Current Optics and Photonics
Vol. 2, No. 4, August 2018, pp. 315-323

ISSN: 2508-7266(Print) / ISSN: 2508-7274(Online)
DOI: https://doi.org/10.3807/COPP.2018.2.4.315

Research on Multiple-image Encryption Scheme Based on Fourier Transform and Ghost Imaging Algorithm

Zhang Leihong[1], **Yuan Xiao**[1]*, **Zhang Dawei**[1], **and Chen Jian**[2]

[1] *University of Shanghai for Science and Technology, Shanghai 200093, China*
[2] *Anhui Province Key Laboratory of Nondestructive Evaluation, Hefei 230031,China*

(Received April 26, 2018 : revised July 4, 2018 : accepted July 11, 2018)

A new multiple-image encryption scheme that is based on a compressive ghost imaging concept along with a Fourier transform sampling principle has been proposed. This further improves the security of the scheme. The scheme adopts a Fourier transform to sample the original multiple-image information respectively, utilizing the centrosymmetric conjugation property of the spatial spectrum of the images to obtain each Fourier coefficient in the most abundant spatial frequency band. Based on this sampling principle, the multiple images to be encrypted are grouped into a combined image, and then the compressive ghost imaging algorithm is used to improve the security, which reduces the amount of information transmission and improves the information transmission rate. Due to the presence of the compressive sensing algorithm, the scheme improves the accuracy of image reconstruction.

Keywords : Fourier transform, Compressive sensing, Ghost imaging, Multiple-image Encryption
OCIS codes : (070.2575) Fractional Fourier transforms; (100.3010) Image reconstruction techniques; (200.4560) Optical data processing

I. INTRODUCTION

With the rapid development of computer and Internet technologies, information security has attracted more and more researchers. Due to the ultra-high speed and multiple dimensional processing, optical information security technology has been popular for a long time, including double random phase encryption technology [1-5] and ghost imaging technology [6-10]. As another important branch of optical encryption, multiple-image encryption technology has attracted more and more attention because it not only improves the encryption ability but also reduces the data volume of the ciphertext. As far as multi-image encryption technology is concerned, it mainly focuses on researching new methods for simultaneous encryption of multiple images, to enhance the security of data and improve the robustness of the system.

Klyshko proposed a ghost imaging scheme that has attracted more and more attention owing to its remarkable physical properties [6]. Katz *et al*. achieved computational ghost imaging based on a compressive sensing algorithm instead of the intensity correlation operation, which greatly reduces the number of measurements; when the signals and images are sparse or can be sparse in some transform domains, the use of a compressive sensing algorithm can directly measure and simultaneously compress the signal or image. Finally, the signal will be reconstructed by the receiver's reconstruction algorithm [11-13].

In order to improve coding efficiency, the methods of multiple-image encryption based on position multiplexing and computational ghost imaging [14]; double random phase encryption [15] etc. have been proposed. Lee and Cho [15] proposed a multiple-image transmission method based on double random phase encryption using orthogonal encoding, which uses two random phase masks and orthogonal encoding. The orthogonal encoding for multiple images uses a larger Hadamard matrix than that for a single image, increasing the security of encryption. Li *et al*. [16] proposed

*Corresponding author: yxhello365@163.com, ORCID 0000-0002-2878-3217.

Color versions of one or more of the figures in this paper are available online.

a multiple-image encryption method based on compressive ghost imaging, in which an improved logistic mapping algorithm and the coordination of sampling were used to achieve multiple-image encryption and decryption; Wu *et al*. [17] proposed a multiple-image encryption scheme based on computational ghost imaging with different diffraction distances, each plane image is encrypted into an intensity vector, and then all the intensity vectors are added together to generate the final density in order to improve the effectiveness and security of the multiple-image encryption scheme; Yuan *et al*. [18] proposed a multi-image encryption scheme with a single-pixel detector according to the principle of ghost imaging. In this scheme, all the emitted light is recorded by a single-pixel barrel detector to obtain ciphertext, and any secret images can be independently decrypted from the ciphertext. The above encryption methods are provided with good security, but in computational ghost imaging, thousands of calculations are needed to obtain acceptable results. In some applications, a large amount of storage space is required for optical image encryption based on ghost imaging. In this sense, we propose a multi-image encryption scheme based on Fourier transforms and compressive ghost imaging. The images adopt Fourier transforms to obtain the image information. According to different sampling rates, multiple images are synthesized into an image in the Fourier space. Then the encryption and decryption was achived by the compressive ghost imaging algorithm, which realizes data compression and reduces the storage space of the data. Firstly, the theoretical analysis and description of the method are given, and then simulation verification is carried out. Finally, the conclusion is drawn.

II. THEORETICAL ANALYSIS

2.1. Optical Encryption Mechanism Based on Compressive Ghost Imaging Algorithm

In the computational ghost imaging encryption system, the spatial light modulator (SLM) that inputs a series of phase masks is used, as shown in Fig. 1 [19]. The plane wave is modulated by the phase masks and a Fresnel diffraction occurrs with a distance Z from phase masks plane to object plane. Then the light intensity distribution in the object plane could be calculated by using the Fresnel diffraction, which can be expressed as [20]

$$I_i(x,y) = \left|FrTz\{\exp[j2\pi\varphi_i(x,y)]\}\right|^2 \tag{1}$$

where $FrT\{\bullet\}$ represents the Fresnel diffraction transform, $\varphi(x,y)$ is the pixel distribution of each phase mask, whose pixel values are randomly from 0 to 1. The subscript "i" represents the i-th measurement value using the i-th phase mask, and the subscript "Z" represents diffraction distance, and the amplitude of the plane wave is defined as unit one.

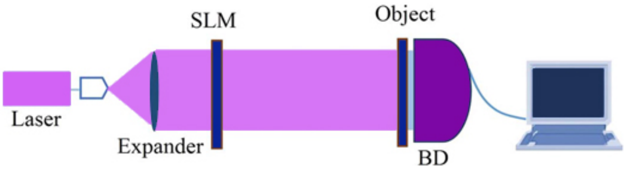


FIG. 1. Schematic of computional ghost image encryption system.

Therefore, the new imaging process only requires a bucket detector (BD) to obtain the ciphertext B_i, which can be expressed as

$$B_i = \int T(x,y)I_i(x,y)dxdy \tag{2}$$

where the $T(x,y)$ is the image to be encrypted. Therefore, the image T to be encrypted is successfully encoded in a series of light intensity ciphertext data B_i using the phase mask key and the distance parameter Z. During the decryption process, an intensity-related operation occurred between the intensity distribution $I(x,y)$ and intensity ciphertext data B_i from the bucket detector to calculate a secret image, which can be expressed as

$$G(x,y) = \langle B_i I_i(x,y)\rangle - \langle B_i\rangle\langle I_i(x,y)\rangle \tag{3}$$

where $\langle\bullet\rangle$ represents the average operation.

However, the ghost imaging algorithm is a statistical feature extraction process. The detection time required for imaging and the resolution time for the reconstruction algorithm are relatively long. In order to solve this problem, Donoho proposed a new reconstruction algorithm based on compressive sensing, which greatly reduced the number of exposure samplings and reduced the amount of computation. At the same time, more encrypted information can be transmitted and the amount of information transmitted is increased under the same calculation conditions. That is to say, the ghost imaging combined with the compressive sensing algorithm successfully solves the problems of long imaging time and low accuracy of object reconstruction. The specific encryption process is: the plaintext image $T(x,y)$ to be encrypted is a two-dimensional image, and the size is $n \times n$ which is stretched into a column vector $(n^2 \times 1)$. For the m-th measurement, the light distribution function of the reference arm at the pixel point (x_p, y_q) is $I_{\mathrm{m}}(x_p, y_q)$, $m = 1,2\cdots N$, $p,q = 1,2\cdots n$, whose matrix expression is:

$$I_{\mathrm{m}} = \begin{bmatrix} I_{11}^m & \cdots & \cdots & I_{1n}^m \\ I_{21}^m & \cdots & \cdots & I_{2n}^m \\ \vdots & \ddots & \ddots & \vdots \\ I_{n1}^m & \cdots & \cdots & I_{nn}^m \end{bmatrix} \tag{4}$$

The matrix size is $n \times n$, I^m_{pq} is the intensity of the light measured by the m-th measurement at the pixel point $(x_{p,} y_q)$ of the CCD measurement plane, which is stretched into a one-dimensional row vector. After N times of measurement, the N $n \times n$ one-dimensional row vectors recorded by the CCD are stored in columns to get a random matrix $I_i(x, y)$, the size of which is $N \times n^2$ and as a measurement matrix ϕ of compressive sensing, ie

$$\Phi = \left[I^m_{11}, I^m_{12}, \cdots I^m_{1n}, I^m_{21}, I^m_{22}, \cdots I^m_{n,n-1}, I^m_{n,n} \right] \tag{5}$$

The expression of the encryption process is:

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_N \end{bmatrix} = \begin{bmatrix} I^1_{11} \cdots I^1_{1n} \cdots I^1_{nn} \\ I^2_{11} \cdots I^2_{1n} \cdots I^2_{nn} \\ \vdots \ \ddots \ \vdots \ \ddots \ \vdots \\ I^N_{11} \cdots I^N_{1n} \cdots I^N_{nn} \end{bmatrix} \begin{bmatrix} T_{11} \\ \vdots \\ T_{1n} \\ \vdots \\ T_{nn} \end{bmatrix} \tag{6}$$

A compressive sensing algorithm is used for decryption. The original signal can be reconstructed from these projections with high probability by solving an optimization problem. The minimum l_1 norm convex programming problem is shown in Eq. (7). The CS reconstruction algorithm recovers the signal as in Eq. (8).

$$\min \| \psi^T X \|_1 \text{ s.t. } Y = \phi \psi^T X \tag{7}$$

$$T_{CS} = T' ; \arg\min \| \psi \{ T'(x, y) \} \| \tag{8}$$

2.2. Fourier Transform Encryption/ Sampling Principle

The two-dimensional image Fourier transform is to convert the distribution of image luminance values in the spatial domain to the frequency domain distribution of the image. In this paper, the fast Fourier transform (FFT) can be used to convert the image signal from the spatial domain to the frequency domain for analysis. Using the sparseness and conjugacy of the spatial spectrum of the image, the important information of the image is obtained according to different sampling rates in the Fourier space. In this paper, four binary images are taken as an example. The spectrum and sampling are shown in Figs. 2 and 3.

2.3. The Method of Multiple-Image Encryption

The multiple-image encryption and decryption process based on the Fourier transform and compressive ghost imaging algorithm are shown in Figs. 4 and 5. The main steps are as follows:

(1) Fourier transforms are applied to the multiple images and converted from spatial domain to frequency domain;
(2) In the frequency domain, multiple images are sampled and combined to form a single ciphertext, and the formed single ciphertext is used as the plaintext image of the next encryption algorithm with ghost imaging.

The matrix of the sampling image is represented in Eq. (9), where (x,y) denotes a two-dimensional matrix in the spatial domain and (u,v) denotes a two-dimensional matrix in the Fourier domain. The value of i varies from 1 to k, where k is the total number of images to be encrypted, the images are sampled by a sampling operation to obtain useful information in the images;

$$s_i(u, v) = \Omega_i(u, v) F\left[f_i(x, y) \right] \tag{9}$$

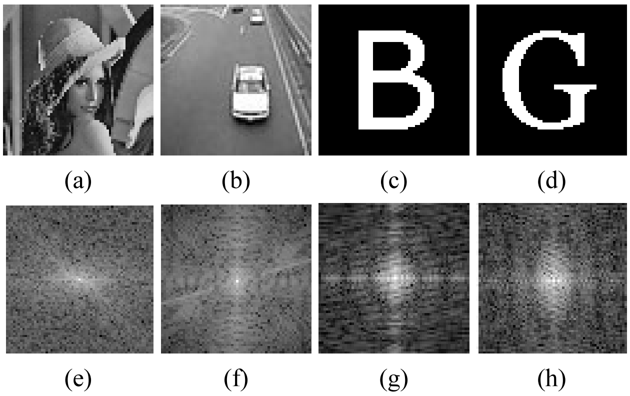


FIG. 2. (a-d) are four original images; (e-h) are their corresponding spectrograms.

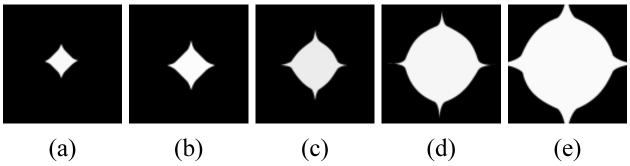


FIG. 3. (a-e) are spatial spectra with sampling rates of 6%, 11%, 25%, 50%, and 75%.

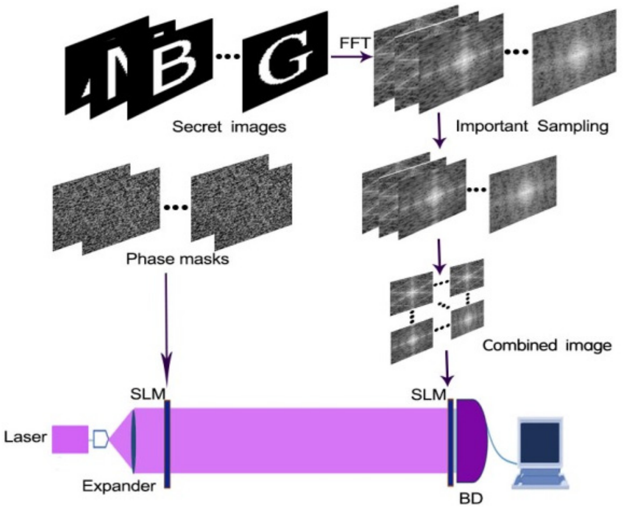


FIG. 4. Multiple-Image encryption schematic based on Fourier transform and Compressive sensing ghost imaging algorithm.

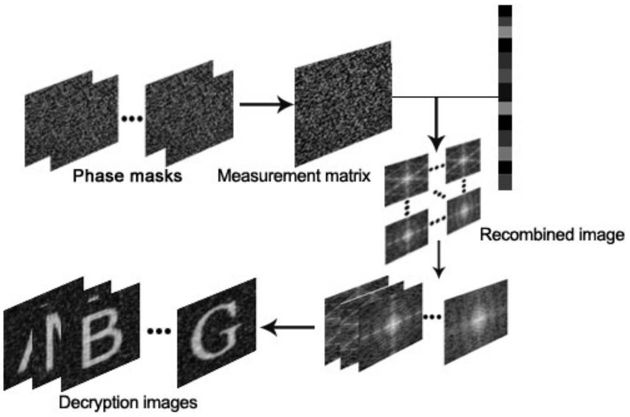


FIG. 5. Multiple-image decryption schematic based Fourier transform and compressive ghost imaging algorithm.

(3) Since the formed single ciphertext is of the characteristics of a complex-valued function, it is separated into real and imaginary parts. Then, they are transmitted and encrypted by using ghost imaging. With a random modulation signal as the key, encryption can be achieved due to the randomness of the key;

(4) The compressive sensing algorithm is used to decrypt separately the transmitted ciphertexts and combine the decrypted parts into a plural form. Therefore, the combined image is obtained. The combined image contains the reconstructed multiple images through $\Omega(u,v)$ operation;

(5) The inverse Fourier transform is performed on the reconstructed images to obtain the original images.

III. SIMULATION RESULTS AND ANALYSIS

In order to verify the effectiveness and feasibility of this method, a numerical experiment was carried out for this method. The experiment was mainly realized by MATLAB software. The selected experimental object is four 64 × 64 binary images. The four binary images adopt are transformed, and the transformed images are sampled according to different sampling rates; the images obtained by Fourier transform sampling are used as the plaintext images of the compressive ghost imaging algorithm. That is, the object $T(x,y)$ to be imaged; Transforming a pre-fabricated light field intensity matrix $I_n(x,y)$ into a row as a measurement matrix ϕ for the compressive ghost imaging algorithm; The measured value obtained by multiplying the pre-determined light field intensity matrix and the binary image is taken as the total light intensity B_n, and the N precast light field intensity matrices are arranged in order to form a measurement matrix ϕ. The object to be imaged is measured to obtain N measurement values, and the image of the object is reconstructed by Eq. (5). The simulation results are shown in Fig. 6.

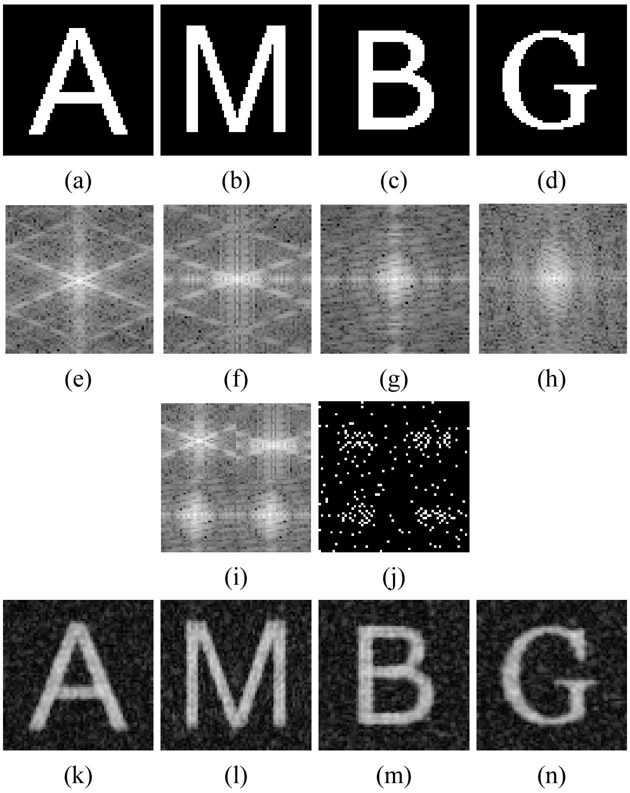


FIG. 6. (a-d) are the original images; (e-h) are the corresponding spectrograms; (i) is the combined image with a sampling rate rate of 50%; (j) is the combined ciphertext (The real part and the imaginary part are respectively subjected to ghost imaging and then recombined into a plural form); (k-n) are different reconstruction images.

3.1. Feasibility Analysis

Feasibility refers to the situation where the recipient recovers the original graphic information by using the key shared by the sender and the ciphertext delivered on the common channel. The feasibility assessment is performed using the optical information encryption method to reconstruct the resolution of the plaintext information, which is measured using subjective judgments and objective parameters. In this section we will discuss the feasibility of the encryption method, and compare the Fourier transform and compressive ghost imaging (FFT-CGI) with the Fourier transform and ghost imaging algorithm (FFT-GI). As shown in Figs. 7 and 8.

In order to objectively and accurately evaluate the quality of the recovered images using the encryption method. The commonly used objective evaluation indicators include mean square error (MSE) and peak signal-to-noise ratio (PSNR). The basic idea is to measure the degree of deviation of the pixels of the reconstructed image from the corresponding pixels of the original image to evaluate the quality of the reconstructed image. For a size of M × N image, the mathematical expression for MSE and PSNR is:

$$MSE=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(V_{i,j}-V_{i,j}^{'})^2}{M\times N} \tag{10}$$

$$PSNR=10\lg\frac{V_{\max}^2}{MSE} \tag{11}$$

where $V_{i,j}$ an $V'_{i,j}$ represent respectively the pixel value of the original image and the restored image, $V_{\max}$ represents the value of the largest pixel in the image. The larger the PSNR value, the more similar the two images are. That is, the higher the recovered picture quality, the better the encryption algorithm is.

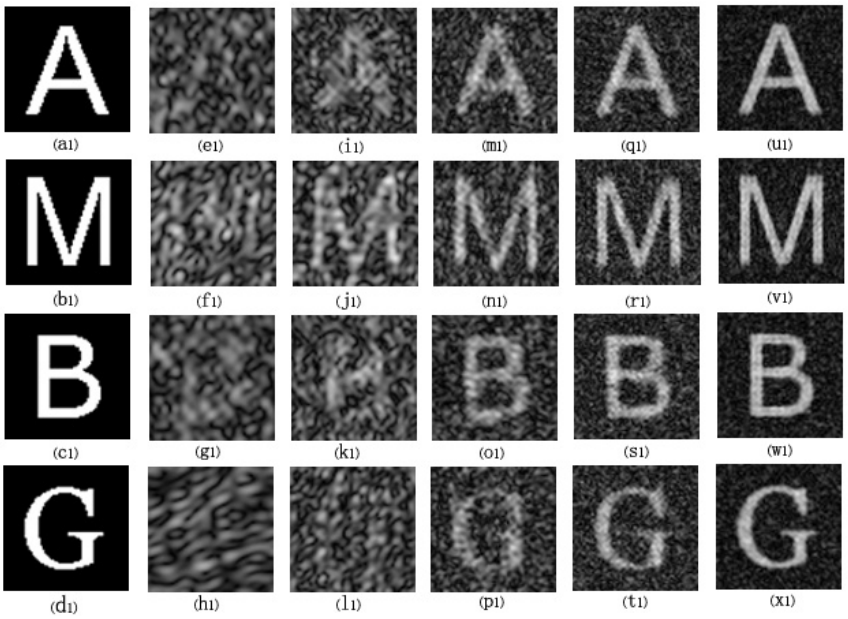


FIG. 7. Reconstruction images of FFT-CGI (a1-d1) are the original images; (e1-h1) are the reconstructed images with the sampling rate of 6%; (i1-l1) are the reconstructed images with the sampling rate of 11%; (m1-p1) are the reconstructed images with the sampling rate of 25%; (q1-t1) are the reconstructed images with the sampling rate of 50%; (u1-x1) are the reconstructed images with the sampling rate of 70%.

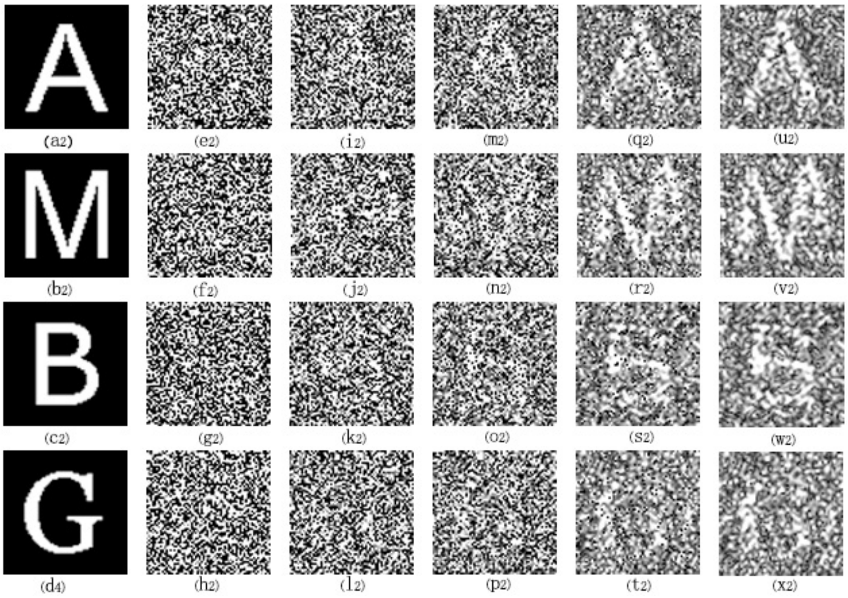


FIG. 8. Reconstruction images of FFT-GI (a2-d2) are the original images; (e2-h2) are the reconstructed images with the sampling rate of 6%; (i2-l2) are the reconstructed images with the sampling rate of 11%; (m2-p2) are the reconstructed images with the sampling rate of 25%; (q2-t2) are the reconstructed images with the sampling rate of 50%; (u2-x2) are the reconstructed images with the sampling rate of 70%.

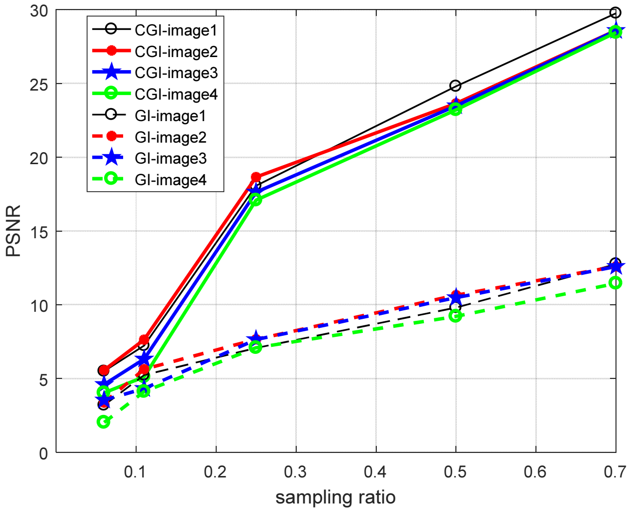


FIG. 9. PSNR curve of two algorithms under different sampling conditions.

The PSNR values of the two methods at different sampling rates are shown in Fig. 9.

The solid lines of different colors in the figure represent the PSNR transformation of different images under different sampling conditions in the FFT-CGI method. The dotted lines of different colors represent the PSNR transformation of different images under different sampling conditions in the FFT-GI method. The trends of the curves in Figs. 8~10 show that: (1) With the increase of the sampling rate, the PSNR value shows an upward trend, that is, the larger the number of samples, the greater the PSNR, the higher the quality of the reconstructed image, and the closer to the original image information; (2) When the sampling rate is 50%, or 70%, the reconstructed images are approximately similar; (3) When the sampling rate is 25%, the corresponding PSNR values of the FFT-CGI scheme are respectively 18.0702, 18.6568, 17.0901. The reconstructed images are close to the original images. However, the corresponding PSNR values of the FFT-GI scheme are respectively 7.1612, 7.5638, 7.6249, 7.1821. In the scheme, the original image cannot be reconstructed when the sampling rate reaches 50%. These experimental results show that the images recovered by the FFT-CGI scheme has better quality, which proves that the scheme is more effective in terms of feasibility. At the same time, it shows that the CS algorithm can achieve the characteristics of low sampling rate and high reconstruction quality.

3.2. Security Analysis

In practical applications, an absolutely secure cryptographic system does not exist. If the cost of deciphering the algorithm is greater than the cost of the encrypted information, the algorithm can be considered secure. Therefore, we need to use existing password attack methods as far as possible to verify the anti-attack performance of the designed system. For example, selected plaintext attack, selected ciphertext attack, known plaintext attack, only ciphertext attack, noise attack and so on. This paper uses only ciphertext attack and noise attack to attack.

3.2.1. Ciphertext-only attack

Ciphertext-only attacks (COA) are that attackers try to analyze the key in the intercepted ciphertext or the plaintext corresponding to the ciphertext. The ciphertext-only attack is the most difficult in all attacks. Attackers usually can guess the plaintext or key only based on the statistical characteristics of the secret text body. If a cryptosystem cannot resist ciphertext-only attacks, in theory, this cryptosystem is insecure. This paper uses the histogram and correlation between neighboring pixels in statistical analysis to count the ciphertext characteristics and to verify the security of the method.

The histogram of the image is a method of analyzing the encryption algorithm. The histogram distributions of different images are different. When the histogram distribution of the corresponding ciphertext image is consistent, the encryption algorithm can resist histogram statistical analysis attacks. It shows that the scheme of this paper has very good security.

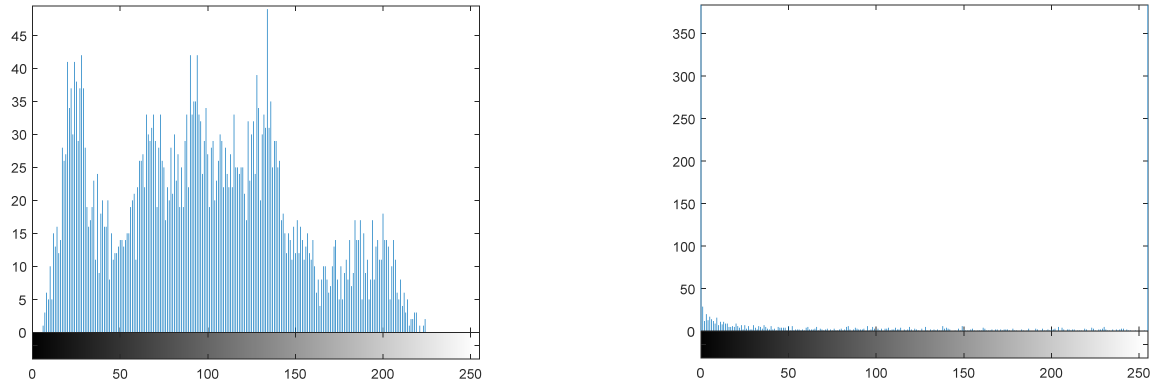
Figure 10 is a histogram before and after encryption using this method: Fig. 10(a) is a histogram distribution of a plaintext image with certain statistical characteristics; Fig. 10(b) is the histogram distribution of the ciphertext image. After the compressive ghost imaging, the information is further compressed and the encrypted image is approximately evenly distributed, which shows that the proposed scheme has good security.

Each pixel in a digital image is not independent and is very relevant. One of the goals of image encryption is to reduce the correlation of adjacent pixels, which mainly include the correlation among horizontal pixels, vertical pixels, and diagonal pixels. Obviously, the smaller the relevance, the better the effect of image encryption and the higher the security. The expression of the pixel correlation coefficient is:

$$
\begin{aligned}
&E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \\
&D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \\
&\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \\
&CC=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}
\end{aligned}
\tag{12}
$$

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

As can be seen from Table 1, the adjacent pixels of the original images have a high correlation and the adjacent

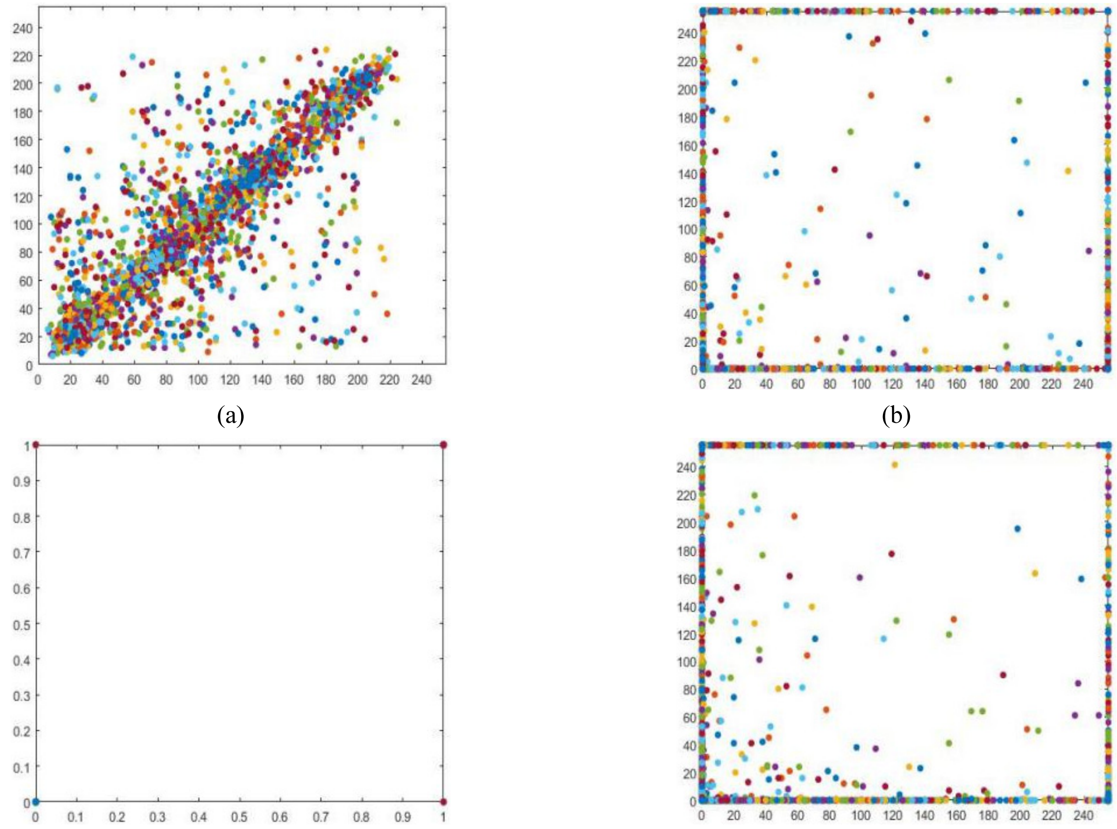


(a) (b)

FIG. 10. Histograms of plaintext and ciphertext (a) The histogram corresponding to the plaintext image; (b) The histogram corresponding to the ciphertext image.

TABLE 1. Correlation coefficients of adjacent pixels to a plaintext image and a ciphertext image

Correlation coefficient	Horizontal	Vertical	Diagonal
Original lena	0.8358	0.6894	0.6397
Encrypted lena	0.0910	0.0241	0.0123
Original A	0.8424	0.8820	0.8088
Encrypted A	0.0514	0.0398	0.0258



(a) (b)

(c) (d)

FIG. 11. Scatter plots corresponding to plaintext and ciphertext: (a)(c) are scatter plots corresponding to different plaintext images; (b)(d) are scatter plots corresponding to different ciphertext images.

pixels of the ciphertext images have a small correlation, with the adjacent pixels are basically irrelevant, which shows that the statistical characteristics of the original images have been diffused into random ciphertext images.

In the experiment, MATLAB software was used to simulate the correlation of adjacent pixels in the vertical direction, and the correlation was shown by a scatter plot, as shown in Fig. 11. Obviously, the correlation of adjacent pixels in the original image shows a clear linear relationship, while the correlation of adjacent pixels of the encrypted image presents a random correspondence.

3.2.2. Noise attack

Noise attack is inevitable in the process of information encryption and propagation, and the noise will affect the imaging quality of the object and the transmission of the image information. Therefore, it is essential to evaluate the robustness of the encryption algorithm when the key or ciphertext is attacked by noise. Figure 12 shows the NC value of the reconstructed image under different noise attack intensities in the scheme of this paper. From the figure, we can see that: (1) With the increase of noise intensity, the NC value has a certain degree of decline; (2) Although a certain noise attack, the reconstructed image can still be distinguished, which shows that the scheme of this paper has effective security.

3.2.3. Compressibility analysis

This paper makes full use of the anti-cutting characteristics of the Fourier transform algorithm, achieving information compression and greatly reducing the amount of information transmitted. In the experiment, the image information after Fourier transform was cut out at different proportions, and then the cropped images adopt compressive ghost imaging. Evaluating the cropped information with the quality of the reconstructed images will not affect the encryption algorithm in this paper. In this paper, similarity (NC) is used to objectively evaluate the degree of similarity between the original plaintext image and the reconstructed image. The obtained NC value is used as an objective index to evaluate the sharpness of the cut image reconstruction, so as to determine the maximum cut ratio of the plaintext image. The largest cutting ratio, thereby minimizing the amount of information transmitted, reducing storage space and increasing the rate of information transmission. For an image of size M × N, the mathematical expression of similarity NC is as follows:

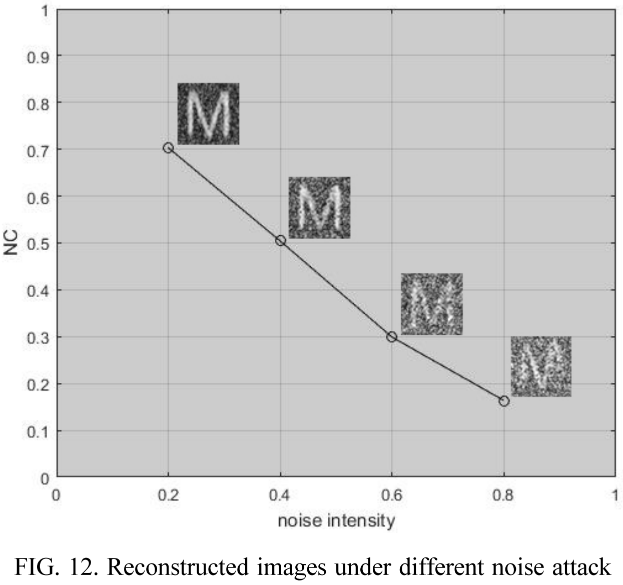


FIG. 12. Reconstructed images under different noise attack intensities.

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}X(i,j)X'(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N}X(i,j)^2} \tag{13}$$

where X is the original plaintext image, X' is the reconstructed image for the cut image. In this experiment, we cut separately 30%, 50%, 75% of the graphic information after Fourier transform. Four 64 × 64 binary images were selected and the sampling rate was 50%. The reconstructed images are shown in Fig. 13 (taking one of the images as an example).

Where (a) represents the original image; (b-e) are respectively the reconstructed images of 30%, 50%, and 75%, whose NC are respectively 0.8749, 0.7432, 0.5828. From the effect images of Fig. 13, it can be seen that the reconstructed images can recognize the contour of the original image when the cropping ratio reaches 75%. Therefore, it is illustrated that the algorithm can successfully reconstruct the original images.

From Table 2, it can be seen that the amount of transmitted information is 2048 bits when the cutting ratio is 75%, which greatly reduces the amount of transmitted

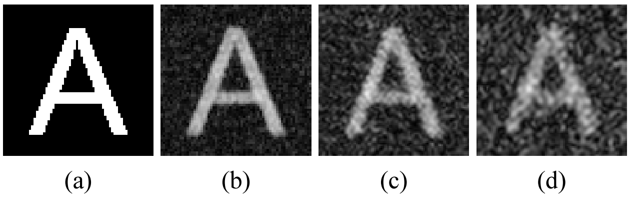


FIG. 13. Reconstructed images with different cut ratios.

TABLE 2. NC values and transmitted information's amount of reconstructed images in different cut ratios

Percent of cutting (%)	Quantity of information	NC
30	5734.4	0.8749
50	4096	0.7432
75	2048	0.5828

information and reduces the storage space. The NC values of the reconstructed images and the corresponding amounts of transmitted information under different cutting ratios are shown in Table 2.

IV. CONCLUSION

This paper proposes a multiple-image encryption algorithm based on Fourier transform and compressive ghost imaging, which solves the problems of low security, long imaging time and other issues of current encryption algorithms, breaking through the limitations of the traditional Nyquist sampling rate, achieving low sampling rate and high reconstruction quality. The encryption algorithm combined the Fourier transform and completes the compression, reducing the amount of transmitted information, reducing the data storage space and improving the speed of information transmission. The encryption algorithm has high security, fast transmission speed and good quality of reconstruction information. Therefore, the encryption algorithm can be applied to information encryption and data storage, which has a good application prospect.

ACKNOWLEDGMENT

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

REFERENCES

1. P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
2. Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253-10265 (2007).
3. I.-H. Lee and M. Cho, "Optical encryption and information authentication of 3D objects considering wireless channel characteristics," J. Opt. Soc. Korea **17**, 494-499 (2013).
4. M. Cho and B. Javidi, "Three-dimensional photon counting double random phase encryption," Opt. Lett. **38**, 3198-3201 (2013).
5. I.-H. Lee and M. Cho, "Double random phase encryption based orthogonal encoding technique for color images," J. Opt. Soc. Korea **18**, 129-133 (2014).
6. D. N. Klyshko, "Combine EPR and two-slit experiments: Interference of advanced waves," Phys. Lett. A **132**, 199-304 (1999).
7. M. Tanha, S. Ahmadi-Kandjani, R. Kheradmand, and H. Ghanbari, "Computational fluorescence ghost imaging," Eur. Phys. J. D **67**, 44 (2013).
8. O. Katz, Y. Bromberg, and Y. Silberberg, "Compressive ghost imaging," Appl. Phys. Lett. **95**, 131110-131113 (2009).
9. V. Katkovnik and J. Astola, "Compressive sensing computational ghost imaging," J. Opt. Soc. Korea A **29**, 1556-1567 (2012).
10. J. H. Shapiro and R. W. Boyd, "The physics of ghost imaging," Quantum. Inf. Process. **11**, 949-993 (2012).
11. J. Garnier, "Ghost imaging in the random paraxial regime," Inverse Probl. Imaging **10**, 409-432 (2017).
12. S. Yuan, J. Yao, X. Liu, X. Zhou, and Z. Li, "Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging," Opt. Commun. **365**, 180-185 (2016).
13. Y Wang and Y Liu, "High speed computational ghost imaging via spatial sweeping," Sci Rep. **7**, 45325 (2017).
14. J. J. Wu, Z. W. Xie, Z. J. Liu, W. Liu, Y. Zhang, and S. T. Liu, "Multipleimage encryption based on computational ghost imaging," Opt. Commun. **359**, 38-43 (2016).
15. I.-H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multipleimage transmission," J. Opt. Soc. Korea **18**, 201-206 (2014).
16. X. Li, X. Meng, X. Yang, Y. Yin, Y. Wang, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," IEEE Photon. J. **8**, 900511 (2016).
17. J. Wu, Z. Xie, Z. Liu, W. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on computational ghost imaging," Opt. Commun. **359**, 38-43 (2016).
18. S. Yuan, X. Liu, X. Zhou, and Z. Li, "Multiple-image encryption scheme with a single-pixel detector," J. Mod. Opt. **63**, 1457-1465 (2016).
19. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**, 221106 (2013).
20. Z. Liu, C. Shen, J. Tan, and S. Liu, "A recovery method of double random phase encoding system with a parallel phase retrieval," IEEE Photon. J. **8**, 7801807 (2016).