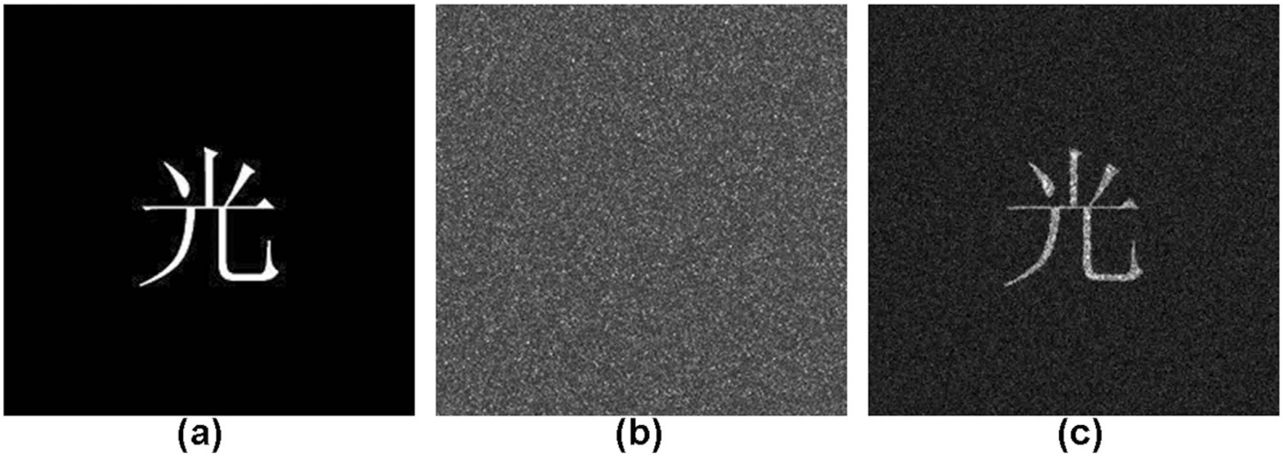

Figure 2. Simulation results with a binary image. (**a**) Binary image; (**b**) one of the encrypted holograms on the DMD plane; (**c**) retrieved image from 256 × 256 × 18.7% measurements using our method.

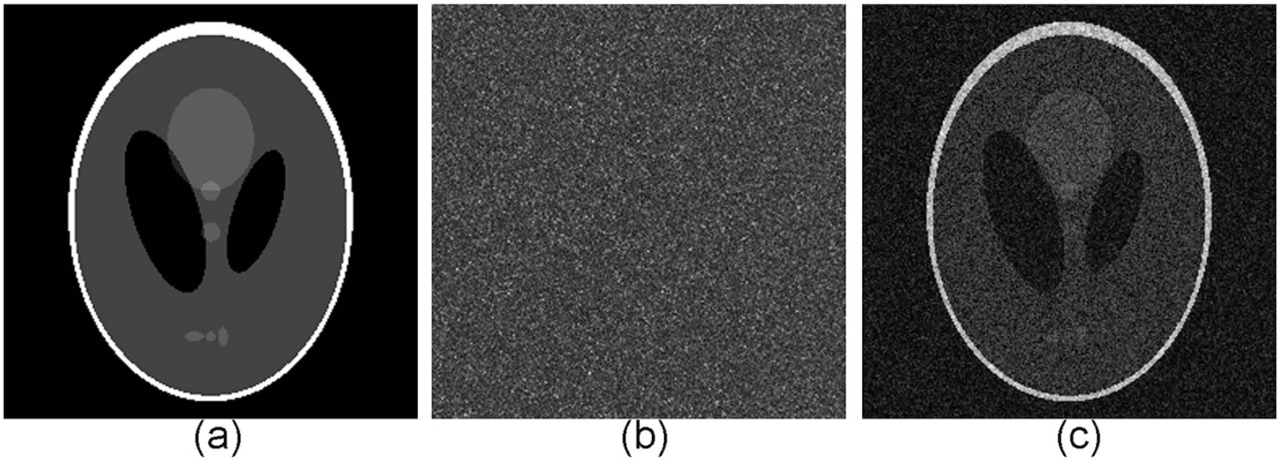

Figure 3. Simulation results with a gray-level image. (**a**) Gray-level image; (**b**) one of the encrypted holograms on the DMD plane; (**c**) retrieved image from 256 × 256 × 42.1% measurements using our method.

$$I_2(x, y; \frac{\pi}{2}) = \left|R \cdot \exp(i \cdot \frac{\pi}{2}) + U(x, y)\right|^2 = I_0(x, y) + 2\mathrm{Im}\left[U(x, y)\right] \cdot R, \tag{3}$$

$$I_3(x, y; \pi) = |R \cdot \exp(i \cdot \pi) + U(x, y)|^2 = I_0(x, y) - 2\,\mathrm{Re}[U(x, y)] \cdot R, \tag{4}$$

where $I_0(x, y) = R^2 + |U(x, y)|^2$ When the complex amplitude field on the DMD plane is modulated by the DMD device and coupled to the photodiode detector via a lens, we can obtain compressive sampling data of the three encrypted interference patterns on the photodiode. Specifically, the final output value on the photodiode detector can be calculated by computing the inner product of the intensity value I of the complex amplitude field and the measurement matrix Φ loaded into the DMD device. When we repeat the process M times, we can obtain the full measurements Y of the compressive sampling. For example, we obtain the measurement data Y_1 through M computations of random linear measurements of intensity I_1 and the measurement matrix Φ in the DMD device. The processing can be expressed as follows:

$$Y_k = \Phi \cdot I_k,\ k = 1, 2, 3, \tag{5}$$

where $Y_k \in R^{M\times 1}$ is the measurement data obtained in the single-pixel detector, $\Phi \in R^{M\times N}$ is the measurement matrix generated by the DMD, $I_k \in R^{\sqrt{N}\times\sqrt{N}\times 1}$, $k = 1, 2, 3$, "·" means the inner product operation.

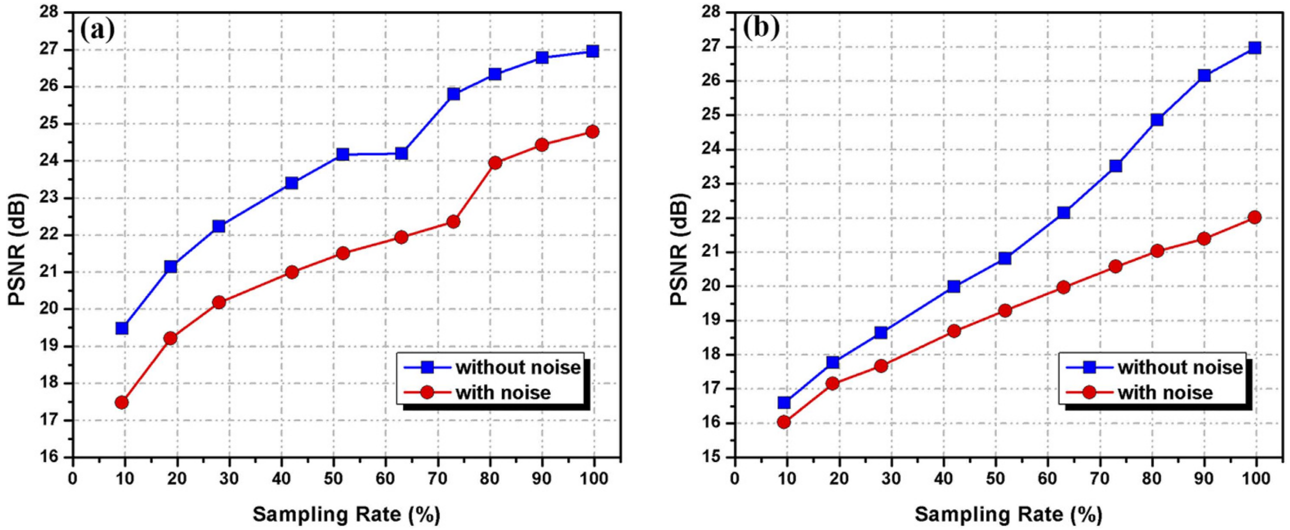

Figure 4. Relations of the sampling rate and PSNR with measurement noise and without measurement noise. (**a**) Relations of the sampling rate and PSNR between the original binary image and reconstructed images; (**b**) Relations of the sampling rate and PSNR between the gray-level image and reconstructed images.

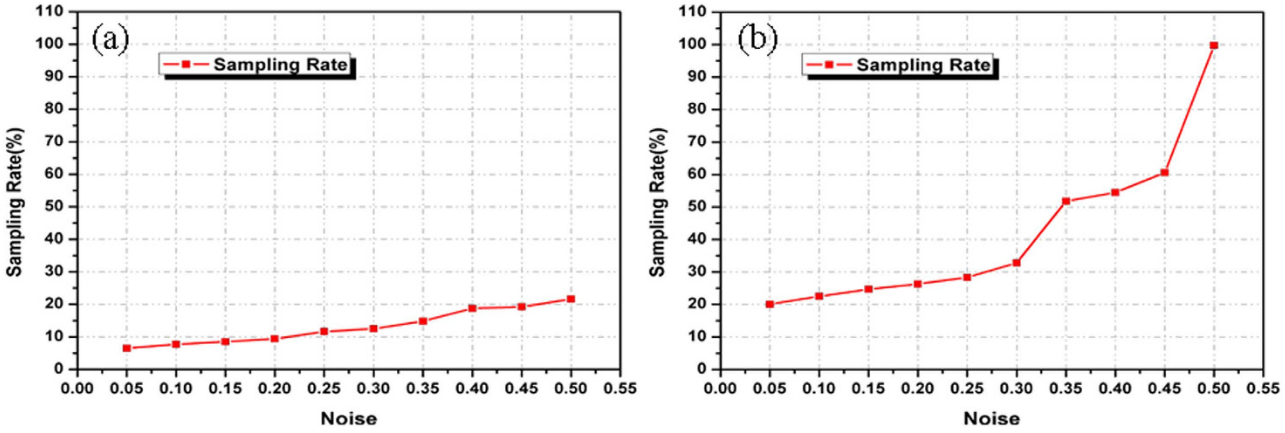

Figure 5. Relations of the number of measurements and the standard deviation σ of the measurement noise when the PSNR is 18 dB with (**a**) a binary image and (**b**) a gray-level image.

Then, we transmit the measurement data and measurement matrix using a conventional channel to the computer, where the image reconstruction and decryption will be performed. For the image signal, because the gradients of most images are sparse, Rudin *et al.* presented a nonlinear total variation (TV) algorithm, which attempts to denoise images in an effective manner. Simultaneously, it can enforce a sparsity constraint and reconstruct images well under compressive sensing theory[39]. The concept of constrained TV minimisation, which attempts to minimise the gradients of images, originated from the field of compressive sensing in the work by Candes *et al.*[18] Specifically,

$$\min \quad ||x||_{TV} \; s.\ t.\ y = \Phi \cdot x, \tag{6}$$

where

$$||x||_{TV} = \sum_{i,j}\sqrt{(x_{i+1,j} - x_{i,j})^2 + (x_{i,j+1} - x_{i,j})^2} = \sum_{i,j}\left|(\nabla x)_{i,j}\right| \tag{7}$$

is the total variation in the image x: the sum of the magnitudes of the gradient. The image can be constructed by solving the convex optimisation problem of minimising the l_1-norm of the image subject to the constraint that the image's DFT matches the measured DFT values. The null space property (NSP) is

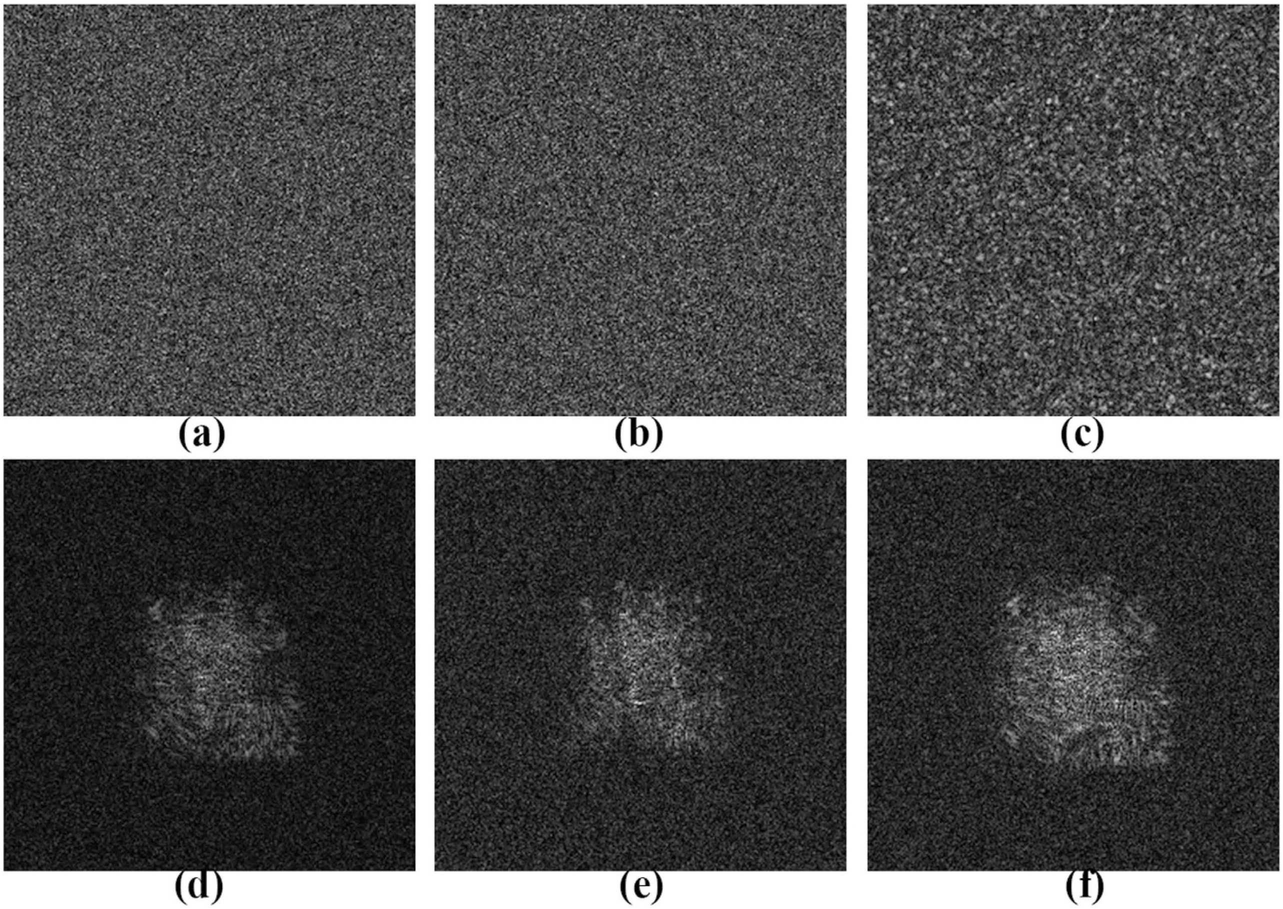

Figure 6. Retrieved images with one incorrect key in the decryption process: (**a**) When the principal key $q(x, y)$ is not used; (**b**) when the measurement matrix Φ is incorrect; (**c**) when only I_{H1} is used; (**d**) when z_1 has a relative error of 1%; (**e**) when z_2 has a relative error of 1%; (**f**) when λ has a relative error of 3%.

a sufficient condition for l_1 convex minimisation to obtain the sparsest solution. We are primarily concerned with how well CS can approximate a given signal from a given budget of fixed linear measurements compared to adaptive linear measurements[40]. Therefore, the advantages of using total variation (TV) is that the TV can considerably reduce the under-sampling ratio as well as offer robustness to noise in the data due to the better null space property (NSP). In the traditional approach of using a regulariser, such as TV, there is a trade-off between data fidelity and image regularity. A group at Duke also developed a TV algorithm to reduce the noise of a compressed hologram and solve the linear inversion problems[41]. In the present work, we are interested in image reconstruction in which the measurement is incomplete. Because of the incompleteness, there will be no unique minimiser of the data-fidelity-objective function, and TV is used to select a unique image out of the set of possible images that agree with the available data.

We first adopt two-step iterative shrinkage (TwIST) algorithm to reconstruct the interference wave intensity $\hat{I}_k$ by solving the optimal problem under additive white Gaussian noise in the system.

$$\min_{I_k} \frac{\mu}{2} \|Y_k - \Phi \cdot \hat{I}_k\|_2^2 + TV(\hat{I}_k) s.\ t.\ Y_k = \Phi \cdot I_k + e, \tag{8}$$

where $e \sim G(\mu, \sigma)$ is measurement noise, $G(\ )$ is the Gaussian noise, μ is the mean value, σ is the standard deviation, $\|Y_k - \Phi \cdot \hat{I}_k\|_2^2$ is the l_2 norm of $Y_k - \Phi \cdot \hat{I}_k$, and μ is a constant. The first penalty is a least-squares term that is small when $\Phi \cdot \hat{I}_k$ is consistent with the correlation vector Y_k. The second penalty $TV(\hat{I}_k)$ is the signal's total variation. As a result, a solution to the ill-posed equation that satisfies both the minimum error energy and minimisation of the recovered signal's total variation is obtained. From the above theoretical analysis, the interference wave intensity $\hat{I}_k$ can be correctly computed by solving the convex optimisation only when the receiver obtains the correct measurement matrix. This proves that the system's security is improved with the addition key space of the measurement matrix; the merits of the system are further discussed in the numerical simulation in the next section.

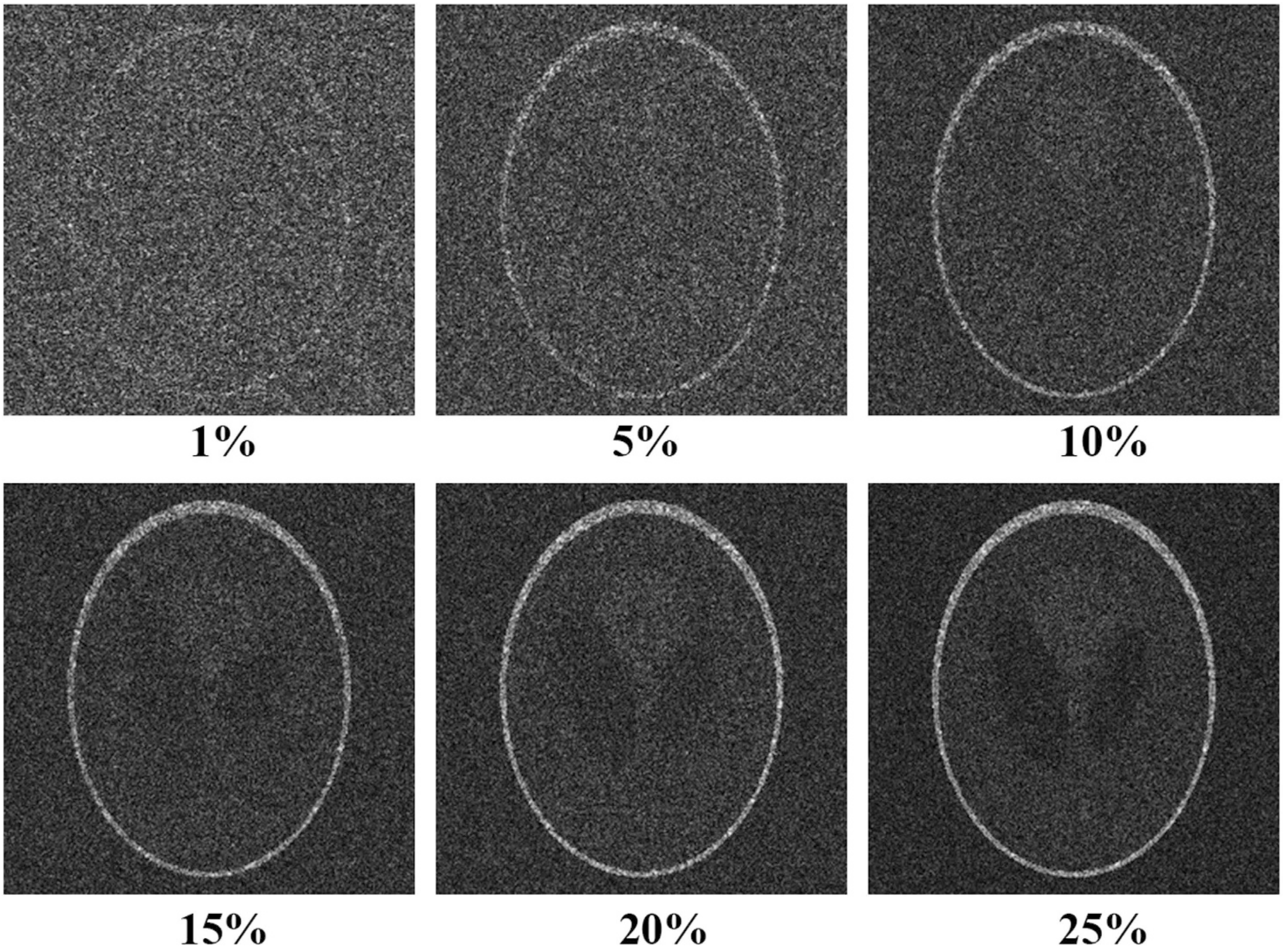

Figure 7. Reconstructed images for partially recovered keys.

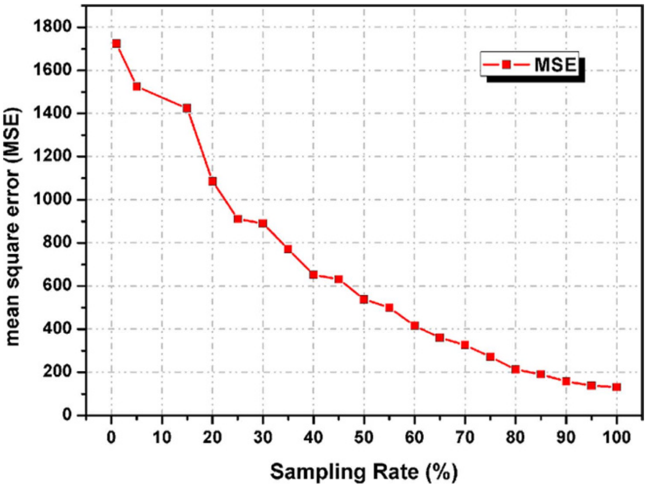

Figure 8. Mean square error (MSE) between the original image and reconstructions versus the sampling rate.

When the intensity patterns $\hat{I}_1$, $\hat{I}_2$, $\hat{I}_3$ are reconstructed with the TwIST algorithm, we can calculate the complex amplitude on the DMD plane

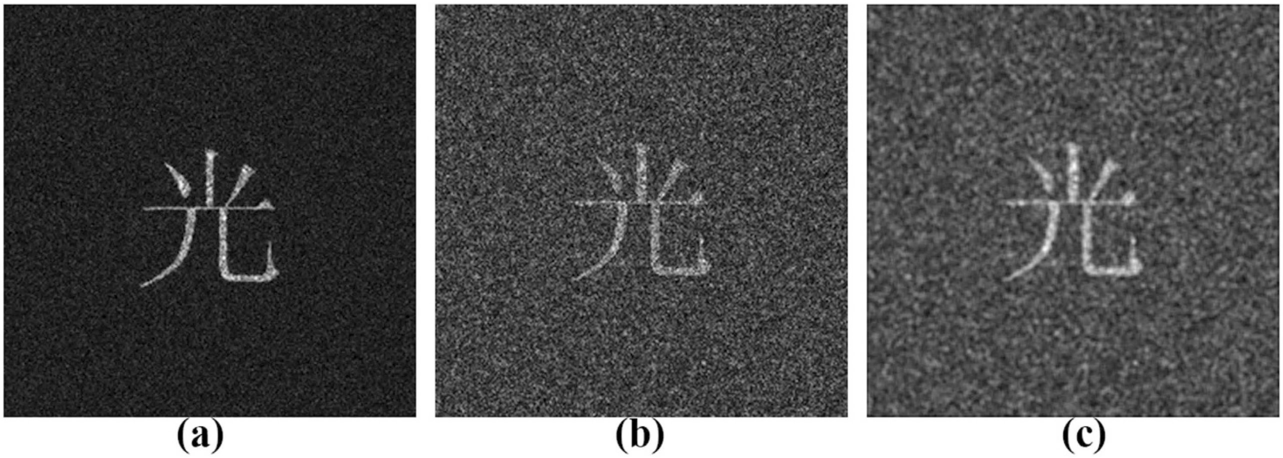

Figure 9. Study of binarisation of the reconstructions. (**a**) Recovered object image from 256 × 256 × 18.7% measurements; (**b**) recovered object image is binarised and (**c**) (**b**) filtered by an average filtering with a 3×3 window size.

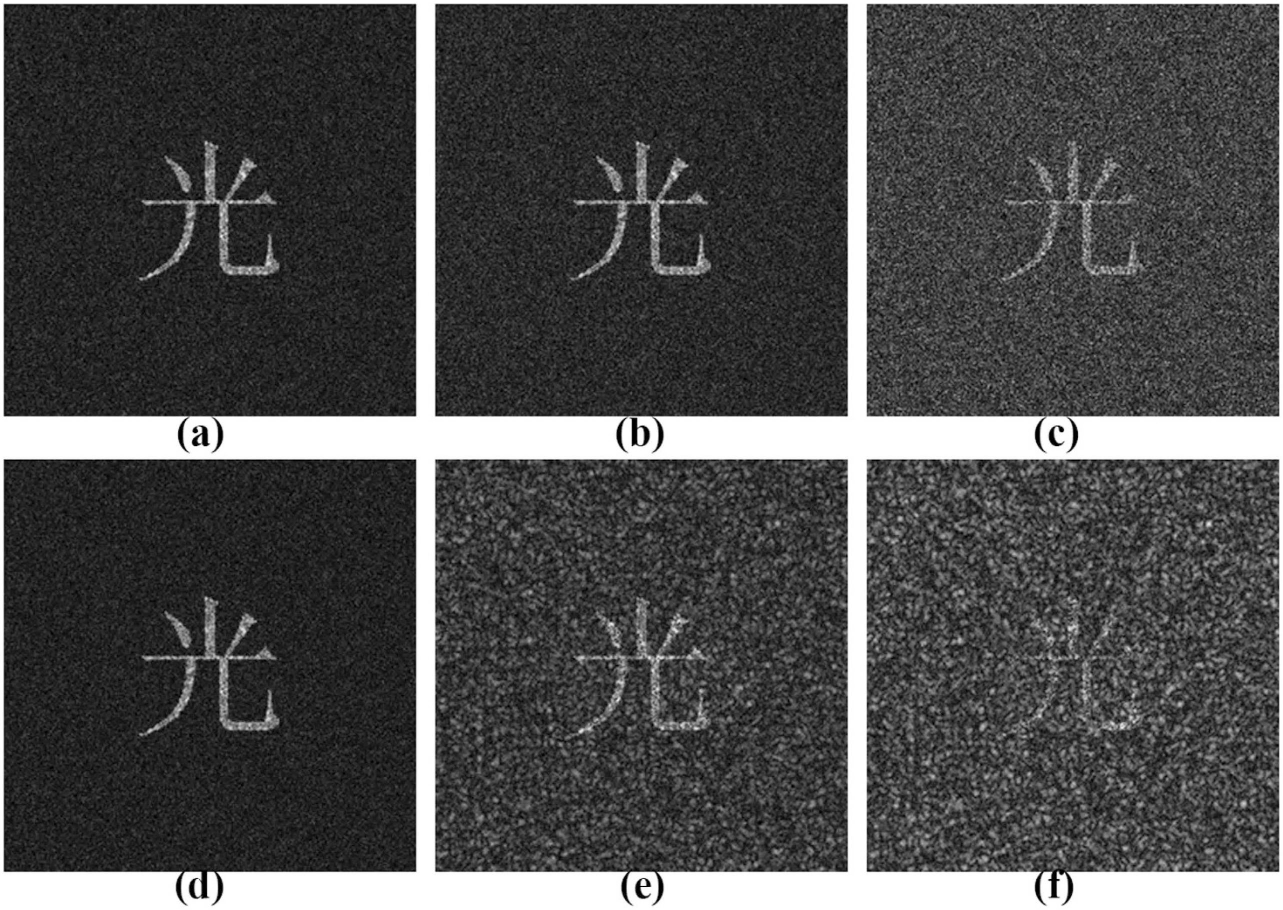

Figure 10. Study of noise perturbations in the encrypted image. The recovered object image from 256 × 256 × 18.7% measurements is corrupted by additive white Gaussian noise with the standard deviation (**a**) $\sigma = 0.1$; (**b**) $\sigma = 0.3$; (**c**) $\sigma = 1$; multiplicative noise with the standard deviation (**d**) $\sigma = 0.1$; (**e**) $\sigma = 0.3$; (**f**) $\sigma = 1$.

$$U(x, y) = \frac{(\hat{I}_1 - \hat{I}_3 + j(2\hat{I}_2 - \hat{I}_1 - \hat{I}_3))}{4}. \tag{9}$$

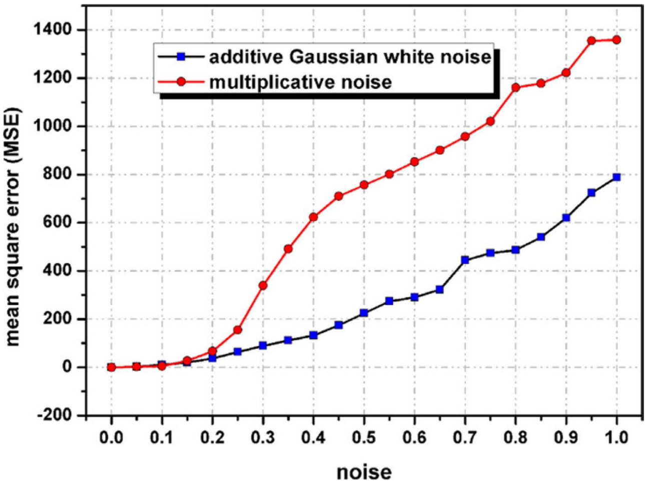

Figure 11. Mean square error (MSE) between the original image and reconstructions versus the standard deviation σ of the additive white Gaussian noise and multiplicative noise.

Once the complex amplitude $U(x, y)$ is known, in addition to random phase masks P_1 and P_2, z_1, z_2 and λ, we can digitally or optically retrieve the original object image from the encrypted image as

$$O'(x_0, y_0) = IFR_{Z1}\left\{IFR_{Z2}\left\{U(x, y)\exp\left[-i2\pi\cdot q(x_0, y_0)\right]\right\}\times\exp\left[-i2\pi\cdot p(x_0, y_0)\right]\right\}, \qquad (10)$$

where IFR_Z denotes the inverse Fresnel transformation of the distance z. Specifically, the original image has been perfectly reconstructed and decrypted.

Results

A series of simulations have been performed to verify the feasibility of our proposed method. This section presents a series of results based on the following conditions. The type of central processing unit (CPU) used in the computer simulation is an Intel(R) Core(TM) i7, and the memory of the computer is 6 GB. We used the MATLAB R2009a software package. The parameters that we used were $\lambda = 632.8$nm, $R = 1.5$, and $z_1 = z_2 = 0.125m$. The measurement matrix size of the DMD used in the computer simulation was 256 × 256 pixels. The measurement matrix generated by the DMD is random sequences of 0/1. The original object images used in the simulation are shown in Figs. 2(a) and 3(a), all with sizes of 256 × 256 pixels. The intensity values of the complex amplitude field containing encrypted object information are first modulated by the DMD, and 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 optical system's parameters. The simulation results for the compressive optical image encryption in a Mach-Zehnder interferometer are shown in Figs. 2 and 3. After performing compressive optical image encryption on the object images, the three encrypted interferograms containing the secret image information on the DMD plane will be sampled with compressive sensing theory; one of these interferograms for Figs. 2(a) and 3(a) is shown in Figs. 2(b) and 3(b). Figures 2(c) and 3(c) show the recovered object images from $256 \times 256 \times 18.7\%$ measurements and $256 \times 256 \times 42.1\%$ measurements using our method. The computer simulations show that this compressive optical image encryption method is performed using a completely optical scheme in the Fresnel domain.

Moreover, we investigated the compression feature and the effects of the measurement noises in our method. The computer simulations are shown in Figs. 4 and 5. 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. 4. In this simulation, the measurement noise described in Equation (8) is additive white Gaussian noise with a zero mean and a standard deviation $\sigma = 0.3$. Figures 4(a) and 4(b) present the relations of the sampling rate in the compressive sampling process and the PSNR for a binary image and gray-level image. The PSNRs clearly increase with increases in the sampling rate. When the sampling rate reaches 20%, the PSNR values are close to or greater than 20 dB. When considering the effects of white Gaussian noise, the relations of the sampling rate and PSNR have the same tendency. Figure 5 also illustrates the minimum number of measurements that enables a decent image retrieval under different measurement noise conditions. Figures 5(a) and 5(b) show the relations of the number of measurements and the standard deviation σ of the additive white Gaussian noise when the PSNR is 18 dB for the binary image and the gray-level image. This shows that the proposed method is effective and exhibits a good performance with a white Gaussian noise in the fully optical domain.

To investigate the security of this compressive optical image encryption method, we reconstruct the original binary image when one of the keys is incorrect, as shown in Fig. 6. Once one of the keys is incorrect, the retrieved image will be greatly affected. Among these keys, the principal key $q(x, y)$ and measurement matrix play critical roles in the security system, as shown in Figs. 6(a) and 6(b), in which the retrieved image is the same as the noise and fully unrecognisable when they do not be used to the reconstruction; when only one compressive sampled hologram dataset is used, there is no correct reconstruction image, as shown in Fig. 6(c); when the two diffraction distances of the object image and the wavelength of the laser exhibit a relative error, there are no correct reconstruction images, as shown in Figs. 6(d)-(f). We have also performed some simulations with other gray-level images and obtained satisfactory retrieval results, which are similar to those obtained with the binary images. Therefore, they are not considered here.

To further test the vulnerability of the proposed compressive encryption scheme, let us assume that a potential eavesdropper, who knows our reconstruction mechanism, has unauthorised access to a fraction Φ of the key parameters and uses the corresponding measurement matrix to reconstruct the image. Figure 7 shows a sequence of object images reconstructed from such a partially recovered key. The encrypted information begins to be retrieved when Φ is as high as 15%, which means that the eavesdropper should capture at least 15% of the measurement matrix numbers. To ensure security against more sophisticated eavesdropping attacks, Alice and Bob might want to synchronously and randomly alter the order of the elements of the key for different objects. The mean square error (MSE) between the original image and reconstructions versus the sampling rate is shown in Fig. 8. Clearly, the MSEs are observed to decrease with increases in the sampling rate. This proves that in addition to the keys above, the data of the measurement matrix are also one of the important keys. Therefore, the space of the key is expanded.

In addition, a series of simulations have been performed to investigate the robustness of our proposed method. In this section, we study the influence of the binarisation of the encrypted image on the recovered image and evaluate the noise performance of our proposed method in the presence of additive white Gaussian noise and multiplicative noise. Figures 9(a) and 9(b) show a recovered object image from $256 \times 256 \times 18.7\%$ measurements and a recovered object image that has been binarised, respectively, where an average filtering with a 3×3 window size is applied in the binarisation image, as shown in Fig. 9(c). Figure 10 shows the noise perturbation on the recovered object image with different standard deviations of additive white Gaussian noise and multiplicative noise. We calculated the MSE between the original and noise-corrupted recovered object images after using all of the correct keys. Figure 11 shows the MSE between the original image and reconstructions versus the standard deviation σ of the additive white Gaussian noise and multiplicative noise. The MSEs decrease as the standard deviations σ increase, and the multiplicative noise has a greater influence on the recovered object image compared with additive white Gaussian noise.

Conclusions

In this paper, an optical image encryption technique based on compressive sensing using fully optical means has been proposed. The simulations show that the method can be used to reconstruct the original image well with fewer measurements established by the Nyquist criterion and can be applied to gray-scale images and binary images to perform image encryption and compression in an all-optical system. With an optical image encryption technique and a compressive sensing technique, the method introduces an all-optical solution to sensing the original object, encrypting the object, and compressing the object in the analogue domain, which will present a superior scheme to overcome the limitations of the large holograms data volume for current optical image encryption systems. In addition, the DMD used in the setup of the compressive optical image encryption can perform high-speed measurements[27]; 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 transmission and naked-eye 3D Television.

References

1. Wang, R. Z., Lin, C.F. & Lin, J.C. Image hiding by optimal LSB substitution and genetic algorithm. *Patt. Recog.* **34,** 671–683 (2001).
2. Petitcolas, F. A. P., Anderson, R. J. & Kuhn, M. G. Information hiding - A survey. *Proc. IEEE.* **87,** 1062–1078 (1999).
3. Tanha, M., Kheradmand, R. & Ahmadi-Kandjani, S. Gray-scale and color optical encryption based on computational ghost imaging. *Appl. Phys. Lett.* **101,** 101108 (2012).
4. Guanrong, C., Yaobin, M. & Chui, C. K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos. Solitons Fract.* **21,** 749–761 (2004).
5. Lu-Zhong, C., Ming-Zhao, H., Qing, L. & Xiu-Lun, Y. Digital image encryption and watermarking by phase-shifting interferometry. *Appl. Opt.* **43,** 3078–3084 (2004).
6. Tajahuerce, E. & Javidi, B. Encrypting three-dimensional information with digital holography. *Appl Opt.* **39,** 6595–6601 (2000).
7. Malik, M., Magana-Loaiza, O. S. & Boyd, R. W. Quantum-secured imaging. *Appl Phys Lett.* **101,** 241103 (2012).
8. Bishop, C. A., Humble, T. S., Bennink, R. S. & Williams, B. P. Quantum-Secured Surveillance Based on Mach-Zehnder Interferometry. *arXiv preprint* **arXiv:1303.6701** (2013).
9. Clemente, P., Durán, V., Tajahuerce, E. & Lancis, J. Optical encryption based on computational ghost imaging. *Opt. Lett.* **35,** 2391–2393 (2010).

10. Jun, L., Tao, Z., Qing-zhi, L. & Rong, L. Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography. *Opt. Commun.* **285,** 1704–1709 (2012).
11. Meng, X. F. *et al.* Two-step phase-shifting interferometry and its application in image encryption. *Opt. Lett.* **31,** 1414–1416 (2006).
12. Jun, L., Jiaosheng, L., Yangyang, P. & Rong, L. Optical image hiding with a modified Mach-Zehnder interferometer. *Opt Laser Eng.* **55,** 258–261 (2014).
13. Jun, L., Jiaosheng, L., Yangyang, P. & Rong, L. Optical image encryption and hiding based on a modified Mach-Zehnder interferometer. *Opt. Express.* **22,** 4849–4860 (2014).
14. Brackett, C. A. *et al.* A scalable multiwavelength multihop optical network: a proposal for research on all-optical networks. *J Lightwave Technol.* **11,** 736–753 (1993).
15. Naughton, T. J., Frauel, Y., Javidi, B. & Tajahuerce, E. Compression of digital holograms for three-dimensional object reconstruction and recognition. *Appl. Opt.* **41,** 4124–4132 (2002).
16. Shortt, A., Naughton, T. J. & Javidi, B. Compression of digital holograms of three-dimensional objects using wavelets. *Opt. Express.* **14,** 2625–2630 (2006).
17. Patten, R. E. *et al.* Speckle photography: mixed domain fractional Fourier motion detection. *Opt Lett.* **31,** 32–34 (2006).
18. Candes, E. J., Romberg, J. & Tao, T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *Ieee T Inform. Theory.* **52,** 489–509 (2006).
19. Donoho, D. L. Compressed sensing. *Ieee T Inform. Theory.* **52,** 1289–1306 (2006).
20. Magana-Loaiza, O. S., Howland, G. A., Malik, M., Howell, J. C. & Boyd, R. W. Compressive object tracking using entangled photons. *Appl. Phys. Lett.* **102,** 231104 (2013).
21. Sun, B. *et al.* 3D Computational Imaging with Single-Pixel Detectors. *Science*. **340,** 844–847 (2013).
22. Clemente, P. *et al.* Compressive holography with a single-pixel detector. *Opt. Lett.* **38,** 2524–2527 (2013).
23. Jun, L., Yuping, W., Rong, L. & Yaqin, L. Coherent single-detector 3D imaging system. *Proceedings of the SPIE - The International Society for Opt Eng.* **8913,** 891303 (891304 pp.)-891303 (891304 pp.) (2013).
24. Li, J. *et al.* Two-step Holographic Imaging Method based on Single-pixel Compressive Imaging. *J Opt Soc Korea.* **18,146**–150 (2014).
25. Katz, O., Bromberg, Y. & Silberberg, Y. Compressive ghost imaging. *Appl. Phys. Lett.* **95,** 131110 (2009).
26. Assmann, M. & Bayer, M. Compressive adaptive computational ghost imaging. *Sci. Rep.-uk* **3,** (2013).
27. Howland, G. A., Lum, D. J., Ware, M. R. & Howell, J. C. Photon counting compressive depth mapping. *Opt. Express.* **21,** 23822–23837 (2013).
28. Chapman, H. N. & Nugent, K. A. Coherent lensless X-ray imaging. *Nat. Photonics.* **4,** 833–839 (2010).
29. Howland, G. A., Schneeloch, J., Lum, D. J. & Howell, J. C. Simultaneous Measurement of Complementary Observables with Compressive Sensing. *Phys. rev. let.* **112,** 253602 (2014).
30. Mirhosseini, M., Magana-Loaiza, O. S., Rafsanjani, S. M. H. & Boyd, R. W. Compressive Direct Measurement of the Quantum Wave Function. *Phys. rev. let.* **113,** 090402 (2014).
31. Zorzi, M., Gluhak, A., Lange, S. & Bassi, A. from today's intranet of things to a future Internet of things: a wireless and mobility related view. *Ieee Wirel Commun.* **17,** 44–51 (2010).
32. Huang, R., Rhee, K. H. & Uchida, S. A parallel image encryption method based on compressive sensing. *Multime Tools Appl.* **72,** 71–93 (2014).
33. Chen, W., Quan, C. & Tay, C. J. Optical color image encryption based on Arnold transform and interference method. *Opt. Commun.* **282,** 3680–3685 (2009).
34. Lu, P., Xu, Z., Lu, X. & Liu, X. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique. *Optik.* **124,** 2514–2518 (2013).
35. Liu, X., Cao, Y., Lu, P., Lu, X. & Li, Y. Optical image encryption technique based on compressed sensing and Arnold transformation. *Optik.* **124,** 6590–6593 (2013).
36. Aidi, Z., Nanrun, Z. & Lihua, G. Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform. *J Comput.* **8,** 2857–2863 (2013).
37. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt Lett.* **20,** 767–769 (1995).
38. Yoder, L. A. *et al.* DLP technolgy: applications in optical networking[C]//International Symposium on Optical Science and Technology. *International Society for Optics and Photonics*, 54–61 (2001).
39. Rudin, L. I., Osher, S. & Fatemi, E. Nonlinear total variation based noise removal algorithms. *Physica D.* **60,** 259–268 (1992).
40. Cohen, A., Dahmen, W. & Devore, R. Compressed sensing and best k-term approximation. *J Am Math. Soc.* **22,** 211–231 (2009).
41. Brady, D. J., Choi, K., Marks, D. L., Horisaki, R. & Lim, S. Compressive Holography. *Opt. Express.* **17,** 13040–13049 (2009).

Acknowledgments

This study was supported by the Project of Department of Education of Guangdong Province, China (No. 2013 KJCX0058) and partly supported by the National Science Foundation for Young Scientists of China (No.11404115).

Author Contributions

L.J. and L.J.S. conceived of the idea and wrote the main manuscript text. P.Y.Y. and L.R. prepared the figures. All authors reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Li, J. *et al.* Compressive Optical Image Encryption. *Sci. Rep.* **5**, 10374; doi: 10.1038/srep10374 (2015).