

Quantum Image Encryption Based on Henon Mapping

Nan Jiang^{1,2,3,4} • Xuan Dong¹ · Hao Hu¹ · Zhuoxiao Ji¹ · Wenyin Zhang²

Received: 18 August 2018 / Accepted: 17 December 2018 / Published online: 3 January 2019 © Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Quantum image processing has great significance as a branch of quantum computing. This paper gives a quantum image encryption based on Henon mapping, which breaks away from the restriction of classical computers and does the work in quantum computers end to end, including the generation of the chaos sequence, the encryption and the decryption. The algorithm is based on the GQIR quantum image representation model and the two-dimensional Henon chaotic mapping. However, the decimal sequence generated by Henon mapping can not be directly applied to quantum computers. Hence, we reform the Henon mapping by binary shift. The quantum image is encrypted by being XORed with the quantum Henon mapping. Simulation experiments indicate that the encrypted image has good radomness and the pixel values are evenly distributed. Since the chaotic sequence itself is suitable for image encryption, coupled with its own quantum confidentiality, the encryption method of this paper is safe, convenient and reliable.

Keywords Quantum image processing · Quantum image encryption · Quantum computation · Chaos encryption · Henon mapping

1 Introduction

In everyday life, people transmit various images through networks. Sometimes, we want to encrypt them to protect important information carried by the images. In 1997, Fridrich proposed the chaos-based image encryption method for the first time [1]. This method can well complete the proliferation and confusion of the cryptosystem and has good security performance. Chaotic system is non-periodic, randomic, ergodic, deterministic and sensitive to initial conditions. Therefore, it is well suited for image encryption. The chaotic image

Nan Jiang jiangnan@bjut.edu.cn

¹ Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

² School of Information Science and Technology, Linyi University, Linyi 276000, China

³ Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

⁴ National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing 100124, China

encryption algorithm generates a pseudo-random sequence based on the nonlinear dynamics of the chaotic system, which is used to encrypt image data [2]. Due to the existence of quantum mechanical superposition, quantum computers are far more efficient than classical computers. Moreover, the non-cloned nature of quantum states ensures the security of quantum image encryption.

Quantum image encryption can be divided into three kinds: image encryption based on spatial domain, image encryption based on transform domain, and image encryption based on chaos. Researchers have developed image encryption based on spatial and transform domain in quantum computers. In 2012, Zhou et al. proposed a quantum image encryption algorithm based on quantum image geometric transformations [3]. In 2014, Song et al. raised quantum image encryption based on restricted geometric and color transformations [4]. In 2015, Zhou and Hua et al. introduced a quantum image encryption method based on Arnold transform [5]. Hua et al. proposed a quantum image encryption algorithm based on image correlation decomposition [6].

Besides, some researchers try to develop chaos based quantum image encryption algorithms. Ref. [7] noticed the advantanges of quantum chaos to encrypt classical images. In 2013, El-Latif et al. proposed a new approach to chaotic image encryption based on quantum chaotic system [8]. In 2014, Cao et al. proposed quantum chaotic image encryption with one time running key [9]. In 2015, Seyedzadeh et al. proposed a novel color image encryption algorithm based on spatial permutation and quantum chaotic map [10]. In 2016, Liang et al. gave a quantum image encryption algorithm based on generalized affine transformation and logistic mapping [11]. In the same year, Tan et al. proposed a quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform [12]. In 2017, Wang et al. proposed a quantum image encryption based on iterative framework of frequency-spatial domain transforms [13]. Li et al. proposed a quantum color image encryption based on multiple discrete chaotic systems [14]. In 2018, Zhou et al. proposed bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system [15]. Recently, Wang et al. gave a quantum image encryption algorithm based on quantum key image [16, 17]. Although they all have a good encryption effect, the encryption sequences are generated on classical computers, which make them still depend on classical computers.

In this paper, Henon mapping is used to encrypt a quantum image, and it is generated in a quantum computer, which breaks away from the restriction of classical computers and increases the security and convenience. Henon mapping is a two-dimensional chaos map and it has better randomness and security than one-dimensional chaos. However, the sequence obtained from Henon mapping has the problem of uneven distribution, which makes it cannot be directly applied to image encryption. Referring to the improvement of the Henon mapping on traditional computers in Ref. [18], we improve the sequence on quantum computers. On the basis of binary storage, each data is shifted left by 13 digits, and the obtained sequence is ideal. Through a series of analysis, it is found that the Henon-based image encryption on quantum computers is feasible, safe and reliable.

2 Related Works

2.1 Henon Mapping

The commonly used chaotic systems include one-dimensional Logistic maps [19], twodimensional Henon maps [20], and three-dimensional Lorenz maps [21].

Fig. 1 Quantum adder



One-dimensional Logistic mapping is too simple and easy to be cracked, and threedimensional Lorenz is too complex to be realized in quantum computers. Hence, we use two-dimensional Henon mapping to do quantum image encryption.

Henon mapping is defined as shown in (1) [20].

$$\begin{cases} x_{i+1} = y_i + 1 - ax_i^2 \\ y_{i+1} = bx_i \end{cases}$$
(1)

It can be seen that the Henon mapping is a chaotic map consisted by two variables x and y, where a and b are control parameters. The Henon mapping is more complicated than the one-dimensional mapping. Hence, the generated encrypted image is less easily cracked, which makes it suitable for image encryption algorithms.

2.2 GQIR Representation of Quantum Images

GQIR can represent quantum images of any size $H \times W$, which needs $\lceil \log_2 H \rceil + \lceil \log_2 W \rceil + q$ qubits, where q is the image color depth, $\lceil \log_2 H \rceil$ is the size of the Y-axis coordinate information, and $\lceil \log_2 W \rceil$ is the size of the X-axis coordinate information [22].

An $H \times W$ quantum image I can be expressed as

$$|I\rangle = \frac{1}{\sqrt{2}^{h+w}} \sum_{u=0}^{H-1} \sum_{v=0}^{W-1} \bigotimes_{i=0}^{q-1} |C_{UV}^{i}\rangle |UV\rangle |UV\rangle = |U\rangle |V\rangle = |u_{0}u_{1}\cdots u_{h-1}\rangle |v_{0}v_{1}\cdots v_{w-1}\rangle, u_{i}v_{i} \in \{0, 1\} |C_{UV}\rangle = |C_{UV}^{0}C_{UV}^{1}\cdots C_{UV}^{q-1}\rangle, C_{UV}^{i} \in \{0, 1\}$$
(2)

2.3 Quantum Adder and Quantum Multiplier

Our algorithm needs some quantum modules. Hence, we introduce them in this section.

A quantum adder is a quantum computation circuit that calculates the sum of the values stored in two quantum registers [23]. By assuming that the two quantum registers are a and b, the quantum adder performs the following function and is shown in Fig. 1.

$$|a,b\rangle \rightarrow |a,a+b\rangle$$

If the black bar in Fig. 1 is on the left side, its function becomes a subtractive device [23]. The subtractor performs the function and is shown in Fig. 2.

$$|a,b\rangle \rightarrow |a,a-b\rangle$$

Fig. 2 Quantum subtractor



In this paper, we also need an subtractor for output $|a-b, a-b\rangle$. Ref. [24] mentions how to get the output of two identical values. We call it as double-output adder (D-ADDER), which can be expressed in the following equation and is shown in Fig. 3.

$$|a,b\rangle \rightarrow |a-b,a-b\rangle$$

Saurabh Kotiyal et al. introduced the quantum multiplier [25]. The quantum multiplier is represented as the following equation and in Fig. 4.

$$|a, b, 0\rangle \rightarrow |a, b, a \times b\rangle$$

3 Quantum Image Encryption Algorithm Based on Henon Mapping

3.1 Encryption

Step 1. This step generates the Henon chaotic sequence in a quantum computer, which has the same size as the quantum image to be encrypted. By assuming the size of the original image is $2^n \times 2^n$, Eq. (1) is iterated $\frac{2^n \times 2^n}{2} + k$ times to get the quantum chaotic sequence, where k is a positive integer. Due to each iteration generates two numbers x and y, $\frac{2^n \times 2^n}{2}$ iteration will output $2^n \times 2^n$ numbers, which has the same size as the image. There are extra k times because the randomness of the beginning part of the Henon chaotic sequence is not good enough. Hence, we take the chaotic sequence from the k + 1 iteration. In general, $k = 2 \times 10^4$.

Fig. 3 Quantum double-subtractor



Fig. 4 Quantum multiplier



For each iteration, as shown in Fig. 5 and according to (1) $x_{i+1} = y_i + 1 - ax_i^2$, firstly, a D-ADDER is used to get two x_i , a MULER is used to get x_i^2 , and another MULER is used to get ax_i^2 . Then, an ADDER helps to get $y_i + 1$. At last, the second and the third D-ADDERs help to get three $y_i + 1 - ax_i^2$, i.e., three x_{i+1} . We call it as "First Part", which is used to generate x_{i+1} and whose inputs include x_i , a and y_i .

The "Second Part" module is for preparing Y sequence: $y_{i+1} = bx_i$ as shown in Fig. 6, which uses one MULER model and one D-ADDER to get two bx_i , i.e., y_{i+1} .

The whole circuit for Henon mapping is shown in Fig. 7. All the x_i and y_i are stored in 21-qubit binary storages. This figure also tells us the reason that "First Part" outputs three x_{i+1} : two are used to generate the quantum Henon sequence and the other is reserved as the Henon sequence, i.e., the reserved one is the output of this step. The reason that "Second Part" outputs two y_{i+1} is the same.

Step 2. The chaotic sequence $\{x_{k+1}, y_{k+1}, x_{k+2}, y_{k+2}, \dots, x_{k+2^{2n-1}}, y_{k+2^{2n-1}}\}$ obtained in Step 1 can not be directly used because it it not uniformly distributed. Hence, the idea in Ref. [18] is used to improve the sequence. In decimal system, $x_i = 10^r x_i - round(10^r x_i)$ is used to map x_i to the range [-0.5, 0.5]. In general, r = 4. In this paper, 2^{13} is used to replace 10^4 because 2^{13} is the closest value to 10^4 in



Fig. 5 $x_{i+1} = y_i + 1 - ax_i^2$ quantum circuit diagram



Fig. 6 $y_{i+1} = bx_i$ quantum circuit diagram

all 2^i and multiplying 2^{13} is easy to realize in quantum binary circuit: omitting the most significant 13 qubits and only reserving the least significant 8 qubits.

Step 3. As Fig. 8 shows, the image is XORed with the chaotic sequence $\{x_{k+1}, y_{k+1}, x_{k+2}, y_{k+2}, \dots, x_{k+2^{2n-1}}, y_{k+2^{2n-1}}\}$ pixel by pixel. For the first pixel $|C_{00}\rangle$, a (2n+1)-CNOT gate (a CNOT gate with 2n+1 control qubits) is used to do XOR, where 2n qubits (the location information $|UV\rangle$ of the image) are 0-control to ensure that pixel (0, 0) is selected and 1 qubit are 1-control to achieve XOR. For the second pixel, $|UV\rangle = |00 \cdots 001\rangle$ to ensure that pixel (0, 1) is selected. Similarly, the control qubits of the last (2n + 1)-CNOT gate are all 1-control to ensure that the last pixel $(2^n - 1, 2^n - 1)$ is selected.



Fig. 7 The quantum circuit of Henon mapping process



Fig. 8 Comparators combine XOR operation circuits

3.2 Decryption

The decryption circuit is exactly the same as the encryption circuit. Firstly, the same Henon chaotic sequence as used in encryption is generated by the circuit shown in Fig. 7. Then, as Fig. 8 shows, the encrypted image is XORed with the chaotic sequence to recover the plain image, because $a \oplus b \oplus b = a$, where $a, b \in \{0, 1\}$ and \oplus is the XOR operation.

4 Analysis of the Algorithm

4.1 Visual Effects

We simulate the above steps through Matlab, with initial value $x_0 = 0.2$, $y_0 = 0.1$, a = 1.4, b = 0.3. The experimental results are shown in Fig. 9. It can be seen obviously that the encrypted images seem meaningless, and we can't see any information about the original images from them. That is to say, our scheme is good enough to protect the original image visually.

4.2 Statistical Analysis

The ability to resist statistical analysis attacks is an important criterion for judging the advantages and disadvantages of image encryption algorithms. Here, histogram and correlation of adjacent pixels are used.

4.2.1 Histogram

Histogram analysis is performed on the original grayscale image and the encrypted image, the result is shown in Fig. 10. In this figure, "Lena" and "Cameraman" are two examples. (a1) and (b1) are the histograms of the original images, and (a2) and (b2) are the histograms of the encrypted images. Figure 10 tells us that the histogram of the original grayscale image has a large fluctuation and uneven distribution of pixels, while the encrypted image is more evenly distributed. That is to say, after encryption, the numbers of all the 256 colors



are almost the same, which makes the entropy approaches the maximum value, i.e., the difficulty of cracking is almost the greatest.

4.2.2 Correlation of Adjacent Pixels

Since a natural image is an information source with memory, it has a high correlation between adjacent pixels. For example, if the current pixel is red, its 8 adjacent pixels are usually red, with very very little difference from the current pixel value. In a Cartesian system, if let I(u, v) as the X-coordinate and I(u, v+1) as the Y-coordinate, all the pixel-pairs (i.e., a point in the Cartesian system) (I(u, v), I(u, v+1)) will appear in the vicinity of the 45-degree slash, because $I(u, v) \approx I(u, v+1)$. Figure 11(c1) and (d1) take "Peppers" and "Boats" as examples to show their adjacent pixel correlation. All the dots roughly compose a 45-degree slash.

However, a good encrypted image is similar to a random number whose adjacent elements have no correlation. Hence, in the (I(u, v), I(u, v+1))-coordinate, all dots should be



Fig. 10 Original image histogram and encrypted image histogram for Lena and Cameraman

evenly distributed throughout the space. Figure 11(c2) and (d2) give the adjacent pixel correlation of the encrypted image. All the dots are actually evenly spread across the space. That is to say, the encrypted image has no correlation, which indicates that Henon encryption is a good image encryption algorithm.



Fig. 11 Adjacent pixel correlation analysis of original image and encrypted image

The correlation coefficients of the adjacent pixels is another index for security. The definition of correlation coefficient R is shown in the following equation.

$$R_{\alpha\beta} = \frac{cov(\alpha,\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}}$$
(3)

D Springer

Image	Correlation coefficient			
	Horizontal	Vertical	Diagonal	
Original Lena	0.9812	0.9673	0.9448	
Original Cameraman	0.9578	0.9369	0.9106	
Original Peppers	0.9822	0.9730	0.9541	
Original Boats	0.9551	0.8269	0.8093	

 Table 1
 Correlation coefficients of adjacent pixels about original images

where, $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_L)$ and $\beta = (\beta_1, \beta_2, \cdots, \beta_L)$ are two sequences of length L, and

$$E(\alpha) = \frac{1}{L} \sum_{i=1}^{L} \alpha_i$$

$$D(\alpha) = \frac{1}{L} \sum_{i=1}^{L} (\alpha_i - E(\alpha))^2$$

$$cov(\alpha, \beta) = \frac{1}{L} \sum_{i=1}^{L} (\alpha_i - E(\alpha))(\beta_i - E(\beta))$$
(4)

That is to say, $E(\alpha)$, $D(\alpha)$ and $cov(\alpha, \beta)$ are mean, variance and covariance respectively.

If $\alpha = \{I(u, v)\}$ and $\beta = \{I(u, v + 1)\}, \beta = \{I(u + 1, v)\}$ or $\beta = \{I(u + 1, v + 1)\}, R_{\alpha\beta}$ is defined as the correlation coefficient of an image in horizontal, vertical or diagonal directions respectively. Tables 1 and 2 give the experimental data. It is obviously that the correlation coefficients of original images is high (near 1 which is the biggest value), and the correlation coefficients of encrypted images is almost 0.

4.3 Key Sensitivity Test

The results of the cryptographic key sensitivity test are shown in Fig. 12. In the figure, (a) is the original image; (b) is the decrypted image with an encryption key of $x_0 = 0.2$, $y_0 = 0.1$, a = 1.4, b = 0.3; (c) is the decrypted image with an encrypted key of $x_0 = 0.2 + 1 \times 10^{-15}$, $y_0 = 0.1$, a = 1.4, b = 0.3; (d) is the decrypted image with an encrypted key of $x_0 = 0.2 + 1 \times 10^{-15}$, $y_0 = 0.1 + 1 \times 10^{-15}$, a = 1.4, b = 0.3; (e) is the decrypted image with an encrypted key of $x_0 = 0.2$, $y_0 = 0.2$, $y_0 = 0.1$, $a = 1.4 + 1 \times 10^{-15}$, b = 0.3; and (f) is the decrypted image with an encrypted key of the encrypted key of $x_0 = 0.2$, $y_0 = 0.1$, $a = 1.4 + 1 \times 10^{-15}$, b = 0.3; and (f) is the decrypted image with an encrypted key of the encryption key and decryption key sensitivity test show that when the encryption key is slightly changed in the range of less than 10^{-15} , the decrypted image changes obviously. The decryption key in the same range of small changes will lead to the decryption failure. Therefore, this algorithm is sensitive to the key.

Image	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Encrypted Lena	-0.0069	0.0070	-0.0014
Encrypted Cameraman	-0.0093	-0.0090	0.0015
Encrypted Peppers	-0.0096	-0.0079	0.0053
Encrypted Boats	0.0019	-0.0036	0.0077

 Table 2
 Correlation coefficients of adjacent pixels about encrypted images

Fig. 12 Key sensitivity



5 Conclusion

This paper gives a quantum image encryption algorithm based on quantum Henon mapping. The main contribution is that it generates the chaos sequence in quantum computers, which is the biggest difference from previous works and breaks away from the restriction of classical computers. Experiments show that Henon map can encrypt the image on quantum computers well. The algorithm has strong key sensitivity and good statistical properties, and has low correlation of encrypted image pixels and uniform pixel value. Hence, quantum image encryption based on Henon mapping is secure.

The next step is to explore a better way to improve the Henon mapping algorithm, so that it can run more efficiently and safely on the quantum computer.

Acknowledgments This work is supported by the National Natural Science Foundation of China under Grants No. 61502016 and 61771230, the Joint Open Fund of Information Engineering Team in Intelligent Logistics under Grants No. LDXX2017KF152, and Shandong Provincial Key Research and Development Program under Grants No. 2017CXGC0701.

References

- 1. Fridrich, J.: Image encryption based on chaotic maps. IEEE Int. Conf. Syst. 2, 1105–1110 (1997)
- Luo, Y.L., Du, M.H.: Image encryption algorithm based on quantum logistic map in wavelet domain. J. South China Univ. Technol. (Nat. Sci. Edn.) 41(6), 53–62 (2013)
- Zhou, R.G., Wu, Q., Zhang, M.Q., Shen, C.Y.: A quantum image encryption algorithm based on quantum image geometric transformations. Int. J. Theor. Phys. 52(6), 480–487 (2012)

- Song, X.H., Wang, S., El-Latif, A.A.A., Niu, X.M.: Quantum image encryption based on restricted geometric and color transformations. Quantum Inf. Process 13(8), 1765–1787 (2014)
- Zhou, N.R., Hua, T.X., Gong, L.H., Pei, D.J., Liao, Q.H.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quant. Inf. Process. 14(4), 1193–1213 (2015)
- Hua, T., Chen, J., Pei, D., Zhang, W., Zhou, N.: Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theor. Phys. 54(2), 526–537 (2015)
- Zheng, F., Tian, X.J., Fan, W.H., Li, X.Y., Gao, B.: Image encryption based on Henon map. J. Beijing Univ. Posts Telecommun. 31(1), 66–70 (2008)
- El-Latif, A.A.A., Li, L., Wang, N., Han, Q., Niu, X.: A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process. 93(11), 2986–3000 (2013)
- Cao, G., Zhou, J., Zhang, Y.: Quantum chaotic image encryption with one time running key. Int. J. Secur. Appl. 8(4), 77–88 (2014)
- Seyedzadeh, S.M., Norouzi, B., Mosavi, M.R., Mirzakuchaki, S.: A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlin. Dyn. 81(1–2), 511–529 (2015)
- Liang, H.R., Tao, X.Y., Zhou, N.R.: Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf. Process 15(7), 2701–2724 (2016)
- Tan, R.C., Lei, T., Zhao, Q.M., Gong, L.H., Zhou, Z.H.: Quantum color image encryption algorithm based on a hyper-chaotic system and quantum fourier transform. Int. J. Theor. Phys. 55(12), 1–17 (2016)
- Wang, H., Wang, J., Geng, Y.C., Song, Y., Liu, J.Q.: Quantum image encryption based on iterative framework of frequency-spatial domain transforms. Int. J. Theor. Phys. 56(8), 1–21 (2017)
- Li, L., Abd-El-Atty, B., El-Latif, A.A.A., Ghoneim, A.: Quantum color image encryption based on multiple discrete chaotic systems. IEEE Comput. Sci. Inf. Sys., 555–559 (2017)
- Zhou, N., Chen, W., Yan, X., Wang, Y.: Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf. Process 17(6), 137 (2018)
- Wang, J., Geng, Y.C., Han, L., Liu, J.Q.: Quantum image encryption algorithm based on quantum key image. International Journal of Theoretical Physics, published online (2018)
- Wang, J., Wang, H., Song, Y.: Quantum endpoint detection based on QRDA. Int. J. Theor. Phys. 56(10), 3257–3270 (2017)
- Chen, X.M., Zhou, P.: Tracking control and synchronization for two-dimension discrete chaotic systems. J. Chin. Univ. Posts Telecommun. 9(3), 7–10 (2002)
- Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic Logistic map. Image Vis. Comput. 24(9), 926–934 (2006)
- Henon, M.: A two-dimensional mapping with a strange attractor. Commun. Math. Phys. 50(1), 69–77 (1976)
- Al-Hazaimeh, O.M., Al-Jamal, M.F., Alhindawi, N., Omari, A.: Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. Neural Comput. Appl., 1–11 (2017)
- Jiang, N., Wang, J., Mu, Y.: Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. Kluwer Acad. Publ. 14(11), 1–26 (2015)
- Vedral, V.V., Barenco, A., Ekert, A.: Quantum networks for elementary arithmetic operations. Phys. Rev. A 54(1), 147 (1995)
- Lu, X.W., Jiang, N., Hu, H., Ji, Z.X.: Quantum adder for superposition states. Int. J. Theor. Phys. 57(9), 2575–2584 (2018)
- Kotiyal, S., Thapliyal, H., Ranganathan, N.: Circuit for reversible quantum multiplier based on binary tree optimizing ancilla and garbage bits. In: IEEE International Conference on VLSI Design and 2014 International Conference on Embedded Systems, pp. 545–550 (2014)