Image compression-encryption algorithm based on 2D compressive sensing and double random phase encoding

1st JinLong Liu1,a, 2nd Miao Zhang1,b, 3rd Xiaojun Tong1,c #, 4th Zhu Wang1,d

1School of Computer Science and Technology, Harbin Institute of Technology, Weihai, China
2a-e-mail: 19s130315@stu.hit.edu.cn, b-e-mail: zhangmiaozm209@126.com, d-e-mail: wangzhu@hit.edu.cn
3c* Corresponding author: tong_xiaojun@163.com
4# These authors contributed equally to this work

Abstract—In this paper, an image compression and encryption algorithm based on 2D compressive sensing and double random phase encoding is proposed. Compared with traditional encryption algorithms, 2D compressive sensing can realize image compression and encryption at the same time, with high execution efficiency. Double random phase encoding can not only realize image encryption fast, but also has robustness. Moreover, combining 2D compressive sensing with double random phase encoding can obtain better encryption security. Simulation results show that this algorithm has better image compression performance, and can ensure security and robustness.

1. Introduction

When images are transmitted in an insecure channel, it is necessary to encrypt the images to avoid the leakage of sensitive information. In addition to image encryption, people often need to compress the images to improve the transmission efficiency. Traditional compression and encryption algorithms usually need to divide image compression and encryption into two stages, so the processing efficiency is low and the realization process is complex.

Compressive sensing (CS) can complete the signal encryption while compressing the signal, and the processing speed is fast. Moreover, the complexity of CS signal reconstruction is high to crack, so CS is widely used in the image compression and encryption [1-2]. However, CS may retain some meaningful information of plain images, and it is a security risk to encrypt the image only in CS. In recent years, lots of encryption techniques have been combined with CS to improve the security of image encryption [3-5]. R. Ponuma et al. [3] perform confusion and diffusion operation on the measurement value of CS to achieve further encryption. Chai et al. [4] construct measurement matrix with the magnetic-controlled memristive chaotic system, and use zigzag path and elementary cellular automata to improve the security of CS image encryption. Zhu et al. [5] use 4D chaotic system to construct the measurement matrix in CS and perform cyclic shift on the measurement value of CS to improve the encryption security. 2D CS measures images from two directions, which is more efficient and can further improve the performance of image compression. In addition, 2D CS is more difficult to crack, so the use of 2D CS for image encryption has also aroused the interest of researchers [6-8]. Xu et al. [6] construct two measurement matrices to compress the images from two directions and re-encrypt the measurement value by using the row and column encryption, which greatly improve the speed of
encryption algorithm with better compression performance. Yang et al. [7] construct two measurement matrices with fractional order hyperchaotic systems to compress images and perform DNA operation on measurement value, which improve execution efficiency and compression performance. Although the above encryption algorithms ensure the security of image encryption, most of them are complex and have low efficiency. Double random phase encoding (DRPE) is widely used in image encryption with advantages of optical implementation and high robustness [9-11].

In this paper, an image compression and encryption algorithm based on the combination of 2D CS and DRPE is proposed. Firstly, the original image is compressed from two directions to obtain the measurement value. Then, DRPE is performed on the measurement value to obtain the final cipher image. Compressing images from two directions can obtain higher compression performance in a shorter time. In addition, the combination of DRPE and 2D CS can improve the execution efficiency of compression encryption and ensure the security and robustness of encryption.

2. Image compression and encryption algorithm based on 2D compressive sensing and double random phase encoding

2.1. Compressive sensing
As a signal acquisition technique, CS can reconstruct sparse signal without losing important information when signal is sampled at a rate lower than Nyquist rate. For sparse signal \( S \), the sample process of 2D CS is as follows:

\[
X = \phi_1 S \phi_2
\]

where \( \phi_1 \) and \( \phi_2 \) are measurement matrices. We can solve Eq. (2) to reconstruct sparse signal \( S \).

\[
\min_{s \in \mathbb{R}} \|s\|_1 \quad \text{s.t.} \quad X = \phi_1 S \phi_2
\]

In this paper, we use discrete wavelet transform to perform sparse transform on images, and the smooth L_{0} algorithm (SL_{0}) is used to solve formula (2) to reconstruct images.

2.2. Double random phase encoding
Two random phase matrices are required for the process of DRPE. For image \( X \), the process of DRPE can be expressed as follows:

\[
Y = \text{FFT}^{-1}(\text{FFT}[X \exp(i2\pi R_1)]\exp(i2\pi R_2))
\]

The inverse process of DRPE can be expressed as formula (4), where \( R_1 \) and \( R_2 \) stand for two phase random matrices, FFT and FFT^{-1} represent the fast Fourier transform and inverse fast Fourier transform respectively.

\[
X = \text{FFT}^{-1}(\text{FFT}[Y \exp(-i2\pi R_2)]\exp(-i2\pi R_1))
\]

2.3. The process of encryption
1) Set the initial values \( x_1, y_1, z_1, w_1 \) and parameter \( \mu \), which are the keys, construct measurement matrix \( \phi_1, \phi_2 \) and random phase matrix \( R_1, R_2 \) with Logistic chaotic system. Logistic chaotic system can be expressed as formula (5), where \( \mu \in [3.57, 4] \) and \( X_0 \in [0, 1] \).

\[
X_{n+1} = \mu X_n (1 - X_n)
\]

2) Perform discrete wavelet transform on image \( T \) to get sparse matrix \( S \), and then perform Arnold transform to scramble \( S \).
3) According to formula (1), perform 2D CS operation on \( S \) to obtain measurement value \( X \).
4) According to formula (3), perform DRPE on measurement value \( X \) to obtain the final cipher image \( Y \).

2.4. The process of decryption
1) Construct measurement matrices and random phase matrices with Logistic chaotic system.
2) According to formula (4), perform the reverse process of DRPE on cipher image to obtain
measurement value $X$.

3) Reconstruct the sparse matrix $S$ using the $SL_0$ algorithm, and then perform the reverse process of Arnold and discrete wavelet transform to reconstruct the original image $T$.

3. **Experimental results and analysis**

3.1. **Experimental results**

In order to verify the feasibility of our algorithm, we implement the algorithm on Matlab 2016B. We use the grayscale images selected from the USC-SIPI image library as the test images to analyze compression performance and security. Figure 1(a)-(i) show the results of image compression encryption and reconstruction with a compression ratio of 0.5.

![Image](image_url)  
(a) Plain image of Lena  
(b) Cipher image of Lena  
(c) Decrypted image of Lena  
(d) Plain image of Female  
(e) Cipher image of Female  
(f) Decrypted image of Female  
(g) Plain image of Cameraman  
(h) Cipher image of Cameraman  
(i) Decrypted image of Cameraman

Figure 1. Encryption and decryption results

The results show the cipher images are similar to noise and occupy less space, and the reconstructed images have almost no difference from the plain images. Therefore, the experimental results preliminarily verify the feasibility of the proposed algorithm.

3.2. **Compression performance analysis**

Peak signal to noise ratio (PSNR) quantifies the image quality by calculating the difference of all corresponding pixel points in the original image and reconstructed image, which can reflect the compression performance of the algorithm. The higher the PSNR value, the better the quality of the reconstructed image. When the PSNR value reaches 30, the reconstructed image has well quality. The PSNR of image X and Y is defined as follows:
\[ \text{MSE} = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} (X(i, j) - Y(i, j))^2 \]

\[ \text{PSNR} = 10 \times \log_{10} \left( \frac{255 \times 255}{\text{MSE}} \right) \]

(6)

Table 1: PSNR (db) of different images

| Image  | Lena   | Female | Cameraman |
|--------|--------|--------|-----------|
| 0.56   | 29.8252| 30.8947| 25.6487   |
| 0.75   | 32.7820| 31.1590| 28.4817   |

Table 2: PSNR (dB) for different algorithms

| Ratio | Ours  | Ref. [4] | Ref. [6] | Ref. [8] |
|-------|-------|----------|----------|----------|
| 0.56  | 29.8252| 29.8200  | 29.2337  | 25.9997  |
| 0.75  | 32.7820| 29.5600  | 29.2184  | 30.6881  |

PSNR values of images reconstructed under different compression ratios are shown in Table 1. The PSNR values of Lena images reconstructed under different encryption algorithms are listed in Table 2. We can see from the results that the algorithm proposed in this paper has better compression performance.

3.3. Statistical attack analysis

The histogram and pixel correlation of cipher images can evaluate the ability of encryption algorithm to resist statistical attack. The histogram of plain image usually contains some features of image. The difference between the histograms of different plain images is large, while the difference of the histograms of different cipher images is little.
Figure 2. The histograms of plain and cipher images

Figure 2 shows the histograms of Lena and Female plain images and their cipher images. We can see that the histograms of two plain images are completely different, while the histograms of their cipher images have almost no difference. The histograms reflect the security of the encryption algorithm in this paper.

The correlation between the pixels of the plain image is high, and the correlation coefficient is close to 1, and the pixel correlation of the cipher image is close to 0. Therefore, the lower the cipher image correlation coefficient, the higher the encryption security. The correlation coefficient of adjacent pixels $x, y$ can be defined as follows:

$$\rho_{x, y} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}$$

Table 3 The correlation coefficient of different images

| Image         | Plain image | Cipher image |
|---------------|-------------|--------------|
|               | Horizontal  | Vertical     | Diagonal     | Horizontal | Vertical | Diagonal     |
| Cameraman     | 0.917       | 0.933        | 0.893        | 0.063      | 0.089    | 0.041        |
| Lena          | 0.977       | 0.956        | 0.953        | 0.064      | 0.089    | 0.053        |
| Female        | 0.965       | 0.902        | 0.954        | 0.038      | 0.068    | 0.096        |

Table 3 shows the pixel correlation coefficient of plain images and cipher images. It can be seen from the results in Table 3 that the pixel correlation coefficient of the cipher images is almost 0, so there is almost no correlation between adjacent pixels. Therefore, the results of statistical attack analysis show that the encryption algorithm has sufficient security.

3.4. Robustness analysis

Cropping attack can be used to analyze the robustness of the image encryption system. In order to analyze the robustness of this algorithm, we crop the cipher images. Figure 3(a)-(c) are Lena cipher images with 12.5%, 25% and 50% pixels cropped, and Figure 3(d)-(f) are their decrypted images.
Figure 3. Robustness of the encryption algorithm

We can see from Figure 3, even if some pixels of cipher images are cropped, the plain images are almost recoverable. Therefore, the algorithm proposed in this paper has good robustness.

4. Conclusions
In this paper, we combine 2D CS with DRPE to design an image compression and encryption algorithm. Firstly, we compress the image from two directions to obtain the measurement value. Then, DRPE is performed on the measurement value to obtain the final cipher image. Simulation results show that this algorithm has better image compression performance with higher efficiency, and can ensure security and robustness.

Acknowledgements
This work was supported by the following projects and foundations: project ZR2019MF054 supported by Shandong Provincial Natural Science Foundation, the National Natural Science Foundation of China (No.61902091) and Innovation Research Foundation of Harbin Institute of Technology (HIT.NSRIF.2020099), the Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-17-004), Equip Pre-research Projects of 2018 supported by Foundation of China Academy of Space Technology (No. WT-TXYY/ WLZDFHJY003)2017 Weihai University Construction Project.

References
[1] Zhou N, Zhang A, Zheng F, et al. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing[J]. Optics & Laser Technology, 2014, 62:152–160.
[2] Zhou N, Zhang A, Wu J, et al. Novel hybrid image compression–encryption algorithm based on compressive sensing[J]. Optik - International Journal for Light and Electron Optics, 2014, 125(18):5075-5080.
[3] Ponuma R, Amutha R. Compressive sensing based image compression-encryption using Novel 1D-Chaotic map[J]. Multimedia Tools & Applications, 2017.
[4] Chai X, Zheng X, Gan Z, et al. An image encryption algorithm based on chaotic system and compressive sensing[J]. Signal Processing, 2018, 148(jul.):124-144.
[5] Zhu S, Zhu C. A new image compression-encryption scheme based on compressive sensing and cyclic shift[J]. Multimedia Tools & Applications, 2019, 78(15):20855-20875.
[6] Xu Q, Sun K, Cao C, et al. A fast image encryption algorithm based on compressive sensing and
hyperchaotic map[J]. Optics and Lasers in Engineering, 2019, 121(OCT.):203-214.

[7] Yu-Guang Yang, Image compression-encryption scheme based on fractional order hyperchaotic systems combined with 2D compressed sensing and DNA encoding[J], Optics and Laser Technology 119 (2019) 105661.

[8] Zhou N, Pan S, Cheng S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics and Laser Technology, 2016: 121-133.

[9] Lu P, Xu Z, Lu X, et al. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique[J]. Optik-International Journal for Light and Electron Optics, 2013, 124(16):2514-2518.

[10] Zhou N R, Hua T X, Gong L H, et al. Quantum image encryption based on generalized Arnold transform and double random-phase encoding[J]. Quantum Information Processing, 2015, 14(4):1193-1213.

[11] Liu H, Liu Y B, Xu G X. Securely compressive sensing using double random phase encoding [J]. Advanced Materials Research, 2015, 926-930:3554-3558.