Applied Physics B (2020) 126:136
https://doi.org/10.1007/s00340-020-07487-4

Applied Physics B
Lasers and Optics

Multi-image holographic encryption based on phase recovery algorithm and ghost imaging

Zhang Leihong[1] · Zhang Zhisheng[1] · Ye Hualong[1] · Kang Yi[1] · Wang Zhaorui[1] · Wang Kaimin[1] · Zhang Dawei[1]

Received: 23 March 2020 / Accepted: 9 July 2020 / Published online: 19 July 2020

Abstract

There is a method that presents for securing much information at the same time, which need not be restricted to a single image data. Based on ghost imaging, this paper proposes a new encryption algorithm: multi-image holographic encryption based on phase recovery algorithm and ghost imaging (PRA-GI). In the encryption process, first, multiple images are combined into one phase hologram image by phase holographic recovery algorithm. Second, the combined image is encrypted by ghost imaging to obtain ciphertext. During the decryption, each receiver can get the same phase hologram image reconstructed by the public key. Finally, each receiver uses the unique assisted private key to get corresponding information. By numerical simulation, it is found that this algorithm can effectively improve the encryption capacity. Experimental results and objective indicators verify the feasibility of this algorithm. At the same time, PRA-GI is suitable for enterprises and governments. For example, the leader license different assisted private keys and the primary public key to different employees according to different permissions. This algorithm implements double encryption, which ensures the security of information and solves crosstalk problems among images.

1 Introduction

Due to the high parallelism, high speed and high storage, optical information processing technology attract more and more researchers. Klyshko proposed a scheme about ghost imaging based on the entanglement behavior of two-photon light [1]. Shapiro and Jeffrey et al. used a spatial light modulator (SLM) to achieve computational ghost imaging [2]. Clemente et al. proposed an optical information encryption method based on computational ghost imaging [3]. He first used ghost imaging in the field of optical encryption. Chi et al. proposed pseudo-inverse ghost imaging and Gong completed the experimental verification [4, 5]. Their algorithm improves the quality of reconstructed images. Ying et al. used a two-step phase-retrieval method to greatly increase the imaging ability of the ghost imaging for the general complex-valued object [6]. Zhang et al. employed permutated Hadamard basis patterns, instead of random intensity illumination patterns, for securing object image information [7]. Jiao et al. proposed the Two novel visual cryptography (VC) schemes by combining VC with single-pixel imaging (SPI) for the first time, which extends the application to more diversified scenarios [8]. These researchers have enhanced the efficiency and quality of ghost imaging [9, 10], but these studies have focused on a single image with complex information.

As an important branch of optical encryption, multi-image optical encryption technology not only improves the encryption capability but also reduces the amount of ciphertext data. Wu et al. first proposed multi-image encryption based on computational ghost imaging [11]. Lee and Cho proposed a multi-image transmission method based on orthogonal encoding and double random phase encryption, which uses two random phase and orthogonal encoding to encrypt multiple images [12]. Le and Meng proposed multi-image encryption based on Compressive Ghost Imaging and Coordinate Sampling [13]. They apply logical mapping algorithms and joint sampling to the encryption and decryption of multiple images. Sui and Zhao proposed an optical multiple-image authentication based on the transport of intensity equation, which applies intensity equation transmission technology to realize optical multi-image authentication [14]. Zhou and Yan proposed a multi-image encryption scheme based on quantum 3D Arnold transform, which saves a lot of storage space [15].

✉ Zhang Dawei
dwzhang@usst.edu.cn

[1] University of Shanghai for Science and Technology, Shanghai 200093, China

Although these multi-image optical encryption algorithms greatly enhance the compressibility of multi-image optical encryption, most of them currently share a common key for multiple pictures. Sharing a public key has great security risks. Once the public key is compromised, all the pictures will be leaked.

We have experimentally demonstrated and proposed a new encryption algorithm: Multi-image holographic encryption based on phase recovery algorithm and ghost imaging (PRA-GI). This paper combines the phase holographic recovery algorithm (Gerchberg–Saxton) with computational ghost imaging encryption technology. Compared with other phase-retrieval works in ghost imaging, this method can encrypt multiple pictures without interference between images. In this paper, each image has the primary public key and an assisted private key, which solves the potential security risks. In this paper, the feasibility of the method is verified by mathematical simulation and experiment. This algorithm extends applications of ghost imaging in the field of optical encryption and provides a reference for improving multi-image compressive encryption.

2 Principle of multi-image holographic encryption based on phase recovery algorithm and ghost imaging

2.1 Principle of computational ghost imaging encryption

Ghost imaging is a new imaging method. Unlike traditional imaging, ghost imaging is non-local imaging. Many scholars proposed different methods for improving information quality and improving reconstruction speed [16–21]. In the field of information encryption, ghost imaging encryption has made great progress.

The principle of computational ghost imaging is shown in Fig. 1. There are N normal Gaussian random distribution matrices $\varphi_i(x,y)$ as a key and $\varphi_i(x,y)$ is evenly distributed over [0, 2π]. Digital micromirror device (DMD) modulates the phase of parallel light. The modulated light (light intensity is $I(x,y)$) illuminates the object $T(x,y)$. The light intensity value is recorded by a bucket detector as B_i, which is measured N times to get N different values as $\{B_i\}_{i=1}^{N}$. This process is shown in Eq. (1), where $I_i(x,y)$ is calculated according to the Fresnel propagation function as shown in Eq. (2):

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

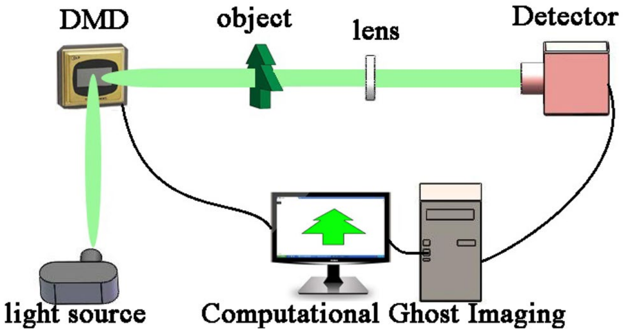


Fig. 1 The principle of computational ghost imaging

$$I_i(x,y) = \left|E_{\text{in}}(x,y)\exp[j\varphi_i(x,y) \otimes h_z(x,y)\right|, \tag{2}$$

where $h_z(x,y)$ is the Fresnel diffraction function for propagating a distance z. $\otimes$ represents the convolution operation. $E_{\text{in}}(x,y)$ is the amplitude distribution of input light fields.

In the encryption process: a two-dimensional image $T(x,y)$ (its size is $n \times n$) is converted into a one-dimensional column vector $\left(n^2 \times 1\right)$. Different random matrices $\varphi_i(x,y)$ are operated to obtain light intensity distribution function according to Eq. (2). The light intensity distribution function at the m time operation is $I_m(x_p, y_q), m = 1, 2, \dots, N; p, q = 1, 2, \dots n$. The matrix expression of light intensity distribution function is:

$$I_m = \begin{bmatrix} I_{11}^m & \cdots & I_{1n}^m \\ \vdots & \ddots & \vdots \\ I_{n1}^m & \cdots & I_{nn}^m \end{bmatrix}, \tag{3}$$

I_{nn}^m is an element at the nth row, the nth column of a matrix at the m time.

The size of this matrix is $n \times n$. Matrix is stretched into a one-dimensional row vector (its size is $1 \times n^2$).

$$I_m = \left[I_{11}^m, I_{12}^m \cdots I_{1n}^m, I_{21}^m I_{22}^m \cdots I_{n,n-1}^m I_{n,n}^m\right], \tag{4}$$

After several measurements, the measurement matrix (its size is $N \times n^2$) is obtained. Information is encrypted into N values to form a one-dimensional vector $\{B_i\}$. The expression of the encryption process is:

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_N \end{bmatrix} = \begin{bmatrix} I_{11}^1 & \cdots & I_{1n}^1 & \cdots & I_{nn}^1 \\ I_{11}^2 & \cdots & I_{1n}^2 & \cdots & I_{1n}^2 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ I_{11}^N & \cdots & I_{1n}^N & \cdots & I_{nn}^N \end{bmatrix} \begin{bmatrix} T_{11} \\ \vdots \\ T_{1n} \\ \vdots \\ T_{nn} \end{bmatrix}, \tag{5}$$

where $\begin{bmatrix} I_{11}^1 & \cdots & I_{1n}^1 & \cdots & I_{nn}^1 \\ I_{11}^2 & \cdots & I_{1n}^2 & \cdots & I_{1n}^2 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ I_{11}^N & \cdots & I_{1n}^N & \cdots & I_{nn}^N \end{bmatrix}$ is the measurement matrix. $\begin{bmatrix} T_{11} \\ \vdots \\ T_{1n} \\ \vdots \\ T_{nn} \end{bmatrix}$ is an image $T(x, y)$.

In the decryption process: calculate light intensity information $I_i(x, y)$ by key according to formula (2). Correlate $I_i(x, y)$ with light intensity measurement (ciphertext) to reconstruct information. The reconstruction formula for computing ghost imaging is:

$$T_{GI}(x, y) = \frac{1}{N} \sum_{i=1}^{N} \left(B_i - \langle B_i \rangle\right) I_i(x, y), \tag{6}$$

$\langle B_i \rangle$ is the average of N-time measurement.

2.2 Principle of the phase recovery algorithm

The phase recovery algorithm in this paper is the Gerchberg–Saxton (G-S) iterative algorithm [22]. It is the way to obtain the phase distribution by iteratively iterating phase between phase planes and image planes. It relies on the principle of the Huygens–Fresnel principle. It iteratively calculates the propagation process between phase planes and image planes. This paper first describes the principle of the Gerchberg–Saxton (G-S) iterative algorithm by generating holograms from two images.

Double-image G-S iterative algorithm process expression is:

$A_1 = \text{Amplitude}(\text{Target1}) * \exp(i * \text{phas}(\text{Rand}n))$

While the error is not satisfied:

$$\begin{aligned} B_1 &= A_1 \otimes f_{\text{fresnel}}^{-Z} \\ B_2 &= \text{Amplitude}(\text{Target2}) * \exp(i * \text{phase}(B_1)) \\ C_1 &= F^{-1}\{B_2\} \\ C_2 &= \text{Amplitude}(\text{Sourse}) * \exp(i * \text{phase}(C_1)) \\ B_3 &= F\{C_2\} \\ A_3 &= B_3 \otimes f_{\text{fresnel}}^{-Z} \\ A_1 &= \text{Amplitude}(\text{Target1}) * \exp(i * \text{phase}(A_3)) \end{aligned} \tag{7}$$

END

Final Phase = Phase (C_1)

f_{fresnel}^{Z} represents the Fresnel diffraction factor transmits forward, Z represents the distance of transmission distance. f_{fresnel}^{-Z} represents the Fresnel diffraction factor transmits backwards, Z represents the distance of transmission distance. F represents a Fourier transform. F^{-1} represents the inverse Fourier transform. A represents the plane in which Target 1 is located, B represents the plane in which Target 2 is located, and C represents the plane in which the phase hologram is located.

The specific flow of double-image G-S iterative algorithm is shown in Fig. 2. In double-image G-S iterative algorithm, the intensity of Target 1 is multiplied by the random phase to obtain the wave function $f(x, y)$. $f(x, y)$ is propagated to the position of Target 2 by the Fresnel diffraction factor (the distance of propagation is z_1), and then $f(x, y)$ is changed to the wave function $t(x, y)$. The phase of $t(x, y)$ is multiplied by the intensity of Target 2 to obtain the wave function $k(x, y)$. Perform inverse Fourier transform on $k(x, y)$ to obtain

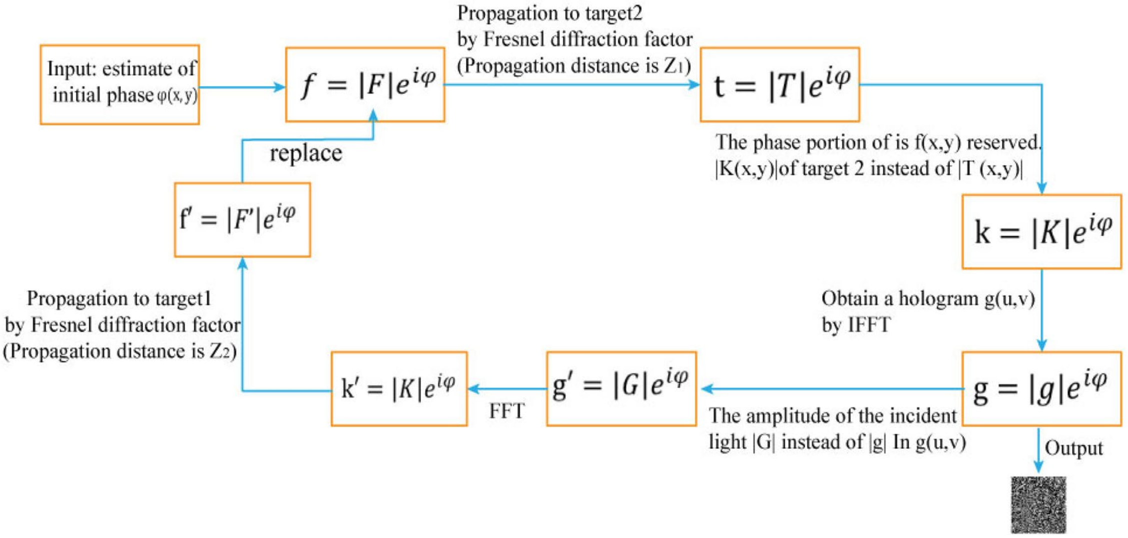

Input: estimate of initial phase φ(x,y)
$f = |F|e^{i\varphi}$
Propagation to target2 by Fresnel diffraction factor (Propagation distance is Z1)
$t = |T|e^{i\varphi}$
The phase portion of is f(x,y) reserved. |K(x,y)|of target 2 instead of |T (x,y)|
$k = |K|e^{i\varphi}$
Obtain a hologram g(u,v) by IFFT
$g = |g|e^{i\varphi}$
Output
The amplitude of the incident light |G| instead of |g| In g(u,v)
$g' = |G|e^{i\varphi}$
FFT
$k' = |K|e^{i\varphi}$
Propagation to target1 by Fresnel diffraction factor (Propagation distance is Z2)
$f' = |F'|e^{i\varphi}$
replace

Fig. 2 The specific flow of double-image G-S iterative algorithm

a hologram. The intensity of the incident light is multiplied by the phase of the hologram to obtain the wave function $g'(x,y)$. $g'(x,y)$ performs a Fourier transform to reproduce the wave function $k'(x,y)$. The reproduced wave function $k'(x,y)$ is propagated to the position of Target 1 by Fresnel diffraction factor (The distance of propagation is z_2). produce a new wave function $f'(x,y)$. Iterate again with new $|F|$(phase of $f'(x,y)$). Repeat the above process to get the phase hologram.

2.3 Multi-image holographic encryption based on phase recovery algorithm and ghost imaging

This paper proposes a new encryption method—multi-image holographic encryption based on phase recovery algorithm and ghost imaging (PRA-GI). As shown in Fig. 3, there are two main steps in the encryption phase and two steps in the decryption phase.

The specific steps of Multi-image holographic encryption based on phase recovery algorithm and ghost imaging (PRA-GI) are (take holographic iterative encryption of three images as an example):

Encryption phase (1) multiply the intensity of Target 1 by the random phase to get the wave function $f(x,y)$. $f(x,y)$ is propagated to the position of Target 2 by the Fresnel diffraction factor (the distance of propagation is z_1), and then $f(x,y)$ is changed to the wave function $t(x,y)$. Multiply the phase of $t(x,y)$ by the intensity of Target 2 to obtain the wave function $w(x,y)$. $w(x,y)$ is propagated to the position of Target 3 by the Fresnel diffraction factor (the distance of propagation is z_2), and then $w(x,y)$ is changed to the wave function $k(x,y)$. Multiply the phase of $k(x,y)$ by the intensity of Target 3 to obtain a wave function. Perform inverse Fourier transform to obtain a hologram. Multiply the intensity of the incident light (parallel light) by the hologram phase to obtain the wave function $g'(x,y)$.

$g'(x,y)$ performs a Fourier transform and then reproduces the wave function $k'(x,y)$. $k'(x,y)$ performs Fresnel diffraction to the position of Target 2, and reproduces the wave function $w'(x,y)$. $w'(x,y)$ is propagated to the position of Target 1 by the Fresnel diffraction factor (the distance of propagation is z_3). produces a new wave function $f'(x,y)$. Iterate again with new $|F|$(phase of $f'(x,y)$). Repeat the above process to get the phase hologram. The whole multi-image phase hologram iterative process is shown in Fig. 4.

Encryption phase (2): The phase hologram is a two-dimensional image. Two-dimensional phase hologram performs computational ghost imaging for encryption. After the second encryption, it gets one-dimensional data as ciphertexts.

Decryption phase (1): It uses an observation matrix as a public key to obtain the light intensity information. PRA-GI reconstructs the ciphertexts and light intensity information by performing ghost imaging to execute the calculation. It reconstructs a two-dimensional matrix as reconstructed phase hologram.

Decryption phase (2): Phase hologram is obtained by reconstruction. Incident parallel light is passed through phase hologram. Then this paper uses different diffraction distances as different private keys for secondary decryption.

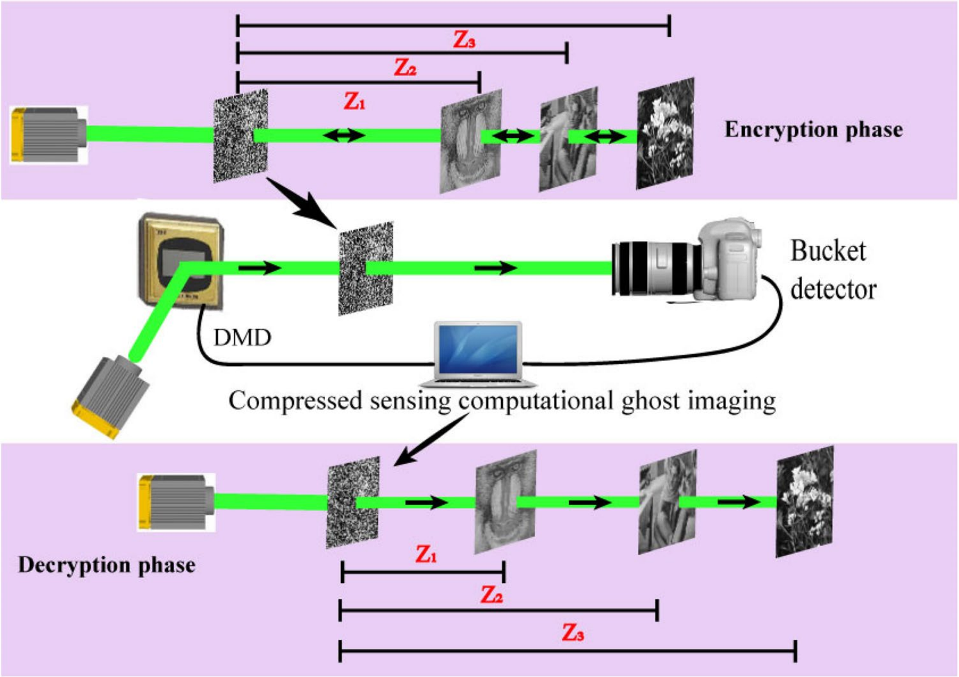


Fig. 3 Method flow

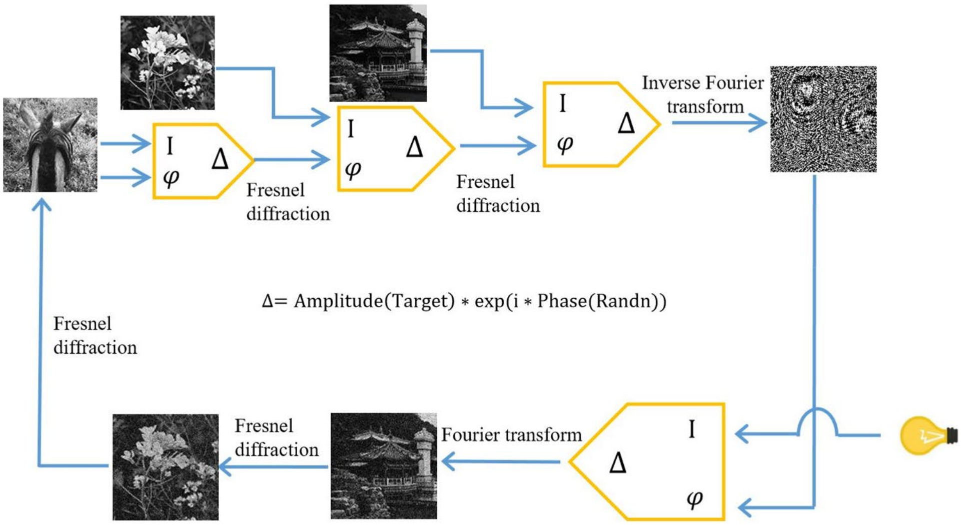


Fig. 4 The multi-image phase hologram iterative process

In other words, Image 1 is displayed when a beam of light passes through the phase hologram and is diffracted by a distance Z_1. Image 2 is displayed when the diffraction distance reaches Z_2. Image 3 is displayed when the diffraction distance reaches Z_3. Since images are imaged at different locations with a beam of light, different images at different locations do not interfere with each other. In this paper, Normal Gaussian random distribution matrices as the primary public key and different diffraction distances Z_n as assisted private keys ensure the security of information.

3 Numerical simulation

This paper strengthens the security of multi-image encryption technology by combining the G-S iterative algorithm with computational ghost imaging. This section takes three images as an example to further analyze PRA-GI. This section uses MATLAB R2019 software to achieve simulation. The object is 128 × 128 grayscale images. The simulation results are shown in Fig. 5. Figure 5a–c are compressed and encrypted into Fig. 5g (phase hologram). Figure 5g (phase hologram) is encrypted by computational ghost imaging. Computational ghost imaging reconstruction is performed by a public key. After reconstruction, this paper extracts the image by different private keys. The final decrypted images are shown in Fig. 5d–f. In Fig. 5, it can be found that the reconstructed images in this paper are clearer than Polarization-multiplexing ghost imaging (reference [23]).

3.1 Security

This section takes three images (letters *Z*, letters *W*, and letters *H* are shown in Fig. 6a) as an example. The objects are 64 × 64 grayscale images. Different decrypted images are obtained by correct keys, single keys, and wrong keys. This section demonstrates decrypted images of PRA-GI in case of normal, disclosure, and attack. The results are shown in Fig. 6b–d.

The histogram is a method of statistics, and the pixel histogram distribution of different images is different. In other words, when the pixel histogram distribution is different, the correlations between images are smaller. In this paper, the pixel histogram is obtained from the decrypted images by different keys. The pixel histogram is shown in Fig. 7.

In Fig. 6, it can be found that (1) the images can be reconstructed if the different private keys and public keys are used correctly. (2) Aliasing and crosstalk are not generated between multiple images in the algorithm of this paper. (3) When the key is compromised, the infringer can only obtain the corresponding image and cannot obtain the remaining images. Figure 6c shows that the diffraction distances Z_n as private keys have a certain effect but only play an auxiliary role. Therefore, we recommend that the primary public key and assisted private keys are used together.

In Fig. 7, the abscissa represents different gray levels in the image, and the ordinate represents the number of pixels in different gray levels. It can be observed from Fig. 7 that the infringer cannot obtain other images by the leaked or wrong key. (1) By comparison, it can be found that the pixel histogram of the image obtained by the leaked key is different from the pixel histogram of the remaining images. (2) The pixel histogram of the image obtained by the wrong key is very different from the pixel histogram of the original images.

This paper will analyze the correlation between the original image and the hologram by pixel correlation. The original images take the first image-letter Z as an example. The inter-pixel correlation of the original image and the hologram are shown in Figs. 8 and 9.

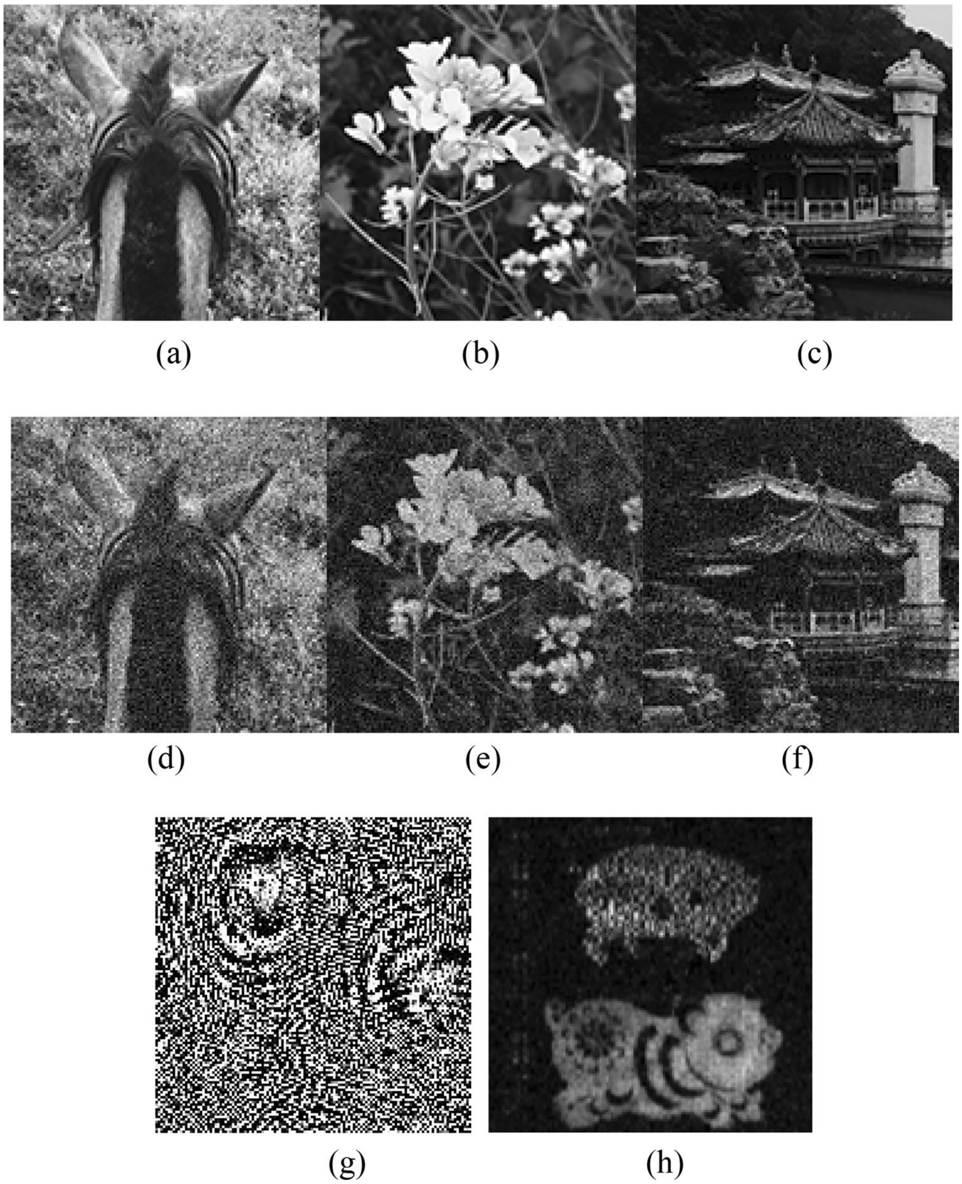


Fig. 5 Numerical simulation results: **a**–**c** is the original image, **d**–**f** is the final decrypted images, **g** is phase hologram. **h** is a reconstructed image in references [23] by polarization-multiplexing ghost imaging

In Figs. 8 and 9, it can be found that (1) the inter-pixel correlation of the original image is completely different from the pixel-to-pixel correlation of the encrypted image. There is a linear relationship between the inter-pixel correlations of the original image. The inter-pixel correlation of the encrypted image is random. (2) The encryption method in this paper plays a good and secure effect, which can hide and compress important information.

3.2 Multi-image encryption capability

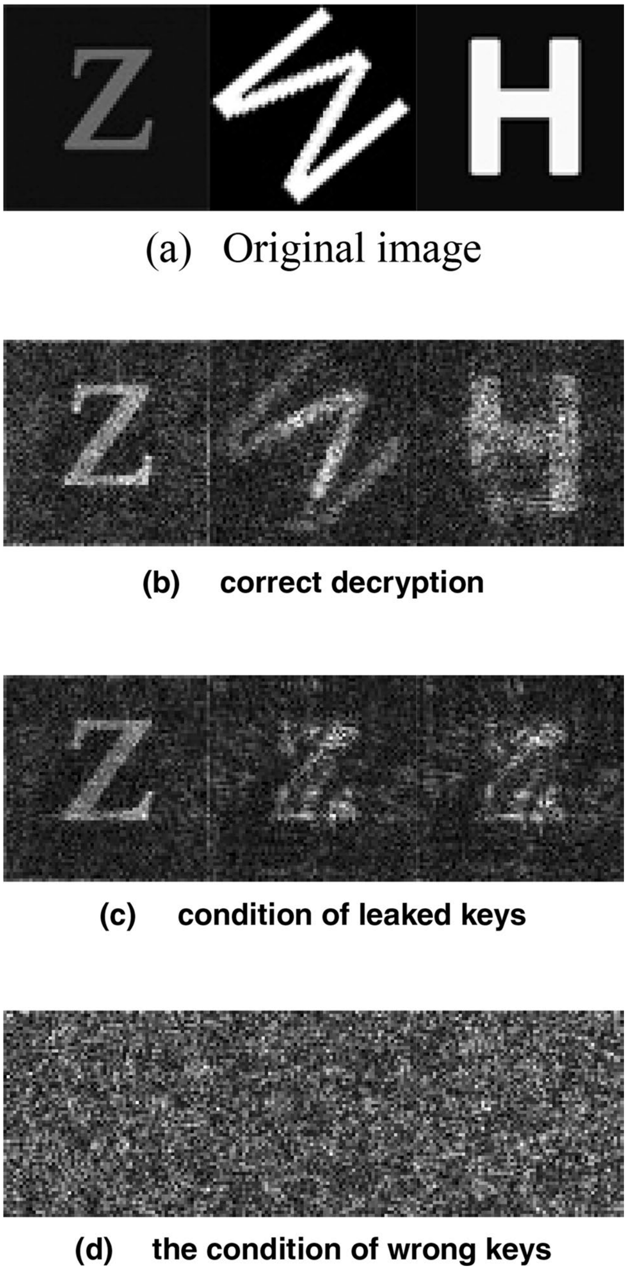
Encryption capability is one of the important indicators to measure multi-image encryption technology. This paper uses CC (correlation coefficient) to measure the correlation between the reconstructed image and the original image. CC reflects the relationship between two variables. the CC value is larger, the correlation between the reconstructed image and the original image is greater. Calculation expression of CC is as follows:

$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} X_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\ COV(x,y) = \frac{1}{N}\sum_{i=1}^{N} (X_i - E(x))(y_i - E(y)) \end{cases},$$

$$\mathrm{CC} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{8}$$

x and y represent two adjacent pixels in the image, CC is the correlation coefficient of two adjacent pixels.

According to the characteristics of Gerchberg–Saxton (G-S) iterative algorithm, if we use more iterations, the


(a) Original image

(b) correct decryption

(c) condition of leaked keys

(d) the condition of wrong keys

Fig. 6 Different decrypted images

more images will be encrypted. If computational ghost imaging uses more sampling number, the clearer reconstructed images will be. The correlation coefficient curve of decrypted images is shown in Fig. 10a and b, take “Z” “W” as an example to encrypt two images by PAR-GI. Take “Z” “W” and “H” as an example to encrypt three images by PAR-GI. Take “Z” “W” “H” and “S” as an example to encrypt four images by PAR-GI. Take “Z” “W” “H” “S” and “R” as an example to encrypt five images by PAR-GI.

In Fig. 10a the green and purple lines represent the reconstructed images of double-images encryptions. In Fig. 10a, the black, red, and blue lines represent the reconstructed images of triple-images encryptions. In Fig. 10a, it can be found that (1) under the same sampling and the small number of encrypted images, the quality of reconstructed images did not decline significantly with the increase of images. (2) This paper improves the quality of two and three decrypted images by increasing the number of samples in computational ghost imaging. PAR-GI can still achieve high-quality reconstruction, and with the increase in sampling, the distortion of reconstructed images is smaller and smaller, close to the original image, which indicates that this method is feasible in encrypting multi-image. In Fig. 10b, the black, red, blue, and green lines represent the reconstructed images of Four-images encryptions. In Fig. 10b, the purple, golden, cyan, brown, and orange lines represent the reconstructed images of five-images encryptions. Compared with Fig. 10a, Fig. 10b can be found that (3) when the number of images is more than three, the final reconstruction quality is closely related to the number of encrypted images. the overall reconstruction quality of the decrypted image decreases as the number of encrypted images increases. At the same time, with the increase of the number, the rising trend caused by sampling rate will not be obvious (4) when the number of images reaches 5, the last two final decrypted images will become blurred. Therefore, we recommend that the number of encrypted images be set to 3.

3.3 Information entropy

To objectively evaluate the effect of the encryption scheme, this paper analyzes the effect of PRA-GI by information entropy. Calculation expression of information entropy is as follows:

$$H = \sum_{i=0}^{255} P_{ij} \log P_{ij}, \tag{9}$$

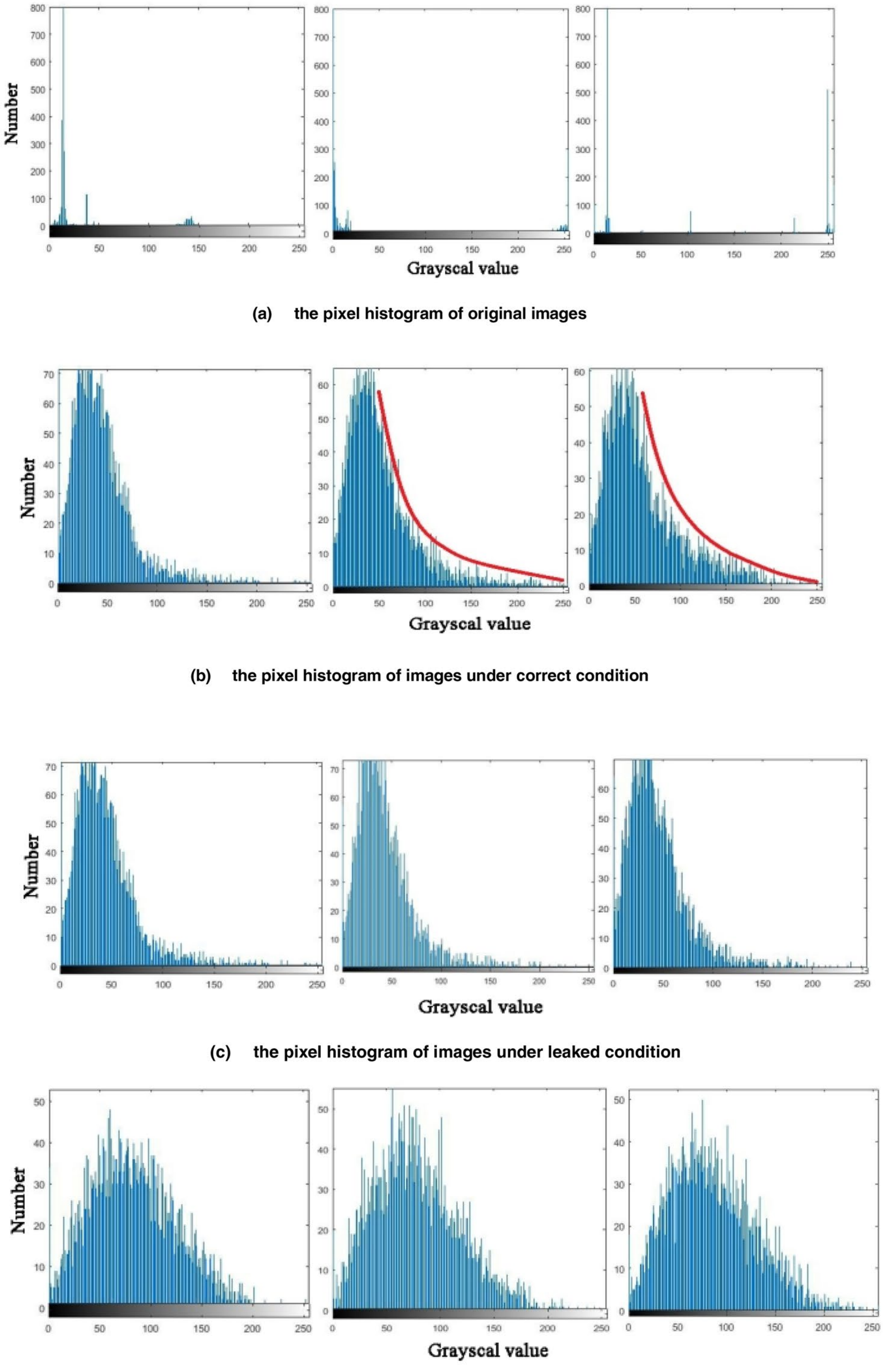
P_{ij} is the probability that a grayscale appears in the image, obtained by a gray histogram.

Information entropy can directly represent the amount of information included in the image. The smaller the information entropy value is, the more orderly the system is, and the higher the image quality is. Table 1 lists the information entropy values after encryption for three different images. The information entropy of the encrypted image in this paper is better than the reference [20] (the information entropy in reference [24] is 7.79,7.85,7.83).

3.4 Noise immunity

In the process of information transmission, it will inevitably be attacked by noise. To detect the anti-noise ability of the algorithm, we use PSNR (peak signal to noise

Fig. 7 Histogram of different key decryption



(a) the pixel histogram of original images

(b) the pixel histogram of images under correct condition

(c) the pixel histogram of images under leaked condition

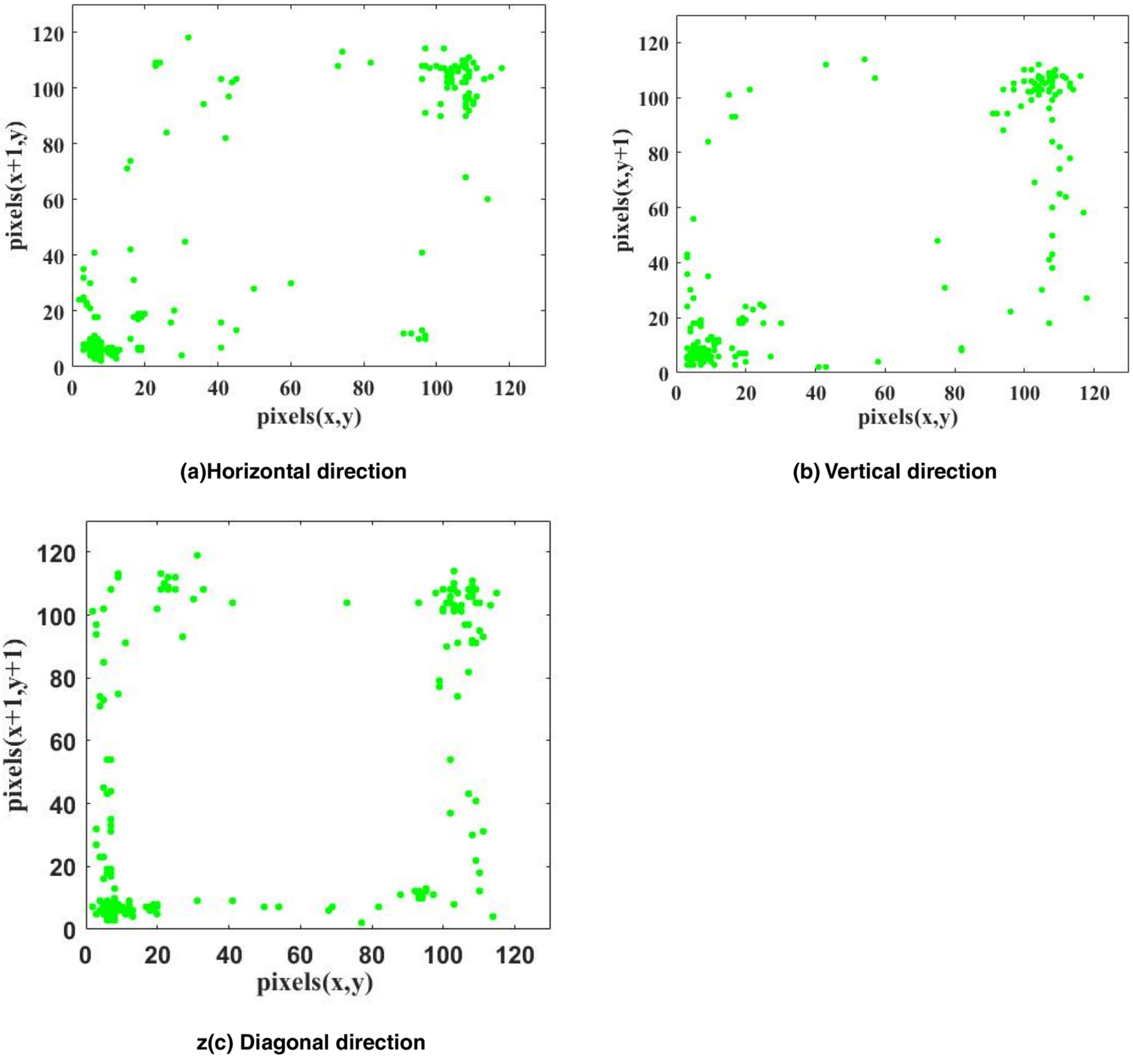
(d) the pixel histogram of images under the wrong condition

ratio) as the quantitative index. This paper analyzes the decrypted image (take "Flowers" as an example.) under different degrees of noise attack. The added noises are salt and pepper, Gaussian, and speckle noise.

The mathematical expression of PSNR is:

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{(2^m - 1)^2}{\mathrm{MSE}}\right], \tag{10}$$

MSE represents the mean square error between the original images and the decrypted images. m is the maximum pixel value.



(a)Horizontal direction

(b) Vertical direction

z(c) Diagonal direction

Fig. 8 The inter-pixel correlation of the original image

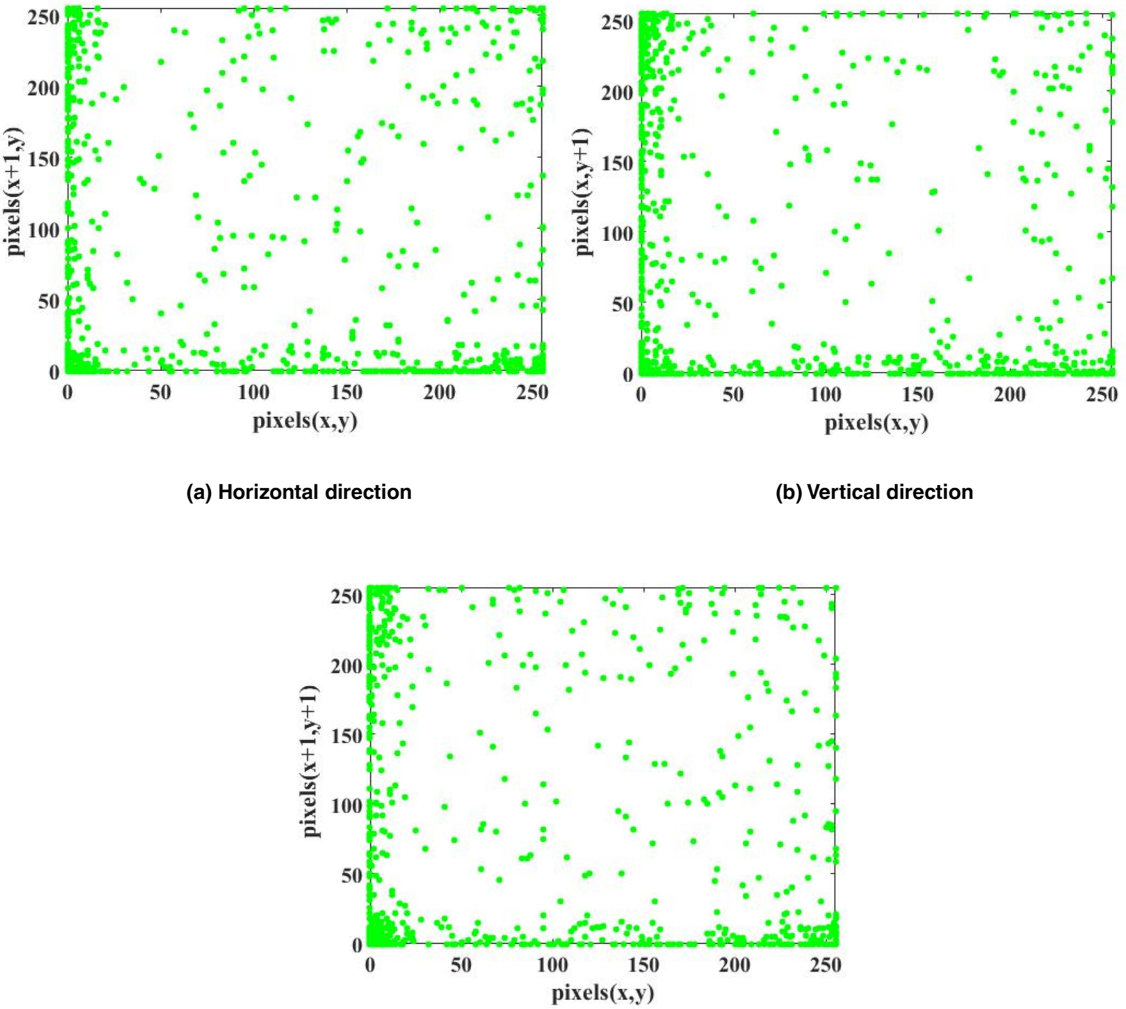
It is shown in Fig. 11 that PRA-GI has good robustness to three kinds of noise attacks and different noise attacks also have different reconstruction qualities for the decrypted images. Overall, with the increase of noise density, the PSNR of PRA-GI remains relatively stable, and the decrypted images are not disturbed by added noises.

Table 2a show a ciphertext image after adding salt and pepper noise with a noise density of 0.03; Table 2b and c shows, respectively, decrypted images after adding Gaussian noise; Table 2d shows a ciphertext image after adding Gaussian random noise with a mean of 0 and a variance of 0.03; Table 2e and f shows, respectively, decrypted images after adding Gaussian noise; Table 2g show a ciphertext image after adding a speckle noise with a mean of 0 and a variance of 0.03; Table 2h, i shows, respectively, decrypted images after adding speckle noise.

Decrypted images after Speckle noise attacks are better than images after Gaussian noise attacks and salt & pepper noise attacks. The decrypted images can still be distinguished, and the outline of images can be seen. The quality of decrypted images has not decreased significantly after noise attack, and the resolution of reconstructed images is acceptable.

In the process of encryption transmission of images, loss of information is inevitable, which affects the quality of the decrypted images. Therefore, the anti-cropping performance of the encryption method is analyzed to verify the robustness of the proposed method. The reconstructed effect is shown in Table 3.

As shown in Table 3, the direction of the cropping is different, and the reconstructed images will be different. the cropping at different directions, the resolution of the



(a) Horizontal direction

(b) Vertical direction

(c) Diagonal direction

Fig. 9 The inter-pixel correlation of the hologram

reconstructed image is not much different, indicating that the proposed method is robust to anti-cropping attacks.

4 Experimental verification

In the experimental verification section, this paper combines mathematical simulation and experimentation. The experiment is part of computational ghost imaging encryption for the holographic images. The main content of the experiment is that the holographic image modulated by a random matrix is received by the bucket detector and encrypted into a one-dimensional ciphertext. The rest of the algorithm is a mathematical simulation.

First encryption: original images are compressed and encrypted into a phase hologram by the G-S iterative algorithm.

Second encryption: this paper will perform a computational ghost imaging on phase holographic images. The experimental device of computational ghost imaging is shown in Fig. 12. Laser diode is the illumination source. The camera lens model is Nikon, AF-S DX 55-200 mm f/4-5.6 G ED (68 mm*79 mm). Bucket Detector is POINTGREY, BFLY-PGE-50H5M (29*29*30 mm). The capture card is M2i.2030-exp. This experiment uses DMD. The target object is a holographic image.

The experimental steps are:

Encryption phase: (1) this paper uses MATLAB software to generate random Gaussian matrices, the random Gaussian matrices are used as the random phase template in this experiment; (2) load these random phase templates onto the DMD chip; (3) place the phase hologram in front of the lens; (4) turn on the signal trigger and start the experiment; (5) the laser diode first illuminates the phase hologram and then

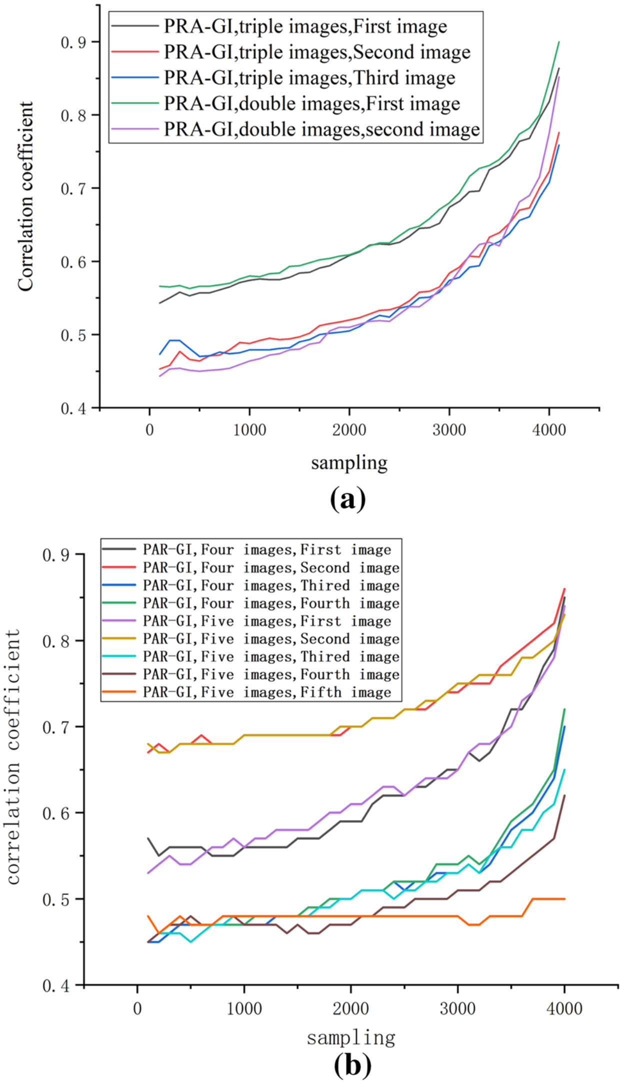
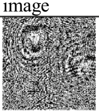
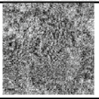


Fig. 10 Correlation coefficient of images

Table 1 Supplementary information entropy of PRA-GI

Information entropy	Holographic encrypted image	Original image		
6.65				
6.14				
6.51				

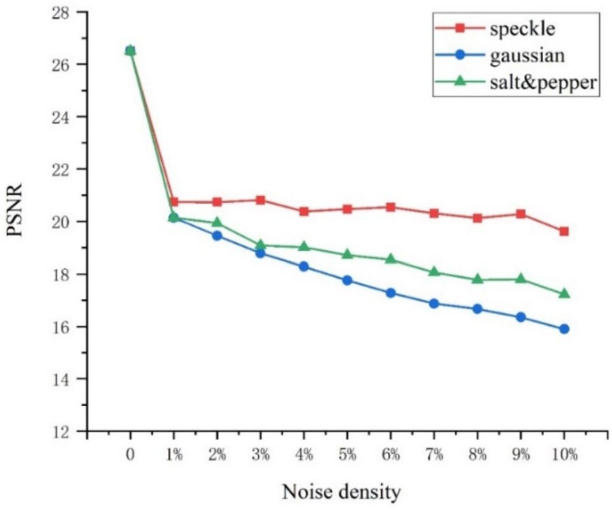
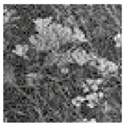
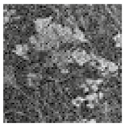
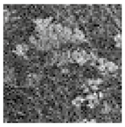
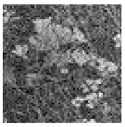


Fig. 11 Anti-noise ability

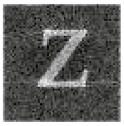
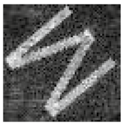
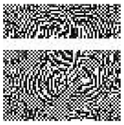
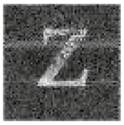
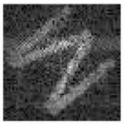
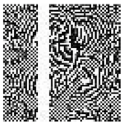
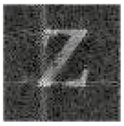
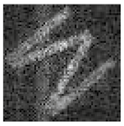
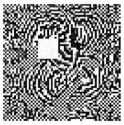
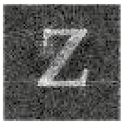
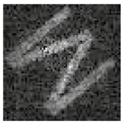
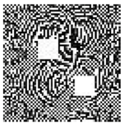
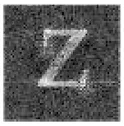
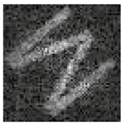
Table 2 Noise attack

Noise	Ciphertext	Decrypted Images of PRA-GI	
NO			
Salt&pepper	 (a)	 (b)	 (c)
Gaussian	 (d)	 (e)	 (f)
speckle	 (g)	 (h)	 (i)

illuminates the DMD chip; (6) the bucket detector receives 4096 times of light from the phase hologram.

Decryption phase: this paper associates the accumulated signal collected by the bucket detector with the

Table 3 Cropping attack

Position	Ciphertext	Reconstruction Images of PRA-GI	
No attack			
Rectangle cropping			
			
			
			

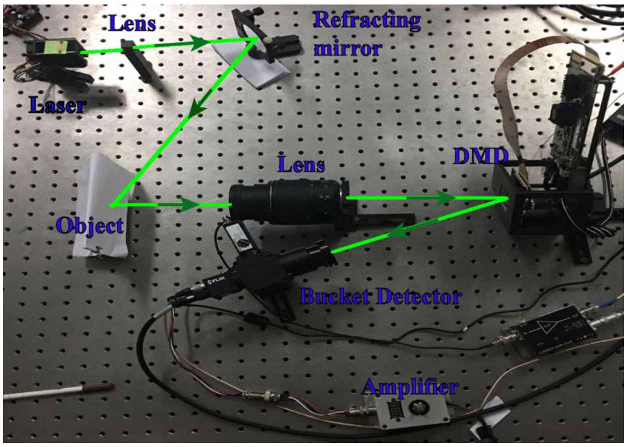


Fig. 12 Experimental device of computational ghost imaging

corresponding light intensity information. The reconstructed phase hologram is obtained by computational ghost imaging reconstruction. Different decrypted images are reconstructed by different diffraction distances.

This paper selects five images of the experiment. The results obtained are shown in Table 4. This paper uses CC and PSNR to objectively evaluate the effect as shown in Table 5.

In experimental results, Tables 4 and 5, it can be found that: (1) it takes 3–4 min for PRA-GI to encrypt 2 or 3 images. It takes 6–8 min for GI to encrypt 2 images, and it takes 9–12 min for GI to encrypt 3 images. It shows that the encryption time required by PRA-GI is much shorter than single image encryption, and the encryption efficiency is also higher than single image encryption. (2) The reconstructed images of PRA-GI can be distinguished, the outline of the images can be seen, and the resolution of reconstructed images is acceptable. (3) Compared with the results of GI, the objective indicators of PRA-GI are reduced, but the safety and efficiency of PRA-GI are much higher than GI. (4) The experimental results are the same as the numerical simulations, which proves that the method has certain feasibility.

5 Conclusion

This paper proposes a new encryption algorithm-Multi-image holographic encryption based on phase recovery algorithm and ghost imaging (PRA-GI). This paper studies its double encryption mechanism. It solves the problem of poor security and compressibility in the current multi-image double encryption algorithm. This paper combines computational ghost imaging with multi-image holographic iterative algorithms. This paper can greatly improve the compression of encrypted multi-image information, improve the security of multi-image double encryption, and achieve secure and accurate information encryption. This method can achieve multiple-image encryption. This method does not cause aliasing and cross-talk between multiple images. PRA-GI can send different ciphertexts to different authorized users, which has broad prospects.

Table 4 Experimental results

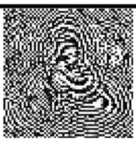
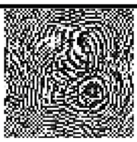
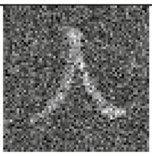
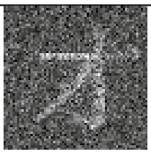
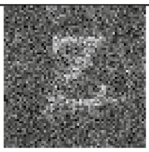
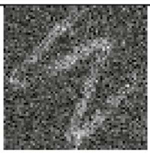
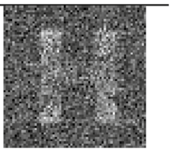
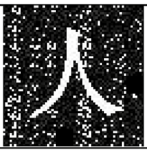
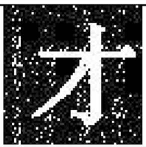
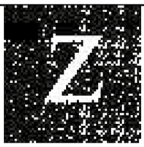
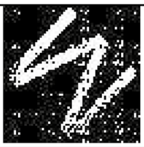
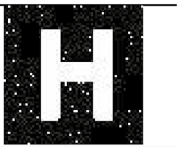
Original image	 Chinese character	 Chinese character	 Alphabet: Z	 Alphabet: W	 Alphabet: H
Holographic encrypted image					
Experimental result	 Chinese character	 Chinese character	 Alphabet: Z	 Alphabet: W	 Alphabet: H
Ghost imaging of Single image					

Table 5 Objective evaluation

Experimental result	Chinese character “人”	Chinese character “才”	Alphabet: *Z*	Alphabet: *W*	Alphabet: *H*
Objective evaluation					
CC of PRA-GI	47.00%	51.53%	42.33%	49.43%	44.37%
PSNR of PRA-GI	13.38	11.07	13.17	9.63	9.09
CC of GI	57%	79%	59%	77%	94%
PSNR of GI	10.12	12.43	10.09	11.62	17.27

References

1. D.N. Klyshko, Two-photon light: influence of filtration and a new possible EPR experiment. Phys. Lett. A **128**(3-4), 133–137 (1988)
2. J.H. Shapiro, Computational ghost imaging. Phys. Rev. A **78**(6), 061802 (2008)
3. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerc, J. Lancis, Optical encryption based on computational ghost imaging. Opt. Lett. **5**(14), 2391–2393 (2010)
4. Z. Chi, G. Shuxu, C. Junsheng, G. Jian, G. Fengli, Object reconstitution using pseudo-inverse for ghost imaging. Opt. Express **22**(24), 30063–30073 (2014)
5. W. Gong, High-resolution pseudo-inverse ghost imaging. Photon. Res. **3**(5), 234–237 (2015)
6. G. Ying, Q. Wei, X. Shen, A two-step phase-retrieval method in fourier-transform ghost imaging. Opt. Commun. **281**(20), 5130–5132 (2008)
7. Z. Zhang, S. Jiao, M. Yao, X. Li, J. Zhong, Secured single-pixel broadcast imaging. Opt. Express **26**(11), 14578–14591 (2018)
8. S. Jiao, J. Feng, Y. Gao, T. Lei, X. Yuan, Visual cryptography in single-pixel imaging. Opt. Express **28**(5), 7301–7313 (2020)
9. W. Chen, X. Chen, Ghost imaging for three-dimensional optical security. Appl. Phys. Lett. **103**(22), 221106 (2013)
10. W. Chen, X. Chen, Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption. EPL **109**(1), 14001 (2015)
11. J.J. Wu, W.X. Zhen, J.L. Zheng, W. Liu, Y. Zhang, S. Liu, Multiple-image encryption based on computational ghost imaging. Opt. Commun. **359**, 38–43 (2016)
12. I.H. Lee, M. Cho, Double random phase encryption using orthogonal encoding for multiple-image transmission. J. Opt. Soc. Korea **18**(3), 201–206 (2014)
13. X. Li et al., Multiple-image encryption based on compressive ghost imaging and coordinate sampling. IEEE Photon. J. **8**(4), 1–11 (2017)
14. L. Sui, X. Zhao, An optical multiple-image authentication based on transport of intensity equation. Opt. Lasers Eng. **116**, 116–124 (2019)

15. N. Zhou, X. Yan, Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. Q. Inf. Process. **17**, 338 (2018)
16. L. Junhui, Y. Dongyue, L. Bin, W. Guohua, Y. Longfei, G. Hong, Image quality recovery in binary ghost imaging by adding random noise. Opt. Lett. **42**(8), 1640–1643 (2017)
17. B. Luo et al., Orthonormalization method in ghost imaging. Opt. Express **26**(18), 23093–23106 (2018)
18. H.C. Liu, J. Xiong, Properties of high-order ghost imaging with natural light. J. Opt. Soc. Am. A **30**(5), 956 (2013)
19. B. Luo, G. Wu, L. Yin, Lensless two-color ghost imaging from the perspective of coherent-mode representation. Chin. Phys. B **9**, 313–318 (2018)
20. J. Chen, W. Gong, S. Han, Sub-Rayleigh ghost imaging via sparsity constraints based on a digital micro-mirror device. Phys. Lett. A **377**(31), 1844–1847 (2013)
21. H. Heyan, Z. Cheng, G. Wenlin, S. Lijun, Block matching low-rank for ghost imaging. Opt. Express **27**(26), 38624–38634 (2019)
22. R.W. Gerchberg, A pratical algorithm for the determination of phase from image and diffraction plane pictures. Optik **35**, 237 (1972)
23. S. Dongfeng, Z. Jiamin, H. Jian, Polarization-multiplexing ghost imaging. Opt. Lasers Eng. **102**, 100–105 (2018)
24. A.A. Karawia, Encryption algorithm of multiple-image using mixed image elements and two-dimensional chaotic economic map. Entropy **20**, 801 (2018)