An analysis method combining cryptographic analysis and image analysis

Zhonglin Yang[1], Yanhua Cao[1], Shuguang Wu[1,2], Haibin Li[1], Hang Chen[1,3*]

[1]School of Space Information, Space Engineering University, Beijing, 101416, China

[2]Beijing Space Information Relay and Transmission Technology Center, Beijing, China

[3]Universitéde Lorraine, CNRS, CRAN UMR 7039, Nancy, 54000, France

[*]Corresponding author: hitchenhang@foxmail.com

Keywords: color image encryption, known plaintext and chosen plaintext attacks, cryptography, performance analysis

Abstract: This paper introduces the concept of digital image and related cryptography, and summarizes and compares different performance analysis methods. Finally, it is concluded that a good performance analysis method needs to be used together with cryptographic analysis and image analysis.

1. Introduction

The development of multimedia technology has greatly enriched people's life. As the mainstream of multimedia, image has been widely used in all aspects of life. But some images involve personal privacy or trade secrets, or state secrets, and they need to be treated confidentially. At present, there are many methods for image encryption, such as traditional cryptography, chaos transformation, optical transformation and so on[1-8]. How to evaluate the encryption effect of an image becomes an important basis for selecting encryption methods.

In order to solve this problem, a cryptographic performance analysis method combining cryptographic analysis and image analysis is proposed in this paper. Firstly, histogram analysis is carried out on the image, which is the basic indicator of whether the encryption method is qualified. The key space test is then carried out. The key space is small, so a general attempt will be achieved. Then the key sensitivity test is carried out to observe whether a small change in the key has a relatively large effect on the result. Then carry out correlation test, good encryption method will make the correlation between image pixels to be very low, avoid correlation analysis attack. Then the robustness of the encryption method is tested, including shear attack and noise attack. Finally, the encryption effect is tested by traditional cryptanalysis methods.

The rest of this paper is organized as follows. In section 2, the concepts related to digital images and cryptography are introduced in detail. Integrated testing methods for cryptography and image analysis are given in section 3. Finally, the concluding remarks are summarized in the last section.

2. Basic knowledge of digital image encryption

The concept of digital image encryption can be explained from two aspects of digital image and cryptography.

2.1 The concept of digital images

Images can be divided into analog images and digital images according to whether they are discrete or not[9]. An analog image is a continuous image whose information changes continuously with the change of spatial position and direction. However, due to the limitation of computer hardware and software, it is necessary to sample the analog signal and convert it into discrete signal for the convenience of computer calculation. The discrete image thus obtained is a digital image, consisting of a limited number of pixels. Related concepts are as follows:

Pixel point: The smallest image unit.

  DOI: 10.25236/iwmecs.2022.008

Digital image: pixel point matrix composed of pixels, also known as the dot matrix. Pixels are generally represented as the abscissa in the matrix and the ordinate in the matrix, so the digital image can be expressed as. The number of pixels is related to the resolution of an image. Since the number of pixels in an image is fixed, the image will appear distortion when the image is enlarged and stretched.

Gray scale: the pixel value is the gray scale value, the range is generally 0-255, white is 255, black is 0, used to indicate the brightness of the image.

Channels: An image can be composed of a matrix of multi-layer pixels, each layer being a color channel. 1. Single channel: a pixel point is represented by a value; 2. Three channels: RGB mode, commonly known as color image, divides the image into three channels: red, green and blue, and all zeros are black; 3. Multi-channel: also known as multi-band or hyperspectral image, it not only contains color information, but also the spectral information of points.

Image resolution: number of pixels per inch in the image. The higher the resolution, the higher the pixel dot density, the more realistic the image.

Spatial resolution: The measure of the smallest discernible detail in an image. If the size of an image is $m*n$, indicating that a sample of $m*n$ was taken at the time of imaging, the spatial resolution is $m*n$.

2.2 The basic concepts of cryptography

Shannon proposed two principles of cryptographic encryption in 1949: confusion and diffusion. Confusion, also known as scrambling, only changes the order or spatial structure of the plaintext, so that the plaintext cannot be correctly interpreted, but does not change the content of the plaintext. Diffusion, also called replacement, diverts plaintext information into ciphertext to hide plaintext information. Here are some basic concepts of cryptography:

Plaintext: use P for information in the form of text, image, or video that needs to be transmitted confidentially.

Ciphertext: C indicates encrypted information.

Key: Parameter K used in the encryption process. It directly determines the encryption and decryption process. The space composed of all keys is called the key space.

Encryption algorithm: A correspondence E between the plaintext space and the ciphertext space, which can be understood as a function and is often expressed.

Decryption algorithm: A correspondence D between the ciphertext space and the plaintext space, which can be understood as the reverse algorithm of the encryption algorithm, often expressed.

The encryption process can be expressed mathematically as follows: $C = E(P, K)$

The decryption process can be expressed mathematically as follows: $P = D(C, K)$

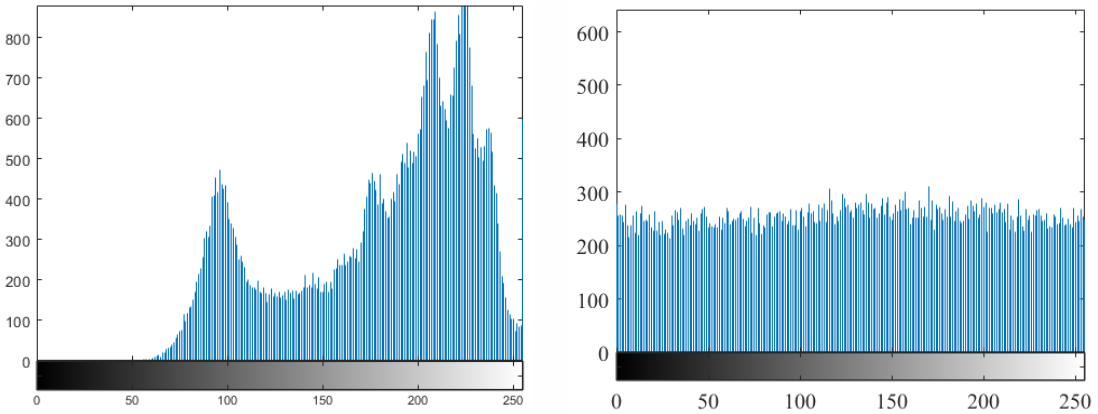
3. Synthetic analysis method

The comprehensive analysis method proposed in this paper combines cryptography analysis and image performance testing, and integrates all kinds of analysis methods in a logical sequence from simple to complex and from shallow to deep. The logical order of performance analysis is histogram analysis[10-11], key space analysis, key sensitivity analysis[12], correlation analysis[13], robustness analysis[14], known and chosen plaintext attack analysis[15-16].

3.1 Histogram analysis

According to the basic knowledge, the basic unit of an image is pixel, and the range of pixel value is generally 0-255. All pixel values of an image are counted and classified according to different pixel values, so the histogram obtained is the image histogram. So histogram analysis is a statistical attack method, a good image encryption scheme can resist this statistical attack method, which is the most basic performance of image encryption scheme. As shown in Figure.1, Figure.1(a) is the histogram of the original image, and Figure.1(b) is the encrypted histogram of the ciphertext image. According to Figure.1(a), the number of different pixel values can be obtained, while the

histogram of Figure.1(b) is smooth with uniform distribution of pixel values, from which it is almost impossible to obtain the number difference between different pixel values, which can resist statistical attacks.



(a) (b)

Fig.1 Histogram of plaintext image and ciphertext image

Scrambling does not change the pixel value, so just scrambling the image will not change the histogram distribution; Diffusion does not change pixel position, so in image encryption, scrambling and diffusion are generally used interspersed.

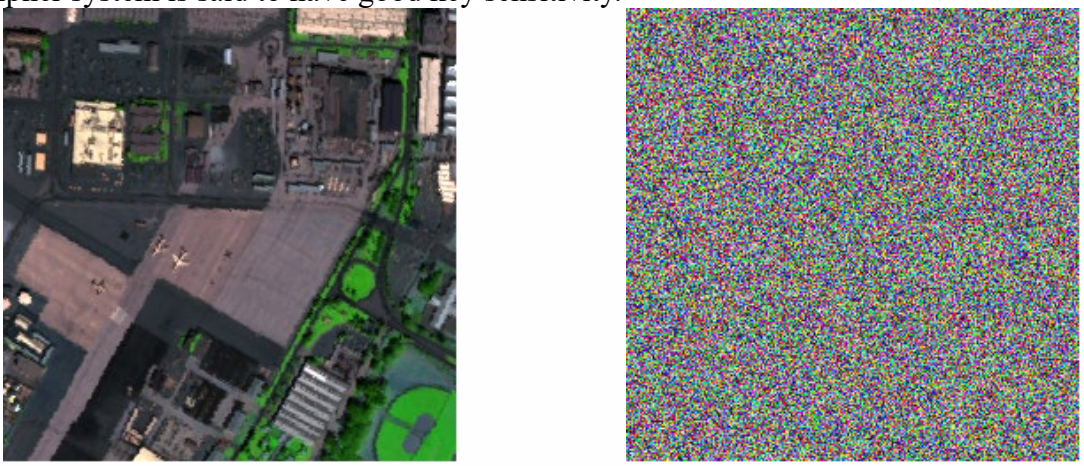
3.2 Key space analysis

Whether text encryption or image encryption, there is a simple and direct means of attack, namely brute force cracking. The method of brute force cracking is to try all possible keys, so to ensure the security of the image encryption scheme, that is, to ensure that there are enough numbers of different keys in the image encryption system, that is, enough large key space. It is proved theoretically that the key space must be larger than 2^{128} to enhance the ability of the algorithm to resist violent attacks.

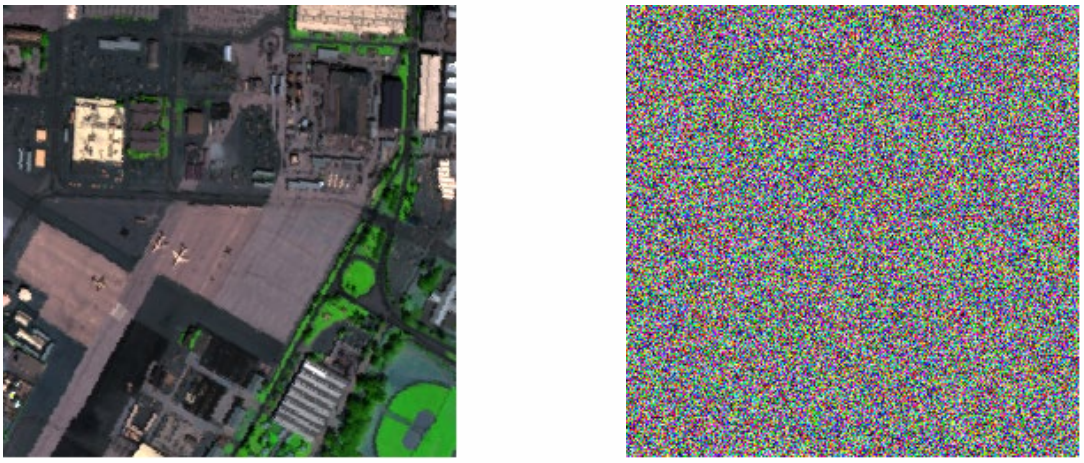
3.3 Key sensitivity analysis

A good encryption system must have good key sensitivity, that is, a slight change of key value in the decryption process will lead to a significant change in the decryption image. Only good key sensitivity can ensure the necessity of the existence of key space.

In the Fig.2, Fig.2(a) is the plaintext image, Fig.2(b) is the ciphertext image, Fig.2(c) is the image obtained by decryption with the correct key, and Fig.2(d) is the image obtained by decryption with the wrong key different from the correct key. Difference of two keys are 10^{-10}. Since there is a big difference between Fig.2(d) and Fig.2(a), almost no information about Fig.2(a) can be obtained, so the cipher system is said to have good key sensitivity.



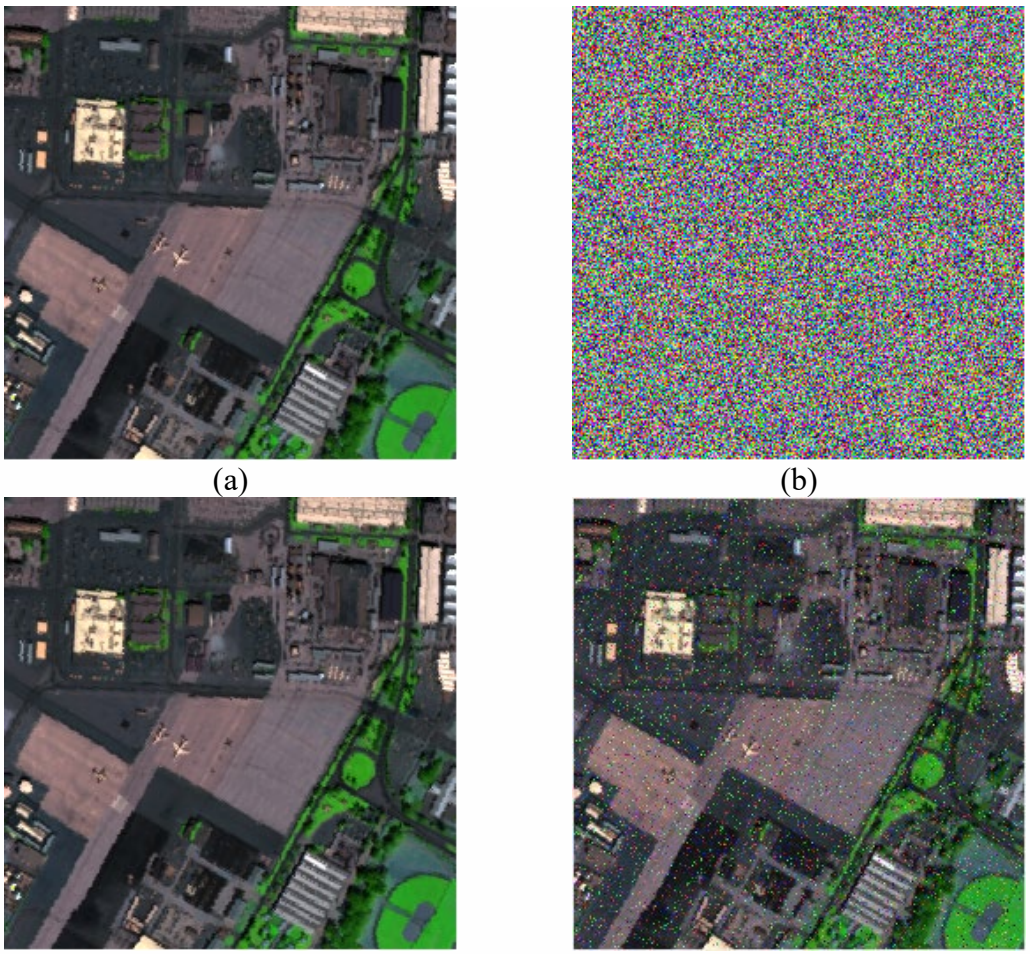
(a) (b)



(c) (d)

Fig.2 The diagram of key sensitivity analysis

In Fig.3, Fig.3(a) is the plaintext image, Fig.3(b) is the ciphertext image, Fig.3(c) is the image obtained by decryption with the correct key, and Fig.3(d) is the image obtained by decryption with the wrong key different from the correct key. Difference of two keys are 10^{-10}. Since the difference between Fig.3(d) and Fig.3(a) is very small, it is said that the key sensitivity of the cryptosystem is poor.



(a) (b)

(c) (d)

Fig.3 The diagram of key sensitivity analysis-2

3.4 Correlation analysis

The decrypted image seen from the figure is visually similar to the original image. So it's not enough just to visually judge the differences between images. A structural similarity exponential

function (SSIM) is introduced, and the difference between the decrypted image and the original image is considered. The closer SSIM value is to 1, the more similar the two images are. If SSIM value is 1, the two images are the same. The closer SSIM value is to 0, the greater the difference between the two images. The mathematical definition of SSIM can be expressed as

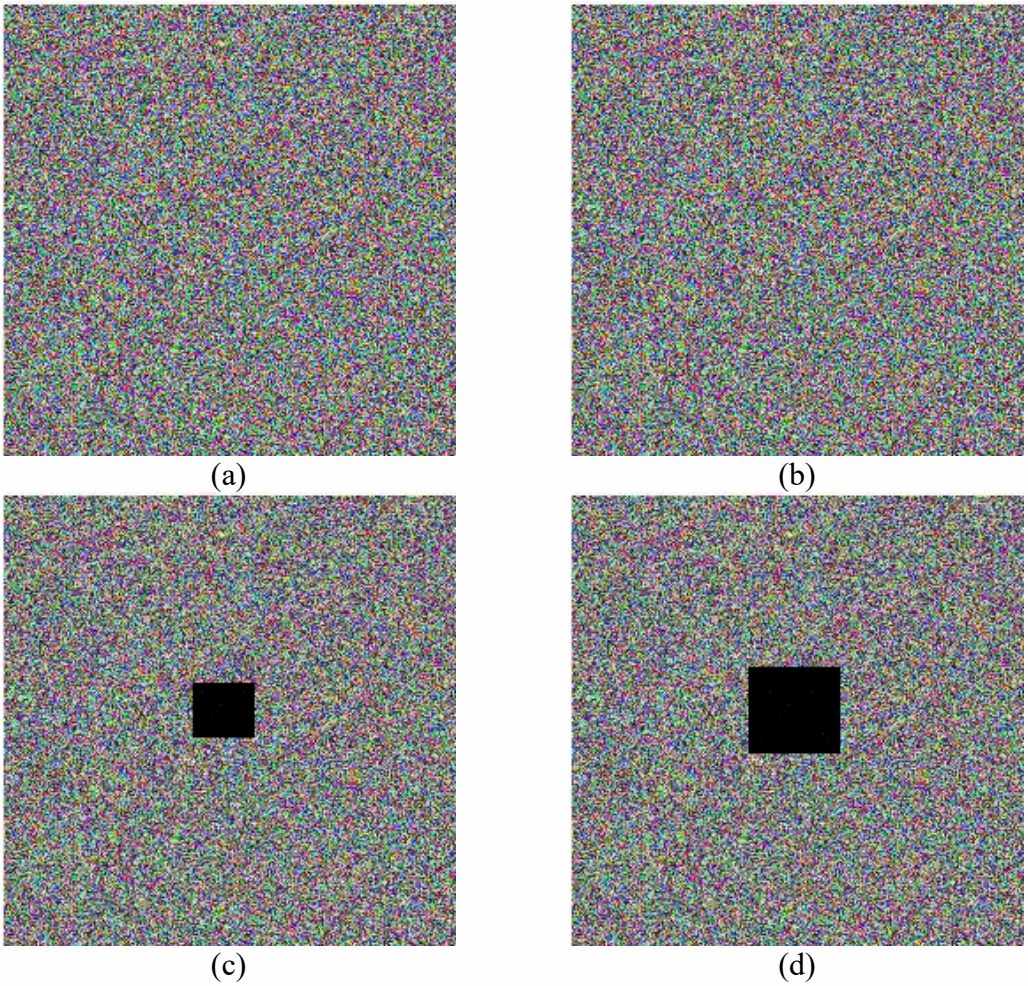
$$SSIM(x,y)=\frac{\left(2u_xu_y+c_1\right)\left(2\partial_{xy}+c_2\right)}{\left(u_x^2+u_y^2+c_1\right)\left(\partial_x^2+\partial_y^2+c_2\right)} \tag{1}$$

Where u_x is the average value of x, u_y is the average value of y, ∂_x^2 and ∂_y^2 is the variance of x and y respectively, ∂_{xy} is the covariance of x and y, and L is the image size, $c_1=\left(k_1L\right)^2$, $c_2=\left(k_2L\right)^2, k_1=0.01, k_2=0.03$.

3.5 Robustness analysis

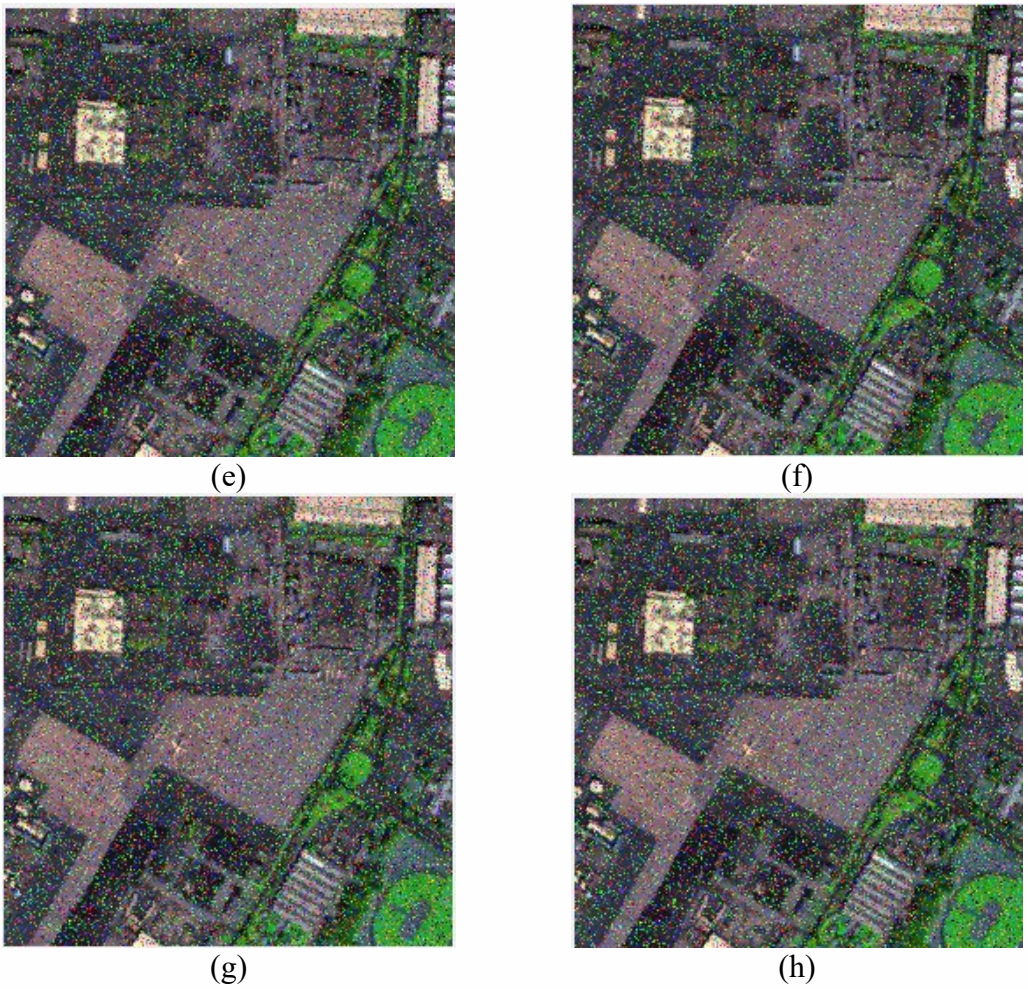
Robustness, also known as robustness and robustness, refers to the control system in a certain (structure, size) parameter perturbation, maintain some performance characteristics. In the process of image ciphertext transmission, some changes will inevitably occur due to objective environmental factors or artificial disturbance. We simulate the disturbance by adding noise or shearing the ciphertext image to test the robustness of the system.

For an example, Fig.4 shows an algorithm robustness analysis results, including Fig.4(a) and Fig.4(b) is to encrypt the image and the speckle noise added 0.23% and 5% respectively, Fig.4(c) is cut off 1% of the encrypted data encryption image, Fig.4(d) is cut off 4% of the encrypted image, Fig.4(e), Fig.4(f), Fig.4(g), Fig.4(h), respectively is Fig.4(a), Fig.4(b), Fig.4(c), Fig.4(d), the disclosure of the results.



(a) (b)

(c) (d)



(e) (f)

(g) (h)

Fig.4 The diagram of key robustness analysis

As can be seen from the above results, under the influence of noise and data loss, we can still clearly identify the decrypted image, which indicates that the algorithm has a good ability to resist data loss.

3.6 Cryptographic analysis

Cryptography and cryptanalysis are two parts of cryptography, which complement and restrain each other. A cryptographic coding system is secure if it can resist cryptanalysis attacks. According to the type and quantity of information obtained by attackers, attackers are classified into four categories, as shown in Table 1.

Table.1 Cryptanalysis method

Attack types	Information held by the attacker
Only ciphertext attacks	The encryption algorithm itself Obtained part of the ciphertext
Known plaintext attack	Select the encryption algorithm itself Obtained partial ciphertext One or more ciphertext plaintext pairs Part of the ciphertext obtained
Chosen plaintext attack	The encryption algorithm itself The plaintext information selected by yourself and the corresponding ciphertext generated by the key
Chosen ciphertext attack	The encryption algorithm itself Obtain a portion of ciphertext Self-selected ciphertext information and corresponding plaintext generated by the key

It can be seen from the table that the more known information, the greater the attack intensity, and the higher the possibility of decrypting the password.

Among the existing attack schemes, the known plaintext attack and the selected plaintext attack are the most widely used schemes to verifying the security of cryptosystem. Therefore, these two attack schemes are implemented against the proposed encryption system. First of all, an encryption model is defined and expressed as follows

$$\mathrm{EC}(x,y) = FN^{\alpha}\{\exp[i\cdot\delta_1(x,y)] * IM(x,y)\}\exp[i\cdot\delta_2(x',y')] \tag{2}$$

Where the symbol FN^{α} denotes the Fresnel transform with rotation angle α. Besides, the functions $\delta_1(x,y)$ and $\delta_2(x',y')$ represent two random phase masks. And the function $EC(x,y)$ is considered as the RGB components of the ciphertexts in this paper. Accordingly, the iterative phase retrieval algorithm and impulse function can be used as the known plaintext attack and chosen plaintext attack, respectively.

4. Conclusion

The comprehensive performance analysis method of image encryption proposed in this paper, which integrates image performance testing and cryptography analysis, has clear logic and complete structure, and has been applied in many research literatures. Encryption that passes this performance test method is generally considered secure.

References

[1] Haojiang, Gao, and, et al. A new chaotic algorithm for image encryption - ScienceDirect[J]. Chaos, Solitons & Fractals, 2006, 29(2):393-399.

[2] Kwok H S, Tang W. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos Solitons & Fractals, 2007, 32(4):1518-1529.

[3] Jui-Cheng, Guo J I. A new chaotic key-based design for image encryption and decryption[C]// IEEE International Symposium on Circuits & Systems. IEEE, 2000.

[4] Dang P P, Chau P M. Image encryption for secure Internet multimedia applications[J]. IEEE Transactions on Consumer Electronics, 2000, 46(3):395-403.

[5] Situ G, Zhang J. Multiple-image encryption by wavelength multiplexing[J]. Optics Letters, 2005, 30(11):1306-8.

[6] Guohai, Situ, Jingjuan, et al. Multiple-image encryption by wavelength multiplexing [J]. Optics Letters, 2005.

[7] Refregier P, Javidi B. Optical image encryption using input plane and Fourier plane random encoding[C]// Optical Implementation of Information Processing. International Society for Optics and Photonics, 1995.

[8] Seyedzadeh E M, Mirzakuchaki S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map[J]. Signal Processing, 2012.

[9] Gonzalez R C, Woods R E. Digital image processing[J]. Prentice Hall International, 2008, 28(4):484 - 486.

[10] Hernando M L, Marks L B, Bentel G C, et al. Radiation-induced pulmonary toxicity: a dose-volume histogram analysis in 201 patients with lung cancer[J]. International Journal of Radiation Oncology, Biology, Physics, 2001, 51(3):650-659.

[11] D Oetzel, Schraube P, Hensley F, et al. Estimation of pneumonitis risk in three-dimensional treatment planning using dose-volume histogram analysis[J]. Int J Radiat Oncol Biol Phys, 1995, 33(2):455-460.

[12] Plassmann K, Norton A, Attarzadeh N, et al. Methodological complexities of product carbon footprinting: a sensitivity analysis of key variables in a developing country context[J]. Environmental Science & Policy, 2010, 13(5):393-404.

[13] Hardoon D R, Szedmak S, Shawe-Taylor J. Canonical Correlation Analysis: An Overview with Application to Learning Methods[J]. Neural Computation, 2004, 16(12):2639-2664.

[14] Rosenhead J. Robustness analysis. In Rational analysis for a problematic world revisited. 2001.

[15] Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys. Opt Lett 2006; 31: 1044-6.

[16] Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt Lett 2006; 31: 3261-3.