Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9893172, 1 page
https://doi.org/10.1155/2023/9893172

Retraction

Retracted: Computer Network Security Management of Data Encryption Technology

Wireless Communications and Mobile Computing

Received 27 June 2023; Accepted 27 June 2023; Published 28 June 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

1. Discrepancies in scope
2. Discrepancies in the description of the research reported
3. Discrepancies between the availability of data and the research described
4. Inappropriate citations
5. Incoherent, meaningless and/or irrelevant content included in the article
6. Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Sun and W. Wang, "Computer Network Security Management of Data Encryption Technology," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6873087, 9 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6873087, 9 pages
https://doi.org/10.1155/2022/6873087

Research Article

Computer Network Security Management of Data Encryption Technology

Caiping Sun and Weijiang Wang

Guangzhou College of Technology and Business, Guangzhou Guangdong 510850, China

Correspondence should be addressed to Caiping Sun; suncaiping@gzgs.edu.cn

Received 30 June 2022; Revised 15 August 2022; Accepted 18 August 2022; Published 2 September 2022

Academic Editor: Mohammad Farukh Hashmi

With the continuous promotion of high and new technologies such as computers and big data, humans enter a new period-information age. Mass data and information can be transmitted and exchanged online through the network. In recent years, research on image encryption based on optical information processing technology is becoming more and more favored by researchers. In this regard, this study will focus on the research of encryption algorithms in optical images and realize encryption through fractional Fourier transform and Arnold transform. This article first introduces the research background of the subject and analyzes the current situation of the subject at home and abroad and then proposes the theoretical guidance basis for the subject research, which covers the fractional Fourier transform, Arnold transform, computational hologram, and picture evaluation index system. Finally, MATLAB simulation and performance analysis are carried out for fractional Fourier transform, Arnold transform, and holographic encryption technology. The results shows that the improved algorithm in this study performs better in the encryption and decryption process.

1. Introduction

With the popularity of mobile devices, the increase of hardware storage space, and the continuous development of computer networks, the unlimited speed and convenience of image transmission through the Internet save a lot of costs [1]. While the network provides convenience to users, it also brings great risks to users. The basic Internet protocol is not a security protocol. When the image information is finally encrypted and transmitted through the network, it can be directly exposed to the entire network [2]. This will provide criminals with a favorable criminal channel to obtain more image information on the network. Therefore, when we use image information communication, we need to strengthen network security protection measures and the research of digital image encryption technology to ensure social stability and national security issues. Most online information involves more personal privacy, such as personal private photos, patient photos, and weapon development. Once used by criminals, it will seriously affect national security [3, 4]. Data encryption technology is of great help to the Internet at this stage. This technology is to encrypt the relevant technologies of the password and then process the password for covert transmission. This is actually the core technical problem of computer security, to provide higher security for the data of the computer network.

Computer-generated hologram (CGH) is a process of simulating recording and manufacturing in a computer based on the principle of optical holography. Compared with optical holography, CGH replaces the field recording of optical holography equipment, simplifies the complexity of the experiment, and can complete the recording of virtual object holograms. It has the characteristics of high repeatability, low noise, and excellent operability, which makes CGH simpler and more flexible than optical holography. Compared with traditional image encryption, CGH image encryption solves the problem of difficult key distribution in traditional image encryption technology. It is more efficient to process images and the encryption performance is improved. With the application of fractional Fourier transform, Fresnel transform, double random phase coding, and

other algorithms in image encryption, the efficiency and capacity requirements of image encryption are gradually improved.

Based on the above analysis, we mainly carry out in-depth research on the use of computational holography for image encryption. In the process, this article focuses on the research on encryption algorithms in optical images and implements encryption design through fractional Fourier transform and Arnold transform [5, 6].

2. Methods

2.1. Namias-Type Fractional Fourier Transform. With the application of Fourier, there are new methods and new ideas for image processing. Compared with the traditional Fourier transform method, the fractional Fourier has a wider application of order, which makes the transform order able to be applied to the fractional problem. The study of fractional Fourier makes people enjoy the great achievements that it brings and creates numerous economic and social values. Fractional Fourier has different forms, but the Namias type and Shih type are often used.

The following is the one-dimensional Fourier transform method under the traditional method [7]:

$$\begin{aligned} G(f) &= \int_{-\infty}^{\infty} g(x) e^{-j2\pi f x} dx, \\ g(x) &= \int_{-\infty}^{\infty} G(f) e^{j2\pi f x} df. \end{aligned} \tag{1}$$

In formula (1), the integration processing operation process demonstrated is the Fourier integral that we are more familiar with daily. The function $G(f)$ is the Fourier transform of the function [8]. If $g(x)$ is a function expression corresponding to a physical quantity in a certain space domain, then, $G(f)$ is a function expression corresponding to $g(x)$ in a frequency domain. When $G(f)$ is a complex function, it can be expressed as follows:

$$G(f) = A(f) e^{j\Phi(f)}. \tag{2}$$

After Namias-type fractional Fourier transform, the corresponding function integral form of one-dimensional function [9] is as follows:

$$F^{\alpha}\{f(x)\} = \int_{-\infty}^{+\infty} f(x) B_{\alpha}(x, x_{\alpha}) dx, \tag{3}$$

where

$$B_a = \frac{\exp\left[j\left(pf'/4 - f/2\right)\right]}{\sqrt{|\sin f|}} \exp\left[jp\left(x^2 \cot f - 2xx_a + x_a{}^2 \cot f\right)\right] \tag{4}$$

In the formula, $\phi = \alpha\pi/2$, $\phi' = \text{sgn}(\sin\phi)$, α is the transformation order of the fractional Fourier transform.

It is worth explaining that when $\alpha = 1$ or -1, formula (4) is traditional Fourier transform or inverse transform; when $\alpha = 0$ or 2, formula (4) has no meaning, so when $\alpha = 0$ or 2, formula (4) can be redefined as follows:

$$\begin{aligned} F^0\{f(x)\} &= f(x), \\ F^2\{f(x)\} &= f(-x). \end{aligned} \tag{5}$$

2.2. Shih-Type Fractional Fourier Transform. The whole process mainly revolves around one-dimensional processing, and the related mathematical transformation forms are as follows:

$$\begin{aligned} G(f) &= \int_{-\infty}^{\infty} g(x) e^{-j2\pi f x} dx, \\ g(x) &= \int_{-\infty}^{\infty} G(f) e^{j2\pi f x} df. \end{aligned} \tag{6}$$

The integrals involved in formula (6) are usually called Fourier integrals. The function $G(f)$ is the Fourier transform of the function or called the frequency spectrum. If $g(x)$is a function expression corresponding to a physical quantity in a certain space domain, then G(x) is a function expression corresponding to a frequency domain.When $G(f)$ is a complex function, it can be expressed as follows:

$$G(f) = A(f) e^{j\Phi(f)}. \tag{7}$$

The frequency spectrum of aperiodic functions is a continuous or piecewise continuous function of frequency, not a discrete function. Generally speaking, the inverse Fourier transform is the frequency complex index obtained after a certain weighting process and the components are superimposed to obtain the required original function $g(x)$. The functions $g(x)$ and $G(f)$ are combined into a pair of Fourier transform operations.

After combined with shih-type transformation processing, the corresponding function integral form of one-dimensional function $f(x)$ is as follows:

$$\begin{aligned} F^{\alpha}\{f(x)\} = \sum_{n=0}^{3} &\cos\left[\frac{(\alpha - n)\pi}{4}\right] \cos\left[\frac{2(\alpha - n)\pi}{4}\right. \\ &\times \exp\left[-j\frac{3(\alpha - n)\pi}{4}\right] f_{\eta}(x). \end{aligned} \tag{8}$$

2.3. Properties of Fractional Fourier Transform. Generally speaking, the two types of fractional Fourier transform methods have the following corresponding characteristics:

(1) Obvious boundary. The fractional Fourier transform is essentially the same as the traditional transform; especially if the order of the fractional Fourier transform is an integer value, it can be easily converted to the traditional Fourier form without any difference

(2) The function shows continuity. This point means that fractional Fourier can perform continuous function transformation in two-dimensional space

(3) Additivity of functional expressions. For the fractional Fourier transform of any order of p_1 and p_2, its expression is as follows:

$$F^{p_1}\{F^{p_2}\{f(x)\}\} = F^{p_2}\{F^{p_1}\{f(x)\}\} = F^{p_1+p_2}\{f(x)\} \quad (9)$$

(4) Convolution. These two functions satisfy in the fractional convolution

$$F^{p}\{f(x) * g(x)\} = F^{p}[f(x)]] \times F^{p}[g(x)] \quad (10)$$

In special cases, Namias-type fractional Fourier transform also has the following properties [9]:

$$\begin{aligned} F^{p} &= F^{p+4}\{f(x)\}, \\ F^{p}\{f(x+t)\} &= F^{p}\{f(x+t\cos t)\}\exp\left[jt\sin t\left(x+\frac{t\cos t}{2}\right)\right], \\ F^{p}\{f(x)\exp(jbx)\} &= F^{p}\{f(x-b\sin\phi)\}\exp\left[jb\cos\phi\left(x-\frac{\phi\sin\phi}{4}\right)\right]. \end{aligned} \quad (11)$$

2.4. Optical Realization of Fractional Fourier Transform. Regarding the optical application under the fractional Fourier transform algorithm, related scholars have used the optical properties of the lens a long time ago to achieve fractional Fourier transformation of the image [9]. This idea has been well confirmed and the related principle [10] method is shown in Figure 1 as follows:

The optical path propagation mode shown in Figure 1 is a combination method of a lens, which is also called a single-lens method here. It can be seen that the entire system is divided into two parts: input and output [10, 11]. There is a plane L1 as a single input plane, which is then transferred to the lens L and then transferred from the lens L to the plane L2 and output via L2. The focal length of the lens L here is f, and the distance between the lens distance fractional Fourier L1 plane and the L2 plane is d. The quantitative relationship between the entire related parameters satisfies the following:

$$d = \left[1-\cos\left(\frac{\alpha\pi}{2}\right)\right]f. \quad (12)$$

According to the meaning of the abovementioned formula, if the focal length f of the lens is a certain value, then, if the distance parameter d is changed appropriately, the first-order fractional Fourier transform operation can be realized here.

2.5. Scrambling Technique of Arnold Transform. The processing principle of this type of method is to use a certain conversion method to change the different pixel points or gray values in a picture, so as to convert the original image display information content into the content that others

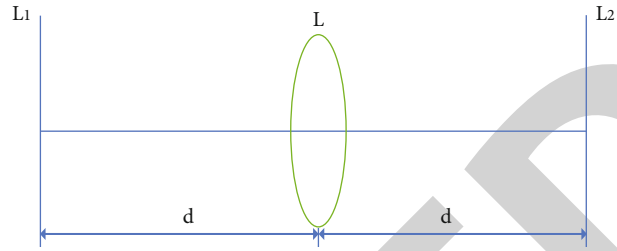


Figure 1: Fractional Fourier transform light path diagram.

cannot understand, thereby realizing the effect that people who want to obtain information cannot really recognize. Under normal circumstances, the transformation process can be marked and the specific description can be seen in formulas (13) and (14), where N is the order of unprocessed information, that is, the digital image matrix that needs to be encrypted. The gray scale of the smallest unit in the image to be processed can be combined with (x, y) and marked as Ux.

$$U_{xy} = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1N} \\ u_{21} & u_{22} & \cdots & u_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{N1} & u_{N2} & \cdots & u_{NN} \end{bmatrix}, \quad (13)$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N), \quad x, y \in \{0, 1, \cdots, N-1\}. \quad (14)$$

In the abovementioned formula, (x, y) represents the coordinates of the smallest unit that needs to be transformed on the original image and (x', y') is the coordinate of the processed smallest unit on the encrypted image, where N indicates the order of the matrix, which is also the size of the image to be processed. When the image to be processed is a square, it needs to be modulo when performing calculations, so it can be ensured that the smallest unit coordinate after processing can be within the range of the matrix subscript [12].

When using this method to transform the position of digital image pixels, the main principle is to replace the position of the smallest unit in Figure 1 with formula (14), that is, to transform the position of each smallest unit (x, y). In this process, due to the changes in the parameters of the smallest unit in the graph, the grayscale curve also shows different distribution states, blurring the information of the original digital image, and then completing the encryption [13, 14]. Under normal circumstances, an image encryption target executes the transformation algorithm once and can only complete one-to-one position exchange. However, to complete the encryption processing of the target, it is often necessary to repeat the cat face transformation, gaining better encryption effect by iterative execution.

The information in the image processed by the algorithm will become blurred, and the image presented is similar to white noise. At this time, the first encryption process

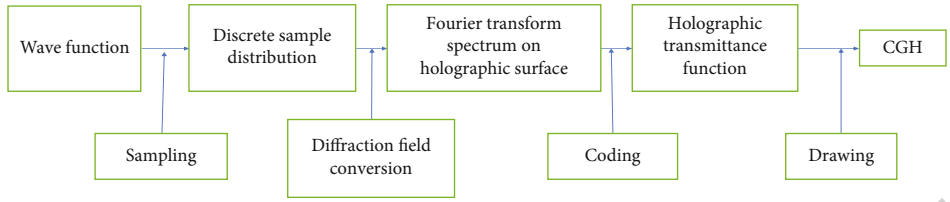


Figure 2: Flow chart of the computational hologram.

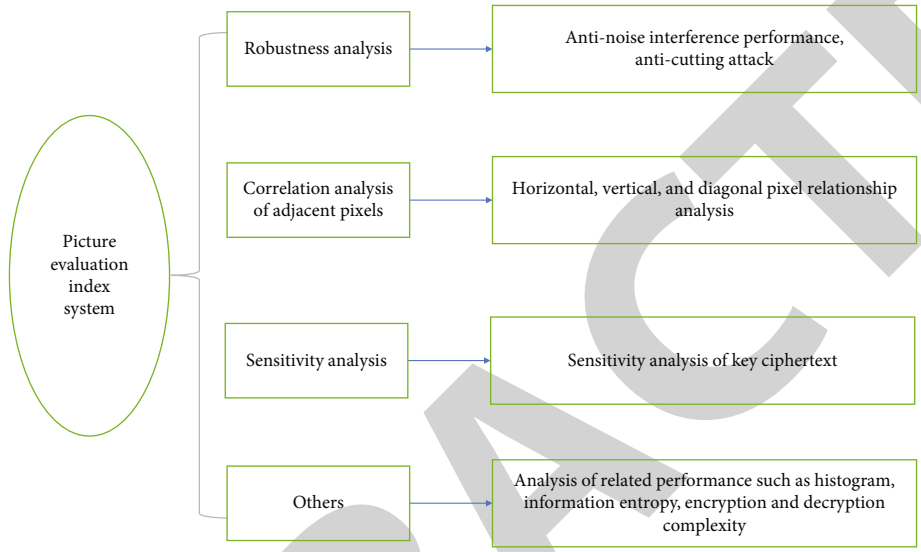


Figure 3: Picture evaluation index system.

of the original image is completed and the secret key can be expressed by the number of iterations performed in the process. In the process of repeatedly performing the conversion operation for a certain number of times, a special situation will occur, that is, the processed image is restored to the original image. It can be seen that the processing in this way has periodicity and the recovery operation of the encrypted digital image can be completed through this characteristic, so that it can complete the decryption in the reverse scrambling.

2.6. Computational Holography. Computer-type holograms need to be calculated according to data and also need to use modern optical principles. However, it can only draw the figure through computer control after the mathematical process of the object wave is processed by a computer without the aid of physical entities. It can also record it to the corresponding device, so as to achieve the drawing effect of the simulated interferogram and copy it to the film. The computer-generated hologram can not only record the amplitude and phase of the light wave relatively comprehensively but also record some complex comprehensive information and the object information that must be recorded in the hologram. Therefore, it has relatively unique advantages and great flexibility.

The flow of the hologram is shown in Figure 2.

2.7. Picture Evaluation Index System. Due to the characteristics of encrypted and decrypted images, specific performance analysis can be done according to the picture evaluation system indicators [15]. The image evaluation system indicators include four major aspects: robustness analysis, adjacent pixel correlation analysis, sensitivity analysis, and others. The specific indicators are as follows (Figure 3):

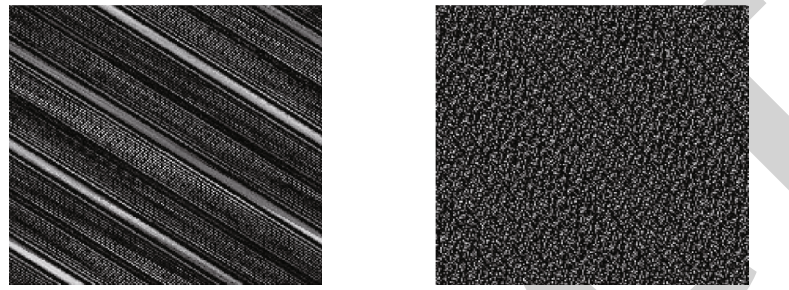
This chapter mainly introduces the theoretical basis of optical image encryption. Firstly, the concept and properties of Namias-type and Shih-type fractional Fourier transform are introduced and the optical implementation of fractional Fourier transform is analyzed. Then, the concept and principle of the scrambling technique of Arnold transform are expounded. Finally, the concept and characteristics of CGH are summarized and the image evaluation index system is established, which lays a theoretical foundation for the research of optical encryption in this paper.

3. Results and Analysis

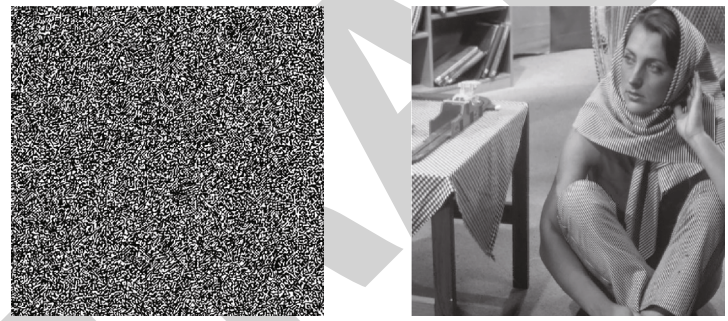
3.1. Image Encryption Simulation and Performance Analysis of Arnold Transform

3.1.1. Simulation of Image Encryption Based on Arnold Transform. For Arnold's optical image encryption algorithm, MATLAB simulation is used to decode with the correct key. Figures 4(a) and 4(f) show the original image and the decrypted image, respectively, and Figures 4(b)–4(e) describe the Arnold transformation image that has undergone once, twice, eight, and fifteen times, respectively.

(a) The original image before Arnold transform encryption (b) The image after Arnold transform once



(c) The image after Arnold transform twice (d) The image after Arnold transform eight times



(e) The image after Arnold transform fifteen times (f) Decrypted image

Figure 4: The image processing.

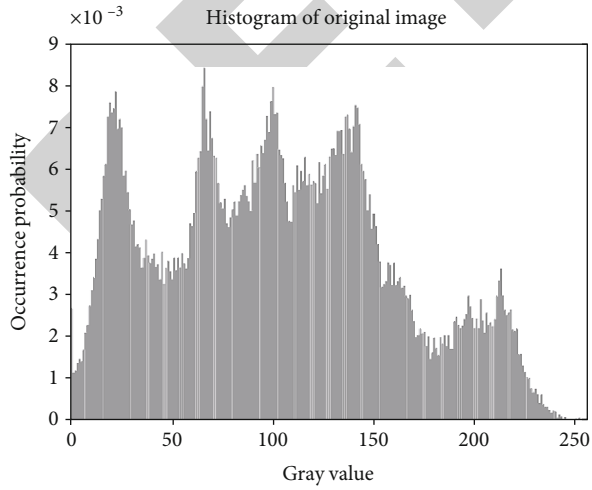


Figure 5: The histogram of the original image of the Arnold transform image encryption algorithm.

3.1.2. Performance Analysis of Image Encryption Based on Arnold Transform. Figures 5 and 6 show the histograms of the original image and encrypted image of the Arnold transform encryption algorithm.

As can be seen in Figures 5 and 6, the graphics of the original image and the coded image are completely different, so the Arnold conversion encryption algorithm has a better coding effect [16, 17]. In addition, by comparing the PSNR and CC values of the original image and the decrypted image, the results can be seen in Table 1.

The calculation results in Table 1 can show that the PSNR of the very low encryption process is very low, indicating that the encryption quality is very high, and the analysis itself can obtain high decryption quality [18].

3.2. Image Encryption Simulation and Performance Analysis Based on Fractional Fourier Transform

3.2.1. Image Encryption Simulation of Fractional Fourier Transform. The principle of the complete encryption algorithm described in this document is based on the Mach-Zed interference structure outside the axis. (x, y) is the space coordinate, (ξ, n) is the holographic plane coordinate, and the real value function $f(x, y)$ represents the encrypted 2D

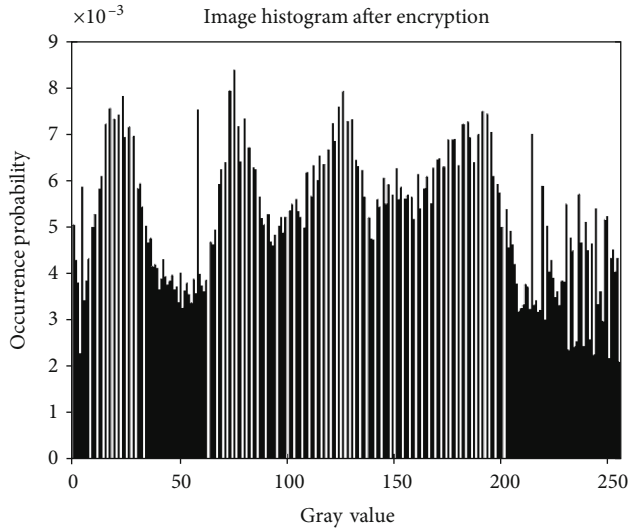


Figure 6: Encryption graph histogram of the Arnold transform image encryption algorithm.

Table 1: Peak signal-to-noise ratio and correlation coefficient of the Arnold transform encrypted image and decrypted image.

Process	Parameter	
	Peak signal-to-noise ratio (PSNR)	Correlation coefficient (CC)
Encryption	9.3214	−0.0071
Decrypt	25.9574	0.8473

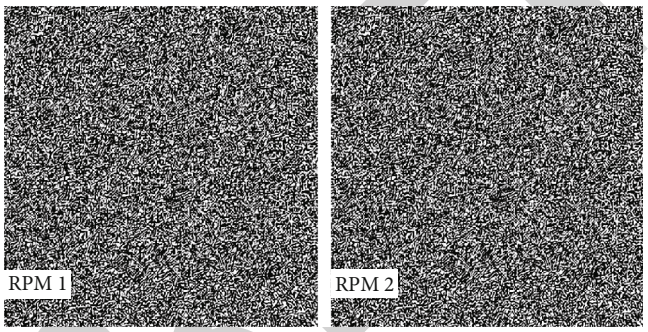


Figure 7: Random phase mask (RPM1 and RPM2).

image. The initial image $f(x, y)$ is phase encrypted, the value is expressed as exp [if(x, y)], the light from the phase mask $p(x, n)$ is used for interference, and the CCD records the encrypted image information. At the same time, the computed hologram of the encrypted image is recorded and digitally reconstructed [19]. The intensity $I_H(\xi, n)$ of this computed hologram has two light interferences expressed in the Fourier domain as follows:

$$\begin{aligned} I_H(\xi,\eta) &= |F(\xi,\eta) + p(\xi,\eta)|^2 \\ &= |F(\xi,\eta)|^2 + |p(\xi,\eta)|^2 \\ &\quad + F^*(\xi,\eta)p(\xi,\eta) + F(\xi,\eta)p^*(\xi,\eta). \end{aligned} \tag{15}$$

Figure 8: Original image before encryption by fractional Fourier transform.

$F(\xi, \eta)$ represents the Fourier transform of exp [if(x, y)]. $p(x, n)$ is selected as the phase function exp $[i\varphi(\xi, \eta)]$; here, (ξ, η) is uniformly distributed on $(0, 2\pi)$. It can be obtained by encrypting the power spectrum of the image and the reference light. $I'_H(\xi, \eta)$ can be obtained using the following data:

$$I'_H(\xi,\eta) = F^*(\xi,\eta)p(\xi,\eta) + F(\xi,\eta)p^*(\xi,\eta). \tag{16}$$

In the formula, by multiplying the random phase mask $R'(\xi, \eta)$, the mathematical expression is a phase function, that is, $R'(\xi, \eta) = \exp[i\varphi'(\xi, \eta)]$, where (ξ, m) is a function of $(0, 2\pi)$ uniform distribution; $I'_H(\xi, \eta) \times R'(\xi, \eta)$ is the result of transforming Fourier into a numerical value, which is called the encrypted image.

The cryptographic hologram is recorded by removing the original physical and transformation lens and single-band planar illumination as follows:

$$k(\xi,\eta) = |1 + p(\xi,\eta)|^2 = |1|^2 + |p(\xi,\eta)|^2 + p^*(\xi,\eta) + p(\xi,\eta). \tag{17}$$

Referring to formula (16), $k'(\xi, \eta)$ can be obtained by using the following password hologram:

$$k'(\xi,\eta) = p^*(\xi,\eta) + p(\xi,\eta). \tag{18}$$

For the decryption process, we first perform Fourier transform on the encrypted image, then multiply it by the total of the random phase mask $R'(\xi, \eta)$, and multiply it with the conjugate function; we get formula (16). By multiplying formulas (16) and (18), we can get the following formula:

$$\begin{aligned} I'_H(\xi,\eta) \times k(\xi,\eta) &= [F^*(\xi,\eta)p(\xi,\eta) + F(\xi,\eta)p^*(\xi,\eta)] \\ &\quad \times [p^*(\xi,\eta) + p(\xi,\eta)] = F^*(\xi,\eta) \\ &\quad + F(\xi,\eta) + F^*(\xi,\eta) \times [p(\xi,\eta)]^2 \\ &\quad + F(\xi,\eta) \times [p^*(\xi,\eta)]^2. \end{aligned} \tag{19}$$

Formula (19) is a numerical transformation of Fourier, where the first and second terms refer to the enhancement

Figure 9: Fractional Fourier transform encrypted image.

Figure 10: Decrypted image of fractional Fourier transform.

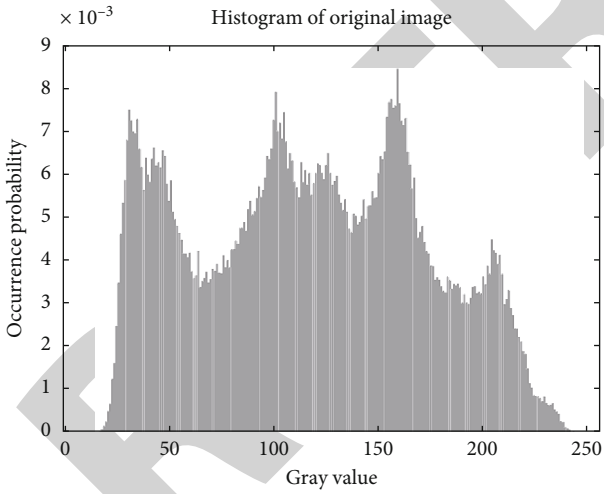


Figure 11: The original image of the Fourier transform image encryption algorithm histogram.

of two conjugate images on different optical axes [20]. The third and fourth items are Fourier transform into a random phase mask to amplify the background noise. The decoded image is a phase image, and it still needs to be converted into an amplitude image.

$$R_D = A_R \exp\left[i\left(\frac{2\pi}{\lambda}\right)\left(k_x m\Delta x + k_y n\Delta y\right)\right]. \quad (20)$$

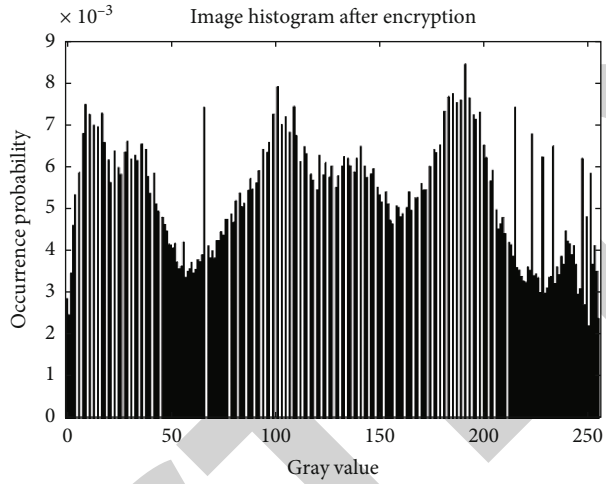


Figure 12: Encryption diagram of Fourier transform image encryption algorithm histogram.

A_R represents the amplitude, and $\Delta x, \Delta y$ is the pixel size of the CCD camera. The parameter (k_x, k_y) is a band vector element and must be adjusted to ensure that the propagation direction is as close as possible to the experimental reference wave. Amplitude A_R can usually be set to 1.

In order to analyze the performance of the encryption algorithm based on fractional Fourier transform, this paper uses MATLAB software to carry out numerical simulation. According to the algorithm described in the previous section, the original image used in the Fourier-based holographic encryption simulation is selected as Barbara's grayscale image with a pixel distribution of 512×512 and the pixel size of the camera is $44\,\mu\text{m} \times 44\,\mu\text{m}$. The Fourier wavelength is 600 nm. We use random phase mask (RPMI) to encrypt the optical path of the object and use random phase mask (RPM) to encrypt the reference optical path [21]. The random phase mask can be seen in Figure 7.

By using the holographic optical image encryption algorithm used for Fourier decomposition transformation and the MATLAB simulation technology, we use the correct key to decrypt and the original image and encryption and decryption diagrams are shown in Figures 8–10.

3.2.2. Performance Analysis of Image Encryption Based on Fractional Fourier Transform. In order to have a deeper understanding of the performance of the encryption algorithm, this paper introduces three parameters: histogram, correlation coefficient CC, and peak signal-to-noise ratio PSNR to analyze the encryption performance of optical images. Among them, the peak signal-to-noise ratio (PSNR) is defined as follows:

$$\begin{aligned} \text{PSNR(dB)} &= 10\lg\frac{P^2}{\text{MSE}}, \\ \text{MSE} &= \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|f(x,y) - f_D(x,y)\right|^2. \end{aligned} \quad (21)$$

Table 2: Peak signal-to-noise ratio and correlation coefficient of Fourier transform encrypted image and decrypted image.

Process	Parameter	
	Peak signal-to-noise ratio (PSNR)	Correlation coefficient (CC)
Encryption	11.3254	−0.0001
Decrypt	25.5472	0.8745

The histogram of the image can show the gray distribution of the value and spatial frequency of the image. If there is a big difference between the two images, there is a difference between the two images. The smaller the CC and the value, the greater the difference between the two images. Therefore, the above three parameters are mainly used to indicate the similarity of two images. Figures 11 and 12 are the histograms of the original image and encrypted image of the fractional Fourier transform encryption algorithm.

As can be seen in Figures 11 and 12, the graphics of the original image and the encoded image are completely different, so the encryption algorithm of the fractional Fourier transform image is more effective. We compare the PSNR and CC values of the original image and the decrypted image, and the results are shown in Table 2.

From the calculation results in Table 2, it can be shown that the PSNR of the very low encryption process is very low, indicating that the encryption quality is very high. The same analysis may indicate that the decryption quality is very high.

4. Conclusions

In recent years, research on image encryption based on optical information processing technology is becoming more and more favored by researchers. In this regard, this study will focus on the research of encryption algorithms in optical images and realize encryption through fractional Fourier transform and Arnold transform:

(1) The theoretical basis of optical image encryption is introduced, and the scrambling technology of fractional Fourier transform, Arnold transform, computational holography, and picture evaluation system indicators are introduced. First, the concept and properties of the Namias-type and shih-type fractional Fourier transform are introduced and the optical realization of the fractional Fourier transform is analyzed. Then, the concept and principle of the scrambling technique of Arnold transform are explained. Finally, the concept and characteristics of computational holography are summarized and a picture evaluation index system is established at the same time, which lays a theoretical foundation for the optical encryption research in this article

(2) We perform simulation and performance analysis for computational holographic encryption algorithms. First, we use MATLAB software for simulation and performance analysis to compare different algorithms; calculate the histogram, peak signal-to-noise ratio PSNR, and correlation coefficient CC of each image; and analyze the encryption and decryption effects of each algorithm

(3) We improve the encryption algorithm of the computational holographic image based on fractional Fourier. Combined with Arnold transform, we compare the image of the algorithm encryption and decryption process and calculate the histogram, peak signal-to-noise ratio PSNR, and correlation coefficient CC of each image. The result shows that the improved algorithm performs better in the encryption and decryption process

Data Availability

The figures and tables used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to show sincere thanks to the techniques that contributed to this research.

References

[1] J. H. Wang and H. B. Wang, "Computer local area network security and management," *Advanced Materials Research*, vol. 1079-1080, pp. 595–597, 2014.

[2] R. W. Shirey, "Security requirements for network management data," *Computer Standards & Interfaces*, vol. 17, no. 4, pp. 321–331, 1995.

[3] D. Melas, I. Ziomas, and I. Kioutsioukis, "Real time calculation of the dispersion of air pollutants from industrial stacks using a personal computer," *Fresenius Environmental Bulletin*, vol. 7, no. 3, pp. 134–140, 1998.

[4] A. J. Babatunde and F. A. Ejiga, "Network security management: solutions to network intrusion related problems," *Global Journal of Computerence & Technology*, vol. 12, no. 6, pp. 239–244, 2014.

[5] O. E. Muogilim, K. K. Loo, and R. Comley, "Wireless mesh network security: a traffic engineering management approach," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 478–491, 2011.

[6] J. Homer and X. Ou, "Sat-solving approaches to context-aware enterprise network security management," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 3, pp. 315–322, 2009.

[7] E. Okamoto and K. Tanaka, "Identity-based information security management system for personal computer networks," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 2, pp. 290–294, 1989.

[8] M. Baltatu, A. Lioy, F. Maino, and D. Mazzocchi, "Security issues in control, management and routing protocols," *Computer Networks*, vol. 34, no. 6, pp. 881–894, 2000.

[9] S. Muftic, "Implementation of the comprehensive integrated security system for computer networks," *Computer Networks and Isdn Systems*, vol. 25, no. 4-5, pp. 469–475, 1992.

[10] S. Demir, K. Yetilmezsoy, and N. Manav, "Development of a modified Hardy-cross algorithm for time-dependent simulations of water distribution networks," *Fresenius Environmental Bulletin*, vol. 17, no. 8A, pp. 1045–1053, 2008.

[11] L. Zhao and Y. Zi, "The network security management problem of library," *Advanced Materials Research*, vol. 760-762, pp. 1241–1243, 2013.

[12] A. B. Odunola, A. A. Olawumi, and O. E. Ajayi, "An adaptive decision-support model for data communication network security risk management," *International Journal of Computer Applications*, vol. 106, no. 8, pp. 1–7, 2014.

[13] O. N. Ozdemir and E. Ucaner, "Validation of genetic algorithms for the hydraulic calibration of a water supply network," *Fresenius Environmental Bulletin*, vol. 16, no. 3, pp. 278–284, 2007.

[14] S. Z. Wu, "Based on computer network security in financial informationization construction of colleges and universities," *Advanced Materials Research*, vol. 989-994, pp. 5415–5418, 2014.

[15] X. H. Yang and Y. F. Chen, "A study of vulnerability detection and prevention on computer network security," *Applied Mechanics and Materials*, vol. 321-324, pp. 2630–2634, 2013.

[16] X. Wei, Y. Guo, H. Cheng et al., "Rock mass characteristics in beishan, a preselected area for China's high-level radioactive waste disposal," *Acta Geologica Sinica*, vol. 93, no. 2, pp. 116–126, 2019.

[17] L. X. Shen, G. Cao, and S. Z. Cao, "A hybrid model for evaluation computer network security risk in commercial bank," *Advanced Materials Research*, vol. 393-395, pp. 531–534, 2011.

[18] C. Shan, "Misuse detection in large-scale network for network security management systems," *Computer Engineering and Applications*, vol. 42, no. 6, pp. 136–139, 2006.

[19] J. Dawkins, K. Clark, G. Manes, and M. Papa, "A framework for unified network security management: identifying and tracking security threats on converged networks," *Journal of Network and Systems Management*, vol. 13, no. 3, pp. 253–267, 2005.

[20] S. Basbas, P. Papaioannou, and A. Kokkalis, "The role of environment in traffic management studies: need for a new approach," *Fresenius Environmental Bulletin*, vol. 15, no. 8, pp. 963–974, 2006.

[21] E. Andriani, M. Brattoli, P. Buono, G. D. Gennaro, L. D. Gennaro, and A. Mazzone, "A GIS tool for atmospheric emission management in south of Italy," *Fresenius Environmental Bulletin.*, vol. 21, no. 11A, pp. 3325–3329, 2012.