A novel encryption method combining software algorithm and spatial light modulator

Biao Wang[a,b], Yuxuan Zhang[a*], Yuhan Ma[a], Tao Lv[a], Xuchen Wei[a], Jiacheng Xie[a], Xu He[a]
[a] School of Instrument Science and Opto-electronics Engineering, Hefei University of Technology, Hefei, 230009, Anhui, China; [b] Anhui Province Key Laboratory of Measuring Theory and Precision Instrument, School of Instrument Science and Optoelectronics Engineering, Hefei University of Technology, Hefei 230009, Anhui, China

ABSTRACT

Images can convey information and needs to be protected, which is usually done by encryption. Traditional image encryption methods usually use software or hardware encryption, which has improvement approach in terms of better safety and robustness. And the study arouses sympathy to researchers based on both software and hardware encryption. This paper proposes an encryption method that combines software algorithm encryption and hardware encryption using a spatial light modulation (SLM) and 4f optical system. Firstly, the image is chaotically encrypted using the chaos encryption algorithm. Secondly, the discrete cosine transform (DCT) is adopted for further encryption based on chaos encryption picture. Thirdly, the cipher text image is transformed into the 4f system using SLM, which performs a random amplitude on the image to achieve hardware encryption. Finally, the simulation and experiment are performed to verify that the scheme, which shows that the method can realize the encryption and unencryption under the combination of software and hardware encryption. The proposed method has application value to guarantee the higher security of information.

Keywords: SLM, image encryption, 4f system, chaotic encryption, DCT

1. INTRODUCTION

The rapid development of the Internet has become a very important symbol of today's era. No matter at any time or any place, all people can publish all kinds of information through the Internet anytime and anywhere. However, while facing such a large amount of information sharing and enjoying the convenience brought by information, a large amount of information is facing more and more risks in the process of transmission. A large amount of information has been leaked, tampered and counterfeited. Therefore, how to ensure the security of information while delivering it has become a key issue for research.

In the development of the Internet and various multimedia technologies, images have become a very important information carrier, Therefore, the storage of image information and various security issues in transportation have also become the concern of many scholars. In order to solve the problem of image information security, encryption of image data has become a hot research direction today.

The traditional image encryption method usually only performs software encryption or hardware encryption once, which has improvement approach in terms of better safety and robustness. Therefore, it is urgent to research a better secure image encryption method. Under such a premise, an image encryption and decryption method based on chaotic DCT with spatial light modulator is proposed in this paper. First, the chaos encryption algorithm is applied to the grayscale image. The chaos algorithm belongs to an adaptive algorithm, which can disrupt the original pixel arrangement order in the image data, and then reorder the disrupted pixels, and because the original regularity disappears after the pixel arrangement is rearranged, a noise-like image will be generated, and then the encryption of the image will be completed. Secondly, after the chaotic encryption, we perform another DCT on the image to ensure the reliability of the encryption, which is a common image processing method, The DCT can be used to transform the pixel values describing the image in the spatial domain into DCT coefficients describing the image in the frequency domain, thus encrypting the image again after chaotic encryption. At this time, we obtained the image after the software secondary encryption. Thirdly, we build a spatial light modulator and 4f optical system to encrypt the image in hardware, that is, to perform a Fourier transform on the image. Finally, we

* 843007581@qq.com

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 1250604
 · 0277-786X · doi: 10.1117/12.2661821

obtain the ciphertext image after combining software encryption and hardware encryption, and then edit the decoding program to decrypt the encrypted image to obtain the decrypted image. To ensure the feasibility of the idea and the correctness of the experimental results, the encrypted images are simulated and decrypted simultaneously during the experiment.

2. CHAOTIC ENCRYPTION ALGORITHM

Chaotic encryption algorithm is an encryption method commonly used in image cryptography. Chaotic systems have good cryptographic properties such as initial value sensitivity, non-periodicity, non-convergence, and pseudo-randomness. Chaotic systems belong to a kind of nonlinear dynamical system. The sequences constructed by chaotic systems do not present a more obvious periodicity and symmetry, but they are not simply disorderly either and have a very rich internal structure[1]. It successfully avoids data scaling, thus reducing transmission costs and transmission delays, and has good encryption of images.

2.1 Chaotic encryption principle

Chaos encryption method is an image encryption method based on Logistic mapping, which is a one-dimensional sequence, and this dynamical system is very simple and therefore widely used in various aspects. Its principle equation is:

$$X_{k+1} = \mu * X_k * (1 - X_k), \quad (k = 0,1,\ldots,n) \tag{1}$$

A set of chaotic sequences can be obtained by using the logistic function for several iterations[2]. The chaotic sequence must satisfy the following two conditions: a, $0 < X_0 < 1$ and b, $3.5699456 < u <= 4$. On the basis of satisfying the above conditions, after *n* iterations, a chaotic sequence of $x_1, x_2, \ldots, x_n$ is obtained. By constructing two logistic chaotic sequences, y_1 and y_2, and transforming them so that their values are unified between 0 and 255, and using the transformed chaotic sequences to construct a two-dimensional matrix, the encrypted image is obtained by processing with the original image matrix[3].

2.2 Encryption method

To perform chaos encryption on grayscale images, two logistic chaotic sequences y_1 and y_2 are first constructed and transformed so that their values are unified between 0 and 255, and the transformed chaotic sequences are used to construct a two-dimensional matrix, which is processed with the original image matrix to obtain the encrypted image. The expressions of y_1 and y_2 are:

$$y_1(i) = (1/\pi) * \arcsin(\sqrt{(x_1(1))}) \tag{2}$$

$$y_2(i) = (1/\pi) * \arcsin(\sqrt{(x_2(1))}) \tag{3}$$

where x_1=0.3; x_2=0.5. After obtaining the two chaotic sequences, the loop is constructed and the original image is encrypted by y_1 and y_2 sequences with grayscale substitution[4]. The grayscale substitution operation is as follows:

$$k(n) = mod(floor(y_1(n) * 10\text{^}15),256) \tag{4}$$

$$k(n) = mod(floor(y_2(n) * 10\text{^}15),256) \tag{5}$$

After that, the gray value image can be obtained after chaotic encryption[5, 6]. The flow chart of the algorithm is shown in Figure 1.

2.3 Chaotic Encryption Simulation Results

According to the above idea, the program is edited to perform chaotic encryption on the grayed-out image, and the encryption result is shown in Figure 2.

It can be found that although some contours remain in the encrypted image compared with the original image, the overall image is basically not effectively distinguishable from the original image.

2.4 Chaos decryption

In order to obtain the information of the image before encryption, we also need to invert the encrypted image to obtain the original image information, in which the principle of inverse chaos is to perform an inverse loop on the image and replace the chaotic sequence obtained by equations (1) and (2) with an inverse operation using a xor operation. The image obtained after inverse chaos is performed on the encrypted image obtained in Figure 2 is shown in Figure 3.

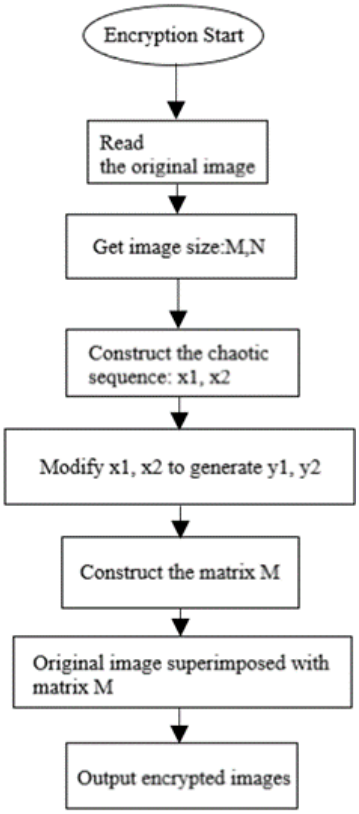

Figure 1. Chaotic encryption flow chart.

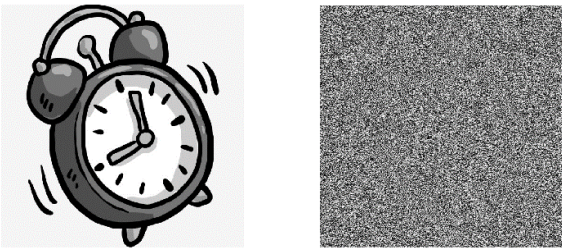

Figure 2. Chaotic encryption results.

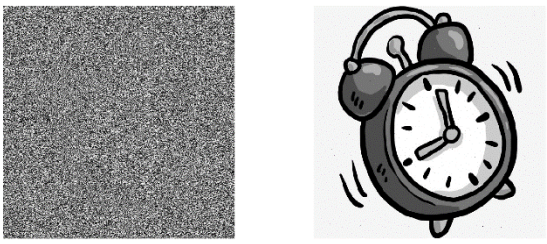

Figure 3. Chaos decoding.

It can be seen that under the conditions of software simulation, the decrypted image differs very little from the original image and does not lose much information. This proves that the idea and programming are correct.

3. DISCRETE COSINE TRANSFORM (DCT)

The full name of DCT is Discrete Cosine Transform, which is a common signal processing, image processing method, using the DCT can be converted from the pixel value of the image in the spatial domain to the DCT coefficients of the image in the frequency domain, which is mainly used for the compression of data or images, with good performance of de-correlation[7]. Because of its considerable encryption effect on the image, we perform secondary encryption on the encrypted ciphertext image using DCT after performing the chaos algorithm on the image.

3.1 DCT variation principle

The DCT is a transform related to the Fourier transform and can be used in image processing for signal and image data compression due to the strong "energy concentration" property of the discrete cosine transform: most of the energy of the natural signal is concentrated in the low frequency part of the discrete cosine transform[8]. For the DCT of the image we use a two-dimensional DCT variation, the principal equation of which is:

$$G(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} g(x,y)\cos\left(\frac{(0.5+x)u\pi}{8}\right)\cos\left(\frac{(0.5+x)v\pi}{8}\right) \quad (6)$$

The equations x and y refer to the coordinates of the pixel in the spatial domain, and u and v are the coordinates of the frequency domain of the basis function. The equation is based on an 8×8 image block and the range of x, y, u, v, are all from 0 to 7. In this formula:

$$\alpha(0) = \alpha(0) = \frac{1}{2\sqrt{2}}, \quad \alpha(u \neq 0) = \alpha(v \neq 0) = \frac{1}{2} \quad (7)$$

G in equation (6) represents the image block after DCT and g represents the original image block. In order to speed up the change and reduce the complexity of the operation, in this thesis we split the image into multiple 8×8 blocks, perform DCT on each block, and output the whole image at the end.

3.2 DCT encryption results

According to the principle of equations (5) and (6), edit the program and encrypt Figure 2. The result is shown in Figure 4.

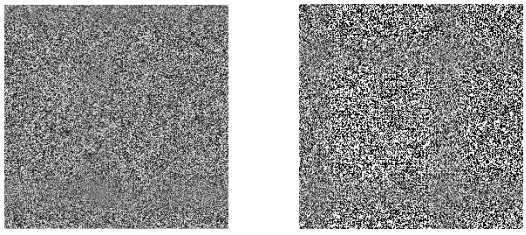

Figure 4. Image of DCT variation after chaotic encryption.

It can be seen that after the chaotic change and DCT change, the encrypted image is completely invisible to the information of the original image.

3.3 DCT decryption

When decrypting the image after DCT, we have to do the inverse DCT. The theoretical basis when doing the inverse DCT on the image is[9]:

$$g(x,y) = \alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} G(u,v)\cos\left(\frac{(0.5+x)u\pi}{8}\right)\cos\left(\frac{(0.5+x)v\pi}{8}\right) \quad (8)$$

The original matrix fast g is found. The decryption program is edited according to equation (8) and the decryption of Figure 4 is simulated, and the output image is shown in Figure 5.

In order to verify that the image after the inverse DCT is correct, we decrypt the obtained image using the procedure of chaotic decryption, and the obtained image is shown in Figure 6. It can be seen that it is consistent with Figure 3, which proves that the DCT encryption idea and decryption result are correct.

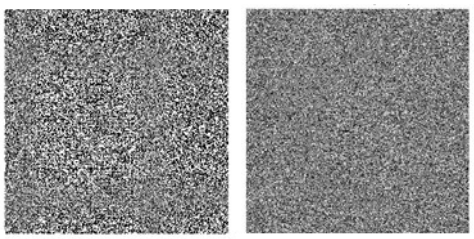

Figure 5. Chaotic image after inverse DCT.

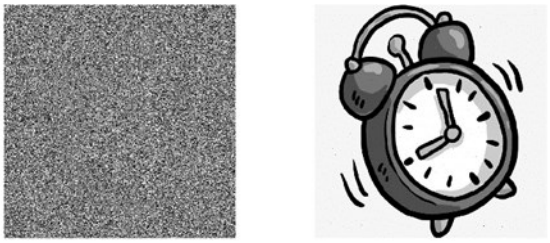

Figure 6. Chaos decryption results.

4. 4F SYSTEM

The 4F optical system is one of the typical optical systems whose main principle is the Fourier change of the light source. Optical Fourier transform technology can be used to realize image addition and subtraction, image differentiation, image encryption, etc.[10]. However, the 4f system may also introduce optical errors such as chromatic aberration and spherical aberration, which we need to avoid in our experiments[11]. In this paper, we have encrypted the image twice with software, and in order to improve the encryption effect, after using software encryption, we then use 4f optical system to perform Fourier change on the ciphertext image, thus achieving hardware encryption.

In the paper, the encrypted image is fed into the 4f system by using a spatial light modulator (SLM), which performs a random amplitude on the image to achieve hardware encryption[12]. And a CCD is placed on the output plane to receive the output image. In the paper, we use the zemax software, input the diameter, thickness, refractive index and other parameters of this lens, simulate the lens spacing when building a 4f system with this lens, and adjust it on this basis when building the optical system to finally determine the specific distance.

5. EXPERIMENTAL STRUCTURE CONSTRUCTION AND EXPERIMENTAL RESULTS

After determining the focal length of the 4f system, the experimental optical path structure is built according to the experimental principle, and the spacing of the 4f system lens is fine-tuned with reference to the results of zemax simulation. The schematic diagram is shown in Figure 7, where: 1 represents the external light source, 2 represents the spatial light modulator, 3 represents the 4f optical system, 4 represents the CCD, and 5 is the computer side.

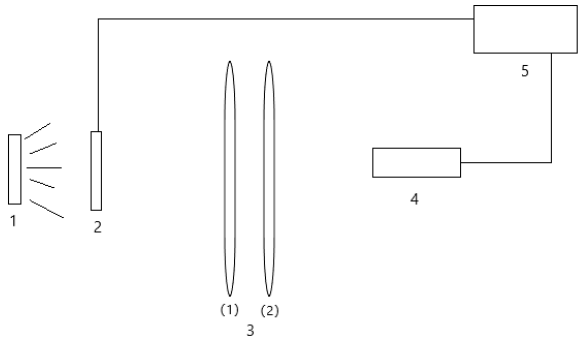

Figure 7. Optical path theoretical structure.

The light is provided by the external light source 1, which hits the spatial light modulator 2. The image on the spatial light modulator is input by the computer terminal 5 in advance, and since the spatial light modulator will generate light and dark pixel blocks according to the image input from the computer terminal, a black and white image can be generated on the spatial light modulator 2 according to the blocking of the pixel blocks to the light source. The image is then passed through a 4F lens, where (1) lens performs a Fourier change on the image, thus enabling hardware encryption. Afterwards (2) the lens performs an inverse Fourier change on the encrypted image, which is received by CCD 4. After that, the CCD uploads the image to the computer terminal 5. Then the size of the received image is adjusted and the received image is decoded according to the previously edited key to obtain a decrypted image. The final actual structure built is shown in Figure 8, and the images are encrypted and decrypted using this structure. In this case, the CCD captured image is shown in Figure 9.

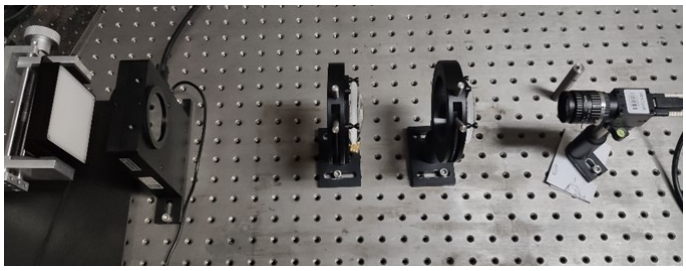

Figure 8. Actual structure diagram.

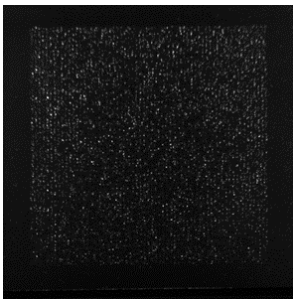

Figure 9. CCD drive captured pictures.

The image is decoded using the decryption program and the image obtained is shown in Figure 10.

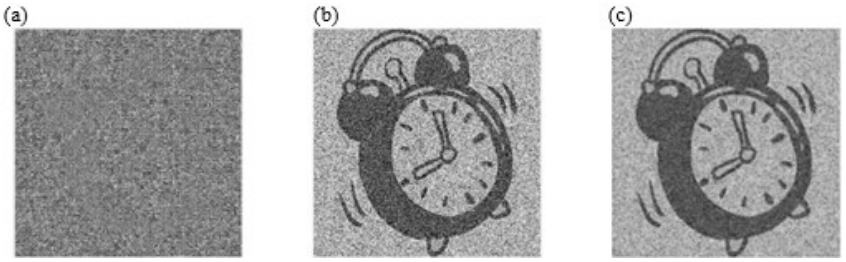

Figure 10. Graph of experimental results. (a) Inverse DCT; (b) Inverse chaos variation; (c) Optimized filtering.

Comparing with the theoretical result in Figure 6, we can see that compared with the original image, the decrypted image loses some details, such as reflection changes or excessive changes in color, but most of the main information of the original image is still retained, with more information retained in the high contrast part.

6. CONCLUSION AND DISCUSSION

In this paper, we improve the existing encryption techniques and propose a method that combines software and hardware encryption, and conducts simulations and performance tests for the proposed encryption method. The encryption system

designed in this paper has better safety and robustness comparing to the single encryption. The simulation results show that the encryption and unencryption method can well realize the original information. The experiment result shows that the combination encryption method can achieve the main information, but have some noise, which has negative effect on restoring the information. The proposed method has application value to guarantee the higher security of information.

However, according to the actual experimental results, although the decrypted image can identify the original image information, there is not a small noise pollution compared with the original image, which is not suitable for high precision image encryption and decryption. After analysis, the experimental decrypted image appears in this way may be due to the following reasons: (1) The Grayscale error in 4f system, in the 4f system will bring grayscale error to the system of many factors, monochromatic imaging or complex color imaging generated by chromatic aberration spherical aberration, etc. the lens will make the image distortion, chromatic aberration and wave phase difference. (2) The effect of random noise and coherent noise. In the general optical system, like dust, noise, thermal noise of optoelectronic devices, etc. will make the optical system produce random noise. As long as there is a slight unevenness on the system devices or distance problems, will produce coherent noise. (3) CCD photography, due to poor grasp of the external light source changes, making the capture of the photo light source is uneven and different from the original input image, resulting in the acceptance of encrypted image information is lost.

ACKNOWLEDGMENTS

This study was supported by National College Students; innovation and entrepreneurship training program (Grant No. 202010359054) and Young Teachers Teaching Research Project of Hefei University of Technology (Grant No. JYQN2015).

REFERENCES

[1] Zhang, Y. and Zhang, B., "Algorithm of image encrypting based on logistic chaotic system," *Application Research of Computers,* 32(6), 4(2015).
[2] Zhou, H., Xie, H. W., Zhang, H. and Zhang, H. T., "Parallel remote sensing image encryption algorithm based on chaotic map and DNA encoding," *Journal of Image and Graphics,* 26(05), 1081-1094(2021).
[3] Cheng, X., Di, X. and Li, J., "Optical image encryption algorithm based on multi chaos and fractional Fourier," *Journal of Nanjing University (Natural Science Edition),* 55(2), 251-263(2019). (in Chinese)
[4] Zhao, X., Jia, P. and Yang, Y., "Image encryption algorithm based on improved joseph traversal and piecewise logistic mapping," *Chinese Journal of Electron Devices,* 44(1), 6(2021).
[5] Liu, L. and Zhang, X., "Image encryption algorithm based on chaos and bit operations," *Journal of Computer Applications,* 33(04), 1070-1073(2013).
[6] Chen, L., Chen, Y. and Zou, P., "Research on image encryption technology based on chaos theory," *Computer Measurement & Control,* 27(8), 4(2019).
[7] Shan, Z. and Gong, T., "JPEG image encryption algorithm based on DCT transform," *Modern Computer,* (25)5, (2021).
[8] Han, Y., Jin, X., Guo, X., Liu, X. and Yang, X., "Application on digital blind watermarking algorithm based on block discrete cosine transform," *Optical Instruments,* 41(2), (2019).
[9] Zhu, P., [Research on Fast Algorithms of Discrete Cosine Transform], Huazhong University of Science and Technology, Master's Thesis, (2008). (in Chinese)
[10] Ma, S., Zeng, C. and Xu, F., "Teaching of 4f system with optical image encryption and decryption simulations," *Physical Experiment of College,* 31(06), 39-45(2018).
[11] Xia, C., Zhong, X., Liu, C., Han, P. and Jin, G., "Analysis of influence factors of resolution in high-resolution 4f imaging system," *Optics and Precision Engineering,* 24(07), 1573-1581(2016).
[12] Xu, P., [Measurement of Optical Modulation Characteristics of Liquid Crystal Spatial Light Modulator and Its Application in Optical Image Processing], Shandong University, Master's Thesis, (2005). (in Chinese)