A New Method of Quantum Image Encryption Based on Arnold Transform and Hyperchaos System

Wei-Dong ZHU[a] and Meng-Zhen CUI[b,*]
Beijing Jiaotong University in Beijing, China
[a]wdzhu@bjtu.edu.cn, [b]16120360@bjtu.edu.cn
*Corresponding author

Keywords: Quantum image encryption, Arnold transform, Hyperchaos system.

Abstract. The traditional encryption technology mainly relies on computer or digital signal processor and other electronic devices to achieve, so the speed and cost were restricted. As a result, people began to study more secure and efficient quantum image encryption technology. In this paper, a new method of quantum image encryption based on Arnold transform and hyperchaotic system is proposed. The encryption process of this paper consists of two phases: scrambling encryption stage and gray scale encryption stage. In this paper, a quantum image encryption algorithm based on hyperchaotic system is adopted in the gray scale encryption stage. The hyperchaotic system is used to generate hyperchaotic sequences, which are used to control non-operation. Theoretical analysis and classical numerical simulation show that this new method of quantum image encryption based on Arnold transform and hyperchaotic system has good security and anti - attack.

Introduction

The image as a special information carrier is widely used, image encryption technology has become a hot topic of concern. The traditional encryption technology mainly relies on computer or digital signal processor and other electronic devices to achieve, so the speed and cost were restricted. As a result, people began to study more secure and efficient quantum image encryption technology. Quantum image encryption technology compared with the traditional encryption technology has a large capacity, high processing speed, high parallelism and other advantages[13]. Thus, it is becoming a popular international research direction in recent years. At present, many image encryption algorithms have been proposed and implemented. The international standard of the encryption algorithm not only apply to the part of the compression algorithm, but also can be applied to the displacement and scrambling. Cellular automata image encryption system meet the replacements and scrambling properties[11]. In order to reduce the correlation between pixels, Arnold transformation because of its good displacement characteristics are widely used in various kinds of image encryption algorithm. Guo proposed discrete random variation and Arnold transform of the image encryption algorithm in IHS color space[1]. However, these algorithms have a weakness, that is the number of iterations Arnold algorithm is very limited. In addition, many encryption algorithms based on chaotic systems have been proposed. Fridrich image encryption algorithm based on chaotic system was put forward for the first time, this algorithm can effectively achieve the cryptosystem confusion and diffusion, and has a good safety performance[2]. Wang and Guo use a series of pseudo random number generated by Logistic mapping and the pseudo random number of a two-dimensional array, by using the array replacement plaintext image left half pixel values, and then through the left half of the cipher image encryption right half clear image[4]. Tang proposed a good encryption algorithm: the clear image is divided into several overlapping image blocks, scrambling the image block. The initial scrambling image is Arnold transform by using chaotic mapping matrix of pseudo random number, the last of the corresponding portions of each image block and the matrix for XOR operation to get the final encrypted image[5]. Norouzi B etc presents a new image encryption scheme based on hyperchaos system, the scheme using two hyperchaos system generate pseudo random key to increased security and sensitivity of the key[3]. With the development of quantum computing, the classic image encryption also extends to the quantum field. Tajima et al.

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

proposed an algorithm for information encryption using the physical process of quantum chaos[6], Akhshani et al. proposed an image encryption method based on nonlinear equations of quantum chaotic system for the first time[7]. In 2013, Luo Yuling et al. proposed an adaptive image encryption scheme combined with scrambling and diffusion based on quantum logistic chaos and discrete wavelet transform. In 2014, Wang Xin et al. proposed a new quantum image encryption scheme based on quantum wavelet transform and double diffusion operation, in the scheme, the Logistic chaotic map is used to generate the encryption key. In 2016, Zhou proposed Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations, its general process is roughly to use a quantum image representation method to prepare the classical image into a quantum image firstly, and then use the chaotic system to generate the chaotic sequence as the stream cipher of image encryption, and then do XOR operation for the stream cipher and the quantum image to generate Image after encrypting. Quantum chaotic mapping is often used as a pseudo-random number generator to improve the security of the encryption algorithm because of its good random characteristics. Statistical analysis and information entropy testing have proved that quantum chaotic mapping has very good randomness and aperiodicity. The hyperchaotic system has more complex nonlinear dynamic properties than chaotic systems.

In this paper, a new method of quantum image encryption based on Arnold transform and hyperchaotic system is proposed. As a classic algorithm, Arnold transformation has its own unique advantages in many ways, but it has an obvious flaw that is cyclical. In order to take advantage of its advantages and avoid defects, image encryption is combined with the Chen hyperchaotic system. Hyperchaotic systems have excellent characteristics such as initial value sensitivity, state traversal, mixed and similar randomness[12]. The encryption process of this paper consists of two phases: scrambling encryption stage and gray scale encryption stage. In the scrambling stage, the size of all pixel values does not change, only the space positions of image pixel are confused. In this paper, the scrambling and encryption phase is realized by generalized Arnold transform. The grayscale encryption phase encrypts the image by changing the pixel values of the image. In this paper, a quantum image encryption algorithm based on hyperchaotic system is adopted in the gray scale encryption stage. The hyperchaotic system is used to generate hyperchaotic sequences, which are used to control non-operation. And then use Control the non-operation to achieve the XOR operation of quantum images, and then complete the quantum image encryption. Theoretical analysis and classical numerical simulation show that this new method of quantum image encryption based on Arnold transform and hyperchaotic system has good security and anti - attack.

The general structure of this paper:1. introduce the operation process of quantum image encryption based on generalized Arnold transform and hyperchaos system; 2. analyze and evaluate the experiment; 3. sum up the thesis of this paper.

Quantum Image Encryption Operations Based on Generalized Arnold Transform and Hyperchaos System

The quantum image encryption process proposed in this paper can be divided into two steps: (1) the location information of the image is upset by Arnold transform; (2) the gray information of the image is encrypted by Chen hyperchaos system. Thus, double encryption of the position and the gray value of the quantum image is realized.

Upsetting Operations

The quantum image representation method used in this paper is NEQR, and the expression of the image is:

$$\left|M\right\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|g(y,x)\right\rangle\left|yx\right\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{yx}^{i}\right\rangle\left|yx\right\rangle \tag{1}$$

The original plaintext image M is operated by the K times quantum generalized Arnold transform to obtain the quantum image, in which the horizontal and vertical position information are respectively represented by $A|\mathrm{x}\rangle$ and $A|\mathrm{y}\rangle$.

$$\begin{aligned} |Q_1\rangle = A(|M\rangle) &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle A(|yx\rangle) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle A(|y\rangle)A(|x\rangle) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|y^{'}x^{'}\rangle \end{aligned} \tag{2}$$

In formula,

$$\begin{cases} |x^{'}\rangle = A(|x\rangle) = |(x+ty) \bmod 2^n\rangle \\ |y^{'}\rangle = A(|y\rangle) = |[mx+(tm+1)y] \bmod 2^n\rangle \end{cases} \tag{3}$$

Among them, A represents the quantum generalized Arnold transform for $|M\rangle$, and $|Q_1\rangle$ represents the image after one time quantum generalized Arnold transform.

Encrypt Quantum Image Gray Information

We use hyperchaotic system to encryption the gray information of quantum image is to apply the XOR operation to the generated random sequences and gray value, so it is divided into the following three steps: the first step, transfer the four chaotic sequence into a sequence of integers range consistent with quantum image gray value; the second step, the corresponding key sequence is generated by the integer sequence of the transformation; the third step, the secret key sequence is combined with the gray value of the corresponding position to perform XOR operation to produce the final encrypted image.

Step1:

Converting the four hyperchaotic sequences into corresponding integer sequences, the process is as follows, where fix (x) represent four to five operations on the X.

$$\begin{aligned} x_i^* &= \mathrm{mod}(|(x_i - fix(x_i)\times 10^3)|,256) \\ y_i^* &= \mathrm{mod}(|(y_i - fix(y_i)\times 10^3)|,256) \\ z_i^* &= \mathrm{mod}(|(z_i - fix(z_i)\times 10^3)|,256) \\ h_i^* &= \mathrm{mod}(|(h_i - fix(h_i)\times 10^3)|,256) \end{aligned} \tag{4}$$

Step2:

In order to perform quantum XOR operation, a hyperchaotic sequence $K=\{k_1,k_2,\cdots,k_{2^{2n}}\}$ is constructed. If $h_i^* \bmod 3 = 0$,then $k_i = x_i^*$ is used to implement control non operation; if $h_i^* \bmod 3 = 1$, then $k_i = z_i^*$ is used to implement control non operation; if $h_i^* \bmod 3 = 2$, then $k_i = z_i^*$ is used to implement control non operation; Integers k_i can be represented in binary form $k_i = h_i^7 h_i^6 \cdots h_i^0$, in this $h_i^j \in \{0,1\}$, $i = 1,2,\cdots 2^{2n}$, $j = 0,1,\cdots 7$.

Step3:

The scrambled gray information of each position of the quantum image performs the XOR operation, using control gate to realize quantum XOR operation.

$\mathrm{B_{YX}}$ is used to implement XOR operations on specific locations of images.

$$
\begin{aligned}
B_{YX}(|Q\rangle) &= B_{YX}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{yx}^{i}\right\rangle|yx\rangle\right) \\
&= \frac{1}{2^n}B_{YX}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{yx}^{i}\right\rangle|yx\rangle+\bigotimes_{i=0}^{7}\left|C_{YX}^{i}\right\rangle|YX\rangle\right) \\
&= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{yx}^{i}\right\rangle|yx\rangle+U_{YX}\bigotimes_{i=0}^{7}\left|C_{YX}^{i}\right\rangle|YX\rangle\right) \\
&= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\ yx\neq YX}}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{yx}^{i}\right\rangle|yx\rangle+\bigotimes_{i=0}^{7}\left|C_{YX}^{i}\oplus h_{YX}^{i}\right\rangle|YX\rangle\right)
\end{aligned}
\tag{5}
$$

Then B_{YX} operations are used to realize 2^{2n} times XOR operations of the whole quantum image.

$$
\begin{aligned}
B(|Q\rangle) &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}B_{YX}(|Q\rangle) \\
&= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}U_{YX}\,|g(Y,X)\rangle|YX\rangle \\
&= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{7}\left|C_{YX}^{i}\oplus h_{YX}^{i}\right\rangle|YX\rangle \\
&= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle
\end{aligned}
\tag{6}
$$

Thus, the position information and the gray information of the quantum image are encrypted separately.

Performance Analysis

There are lots of kinds methods of performance made on Image encryption algorithm, which includes Histogram analysis method, correlation analysis method, Key space analysis methods information Entropy test method and operating speed test methods and so on. In this paper, we use the original image Peppers of which the pixel size is 512*512 as a test picture, as Fig. 1 (a). And now we will use three methods to analyze the encryption algorithm mentioned above, such as Histogram analysis method, correlation analysis and information Entropy test method. Because of the limited environment, we only use Computer simulations based on MATLAB for the numerical simulation test. According to the broad definition about Arnold transformation, the cycle depends on the size of images. Therefore, we offer the image with 512*512 PXs for the test mentioned above. Based on such pixel size, the cycle is T=384[14]. In the simulation, we set parameters as the fallowing formula, such as t=600, m=300 and k=45. The initial condition of hyper-chaotic is sought as $x_0 = 0.325, y_0 = -0,432, z_0 = 1.253, h_0 = 1$. And the cipher-image likes Fig. 1 (b), in which we can't get any useful information.

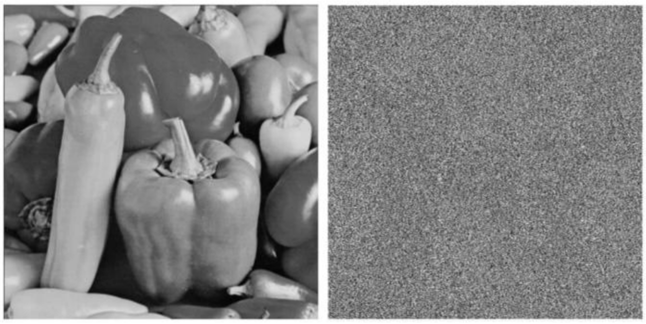

Fig. 1 (a)The plaintext image of peppers; (b)Ciphertext image

Histogram Analysis

The Fig. 2 shows the Peppers original image and the gray scale histogram (VGH) of the encrypted image. We can draw a conclusion from the distribution of the histogram that the VGH of the encrypted image has come very close to an ideal uniform distribution. As a result, the algorithm can protect the information in encrypted images' VGH from being stolen by illegal message receivers, which avoids the useful information being decoded effectively.

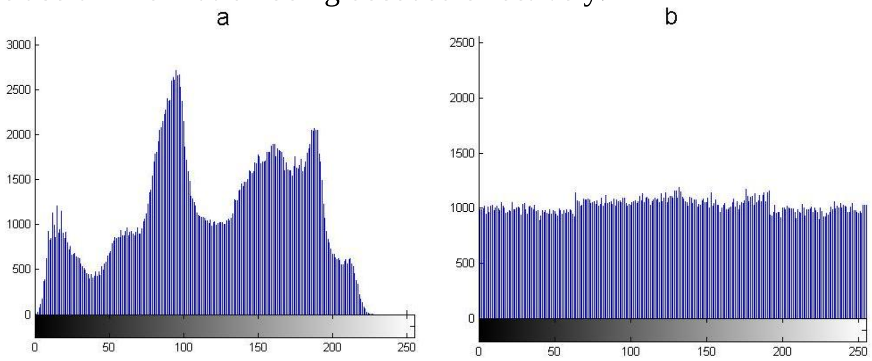

Fig. 2 (a)The plaintext histogram of peppers; (b)Ciphertext histogram

Correlation Analysis

The correlation between two adjacent pixels of the plain image is generally very close to 1, however, a valid encryption algorithm should ensure that the correlation between two adjacent pixels of the encrypted image is close to 0. In order to analyze and discuss the correlation between adjacent pixels of the encryption algorithm, respectively, this paper calculated the correlation coefficients of adjacent pixels in the horizontal, the vertical and diagonal directions of original image and encrypted image, the calculation results are shown in Table 1. Fig. 3, Fig. 4 and Fig. 5 show the distribution of correlation between adjacent pixels of the plaintext image Peppers and encrypted image in horizontal, vertical, diagonal direction. We can see that each pixel of plaintext image has a strong correlation in adjacent direction, but each pixel of plaintext image has a weak correlation in adjacent direction from the figure and table. This indicates that the useful information of encrypted image is well hidden, and the algorithm can weaken the correlation effect of adjacent pixels in plaintext image well. So attackers cannot attack by using the correlation.

Table 1 Correlation coefficient

Image	Plaintext horizontal direction	Plaintext vertical direction	Plaintext diagonal direction	Ciphertext horizontal direction	Ciphertext vertical direction	Ciphertext diagonal direction
Peppers	0.975271	0.970560	0.945909	0.014111	-0.138573	0.026059
Boat	0.942692	0.819416	0.828320	0.002370	-0.158463	0.004849
Plane	0.962217	0.968832	0.944390	0.021053	-0.115389	0.013149

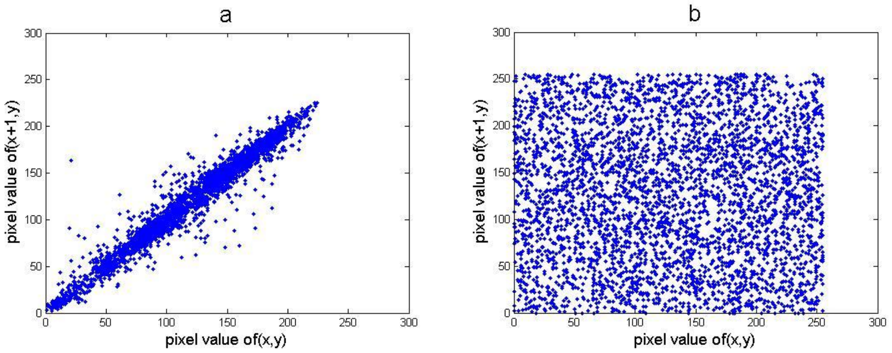

Fig. 3 (a)Horizontal direction relevance of the plaintext; (b)Horizontal direction relevance of the ciphertext

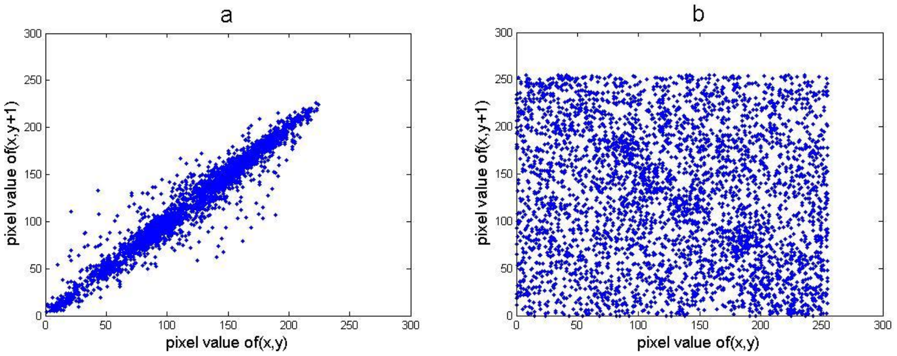

Fig. 4 (a)Vertical direction relevance of the plaintext; (b)Vertical direction relevance of the ciphertext

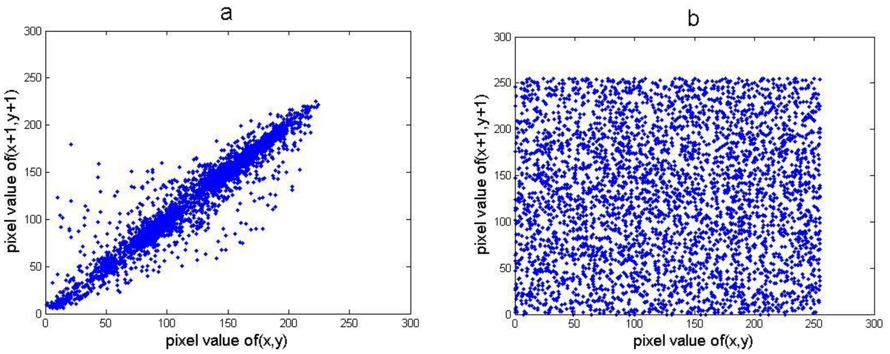

Fig. 5 (a)Diagonal direction relevance of the plaintext; (b)Diagonal direction relevance of the ciphertext

Entropy of Information Test

Entropy of information can be used to express the uncertainty of image information. If the gray value distribution of the image is more uniform, then the entropy value is greater. The entropy of the original image and the ciphertext image is given in Table 2. From the data in the table, we can know that the information entropy of the ciphertext image is very close to the ideal value. Therefore, the encryption algorithm can resist the information entropy attack and has very good security.

Table 2 Information entropy

Image	Information entropy of plaintext	Information entropy of ciphertext
Peppers	7.592451	7.983521
Boat	7.191370	7.897712
Plane	6.705888	7.864890

Conclusion

In this paper, we first use the quantum generalized Arnold transform to scramble the position information of the quantum image. The parameter of the Arnold transform coefficient matrix is used as the key to expand the key space, which makes the replacement effect more obvious. Then, we construct the XOR operation of quantum image, modify the pixel value of the image by using hyperchaotic chaotic sequence of Chen hyperchaotic system to achieve the effect of image scrambling, and eliminate the periodic effect caused by Arnold transform. The initial value of Chen hyperchaotic system as a key to the encryption algorithm has a very large key space, can resist strong attack. Experiments show that the encryption algorithm has a high security and strong anti-attack capability.

In a word, the fusion of classical and Quantum image encryption algorithm makes image encryption performance beyond the classical image encryption. And it has the security of classical information theory and the security of quantum information theory, increasing the anti-attack capacity and security of the encryption system.

References

[1] Guo Q, Liu Z, Liu S. Color image encryption by using Arnold and discrete fractional random transforms in IHS space[J]. Optics & Lasers in Engineering, 2010, 48(12):1174-1181.

[2] Fridrich J. Symmetric Ciphers Based On Two-Dimensional Chaotic Maps[J]. International Journal of Bifurcation & Chaos, 2011, 8(06):1259-1284.

[3] Norouzi B, Mirzakuchaki S. A fast color image encryption algorithm based on hyper-chaotic systems[J]. Nonlinear Dynamics, 2014, 78(2):995-1015.

[4] Wang X, Guo K. A new image alternate encryption algorithm based on chaotic map[J]. Nonlinear Dynamics, 2014, 76(4):1943-1950.

[5] Tang Z, Zhang X, Lan W. Efficient image encryption with block shuffling and chaotic map[J]. Multimedia Tools and Applications, 2015, 74(15):1-20.

[6] Tajima A, Tanaka A, Maeda W, et al. Practical Quantum Cryptosystem for Metro Area Applications[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2007, 13(4):1031-1038.

[7] Akhshani A, Akhavan A, Lim S C, et al. An image encryption scheme based on quantum logistic map[J]. Communications in Nonlinear Science & Numerical Simulation, 2012, 17(12):4653-4661.

[8] Luo Yuling, Du Minghui. Image Encryption Algorithm in Wavelet Domain Based on Quantum Logistic Mapping[J]. Journal of Huanan ligong University (NATURAL SCIENCE EDITION), 2013, 41(6):53-62.

[9] Wang S, Song X, Niu X. A Novel Encryption Algorithm for Quantum Images Based on Quantum Wavelet Transform and Diffusion[J]. 2014, 298:243-250.

[10] Gong L H, He X T, Cheng S, et al. Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations[J]. International Journal of Theoretical Physics, 2016, 55(7):3234-3250.

[11] Zhang Y, Lu K, Gao Y, et al. NEQR: a novel enhanced quantum representation of digital images[J]. Quantum Information Processing, 2013, 12(8):2833-2860.

[12] Hua Tianxiang. Quantum Image Encryption Algorithm Based on Transformation Theory[D]. Nanchang University, 2015.

[13] Zhu Congxu, Hu Yuping, Sun Kehui. A New Image Encryption Algorithm Based on Hyperchaotic System and Ciphertext Staggered Diffusion[J]. Journal of electronics and information, 2012, 34(7):1735-1743. [14] Peng J, Jin S, Liao X. A Novel Digital Image Encryption Algorithm

Based on Hyperchaos by Controlling Lorenz System[C]// International Conference on Natural Computation. IEEE, 2009:395-399.