Digital Image Encryption Scheme Based on Chaos and Fractal

Yanling Sun*, Shitong Liu, Jing Na, Peng Wang, Jie Wang and Huixin Ma
College of Science, Shenyang Jianzhu University, Shenyang, Liaoning, China

*Corresponding author e-mail: alphasmh@sjzu.edu.cn

Abstract. With the rapid development of Internet technology, images are increasingly used as a means of user information exchange. Therefore, ensuring the security of image information has become the focus of attention. Chaos and fractal has the characteristics of self-similarity, pseudo-randomness, and high complexity of image structure, and it’s an important subject in ensuring information security. This paper proposes an image encryption algorithm based on chaotic and fractal. The algorithm uses the Julia set constructed by the Hilbert curve to form the encryption key, and the image is diffused horizontally and vertically. Experimental results show that this algorithm has a large key space, high sensitivity to the initial value of the key, and can resist attacks. The research on the image encryption method proposed in this paper helps to improve the effect of image encryption.

Keywords: Image Encryption, Chaos and Fractal, Hilbert Curve, Chaos Scrambling

1. Introduction
With the development of the information age, digital images are one of the common forms of information on the Internet. In the information transmission system, the transmission accuracy of the image requires reliable image encryption technology. Therefore, image encryption technology has been paid more and more attention.

At present, the methods of image encryption mainly include scrambling encryption of the original image, encryption combined with other data processing technologies and encryption using key encryption. Among the image scrambling algorithms, there are algorithms that scramble according to certain transformation rules, such as Liping Shao’s avalanche image scrambling transformation method based on high-dimensional matrix transformation [1]; and scrambling based on the characteristics of the image itself. Algorithms, such as Nan Jiang etc., use the method of block scrambling first and then second scrambling based on DCT transform [2]. Among the algorithms that use key encryption, there are many researches on chaotic cryptography. For example, Guanrong Chen et al generate keys based on three-dimensional chaotic mapping, and perform "different places" operation encryption on images. Xiaofeng Liao et al. Improved symmetric image encryption algorithm [3], Xingyuan Wang et al analyzed and improved an encryption system based on Logistic mapping [4], Xianghua Zhang proposed a digital image encryption algorithm based on chaotic mapping network and standard magic square transformation [5]. At the same time, chaos and fractal theory has also been applied to encryption algorithms. For example, Wentao Liu et al used the irregularity of fractal graphs to give plaintext to ciphertext algorithms. Zhifei Lian et al combined fractal encoding with magic square
transformation to hide image information [6], Zhenxiang Dai et al studied the application of fractal geometry in cryptography [7], Fangxiu Wang generated a key file by drawing a random Koch curve, and Rozouvan used the Mandelbrot set as a key to encrypt the image.

This paper proposes an image encryption system based on chaos and fractal. The system given in this paper corresponds to a large key space, and the initial value of the key is highly sensitive and strong against attacks. Therefore, the research in this paper helps to improve the effect of image encryption.

2. Basic Theory
Chaos dynamics and fractal geometry are important components of nonlinear science and are also the frontiers of current scientific research. The use of chaos and fractal theory combined with the research of digital image encryption can further explore the proof and construction mechanism of intuitive and vivid visual image encryption algorithms, and provide new ideas for the discovery of new phenomena and new laws of digital image encryption technology. As an important means of digital image protection, digital encryption technology has been increasingly valued and studied by many scholars, so digital image encryption algorithms based on chaotic fractals.

2.1. Chaos and Fractal
In the final analysis, the cause of chaos is that the things that are connected to each other are not unilaterally affected, but they are mutually influenced, restricted and interdependent. The performance of this interaction in a dynamic system is that the state variables are coupled with each other, so the dynamic system must be nonlinear. Chaos is ubiquitous in real life and practical engineering technical problems.

Fractal theory, known as the geometry of nature, is a new branch of modern mathematics, but its essence is a new worldview and methodology. It is cross-combined with the chaos theory of dynamical system and complements each other. It recognizes that parts of the world may be similar to the whole in a certain aspect (form, structure, information, function, time, energy, etc.) under certain conditions and processes. It recognizes that changes in spatial dimensions can be either Discrete can also be continuous, thus expanding the field of vision [8]

2.2. Hilbert Curve
The Hilbert curve was discovered and proposed by the German mathematician David Hilbert in 1891. It is a wonderful curve. As long as the function is selected appropriately, a continuous parameter curve is drawn. When the parameter t is in the interval of 0, 1, the curve will traverse all the points in the unit square to obtain a curve full of space. The Hilbert curve is a continuous and non-derivable curve. Since the direction of the Hilbert curve is different, the point after Hilbert's scrambling is very different from the original position.

The formation process of the Hilbert curve is: First, divide a square of 2*2 size into four small squares of equal size. The curve enters the square from the lower left corner of the square, reaches the upper left square, and then passes through the upper right square to the right. And finally reach the square in the upper right corner. After one iteration, a one-dimensional Hilbert curve is formed. When the square size is 16, the Hilbert path only needs to splice four 2*2 squares together. The exit of each square is the entrance of another square. In the 4ⁿ square, the Hilbert curve has gone through two iterations. We call it a two-dimensional Hilbert curve. When the square is divided into infinite sizes, the Hilbert curve goes through infinite iterations. In the squares passed by the Hilbert curve, the Hilbert curve traverses all squares, but it does not pass through the same square repeatedly. The Hilbert curve is suitable for a square with a size of 4ⁿ. Figure 1 is an image of Hilbert curve.

In the first-order Hilbert curve, if the entry point and exit point of the Hilbert curve are different, the order of traversing the pixels is different, resulting in a different order of the last scrambled pixels. According to the different order of Hilbert traversal of pixels, the final Hilbert curve generated is different. There are 8 kinds of Hilbert curves in each iteration. It is precisely because of this
characteristic of the Hilbert curve that the image scrambled by the Hilbert curve is also random. When used for image encryption, combined with the key generated by the Julia set, it is not easy to be attacked.

![Image of Hilbert curve](image.png)

Figure 1. Image of Hilbert curve

3. Image Encryption Algorithm Based on Chaos and Fractal

This algorithm encrypts the image through the image scrambling of the Hilbert curve [9-11]. The image format adopted in this article is BMP, which consists of three layers of RGB. This article uses 256*256 image encryption, and each layer consists of 8 bits. When each layer is scrambled, the odd-numbered bits of the 8-bit layer are subjected to Hilbert forward scrambling, and the even-numbered bits are subjected to Hilbert backward scrambling. The specific steps are as follows:

1. Using the fractal escape time algorithm to get the Julia set image, this paper selects the Julia set image boundary structure to compare and adjust the image size to generate a standard image of 256*256 size;
2. This paper selects the current coordinates of the Julia image of the Hilbert curve, and then finds the coordinates after the forward step and the backward step. After converting the pixel values of these two coordinates into binary form, it performs "different places" and assigns the result of "different places" to the pixel value of the current coordinate to obtain the scrambled key;
3. In this paper, the generated key and the plaintext image are modulo arithmetic to obtain the first encrypted temporary ciphertext;
4. The temporary ciphertext image is first diffused horizontally and then diffused vertically. And each time it is diffused, the RGB three layers of the color image are sequentially diffused. And provide the key value for the next layer of diffusion every time;
5. To enhance the encryption effect, this article can repeat steps (3) and (4);
6. Get the final ciphertext image.

The encryption flowchart of the algorithm is shown in Figure 2.

This algorithm is a symmetric encryption algorithm, so the decryption process of the ciphertext is the inverse process of the algorithm. The ciphertext image to be obtained is first de-diffused, and then decrypted by modulo operation according to the known key.
Figure 2. The encryption flowchart of the algorithm

When de-diffusing the diffusion algorithm, de-diffusion is the inverse process of diffusion. When diffusing, the first pixel in the plaintext is first diffused, and then from left to right, from top to bottom. When despreading, this algorithm starts from the last pixel of the ciphertext, then it proceeds from right to left, and from bottom to top.

4. Conclusion
This paper proposes an image encryption scheme based on chaos and fractal. Using Hilbert curve to scramble the fractal set, the encryption key of the modular operation stage is obtained. Combined with the diffusion algorithm, the known plaintext attack and the selected plaintext attack of the encryption algorithm in this paper are improved. In summary, the algorithm key storage space in this paper is small, the calculation is simple, the encryption speed is fast, and the original image is not damaged.

Acknowledgments
This work was financially supported by Science and Technology Department of Liaoning Province Project (2019-ZD-0667); Liaoning Provincial Department of Education Project (lnqnp201919); Shenyang Jianzhu University Project (2018-185:2-7); National Undergraduate Entrepreneurship Project (2020) fund.

References
[1] Liping Shao, etc. Avalanche Image Scrambling Transformation Based on High-dimensional Matrix Transformation. Journal of Images and Graphics, 2008, 13 (8): 1429-36.
[2] Nan Jiang, etc. An Encryption Algorithm for Image Transmission Based on Double Permutation. Journal of Images and Graphics, 2009, 14 (5): 897-904.
[3] Wei Zhang, etc. A Modified Symmetric Image Encryption Scheme Based on Chaotic Map. Computer Science, 2007, 34 (12): 248-251.
[4] Xianghua Zhang. Digital Image Encryption Algorithm Based on Chaotic Map Network. Computer Engineering, 2010, 36 (6): 175-177.
[5] Wentao Liu, etc. Application of Fractal Theory in Cryptographic Algorithm. Journal of CAEIT,
2008, 3 (6): 580-585.

[6] Zhifei Lian, etc. Magic square transform encrypted fractal graph. Fujian Computer, 2009, 25 (12): 111-112.

[7] Wei Zhang, etc. A Modified Symmetric Image Encryption Scheme Based on Chaotic Map. Computer Science, 2007, 34 (12): 248-251.

[8] Yanling Sun. Visualizing research of construction of dynamic system with plane symmetry in different sizes of cycle windows. Shen Yang: Shenyang Jianzhu University, 2009.

[9] Wenjian Gao, etc. Digital image encryption scheme based on generalized Mandelbrot-Julia set. International Journal for Light and Electron Optics, 2019, 185: 917-929.

[10] Yi-Chiuan Chen etc. Simple proofs for the derivative estimates of the holomorphic motion near two boundary points of the Mandelbrot set. Journal of Mathematical Analysis and Applications, 2019, 473: 345-356.

[11] Min Wang, etc. A color image encryption algorithm based on matrix transformation. Image Processing and Multimedia Technology, 2010, 29 (02): 61-65.