PROGRESS IN ELECTRICAL ENGINEERING
Vol. 1, No. 2, 2020, 217-230

URL : www.arfjournals.com

Research of Digital Image Encryption Based on Generalized Alternated Julia Set

Pei Wang[1]

[1]Department of Electrical Engineering and Automation, Qilu University of Technology (Shandong Academy of Sciences), Jinan, China
E-mail: wppink@126.com

Received: 12 October 2020 / Revised: 20 October 2020 / Accepted: 25 November 2020 / Published: 28 December 2020

Abstract: Compared with the classical fractal set, the Julia set of the generalized alternating system has stronger sensitivity to initial conditions. In this paper, a digital image encryption scheme based on generalized alternated Julia set is proposed. This encryption algorithm utilizes generalized alternated Julia set to generate the random key, and the key space of this scheme large enough. Since the generalized alternated Julia set can be generated with only six parameters, it can reduce the storage space greatly. At the same time, the generalized alternated Julia set has good sensitivity to initial conditions, which can improve the security of encryption as the initial key. In order to verify the security of this encryption scheme, some relevant performance indicators of this encryption scheme are analyzed, which show that all performance indicators meet the image encryption security performance test standards.

Index Terms: Digital Image Encryption, Fractal, Generalized Alternated Julia Set, Safety Performance Analysis

I. INTRODUCTION

With the popularization of communication devices such as computers and mobile phones, information exchange between people is becoming more and more frequent, therefore, the network has become an important medium for information exchange. In the transmission of information, information is mainly transmitted using image text as a carrier. Multimedia, because its style of passing information is richer and easier to understand, has been widely used. In other words, to protect the security of information in transmission, that is, to protect its content, to avoid being stolen or tampered by attackers. Therefore, the security of information in the process of network transmission has become a hot-spot for many scholars in recent years.

This work was supported by the Natural Science Foundation of Shandong Province under Grant No. ZR2018QF004.

Digital image encryption [1] is a direct and effective technical means to protect information security. The design of encryption algorithm and the selection of secret key are the foundation of information security. However, in the encryption algorithm, the randomness of secret key is the basis of the encryption system. Irregularity is one of the important features of fractal sets. Moreover, the fractal set has a strong sensitivity to the initial value. Any slight change of the initial value will make the whole set very different. Any slight change in the initial value will make the whole set have a big difference. Applying fractal sets to encryption algorithm, which will increase the randomness of the secret key, thereby improving the ability of the encryption system to resist attacks. Therefore, fractal has an important role in the encryption system [2-9].

The Julia set [10-12], which is one of the classic collections in the field of fractals, is obtained through iteration of complex mapping $\mathbf{z}_{n+1} \leftarrow \mathbf{z}^2{}_n$.

Y. Sun [13] generated a random secret key using the boundary of Julia set image, and proposed an encryption scheme combined with Hilbert curve and dictionary compression. N.B. Slimane [14] designed a new multi- scroll chaotic system using the fractal process of the Julia set and Logistic map, and verified the effect of this system in image encryption. W.J. Gao [15] proposed an image encryption scheme based on generalized Mandelbrot-Julia, and verified that the secret space of the scheme is not only large, but also dynamically changeable.

Alternated Julia set [16] is obtained by the iteration $z_{n+1} = z_n^2 + c_i (i = 1,2)$. The focus of the research is more on the control and synchronous control of the Julia set in alternated systems [17]. So far, no one applies alternated Julia sets to the encryption of information.

In this paper, an encryption scheme based on Julia sets in generalized alternated systems is proposed. As an initial key, generalized alternated Julia set has better initial value sensitivity than traditional Julia set, which can be reflected in its Lyapunov exponent. In addition, in order to further improve the security of encryption, the Hilbert function is used to scramble the generalized alternated Julia set. Moreover, exclusive-OR operation multi-cyclic encryption is utilized in the encryption process to improve the security of the cipher-text and the ability to resist attacks.

II. GENERALIZED ALTERNATED JULIA SETS

In order to discuss the digital image encryption based on alternated Julia sets, the following alternated system is taken,

$$z_{n+1} = \begin{cases} az_n^p + c_1, n \text{ is even} \\ az_n^p + c_2, n \text{ is odd} \end{cases}, \quad (1)$$

where $c_1 \neq c_2$, $c_1, c_2 \in \mathbb{C}$, $a, p \in \mathbb{R}$ and $n \in \mathbb{N}$.

Fig. 1 shows some fractal graphs of the alternated Julia sets with different c_1 and c_2 when $a = 1$, $p = 2$.

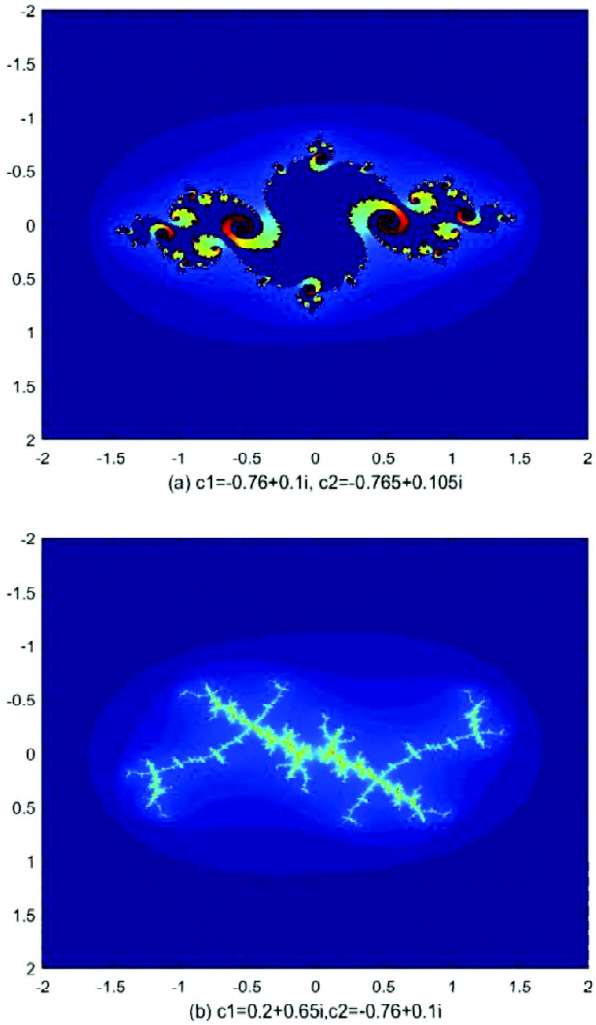

Figure 1: The alternated Julia set of System (1) with different c_1 and c_2.

The alternated Julia set has the characteristics of the classical fractal set, and it has a more complicated form of expression, and more variables can be used for the design of the secret key.

In this paper, the alternated Julia set and diffusion algorithm are combined to encrypt digital image information, which make the encryption scheme resistant to key attacks effectively. In addition, this encryption scheme applies modular arithmetic to the digital image information directly, which is simple and effective.

III. ENCRYPTION SCHEME BASED ON GENERALIZED ALTERNATED JULIA SET

A. Design secret key based on generalized alternated Julia set

As a fractal set, the boundary of alternated Julia set has infinite self-similarity and fine nested topology. Therefore, we select a part of the Julia set image on the boundary and zoom in, to construct the secret key and then perform key conversion. In order to ensure the effect of this encryption scheme, the complex region on the boundary of the alternated Julia set is selected, and then converted to a new complex plane area after zooming in, and remap it to the digital image finally.

Firstly, we use the Hilbert curve to scramble the alternated Julia set image, and use it as a secret key to encrypt the image to be encrypted. Then, we get encrypted image through the simplest two rounds of XOR algorithm. The secret key based on the alternated Julia set consists of nine keys, comprising the range region on a complex plane X_{max}, X_{min}, Y_{max}, Y_{min} and X_{min} are the maximum and minimum values on the real axis X, Y_{max} and Y_{min} are the maximum and minimum values on the imaginary axis Y), and the parameters a, p, x_1, y_1, x_2, y_2, which can determine the nature of the alternated Julia set.

B. Process of encryption algorithm

The process of this encryption scheme is divided into the following steps.

Input: The original image P with size of $n \times n$, and selected generalized alternated Julia set J with suitable size $n \times n$;

Output: The ciphered image C with the same size.

Step 1: Use the Hilbert curve to scramble the selected part of alternated Julia set J, then get the initial key;

$$H_x = x - \left|\frac{x-1}{\gamma+1}\right| \times (\gamma+1) + (k-1)(\gamma+1),$$

$$H_y = y - \left|\frac{y-1}{\gamma+1}\right| \times (\gamma+1) + (l-1)(\gamma+1),$$

where ($\boldsymbol{x}$, $\boldsymbol{y}$) is the coordinate of the current pixel, $\boldsymbol{x}$, $\boldsymbol{y} \in$ (l, n), k and l are the intermediate variables used for conversion, ($\boldsymbol{H}_x$, $\boldsymbol{H}_y$) is the transformed coordinate, γ represents the number of intervals between two pixels, and its range is (0, $\boldsymbol{n}$ – 2). Then the Julia set after scrambling is $\boldsymbol{J'}_{xy}$.

Step 2: Two random sequences $\boldsymbol{Rs}_i$ and $\boldsymbol{Is}_j$ can be obtained using Equations (2) and (3).

$$Rs_i = \boldsymbol{floor}(\boldsymbol{RJ'}_i \times 10^{14}) \bmod 256, \tag{2}$$

$$\mathbf{Is}_j = \mathbf{floor}\ (\mathbf{IJ'}_i \times 10^{14}) \bmod 256,$$

where $\boldsymbol{RJ}_i$ and $\boldsymbol{IJ}_i$ represent the real and imaginary parts of the graph $\boldsymbol{J}_{xy}$ respectively, and $\mathbf{i}$, $\mathbf{j} \in$ (1, $\mathbf{n} \times \mathbf{n}$).

Step 3: Use the real sequence $\boldsymbol{Rs}_i$ to encrypt the image $\boldsymbol{P}$ using XOR operation for the first time, then we obtain a temporary cipher-text, use the imaginary sequence $\boldsymbol{Is}_i$ to encrypt the temporary cipher-text to get the cipher-text $\boldsymbol{C}$. The encryption method can be expressed as Equations (4) and (5),

$$\boldsymbol{C}_i = (\boldsymbol{P}_i + \boldsymbol{C}_{i-1}) \bmod 256 \oplus \boldsymbol{Rs}_i, \tag{4}$$

$$\boldsymbol{C}_j = (\boldsymbol{P}_j + \boldsymbol{C}_{j-1}) \bmod 256 \oplus \boldsymbol{Is}_j, \tag{5}$$

Step 4: Get the final cipher-text image $\boldsymbol{C}$.

The process of this encryption scheme is shown in Fig. 2.

C. Process of decryption algorithm

When decrypting, since the algorithm is a symmetric encryption algorithm, the decryption process of the cipher-text is the inverse process of this encryption algorithm.

Input: Cipher-text $\boldsymbol{C}$ and the decryption key.

Output: The original image $\boldsymbol{P}$.

Step 1: Because it is a symmetric encryption algorithm, the same real sequence $\boldsymbol{Rs}$ and imaginary sequence $\boldsymbol{Is}$ can be obtained according to the key.

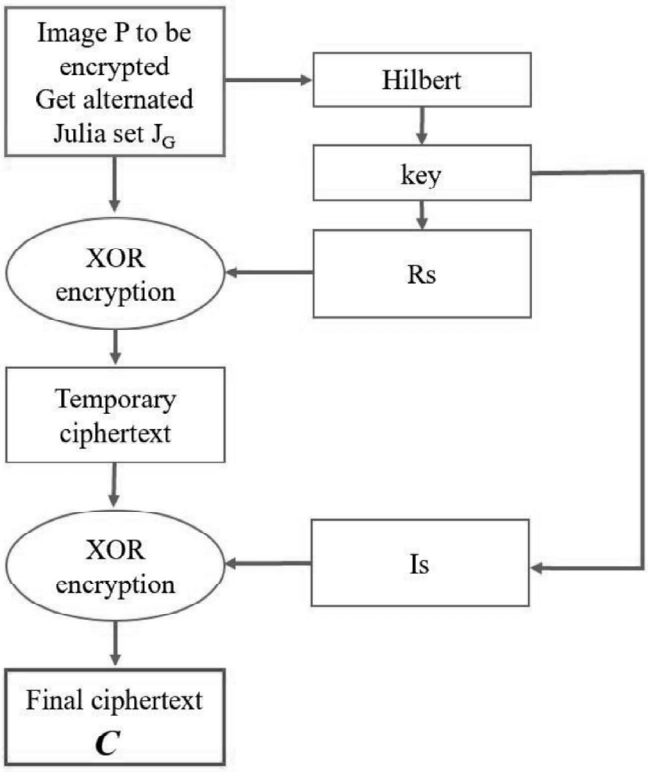

Figure 2: The process of this encryption algorithm

Step 2: Using **Is** to decrypt the cipher-text $\boldsymbol{C}$, that is

$$\boldsymbol{P}_j = (\boldsymbol{C} \oplus \boldsymbol{Is}_j - C_{j-1}) \bmod 256. \tag{6}$$

Step 3: Using $\boldsymbol{Rs}$ to decrypt the temporary cipher-text

$$\boldsymbol{P}_i = (\boldsymbol{C}_i \oplus \boldsymbol{Rs}_i - \boldsymbol{C}_{i-1}) \bmod 256. \tag{7}$$

The detailed process of decryption is shown in Fig. 3.

IV. SIMULATIONS

$\boldsymbol{a} = 1$, $\boldsymbol{p} = 12$, $\boldsymbol{c}_1 = 0.5 - 0.7\boldsymbol{i}$, $\boldsymbol{c}_2 = 0.5005 - 0.7005\boldsymbol{i}$ are taken in System (1) to generate the generalized alternated Julia set. In Fig.4, the generalized alternated Julia set is shown. Select an area and enlarge the image after 10000 times with size 512 × 512, as shown in Fig. 5.

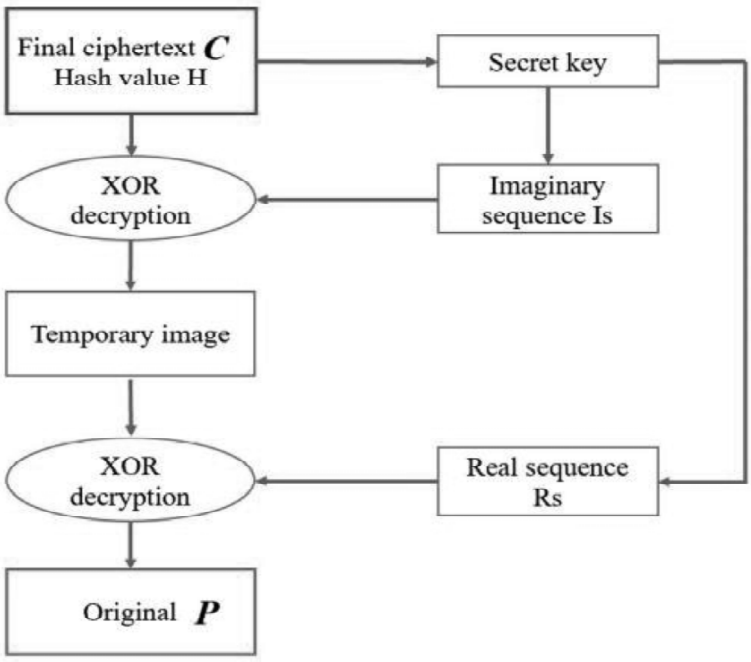

Figure 3: The process of this decryption algorithm

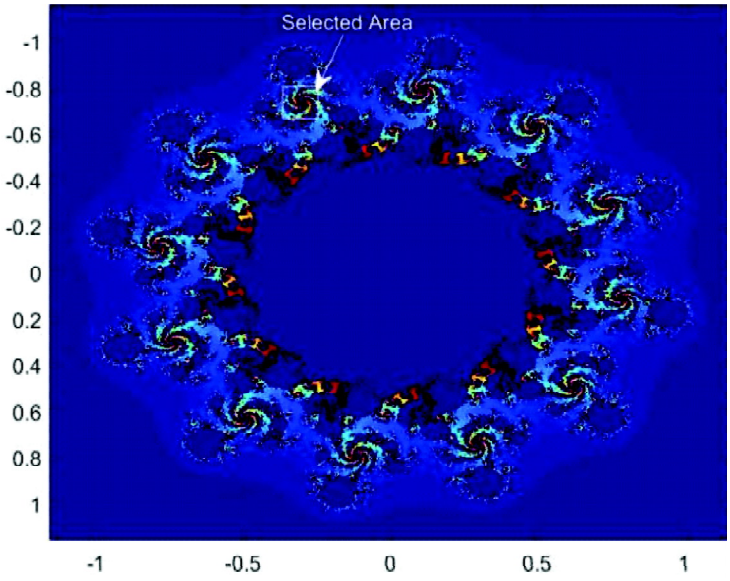

Figure 4: The alternated Julia set of System (1) with given parameters

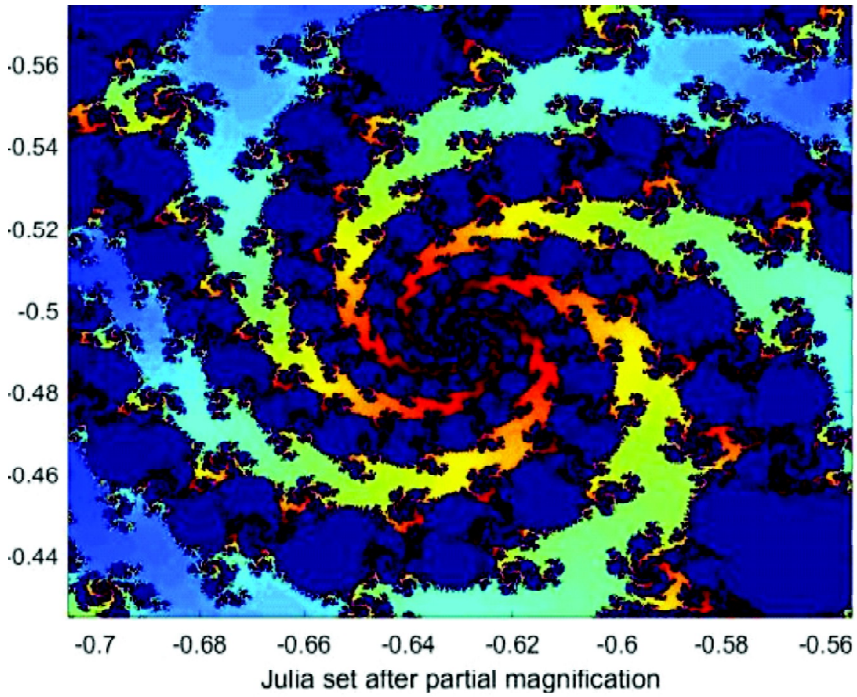

Figure 5: The selected area of alternated Julia set after enlargement

The standard sample images with 512 × 512 is taken to testify the effect of this encryption scheme. The original image, encrypted image and the decrypted image are shown in Fig. 6. In order to verify the effect of this encryption scheme, we encrypt a solid color image, the encryption effect is shown in Fig. 7.

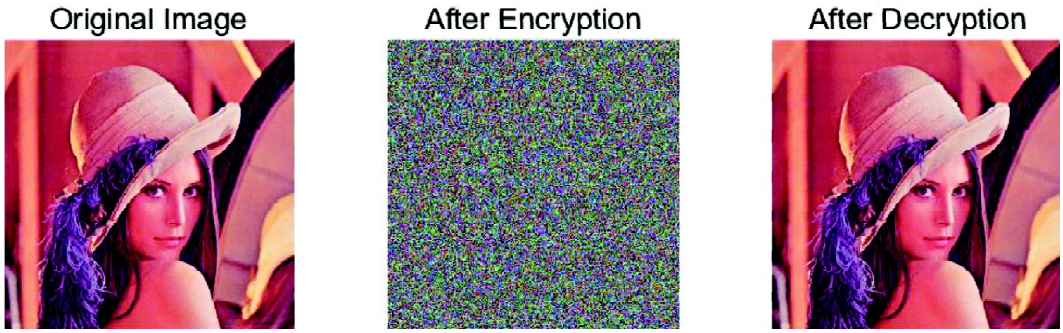

Figure 6: The effect diagram of encryption and decryption for Lena

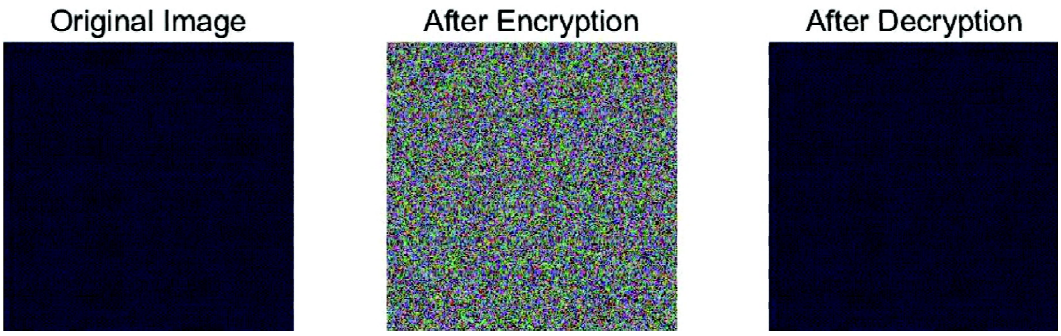

Figure 7: The effect diagram of encryption and decryption for solid color image

V. ANALYSIS OF ENCRYPTION ALGORITHM

In order to test the security of this encryption scheme, we analyzed the effect of this encryption algorithm from multiple aspects, such as key space, key sensitivity, histogram and adjacent pixel correlation.

A. Key space

In this encryption scheme, the key space consists of the alternated Julia set keys and diffusion keys. The key space is the product of alternated Julia set's key and diffuse key. The alternated Julia set key consists of X_{max}, X_{min}, Y_{max}, Y_{min}, a, p, x_1, y_1, x_2, y_2. The diffusion key is (H_x, H_y). Then the key space is

$$S_k = S(X_{max}, X_{min}, Y_{max}, Y_{min}, a, p, x_1, y_1, x_2, y_2) \times S\,(RH_x, IH_y).$$

Since all X_{max}, X_{min}, Y_{max}, Y_{min}, a, p, x_1, y_1, x_2, y_2 are double type, the double type in computer memory is 8 bytes, so each key space is 8 bytes, so each key space is 2^{64}. The diffusion key (H_x, H_y) is double type, so each key space is 2^{64}. The key space of the encryption algorithm is

$$S_k = (2^{64})^{10} \times (2^{64})^2 = 2^{768}.$$

It can be seen that the key space can fully meet the current requirements for key space ($\geq 2^{256}$).

B. Key Sensitivity

A secure encryption scheme should be extremely sensitive to the secret keys. Key sensitivity means that when use two keys with very small difference to encrypt the same original image, two very different cipher text images will be obtained.

Fig. 8 shows the Lyapunov exponent with $a = 1$, $p = 12$ and $z_0 = 1.2 + 0.8i$. As can be clearly seen from Fig. 8, for these given parameters, System (1) has a positive Lyapunov exponent. Therefore, System (1) has good initial value sensitivity, and meets the requirements of the initial key. Compared with the traditional Julia set, the cryptographic algorithm based on the generalized alternated Julia set is more secure and can resist attacks more effectively.

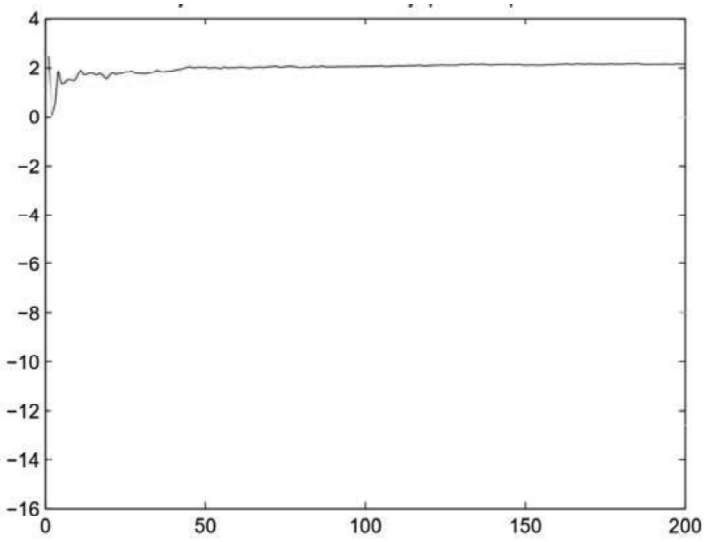

Figure 8: The Lyapunov Exponent.

C. Histogram analysis

Histogram is one of the important indicators of safety performance. The flatter the histogram distribution, the worse the readability of the encrypted image and the higher the security of encryption. The histograms of the three layers of the plain-text image and the cipher-text image are shown in Fig. 9 and Fig.10 respectively, where the abscissa represents the gray level, and the ordinate represents the frequency of the gray level in the image.

From Fig. 10, it is known that the distribution of each gray value in the cipher-text image is relatively uniform, indicating that the diffusion process of this encryption algorithm is more effective, and greatly changed the statistical characteristics of the original image. According to the simulation results, the gray value of each layer in the image tends to be balanced after encryption, indicating that the gray-scale diffusion effect of the image is better.

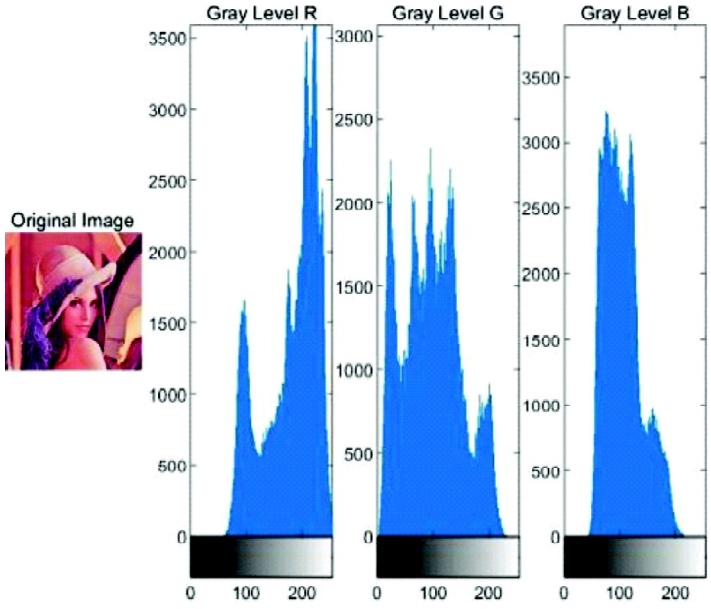

Figure 9: The original image and its histogram

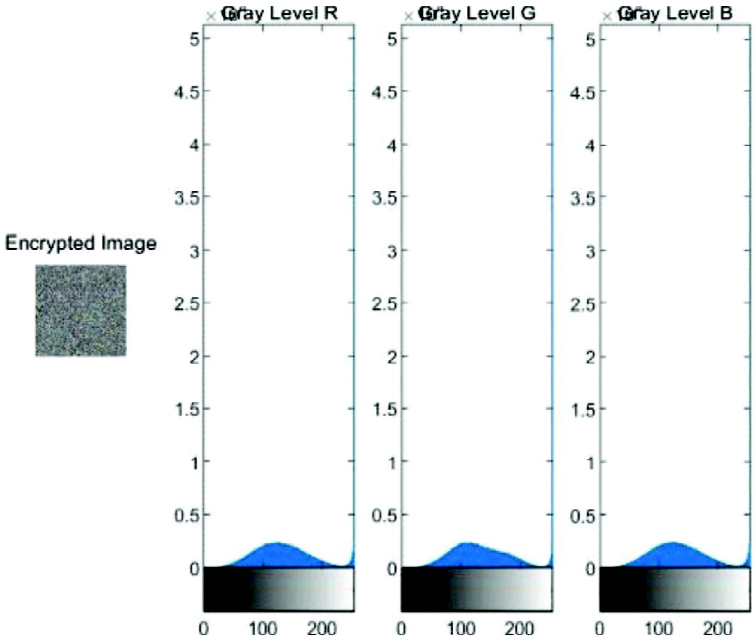

Figure 10: The encryption image and its histogram

D. Correlation analysis of adjacent pixels

The correlation coefficient of adjacent pixels can verify the degree of scrambling of the encryption algorithm to an image. The smaller the correlation coefficient, the better the security of the encrypted image and the less vulnerable to attack; conversely, the larger the correlation coefficient, the worse the security of the encrypted image and the easier it is to be attacked.

The calculation formula for the correlation of adjacent pixels is as follows,

$$c_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x))(y_i - E(y))],$$

where **x** and **y** are the pixel values of adjacent pixels, and N represents the number of selected pixel values,

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i.$$

We randomly selected 1500 pairs of adjacent pixels and calculated their correlation coefficients in different directions. Table I shows the correlation coefficients in different adjacent directions with N = 1500.

Table 1
Comparison of Correlation Coefficients

Direction	*Lena*	*encrypted image*
Horizontal	95.73%	1.27%
Vertical	95.69%	0.59%
Diagonal	98.37%	1.83%

From Table I, it can be seen that the correlation coefficient of adjacent pixels of the encrypted image is very small, which indicating that a good scrambling effect has been achieved.

VI. CONCLUSIONS

In this paper, the Julia set in generalized alternated system, which is more sensitive to the initial value, is used as the key in the encryption algorithm, and multiple XOR operations are added to the encryption algorithm, and the following conclusions are obtained:

(i) The key based on generalized alternated Julia set can be obtained by a small number of parameters;

(ii) The boundary of generalized alternated Julia set is chaotic, which makes that the key is very sensitive to slight changes of parameters, thus it greatly improving the security of the encryption algorithm;

(iii) The improved algorithm proposed in this paper has a good scrambling effect. The algorithm has a larger key space and enhances the resistance to attacks.

In summary, the encryption algorithm has a large key space (with fewer parameters) and a fast encryption speed, moreover, it is simple to calculate. The simulation results verify the effectiveness of the encryption algorithm. This research is a cross-study of fractal theory and information security, and it has important significance for the application of fractal theory in information security.

ACKNOWLEDGEMENT

This work was supported by the Natural Science Foundation of Shandong Province under Grant No. ZR2018QF004.

REFERENCES

[1] Furht B., Kirovski D. (2005). Multimedia Security Handbook. Florida: CRC Press.

[2] Sangavi V., Thangavel P. (2019). An Image Encryption Algorithm Based on Fractal Geometry. *Procedia Computer Science*. 165, 462-469.

[3] Anandkumar R., Kalpana R. (2019). Designing a fast image encryption scheme using fractal function and 3D Henon Map. *Journal of Information Security and Applications*. 102390.

[4] Rozouvan V. (2009). Modulo image encryption with fractal keys. Optics and Lasers in Engineering. 47, 1-6.

[5] Yoon E., Yoo K. (2010). Cryptanalysis of a modulo image encryption scheme with fractal keys. *Optics and Lasers in Engineering*. 48, 821-826.

[6] Hennelly B.M., Sheridan J.T. (2003). Image encryption and the fractional Fourier transform. *Optik*. 114, 251-265.

[7] Singh N., Sinha A. (2008). Optical image encryption using fractional Fourier transform and chaos. *Opt Lasers Eng*. 46, 117-123.

[8] Liu Z.J., *et al.* (2013). Opto-digital image encryption by using baker mapping and 1-d fractional flourier transform. *Opt. Lasers Eng*. 51, 224-229.

[9] Wang M.M., *et al.* (2020). Optical image encryption scheme based on apertured fractional Mellin transform. Optics and Laser Technology. 124, 106001.

[10] Liu S.T., Wang P. (2018). Fractal control theory. Springer. [11] Kilbas A., Srivastava H., Trujillo J. (2006). Theory and applications of fractional differential equations. Amsterdam: Elsevier Science Limited.

[12] Mandelbrot B. (2004). Fractals and chaos: the Mandelbrot set and beyond. New York: Springer.

[13] Sun Y,Y., *et al.* (2013). Research on modulo image encryption algorithm utilizing Julia sets. *Computer Engineering and Applications*. 49, 75-79.

[14] Slimane N.B., Bouallegue K., Machhout M. (2017). Designing a multi-scroll chaotic system by operating Logistic map with fractal process. Nonlinear Dyn. 88, 1655-1675.

[15] Gao W.J., *et al.* (2019). Digital image encryption scheme based on generalized Mandelbrot-Julia set. Optik-*International Journal for Light and Electron Optics.* 185, 917-929.

[16] Danca M., Romera M., Pastor G. (2009). Alternated Julia sets and connectivity properties. *Int J Bifurcat Chaos*. 19, 2123-2129.

[17] Wang P., Liu S.T. (2015). The gradient control of spatial- alternated Julia sets. *Nonlinear Dynamics*. 80, 1291-1302.