Optical encryption based on the algorithm of compressive ghost imaging and phase-shifting digital holography

[1] Zhang Leihong, [1] Xiong Rui, [2] Zhang Dawei and [3] Chen Jian

[1] College of Communication and Art Design, University of Shanghai for Science and Technology, Shanghai 200093, China, xiongrui2017usst@sina.com
[2] School of Optical Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
[3] Anhui Province Key Laboratory of Nondestructive Evaluation, Anhui 230088, China

Received: 07.05.2018

Abstract. We present a compressive ghost-imaging encryption (GIE) scheme based on phase-shifting digital holography (PSDH). With our technique based on the PSDH, the optical information is recorded from each point of an object. Then each part of a hologram can reconstruct the original image, thus improving resolution of a reconstructed image. Using the characteristics of randomness of the PSDH, we improve security of the encryption scheme. In our simulations, a binary image is taken as a target and the mutual information, the PSDG degree and the peak signal-to-noise ratio are calculated. The compressive GIE scheme based on the PSDH is compared with a pseudo-inverse algorithm based on PSDH and a common GIE scheme based on the PSDH. The simulation results demonstrate that our compressive scheme manifests better reconstruction quality, compressibility and security.

Keywords: phase-shifting digital holography**,** ghost imaging, compressive sensing, optical encryption

PACS: 42.30.Va, 42.40.My
UDC: 535.8

1. Introduction

Encryption is an important issue in the field of information security. Optical information encryption technologies are favoured due to their parallelism, high speed and low cost. At present, the studies of these technologies include mainly double random-phase encoding, as well as the encryptions based on Fourier or Fresnel transforms. One of the known correlation-imaging techniques is a ghost imaging (GI). In particular, Shapiro [1] and Bromberg et al. [2] have used a spatial light modulator (SLM) to preset a light field in the reference arm, and realized for the first time the experiment on computational GI.

Since then, Katz and co-workers [3] have suggested a compressive GI (CGI) scheme that combines compressive sensing with the GI [1–13]. This scheme reduces the requirements for iterative computations in the GI-based image reconstruction techniques and improves the reconstruction rate via compressive-sensing computations. Basing on this, the study [14] uses the CGI and a normalized reference illumination in order to reduce reconstruction times and improve a signal-to-noise ratio. The work [15] has suggested a new CGI algorithm, which employs joint orthogonal transformation to improve sparse representation of a signal. The authors [16] have analyzed computational ghost images encoded using SLM, thus enabling reconstruction of a target from multiple intensities. The above methods represent nonlinear encryption systems, which are good enough with respect to security but reveal not so high resolution for optically decrypted reconstructed images.

Digital holography is a novel technology for recording and reconstructing holograms. It has already been applied in the field of optical encryption. In the work [17], a new two-step phase-shifting holographic optical-encryption technique has been introduced, and decryption performance has been analyzed. The authors [18] have combined the two-step phase-shifting holography with the compressive sensing in order to reduce the amount of data in their optical image-encryption system. Finally, a new holographic image-reconstruction method has been proposed in Ref. [19], which combines a convolution algorithm, a four-step phase-shifting method and information hiding, with the aim of improving information-transmission security.

Following from the results mentioned above, one can notice that each part of a phase-shifting digital hologram (PSDH) can reproduce the characteristics of entire image and randomness. The present study introduces a new CGI encryption scheme based on PSDH. Our main purpose is to improve further the resolution and encryption security of reconstructed images.

2. Fundamentals of CGI

The CGI technique works as follows. Assume that a sender of information, Alice, and its receiver, Bob, share a key in the entire encryption process. The key is given by the normal Gaussian random distribution matrix $\{\varphi_i(x,y)\}_{i=1}^{N}$ generated by Alice, so that $\varphi_i(x,y)$ obeys a uniform distribution in the region [0, 2π]. The SLM is used to preset the light field in the reference arm. This is based on modulation of the phase pattern in the input. If a parallel beam is incident on the SLM, the light field distribution $I_i(x,y)$ is known. It can be calculated using the Fresnel propagation function. A random spot generated after the SLM is irradiated by an object $T(x,y)$ to be imaged. Subsequently, the light intensity of the object collected by a single-pixel bucket detector is equal to B_i, which is given by

$$B_i = \int dxdy I_i(x,y) \times T(x,y) \tag{1}$$

This calculation is repeated N times to get N different measured values $\{B_i\}_{i=1}^{N}$, thus completing the encryption process. Finally, the correlation function that restores the original information about the object completes the decryption process:

$$T_{GI}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(B_i - \langle B\rangle)I_i(x,y) \tag{2}$$

In Eq. (2), $T_{GI}(x,y)$ represents the reconstructed original information, and $\langle\cdot\rangle$ gives the arithmetic mean.

Scrutinizing the CGI process, we explain its further details. Let T(x,y) be a two-dimensional image to be encrypted with the size $n\times n$, which is rearranged into an $n^2\times 1$ column vector. The light field-intensity matrix $I_i(x,y)$ is transformed into a one-dimensional row vector by a row-connection procedure, and N light-field intensity matrices are sequentially arranged to form the measurement matrix ϕ:

$$\phi = \begin{bmatrix} I_1(1,1) & \cdots & I_1(1,n) & \cdots & I_1(n,n) \\ I_2(1,1) & \cdots & I_2(1,n) & \cdots & I_2(n,n) \\ \vdots & & \vdots & & \vdots \\ I_N(1,1) & \cdots & I_N(1,n) & \cdots & I_N(n,n) \end{bmatrix} \tag{3}$$

Then the encryption process is expressed by

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_N \end{bmatrix} = \begin{bmatrix} I_1(1,1) & \dots & I_1(1,n) & \dots & I_1(n,n) \\ I_2(1,1) & \dots & I_2(1,n) & \dots & I_2(n,n) \\ \vdots & & \vdots & & \vdots \\ I_N(1,1) & \dots & I_N(1,n) & \dots & I_N(n,n) \end{bmatrix} \begin{bmatrix} T(1,1) \\ T(1,n) \\ \vdots \\ T(n,n) \end{bmatrix} \tag{4}$$

During the CGI process, a single-pixel bucket detector receives the light intensity of a randomly distributed optical field, which reflects the whole information from all the points of a target object. Therefore the information-acquisition mechanism of the CGI and that of the single-pixel compressive sensing are essentially the same. In the compressive sensing used to decrypt the original image, the original image can be reconstructed from these projections with high probability by solving an optimization problem

$$T_{CS} = T(x,y) : argmin \left\| \Psi \mathrm{T}(x,y) \right\|_{I_1} \tag{5}$$

where $\|\cdot\|_{I_1}$ denotes the 1-norm, Ψ the sparse matrix, and T_{CS} the image reconstructed using the compressive-sensing algorithm.

3. PSDH technique

To perform PSDH recording, one should introduce a high-precision phase-shifting device in the reference optical path, so that the object light and the reference light result in a continuous relative phase shift to form a time series of multiple interference images. A CCD detects the sequence of the interference intensities at each pixel point. Then the corresponding numerical values are input into a computer to calculate the spectral complex-amplitude distribution. Using the PSDH, one can simulate the object light-field distribution by a numerical-reconstruction algorithm, and a digital representation of the hologram is realized in a computer.

A schematic setup used to implement the PSDH technique is shown in Fig. 1. Here an object light wave recorded by the CCD is $O(x,y)$. We use a four-step phase-shifting technology and record four holograms. When a hologram is recorded, the reference light $R(x,y)$ is used to introduce the phase shift of 0, $\pi/2$, π and $3\pi/2$. The four interference intensity distributions can be

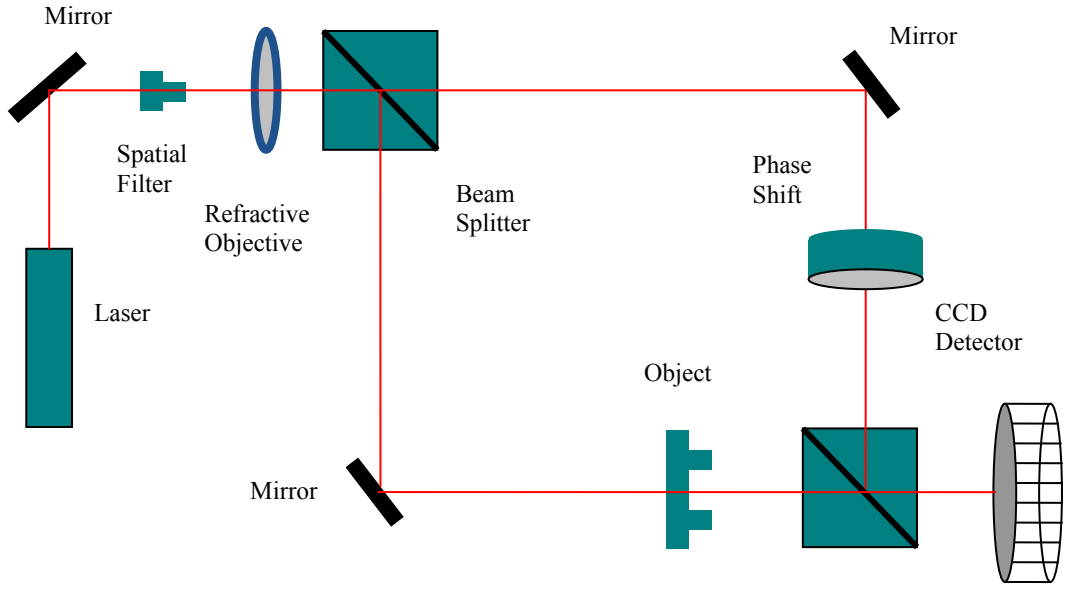


Fig. 1. Scheme of setup used in the frame of PSDH technique.

expressed as

$$\begin{aligned} I_1(x,y,0) &= |O(x,y)|^2 + |R(x,y)|^2 + 2R(x,y)O(x,y)cos\phi \\ I_2\left(x,y,\frac{\pi}{2}\right) &= |O(x,y)|^2 + |R(x,y)|^2 + 2R(x,y)O(x,y)sin\phi \\ I_3(x,y,\pi) &= |O(x,y)|^2 + |R(x,y)|^2 - 2R(x,y)O(x,y)cos\phi \\ I_4\left(x,y,\frac{3\pi}{2}\right) &= |O(x,y)|^2 + |R(x,y)|^2 - 2R(x,y)O(x,y)sin\phi \end{aligned} \tag{6}$$

where $O(x,y)$ implies the object light wave, $R(x,y)$ the reference light, and φ the phase distribution of the object light wave on the recording surface. Using the four holograms described above, one obtains

$$O(x,y) = \frac{1}{4R(x,y)}\left\{I_1(x,y,0) + jI_2\left(x,y,\frac{\pi}{2}\right) - I_3(x,y,\pi) - jI_4\left(x,y,\frac{3\pi}{2}\right)\right\} \tag{7}$$

The method given by Eq. (7) can eliminate both the conjugate and zero-order images. It improves the signal-to-noise ratio for the digital hologram and improves the quality of the reconstructed image. Finally, the principal scheme of CGI encryption based on the PSDH technique is illustrated in Fig. 2. Here an SLM is introduced in the reference arm for changing one of the parameters of the SLM. These are the amplitude, the intensity, the phase or the wavelength.

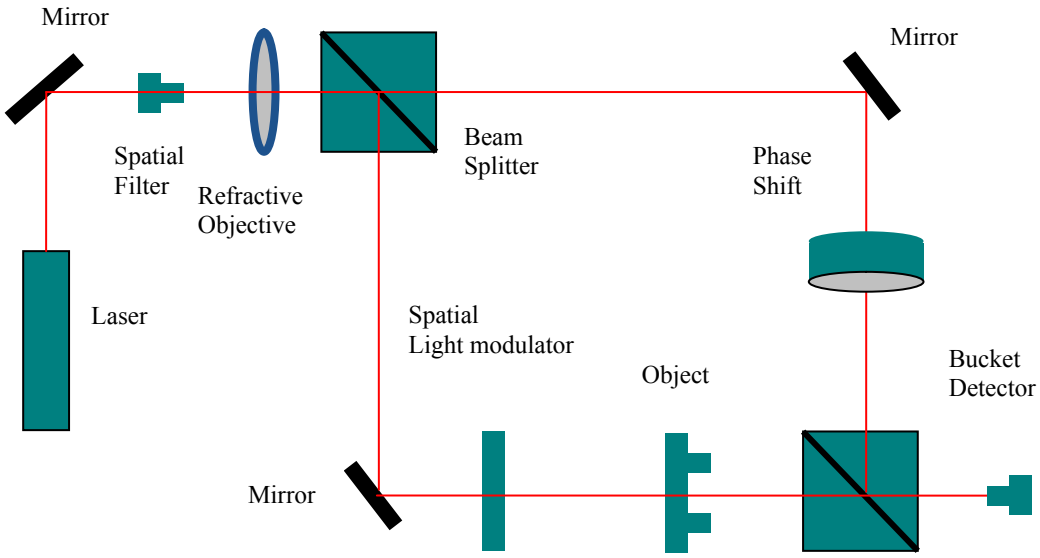


Fig. 2. Principal scheme of CGI encryption based on the PSDH technique.

4. Optical encryption based on CGI algorithm and PSDH technique

The main steps of our optical encryption procedures based on the CGI algorithm and the PSDH technique are as follows.

Step 1: Use the PSDH to encrypt the original image and obtain the hologram image. The hologram image is a clear text of the next GI encryption algorithm.

Step 2: Use a part of the data contained in the hologram image and employ the GI algorithm for image transmission encrypting. Here the imaging could be realized under interference in the

external environment, whereas a random signal can be used as a key because the randomness of this key can be encrypted.

Step 3: Use the compressive-sensing algorithm to decrypt the hologram and obtain the reconstructed PSDH.

Step 4: Invert the PSDH and obtain the original image.

5. Simulations and analysis

Simulations of the CGI encryption scheme based on PSDH have been completed using a MATLAB platform. The process is as follows: (1) the hologram is obtained by the PSDH using a so-called 'USST' binary image with the size 64×64 pixels; (2) the hologram image serves as a clear text $T(x,y)$ using the GI encryption algorithm; (3) a prefabricated light intensity matrix $I_i(x,y)$ is connected in rows, and N matrices are arranged in sequence to form the measurement matrix ϕ; (4) the value obtained by multiplying the measurement matrix and the binary image is taken as a total light intensity B_N; (5) N measurements (B_1, B_2...B_N,) of the imaged object are taken. Finally, the reconstructed image is obtained using decryption performed according to the compressive-sensing algorithm given by Eq. (5). The simulation results obtained for the case of the sampling frequency 4096 are shown in Fig. 3.

Fig. 3. Computer simulation results obtained for optical encryption of a binary image: (a) original image, (b) hologram image, (c) reconstructed hologram image, and (d) reconstructed original image.

5.1. Feasibility

By this term, we imply stability with respect to possible problems arising in the situation when a recipient uses a secret message shared with a sender and a public channel in order to restore the original-image information. We discuss the feasibility of our encryption method and compare it with the PSDH-based CGI encryption scheme (PSDH-CGI), the PSDH-based pseudo-inverse algorithm (PSDH-PI) and the PSDH-based GI algorithm (PSDH-GI). The corresponding results are illustrated in Fig. 4.

In order to quantify correlation of reconstructed and original images, we introduce a standard parameter associated with mutual information:

$$\begin{aligned} \mathrm{H[X]} &= \sum_{i=0}^{\mathrm{L}} \mathrm{P}_i[\mathrm{X}\log \mathrm{P}_i(\mathrm{X})] \\ \mathrm{H[Y]} &= \sum_{i=0}^{\mathrm{L}} \mathrm{P}_i[\mathrm{Y}\log \mathrm{P}_i(\mathrm{Y})] \\ \mathrm{H[XY]} &= \sum_{i=0}^{\mathrm{L}} \mathrm{P}_i[\mathrm{XY}\log \mathrm{P}_i(\mathrm{XY})] \\ \mathrm{I(X;Y)} &= \mathrm{H[X]+H[Y]-H[XY]} \end{aligned} \tag{8}$$

where the X and Y variables are associated respectively with the original and reconstructed images,

H[X] and H[Y] are the corresponding entropies, H[XY] denotes the joint entropy, and I[X;Y] the mutual information. In Eq. (8), P_i represents the probability of occurrence of image pixels, and L the gray level of the image. The relationship of the mutual information and the sampling number for different encryption methods is shown in Fig. 5.

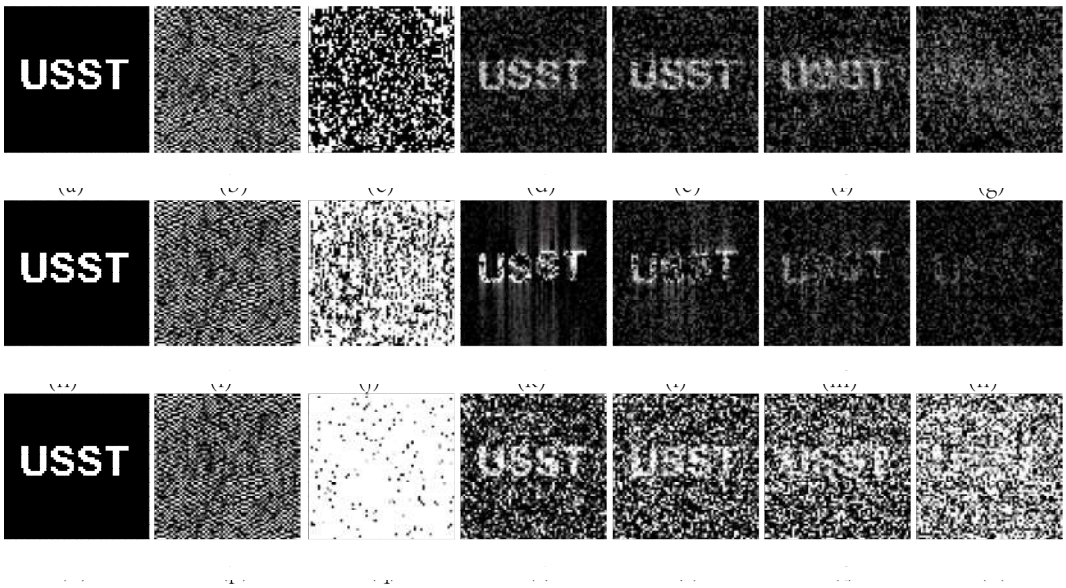


Fig. 4. Results of computer simulations for the optical encryption by different methods: (a), (h) and (o) original image; (b), (i) and (p) hologram image; (c), (j) and (q) reconstructed hologram image (CGI, PI, GI); (d), (k) and (r) reconstructed original image (the sampling frequency 4000); (e)–(g), (l)–(n) and (s)–(u) reconstructed original image (the sampling frequencies are respectively 3000, 2000 and 1000).

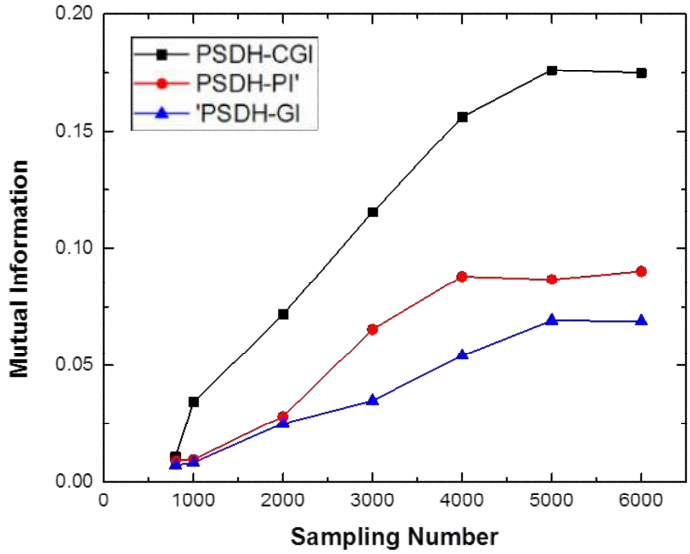


Fig. 5. Relationships of mutual information and sampling number obtained for different encryption methods.

The entropy H[X] of the original image is 0.253, which is a theoretically maximal value that can be reached. If we wish to reach it, we need to recover the whole information of the image with no distortions. Of course, it would be very difficult to achieve and, moreover, it would consume a great deal of time thus outweighing its benefits. The real situation seen from Fig 5 can be

summarized as follows.

(1) Higher mutual information can be achieved when the sampling number is 4000, although this parameter becomes lower when the sampling number increases and becomes larger than 4000;

(2) The mutual information value for the PSDH-PI and PSDH-GI schemes are very close to each other, whenever the sampling number is smaller than 2000. As the latter increases up to 2000 or more, the mutual information for the PSDH-PI scheme is larger than that for the PSDH-GI scheme. This indicates that the quality of the image reconstructed by the PSDH-PI scheme is better than that of the PSDH-GI;

(3) For large sampling numbers, the mutual information obtained for the PSDH-CGI scheme is larger than that found for PSDH-PI and PSDH-GI, thus implying that the PSDH-CGI scheme is superior to the other two ones.

Hence, our simulation results demonstrate that the images reconstructed using the scheme suggested in the present work are of better quality, thus proving feasibility of our scheme.

5.2. Robustness

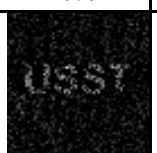
Making use of anti-cutting characteristics of the PSDH, one can compress the appropriate information and reduce greatly the amount of information transmitted. In our simulations, we cut different portions of hologram information at first. Then the cut image is compressed. Finally, the quality of the reconstructed image is used to evaluate whether the cutting information affects the encryption algorithm or not. A standard NC similarity measure is used to evaluate objectively how similar the original and reconstructed images become after cropping. For the image size $M \times N$, the mathematical expression of the NC similarity is as follows:

$$\mathrm{NC} = \frac{\sum_{i=1}^{\mathrm{M}} \sum_{j=1}^{\mathrm{N}} \mathrm{X}(i,j)\mathrm{X}'(i,j)}{\sum_{i=1}^{\mathrm{M}} \sum_{j=1}^{\mathrm{N}} \mathrm{X}(i,j)^2} \tag{9}$$

where X corresponds to the original image and X' to the reconstructed image obtained after cropping.

In our simulations, the holographic images and the reconstructed holographic images have been cut by 10, 20, 30, 40 and 50%. The sampling number in this experiment remains constant, 4096. The images obtained after cutting and the corresponding NC values for the reconstructed images are displayed in Table 1.

Table 1. Reconstructed images and NC values obtained with different cut ratios

Proportion	10%	20%	30%	40%	50%
NC for the hologram image					
	0.582	0.489	0.449	0.417	0.268
Proportion	10%	20%	30%	40%	50%
NC for the reconstructed hologram image					
	0.481	0.365	0.307	0.297	0.237

When the sampling frequency is equal to 4096 and the hologram is not cropped, the NC value for the reconstructed image amounts to 0.841. As seen from Table 1, the reconstructed images become more blurred with the increase of the cutting ratio, and the NC values become lower. Furthermore, when the cutting proportion for the holographic images reaches 40%, the NC value is equal to 0.417. Then the reconstructed image can identify only the outlines of the original image. Finally, we get the NC value of 0.297 when the cutting proportion is equal to 40%. The reconstructed image can be seen only vaguely, while the outlines themselves cannot be observed. Hence, the effect of cutting for the holographic image is weaker than that for the reconstructed holographic image. Finally, the original image can be successfully reconstructed whenever the hologram is cut as large as by 40%.

Fig. 6 compares the CGI encryption scheme based on the PSDH with the pure CGI scheme. Here the PSDH-CGI algorithm is performed for the case of the sampling number 4096. The similarity between the original and reconstructed images is evaluated by the peak signal-to-noise ratio, PSNR, and the mean-square errorm MSE:

$$\begin{aligned} \mathrm{PSNR}&=\lg\left(\frac{a_{\max}^2}{MSE}\right) \\ MSE&=\frac{1}{\mathrm{MN}}\sum_i^{\mathrm{M}}\sum_j^{\mathrm{N}}\left(\mathrm{R}(i,j)-F(i,j)\right)^2 \end{aligned} \tag{10}$$

Here R(i ,j) and F(i ,j) are the pixel values corresponding respectively to the original and reconstructed images, and a_{max} is the largest pixel value in the image.

As seen from Fig. 6, increasing cutting ratio (i.e., decreasing sampling number in the CGI) decreases gradually the peak signal-to-noise ratio, which means a decreased relevance of the reconstructed image and the reduced original image. Moreover, the peak signal-to-noise ratio obtained with the PSDH-CGI is always higher than that obtained with the CGI. This fact testifies that the former method is better than the latter in case when the cropping proportion increases. The above conclusions demonstrate that the PSDH-CGI scheme manifests better compressibility. The corresponding reconstructed images are more similar to the original ones and have higher resolutions.

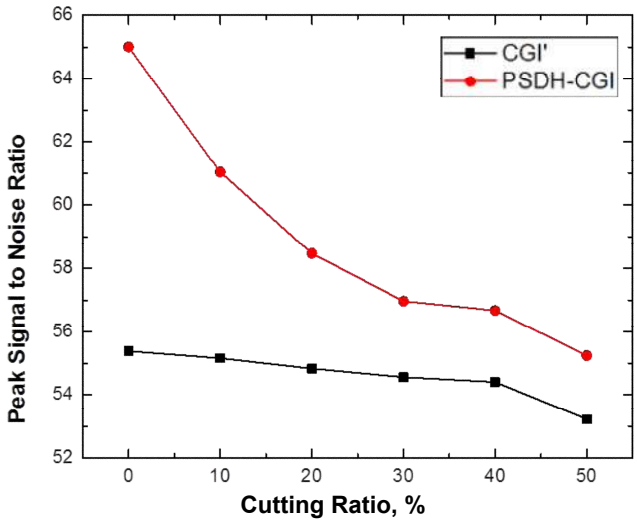


Fig. 6. Peak signal-to-noise ratios for the images reconstructed using PSDH-CGI and CGI with different cut ratios.

5.3. Security

Below we verify security of the CGI encryption scheme based on the PSDH. For any encryption scheme, the security is one of important indicators that measure the quality of encryption algorithm. In general, there is no absolutely secure encryption system. Of course, the algorithm can be considered to be surely safe only when the cost of decoding algorithm is equal to or greater than that of encrypted information. Further on, we use a known password-attack method to verify anti-attack performance of the system designed by us.

Cipher text-only attack. A cipher text-only attack implies that an attacker knows only a cipher text and then tries to analyze the intercepted text in order to find the key or the plain text that corresponds to the cipher text. From the viewpoint of an attacker, the cipher text-only attack is the most difficult of all the attacks. As a result, a cryptographic system is considered to be theoretically unsafe if it cannot resist even the cipher text attack. Below we use the image histogram as a method to analyze whether the encryption algorithm is good or bad in this respect. Of course, different histogram distributions that correspond to different images should be different. The algorithm reveals a good security if the histogram of the encrypted image is approximately uniformly distributed and the encrypted image is similar to the random noise.

Fig. 7 shows gray-scale histogram distributions in which the abscissas indicate the gray levels and the ordinates the frequencies at which these levels appear. After compressive sensing, the information is further compressed. It is seen that the histogram of the encrypted image is approximately uniform, thus pointing out that our scheme has good security.

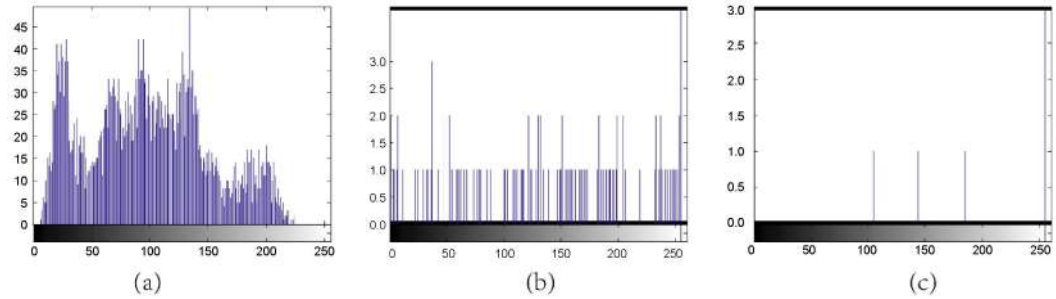


Fig. 7. Gray-scale histogram distributions for the original image (a), the hologram (b) and the reconstructed hologram (c). Abscissa corresponds to the gray level and ordinate to the frequency at which this gray level appears.

The correlation of adjacent pixels reflects the degree of correlation of the pixel values in the adjacent positions of image. Reducing the correlation between the adjacent pixels is one of the aims of image encryption. This includes the correlations along horizontal, vertical and diagonal directions. The smaller the correlation between the adjacent pixels, the better the image encryption and the higher security are. The formulae for the pixel correlation coefficients are as follows:

$$\begin{aligned} \mathrm{E}(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \mathrm{E}(x)\right)^2 \\ cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \mathrm{E}(x)\right)\left(y_i - \mathrm{E}(y)\right) \\ CC &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{aligned} \tag{11}$$

where x_i and y_i are the pixel values for the two adjacent pixels in the image, $cov(x,y)$ is the correlation of pixel values, $E(x)$ the mean, and $D(x)$ the mean-squared error.

Table 2. Correlations between the plain-text image and the cipher-text image as calculated for adjacent pixels

Correlation coefficient	Horizontal direction	Vertical direction
Original image	0.754	0.695
Encrypted image	0.029	0.044

As seen from Table 2, the correlation of the adjacent pixels in the original image is very high. Instead, it becomes very small after encryption, so that the adjacent pixels are largely irrelevant. This testifies that statistical characteristics of the original image have been transformed into a random cipher text in the latter image. Distributions of the correlations between the adjacent pixels in the original and encrypted images are shown in Fig. 8. It is evident that the correlations between the pixels in the original image reveal a clear linear distribution, while in the encrypted image they have a random character.

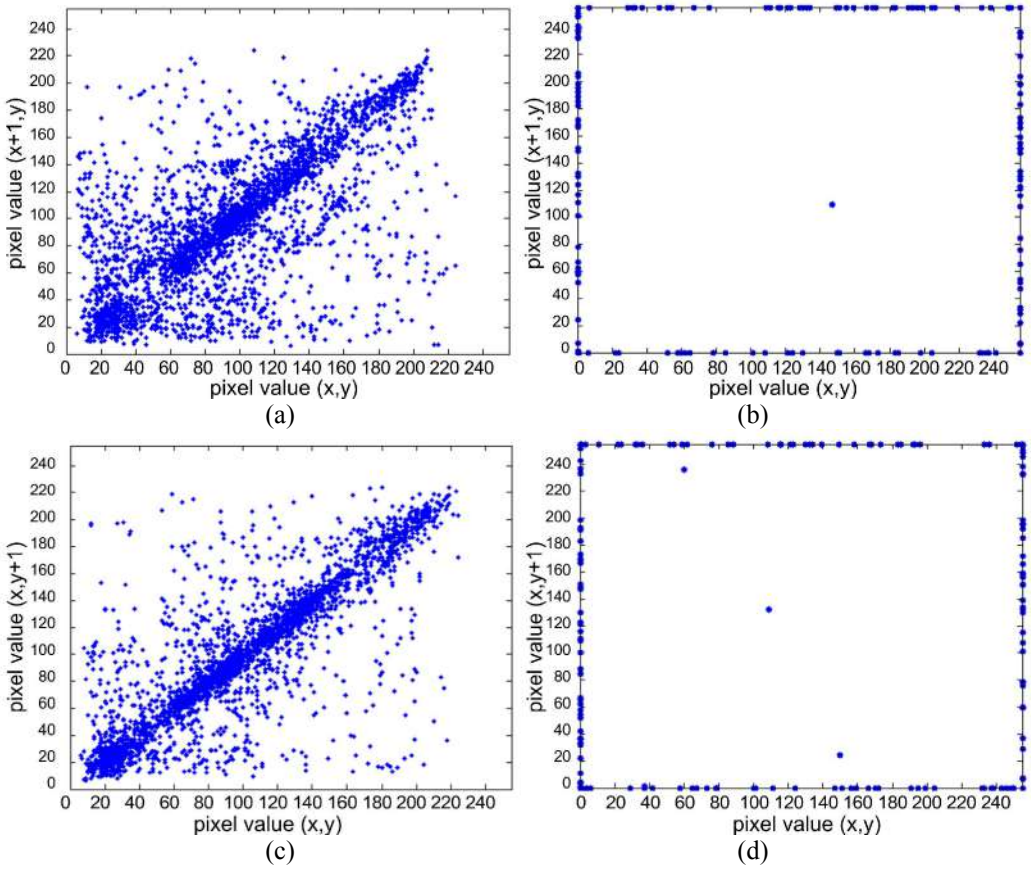


Fig. 8. (a) Correlation of adjacent pixels along horizontal direction for the original image, (b) correlation of adjacent pixels along horizontal direction for the encrypted image, (c) correlation of adjacent pixels along vertical direction for the original image, and (d) correlation of adjacent pixels along vertical direction for the encrypted image.

Noise attack. A noise attack is inevitable in the process of information encryption and transmission. Since the noise influences the quality of object images, it is necessary to evaluate

robustness of the encryption algorithm under the condition that either the key or the cipher text is attacked by the noise. The NC values for the reconstructed images obtained for the cases of pure CGI scheme and CGI scheme based on PSDH are compared in Fig. 9. Obviously, the NC value reveals a certain decline when the noise attacks the algorithms of the both kinds. However, the NC value for the PSDH-CGI scheme is always higher than that for the pure CGI, thus indicating that the CGI encryption scheme based on the PSDH is more secure.

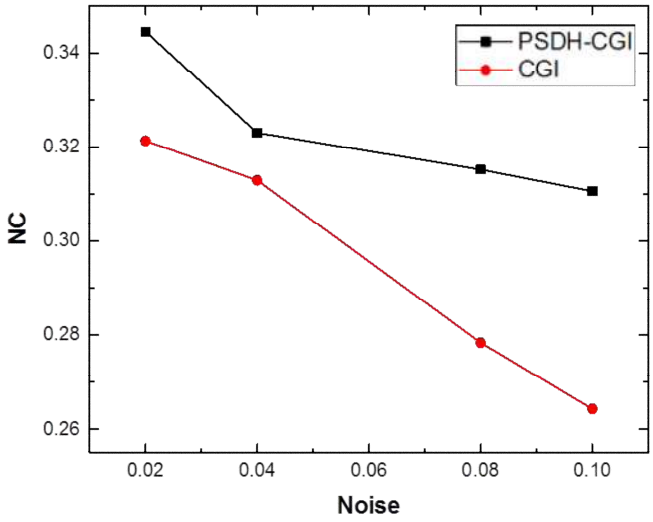


Fig. 9. Dependence of NC value for the reconstructed image on the noise.

6. Conclusion

The PSDH technique and the CGI algorithm are combined in order to improve both the resolution and the security of images. The CGI encryption scheme based on the PSDH measures the intensity of interfering light with a bucket detector. This intensity is acquired using the four-step phase-shifting method and, finally, the CGI parameters are calculated to obtain the reconstructed image. To check our theoretical suggestions, we have built a platform based upon numerical simulations. The appropriate simulation results demonstrate that the PSDH-CGI encryption scheme can obtain reconstructed images with higher resolutions. In particular, this is true if one compares the image resolutions obtained using the PSDH-PI and PSDH-GI techniques under the condition of the same sampling frequencies.

Acknowledgment

This study was supported by the Natural Science Foundation of Shanghai (Grants No. 14ZR1428400 and 18ZR1425800) and the Open Project of Anhui Province Key Laboratory of Nondestructive Evaluation (Grant No. CGHBMWSJC03).

References

1. Shapiro J H, 2008. Computational ghost imaging. Phys. Rev. A **78**: 061802(R).
2. Bromberg Y, Katz O and Silberberg Y, 2009. Ghost imaging with a single detector. Phys. Rev. A. **79**: 053840.
3. Katz O, Bromberg Ya, and Silberberg Ya, 2009. Compressive ghost imaging Appl. Phys. Lett. **95**: 131110.
4. Katkovnik V and Astola J, 2012. Compressive sensing computational ghost imaging. J. Opt. Soc. Amer. A. **29**: 1556–1567.

5. Clemente P, Duran V, Torrescompany V, Tajahuerce E and Lancis J, 2010. Optical encryption based on computational ghost imaging. Opt. Lett. **35**: 2391–2393.
6. Shapiro J H and Boyd R W, 2012. The physics of ghost imaging. Quant. Inf. Process. **11**: 949–993.
7. Huang H C and Chang F C, 2014. Robust image watermarking based on compressed sensing techniques. J. Inform. Hiding & Multimedia Signal Process. **5**: 275–285.
8. Rawat N, Hwang I C, Shi Y and Lee B, 2015. Optical image encryption via photon-counting imaging and compressive sensing based ptychography. J. Opt. **17**: 065704.
9. Liu H, Xiao D, Zhang R, Zhang Y and Bai S, 2016. Robust and hierarchical watermarking of encrypted images based on compressive sensing. Signal Process. Image Commun. **45**: 41–51.
10. Wu Jingjing, Xie Zhenwei, Liu Zhengjun, Liu Wei, Zhang Yan and Liu Shutian, 2016. Multiple-image encryption based on computational ghost imaging. Opt. Commun. **359**: 38–43.
11. Garnier J, 2017. Ghost imaging in the random paraxial regime. Inverse Problems & Imaging. **10**: 409–432.
12. Yuwang Wang, Yang Liu, Jinli Suo, Guohai Situ, Chang Qiao & Qionghai Dai, 2017. High-speed computational ghost imaging via spatial sweeping. Sci. Rep. **7**: 45325.
13. Balasubramanian R and Ramesh A, 2017. Optical cryptography based on compressive ghost imaging using multi-image encryption scheme. Int. J. Mod. Trends Eng. Sci. **4**: 8–9.
14. Wenlin Gong, Chengqiang Zhao, Hong Yu, Mingliang Chen, Wendong Xu & Shensheng Han, 2016. Three-dimensional ghost imaging lidar via sparsity constraint. Sci. Rep. **6**: 26133.
15. Shengmei Zhao and Peng Zhuang, 2014. Correspondence normalized ghost imaging on compressive sensing. Chin. Phys. B. **23**: 287–291.
16. Yi Chen, X Fan and Z Liang, 2016. Application of joint orthogonal bases in compressive sensing ghost image. Proc. SPIE, Selected Papers of the Chinese Society for Optical Engineering Conferences. **10141**: 101410Q.
17. Seok-Hee Jeon and Sang-Keun Gil, 2011. 2-step phase-shifting digital holographic optical encryption and error analysis. J. Opt. Soc. Korea. **15**: 244–251.
18. Li J, Li H, Li J, Pan Y and Li R, 2015. Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography. Opt. Commun. **344**: 166–171.
19. Wang Li, Fu Zirui, Liu Fuping, Lu Zhipeng and Wang Yukun, 2017. Holographic information hiding based on the four-step phase-shifting method. J. Beijing Inst. Graphic Commun. **25**: 30 – 34.

Zhang Leihong, Xiong Rui, Zhang Dawei and Chen Jian. M. 2018. Optical encryption based on the algorithm of compressive ghost imaging and phase-shifting digital holography. Ukr.J.Phys.Opt. **19**: 179 – 190. doi: 10.3116/16091833/19/3/179/2018

Анотація. *Представлено схему шифрування на основі фантомних зображень (ШФЗ) зі стисканням і фазозсувних цифрових голограм (ФЗЦГ). Використовуючи метод, заснований на ФЗЦГ, оптичну інформацію записують від кожної точки об'єкта. Тоді кожна частина голограми може реконструювати вхідне зображення, тим самим підвищуючи роздільну здатність відновленого зображення. Використовуючи характеристики випадковості ФЗЦГ, підвищено безпеку схеми шифрування. У моделюванні використано вхідне бінарне зображення та розраховано взаємну інформацію, ступінь ФЗЦГ і пікове відношення сигнал/шум. Схему ШФЗ зі стисканням на основі ФЗЦГ порівняно із псевдо-оберненим алгоритмом на основі ФЗЦГ і звичайною схемою ШФЗ на основі ФЗЦГ. Результати моделювання показують, що наша схема зі стисканням виявляє ліпші якість відновлення, ступінь стиснення та безпеку.*