Image Encryption Based on Arnod Transform and Fractional Chaotic

Chao Chen[12], Hongying Zhang[1], Bin Wu[1]*

[1*] Southwest University of Science and Technology, Sichuan Province, Mianyang, China

2 Data Recovery Key Laboratory of Sichuan Province, Neijiang, China

*** Correspondence:**
Bin Wu
email: wubin@swust.edu.cn

Keywords: fractional derivative, Arnold Transform, XOR involving fractional order chaotic sequence, encryption and decryption.
OCIS : 100.2000, 100.2960 , 100.3008, 100.3010

Abstract

In view of the problem of cracking easily and partial distortion of images after encryption or decryption, a novel image encryption and decryption algorithm based on Arnod Transform and fractional chaotic is proposed. To begin with, the Arnold transform is used to encrypt. So that the spatial confidence of the original image has been comprehensively disturbed. Secondly, the XOR involving the fractional order chaotic sequence is used to encrypt. The key sequence is dynamically generated to ensure the randomness and difference of key generation. When decryption is required, the first decryption is performed using the key and XOR. Then the second decryption is carried out by using the inverse Arnold transform, and finally the decrypted image is obtained. Experimental results show that the improved algorithm has achieved better performance in encryption and decryption.

1 Introduction

With the popularity of smart phones, image encryption in the process of transmission has become an important research topic. The security of image transmission is closely related to personal privacy and property safety. It seems to be somewhat inadequate by relying on only legal constraints. Li X, Zhou put forward the idea of DNA and space-time chaos, which made good use of the coding characteristics of DNA to encrypt images, and achieved good results [1]. Liu H and Jin proposed to encrypt images based on Arnold transform, quantum chaos and S-Box model [2, 3]. Quantum chaos spreads well the degree of scrambling of plaintext and achieves better encryption effect. Some scholars also used YCbCr space to encrypt images [4], convert to color images to encrypt images. It makes good use of the effect of image stratification. Ni Z and Kang improved the Arnold transformation and quantum chaos [5-6]. With a very good combination of each others' advantages, encryption effect is remarkable. Xu L, Gou and others put forward an image encryption algorithm based on improved standard mapping, and used function to map image encryption algorithm, and achieved remarkable results [7]. Vaish A, Kumar used MSVD, DWT and Arnold transformed to encrypt images [8], which effectively prevented the hacker's violent attack. Chai X and Gan Z. put forward the compress perception to encrypt images combined with the related concepts of physics, and the encryption effect was good [9]. Domestic scholars put forward the research of Arnold transform and Gray code transformation, the blind detection robust digital watermark embedding strategy, the combination of Tetrolet transform and SVD, the digital image encryption algorithm based on Arnold hierarchical cyclic transformation, and used Logistic and Rossler to encrypt the image image [10-14]. Gong Lihua introduced fractional partial derivative [15], convert to frequency

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

domain filter and combine two dimensional Arnold transform to encrypt image, so that the image was encrypted in both spatial and frequency domain, and good encryption effect has been obtained. However, the method is simple and easy to be attacked by hackers. In recent years, skew tent chaos mapping combined with Arnold transform have been proposed to encrypt images by means of enhanced singular value decomposition and zero watermark of cellular neural network [16-18]. However, this only changes the spatial location information of pixels. After finding the Arnold Transform inverse function, the key can be quickly obtained. Good results have been achieved in encryption, but there were still some flaws in the hacker's violent decryption of the encrypted image. In view of the fact that image encryption is not absolutely safe and partly distorted after image restoration. An image encryption and decryption algorithm based on Arnold transform is put forward to disturb texture of the image and spatial pixel distribution. Then it uses the XOR involving the fractional order chaotic sequence to change the pixel value itself. After two encryption, the difficulty of hacking is greatly enhanced. After receiving the image, the information of the original image can be obtained after two decryption. Experimental results have shown that the improved algorithm achieves better results, and the security and difficulty of image transmission are greatly improved. It is difficult to decipher the real data of the image without obtaining the random fractional derivative sequence.

2 Preliminary

2.1 The Principle of Image Encryption Using Arnold Transform

The essence of Arnold transform is used to change the coordinates of original pixels in the spatial domain. Arnold transformatiosn is also commonly known as "cat-facet ransformation" [3]. The specific two-dimensional Arnold transformation formula can be written as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (1)$$

Where: (x, y) is the spatial 2-dimensional coordinates of the pixel located in the image to be encrypted (x', y') is 2-dimensional coordinates transformed after the cat is transformed. The Arnold transform matrix is symmetrical. Using the Arnold transform to encrypt the image basing on first encryption. It became chaotic in space, so as to achieve the effect of searching for regularity when disturbing hacker attacks.

2.2 First Image Encryption Principle of Arnold Transform

Arnold Transformation has periodicity [11-12], and periodicity is not proportional to the size of the image. Table 1 shows the relationship between the order of image and the period [15-18]:

Table 1 Relationship between the period of Arnold transformation and the number of images

Order	period	Order	period
4	3	64	48
8	6	128	96
16	12	256	62
32	24	512	384

All the image sizes to be encrypted in this experiment are normalized to 128*128. According to the relationship between the Arnold transform cycle and the order of image displayed in Table 1, the Arnold transform period of this experiment was 96. The Arnold transform encrypted image can recover image original data by inverse operation.

3. Analysis of Proposed Method

3.1 Improving the Principle of Image Encryption and Decryption

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

The improving two-dimensional Arnold transformation formula can be written as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \quad (2)$$

where

$$a = \text{ceil}(\text{mean}(u_{(0)} + \frac{\mu}{\Gamma(v)} \sum_{j=1}^{n} \frac{\Gamma(n-j+v)}{\Gamma(n-j+1)} u(j-1)(1-u(j-1)))) \quad (3)$$

$$b = \text{ceil}(\text{mean}(u_{(0)}{}' + \frac{\mu'}{\Gamma(v)} \sum_{j=1}^{n} \frac{\Gamma(n-j+v)}{\Gamma(n-j+1)} u'(j-1)(1-u'(j-1)))) \quad (4)$$

Where mean is the mean values of the generated random sequences, ceil is an integer round up. Obverously, the parameters of Arnold transformation matrix a and b are symmetrical in form. The parameters in Equation (3) are

$$v = 0.7, \mu = 2.4, \mu(0) = 0.1.$$

The parameters in Equation (4) are

$$v = 0.8, \mu = 2.5, \mu(0) = 0.2.$$

Equation (3) and Equation (4) were brought into Equation (2). Finally, a transformation matrix(in Equation (2)) is obtained.

3.2 Arnold Transformation Using the Fractional Logistic Map

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, which often cited as an archetypal example of complex, so that chaotic behaviour can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst. One-dimensional Logistic mapping is the most widely applied chaotic mapping currently, the chaotic models generated by it are also known as insect amount model, and its mathematical defined as follows [16-17] [25-27]

$$\mu_{n+1} = \mu_0 + \mu_n (1-\mu_n). \quad (5)$$

The dynamic state of Logistic mapping is chaotic. At this time, the chaotic sequence generated by Logistic mapping has significant non-periodicity and non-convergence. Many hackers are familiar with this conventional encryption method, so this encryption method is relatively mature and easy to crack, so that the security of image encryption method can not be guaranteed.

Inspired by Guocheng Wu 's related literature[22], and non-Fourier's heat flux and non-Fick's mass flux theory had been used to save the numerical study of bioconvection flow of nanofluids[23-27]. we introduce the fractional order chaotic sequence to improve the Arnold transform.

$$u_{(n)} = u_{(0)} + \frac{\mu}{\Gamma(v)} \sum_{j=1}^{n} \frac{\Gamma(n-j+v)}{\Gamma(n-j+1)} u(j-1)(1-u(j-1)) \quad (6)$$

Where Γ is Gamma function, v is fractional order. The stability, turbulence and chaos of Equation (6)can be discussed in reference to [19-20] [26].

3.3 Arnold Transformation Using the Fractional Logistic Map

Research shows that when the determinant value of the transformation matrix $\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$ is 1, Arnold

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

map enters chaotic state. But there is a one to one relationship between the spatial coordinates before and after transformation, and the periodic T before Arnold will be extended indefinitely. After *n* times of Arnold transformation, the image scrambling effect is very good, the distribution of image pixels is fairly uniform, and the irrelevance between pixels is enhanced to achieve a good encryption effect. Based on the periodicity and reversibility of Arnold transform and the randomness of fractional chaotic sequence, a color digital image encryption algorithm based on Arnold transform is proposed. Through the improved Arnord transform, the image is encrypted by disorderly and distinct images, and it is difficult to correlate with the original image. The improved method not only simplifies the image encryption and decryption operations, but also does not add additional storage space. Theoretically, it can restore the encrypted image completely lossless.

3.4 Fractional Order Logistic Chaos XOR

XOR algorithm principle: The XOR operation has a curious feature: if you do XOR twice in a row to a value, it returns the value itself. XOR operation is most suitable for simple encryption and decryption. The principle of this method is that when XOR operation is performed on one number A and another number B, another number C will be generated. If XOR operation is performed on Key and B, then C will be restored to A. Compared with other simple encryption algorithms, XOR algorithm has many advantages, such as the algorithm is simple, speed is fast and encryption of the gray value of the image can achieve complete lossless reduction.

We randomly select a sequence from the 3 fractional order chaotic sequences as the XOR encryption key. On the basis of the first use of Arnord transform, XOR operation is used for secondary encryption to enhance the security of image encryption again.

$$Key = \text{ceil}(\text{mean}(u_{(0)}\text{"}+\frac{\mu\text{"}}{\Gamma(v)}\sum_{j=1}^{n}\frac{\Gamma(n-j+v)}{\Gamma(n-j+1)}u\text{"}(j-1)(1-u\text{"}(j-1)))) \quad (7)$$

4 Implementation

The image contains R, G, B three primary colors, respectively, and encryption and decryption of the three primary colors. This paper only deals with the two level decomposition of encrypted color digital images. The above methods are used to encrypt the G and B primary color matrix of the image. Finally, the encrypted R, G and B primaries are combined to get the encrypted color digital images. And Arnold inverse transform for the current image. Because the Arnold transform is periodic, that is to say, assuming that the Arnold period of an image is T, the original image is scrambled by T times Arnold transform and then returns to the original image. Therefore, if the number of scrambling of Arnold transform is *k* when the original R- base color is encrypted, then the encrypted R-base color is re- transformed by *T-k* Arnold transform, and the unencrypted R-base color is returned, that is to say, the decryption effect is achieved, and satisfactory decryption effect can be achieved. For the encrypted images, the G and B primary color matrices are encrypted by the above methods. Finally, the decrypted R, G and B primaries are combined to get the deciphered color digital images. **Procedure of our proposed algorithm are as follows . Imported two original images are as the input of our proposed algorithm.**

Step0: Three fractional order chaotic sequences are generated and two are chosen randomly as a, b in Arnold transform matrix.

Step1: Using fractional order Logistic chaos Arnold transform to realize encryption of spatial coordinates;

Step2: Three fractional order chaotic sequences are generated and one is chosen randomly as key. The parameters in this key are: $v=0.9, \mu=2.7, \mu(0)=0.3$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

Step3: Using XOR involving key to realize encryption.

Step4: Taking the encrypted image with the key (fractional order logistic chaotic sequence to) to decrypt the image.

Step5: Using Arnold inverse transformation to realize secondly encryption of spatial coordinates.

Finally, the result of the output is a decrypted complete image.

5 Experiment and Performance Comparison

5.1 Distribution Characteristic of Pixel Value

The histogram of plaintext image and the histogram of the ciphertext image are very different, so it can not reflect the pixel distribution characteristics of the image. Deliberately stitching the opponent's image and scrambling spatial coordinates will effectively confuse the hacker against the use of statistical gray value distribution to attack encrypted images.The experimental results show that there are great differences in histogram before and after scrambling.

5.2 Correlation Analysis of Each Other Image

The adjacent pairs of pixels in horizontal, vertical and diagonal directions are calculated by Equation (8) .

$$r = \frac{\sum_{i=1}^{M_0}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{M_0}(x_i - \bar{x})^2 (y_i - \bar{y})^2}} \qquad (8)$$

The two pixel values of the adjacent pixels X_i and Y_i of group i in the image, x, y are the mean values of pixel values X_i and Y_i, respectively, M is neighbor pixel. The improved algorithm can be very good at disordering the correlation between pixels.

5.3 Analysis of the Ability to Resist the Difference Attack

NPCR:Number of Pixels Change Rate. It measures Sensitivity of encryption algorithm to plaintext [14-18]; UACI: Unified Average Changing Intensity measures Sensitivity of encryption [14-18]. When there is only one pixel in the process of encryption and decryption, set the pixel values of their (i, j) points in their ciphertext images respectively $C_{1(i,j)}$ and $C_{2(i,j)}$. If $C_{1(i,j)} = C_{2(i,j)}$, define $D_{(i,j)} = 0$; If $C_{1(i,j)} \neq C_{2(i,j)}$, define $D_{(i,j)}$. So formulas for the calculation of NPCR are as follows [14-18]

$$NPCR = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) * 100\% \qquad (9)$$

$$UACI = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|c_1(i,j) - c_2(i,j)|}{255} * 100\% \qquad (10)$$

The expected value of the two is calculated by using the Equation (11) and Equation (12)[14-18]:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

$$NPCR_E = (1-2^{-n}) \times 100\% \tag{11}$$

$$UACI_E = \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n-1} i*(i+1)}{2^n-1} \times 100\% \tag{12}$$

There are M pixels in the vertical direction of the image and N pixels in the horizontal direction of the image, which can test the sensitivity before and after encryption.

5.4 Information Entropy Analysis

Using Equation (13) to calculate information entropy, which is an important measure to reflect the randomness of information [14-18]

$$H(S) = -\sum_{i=0}^{2^n-1} P(s_i) \log 2(P(s_i)) \tag{13}$$

Where: $P(s_i)$ represented the probability of the emergence of pixel S_i, 2^n represented the number of states that appear in total, $H(S)$ can test the amount of information covered by encrypted images and pre-encrypted images.

5.5 Abbreviatio of the Relative Comparative Experimental Data

To simplify the representation, we simplify the relevant parameters here. Hm1: The information entropy of the original image. Hm2: Information entropy of encrypted image, NPCR: Pixel number change rate, UACI:Normalized pixel value average change intensity .

5.6 Detailed Experimental Data

a) First Group Contrastive Experiment

The original image, encrypted image, and decrypted image of the lena image are shown in Figure 1 respectively.

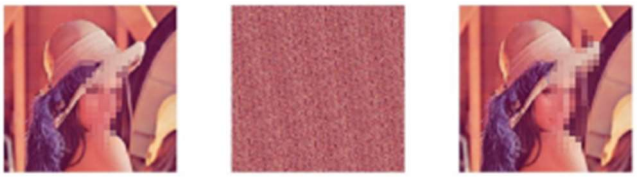

Figure 1 comparison map before and after encryption of the lena

We can see that the encrypted image is completely misplaced in space, and there is no connection between the encrypted image and the original lena image. The decrypted lene image has no change with the original image. 3 color RGB channels' s histogram of original Lena image is shown in Figure 2.

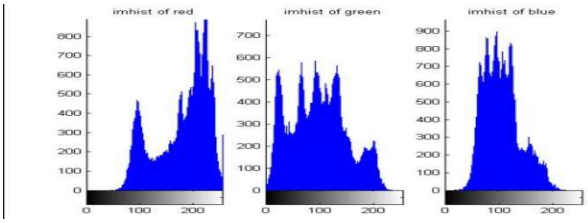

Figure 2 Histogram of original Lena image

Three color RGB channels' s histogram of Lena' s encrypted image is shown in Figure 3.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

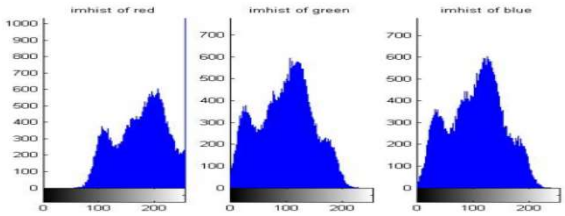

Figure 3 Histogram of encrypted Lena image

It can be seen that the histogram has undergone a large transformation and can hardly reflect the gray value distribution of the three channels. Correlation analysis of original image and the encrypted image is shown in Figure 4.

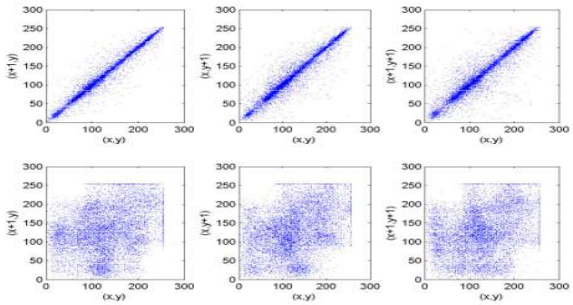

Figure 4 Correlation charts of three directions before and after encrypted Lena image

The encrypted image is well scrambled in three directions. Analysis of the ability to resist the difference attack, details are shown in Table 2.

Table 2 Lena' s information entropy and NPCR，UACI

	Hm1	Hm2	NPCR	UACI
Lena	7.7580	7.7816	0.1723	0.0725

As can be seen from Table 2, the encryption effect is good, and it can withstand the attack of hackers well.

b) Second Group Contrastive Experiment

The original image, encrypted image, and decrypted image of the girl image are shown in Figure 5 respectively.

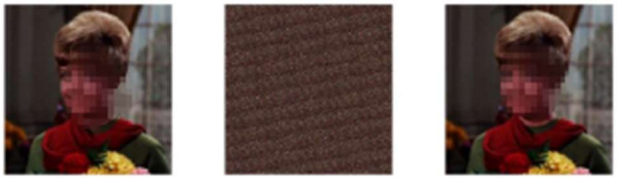

Figure 5 comparison map before and after encryption of the girl

The encrypted image is a mess. We can see that the encrypted image is fundamentally not related to the original image. Three color RGB channels' s histogram of girl' s encrypted image is shown in Figures 6 and 7.

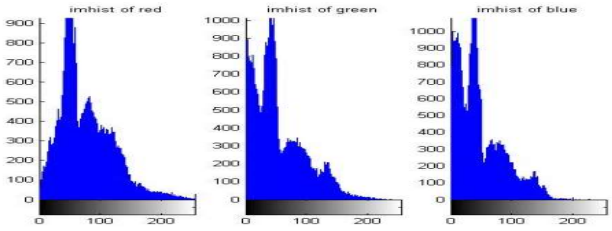

Figure 6 Histogram of original girl image

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

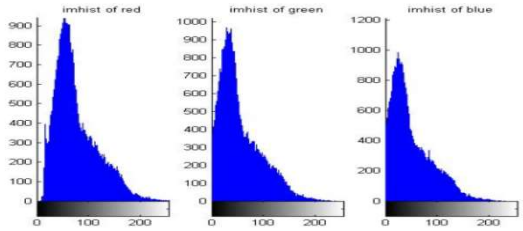

Figure 7 Histogram of encrypted girl image

From the histogram information, we can know that the gray value distribution of the image changes obviously, which can disturb the hacker's feature analysis very well. Three directions correlation before and after encryption are shown in Figure 8 .

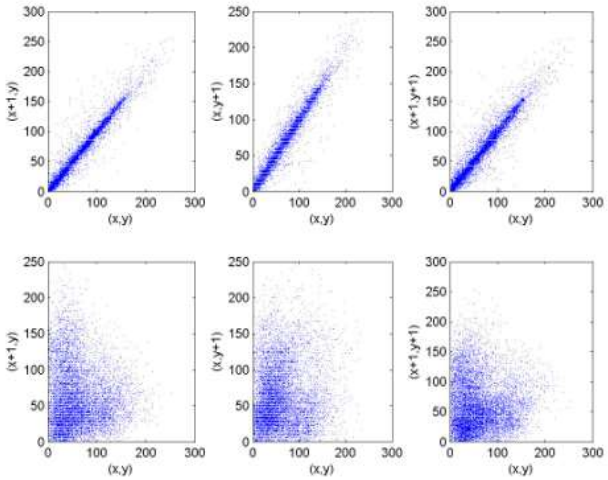

Figure 8 Correlation charts of three directions before and after encrypted girl iamge

We disturb the correlation analysis of hackers from three directions and analyze of the ability to resist the difference attack. The details are shown in Table 3.

Table 3 girl' s information entropy and NPCR，UACI

	Hm1	Hm2	NPCR	UACI
girl	7.0467	6.9732	0.1638	0.0586

c) Third Group Contrastive Experiment

The original image, encrypted image, and decrypted image of the peppers image are shown in Figure 9 respectively.

Figure 9 comparison map before and after encryption of the peppers

In the first image of Figure 9, only one pixel wide text is scrambled, and after decryption, the original image is completely restored. Three color RGB channels' s histogram of peppers' s encrypted image is shown in Figures 10 and 11.

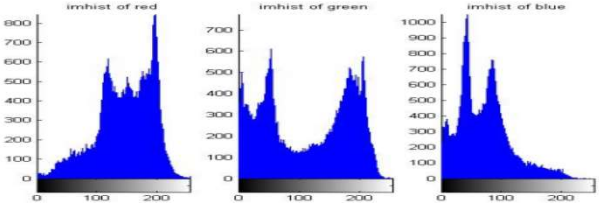

Figure 10 Histogram of original peppers image

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

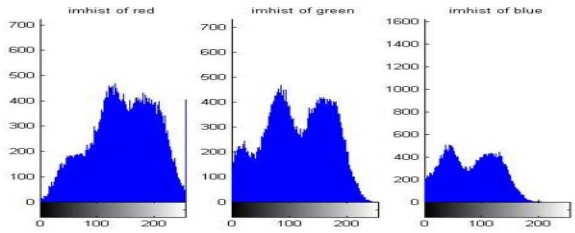

Figure 11 Histogram of encrypted peppers image

From the histogram information, we can know that Histogram information has been greatly changed, which can increase the difficulty of cracking encrypted images. In particular, the feature distribution of red channel and green channel changed greatly. However, histogram, as an important analysis means to crack image encryption, can well prevent crackers from analyzing image features. Three directions correlation before and after encryption are shown in Figure 12 .

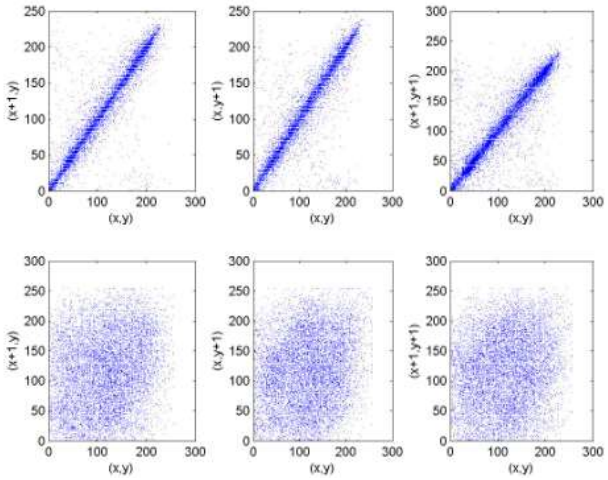

Figure 12 Correlation charts of three directions before and after encrypted peppers image

The correlation between the three directions indicates the degree of correlation between them. As for the analysis of the ability to resist the difference attack, the details are shown in Table 4.

Table 4 peppers' s information entropy and NPCR，UACI

	Hm1	Hm2	NPCR	UACI
peppers	7.5743	7.4929	0.1661	0.0757

Information Entropy can well express how much information the image contains. As long as there are some differences, it will increase many difficulties in cracking the content of image encryption.

d) Fourth Group Contrastive Experiment

For animals, hair is the most important feature, and the basic five features are embedded in it. Here our algorithm can integrate these features very well, especially the number of a pixel in it is also well encrypted, which is difficult to crack through conventional algorithms. Used the corresponding inverse transform, the image information can be restored completely. The original image, encrypted image, and decrypted image of the peppers image are shown in Figure 13 respectively.

Figure 13 comparison map before and after encryption of the baboon

The encrypted image presents complete confusion, which has caused more obstacles to the cracked person. Three color RGB channels's histogram of baboon's encrypted image is shown in Figures 14 and 15.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 December 2021 doi:10.20944/preprints202112.0269.v1

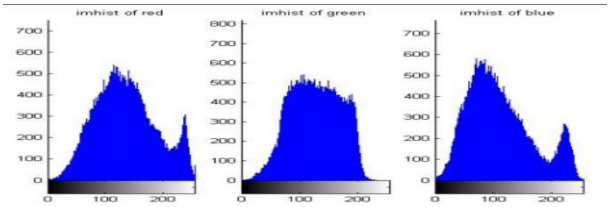

Figure 14 Histogram of original baboon image

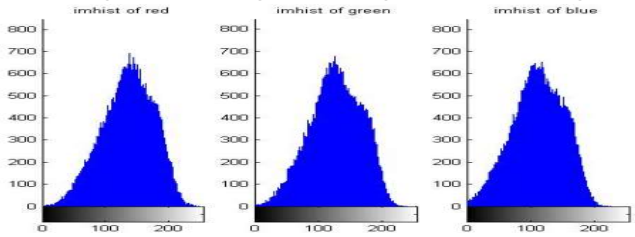

Figure 15 Histogram of encrypted baboon image

From the histogram information, the gray value distribution of the three color channels has changed greatly. Three directions correlation before and after encryption are shown in Figure 16.

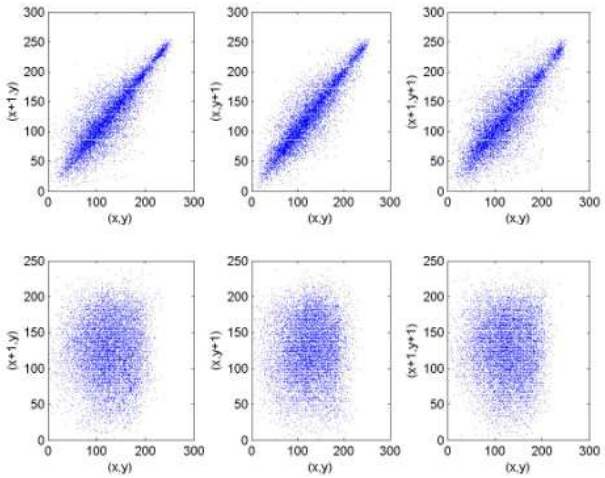

Figure 16 Correlation charts of three directions before and after encrypted baboon image

The correlation between the three directions indicates the degree of correlation between them. As for the analysis of the ability to resist the difference attack, details are shown in Table 5.

Table 5 baboon' s information entropy and NPCR，UACI

	Hm1	Hm2	NPCR	UACI
baboon	7.6701	7.39777	0.1602	0.0682

For the encryption of animal images, the meaning is very important, which can well disrupt the information of hunter' s pursuit path and so on. Even if poachers get animal image information, it is difficult to obtain normal and real information. Information Entropy can well express how much information the image contains. As long as there are some differences, it will increase many difficulties in cracking the content of image encryption.

6 Concluding and Discussion

In view of the security in need of the network transmission image, the encrypted image is easy to be cracked by hackers or difficult to completely restore the encrypted image. According to the features of each image, there are obvious changes in the main features before and after encryption. The decrypted image is inferior to the original image, and the value obtained is very small. After being converted into image format, the decryption effect is very good. The encryption and decryption algorithm proposed in this paper is simple and easy to implement, which not only reduces the computational complexity of the encryption algorithm, but also improves the security of the

encryption algorithm. The information contained in the decrypted image and the original image had not changed much, which shows that the decryption effect is good. The validity of the proposed algorithm has yet to be verified in detail on large international data sets.The future research direction will introduce modern intelligent algorithm, deep neural network and so on to encrypt or decrypt the image, or introduce varied chaos system to protect the image. In the future,comprehensive modern intelligent algorithms may be introduced to encrypt and decrypt, or to introduce varied chaotic systems and convert them into frequency domain to encrypt, so that the security of image transmission can be guaranteed.

REFERENCES

[1]Li X, Zhou C, Xu N. A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos. International Journal of Network Security. (2018) , 20(1). doi: 10. 6633/ IJNS. 201801. 20(1). 12.

[2]Liu H, Jin C. A color image encryption scheme based on arnold scrambling and quantum chaotic. International Journal of Network Security. (2017), 19.

[3]Farwa S, Shah T, Muhammad N, et al. An Image Encryption Technique based on Chaotic S-Box and Arnold Transform[J].International Journal of Advanced Computer Science & Applications. (2017), 8(6). doi: 10.1007/s13319 -017- 0135- x

[4]Jin X,Yin S, Li X, et al. Color image encryption in YCbCr space[C]// International Conference on Wireless Communications & Signal Processing. IEEE, (2016). doi: 10.1109/WCSP.2016.7752646

[5]Ni Z, Kang X, Wang L. A novel image encryption algorithm based on bit-level improved Arnold transform and hyper chaotic map[C]// IEEE International Conference on Signal and Image Processing. IEEE, 2017:156-160. doi: 10.1109/SIPROCESS.2016.7888243

[6]Hu Y, Xie X, Liu X, et al. Quantum Multi-Image Encryption Based on Iteration Arnold Transform with Parameters and Image Correlation Decomposition. International Journal of Theoretical Physics.(2017) 56(7):2192- 2205. doi: 10. 1007/ s10773- 017- 3365- z

[7]Xu L, Gou X, Li Z, et al. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Optics & Lasers in Engineering. (2017), 91:41-52. doi: 10.1016/ j. optlaseng. 2016. 10. 012

[8]Vaish A,Kumar M. Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. Optik-International Journal for Light and Electron Optics. (2017), 145. doi： 10. 1016/ j.ijleo. 2017. 07. 041

[9]Chai X, Gan Z,Chen Y, et al.A visually secure image encryption scheme based on compressive sensing. Signal Processing. (2017), 134: 35- 51. doi: 10.1016/ j. sigpro. (2016). 11. 016

[10] Song Lili, Yang Fan, Pan Guofeng. Arnold transform and Gray code transformation of the dual scrambling algorithm to study. computer applications and software, 2016, 33 (3): 304-307.

[11] riot,Zhang Zhenkai,Li Yuanjiang. Tetrolet transform and SVD combination of blind detection robust digital watermarking embedding strategy [J]. computer engineering and science. (2017) 39 (3): 492-499.

[12] Xie Guobo,Su Ben Hui. Digital image encryption algorithm based on Arnold hierarchical cyclic transformation. computer engineering and design, 2017, 38 (5): 1200-1204.

[13] Zhang Yonghong, Zhang Bo. Image encryption algorithm based on Logistic chaotic system . computer application research. (2015) 32 (6): 1770-1773.

[14] Wang Yaqing, Zhou Shangbo. Image encryption algorithm based on fractional Chen's chaotic system. computer applications, 2013, 33 (4): 1043-1046. doi: 10.3724/ SP. J. 1087. 2013. 01043

[15]Gong Lihua, Ceng Shaoyang, Zhou Nan run. Color image encryption algorithm based on spectral cutting and two-dimensional Arnold transform. computer application, 2012, 32 (9): 2599- 2602. doi: CNKI:SUN:JSJY.0.2012-09-059

[16] Li Chunhu, Luo Guangchun, Li Chunbao. Image encryption scheme based on skew tent chaos map and Arnold transform . computer application research in (2017).

[17] Li Shuquan, Fang Dong Li, LIAhu-quan, et al. A color image watermarking algorithm based on Amold transform. microelectronics and computer, 2017 (1): 53-57.

[18] Xiao Zhenjiu, Zhang Han, Chen Hong, et al. Zero watermarking for enhanced singular value decomposition and cellular neural network .Chinese Journal of image and graphics.(2017) 22 (3): 288- 296. doi: 10.11834/ jig. 20170302

[19]Wu G C , Baleanu D, Xie H P , et al. Chaos synchronization of fractional chaotic maps based on the stability condition. Physica A Statistical Mechanics & Its Applications. (2016) 460:374-383. doi: 10.1016/ j. physa. 2016. 05. 045

[20] Wu G C , Baleanu D . Discrete chaos in fractional delayed logistic maps. Nonlinear Dynamics. (2015), 80(4): 1697- 1703. doi: 10.1007/ s11071- 014- 1250- 3

[21] *T. Abdeljawad, S. Banerjee, G.C. Wu, Discrete tempered fractional calculus for new chaotic systems with short memory and image encryption, Optik, 203 (2020) 163698.

[22] *G.C. Wu, Z. G. Deng, D. Baleanu, D. Q. Zeng, New variable-order fractional chaotic systems for fast image encryption, Chaos, (2019)29 :083103.

[23] Saeed, S. T. , et al. "Exact Symmetric Solutions of MHD Casson Fluid Using Chemically Reactive Flow with Generalized Boundary Conditions." Energies 14(2021).

[24] Aneja, Madhu , and S. Sharma . "Numerical study of bioconvection flow of nanofluids using non-Fourier's heat flux and non-Fick's mass flux theory." International Journal of Modern Physics B (2020).

[25] Syed Tauseef Saeed,Muhammad BILAL Riaz.A fractional study of generalized Oldroyd-B fluid with ramped conditions via local & non-local kernels.Nonlinear Engineering 2021,10(1):177-186.DOI:10.1515/nleng-2021-0013

[26]Aziz Ur Rehman, Muhammad Bilal Riaz, Ali Akgül, Syed Tauseef Saeed, Dumitru Baleanu Heat and mass transport impact on MHD second-grade fluid: A comparative analysis of fractional operators.（2021）6.https://doi.org/10.1002/htj.22216

[27] Abdeljawad, Thabet , et al. "MHD Maxwell Fluid with Heat Transfer Analysis under Ramp Velocity and Ramp Temperature Subject to Non-Integer Differentiable Operators." Computer Modeling in Engineering & Sciences (2021).

 doi:10.20944/preprints202112.0269.v1

UTHORS' BACKGROUND

Your Name	Title[1]*	Research Field	E-mail
Chen Chao	Lecturer\PHD candidate	digital image processing	ch10503@126.com
Wu Bin	Doctor\professor	computer vision	wubin@swust.edu.cn
Zhang Hongying	Doctor\professor	computer vision	zhywyd@163.com