

Ghost imaging-based optical cryptosystem for multiple images using integral property of the Fourier transform

Yi Kang(康祎), Leihong Zhang(张雷洪), Hualong Ye(叶华龙), Dawei Zhang(张大伟), and Songlin Zhuang(庄松林)
Citation: Chin. Phys. B, 2021, 30 (**12**): 124207. DOI: 10.1088/1674-1056/ac0815
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Computational ghost imaging with deep compressed sensing

Hao Zhang(张浩), Yunjie Xia(夏云杰), and Deyang Duan(段德洋)
Chin. Phys. B, 2021, 30 (**12**): 124209. DOI: 10.1088/1674-1056/ac0042

High speed ghost imaging based on a heuristic algorithm and deep learning

Yi-Yi Huang(黄祎祎), Chen Ou-Yang(欧阳琛), Ke Fang(方可), Yu-Feng Dong(董玉峰), Jie Zhang(张杰), Li-Ming Chen(陈黎明), and Ling-An Wu(吴令安)
Chin. Phys. B, 2021, 30 (**6**): 064202. DOI: 10.1088/1674-1056/abea8c

Handwritten digit recognition based on ghost imaging with deep learning

Xing He(何行), Sheng-Mei Zhao(赵生妹), and Le Wang(王乐)
Chin. Phys. B, 2021, 30 (**5**): 054201. DOI: 10.1088/1674-1056/abd2a5

Compressed ghost imaging based on differential speckle patterns

Le Wang(王乐), Shengmei Zhao(赵生妹)
Chin. Phys. B, 2020, 29 (**2**): 024204. DOI: 10.1088/1674-1056/ab671a

Experimental demonstration of influence of underwater turbulence on ghost imaging

Man-Qian Yin(殷曼倩), Le Wang(王乐), Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2019, 28 (**9**): 094201. DOI: 10.1088/1674-1056/ab33ee

---

Ghost imaging-based optical cryptosystem for multiple images using integral property of the Fourier transform*

Yi Kang(康祎), Leihong Zhang(张雷洪)†, Hualong Ye(叶华龙), Dawei Zhang(张大伟), and Songlin Zhuang(庄松林)

University of Shanghai for Science and Technology, Shanghai 200093, *China*

(Received 13 April 2021; revised manuscript received 2 June 2021; accepted manuscript online 4 June 2021)

A novel ghost imaging-based optical cryptosystem for multiple images using the integral property of the Fourier transform is proposed. Different from other multiple-image encryption schemes, we mainly construct the modulation patterns related to the plaintext images to realize the encrypted transmission of multiple images. In encryption process, the first image is encrypted by the ghost imaging encryption scheme, and the intensity sequence obtained by the bucket detector is used as the ciphertext. Then modulation patterns of other images are constructed by using the integral property of the Fourier transform and used as the keys. Finally, the ciphertext and keys are transmitted to the receiver to complete the encryption process. During decryption, the receiver uses different keys to decrypt the ciphertext and gets different plaintext images, and decrypted images have no image aliasing problem. Experiments and simulations verify the feasibility, security, and robustness of the proposed scheme. This scheme has high scalability and broad application prospect, which provides a new idea for optical information encryption.

Keywords: ghost imaging, image encryption, Fourier transform

PACS: 42.30.–d, 42.30.Va, 42.30.Wb **DOI:** 10.1088/1674-1056/ac0815

1. Introduction

With the development of science and technology, information exchange becomes more and more frequent, but with the emergence of "PRISM", people pay more and more attention to the security of information. Optical information security technology has been the focus of attention and studied because of its high speed, parallelism, multi-dimensionality, and other characteristics.[1,2] As an information carrier, image has the advantages of a large amount of information, specific, vivid images, *etc*., so image encryption is an important part of optical information security technology.[3,4]

In 1995, Refregier and Javidi realized optical image encryption by using double random phase encoding (DRPE).[5] DRPE is easy to operate and can be combined with other technologies, which promotes the rapid development of optical image encryption technology. With the progress and development of technology, multiple-image encryption has been deeply studied to meet the growing needs of people.[6–9] However, the existing optical image encryption technology requires high precision of the optical instrument, and the ciphertext is expressed by complex amplitude, which is not conducive to transmission and storage. Therefore, a simple and fast optical encryption method is urgently needed, while ghost imaging technology provides a new way to solve this problem.

Different from traditional imaging techniques, ghost imaging mainly uses the higher-order correlation of the light field to obtain the spatial and phase distribution information of the object, and can realize single-pixel imaging.[10,11] Ghost imaging has received widespread attention since it was proposed. The research on ghost imaging is also gradually deepened from the aspects of reconstruction algorithm, experimental device, and modulation pattern.[12–15] In 2010, Pere Clemente took the lead in combining optical encryption and ghost imaging, opening the door for the application of ghost imaging in information security.[16] Tanha used the ghost imaging technique to encrypt the discrete cosine transform coefficients of the image.[17] Kong *et al.* realized optical image encryption by controlling the initial coordinates of the light source.[18] Chen *et al.* proposed an information authentication method based on ghost imaging.[19] Zhao *et al.* encrypted information by changing the order of modulation patterns of ghost imaging.[20] To further improve the encryption efficiency of ghost imaging, Wu *et al.* took the lead in using position multiplexing to realize multiple-image encryption of ghost imaging.[21] Meng *et al.* applied row scanning, logistic map, lifting wavelet transform, and other schemes to ghost imaging encryption scheme to realize multiple-image encryption.[22–24] Shi *et al.* used encoded multiplexing patterns to illuminate multiple objects to achieve the purpose of multiple-image encryption.[25]

However, for multiple-image encryption, the problem of image aliasing is inevitable, which affects the quality of decryption. To solve this problem, we propose a novel multiple-

*Project supported by the Natural Science Foundation of Shanghai, China (Grant No. 18ZR1425800) and the National Natural Science Foundation of China (Grant Nos. 61875125 and 61775140).

†Corresponding author. E-mail: lhzhang@usst.edu.cn

© 2021 Chinese Physical Society and IOP Publishing Ltd

image encryption scheme based on ghost imaging. In this scheme, firstly, an image is encrypted by the ghost imaging encryption scheme and the generated bucket detector values as ciphertext. Then modulation patterns of other images are constructed by using the integral property of the Fourier transform and used as the key of the corresponding image. Finally, the ciphertext and keys are transmitted to the receiver to complete the encryption process. The receiver uses different keys to decrypt the ciphertext, different plaintext images can be obtained. This scheme differs from other schemes in that it is mainly the ciphertext determines the key, not the key determines the ciphertext. Ciphertext generation only requires one encryption. This scheme can improve the encryption efficiency and solve the problem of image crosstalk. Experiments and simulations verify the effectiveness, safety, and robustness of this scheme. This scheme also can be adopted for one-encryption and multi-decryption scenario, such as multi-level information authentication system or one-to-many encryption transmission.

2. Image encryption scheme based on computational ghost imaging

The traditional ghost imaging encryption scheme is shown in Fig. 1. Alice wants to encrypt the plaintext information $T(x,y)$ and transmit it to Bob. She uses the computational ghost imaging experiment device shown in Fig. 1(b). A spatially coherent monochromatic laser beam passes through a spatial light modulator (SLM), which introduces an arbitrary phase-only mask, with phase values uniformly distributed in the range $[0-2\pi]$. The modified beam $I_i(x,y)$ illuminates the object, and the transmitted light is collected by a bucket detector, a bucket detector value D_i is generated, as shown below:

$$D_i = \int I(x,y)T(x,y)\,\mathrm{d}x\mathrm{d}y. \tag{1}$$

This operation is repeated N times for N different phase profiles $\varphi_i(x,y)$. Next, a series of bucket detector values are shared with Bob using a public channel. And N different phase profiles are transmitted to Bob through a secure channel. Bob calculates the corresponding optical field intensity distribution of each phase profile according to Fresnel diffraction, as shown below:

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

where $E_{\mathrm{in}}(x,y)$ is the complex field of the coherent light beam, $h_z(x,y)$ is the Fresnel propagation kernel at distance z and $\otimes$ denotes the two-dimensional (2D) convolution operation. According to the bucket detector values D and intensity distribution $I_i(x,y)$, the object information can be recovered through the following liner operation, where $\langle\cdot\rangle$ denotes the average calculation:

$$T'(x,y) = \langle I_i(x,y)D_i\rangle - \langle I_i(x,y)\rangle\langle D_i\rangle. \tag{3}$$

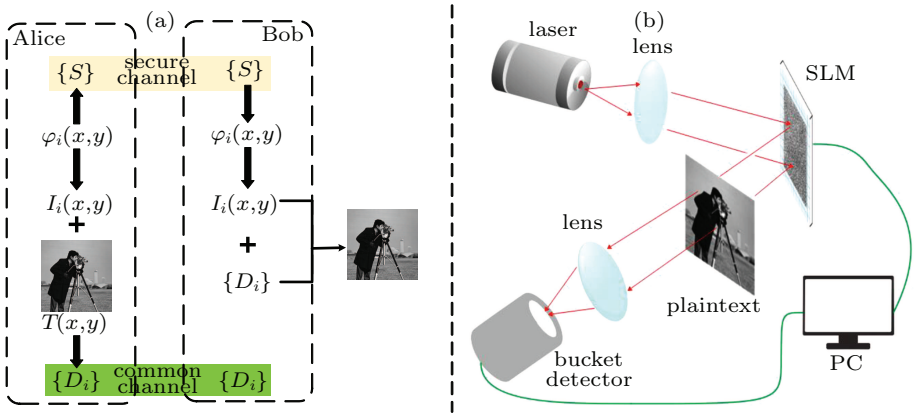


Fig. 1. Scheme of the encryption method based on computational ghost imaging: (a) block diagram showing encryption/decryption procedure; (b) experiment setup of computational ghost imaging.

3. Multiple-image encryption scheme based on computational ghost imaging

3.1. Key generation

In previous studies, for ghost imaging encryption schemes, the modulation patterns were always constructed firstly, and then the plaintext information was encrypted. Especially for multiple-image encryption, multiple modulation patterns need to be constructed. This means that the ciphertext is always determined by the key, so, can the key be designed depends on the ciphertext?

Assuming that the target image $T(x,y)$ is illuminated by its modulation pattern $I_i(x,y)$, the ciphertext D_i can be obtained. Can the modulation pattern $H_i(x,y)$ be designed for the target image $M(x,y)$ so that its ciphertext is also D_i? As shown in Eq. (4).

$$\begin{aligned}\int I_i(x,y)T(x,y)\,\mathrm{d}x\mathrm{d}y &= D_i \\ = \int H_i(x,y)M(x,y)\,\mathrm{d}x\mathrm{d}y.\end{aligned} \tag{4}$$

According to the integral property of the Fourier transform[26]

$$\int H_i(x,y)M(x,y)\mathrm{d}x\mathrm{d}y = \mathrm{FT}[H_i(x,y)M(x,y)](\varepsilon,\eta)|_{\varepsilon=0,\eta=0}, \quad (5)$$

where FT$[\cdot]$ is the Fourier transform. And equation (4) could be rewritten as

$$\mathrm{FT}[H_i(x,y)M(x,y)](\varepsilon,\eta)|_{\varepsilon=0,\eta=0} = D_i. \quad (6)$$

According to the above equation, this issue could be converted to an equivalent problem, that is, given target image $M(x,y)$ as the constraint in the signal domain, how does one design the $H_i(x,y)$ to satisfy the constraint in the Fourier domain as Eq. (6)? It can be shown in Fig. 2. IFT is inverse Fourier transform.

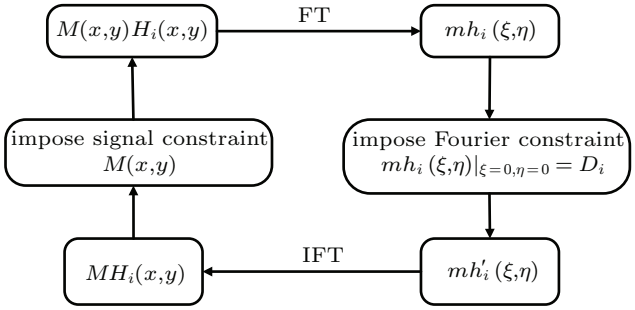


Fig. 2. Block diagram of the constraint in the signal and Fourier domain.

So, this problem can be understood as the problem of recovering phase information by using intensity information, that is a phase retrieval problem. Therefore, when image information $M(x,y)$ and ciphertext D_i are given, the modulation pattern can be generated in the following ways:

Step 1 Generating a modulation pattern $H_{i-1}(x,y)$ for initialization;

Step 2 Performing the Fourier transform for $H_{i-1}(x,y)M(x,y)$ and get $mh_{i-1}(\varepsilon,\eta)$. With ciphertext D_i as constraint, equation (6) is applied to the spectrum to generate a new Fourier spectrum $mh_i(\varepsilon,\eta)$.

Step 3 Inverse Fourier transform the modified Fourier spectrum $mh_i(\varepsilon,\eta)$ back to the signal domain and generate a modulation pattern $H_i(x,y)$ according to

$$H_i(x,y) = \frac{mh_i(\xi,\eta)}{M(x,y)+eps}. \quad (7)$$

According to the number of ciphertexts, the modulation pattern can be generated according to the cycle shown in Fig. 3. This assumes that the number of ciphertexts is K.

To this point, we can find that for a given image, we can construct special modulation patterns to meet the requirements of ciphertext. That is, we can design keys according to the ciphertext.

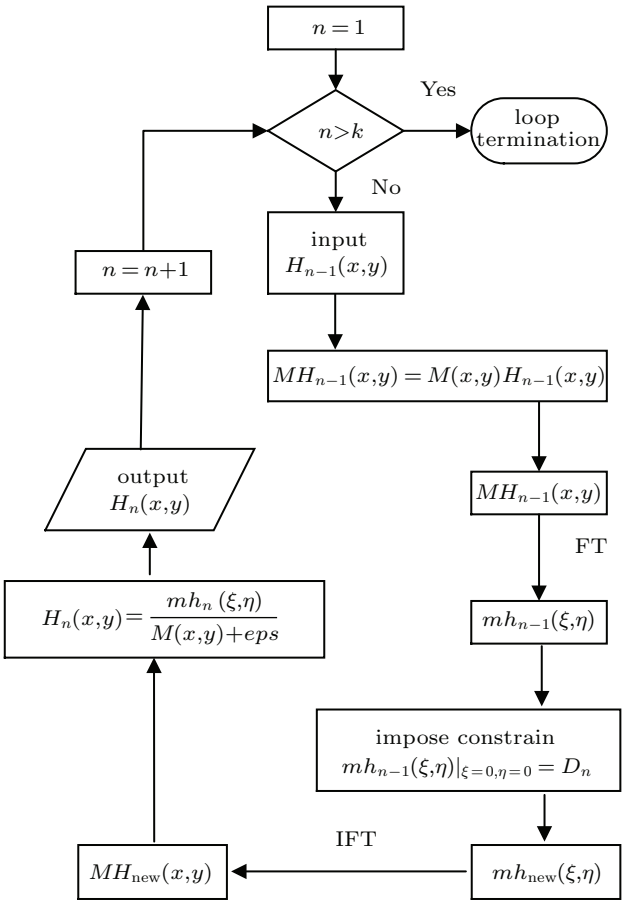


Fig. 3. Flow chart of modulation patterns generation.

3.2. Encryption process

According to the principle of modulation patterns generation, we propose a novel multiple-image encryption scheme based on ghost imaging, as shown in Fig. 4. In this scheme, different keys are designed to decrypt the same ciphertext and different images can be obtained.

Step 1 A series of random patterns K_1 are used to encrypt a single plaintext image T, and a series of bucket detector values D are obtained as ciphertext.

Step 2 The ciphertext as the constraint is used to generate modulation patterns of different images according to the way shown in Fig. 3. And these modulation patterns are used as the keys of corresponding images.

Step 3 The ciphertext D and the generated keyring $\{K_1, K_2, \ldots, K_i\}$ are transmitted to the receiver to complete the encryption process.

3.3. Decryption process

After receiving the ciphertext and the keyring, the receiver can extract different keys from the keyring to decrypt the ciphertext and obtain different plaintext images from it. The decryption method can be seen in Eq. (3).

But the correlation algorithm requires a large amount of ciphertext information, which means multiple sampling is needed. This also leads to substantially reduced decryption

efficiency. To solve this problem, the compressive sensing algorithm is used for decryption.[27] If we spread a modulation pattern in a row as a row vector Ir, then a series of modulation patterns can be considered a measurement matrix in compressive sensing. So, the decryption process can be obtained by solving a convex optimization program that is expressed as

$$Tc_{cs} = \arg\min : \|Tc\|_1 \quad \text{s.t} : D = Ir \times Sc, \tag{8}$$

where $\|\cdot\|$ is the l_1-norm. The application of the compressive sensing algorithm improves the reconstruction quality of plaintext image and can reconstruct plaintext image under the condition of less ciphertext.

The MGI mainly realizes the secure transmission of multiple-image by constructing the modulation patterns of different images. In encryption process, it only needs to encrypt an image instead of all images. Ciphertext data is small and easy to be transmitted. In decryption process, different images can be decrypted only with corresponding modulation patterns, and the decryption algorithm is simple.

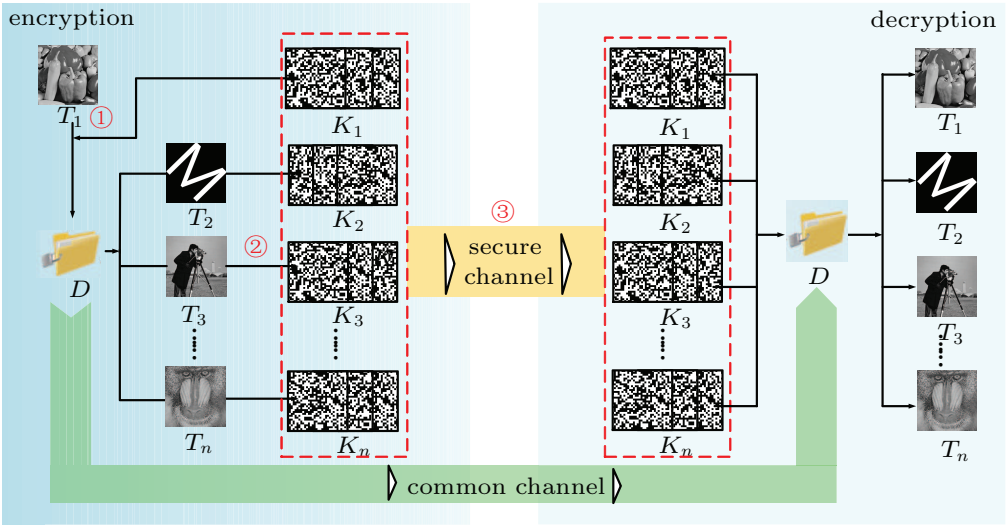


Fig. 4. Encryption and decryption process of MGI.

4. Simulation

Firstly, the proposed scheme is analyzed by simulation. The simulation is carried out under a 64-bit Windows 10 system, and the platform is MATLAB 2019b. The size of the plaintext image is 64×64 pixels. The sampling ratio is 100%, the sampling ratio is defined as the ratio of sampling number and plaintext image pixels (*i.e.*, the sampling numbers are 4096, which also means that the modulation patterns are 4096). The decryption algorithm is the orthogonal matching pursuit algorithm in the compressive sensing algorithm. To evaluate the decryption quality objectively, the correlation coefficient (CC) is used as the objective evaluation standard to evaluate the similarity between the original image and the decrypted image.[28] The closer to 1 the value of the CC is, the better the reconstruction effect is. Where x and y represent the original plaintext image and the decrypted image respectively.

$$\begin{cases} E(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N} x, \\ D(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N} (x_i - E(x))^2, \\ \mathrm{Cov}(x,y) = \dfrac{1}{N}\sum\limits_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \\ \mathrm{CC} = \dfrac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \end{cases} \tag{9}$$

4.1. Feasibility analysis

Four different images are used as plaintext information, including binary images and grayscale images. We use Hadamard patterns as the key to encrypt the first plaintext image and get the ciphertext. Ciphertext is a series of meaningless intensity sequences, as shown in Fig. 5(i). Then, the keys of the other three images are generated by using the method of this paper and the obtained ciphertext. Finally, the ciphertext and keys are transmitted to the receiver to complete the image encryption.

The receiver uses different keys to decrypt the same ciphertext to obtain different reconstructed plaintext images. Figure 5 shows that CC between the four decrypted images and the original plaintext images are 0.9875, 09975, 0.9462, and 0.9204, respectively. Obviously, the plaintext information can be reconstructed well. The first image uses the Hadamard pattern as the key, so it has a better reconstruction effect (The Hadamard patterns are a deterministic orthogonal set, in principle, the image can be reconstructed without noticeable difference from the target image, when is fully sampled). The second image as a binary image has a higher sparsity, it can be reconstructed better under the same sampling ratio. The third and fourth image are not special in terms of key and sparsity,

so the reconstruction effect is worse than the first two, but the contrasts and details can still show the plaintext information very well. The results show that when only a single ciphertext is transmitted, different plaintext information can be decrypted with different keys, and all images have a good reconstruction effect.

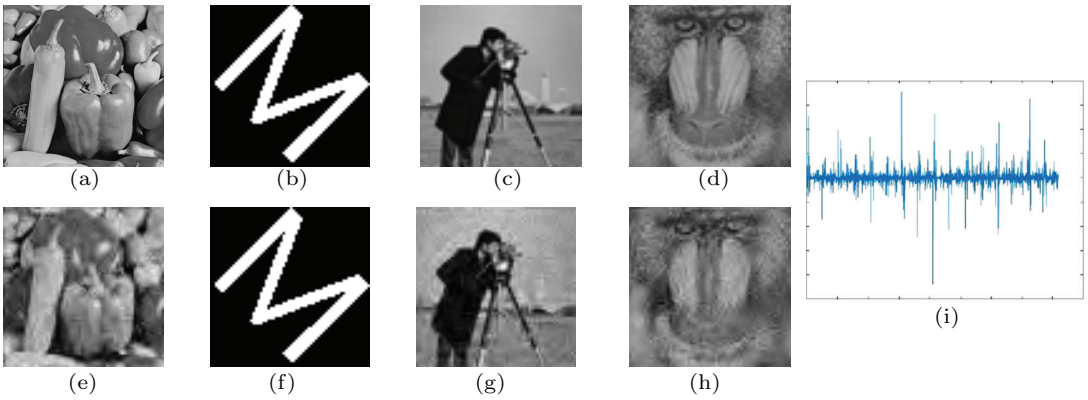


Fig. 5. Panels (a)–(d) are the original plaintext images; panels (e)–(h) are the decrypted images; panel (i) is the ciphertext.

4.2. Security analysis

For an encryption system, ensuring the security of information is the prerequisite of system effectiveness. For an attacker, if the statistics law of information in ciphertext is the same as the plaintext, the attacker can break out the encrypted information through the ciphertext-only attack. As shown in Table 1, for different plaintext information, these corresponding ciphertext displays a similar tendency. Obviously, it is difficult for an attacker to analyze valid information from the ciphertext, ensuring the security of the plaintext. MGI fully realizes the diffusion and confusion of plaintext information.

In cryptography, according to the relationship between plaintext and ciphertext, the attacker can obtain the keys through the iterative algorithm, and then break out the encryption system. We use the known-plaintext attack (KPA) of paper[29] to further analyze the security of MGI. The idea of the attack scenario is that for a sample, a fixed modulation pattern illuminates multiple images in sequence and obtains the corresponding bucket detector values, which can also be understood as multiple images illuminate a fixed modulation pattern. If information of multiple images is known, the modulation pattern can be obtained by solving linear equations. After many cycles, keys can be obtained.

Table 1. Histogram of plaintext and ciphertext.

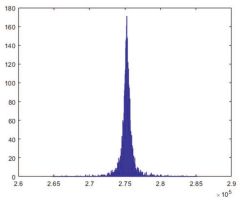
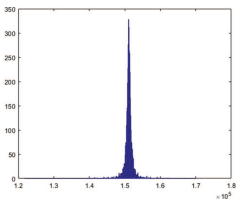
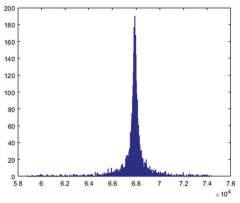
Plaintext	Ciphertext
	
	
	



Fig. 6. KPA results. Panel (a) is the cracked information of the first image under KPA when the modulation patterns are fixed; Panels (b)–(d) are the cracked information of other images under KPA.

As shown in Fig. 6, for the fixed modulation patterns, KPA can be obtained keys of the first image and the first image can be decrypted. However, the information of the other three images cannot be obtained. Because the first image uses fixed patterns (*i.e.*, keys are fixed), which can be cracked, but the keys of other images are related to the image itself and cannot

be cracked, effectively guaranteeing the validity of most information. For chosen-ciphertext attack and known-plaintext attack, only the key of the first image can be cracked, but the keys of other images cannot be cracked. It is worth stating that we are simply assuming that the key to the first image is fixed, and that if it is random, the security of the first image is guaranteed.

Based on the above analysis, it is obvious that MGI can effectively resist various attack modes.

4.3. Robustness analysis

During the encryption and transmission of information, the effect of noise and the loss of information are inevitable. Therefore, a qualified encryption system needs strong robustness.

In practical applications, the thermal noise caused by optical devices and interference caused by the non-ideal channel will affect the information. Therefore, we introduce different types of noise to verify the anti-noise ability of MGI. For thermal noise caused by optical devices, we introduce Gaussian noise with different signal-to-noise ratios (SNR) in each sampling process. The higher the signal-to-noise ratio, the weaker the noise. For the interference caused by the non-ideal channel, we add multiplicative noise to the transmitted ciphertext. We suppose the noise is added to the ciphertext in the following form:

$$D' = D + i \cdot D, \tag{10}$$

where i is represented as a random noise with mean 0 and different variances, and D is ciphertext information.

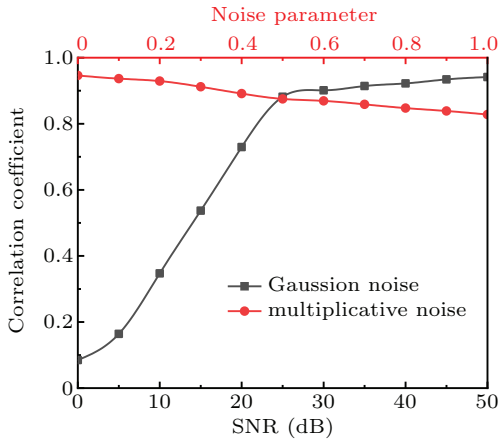


Fig. 7. CC between the plaintext and reconstruction information under different types of noise.

Figure 7 shows that for Gaussian noise, with the increase of SNR, the reconstruction quality is gradually improved. The reconstruction result is good when the SNR is 20. For multiplicative noise, with the increase of noise intensity, the reconstruction effect shows a downward trend. When the noise is sufficiently large, the CC between the decrypted image and the original image is still above 0.8. The results show that the thermal noise generated by the optical devices in the system has some influence on the decryption, the impact of interference caused by the non-ideal channel on the decryption is relatively small. The interruption of the channel or the interference of the attacker may cause the loss of ciphertext, and thus affect the decryption effect. In the following, different numbers of ciphertext are cropped to verify capacity of MGI to resist to the ciphertext loss. Take a binary image as an example, as shown in Fig. 8, as the loss of ciphertext gradually increases, the difference between the decrypted information and the original information becomes larger. However, when the loss ratio of the ciphertext is 50%, the valid information can still be decrypted. The results show that MGI can resist the loss of ciphertext effectively.

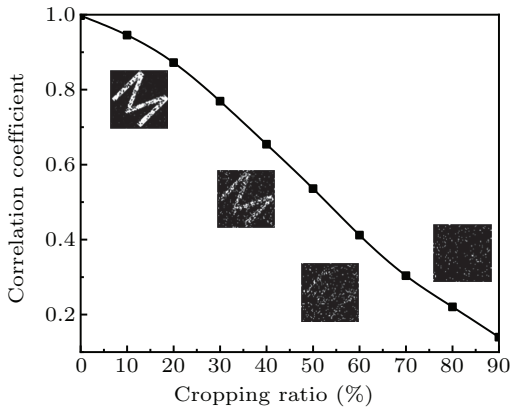


Fig. 8. CC between the plaintext and reconstruction information under different cropping ratios.

The results of noise attack and cropping attack show that MGI can resist noise interference and ciphertext loss effectively. MGI has strong robustness.

4.4. Information capacity analysis

As a multiple-image encryption scheme, whether the increase of data quantity will cause image aliasing is a problem to be considered. We verify this problem by increasing the number of images and compare the reconstruction results of MGI with multiple-image encryption scheme based on ghost imaging and position multiplexing (PM-MGI) and multiple-image encryption scheme based on lifting wavelet transform and ghost imaging (LWT-MGI) in paper.[21,22] Multiple images adopted are binary images.

Figure 9 shows that with the increase in the number of encrypted images, CC of LWT-MGI and PM-MGI shows a downward trend. Especially for PM-MGI, the decrypted quality drops seriously when the number of images to be encrypted increases. For MGI, the increase in the number of images does not affect the decrypted effect, which ensures the accuracy of the decrypted information while improving the number of encrypted images. Because for MGI, the realization of multiple-image encryption and decryption is based on the generation

of keys, and there is no information overlap in encryption process. For PM-MGI, position multiplexing leads to ciphertext aliasing. Therefore, the increase in the number of images will affect the decryption effect. For LWT-MGI, this method mainly uses image sparsity to achieve multiple-image encryption, but with the increase of the number of images, less detail is retained after each image sparse, which affects the quality of the reconstruction image.

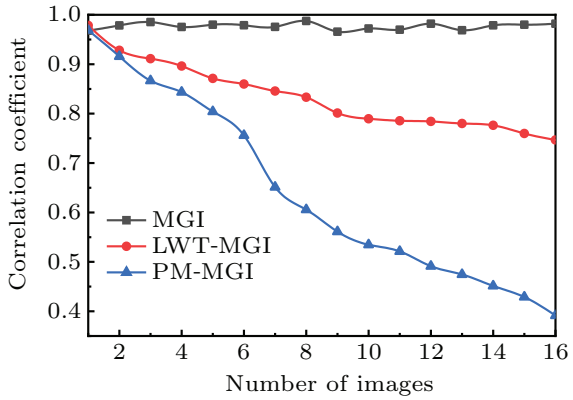


Fig. 9. CC between the plaintext and reconstruction information under different numbers of images.

Schematically, our scheme is entirely different from the traditional multiple-image encryption schemes. In existing multiple-image encryption schemes, the ciphertext is mostly determined by the key (That is to use the given key to encrypt the plaintext and get the ciphertext). However, the ciphertext determines the key in our scheme (The keys are calculated from the given ciphertext according to the images). Most of the images in our scheme don't need to be encrypted (Except the first image), and only to participate in the generation of the keys. Therefore, there is no need to mix or overlap multiple images in encryption process, and the reconstructed images don't have image aliasing problem.

5. Experiment

The experiment scheme proposed in this paper is shown in Fig. 10, which is specifically divided into three steps: encryption, key generation, and decryption. For encryption process, the laser irradiates the object through the beam expander, and the reflected light is focused on the digital micromirror device (DMD, V-7001) display screen through the lens. DMD introduces Hadamard patterns to simulate the pseudo-thermal light source. The object focused on the DMD display screen is modulated by the pseudo-thermal light source, and the reflected light is received by the photomultiplier tube (PMT, H10721-01)) and transmitted to the acquisition card (M2i.2030-exp). A series of intensity sequences are generated and as ciphertext to complete the encryption process. The key generation mainly uses ciphertext as a constraint to generate corresponding modulation patterns of multiple images. The specific operation process is implemented on the computer. For decryption process, different images can be decrypted using different modulation patterns.

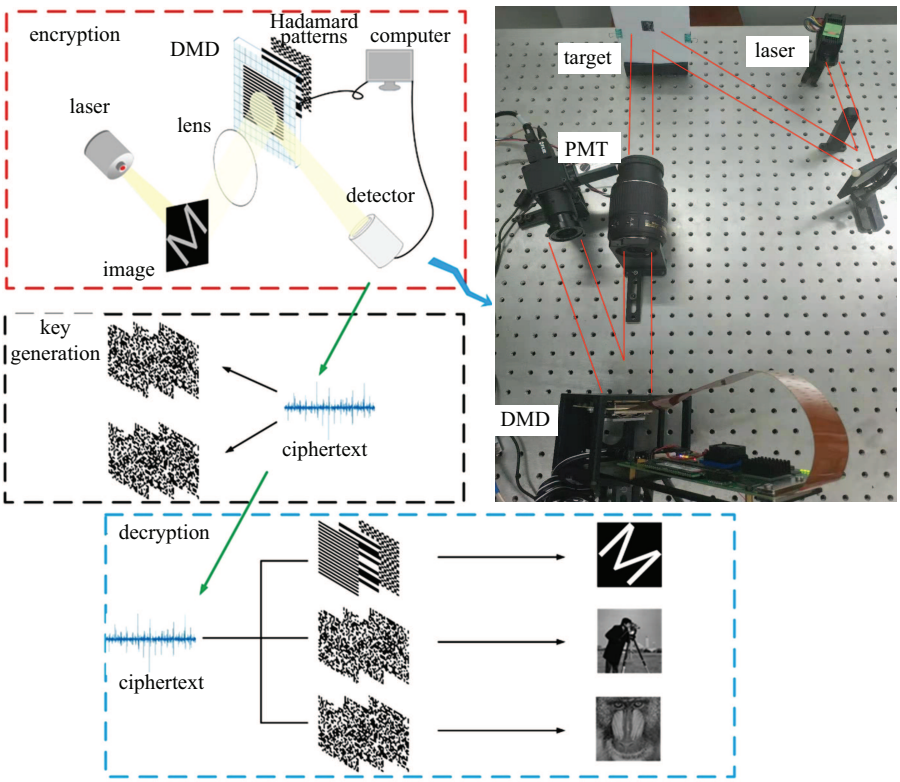


Fig. 10. Experimental flow and device diagram.

The above experimental flow is used to encrypt three images to verify the effectiveness of MGI in practical application. Figure 11 shows that the CC between the reconstruction image and the original image are 0.8965, 0.9436, and 0.9081, respectively. The reconstruction results are good and there is no image aliasing problem. For the first image, because of lens focus and operation error, there are problems of edge blur and position shift, compared with other images, CC is lower. The latter two images are mainly decrypted by keys without repeated optical encryption. Experimental results show that MGI is effective in practical application, and there is no aliasing between images.

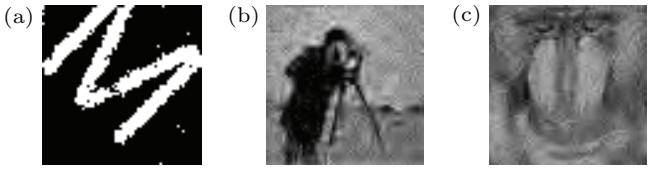


Fig. 11. Experiment results.

6. Discussion

A key advantage of our design over previous work is that can effectively avoid the problem of information aliasing caused by the increase of plaintext information and not lose plaintext information details. The reconstruction quality of the plaintext doesn't decrease with the increase of information. For different plaintext information, the keys are also different. This can achieve high security just like the "one-time-pad" scheme. It can effectively resist various attack modes (*e.g.* known/chosen-plaintext attack), and the amount of ciphertext data is small, so this scheme can be well adapted to the ghost imaging broadcasting system for public detection. Besides, because different plaintext information corresponds to different keys, the scheme is suitable for one-encryption and multi-decryption scenario, such as multi-level information authentication system or one-to-many encryption transmission. Ghost imaging can achieve indirect-line-of-sight imaging and weak-light imaging, and it demonstrates advantages in some invisible wavebands. These characteristics also provide the possibility for our scheme to encrypt information in special scenarios.

The main limitation of our system is the amount of data. With the increase of the image number, the size of keys is increased rapidly. In the existing multi-image encryption schemes, researchers mostly construct special modulation patterns to decrypt multiple images with few keys. But this kind of scheme will often cause image aliasing. The details of plaintext will be lost in the process of transformation and selection (*e.g.* discrete cosine transformation). Besides, from a security perspective, if the keys are stolen, all information will be threatened.[23,30] Although the amount of data transmitted in our system will increase with the amount of plaintext image, it also reduces the risk of all information being stolen to some extent. The development of machine learning also makes it possible to reduce the amount of transmitted data and speed up information reconstruction.[31,32]

7. Conclusion

In this paper, we proposed a novel ghost imaging-based optical cryptosystem for multiple images using the integral property of the Fourier transform. Compared with other multiple-image optical encryption schemes, we mainly construct different keys to achieve the encrypted transmission of multiple images. In encryption process, firstly, we use the ghost imaging encryption scheme to encrypt the first image. Then, the generated ciphertext is used as a constraint to realize the generation of keys of other images according to the integral property of the Fourier transform. Finally, the generated key and ciphertext are transmitted to the receiver to complete the encryption process. In decryption process, the receiver uses different keys to decrypt the same ciphertext and different images can be obtained. In this scheme, the key of each image is related to the image itself, so it can effectively resist various attack modes. And this scheme also solves the problem of aliasing of decrypted information. Simulations and experiments show the effectiveness, security, and robustness of this scheme. This scheme provides a new idea for optical image encryption and information authentication, among others.

References

[1] Gaiarin S, Perego A M, Silva E P D, Ros F D and Zibar D 2018 *Optica* **5** 263
[2] Shi Y S and Yang X B 2017 *Chin. Phys. Lett* **34** 114204
[3] Li J, Kamin S, Zheng G, Neubrech F, Zhang S and Liu N 2018 *Sci. Adv.* **4** eaar6768
[4] Zhang X P, Guo R, Che H W, Zhao Z M and Wang J Y 2018 *Chin. Phys. B* **27** 080701
[5] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[6] Situ G H and Zhang J 2005 *Opt. Lett.* **30** 1306
[7] Liang X, Li X S, Liu X and Zeng S 2011 *Opt. Laser. Technol.* **43** 889
[8] Sui L, Xu M and Tian A 2013 *Opt. Lett.* **38** 1996
[9] Zhang X, Meng X F, Wang Y R, Yang X L and Yin Y K 2018 *Chin. Phys. B* **27** 074205
[10] Pittman T B, Shih Y H, Strekalov D V and Sergienko A V 1995 *Phys. Rev. A* **52** R3429
[11] Wang L and Zhao S M 2020 *Chin. Phys. B* **29** 024204
[12] Shapiro J H 2008 *Phys. Rev. A* **78** 061802
[13] Lin J and Cheng J 2011 *Chin. Phys. Lett.* **28** 094203
[14] Zhou Y, Guo S X, Zhong F and Zhang T 2016 *Photon. Res.* **4** 240
[15] Lyu M, Wang W, Wang H, Li G, Chen N and Situ G H 2017 *Sci. Rep.* **7** 17865
[16] Clemente P, Durán V, orres-Company V, Tajahuerce E and Lancis J 2010 *Opt. Lett.* **35** 2391
[17] Tanha M, Kheradmand R and Ahmadi-Kandjani S 2012 *Appl. Phys. Lett.* **101** 5903

[18] Kong L, Li Y, Qian S, Li S, Tu C and Wang H 2013 *Phys. Rev. A* **88** 013852
[19] Chen W and Chen X 2015 *Opt. Lasers Eng* **73** 123
[20] Zhang Y D and Zhao S M 2017 *Chin. Phys. B* **26** 054205
[21] Wu J, Xie Z, Liu Z, Liu W, Zhang Y and Liu S 2016 *Opt. Commun.* **359** 38
[22] Li X, Meng X, Yang X, Wang Y, Yin Y, Peng X, He W, Dong G and Chen H 2018 *Opt. Lasers Eng.* **102** 106
[23] Li X, Meng X, Wang Y, Yin Y, Wang Y, Peng X, He W, Dong G and Chen H 2016 *IEEE Photon. J.* **8** 1
[24] Li X, Meng X, Wang Y, Yin Y, Wang Y, Peng X, He W, Dong G and Chen H 2017 *Opt. Lasers Eng.* **96** 7
[25] Shi D, Huang J, Wang Y, Yuan K, Xie C, Liu D and Zhu W 2017 *Sci. Rep.* **7** 13172
[26] Wang W, Hu X, Liu J, Zhang S, Suo J and Situ G H 2015 *Opt. Express* **23** 28416
[27] Xiao D, Cai H K and Zheng H Y 2015 *Chin. Phys. B* **24** 060505
[28] Zhao T, Ran Q, Yuan L, Chi Y and Ma J 2016 *Opt. Lasers Eng.* **83** 48
[29] Jiao S, Lei T, Gao Y, Xie Z and Yuan X 2019 *IEEE Access* **7** 119557
[30] Yuan X, Zhang L, Chen J, Wang K and Zhang D 2019 *Appl. Phys. B* **125** 174
[31] Wang F, Wang H, Wang H, Li G and Situ G H 2019 *Opt. Express* **27** 25560
[32] Guo Y, Che W and Jing S W 2020 *Chin. Phys. B* **29** 054203