Hindawi
Advances in Multimedia
Volume 2022, Article ID 9873290, 1 page
https://doi.org/10.1155/2022/9873290

Retraction

Retracted: Research on High Robust Multimedia Image Encryption Based on Gyrator Transform Domain Model

Advances in Multimedia

Received 5 November 2022; Accepted 5 November 2022; Published 23 November 2022

Advances in Multimedia has retracted the article titled "Research on High Robust Multimedia Image Encryption Based on Gyrator Transform Domain Model" [1] due to concerns that the peer review process has been compromised.

Following an investigation conducted by the Hindawi Research Integrity team [2], significant concerns were identified with the peer reviewers assigned to this article; the investigation has concluded that the peer review process was compromised. We therefore can no longer trust the peer review process, and the article is being retracted with the agreement of the editorial board.

References

[1] X. Cheng, "Research on High Robust Multimedia Image Encryption Based on Gyrator Transform Domain Model," *Advances in Multimedia*, vol. 2021, Article ID 2225114, 10 pages, 2021.

[2] L. Ferguson, "Advancing Research Integrity Collaboratively and with Vigour," 2022, https://www.hindawi.com/post/advancing-research-integrity-collaboratively-and-vigour/.

Hindawi
Advances in Multimedia
Volume 2021, Article ID 2225114, 10 pages
https://doi.org/10.1155/2021/2225114

Research Article

Research on High Robust Multimedia Image Encryption Based on Gyrator Transform Domain Model

Xiaojing Cheng

School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723000, China

Correspondence should be addressed to Xiaojing Cheng; 41804421@xs.ustb.edu.cn

Received 24 August 2021; Accepted 21 October 2021; Published 11 December 2021

Academic Editor: Zhendong Mu

The encryption and privacy protection of multimedia image resources are of great value in the information age. The utilization of the gyrator transform domain model in multimedia image encryption can select parameters more accurately, so it has a wider scope of utilization and further ameliorates the stability of the whole system. On account of this, this paper first analyzes the concept and connotation of gyrator transform, then studies the image encryption algorithm on account of gyrator transform, and verifies the robustness of the gyrator transform algorithm under the influence of noise interference, shear attack, and other factors through the high robust multimedia image encryption and result analysis of gyrator transform.

1. Introduction

With the iterative maturity and popularization of computer information technology, it has been widely and deeply applied in many fields and achieved remarkable results. However, the encryption and security of computer information have become the focus and difficulty of people's research and attention. On the one hand, many information resources represented by digital images are widely used in many fields. On the other hand, under the background of the deepening network threats and attacks faced by the Internet platform, the encryption and privacy protection of information multimedia image resources have become an unavoidable problem and the focus of attention and research by many scholars. Specific to the encryption level of multimedia images, if the encryption transmission and sharing of image information want to be more flexible and convenient, it is more and more inseparable from the support of data security protection technology.

In the process of multimedia image transmission, due to its own particularity, it is necessary to encrypt and protect the privacy information contained in it so as to avoid data tampering and interception. At present, the encryption methods of multimedia images mainly include linear canonical transform, Fourier transform, and wavelet transform. Among them, Fourier transform has expanded its utilization field with its extensive research and much visualization results and has strong utilization flexibility and utilization advantages. In contrast, linear canonical transformation has the typical advantages of flexibility and stronger processing power, but it has its own shortcomings in the amount of computation and parameter selection [1]. Therefore, the introduction of gyrator transform in the encryption process of multimedia image can better realize the organic integration of transformation efficiency and flexibility, so it has better applicability.

In addition, the utilization of gyrator transform in the field of multimedia image encryption can further ameliorate the parallelism and robustness of image processing, so it has gradually become the key direction of the research and utilization of the multimedia image encryption algorithm in the transform domain. The operation process of the multimedia image encryption algorithm integrating the gyrator transform domain model is shown in Figure 1, which fully releases the operation efficiency of the algorithm and the data conversion ability between spatial domains and transform domain. Generally speaking, multimedia image encryption under the transform domain model will lead to a significant increase in the amount of data operation and affect the calculation accuracy, resulting in the decline of

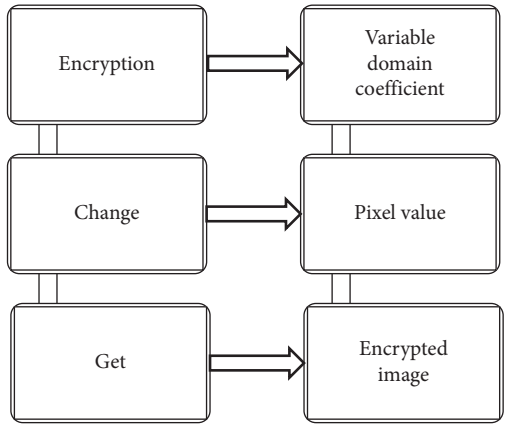


Figure 1: Architecture of the system for predicting and analyzing the quality of multimedia professional talent.

image accuracy. The multimedia image encryption of the gyrator transform domain model can select parameters more accurately, has a wider range of utilization, and further ameliorate the stability of the whole system.

In short, the encryption of multimedia images needs to pay attention to the encryption efficiency, transmission efficiency, and use cost of images on the premise of paying attention to the security of cipher-text. The multimedia image encryption algorithm integrating the gyrator transform domain model uses different transforms to process different matrices, which greatly optimizes the distribution and management of multimedia image key, and has great advantages in security and sensitivity. Therefore, it is of great practical value to study the robustness of the multimedia image encryption algorithm integrating the gyrator transform domain model.

2. The Concept and Connotation of Gyrator Transformation

2.1. The Concept of Gyrator Transformation. As an important measure to realize image data information conversion, Fourier transform has typical advantages of convenient beam transmission and pure fractional spectrum signal [2]. Similarly, as a linear regular integral transformation, the integral kernel matrix of gyrator transformation is a symmetrical structure, as shown in equation (1). Among them, α is the rotation angle, and $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ is the position spatial frequency plane. The characteristic matrix of gyrator linear transformation is shown in equation (2). In addition, the mathematical definition of gyrator transformation can be obtained by substituting the transfer matrix into equation (2), with $X = \begin{bmatrix} \cos\alpha & 0 \\ 0 & \cos\alpha \end{bmatrix}$ and $Y = \begin{bmatrix} 0 & \sin\alpha \\ \sin\alpha & 0 \end{bmatrix}$.

$$\begin{pmatrix} a_o \\ b_o \end{pmatrix} = \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} \begin{pmatrix} a_i \\ b_i \end{pmatrix} = T(\alpha) \begin{pmatrix} a_i \\ b_i \end{pmatrix}, \quad (1)$$

$$C_M = [f(v')](v) = \int C_M(v, v') f(v') \mathrm{d}v'. \quad (2)$$

2.2. Typical Multimedia Image Encryption Technologies. Typical image encryption technologies include pixel scrambling based on spatial domain, encryption algorithm based on transform domain, encryption algorithm based on turbidity, DNA coding technology, encryption based on neural network and cellular automata, and algorithms based on secret segmentation and secret sharing. Among them, the security technology of pixel scrambling based on spatial domain is poor, which often needs to be combined with other encryption technologies. In addition, the security evaluation criteria for these typical image encryption algorithms include key space analysis, statistical feature analysis, adjacent pixel correlation analysis, information entropy analysis, sensitivity analysis, integrity analysis, and anticlipping analysis.

2.3. Typical Properties of Gyrator Transformation. Multimedia image encryption on account of the gyrator transform domain model is mainly carried out with the help of the advantages and features of gyrator transform. The typical features of gyrator transform are not only limited to exponential additivity and reversibility but also have their own unique characteristics, as shown in Figure 2.

The linear expression of gyrator transformation is shown in equation (3), and b_1 and b_2 are complex constants. Exponential additivity and commutativity make gyrator transform more flexible. The typical properties of gyrator transform make its utilization in multimedia image encryption have significant advantages, such as convenient multilevel and channel image information encryption and decryption.

$$R^{\beta} = [b_1 f(s) + b_2 f(s)] = b_1 R^{\beta}\{f(s)\} + b_2 R^{\beta}\{f(s)\}. \quad (3)$$

2.4. Implementation of Gyrator Transform. In order to realize high robust multimedia image encryption, firstly, an efficient cascade system needs to be constructed at the optical level to realize wide-angle gyrator transform. The architecture of the efficient cascaded optical system is shown in Figure 3. Its main components include thin lens group and phase modulation system. In the system shown in Figure 3, the generalized lens T and the thin lens group on the right are covered, and the principle of phase modulation is shown in equation (4). Among them, λ is the wavelength of the light wave, f is the focal length, and is the position of the symmetry axis of the cylindrical thin lens relative to the Y axis.

In the phase modulation system shown in Figure 3, there are two identical lenses T1 in the Z axis, and their phase modulation functions are also the same. The angle of gyrator transformation is obtained by rotating the cylindrical thin lens constituting the generalized lens and plays a key and decisive role in the composition of the generalized lens in the experimental device. In addition, under a specific angle, the phase modulation system shown in Figure 3 can be considered as a typical special extension of the Fourier transform stacking system.

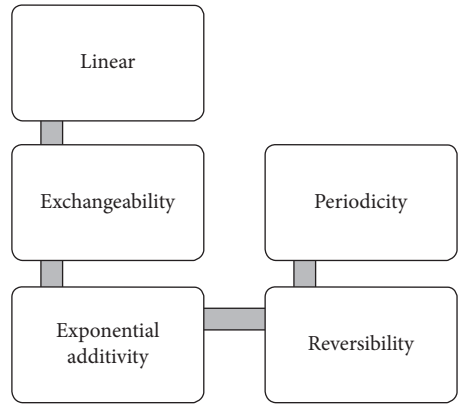


Figure 2: Typical properties of gyrator transformation.

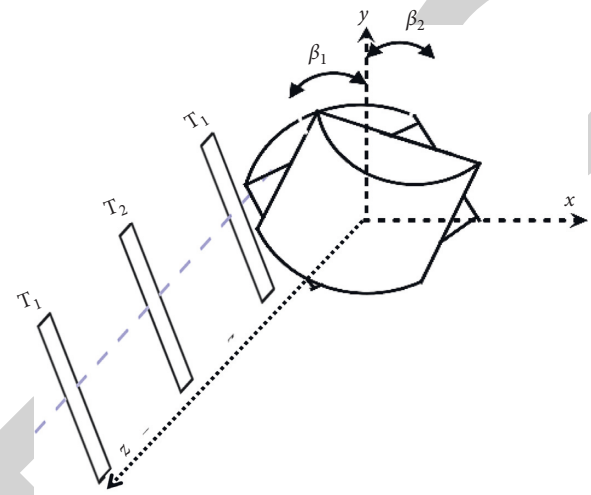


Figure 3: Cascade phase modulation system architecture.

$$f(x_o, y_o) = \exp\left(-i\pi \frac{{x_o}^2 + {y_o}^2 - 2x_o y_o \sin 2\beta}{\lambda f}\right) f_i(x_o, y_o). \tag{4}$$

Multimedia image encryption with high robustness also needs to be realized at the numerical level, and its principle is shown in equation (5). Among them, the situations in the formula need to be treated differently, and different simulation forms should be selected, respectively, such as FFT or IFFT. In the implementation of the fast discrete algorithm of gyrator transform, the modulation function needs to be input first, and then it is further transformed by FFT or IFFT to verify the additivity of the order of gyrator transform [3]. Optical transformation of the gyrator and the analysis and utilization of the fast numerical implementation algorithm are helpful to establish an effective premise for the utilization of this algorithm in highly robust multimedia images.

$$\begin{aligned} R^{\beta}\{g(x_i, y_i)\} &= \iint f_i(x_i, y_i) H_{\beta}(x_i, y_i, x_o, y_o) \mathrm{d}x_i \mathrm{d}y_i \\ &= \frac{1}{|\sin \beta|} \iint f_i(x_i, y_i) \exp\{i2\pi(x_i y_i + x_o y_o)\cot \beta\} \times \exp\{-i2\pi(x_i y_i + x_o y_o)\csc \beta\} \mathrm{d}x_i \mathrm{d}y_i \\ &= \frac{1}{|\sin \beta|} \exp\{i2\pi(x_o y_o)\cot \beta\} \iint A_{\beta}(x_i, y_i) \times \exp\left\{-i2\pi\left(x_i \frac{y_o}{\sin \beta} + y_i \frac{x_o}{\sin \beta}\right)\right\} \mathrm{d}x_i \mathrm{d}y_i. \end{aligned} \tag{5}$$

2.5. Image Encryption Algorithm on account of Gyrator Transform. Generally speaking, the encryption process of multimedia image is a hidden processing process of sensitive information [4]. Therefore, as long as the algorithm can realize the smooth conversion between the original image and the encrypted image, the image can be encrypted. With the continuous progress and amelioration of the computing power level of the computer system, its efficiency in the encryption processing of multimedia images is also improving accordingly. Gyrator transform has been widely studied and popularized in many fields because of its many utilization advantages [5]. Secondly, the transform domain algorithm has many similarities with FFT, so it has important utilization value in the field of high robust multimedia image encryption. Image encryption on account of gyrator transform pays more attention to the visibility, self-similarity, and correlation of image information in the process of encryption and decryption and ameliorates the encryption and decryption efficiency of the whole system. The advantages of gyrator transform in algorithm efficiency, accuracy, and security make its utilization in the field of multimedia image encryption have a good development prospect and can greatly ameliorate the robustness of multimedia image encryption.

2.6. Principle of Multimedia Image Encryption on account of Gyrator Transform. FFT has typical utilizations in the field of multicolor image encryption, and its efficiency is remarkable. Gyrator transform, as a changed form of FFT, further highlights the advantages of FFT transform and strengthens its adaptability and matching in the field of multimedia image encryption with the help of its unique characteristics; therefore, it has good utilization and development prospects and potential [6]. Secondly, the N-cascade encryption process of the image encryption change fused with gyrator transform is shown in equation (6), in which the κ -order gyrator transform of image $g(x, y)$ is $G(x_o, y_o)$. $F(x_o, y_o)$ and $H(x_o, y_o)$ are the amplitude and phase of the image encryption κ-order transform domain, respectively, and $S(x_o, y_o)$ and $X(x_o, y_o)$ are the real part and imaginary part of the κ-order transformation domain.

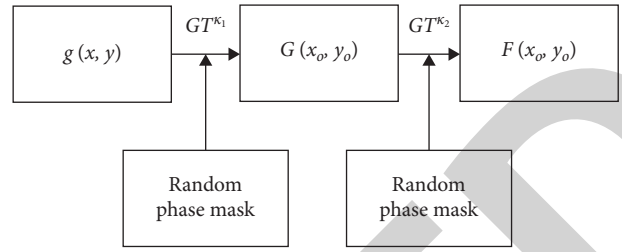


Figure 4: Gyrator transforms image encryption process.

$$f = \exp(-2\pi\alpha_1)R^{-\kappa_1}\left[\left[\exp(-2\pi\alpha_{N-1})\right]R^{-\kappa_{N-1}}\left[\exp(-i2\pi\alpha_N)R^{-\kappa_N}[F]\right]\right]. \tag{6}$$

The image encryption process of gyrator transform is shown in Figure 4. When encrypting the multimedia image, the transformation and operation are cascaded for many times so as to flexibly use the encryption parameters to ensure the security of the encrypted image to the greatest extent. The gyrator transform multimedia image algorithm is more suitable for practical utilization scenarios [7]. In addition, the fusion with double random phase coding technology is not conducive to practical utilization. Although this method increases the key multiplicity, it also leads to the complexity of its algorithm.

2.7. Single Image Encryption on account of Gyrator Transform. For a single image, the κ-order gyrator transform is shown in equation (7), where $Z(a, b)$ and $X(a, b)$ are the amplitude and phase of gyrator transform spectrum, respectively. Secondly, through the mathematical operation of single image encryption of gyrator transform, the difficulty of decryption process can be effectively reduced, so as to effectively deal with the adverse effects of cascading and interchangeability [8]. In addition, the real and imaginary parts of the gyrator transform spectrum are transposed or added or subtracted to obtain the encryption result of the image. In order to recover the information of the original image, the level inverse transformation is carried out, and further the inverse operation of the operator is carried out to obtain the κ-order gyrator transform spectrum of the image, and then the -κ order inverse transformation is carried out to obtain the image, so as to complete the image decryption process.

$$\begin{aligned} G(a,b) &= R^{\kappa}\{g(a,b)\} \\ &= \iint g(a,b)K_{\kappa}(x,y,a,b)\mathrm{d}x\mathrm{d}y \\ &= \frac{1}{|\sin\kappa|}\iint \exp\left[i2\pi\frac{(ab+xy)\cos\kappa-(ab+xy)}{\sin\kappa}\right]g(a,b)\mathrm{d}x\mathrm{d}y = Z(a,b)\exp[jX(a,b)]. \end{aligned} \tag{7}$$

Gyrator transform can be verified by optical path experiment. Secondly, in order to ameliorate the security of multimedia image encryption, it can be further realized by increasing the number of keys. With the help of computer simulation software, the effectiveness of the gyrator transformation algorithm can be verified. Gyrator transformation is performed on the specific image shown in Figure 5(a). After obtaining its map distribution, the matrix transpose and imaginary part matrix in the distribution are added, and then the calculated results are recombined to obtain a new matrix complex matrix [9]. In addition, by performing gyrator transformation on the complex matrix, the new image is shown in Figure 5(b). It can be seen that the image after gyrator transformation has completely become a noise image and completely implies sensitive and real information, it can well realize the encryption of multimedia images.

As can be seen from Figure 5, the gyrator transformed image of the original image can not only obtain its image spectral distribution but also obtain the original image through inverse operation. Through the inverse operation of gyrator transform encryption program, the original image can be recovered, the original image can be decrypted, and its complete real information can be retained [10]. The distribution shown in Figures 6(a) and 6(b) is the result of the failed inverse transformation, which is the result of the gyrator transformation, the primary and secondary transformation errors, and the correct t operation.

It can be seen from the inverse transformation results of Figure 6 that Figure 6(b) can better the original encrypted information, which shows that the secondary gyrator transformation is very necessary. Therefore, adding double random phase coding to the multimedia algorithm integrating gyrator transformation can better realize the image encryption effect. In addition, it can be seen from the effect of change and encryption that gyrator transform is similar to FFT transform and has the typical characteristics of cascade and exchange, but its decryption process is relatively simple, and the complexity needs to be further ameliorated to ensure the security of the decryption process.

In addition, in order to verify the anti-interference ability of the encrypted image fused with gyrator transform, certain white noise interference needs to be verified. As shown in Figure 7(a), interfere with the decryption process, apply 15 dB, 10 dB, and 5 dB Gaussian noise, respectively, and ensure the correctness of the decryption process key. The decrypted image results are shown in Figures 7(b)–7(d). As can be seen from Figure 7, after the original encrypted image is disturbed by noise, the decrypted image will lose some real information, resulting in the impact on the detail restoration of the image, but the basic content of the original image can still be obtained and judged [11]. This shows that the algorithm integrating gyrator transform can resist the interference of dead noise to a certain extent, but with the increase in noise intensity, the image quality and content details obtained by decryption will decrease significantly, resulting in further annihilation of real information.

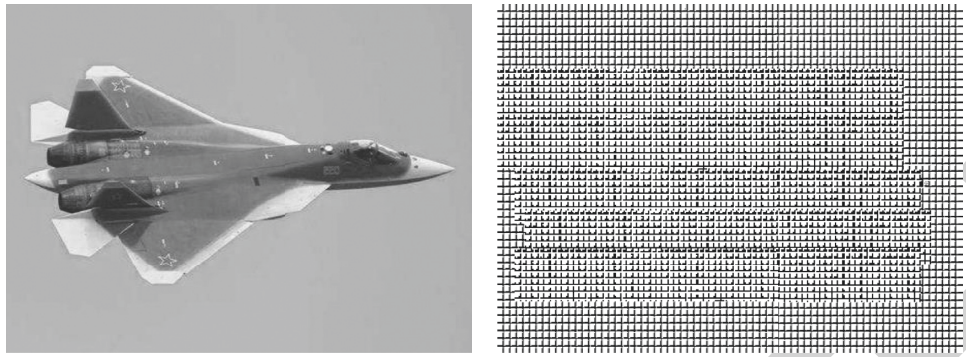
2.8. Multi-Image Encryption on account of Gyrator Transform. FFT can effectively concentrate the spectrum. After the gyrator transformed image is rotated by a specific rotation angle usually π 2, the image information will be further concentrated in the low-frequency spectrum region [12]. When the rotation angle is further reduced, after gyrator transformation, the original image content with more readable details needs to be restored with the help of the central spectrum. Figure 8 shows the recovery effect of the gyrator transform spectrum after different rotation angles. As can be seen from the figure, there is basically no interference between images in the process of multi-image encryption and decryption, which is also the advantage of this algorithm.

Similarly, the numerical simulation and optical implementation of multimedia image encryption need to be realized with the help of computer simulation software so as to further analyze the practicability of the image encryption algorithm. Generally speaking, the size of the central spectral area is negatively correlated with the number of original images but positively correlated with the spectrum information [13]. Therefore, a certain central spectral area is required to ensure the authenticity of the decrypted multimedia image and the details of the information. In addition, the concentration of spectral energy of gyrator transform is positively correlated with the rotation angle, while the central spectral size required for decryption is negatively correlated with the rotation angle. This shows that there is an upper limit on the number of encrypted images that can be realized by the multi-image encryption algorithm, and the upper limit value will vary with the difference of rotation angle.

2.9. Verification of the Encryption Effect and Security Principle in the Decryption Process. After obtaining the different information components of the decrypted multimedia image, the original multimedia image can be restored by combining the three decrypted component information. So far, the decryption process is completed. Different chaotic initial values, different transform iteration times, and different gyrator transform rotation angles are used for encryption and decryption. They will be used as the key information of the encryption system. The experiments show that the gyrator transform encryption algorithm in this paper has good encryption effect and security.

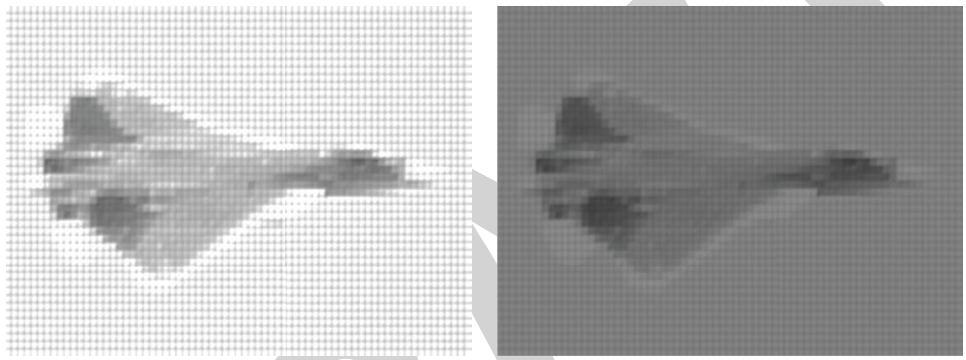
3. Multimedia Image Encryption and Result Analysis

3.1. High Robustness Multimedia Image Encryption on account of Gyrator Transform. The multimedia images to be encrypted are combined, and the combined multimedia image matrix is phase coded. By combining the virtual and real parts of the combined image, the numerical decomposition of the real matrix is realized. Secondly, the multimedia cipher-text image is obtained by singular value decomposition [14]. With the help of the key, the plaintext image can be obtained by inverse transformation, which is



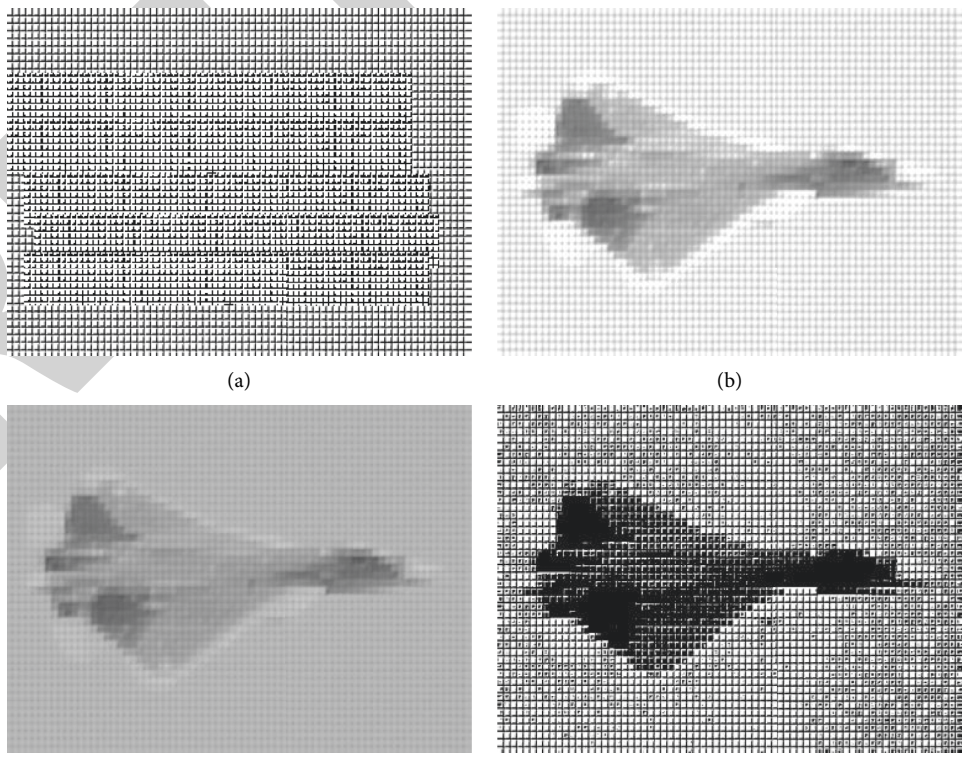
(a) (b)

Figure 5: Gyrator transformation result of specific image.



(a) (b)

Figure 6: Result of decrypting image with wrong password.



(a) (b)

(c) (d)

Figure 7: Encrypted image and corresponding decryption changes in noise interference environment.

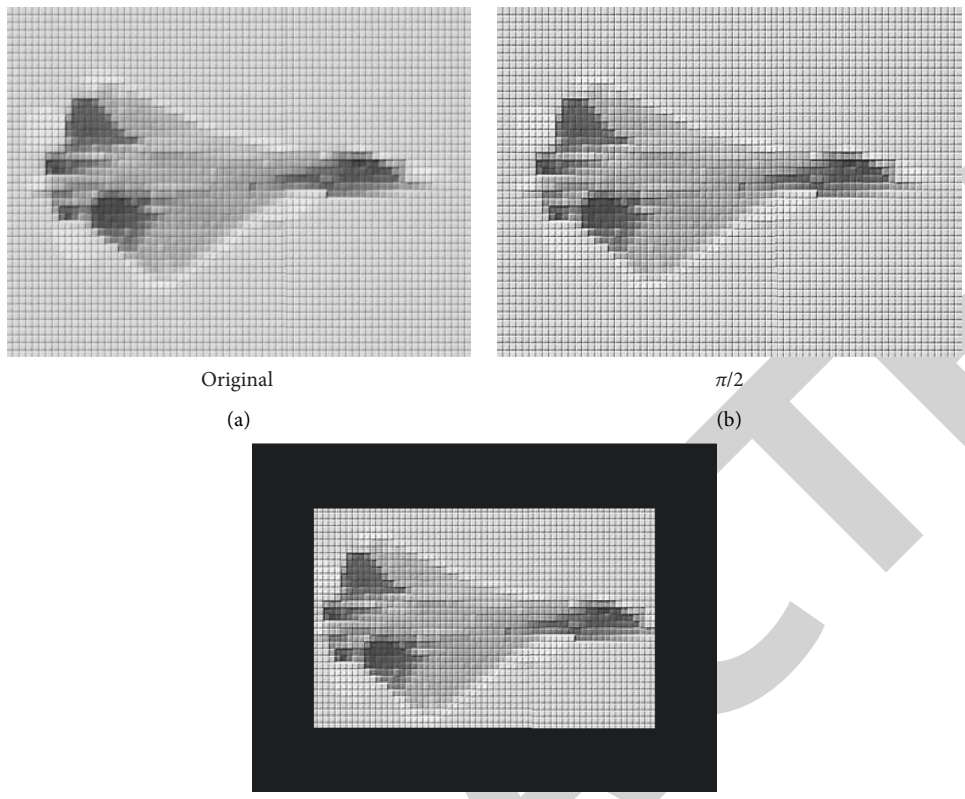


Figure 8: Gyrator transformation effect under different rotation angles.

realized by recombining the singular value decomposition through the orthogonal matrix. For the original multimedia image that needs to be encrypted, it is first necessary to combine the images, establish the corresponding virtual part image set and real part image set, and then calculate the real value of the image set. The process is shown in the following equations:

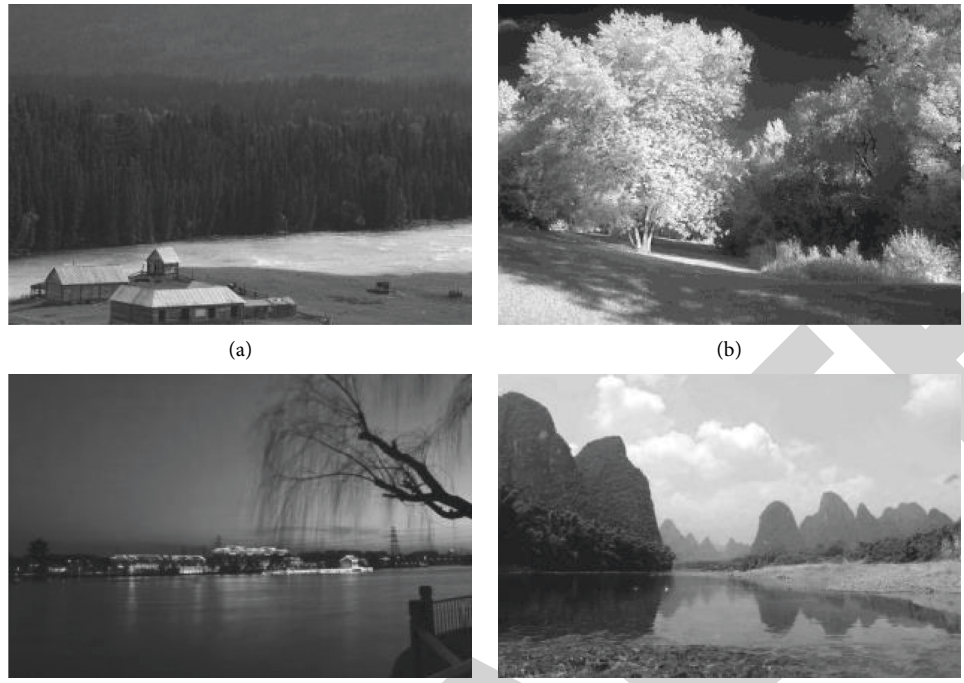
$$A_0 = \frac{2/n}{\sum_{g\in S}\sum_{i=0}^{N} g(i)\cdot Z(i)}, \tag{8}$$

$$A_1 = \frac{2/n}{\sum_{g\in S'}\sum_{i=0}^{N} g(i)\cdot Z(i)}. \tag{9}$$

Among them, $g(x, y)$ is the original multimedia image. For n original images to be encrypted, they are combined to establish a complex matrix. Secondly, the real part and imaginary part image sets s and s' are established, respectively, and the ameliorated mapping initial values are obtained by calculating the real values A_0 and A_1. Z is the distribution of gray histogram of original multimedia image. Through the iterative calculation of the above formula, the chaotic phase mask is obtained [15]. Further, the complex matrix is transformed by gyrator to obtain the matrix, and the real part and imaginary part components in the transformation matrix are extracted and recombined to construct the real matrix. By extracting the real and imaginary components of the transformed matrix, respectively, and further combining them, the combined real matrix is obtained. In addition, the orthogonal matrix is obtained by multiresolution singular value decomposition of the combined real matrix, and the orthogonal matrix is combined to obtain the Gaussian matrix parameter key.

3.2. Decryption Process with the Help of Key Inverse Process. Firstly, the cipher-text is solved by means of Clem's law, and the results of multiresolution singular value decomposition are obtained. Secondly, the complex matrix is obtained by inverse process operation of the multiresolution singular value decomposition results. Then, the complex matrix is transformed by gyrator, and the transformation angle is the complex of the encryption process, so as to obtain the complex matrix. Finally, the imaginary and real parts of the complex matrix obtained by the inverse transformation are extracted, respectively, and then the original multimedia image is obtained.

3.3. Experimental Results and Analysis. Firstly, the computer simulation platform and simulation software are used to randomly extract the multimedia plaintext image to be encrypted in the database, and the size of the image is optimized and adjusted. The simulation software selected in



(a) (b) (c) (d)

Figure 9: Selected test image.

this paper is Matlab2018Rb, the hardware is a quad core Intel (R) i7-5100U processor, the memory is 16g, and the operating system is Windows 10. At the selection level of test image, select the image shown in Figure 9 and set the mapping control parameters, and the square difference and mean value of random Gaussian matrix are 4.96, 1 and 0.5.

3.4. Multimedia Image Encryption and Decryption Results. In order to ensure the scientificity and objectivity of multimedia image encryption and decryption results, PSNR, CC, and SSIM are used as evaluation parameters. The original multimedia image and the decrypted image are represented by $G(x, y)$ and $G'(x, y)$, respectively, and the calculation process of evaluation indexes PSNR, CC, and SSIM is shown in the following equations:

$$\mathrm{PSNR} = \log\left(\frac{N^2}{1/\mathrm{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(g(x,y) - g'(x,y)\right)^2}\right), \tag{10}$$

$$\mathrm{SSIM} = \frac{\left(2\mu_g\mu_{g'} + c_1\right)\left(2\sigma_{gg'} + c_2\right)}{\left(\mu_g^2 + \mu_{g'}^2 + c_1\right)\left(\mu_g^2 + \mu_{g'}^2 + c_2\right)}, \tag{11}$$

$$\mathrm{CC} = \frac{E\left(\left[g - E(g)\right]\left[g' - E(g')\right]\right)}{\sqrt{E\left(\left[g - E(g)\right]^2\right)}\sqrt{E\left(\left[g' - E(g')\right]^2\right)}}, \tag{12}$$

in which μ_g and $\mu_{g'}$ are the mean of the original multimedia images $g(x, y)$ and $g'(x, y)$, σ_g and $\sigma_{g'}$ are the standard deviation of the original multimedia images $g(x, y)$ and $g'(x, y)$, respectively, $\sigma_{gg'}$ is the covariance of the original image, c_1 and c_2 are constants, and E is the expected value operation. According to the definition of the formula, it can be seen that the PSNR value is positively correlated with the quality of the decrypted image.

Table 1: Statistical results of PSNR under different parameter values.

$p \times q$	Min value	Max value	Mean value
2×2	292.7261	287.4872	290.3564
2×3	291.1632	287.5681	289.6482
3×3	290.8744	287.6319	288.4521
2×4	289.9656	287.5143	287.9633
4×2	288.8543	287.1253	286.7426
4×4	287.1652	287.2943	285.9518

With the help of computer simulation, the effect of singular value decomposition factor on the decryption image effect is studied, and the selected images are experimentally analyzed. The displayed results are shown in Table 1. It is not difficult to see from the results in Table 1 that the decryption effect of the original multimedia image is the best when the value of the parameter (p, q) equals (2, 2). In addition, at the level of antistatistical attack performance, there are significant differences in the histogram peaks of different original multimedia images. The encrypted image is similar to Gaussian white noise by fusing gyrator changes, which effectively masks the details of the original image.

3.5. Robustness Analysis of Multimedia Image Encryption. Some noise pollution is inevitable in the process of multimedia image encryption data transmission, and the quality of multimedia decrypted image is negatively correlated with

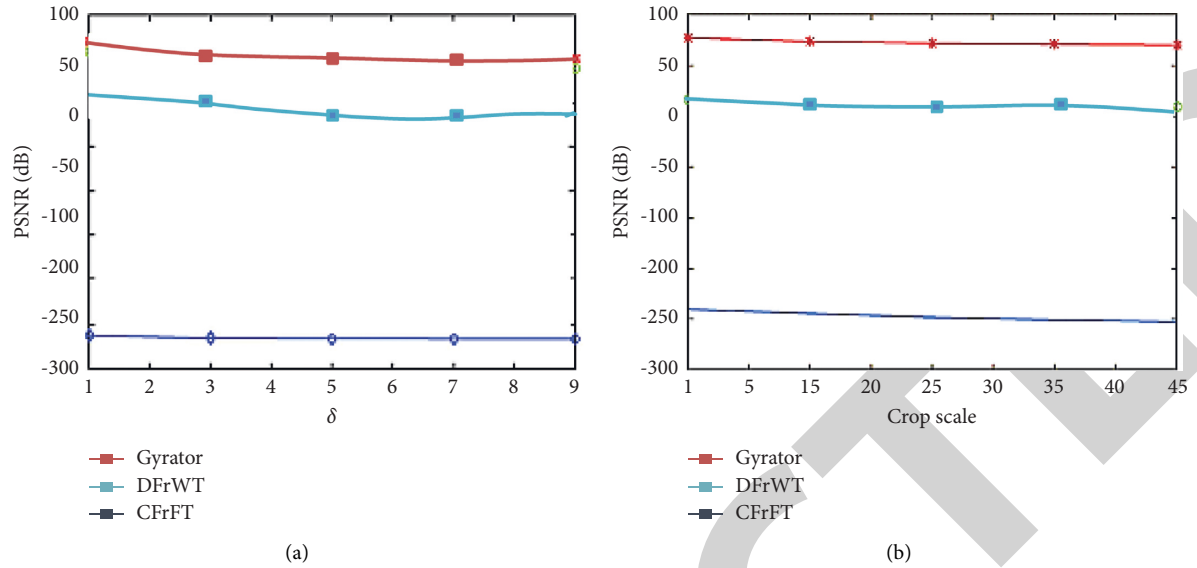


Figure 10: Selected test image.

the noise intensity. The algorithm used in this paper can better regional noise attack, which shows that the robustness of the algorithm is better, as shown in Figure 10(a). In addition, the multimedia image encryption algorithm fused with the gyrator transform domain model is less vulnerable to shear attack, and the data content of the original multimedia image is less vulnerable to cipher-text loss, as shown in Figure 10(b). These experimental results show that the multimedia image encryption algorithm on account of the gyrator transform domain model has strong robustness.

4. Conclusions

The flexible and convenient encryption transmission and sharing of multimedia image information are more and more inseparable from the support of data security protection technology. In the process of multimedia image encryption, the introduction of gyrator transform can better realize the organic integration of transformation efficiency and flexibility, so it has better applicability. By studying the concept and connotation of gyrator transform, this paper analyzes the properties and implementation of gyrator transform. By analyzing the image encryption algorithm on account of gyrator transform, the image encryption algorithm integrating gyrator transform is studied. Finally, the robustness of the gyrator transform domain model in the multimedia image encryption algorithm is verified by analyzing the high robustness multimedia image encryption and results of gyrator transform.

Data Availability

The data used to support the findings of this study are available upon request to the author.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This research study was sponsored by these projects: project one: University Level Project of Shaanxi University of Technology, the name of the project is Quasiperiodic Solutions of a Class of Second-Order Differential Equations, and the project number is SLGKY16-08; project two: Foundation of Shaanxi Educational of Committee, the name of the project is Research on the Structure and Shape Analysis of Some Curves and Surfaces in Geometric Design, and the project number is 11JK0514. The author would like to thank these projects for supporting this article.

References

[1] O. S. Faragallah and A. Afifi, "Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding," *Optical and Quantum Electronics*, vol. 49, no. 3, pp. 1003–1012, 2017.

[2] G. L. Giuliano and P. J. Miranda, "Lyapunov exponent for Lipschitz maps," *Nonlinear Dynamics*, vol. 92, no. 3, pp. 1217–1224, 2018.

[3] R. A. Muhammad, "An asymmetric single-channel color image encryption on account of hartley transform and gyrator transforms," *Optics & Lasers in Engineering*, vol. 69, no. 8, pp. 49–57, 2016.

[4] C. C. Lee, A. Mandangana, D. Muhamad Azlan, and H. Che Haziqah Che, "On the efficiency of the image encryption and decryption by using logistic - sine chaotic system and logistic-tent chaotic-system," *AIP Conference Proceedings*, vol. 18, no. 1, pp. 1–7, 2017.

[5] Y. Tan, P. Tang, and J. Xia, "Research on panoramic image enhancement algorithm on account of adaptive guided filtering," *Journal of Jinggangshan University (Natural Science Edition)*, vol. 39, no. 4, pp. 34–42, 2018.

[6] M. Isha, K. R. Sudheesh, and K. Naveen, "Cryptanalysis of an image encryption scheme on account of joint transform correlator with amplitude - and phase-truncation approach," *Optics and Lasers in Engineering*, vol. 52, no. 9, pp. 167–173, 2014.

[7] X. H. Wang and Y. Q. Sun, "Region of interest watermarking algorithm on account of QR code and schur decomposition," *Photoelectron Laser*, vol. 28, no. 4, pp. 419–425, 2017.
[8] H. Singh, A. K. Yadav, and S. Vashisth, "Optical image encryption using Devil's vortex toroidal lens in the fresnel transform domain," *International Journal of Optics*, vol. 129, no. 10, pp. 101–109, 2015.
[9] L. Chen, B. He, X. Chen, X. Gao, and J. Liu, "Optical image encryption on account of multi-beam interference and common vector decomposition," *Optics Communications*, vol. 361, no. 15, pp. 6–12, 2016.
[10] Z. H. W. Tu and C. Jin, "Applicable to pixel exclusive or image block encryption algorithm for android phones," *Electronic Measurement Technology*, vol. 38, no. 10, pp. 46–52, 2015.
[11] S. E. Azoug and S. Bouguezel, "A non-linear preprocessing for optodigital image encryption using multiple-parameter discrete fractional Fourier transforms," *Optics Communications*, vol. 359, pp. 85–94, 2016.
[12] C Zhang, J. Li, and S. Wang, "Encrypted medical image retrieval algorithm on account of discrete wavelet transform and perceptual hash," *Journal of Computer Utilizations*, vol. 38, no. 2, pp. 539–544, 2018.
[13] J. F. Hou, S. J. Huang, and G. H. Situ, "Nonlinear optical image encryption," *Editorial Office of Optics*, vol. 35, no. 8, pp. 85–90, 2015.
[14] Y. B. Tang, N. Xu, and C. H. Yao, "Image denoising on account of rotational invariant sparse representation and manifold learning," *Instrumentation*, vol. 35, no. 5, pp. 1101–1108, 2014.
[15] Y. L. Cheng, *Design and Implementation of Medicalimage Encryption Algorithm on Account of Memristor Hyperchaossystem*, pp. 28–46, Henan University, Kaifeng, China, 2016.