CCF Transactions on High Performance Computing (2020) 2:228–253
https://doi.org/10.1007/s42514-020-00043-8

REGULAR PAPER

Quantum image encryption algorithm based on generalized Arnold transform and Logistic map

Wen-Wen Hu[1,2] · Ri-Gui Zhou[1,2] · SheXiang Jiang[3,1,2] · XingAo Liu[1,2] · Jia Luo[1,2]

Received: 30 December 2019 / Accepted: 16 July 2020 / Published online: 4 August 2020

Abstract
In the era of big data, image security and real-time processing become more and more important and increasingly difficult to satisfy. To improve the security and processing efficiency of image encryption algorithm, an enhanced quantum scheme is proposed for generalized novel enhanced quantum image representation. The proposed quantum encryption scheme mainly consists of two-stage operation in order, i.e., twice scrambling based generalized Arnold transform and pixel encryption based on the quantum key image (which are generated and prepared based on Logistic map). In the first stage, generalized Arnold transform are employed to simultaneously disturb the coordinate information and pixel gray value of quantum plain image. Following that, the scrambled image is further encrypted into a quantum cipher image based on quantum key image, which is divided into three sub-processes in detail, i.e., CNOT operations, bit-plane scrambling and controlled perfect shuffle permutations are executed orderly. The quantum image decryption process can be easily implemented in a reverse way. The complete quantum circuit implementation for above two stages operation is constructed and analyzed in terms of quantum cost and time complexity. Compared to classical image processing algorithm, the investigated quantum encryption algorithm demonstrates an exponential speedup with computational cost of O(n) for a $2^n \times 2^n$ quantum grayscale or color images. The proposed scheme is simulated and verified on a classical computer with MATLAB environments, i.e., not in a real quantum version that not considers the effects of quantum noise. Experimental results and numerical analysis indicate that the presented quantum algorithm has good visual effects and high security.

Keywords Quantum computers · Image encryption/decryption · Generalized arnold transform · Logistic map · Computational complexity

1 Introduction

Feynman R.P. first proposed the concept of simulating physics with computers, i.e., quantum computers (Feynman 1982). The information is stored in quantum systems and regarded as quantum bits (qubits) (Stajic 2013). Due to the inherent properties of quantum mechanics such as coherence, entanglement, and superposition of qubits, quantum information processing (QIP) is deemed to precede its classical counterparts in aspects of information storage, parallel computing and security (Michael and Isaac 2000). Although a real physical quantum computer has not been realized yet, it seems very necessary to develop quantum image processing tasks on account of that a quantum computer will inevitably need images displaying and processing ability. With the rapid development of QIP in recent years, classical image processing tasks are naturally extended to quantum scenarios named as quantum image processing (QImP). QImP is an emerging

This work is supported by the National Key R&D Plan under Grant No. 2018YFC1200200 and 2018YFC1200205.

✉ Ri-Gui Zhou
rgzhou@shmtu.edu.cn

Wen-Wen Hu
vienvinhu@gmail.com

SheXiang Jiang
sxjiang8888@163.com

XingAo Liu
liuxingao@stu.shmtu.edu.cn

Jia Luo
luojia@stu.shmtu.edu.cn

[1] College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China

[2] Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai 201306, China

[3] School of Computer Science and Engineering, Anhui University of Science & Technology, Huainan 232001, Anhui, China

sub-discipline that focuses on extending conventional image processing tasks and operations to the quantum computing framework (Iliyasu 2013; Yan et al. 2016, 2017). Compared to image processing algorithm implemented within classical computers in a conventional way, an efficient quantum image encryption algorithm based on the principle of quantum mechanics are assumed to improve the computational cost greatly, and can guarantee high security in theoretical. At present, the development of QImP can be classified into two aspects: quantum image representation and quantum image processing algorithm.

Quantum image representation encodes digital images within quantum computers. Many representation models of quantum images are investigated. Qubit Lattice is deemed as the first quantum image representation model (Venegas-Andraca 2003), which stores a $2^n \times 2^n$ color image in quantum systems with 2^{2n} qubits. To reduce the number of qubits used for encoding the quantum images, the flexible representation of quantum images (FRQI) proposed in (Li et al. 2018) stores a $2^n \times 2^n$ grayscale image with $2n+1$ qubits, which stores pixel's coordinate information into $2n$-qubit computational basis states and encodes the pixel's color information into a single qubit via angle encoding. For the convenience of color processing, the novel enhanced quantum representation (NEQR) of digital images (Zhang et al. 2013a) improves the FRQI model, which utilizes q-qubit computational basis state to store pixel's gray value ranged $[0, 2^q - 1]$. Next, the flexible quantum representation for gray-level images (FQRGI) was proposed by (Yang et al. 2014) that encode pixel's gray-level information within single qubit phases. A normal arbitrary quantum superposition state (NAQSS) was proposed by (Li et al. 2014) to store a k-dimensional color digital image using amplitudes of computational basis state. Inspired by NEQR model, some quantum image representation models use computational basis states to store pixel's gray value information were proposed, such as quantum log-polar image (QUALPI) (Zhang et al. 2013b) and novel quantum representation of color digital images (NCQI) (Sang et al. 2017). To further improve the storage performance, quantum image representation models based on bit-plane was also proposed in (Li et al. 2018; Wang et al., 2019; Li et al. 2019). Quantum image representation based on bit-planes (BRQI) presented in (Li et al. 2018) uses $(n+4)$ and $(n+6)$ qubits to store a grayscale or RGB color image of 2^n pixels, respectively. The quantum representation model of color digital images (QRCI) in (Wang et al. 2018) stores a $2^n \times 2^n$ color image with $2n+6$ qubits. The generalized model of NEQR (GNEQR) presented in (Li et al. 2019) uses $2n+10$ qubits to encode a $2^n \times 2^n$ RGB color image. Based on the coding method of pixel information, quantum image representation models described above can be classified into three categories: the first encodes pixel information via amplitude of qubit that includes Qubit Lattice and FRQI (Venegas-Andraca 2003; Li et al. 2018); the second utilizes the phase of qubit encoding pixel information that contains FQRGI and NAQSS (Yang et al. 2014; Li et al. 2014); the third using the basis states of qubits stores the pixel information, which includes NEQR, QUALPI, NCQI, BRQI, QRCI and GNEQR (Zhang et al. 2013a; Zhang et al. 2013b; Sang et al. 2017; Li et al. 2018; Wang et al., 2019; Li et al. 2019).

Image encryption aims at providing information secrecy in public environment through disturbing an image into meaningless form using different methods. Up to now, quantum image encryption has gained researchers' considerable interest and mainly classified into following two classes: (1) image encryption in spatial domain based on quantum transformations; (2) image encryption based on chaos theory. In first category, a series of quantum encryption algorithms were investigated, such as quantum image scrambling based on Arnold, Fibonacci and Hilbert transforms (Jiang et al. 2014a, b; Jiang and Wang 2014), quantum image encrypted based on quantum Fourier transform and double phase encoding (Yang et al. 2014; Li et al. 2018a, b, c), quantum image encrypted based on generalized Arnold transform and double random-phase encoding (Zhou et al. 2015), quantum image encrypted based on block geometric transformation and bit-plane scrambling (Li et al. 2019). In second category, Liang et al. investigated quantum image encryption based on generalized affine transform and Logistic map (Liang et al. 2016). Tan et al. proposed a quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform (Tan et al. 2016). Ran et al. proposed the quantum color image encryption based on coupled hyper-chaotic Lorenz system (Ran et al. 2018). Subsequently, more quantum image encryption algorithms based on chaos theory were also reported in (Li et al. 2017; Zhou et al. 2018; Jiang et al. 2019).

However, above-mentioned quantum transformation based image encryption scheme only disturbing the coordinate information have several disadvantages. Such as the histogram graphs are unchanged, and the quantum transformations need to perform many times to obtain a better encryption effect. On the other hand, chaos theory based quantum image encryption algorithms described above are similar to the "one-time pad" encryption, which involves high complexity in processing the pixel step-by-step according to the specific key stream. Furthermore, the former chaos-based quantum image encryption literatures also not provide the intact quantum implementation circuit.

To conquer the disadvantage of quantum transformation based quantum image encryption algorithms and improve the computational efficiency of chaos theory based quantum image encryption algorithms, an enhanced quantum image encryption scheme that combines generalized Arnold transform and Logistic map technologies are investigated. The main contributions of our work can be stated as: (1) twice scrambling based on generalized Arnold transform are implemented to simultaneously encrypt the image coordinate information and pixel gray value; (2) the complete quantum circuit implementation for encrypting the image information based on quantum key image (generated via Logistic map) are constructed and illustrated, which can process all image pixel's information in parallel. On the basis of computational complexity and experimental result analysis demonstrated in latter, it proves that our investigated quantum encryption scheme has lower complexity and high security.

The rest of this paper is organized as follows: In Sect. 2, we provide the basic knowledges needed for the proposed algorithm, including quantum qubits and gates, NEQR and GNEQR models, twice scrambling based on generalized Arnold transform, Logistic map and some quantum circuit modules. Section 3 describes the proposed quantum encryption and decryption algorithms in detailed. Section 4 analyses the quantum cost and time complexity of the quantum implementation circuits, and comparisons with related references in terms of quantum cost. Experimental results and numerical analyses are demonstrated in Sect. 5. Finally, the conclusion works are stated in Sect. 6.

2 Preliminaries

2.1 Quantum bits and gates

2.1.1 Quantum bits

The quantum bit (qubit) is the elementary memory unit in a quantum computer. Quantum information can be stored, manipulated and measured via qubits. The state of single qubit can be mathematically described by a unit vector in two-dimensional Hilbert space. One useful picture in thinking about single qubit is the Bloch sphere as shown in Fig. 1 (Michael and Isaac 2000). A single qubit $|\psi\rangle$ can be expressed as:

$$\begin{aligned}|\psi\rangle &= \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \\ &= \alpha|0\rangle + \beta|1\rangle,\end{aligned} \tag{1}$$

where $\theta \in [0,\ \pi]$, $\varphi \in [0,\ 2\pi]$, and $|\alpha|^2 + |\beta|^2 = 1$ subjects to the normalization condition.

The qubit states $|0\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$ and $|1\rangle = \begin{bmatrix} 0 & 1 \end{bmatrix}^T$ are called as the computational basis state spanning H^2 in 2-D Hilbert space. The tensor product, denoted by $\otimes$, is utilized to put the small vector spaces together forming a larger vector space in Hilbert space. Let A be a $n \times n$ matrix and B be a $m \times m$ matrix, then the tensor product A $\otimes$ B is a $nm \times nm$ block matrix defined as:

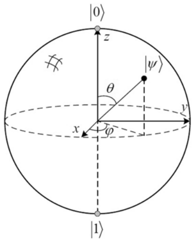


Fig. 1 Bloch sphere representation of a qubit

$$A \otimes B = \begin{bmatrix} A_{0,0}B & \cdots & A_{0,n-1}B \\ \vdots & \ddots & \vdots \\ A_{n-1,0}B & \cdots & A_{n-1,n-1}B \end{bmatrix}. \tag{2}$$

Suppose that $|i\rangle$ is the computational basis state in a $2^n\!-\!D$ Hilbert space, where the state $|i\rangle$ $(i = 0,\ 1,\ 2,\ \cdots,\ 2^n - 1)$ consists of the tensor products of the n computational basis states defined as:

$$|i\rangle = |i_{n-1}\rangle \otimes |i_{n-2}\rangle \otimes \cdots \otimes |i_1\rangle \otimes |i_0\rangle = |i_{n-1}i_{n-2}\cdots i_1 i_0\rangle, \tag{3}$$

where $i = \sum_{j=0}^{n-1} i_j \times 2^j, i_0,\ i_1,\ \cdots,\ i_{n-1}\ \in \{0,\ 1\}$. Thus, the quantum system of *n-qubit* can be described as a superposition state of 2^n quantum computational basis states:

$$|\psi\rangle = \sum_{k=0}^{n-1} a_k|k\rangle,\ k = k_{n-1}k_{n-2}\cdots k_1k_0,\ k_i \in \{0,\ 1\}, \tag{4}$$

and also satisfying the normalization condition $\sum\limits_{k=0}^{n-1} |a_k|^2 = 1$.

2.1.2 Quantum gates

Quantum gates are the necessary elements in constructing the quantum circuit. Some basic quantum gates and their corresponding matrices are demonstrated in Fig. 2.

Quantum Identity (I_2) gate denotes the quantum circuit line of single qubit. Similarly, $\left(I_2\right)^{\otimes n} = I_{2^n}$ denotes the quantum circuit line of n qubits.

Quantum NOT (also denoted as X) gate is similar to classical NOT operation, expressed as $X|a\rangle = |\overline{a}\rangle, a \in \{0, 1\}$, $\overline{a} = 1 - a$.

Quantum Hadamard (H) gate operated on single qubit $|0\rangle$ and $|1\rangle$ can transform the quantum state into an equal superposition state, i.e., $H(|0\rangle) = 1\big/\sqrt{2}(|0\rangle + |1\rangle)$, $H(|1\rangle) = 1\big/\sqrt{2}(|0\rangle - |1\rangle)$.

Quantum Controlled-NOT (CNOT) gate is usually used to realize the similar function of the classical XOR operation, which has two input qubits: control qubit and target qubit. It has two different forms *1-CNOT* and *0-CNOT*, which mean the control qubit in state of $|1\rangle$ and $|0\rangle$, respectively. Thus $1\!-\!CNOT(|a, b\rangle) = |a, a \oplus b\rangle$ and $0\!-\!CNOT(|a, b\rangle) = \left|a, \overline{a} \oplus b\right\rangle$.

The Swap gate is used to interchange the two qubit state, i.e., $Swap(|a, b\rangle) = |b, a\rangle$, and it can be decomposed into three 1-CNOT gates.

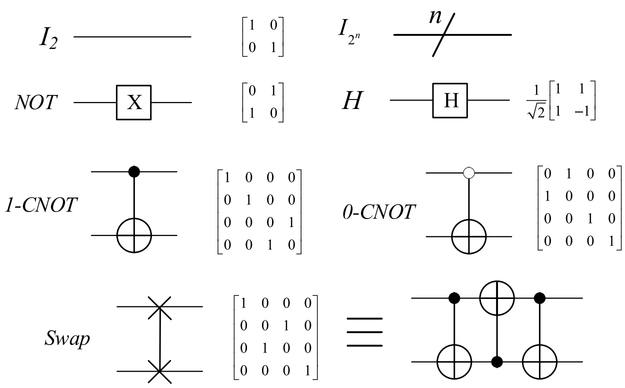

I_2
$\begin{bmatrix}1&0\\0&1\end{bmatrix}$
I_{2^n}
n
NOT
X
$\begin{bmatrix}0&1\\1&0\end{bmatrix}$
H
H
$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$
1-CNOT
$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
0-CNOT
$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$
Swap
$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$
≡

Fig. 2 Notations for some basic quantum gates with their corresponding matrices expression

2.2 NEQR and GNEQR

Quantum image representation model NEQR (Zhang et al. 2013a, b) uses two entangled qubit sequences to encode the whole image information into a normalized superposition state. For a $2^n \times 2^n$ quantum image with grayscale ranged $[0, 2^q - 1]$, the representative expression is expressed as:

$$|I\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|I_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|I_{YX}^{K}\right\rangle|Y\rangle|X\rangle, \tag{5}$$

where the binary sequence $I_{YX} = I_{YX}^{0}I_{YX}^{1}\cdots I_{YX}^{q-2}I_{YX}^{q-1}$ encodes the pixel's gray value in corresponding position (Y, X). $Y = y_{n-1}\cdots y_1y_0$ and $X = x_{n-1}\cdots x_1x_0$ denote the pixel's location information in vertical and horizontal directions, respectively.

When $q=8$, $|I\rangle$ represents a grayscale image. As an example, Fig. 3 gives a 2×2 NEQR grayscale image, its quantum circuit line, and the representative expression.

A RGB color image can be decomposed into three channels of Red, Green, Blue, and each channel is a grayscale image defined as:

$$|I_R\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|R_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|R_{YX}^{K}\right\rangle|Y\rangle|X\rangle,$$
$$|I_G\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|G_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|G_{YX}^{K}\right\rangle|Y\rangle|X\rangle,$$
$$|I_B\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|B_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|B_{YX}^{K}\right\rangle|Y\rangle|X\rangle, \tag{6}$$

where $|I_R\rangle$, $|I_G\rangle$, $|I_B\rangle$ encode the grayscale image in channels of Red, Green, and Blue, respectively.

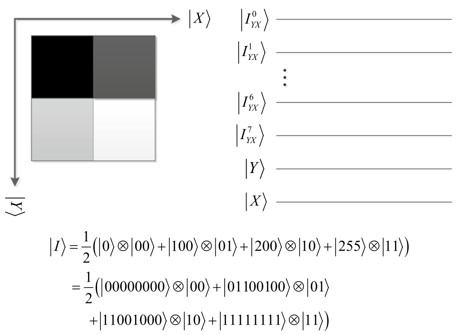

$|X\rangle$
$|Y\rangle$
$|I_{YX}^{0}\rangle$
$|I_{YX}^{1}\rangle$
⋮
$|I_{YX}^{6}\rangle$
$|I_{YX}^{7}\rangle$
$|Y\rangle$
$|X\rangle$
$|I\rangle = \frac{1}{2}(|0\rangle\otimes|00\rangle + |100\rangle\otimes|01\rangle + |200\rangle\otimes|10\rangle + |255\rangle\otimes|11\rangle)$
$= \frac{1}{2}(|00000000\rangle\otimes|00\rangle + |01100100\rangle\otimes|01\rangle$
$+ |11001000\rangle\otimes|10\rangle + |11111111\rangle\otimes|11\rangle)$

Fig. 3 A 2×2 NEQR image

Based on three components of grayscale image within RGB color image, the generalized model of NEQR (GNEQR) (Li et al. 2019) that represents a quantum RGB color image is defined as:

$$\begin{aligned}|G\rangle &= \frac{1}{\sqrt{3}}\left(|I_R\rangle|01\rangle + |I_G\rangle|10\rangle + |I_B\rangle|11\rangle\right)\\ &= \frac{1}{\sqrt{3}} \times \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(|R_{YX}\rangle|YX\rangle|01\rangle + |G_{YX}\rangle|YX\rangle|10\rangle\right.\\ &\qquad \left.+ |B_{YX}\rangle|YX\rangle|11\rangle\right)\end{aligned} \tag{7}$$

Figure 4 illustrates the quantum circuit implementation for GNEQR image, where the quantum oracle NEQR (i.e., a quantum black box) prepares a NEQR quantum image (Zhang et al. 2013a, b), and the unitary operation $R_x\left(\arctan\sqrt{2}\right)$ is defined as:

$$R_x(\arctan\sqrt{2}) = \begin{bmatrix}\cos(\arctan\sqrt{2}) & \sin(\arctan\sqrt{2})\\ \sin(\arctan\sqrt{2}) & -\cos(\arctan\sqrt{2})\end{bmatrix} = \begin{bmatrix}1/\sqrt{3} & \sqrt{2}/\sqrt{3}\\ \sqrt{2}/\sqrt{3} & -1/\sqrt{3}\end{bmatrix}. \tag{8}$$

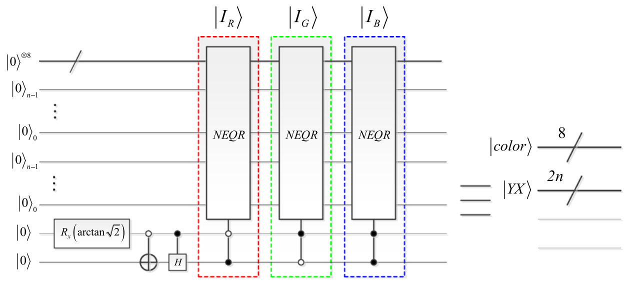


Fig. 4 Quantum circuit for the preparation of GNEQR image and its quantum circuit line

2.3 Twice scrambling based on generalized Arnold transform

Arnold transform, also called as cat map, was proposed by (Arnold and Avez, 1968) in the research of ergodic theory. Dyson and Falk quoted the transform as an image scrambling method (Dyson and Falk, 1992). On the basis of Arnold transform, the two-dimension generalized Arnold transform (Zhou et al. 2015) is defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & t \\ m & t \cdot m + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N), \tag{9}$$

where (x, y) and (x', y') are the pixel's coordinates of the original image and scrambled image, respectively. N is the size of the square image, t and m are the positive integers.

The generalized Arnold transform in the form of coordinates can be expressed as:

$$\begin{aligned} x' &= (x + t \cdot y) \bmod N, \\ y' &= \left[m \cdot x + (t \cdot m + 1)y\right] \bmod N. \end{aligned} \tag{10}$$

Accordingly, the inverse generalized Arnold transform is defined as:

$$\begin{aligned} \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 1 & t \\ m & t \cdot m + 1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} (\mathrm{mod} N) \\ &= \begin{bmatrix} t \cdot m + 1 & -t \\ -m & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (\mathrm{mod} N). \end{aligned} \tag{11}$$

The inverse generalized Arnold transform in the form of coordinates is expressed as:

$$\begin{aligned} x &= \left[(t \cdot m + 1)x' - t \cdot y'\right] \bmod N, \\ y &= \left(y' - m \cdot x'\right) \bmod N. \end{aligned} \tag{12}$$

Only implementing the generalized Arnold transform on the image's coordinate information do not changes histogram graph of the scrambled image. To enhance the security of the scrambled image, the generalized Arnold transform also can be used to scramble the pixel's gray value. Assume that the pixel's grayscale information I_{YX} shown in Eq. (5) is divided into following two parts:

$$\begin{aligned} &I_{YX} = I1_{YX} I2_{YX}, \\ &I1_{YX} = I_{YX}^{0} I_{YX}^{1} I_{YX}^{2} I_{YX}^{3}, \quad I2_{YX} = I_{YX}^{4} I_{YX}^{5} I_{YX}^{6} I_{YX}^{7}. \end{aligned} \tag{13}$$

Then the generalized Arnold transform and its inverse transform implemented on grayscale space can be defined as:

$$\begin{aligned} &\begin{cases} I1'_{YX} = (I1_{YX} + t \cdot I2_{YX}) \bmod 16 \\ I2'_{YX} = \left(m \cdot I1_{YX} + (t \cdot m + 1) \cdot I2_{YX}\right) \bmod 16 \end{cases}, \\ &\begin{cases} I1_{YX} = \left[(t \cdot m + 1) I1'_{YX} - t \cdot I2'_{YX}\right] \bmod 16 \\ I2_{YX} = \left(I2'_{YX} - m \cdot I1'_{YX}\right) \bmod 16 \end{cases}, \end{aligned} \tag{14}$$

where $I'_{YX} = I1'_{YX} I2'_{YX} = I_{YX}^{0\prime} I_{YX}^{1\prime} I_{YX}^{2\prime} I_{YX}^{3\prime} I_{YX}^{4\prime} I_{YX}^{5\prime} I_{YX}^{6\prime} I_{YX}^{7\prime}$ is the pixel's color information of encrypted image in position *(Y,X)*.

2.4 Logistic map

The chaotic Logistic map (Jafarizadeh and Behnia 2011) is widely studied in dynamic system, which is defined as:

$$x_{k+1} = \mu \cdot x_k (1 - x_k), \tag{15}$$

where $0 \le \mu \le 4,\ k = 0, 1, 2, 3, \cdots, n$ and $0 < x_0 < 1$.

The study of chaotic dynamics shows that the Logistic map is in chaos when $3.56 < \mu \le 4$. As an example, Logistic map curves under two different initial values with 100 iteration times are illustrated in Fig. 5, from which it is easily to find that the Logistic map curves are very sensitive to the initial values.

2.5 Quantum circuit modules

In this subsection, some quantum circuit modules are introduced, which play a key element to construct the quantum circuit for the presented quantum scheme.

2.5.1 ADDER module

The quantum ADDER originally introduced in (Vedral et al. 1996) is used to add two integers. Figure 6 illustrates the quantum circuit implementation for ADDER, which calculates the sum of two binary numbers A and B, where $A = a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ and $B = b_{n-1} b_{n-2} \cdots b_2 b_1 b_0$, $a_i,\ b_i \in \{0,\ 1\}$. The sum of $A + B$ is stored as $S = s_n s_{n-1} s_{n-2} \cdots s_2 s_1 s_0,\ s_i \in \{0,\ 1\}$. Therein, the basic modules of CARRY and SUM (its quantum circuits are shown in Fig. 7a) are used to respectively calculate the carry of three binary bits and the sum of two binary bits.

According to the property of binary bits, quantum ADDER-MOD module to calculate the mod operation of $(A + B) \bmod 2^n$ was proposed (Jiang and Wang, 2014), which can be easily realized through omitting the highest bit s_n of S. That is, $(A + B) \bmod 2^n = s_{n-1} s_{n-2} \cdots s_1 s_0$. For simplicity, Fig. 7b gives the simplified diagram of ADDER-MOD 2^n.

Noting that the positions of black boxes in the left and right within the CARRY module consists of all the same quantum gates but rearranged in a reverse order. In the following, we also adapt similar abbreviation notations to

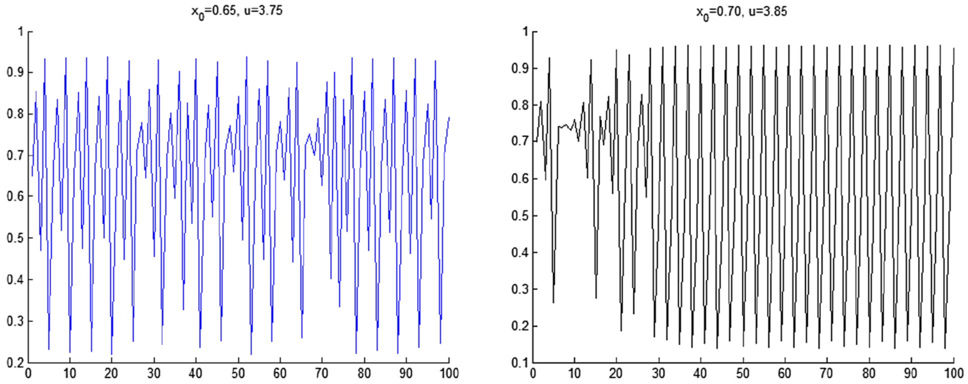


Fig. 5 Two Logistic map curves under different initial values within 100 iteration times

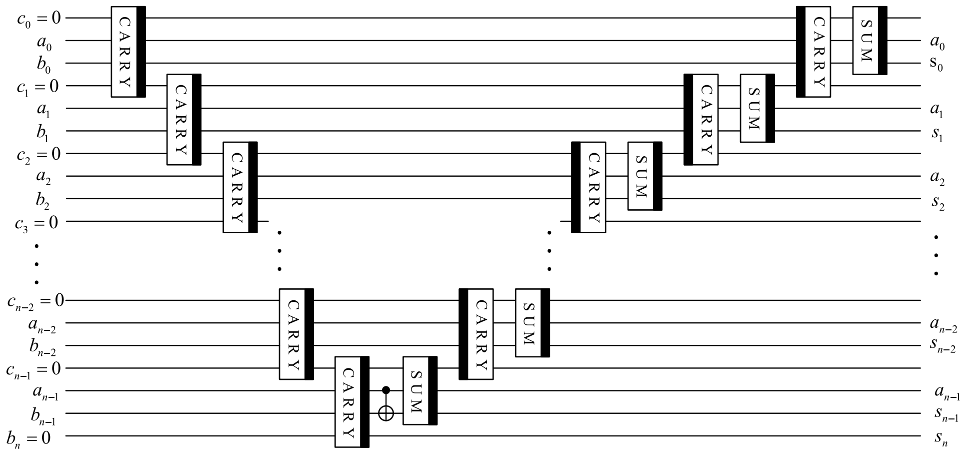


Fig. 6 Quantum effective circuits for ADDER

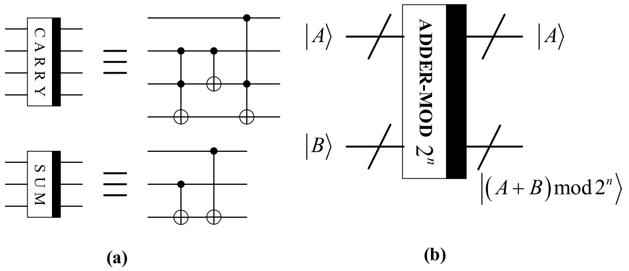


Fig. 7 a Quantum circuit for CARRY and SUM, (b) the simplified diagram of ADDER − MOD 2^n

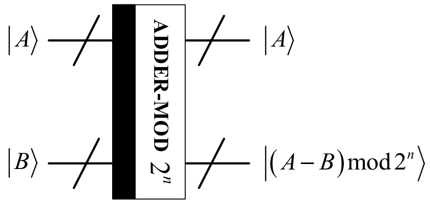


Fig. 8 Simplified diagram of quantum circuit module $(A-B)$ mod 2^n equation

denote the quantum modules that include same quantum gates but rearrange in a reverse order.

Due to the reversibility of quantum gates, if we reverse the action of the plain adder network with the initial two inputs $|A\rangle$ and $|B\rangle$, the output will produce $(|A\rangle, |A-B\rangle)$ when A > B. When A < B, the output is $(|A\rangle, |2^n-(B-A)\rangle)$, where $(n+1)$ is the size of the second register $|B\rangle$ with the most significant qubit (b_n) will always contain 1 (Vedral et al. 1996). Therefore, the quantum circuit realization of $(A-B)$ mod 2^n is similar to the ADDER-MOD, which is realized by sequencing all of the quantum gates within ADDER in a reverse order directly and with the most significant bit $b_n=1$ of the second register $|B\rangle$. The proof verifies this can be seen in Appendix 1. Figure 8 gives the simplified diagram of quantum circuit module of $(A-B)$ mod 2^n.

2.5.2 Perfect shuffle permutation

The perfect shuffle permutation can be used to cyclic shift qubit sequence (Li et al. 2019a, b, c). For n-qubit sequence, it has two different forms of $P_{2^{n-1},2}$ and $P_{2,\,2^{n-1}}$ recursively defined as:

$$\begin{aligned} P_{2^{n-1},\,2} &= \left(P_{2^{n-2},\,2} \otimes I_2\right)\left(I_{2^{n-2}} \otimes P_{2,\,2}\right), \\ P_{2,\,2^{n-1}} &= \left(P_{2,2} \otimes I_{2^{n-2}}\right)\left(I_2 \otimes P_{2,\,2^{n-2}}\right), \end{aligned} \tag{16}$$

where $P_{2,\,2}$ is the *Swap* gate as shown in Fig. 2.

Thus $P_{2^{n-1},2}$ and $P_{2,\,2^{n-1}}$ respectively transform the n-qubit $|X\rangle = |x_{n-1}x_{n-2}\cdots x_1x_0\rangle$ into following forms:

$$\begin{aligned} P_{2^{n-1},2}|X\rangle &= |x_0x_{n-1}x_{n-2}\cdots x_1\rangle, \\ P_{2,\,2^{n-1}}|X\rangle &= |x_{n-2}\cdots x_1x_0x_{n-1}\rangle. \end{aligned} \tag{17}$$

Figure 9 illustrates the quantum circuits for $P_{2^{n-1},2}$ and $P_{2,\,2^{n-1}}$, and their corresponding abbreviation notations are shown on the right.

2.5.3 Quantum equal

Quantum Equal module introduced in (Zhou et al. 2107) is used to compare two bit sequences whether they are equal or not. The quantum circuit for Quantum Equal and its simplified module are illustrated in Fig. 10, where $|Y\rangle = |y_{n-1}\cdots y_1y_0\rangle$, $|X\rangle = |x_{n-1}\cdots x_1x_0\rangle$, $x_i, y_i \in \{0,\ 1\}$. The output C represents the relationship between Y and X, i.e., if $C=1$, then $Y=X$; otherwise, $Y \neq X$ when $C=0$.

3 Quantum image encryption and decryption

On the basis of generalized Arnold transform and Logistic map, our investigated quantum image encryption and decryption algorithms as well as the intact quantum implementation circuits are described in detail within this section.

3.1 Encryption and decryption processes

Figure 11 gives the whole procedure of our investigated quantum image encryption and decryption schemes. As shown in Fig. 11a, the encryption process mainly divides into two stages, i.e., twice scrambling and pixel encryption. Due to the decryption is exact the inverse operation of encryption, which also contains two stages, i.e., pixel decryption and inverse twice scrambling (as shown in Fig. 11b).

As illustrated in Fig. 11a, to encrypt a quantum plain image $|I\rangle$ or $|G\rangle$ (respectively expressed as Eqs. (5) and (7)), a secret quantum image $|K\rangle$ with size of $2^n \times 2^n$ is needed to be prepared

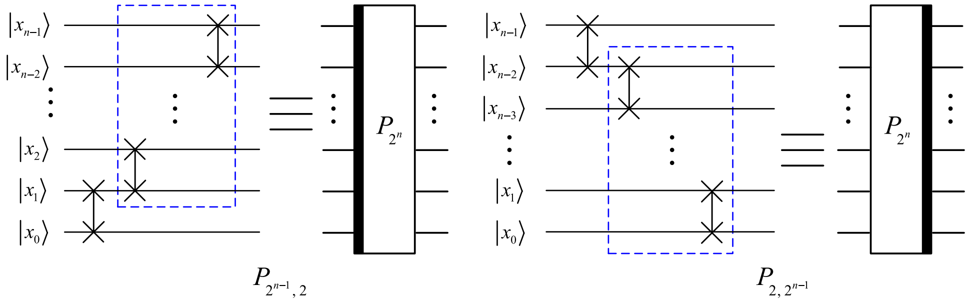


Fig. 9 Quantum circuits for $P_{2^{n-1},2}$ and $P_{2,\,2^{n-1}}$

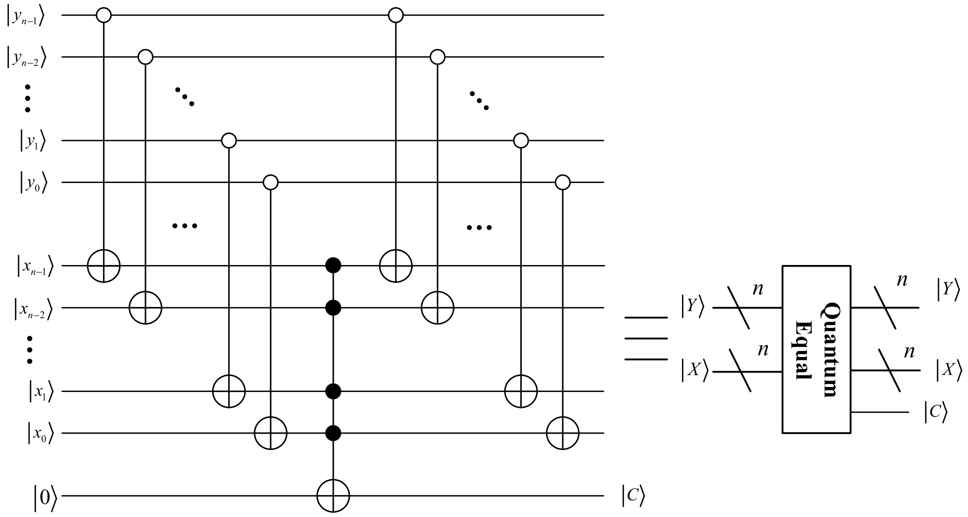


Fig. 10 Circuit design for Quantum Equal

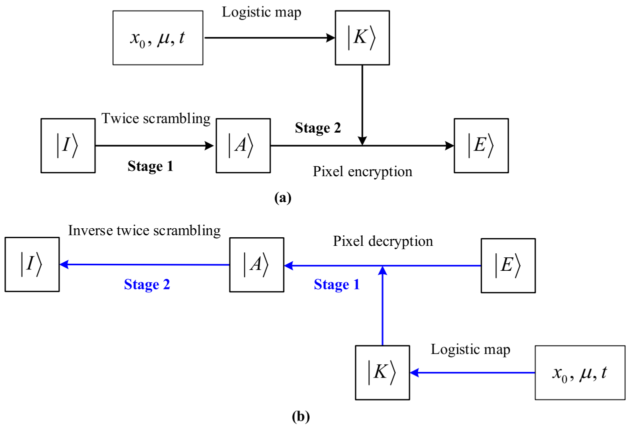


Fig. 11 Quantum image encryption and decryption processes: **(a)** encryption, **(b)** decryption

first. Herein, K is a classical grayscale image generated based on Logistic map first, and then encoded into a quantum image $|K\rangle$ based on NEQR model (Zhang et al. 2013a, b), which can be expressed as:

$$\begin{aligned}|K\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|K_{YX}\rangle|Y\rangle|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{7}\left|K_{YX}^T\right\rangle|Y\rangle|X\rangle,\end{aligned} \tag{18}$$

where $K_{YX} = K_{YX}^0 K_{YX}^1 \cdots K_{YX}^6 K_{YX}^7 = \sum_{i=0}^{7} K_{YX}^i \times 2^{7-i},\ K_{YX}^i \in \{0,1\}$ are generated by Logistic map under the initial values $x_0,\ \mu$ with iteration times $t = 2^{2n}$. The relationship of K_{YX}, x_t, Y, X, t can be described:

$$\begin{aligned}&K_{YX} = floor\left[\mathrm{mod}\left(\left(x_t \times 256\right), 256\right)\right],\ t \in \left\{1,\ 2,\ \cdots,\ 2^{2n}\right\},\\ &Y = y_{n-1}y_{n-2}\cdots y_1y_0,\ X = x_{n-1}x_{n-2}\cdots x_1x_0,\ y_i,\ x_i \in \{0,\ 1\},\\ &t = Y \times 2^n + X + 1,\end{aligned} \tag{19}$$

where floor and mod respectively stand for round down and modulus operations.

3.2 Quantum image encryption

The quantum image encryption is composed of two stages as illustrated in Fig. 11a. It can be described in detail as follows:

Stage 1 twice scrambling.

Suppose the final encrypted image $|A\rangle$ in first stage can be written as:

$$|A\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|A_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{q-1}\left|A_{YX}^T\right\rangle|Y\rangle|X\rangle. \tag{20}$$

According to Eq. (10), the coordinate of encrypted image $|A\rangle$ is defined as:

$$\begin{aligned}|X_A\rangle &= \left|\left(X_I + t\cdot Y_I\right) \bmod 2^n\right\rangle,\\ |Y_A\rangle &= \left|\left[m\cdot X_I + (t\cdot m + 1)Y_I\right] \bmod 2^n\right\rangle,\end{aligned} \tag{21}$$

where $|Y_I\rangle$ and $|X_I\rangle$ are the coordinates information of quantum image $|I\rangle$, $|Y_A\rangle$ and $|X_A\rangle$ denote the coordinates information of quantum image $|A\rangle$.

Due to the nature of modulo operation, we have:

$$(X + 2\cdot Y) \bmod 2^n = \left[(X + Y) \bmod 2^n + Y\right] \bmod 2^n. \tag{22}$$

Thus $|Y\rangle_A$ and $|X\rangle_A$ can be calculated in following forms:

$$\begin{aligned}&\left(Y_I, X_I\right) \to \left(Y_I, \left(X_I + Y_I\right) \bmod 2^n\right) \to \left(Y_I, \left(X_I + 2\cdot Y_I\right) \bmod 2^n\right) \to\\ &\cdots \to \left(Y_I, \left(X_I + (t-1)\cdot Y_I\right) \bmod 2^n\right) \to \left(Y_I, \underbrace{\left(X_I + t\cdot Y_I\right) \bmod 2^n}_{X_A}\right).\end{aligned} \tag{23}$$

$$\begin{aligned}&\left(X_I, X_I\right) \to \left(X_I, 2\cdot X_I \bmod 2^n\right) \to \cdots \to \left(X_I, m\cdot X_I \bmod 2^n\right)\\ &\left(Y_I, m\cdot X_I \bmod 2^n\right) \to \left(Y_I, \left(m\cdot X_I + Y_I\right) \bmod 2^n\right)\\ &\to \left(Y_I, \left(m\cdot X_I + 2\cdot Y_I\right) \bmod 2^n\right) \to \cdots \to \left(Y_I, \left(m\cdot X_I + t\cdot Y_I\right) \bmod 2^n\right)\\ &\to \left(Y_I, \underbrace{\left(m\cdot X_I + (t+1)\cdot Y_I\right) \bmod 2^n}_{Y_A}\right).\end{aligned} \tag{24}$$

Based on quantum ADDER MOD 2^n shown in Fig. 7(b), Fig. 12 illustrates the integrated quantum circuit implementation for calculating the coordinate information of the encrypted image $|A\rangle$, in which the detailed quantum circuit for Box 1 is shown in Fig. 13.

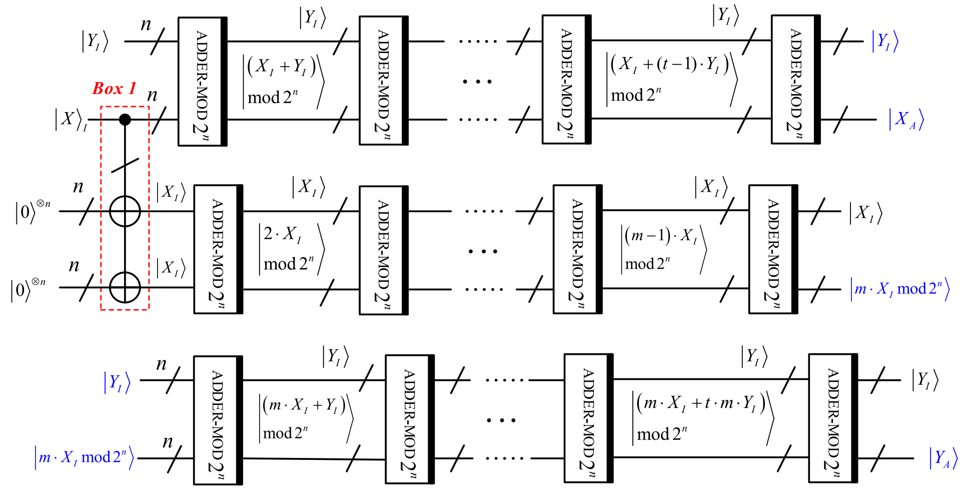
Based on generalized Arnold transform, the pixel's color information of quantum encrypted image $|A\rangle$ is defined as:

$$\begin{aligned}&|A1_{YX}\rangle = \left|\left(I1_{YX} + t\cdot I2_{YX}\right) \bmod 2^n\right\rangle,\\ &|A2_{YX}\rangle = \left|\left[m\cdot I1_{YX} + (t\cdot m + 1)I2_{YX}\right] \bmod 2^n\right\rangle,\\ &I1_{YX} = I_{YX}^0 I_{YX}^1 I_{YX}^2 I_{YX}^3,\ I2_{YX} = I_{YX}^4 I_{YX}^5 I_{YX}^6 I_{YX}^7,\\ &A1_{YX} = A_{YX}^0 A_{YX}^1 A_{YX}^2 A_{YX}^3,\ A2_{YX} = A_{YX}^4 A_{YX}^5 A_{YX}^6 A_{YX}^7,\end{aligned} \tag{25}$$

where $I_{YX} = \left(I1_{YX}, I2_{YX}\right)$ is the pixel color information of plain image $|I\rangle$.$A_{YX} = \left(A1_{YX}, A2_{YX}\right)$ is the pixel color information of encrypted image $|A\rangle$. Figure 14 illustrates the intact quantum circuit implementation for encrypting pixel color information based on generalized Arnold transform.

Stage 2 pixel encryption.

Herein, suppose that the final encrypted image $|E\rangle$ in stage 2 is written as:



$|Y_I\rangle$
$|X\rangle_I$
Box 1
n
$|0\rangle^{\otimes n}$
$|X_I\rangle$
ADDER-MOD 2^n
$|(X_I+Y_I) \bmod 2^n\rangle$
$|(X_I+(t-1)\cdot Y_I) \bmod 2^n\rangle$
$|X_A\rangle$
$|2\cdot X_I \bmod 2^n\rangle$
$|(m-1)\cdot X_I \bmod 2^n\rangle$
$|m\cdot X_I \bmod 2^n\rangle$
$|(m\cdot X_I+Y_I) \bmod 2^n\rangle$
$|(m\cdot X_I+t\cdot m\cdot Y_I) \bmod 2^n\rangle$
$|Y_A\rangle$

Fig. 12 Quantum circuits for encrypting the coordinate information

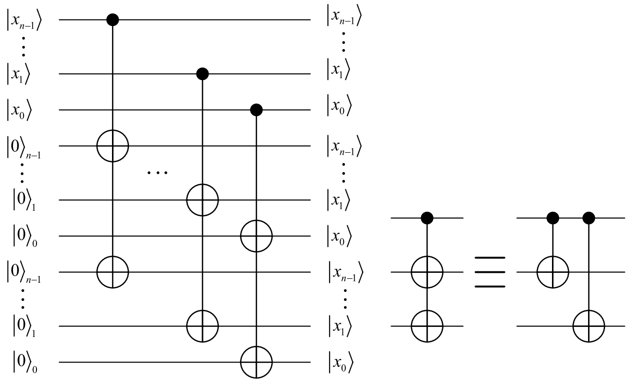


Fig. 13 Quantum circuit for box 1

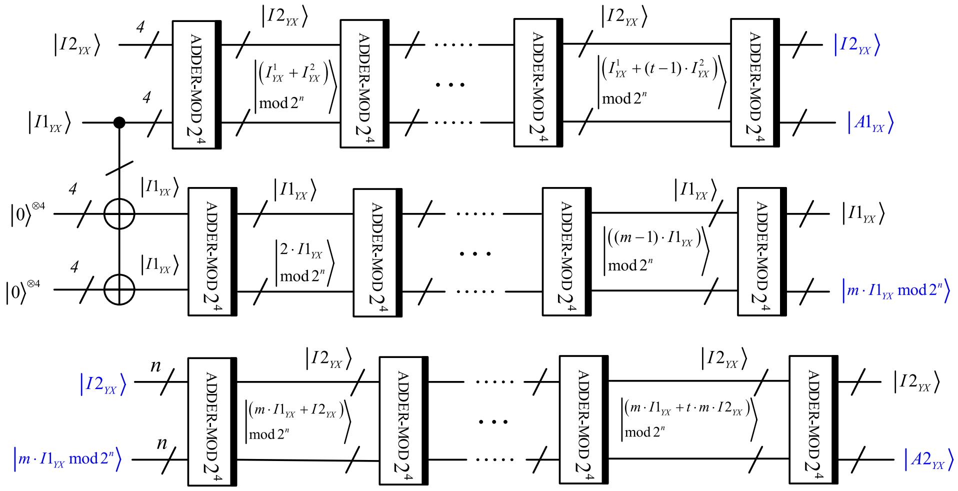
$$|E\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|E_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{q-1}|E_{YX}^T\rangle|Y\rangle|X\rangle. \tag{26}$$

The aim of current stage is to encrypt the pixel's color information of image $|A\rangle$ in first stage. The integrated quantum circuit for pixel information encryption is demonstrated in Fig. 15, which can be described as follows.

First, quantum Equal module is employed to compare the coordinate information of the two quantum images $|K\rangle$ and $|A\rangle$. The comparison results are denoted by the single output qubit $|C\rangle$ defined as:

$$\begin{cases} |YX\rangle_K = |YX\rangle_A, & |C\rangle = |1\rangle, \\ |YX\rangle_K \neq |YX\rangle_A, & |C\rangle = |0\rangle, \end{cases} \tag{27}$$

where $|YX\rangle_K$ and $|YX\rangle_A$ respectively denote the pixel's location information of quantum images $|K\rangle$ and $|A\rangle$.



$|I2_{YX}\rangle$
$|I1_{YX}\rangle$
4
$|0\rangle^{\otimes 4}$
ADDER-MOD 2^4
$|(I_{YX}^1+I_{YX}^2) \bmod 2^n\rangle$
$|(I_{YX}^1+(t-1)\cdot I_{YX}^2) \bmod 2^n\rangle$
$|A1_{YX}\rangle$
$|2\cdot I1_{YX} \bmod 2^n\rangle$
$|((m-1)\cdot I1_{YX}) \bmod 2^n\rangle$
$|m\cdot I1_{YX} \bmod 2^n\rangle$
n
$|(m\cdot I1_{YX}+I2_{YX}) \bmod 2^n\rangle$
$|(m\cdot I1_{YX}+t\cdot m\cdot I2_{YX}) \bmod 2^n\rangle$
$|A2_{YX}\rangle$

Fig. 14 Quantum circuits for encrypting the pixel color information

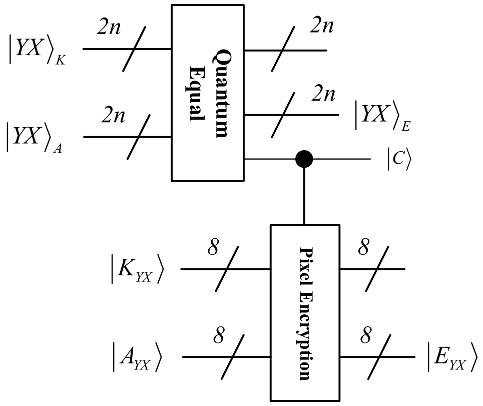


Fig. 15 Quantum circuit for pixel encryption

Second, quantum Pixel Encryption module is used to encrypt the pixel's color information of image $|A\rangle$ when the coordinate information of two images $|K\rangle$ and $|A\rangle$ are equal. That is, the output qubit $|C\rangle$ in state of $|1\rangle$ is utilized to act as a controlled qubit for Pixel Encryption module. The intact quantum circuit implementation for Pixel Encryption module is illustrated in Fig. 16, which consists of three steps described as follows.

Step 1 encrypt the pixel's color information of image $|A\rangle$ through CNOT gates, where the qubit $\left|K^i_{YX}\right\rangle$ is the control qubit while qubit $\left|A^i_{YX}\right\rangle$ is the target qubit, $i = 0, 1, \cdots, 7$. Assume that the encrypted image is $|AX\rangle$, then it can be defined as:

$$\begin{aligned}|AX\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|A_{YX} \oplus K_{YX}\rangle|YX\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{q-1}\left|A^T_{YX} \oplus K^T_{YX}\right\rangle|Y\rangle|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{q-1}\left|AX^T_{YX}\right\rangle|Y\rangle|X\rangle.\end{aligned} \tag{28}$$

Step 2 current step consists of two substeps described as follows:

Substep 2.1 perform the bit-plane scrambling operation on image $|AX\rangle$, then the obtained encrypted image $|AB\rangle$ can be defined as:

$$\begin{aligned}|AB\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=7}^{4}\left|AX^T_{YX}\right\rangle\left|AX^7_{YX} \oplus AX^3_{YX}\right\rangle\left|\overline{AX^6_{YX}} \oplus AX^2_{YX}\right\rangle\\ &\qquad \otimes\left|AX^5_{YX} \oplus AX^1_{YX}\right\rangle\left|\overline{AX^4_{YX}} \oplus AX^0_{YX}\right\rangle|Y\rangle|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=7}^{4}\left|K^T_{YX} \oplus A^T_{YX}\right\rangle\otimes\left|K^7_{YX} \oplus A^7_{YX} \oplus K^3_{YX} \oplus A^3_{YX}\right\rangle\\ &\qquad \otimes\left|\overline{K^6_{YX} \oplus A^6_{YX}} \oplus K^2_{YX} \oplus A^2_{YX}\right\rangle \otimes \left|K^5_{YX} \oplus A^5_{YX} \oplus K^1_{YX} \oplus A^1_{YX}\right\rangle\\ &\qquad \otimes\left|\overline{K^4_{YX} \oplus A^4_{YX}} \oplus K^0_{YX} \oplus A^0_{YX}\right\rangle|Y\rangle|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{q-1}\left|AB^T_{YX}\right\rangle|Y\rangle|X\rangle.\end{aligned} \tag{29}$$

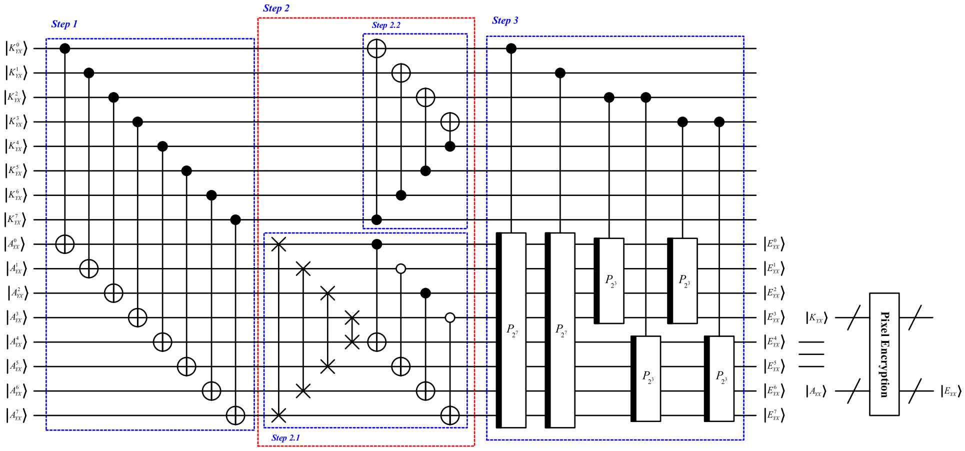
Substep 2.2 implement the CNOT gates on image $|K\rangle$. Then the obtained image $|KX\rangle$ is defined as:

$$\begin{aligned}|KX\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{3}\left|K^T_{YX} \oplus K^{7-T}_{YX}\right\rangle\left|K^4_{YX}K^5_{YX}K^6_{YX}K^7_{YX}\right\rangle|Y\rangle|X\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{T=0}^{7}\left|KX^T_{YX}\right\rangle|Y\rangle|X\rangle.\end{aligned} \tag{30}$$

Step 3 under the control of qubits K^0_{YX}, K^1_{YX}, K^2_{YX}, K^3_{YX}, implement the controlled perfect shuffle permutation $P_{2^7,2}$ or $P_{2^3,2}$ on image $|AB\rangle$. Since it is hard to describe the encryption process of this step in formula form, we omit it from here for simplicity. Assume that the image $|AB\rangle$ after perfect shuffle permutation operations is final encrypted image $|E\rangle$ written as Eq. (26).

Figure 17 gives the complete quantum circuit implementation for the proposed quantum image encryption process.

Fig. 16 Quantum circuit for Pixel Encryption module



Herein, the simplified diagram of "Generalized Arnold" means the twice scrambling based on generalized Arnold transform in stage 1, and the simplified diagram of "Pixel Encryption Based on Key Image" means the pixel encryption process in stage 2. Figures 17a, b respectively denote the encryption for the quantum grayscale and color images.

3.3 Quantum image decryption

Quantum image decryption is the inverse process of encryption as illustrated in Fig. 11b. Based on quantum key image $|K\rangle$ and quantum encrypted image $|E\rangle$, the decryption process that recovering the quantum plain image $|I\rangle$ can be described within following two stages.

Stage 1 pixel decryption.

The quantum circuit module for pixel decryption operation in this stage is shown in Fig. 18. The process can be explained as follows.

First, the Quantum Equal module is employed to compare whether the coordinate information of two images $|K\rangle$ and $|E\rangle$ are equal or not.

Second, the output qubit $|C\rangle$ of Quantum Equal module is used to act as the control qubit for quantum Pixel Decryption module. Figure 19 illustrates the detailed quantum circuit implementation for Pixel Decryption module, which consists of following three steps.

Step 1 current step consists of two substeps described as follows:

Substep 1.1 implement the CNOT operations within image $|K\rangle$, and then obtain the image $|KX\rangle$ described as Eq. (30).

Substep 1.2 under the control of qubits K^0_{YX}, K^1_{YX}, K^2_{YX}, K^3_{YX}, implement the controlled perfect shuffle permutation $P_{2^7,2}$ or $P_{2^3,2}$ on image $|E\rangle$. Then, we can decrypt the quantum image $|E\rangle$ into $|AB\rangle$ written as Eq. (29).

Step 2 current step includes following two substeps described as:

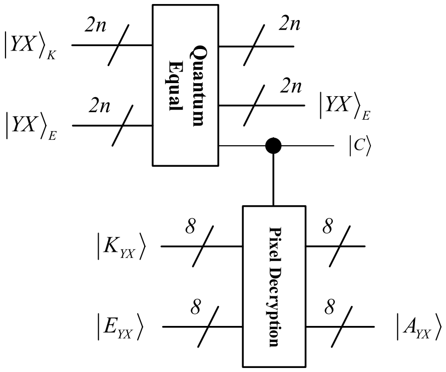


Fig. 18 Quantum circuit module for Pixel Decryption operation

Susbstep 2.1 implement the CNOT operations on quantum image $|KX\rangle$, which can transform image $|KX\rangle$ into image $|K\rangle$.

Substep 2.2 implement the inverse bit-plane scrambling operation for quantum image $|AB\rangle$. Then we can obtain image $|AX\rangle$ written as Eq. (28).

Step 3 implement the CNOT operations between images $|K\rangle$ and $|AX\rangle$, then $|AX\rangle$ is transformed into the $|A\rangle$ written as Eq. (20).

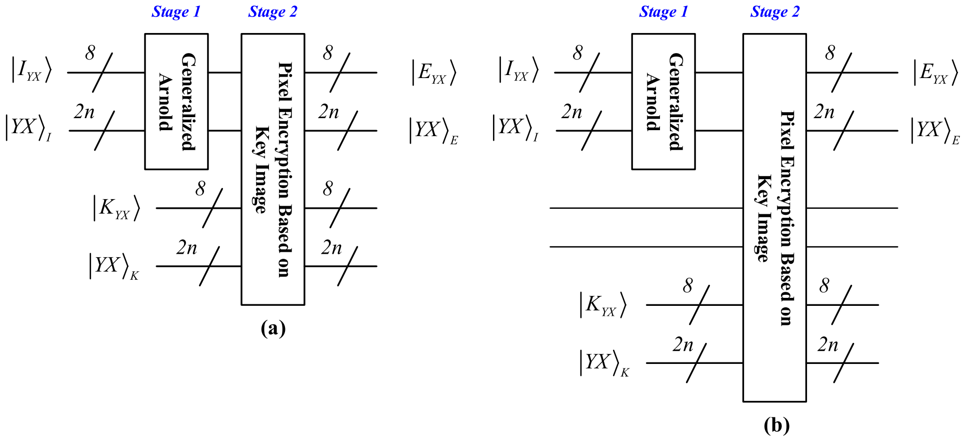
Stage 2 inverse twice scrambling.

Based on Eq. (12), the coordinate information based on inverse generalized Arnold transform can be defined as:

$$\begin{aligned} |X_I\rangle &= \left|\left[(t\cdot m+1)\cdot X_A - t\cdot Y_A\right] \bmod 2^n\right\rangle, \\ |Y_I\rangle &= \left|\left(Y_A - m\cdot X_A\right) \bmod 2^n\right\rangle. \end{aligned} \tag{31}$$

Similarly, due to the nature of mod operation, we can deduce the following relationship:

Fig. 17 Quantum circuit modules for quantum image encryption process: **(a)** quantum grayscale image; **(b)** quantum color image



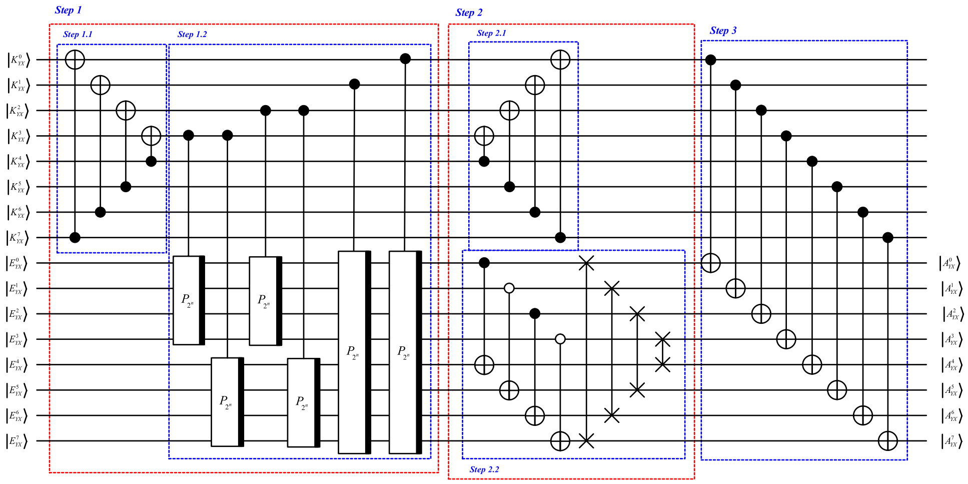


Fig. 19 Quantum circuit for Pixel Decryption module

$$
\begin{aligned}
&(t \cdot X - m \cdot Y) \bmod 2^n \\
&= (t \cdot X \bmod 2^n - m \cdot Y \bmod 2^n) \bmod 2^n \\
&= \left\{ \begin{array}{l} \left[(t-1) \cdot X \bmod 2^n + X\right] \bmod 2^n \\ -\left[(m-1) \cdot Y \bmod 2^n + Y\right] \bmod 2^n \end{array} \right\} \bmod 2^n.
\end{aligned} \tag{32}
$$

Thus, based on the quantum module ADDER − MOD 2^n (shown in Fig. 7(b)) and its inverse module ADDER − MOD 2^n (shown in Fig. 8), the coordinate information $|Y_I\rangle$ and $|X_I\rangle$ can be calculated as follows:

$$
\begin{cases}
\left(X_A, X_A\right) \to \left(X_A, 2 \cdot X_A \bmod 2^n\right) \to \cdots \to \left(X_A, tm \cdot X_A \bmod 2^n\right) \\
\to \left[X_A, (tm+1) \cdot X_A \bmod 2^n\right]
\end{cases}
$$

$$
\begin{cases}
\left(Y_A, Y_A\right) \to \left(Y_A, 2 \cdot Y_A \bmod 2^n\right) \to \\
\cdots \to \left(Y_A, t \cdot Y_A \bmod 2^n\right)
\end{cases}
$$

$$
\begin{cases}
\left[(tm+1) \cdot X_A \bmod 2^n, t \cdot Y_A \bmod 2^n\right] \\
\to \left\{ (tm+1) \cdot X_A \bmod 2^n, \underbrace{\left[(tm+1) \cdot X_A - t \cdot Y_A\right] \bmod 2^n}_{X_I} \right\}.
\end{cases} \tag{33}
$$

$$
\begin{aligned}
&\left(X_A, X_A\right) \to \left(X_A, 2 \cdot X_A \bmod 2^n\right) \to \cdots \to \left(X_A, m \cdot X_A \bmod 2^n\right) \\
&\left(Y_A, m \cdot X_A \bmod 2^n\right) \to \left[Y_A, \underbrace{\left(Y_A - m \cdot X_A\right) \bmod 2^n}_{Y_I} \right].
\end{aligned} \tag{34}
$$

On the basis of Eqs. (33) and (34), Fig. 20 illustrates the integrated quantum circuit for calculating the coordinate information of the plain image $|I\rangle$.

Based on Eq. (14), the pixel's color information of plain image $|I\rangle$ can be defined as:

$$
\begin{aligned}
\left|I1_{YX}\right\rangle &= \left|\left[(t \cdot m + 1) \cdot A1_{YX} - t \cdot A2_{YX}\right] \bmod 2^n\right\rangle, \\
\left|I2_{YX}\right\rangle &= \left|\left(A2_{YX} - m \cdot A1_{YX}\right) \bmod 2^n\right\rangle.
\end{aligned} \tag{35}
$$

According to Eq. (35), Fig. 21 illustrates the intact quantum circuit implementation for recovering pixel's color information of image $|I\rangle$.

Based on above-mentioned two stages operation, Fig. 22 illustrates the whole quantum circuit implementation module for proposed quantum image decryption scheme. Wherein, Figs. 22a, b respectively denote the decryption for the quantum grayscale and color images. The simplified diagram of "Pixel Decryption Based on Key Image" means the decryption process within stage 1, and the simplified diagram of "Inverse Generalized Arnold" means the inverse twice scrambling operation within stage 2.

4 Complexity analyses

To give a detailed analysis about the computational complexity, the quantum cost and time complexity of a quantum circuit defined in (Li et al. 2018a, b, c) are adopted, which are defined as:

(1) The quantum cost of a quantum circuit can be regarded as the total number of basic operations which simulate the circuit.

(2) The time complexity of a quantum circuit is defined by the total number of time steps. In a time step, only one basic operation is executed or multiple ones can be performed in parallel.

4.1 Quantum cost

The complex quantum circuit on many qubits n can be decomposed into a sequence of one-qubit and two-qubit

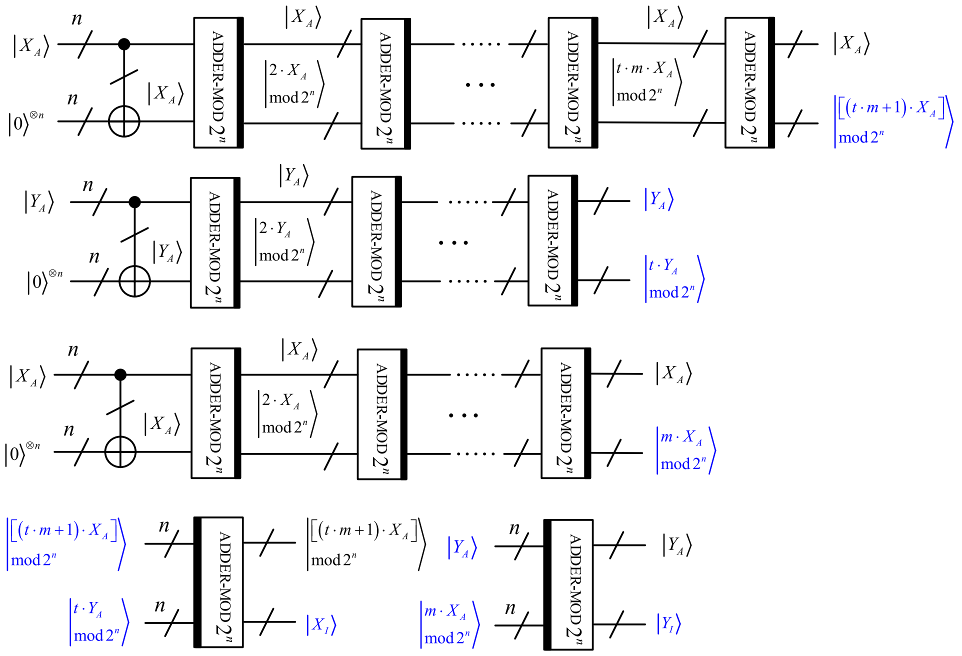


Fig. 20 Quantum implementation circuits of the inverse generalized Arnold transform for coordinate information

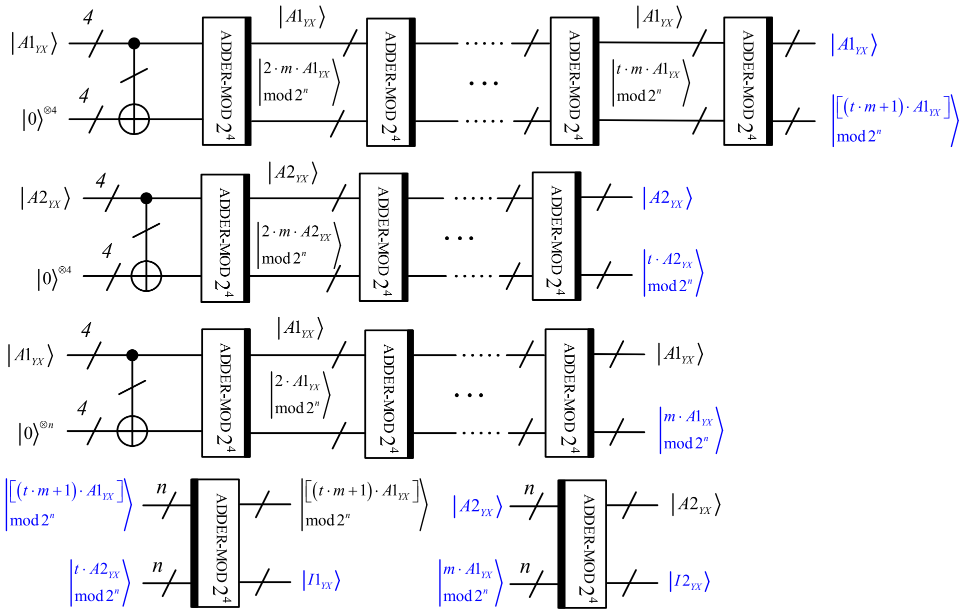


Fig. 21 Quantum circuits of inverse generalized Arnold transform for the pixel information

quantum gates compositions (Michael and Isaac 2000; Barenco 1995). Herein, the quantum cost of one-qubit and two-qubit quantum gates are taken as unit. Furthermore, it pointed out that a quantum $C^n(X)$ gate can be decomposed into *2(n-1)* Toffoli gates and a CNOT gate with *n-1* ancillary qubits (Michael and Isaac 2000), in which n ($n \geq 3$) is the number of control qubits and X is NOT gate (as illustrated in Fig. 23), and one Toffoli gate (i.e., $C^2(X)$) can be simulated by five two-qubit quantum gates illustrated in Fig. 24 (Michael and Isaac 2000). Thus the quantum cost of a $C^n(X)$ gate is deduced as $2(n-1) \times 5 + 1 = 10n - 9$.

Since the investigated quantum image encryption process mainly consists of two stages, i.e., twice scrambling within

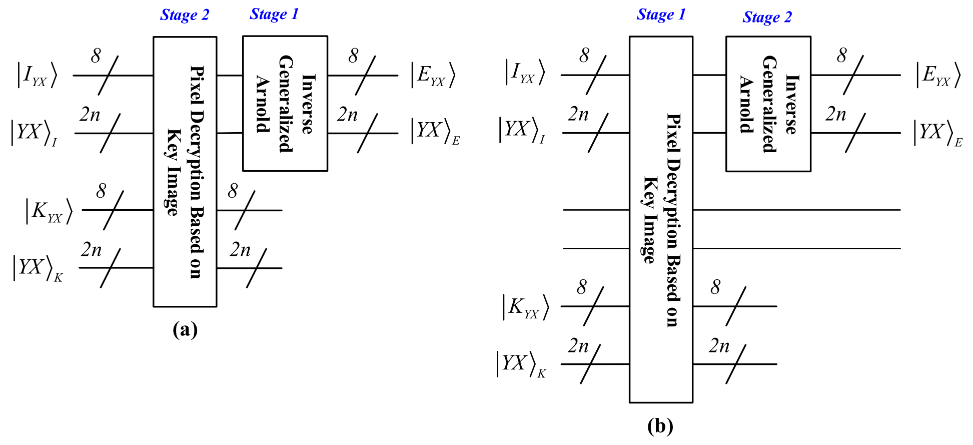


Fig. 22 Quantum circuit module for quantum image decryption: (**a**) quantum grayscale image; (**b**) quantum color image

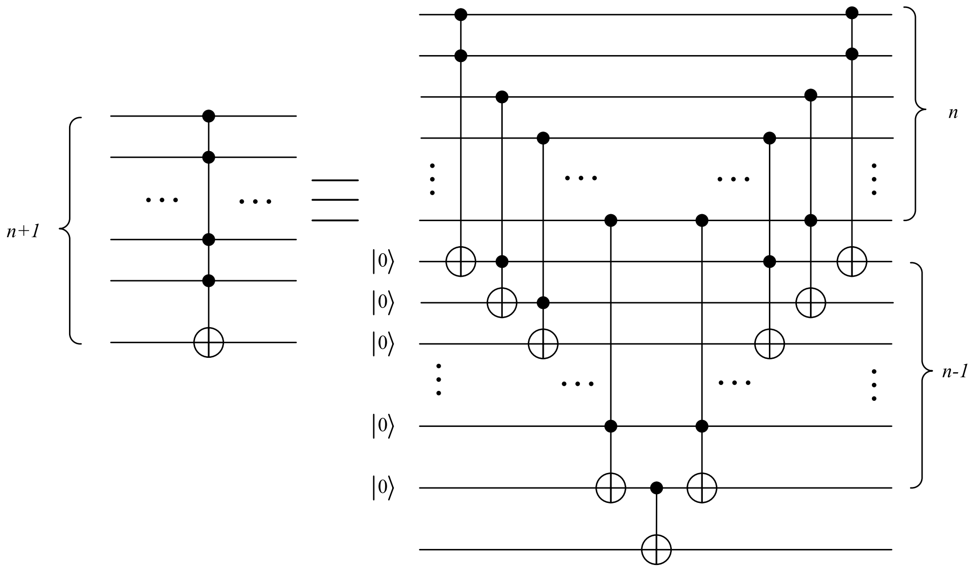


Fig. 23 The decomposition of $C^n(X)$ gate via Toffoli gates and CNOT gate

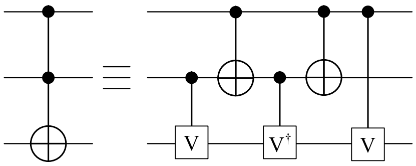


Fig. 24 The decomposition of Toffoli gate via five two-qubit quantum gates

stage 1 and pixel encryption within stage 2, the quantum cost of intact quantum circuit for image encryption can be discussed as follows:

Stage 1 twice scrambling.

The quantum cost in current stage is dependent on the number of quantum ADDER-MOD module used. The quantum circuit implementations are illustrated in Figs. 12 and 14. For the coordinate information encryption shown in Fig. 12, the number of ADDER $-$ MOD 2^n module is $t \cdot m + t + m - 1$, and as well as $2n$ additional CNOT gates. For pixel's gray value encryption shown in Fig. 14, the number of ADDER $-$ MOD 2^4 module also is $t \cdot m + t + m - 1$, and as well as additional *8* CNOT gates. The detailed quantum circuit for ADDER is shown in Fig. 6, which contains *(2n-1)* CARRY modules (a CARRY module consists of *2* Toffoli and *1* CNOT gates), *n* SUM modules (a SUM module consists of *2* CNOT gates), and an additional CNOT gate. Thus, the quantum cost of ADDER $-$ MOD 2^n is calculated as:

$$(2n - 1) \times (2 \times 5 + 1) + 2n + 1 = 24n - 10. \qquad (36)$$

Thus, the quantum cost of twice scrambling in stage 1 can be deduced as:

$$\begin{aligned} & k_1 \times [(24n - 10) \times (t \cdot m + t + m - 1) + 2n] \\ & + k_2 \times [(24 \cdot 4 - 10) \times (t \cdot m + t + m - 1) + 8] \\ & = \mathrm{O}(n), \end{aligned} \tag{37}$$

where two positive integers k_1 and k_2 are constants denote the iteration times of generalized Arnold transforms implemented on pixel's coordinate and color information, respectively.

Stage 2 pixel encryption.

The quantum circuit within current stage 2 mainly consists of two modules: Quantum Equal and Pixel Encryption. According to effective circuit of Quantum Equal shown in Fig. 10, we can infer that the Quantum Equal module within current stage contains *4n* CNOT gates and an additional $C^{2n}(X)$ gate. Thus, the quantum cost of Quantum Equal module is $24n - 9$. For the Pixel Encryption module shown in Fig. 16, it contains 16 CNOT gates, 4 Swap gates, 2 controlled $P_{2^7,2}$ modules and 4 controlled $P_{2^3,2}$ modules. Noting that Swap gate can be decomposed into three CNOT gates (shown in Fig. 2), then the controlled Swap gate (with one control qubit) can be regarded as consisting of three Toffoli gates. Then the quantum cost of Pixel Encryption module is calculated as: $16 + 4 + (2 \times 7 + 4 \times 3) \times 3 \times 5 = 410$. Thus, the quantum cost in stage 2 is calculated as:

$$24n - 9 + 410 = 24n + 401 = \mathrm{O}(n). \tag{38}$$

Based on above two stage analysis, the quantum cost of presented quantum image encryption process is calculated as $\mathrm{O}(n)$. Furthermore, due to the decryption is exactly the inverse process of encryption, we can infer that the quantum cost of image decryption process is also $\mathrm{O}(n)$.

4.2 Time complexity

Similar to quantum cost analysis, the time complexity of quantum image encryption process is divided into following two stages.

Stage 1 twice scrambling.

Noting that the CARRY and SUM modules within ADDER are executed in sequence (shown in Fig. 6), and the quantum gates (i.e., Toffoli and CNOT gates) within these modules are also executed in sequence (shown in Fig. 7a). Thus, the time complexity of single ADDER module is *24n-10*. For the quantum circuit of Box 1 shown in Fig. 12, it can be designed in parallel within two steps. Because the generalized Arnold transform implemented on pixel's coordinate and color information are independent (i.e., these two processes can be executed in parallel), the time complexity of twice scrambling in stage 1 can be deduced as:

$$max \left\{ \begin{array}{l} k_1 \times [(24n - 10) \times (t \cdot m + t + m - 1) + 2], \\ k_2 \times [(24 \cdot 4 - 10) \times (t \cdot m + t + m - 1) + 2] \end{array} \right\}, \tag{39}$$

where *max* means taking the maximum.

Stage 2 pixel encryption.

For the Quantum Equal module shown in Fig. 15, the *4n* CNOT gates can be executed in parallel with 2 steps, and the $C^{2n}(X)$ gate can be decomposed into *(2n-1)* Toffoli gates and 1 CNOT gate executed in sequence. Thus, the time complexity of Quantum Equal module calculated as $2 + (2n - 1) \times 5 + 1 = 10n - 2$. For the Pixel Encryption module, it is divided into three steps: (1) the CNOT operations of step 1 can be executed in parallel with one step; (2) the Swap operations and CNOT operations of step 2 can be executed in parallel with two steps; (3) the controlled perfect shuffle permutations in step 3 contains 26 controlled Swap gates, where a controlled Swap gate can be regarded as three Toffoli gates. Thus, the time complexity step 3 is $26 \times 3 \times 5 = 390$. Therefore, the time complexity of stage 2 is calculated as:

$$10n - 2 + 1 + 2 + 390 = 10n + 391. \tag{40}$$

From above two stages analyses, it is easily to infer that the time complexity for our investigated quantum image encryption and decryption schemes are both $\mathrm{O}(n)$. Noting that in classical image processing algorithms, the pixels needs to be processed one-by-one, it requires a computational complexity of at least $\mathrm{O}\left(2^{2n}\right)$ for a $2^n \times 2^n$ digital image. Thus the presented quantum image encryption and decryption schemes have achieved an exponential speedup than the classical algorithms.

4.3 Comparisons

Compared to classical image processing algorithm that process the pixel's information pixel-by-pixel, our presented quantum image encryption algorithm obviously has a lower complexity. Therefore, we only compare our presented quantum scheme with others existing quantum schemes to evaluate the performance in terms of quantum cost. Table 1 gives the comparisons in terms of quantum cost

Table 1 Comparisons in terms of quantum cost

Works	Images	Quantum cost
Yang et al. (2013)	Grayscale	$O(n^2)$
Yang et al. (2014)	Color	$O(n^2)$
Jiang, Wu and Wang, (2014a, b)	Grayscale	$O(n)$
Jiang, Wang and Wu (2014a, b)	Grayscale	$O(n^2)$
Zhou et al. (2015)	Grayscale	$O(n^2)$
Liang et al. (2016)	Grayscale	$O(n)$
Zhou et al. (2018)	Color	$O(n)$
Li et al. (2018a, b, c)	Grayscale or color	$O(n2^n)$
Li et al. (2019a, b, c)	Grayscale or color	$O(n^2)$
Our scheme	Grayscale or color	$O(n)$

with existing researches, from which we can conclude that our investigated quantum scheme has the same or lower quantum cost than existing works.

5 Experimental results and numerical analysis

Due to the absence of a practical and functional quantum computer, our experimental results are simulated under the classical computers equipped with the MATLAB environment. I.e., in a classical version (no quantum version) with an ideal environment without considering the effects of quantum noise introduced when implements the quantum gate and quantum measurement operations. MATLAB is a good tool that facilitates the representation and manipulation of large arrays of vectors and matrices, which makes it simulate quantum states and operators effectively, such as the superposition states of quantum images and the quantum unitary operations.

To evaluate the performance of our presented quantum encryption scheme, two grayscale images (Lena and Cameraman) and two color images (Lena and Airplane) with size of 256 × 256 are used as the tested images illustrated in Fig. 25.

5.1 Experimental results

For simplicity, Figs. 26 and 27 only demonstrate several cases of the encrypted images based on our investigated quantum encryption algorithm. Figure 26 illustrates the visual effects

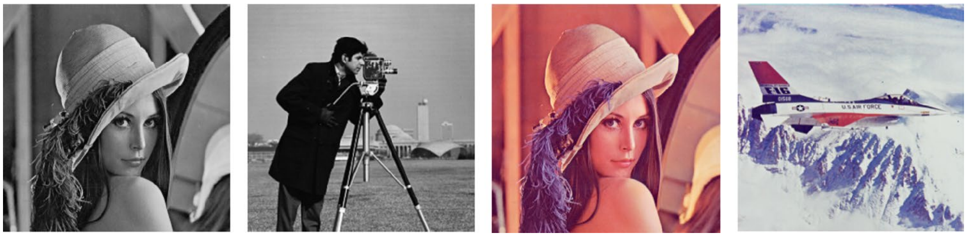


Fig. 25 Tested images used in our simulation

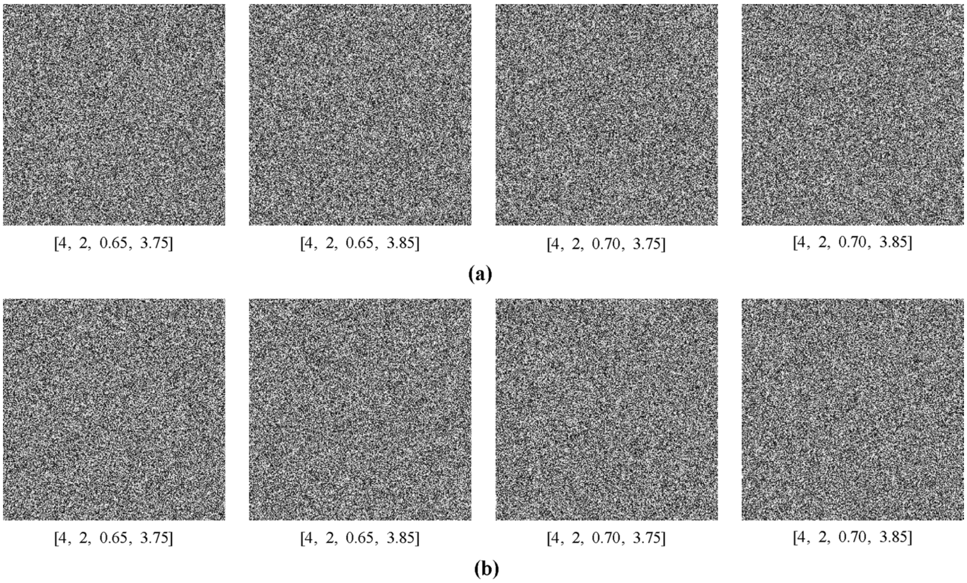
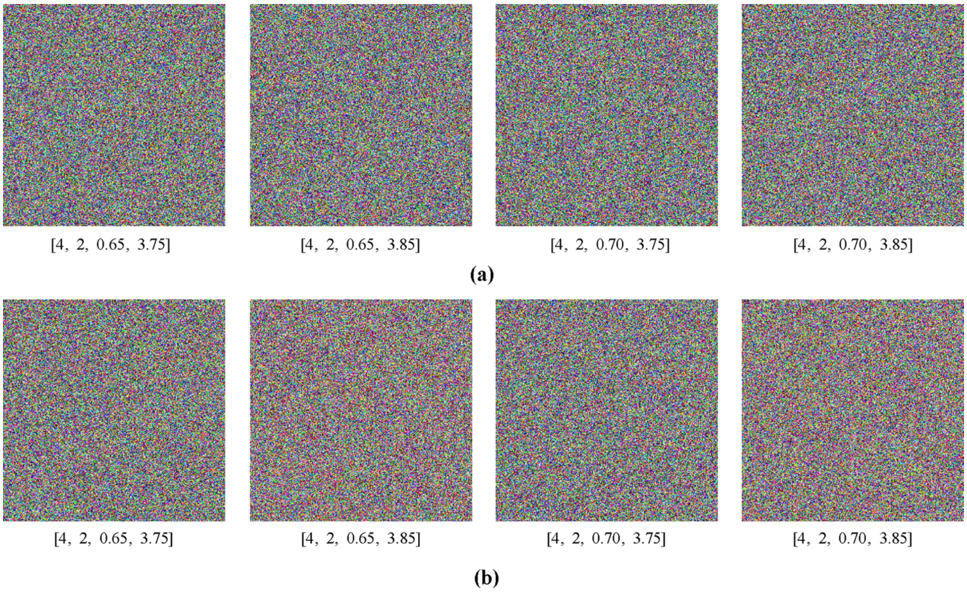


Fig. 26 Visual effects of the encrypted grayscale images: **(a)** Encrypted Lena, **(b)** Encrypted Cameraman



[4, 2, 0.65, 3.75] [4, 2, 0.65, 3.85] [4, 2, 0.70, 3.75] [4, 2, 0.70, 3.85]

(a)

[4, 2, 0.65, 3.75] [4, 2, 0.65, 3.85] [4, 2, 0.70, 3.75] [4, 2, 0.70, 3.85]

(b)

Fig. 27 Visual effects of the encrypted color images: **(a)** Encrypted Lena, **(b)** Encrypted Airplane

of the encrypted grayscale images Lena and Cameraman. Herein, the iteration times of generalized Arnold transform with initial values $t = m = 2$ implemented in pixel's coordinate and color information are *4* times and *2* times, respectively. Figure 27 illustrates the visual effects of the encrypted color images Lena and Airplane under the same conditions as Fig. 26 does. Herein, the text below encrypted image with four initial values (from left to right) respectively represent iteration times of generally Arnold transform implemented on pixel's coordinate and color information, and two initial values $x_0,\ \mu$ of Logistic map.

5.2 Statistical analysis

5.2.1 Mean square error

A perfect encrypted image should significantly differ with the original one. The mean square error (MSE) is an effective merit that characterizes the difference between encrypted images and original versions. For two grayscale images with size of $2^n \times 2^n$, MSE is defined as:

$$MSE = \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \left[I(i,j) - E(i,j)\right]^2, \tag{41}$$

where $I(i,j)$ and $E(i,j)$ are the pixel gray value of original and encrypted images in position *(i,j)*, respectively. Similarly, for two color images, MSE is defined via three channels red, green and blue as:

$$\begin{aligned} MSE_R &= \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \left[I_R(i,j) - E_R(i,j)\right]^2, \\ MSE_G &= \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \left[I_G(i,j) - E_G(i,j)\right]^2, \\ MSE_B &= \frac{1}{2^n \times 2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \left[I_B(i,j) - E_B(i,j)\right]^2, \end{aligned} \tag{42}$$

where $I_K(i,j)$ and $E_K(i,j)$ are pixel gray value of original and encrypted images in position *(i,j),* respectively. $K = R,\ G,\ B$ respectively denote the red, green and blue channels of RGB color image.

Obviously, the larger the MSE value is, the better the encryption effects is. For the four plain images shown in Fig. 25, the MSE values of the encrypted images shown in Fig. 26 based on our presented scheme are calculated as shown in Table 2. The MSE values of color image in three channels Red, Green and Blue for the encrypted color images Lena and Airplane shown in Fig. 27 are demonstrated in Table 3. Apparently, the numerical values in Tables 2 and 3 with high MSE values indicate that the images encrypted by using our proposed scheme are quite

Table 2 MSE values of the encrypted grayscale images with original version

MSEs Images	Encrypted images under different initial values			
	[4,2, 0.65, 3.75]	[4, 2, 0.65, 3.85]	[4, 2, 0.70, 3.75]	[4, 2, 0.70, 3.85]
Lena	9.0052e+03	9.0204e+03	9.1091e+03	9.0992e+03
Cameraman	9.4319e+03	9.2363e+03	9.4141e+03	9.2563e+03

Table 3 MSE values of the encrypted color images with original version

MSEs Images	Channels	Encrypted images under different initial values			
		[4,2,0.65, 3.75]	[4,2, 0.65, 3.85]	[4, 2, 0.70, 3.75]	[4, 2, 0.70, 3.85]
Lena	Red	3.4825e+03	3.4934e+03	3.5262e+03	3.4901e+03
	Green	3.0044e+03	2.9991e+03	3.0115e+03	3.0042e+03
	Blue	2.3695e+03	2.3662e+03	2.3576e+03	2.3433e+03
Jetplane	Red	3.2179e+03	2.9447e+03	3.1872e+03	2.9561e+03
	Green	3.5487e+03	3.5711e+03	3.5822e+03	3.5858e+03
	Blue	3.5506e+03	3.5280e+03	3.4822e+03	3.5179e+03

Table 4 MSE values of two encrypted grayscale images

MSEs Images	Encrypted images under different initial values			
	[4,2, 0.65, 3.75]	[4, 2, 0.65, 3.85]	[4, 2, 0.70, 3.75]	[4, 2, 0.70, 3.85]
Lena	1.0847e+04		1.0967e+04	
Cameraman	1.0840e+04		1.0853e+04	

Table 5 Comparisons with other existing works

MSEs Images	Channels	Our scheme	Li and Zhao 2017	Ran et al. 2018
		[4,2,0.65, 3.75]	–	–
Lena	Red	3.4825e+03	1.062+e4	9.114e+03
	Green	3.0044e+03	9.064+e3	9.784e+03
	Blue	2.3695e+03	7.111+e3	1.066e+04

differ with the original images. Thus, our investigated image encryption algorithm has good encryption effects. Furthermore, to test the chance of a successful attack when decrypts an encrypted image using two very close initial values of Logistic map, the MSE of two encrypted grayscale images Lena and Cameraman are shown in Table 4 as examples. Obviously, the MSE values of two encrypted grayscale images under very two close initial values of Logistic map are larger than 1.08e+04. Thus we can infer that the similarity of these two encrypted images is very small.

To compare the performance of our presented scheme with existing references, Table 5 illustrates the MSE values of encrypted color image Lena in Li and Zhao 2017, Ran et al. 2018 and our scheme. The MSEs of our proposed encrypted image is a little small than the MSEs of schemes in Li and Zhao 2017, Ran et al. 2018.

5.2.2 Correlation between adjacent pixels

Correlation Coefficient (CC) reflects the degree of similarity between two variables. Suppose that *x, y* are the grayscale values of adjacent pixels set. Then, the correlation coefficient between *x* and *y* is defined as:

Table 6 Correlation coefficients of the original grayscale images

CC Images	Three different directions		
	Horizontal	Vertical	Diagonal
Lena	0.9069	0.9480	0.9226
Cameraman	0.9445	0.9210	0.8291

$$CC_{XY} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} = \frac{\frac{1}{n}\sum_{i=1}^{n}\left[\left(x_i - E(x)\right)\left(y_i - E(y)\right)\right]}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i - E(x)\right)^2 \frac{1}{n}\sum_{i=1}^{n}\left(y_i - E(y)\right)^2}} \quad (43)$$

where $E(x) = 1/n\sum_{i=1}^{n} x_i$ and $E(y) = 1/n\sum_{i=1}^{n} y_i$ are the mean of two variables *x* and *y*, respectively. *cov(x,y)* is called the covariance of two variables *x* and *y*, and *D(x)* and *D(y)* are the variance of two variables *x* and *y,* respectively.

An effective image encryption algorithm should produce the encrypted image with sufficiently low correlation in horizontal, vertical and diagonal directions. Generally, the CC of original image in three directions (i.e., vertical, horizontal and diagonal) is close to 1 because each two pixels within image are highly correlated to each other. On the contrary, the CC of an encrypted image should be close to 0. To calculate the CC of original image and corresponding encrypted image, 8000 pairs of two adjacent pixels from horizontal, vertical and diagonal directions, are randomly

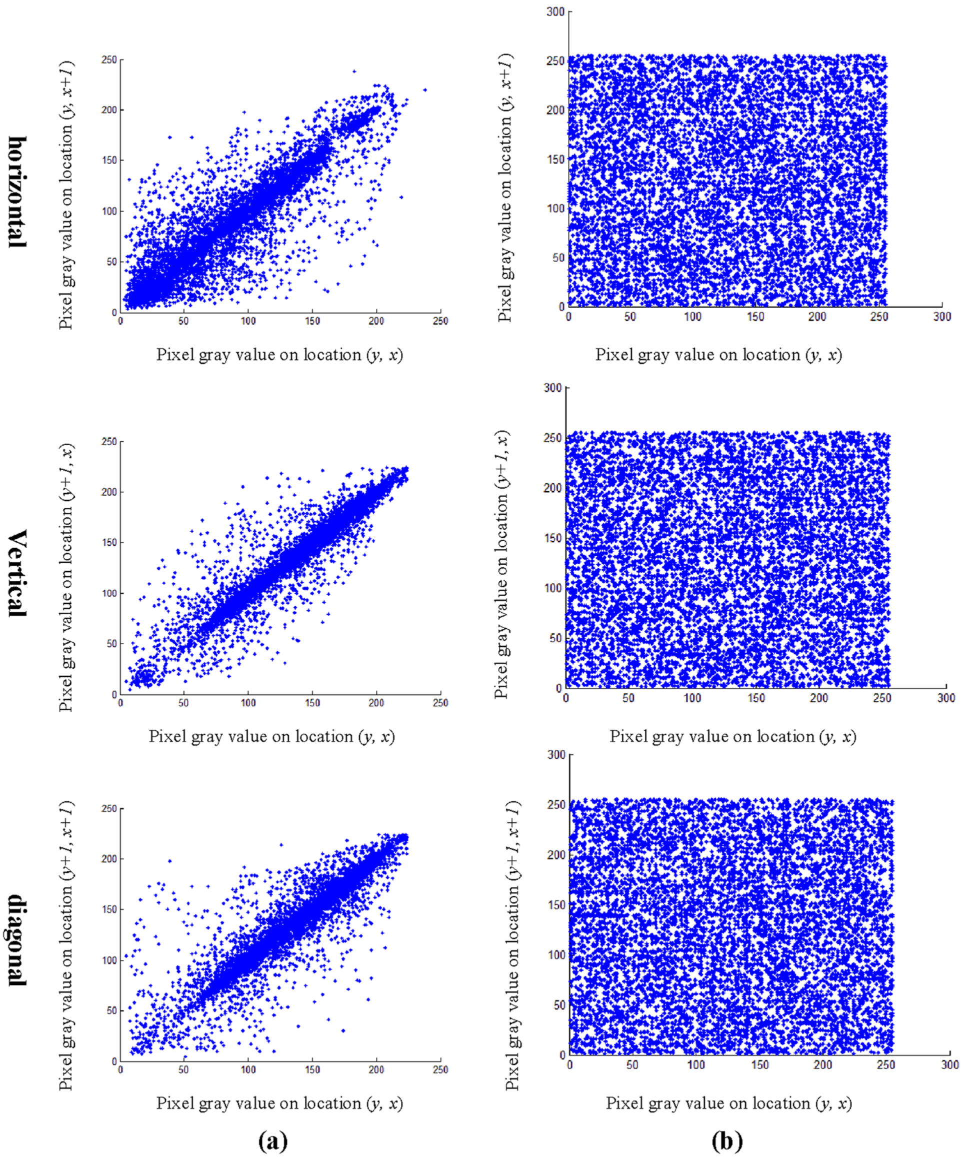
Table 7 Correlation coefficients of the encrypted color images

CC Images	Encrypted images under different initial values	Three different directions		
		Horizontal	Vertical	Diagonal
Lena	[4, 2, 0.65, 3.75]	0.0150	– 0.0169	0.0121
	[4, 2, 0.65, 3.85]	– 0.0007	0.0056	– 0.0041
	[4, 2, 0.70, 3.75]	– 0.0043	– 0.0125	0.0064
	[4, 2, 0.70, 3.85]	0.0003	– 0.0041	0.0119
Cameraman	[4, 2, 0.65, 3.75]	– 0.0166	– 0.0027	0.0043
	[4, 2, 0.65, 3.85]	– 0.0048	0.0005	0.0093
	[4, 2, 0.70, 3.75]	0.0129	– 0.0104	– 0.0004
	[4, 2, 0.70, 3.85]	0.0147	– 0.0080	0.0127

choose, respectively. Table 6 illustrates the CCs of original images Lena and Cameraman in three directions, which is all close to 1. Table 7 gives the CCs of encrypted grayscale images under different initial values in three directions which are all close to zero. Apparently, on the basis of specific values shown in Tables 6 and 7, it is easily to find that the correlation between the adjacent pixels in original image is very strong while in encrypted image are almost irrelevant. So that there is no information obtained about the original image by analysis the correlations of neighborhood pixels in encrypted image.

To present the intuitive visual effects, Figs. 28 and 29 show the comparison of correlation distributions of two adjacent pixels in three directions between the original grayscale images and encrypted versions. Herein, images are encrypted under four initial values [4, 2, 0.65, 3.85]. Obviously, it is also clear from Figs. 28 and 29 that the correlation between the adjacent pixels in the original image is very strong and adjacent pixels in the encrypted image are almost irrelevant.

Fig. 28 Correlation distributions between two adjacent pixels in three directions: **(a)** image Lena and **(b)** encrypted image Lena



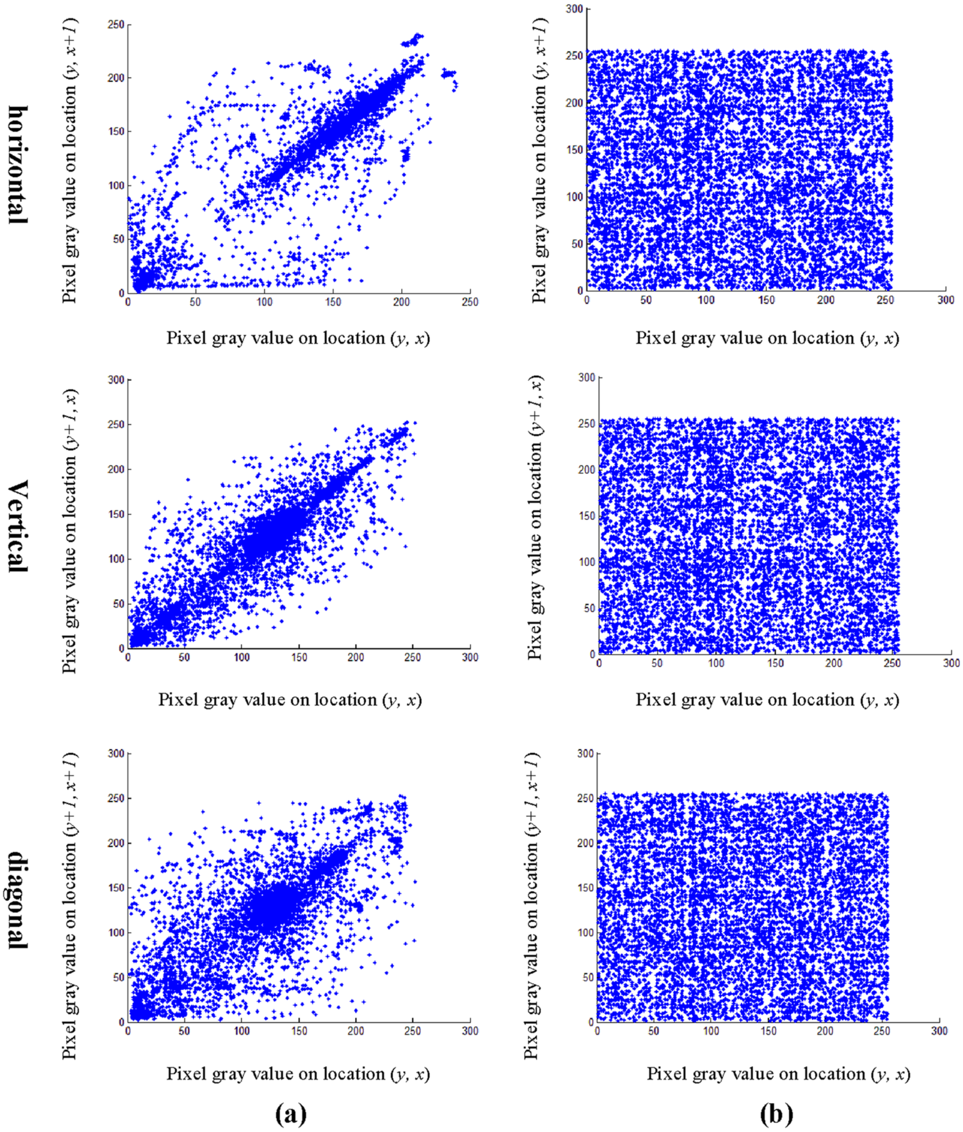


Fig. 29 Correlation distributions between two adjacent pixels in three directions: **(a)** image Cameraman and **(b)** encrypted image Cameraman

5.2.3 Information entropy

Information Entropy (IE) is a statistical measure of uncertainty feature of the image. The computing formula of information entropy $H(s)$ for message source is defined as:

$$H(s) = -\sum_{i=0}^{2^n-1} p(s_i)\log_2 p(s_i) \tag{44}$$

where $p(s_i)$ represents the probability of the occurrence of symbol s_i, and the ideal entropy value for an encrypted grayscale image should be 8 bits in ideal conditions. In another words, if the gray values of an image are distributed more even, and then the entropy value is closer to the ideal value 8 to resist the entropy attacks.

The information entropy of original grayscale images Lena, Cameraman and their corresponding encrypted versions is listed in Table 8. From the results of statistics, the loss in the processing of information encryption is completely weak. Thus, the proposed scheme is stable and secure against entropy attack.

5.3 Security analysis

5.3.1 Histogram

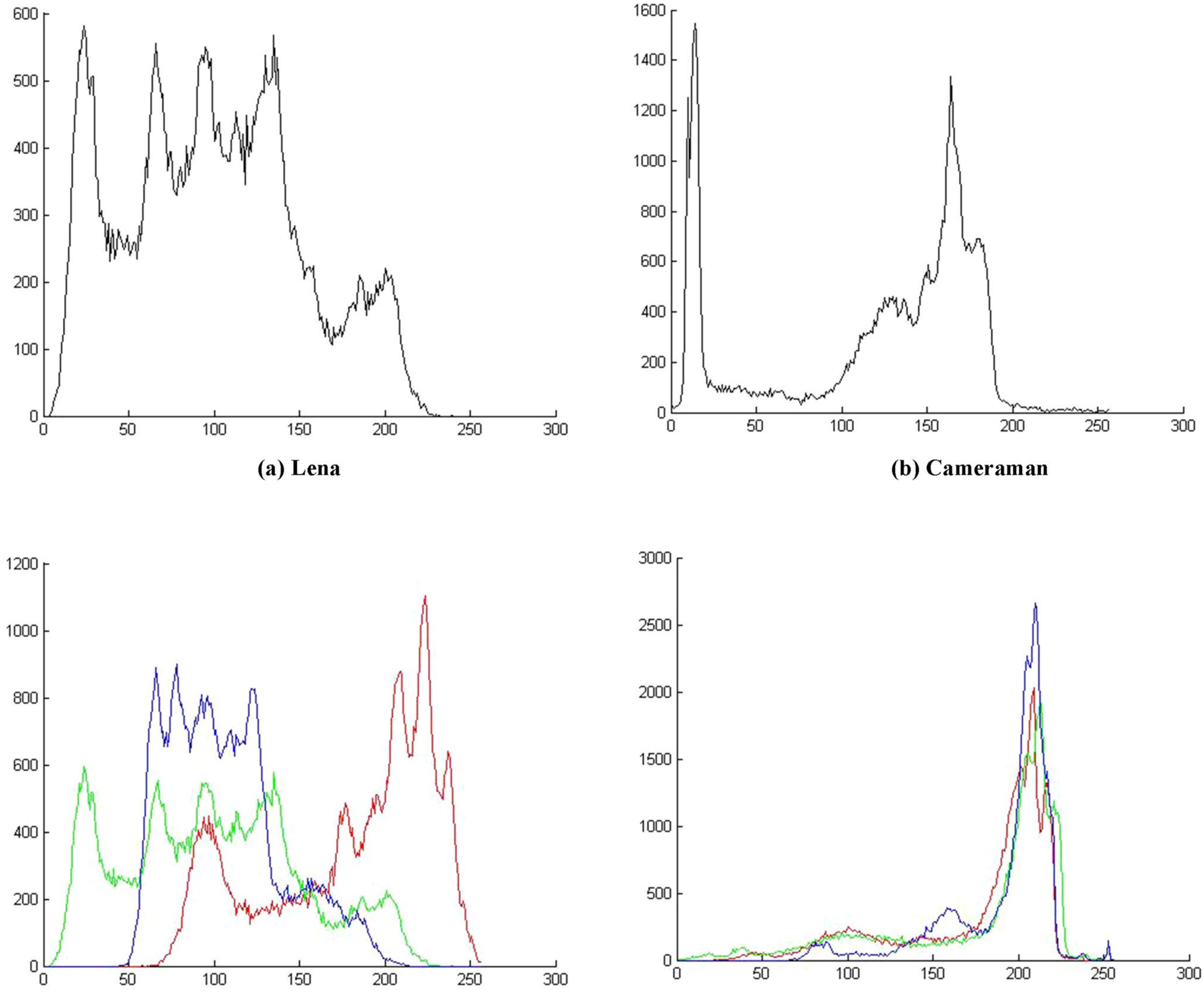
Image histogram reflects the distribution of an image's pixel gray value, which is an essential merit to assess the performance of any image encryption algorithm. A good secure

Table 8 Information entropy of the original and encrypted images (bit)

IEs Images	Original images	Encrypted images under different initial values			
		[4, 2, 0.65, 3.75]	[4, 2, 0.65, 3.85]	[4, 2, 0.70, 3.75]	[4, 2, 0.70, 3.85]
Lena	7.5683	7.9881	7.9535	7.9875	7.9555
Cameraman	7.0486	7.9831	7.9224	7.9809	7.9220

encryption algorithm should guarantee that the histograms of encrypted images are completely different to histograms of original versions. Figure 30 illustrates the histogram of original plain images, i.e., grayscale images Lena and Cameraman in first row, and color images Lena and Airplane in three channels (Red, Green and Blue) in second row.

Figures 31 and 32 respectively demonstrate the histograms of encrypted images based on our presented scheme. Obviously, the histogram of the encrypted grayscale images Lena and Cameraman (shown in Fig. 31) are totally a different distribution forms compared to the original versions as well as the histogram of encrypted color images Lena and Airplane (shown in Fig. 32). Furthermore, under different initial values of Logistic map for generating the secret key image, the histogram graphs are also very similar to each other. Therefore, we can conclude that there is no similarity in terms of histograms between the plain images and the encrypted versions.



(a) Lena

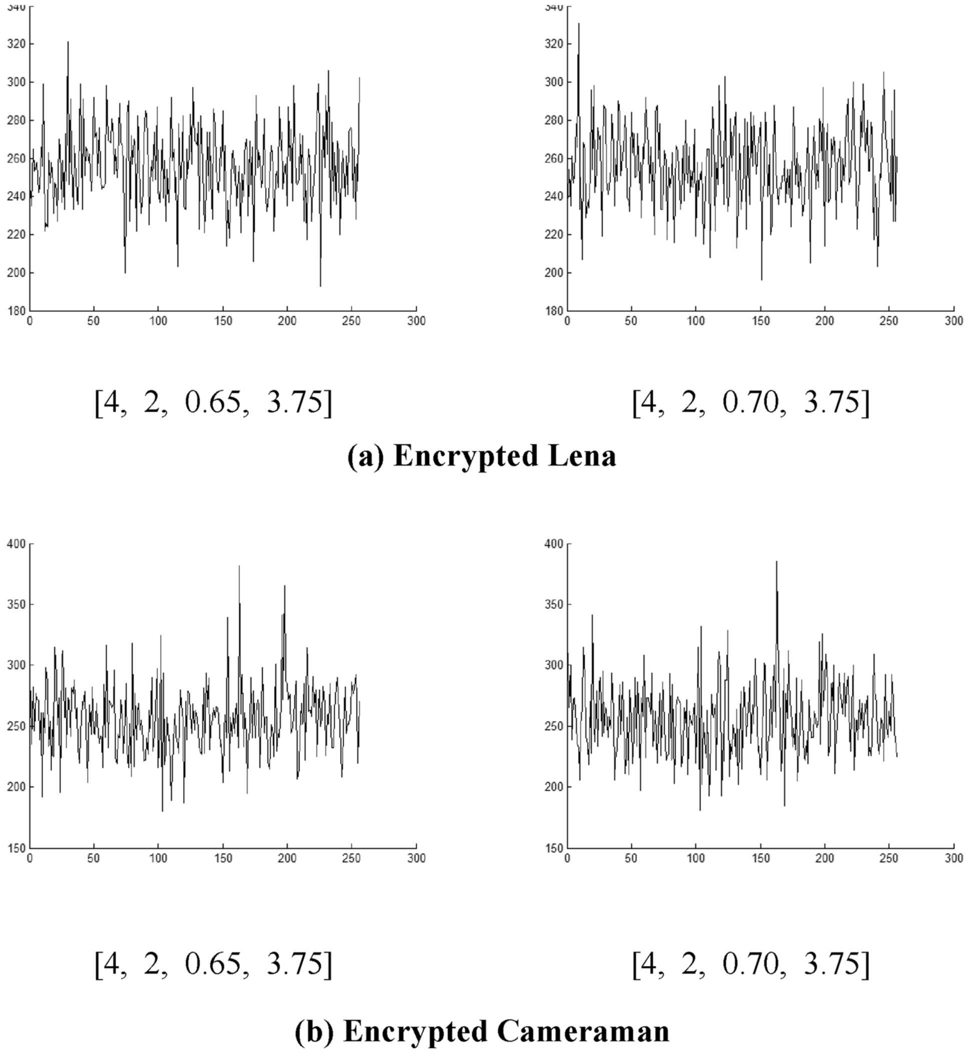
(b) Cameraman

(c) Lena

(d) Airplane

Fig. 30 Histograms of tested images shown in Fig. 25

Fig. 31 Histograms of encrypted grayscale images under the specific keys



[4, 2, 0.65, 3.75] [4, 2, 0.70, 3.75]

(a) Encrypted Lena

[4, 2, 0.65, 3.75] [4, 2, 0.70, 3.75]

(b) Encrypted Cameraman

5.3.2 Key analysis

Key space is the number of different keys can be used to encrypt the plain image. Key sensitivity is known as the sensitivity of the secret key to decrypt effect, which ensures that one cannot obtain any useful information from the decrypted image when a tiny change occurs to the keys. Large key space plus sensitive key are the essential property for good image encryption algorithm, which can stand up to the brute-force attack.

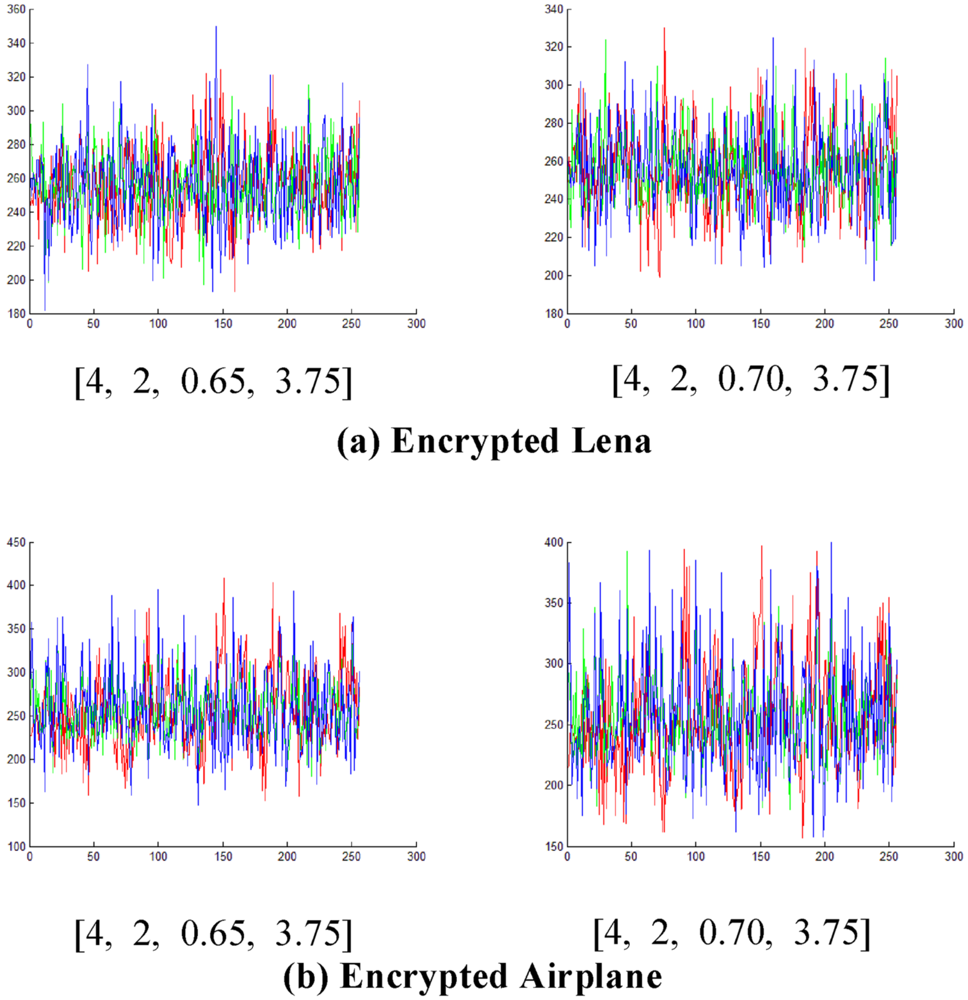
The proposed quantum scheme has four initial values: k_1, k_2,x_0 and μ. Wherein, positive integer k_1 and k_2 respectively denote the iteration times of generally Arnold transform implemented on plain image pixel's coordinate and color information. Keys x_0 and μ are real numbers that belong to the initial values of Logistic map under condition of $0 < x_0 < 1,\ \ 3.56 < \mu \leq 4$. Thus the total key space can be deduced as:

$$k_1 \times k_2 \times c_1 \times c_2 \rightarrow \propto \qquad (45)$$

where positive integers c_1 and c_2 respectively represent the number of real numbers x_0 and μ can be chose in interval of $(0,\ 1)$ and $(3.65,\ 4]$.

To verify our presented quantum scheme has a sensitive key, an example is tested as illustrated in Fig. 33. Herein, the visual effects and corresponding histogram graphs for the encrypted grayscale image Lena under the initial value [4, 2, 0.65, 3.75] are decrypted with the correct key and three different wrong keys [4, 2, 0.65, 3.85], [4, 2, 0.70, 3.75], [4, 2, 0.70, 3.85] demonstrated in Fig. 32. Apparently, the decrypted image with wrong initial keys are total disordered or meaningless, and the corresponding histogram graphs are quite different from its original versions and similar to each other. Thus, it can infer that our presented quantum scheme has a very sensitive key and the plain image can only be decrypted via correct keys.

Fig. 32 Histograms of encrypted color images under specific keys



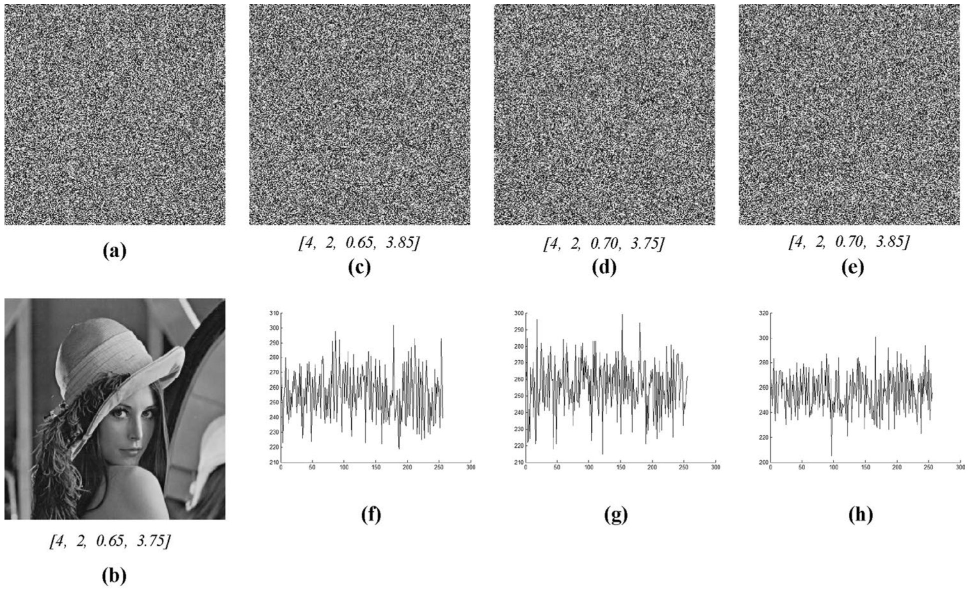
[4, 2, 0.65, 3.75] [4, 2, 0.70, 3.75]

(a) Encrypted Lena

[4, 2, 0.65, 3.75] [4, 2, 0.70, 3.75]

(b) Encrypted Airplane

Fig. 33 Visual effects of decrypted images under correct and wrong initial values: **(a)** is the encrypted grayscale image Lena; **(b)** is the decrypted image under the correct initial values; **(c, d)** and **(f)** are the decrypted Lena images with wrong initial values as text shown; **(f, g)** and **(h)** are the corresponding histogram graphs of decrypted Lena images **(c, d)** and **(e)**, respectively


(a)

[4, 2, 0.65, 3.85]
(c)

[4, 2, 0.70, 3.75]
(d)

[4, 2, 0.70, 3.85]
(e)

[4, 2, 0.65, 3.75]
(b)

(f) **(g)** **(h)**

6 Conclusions

Based on chaos theory of the generalized Arnold transform and Logistic map, a two-stage quantum image encryption algorithm is investigated in this paper. In stage 1, twice scrambling operation based on generalized Arnold transform is proposed. Following that, according to the quantum key image generated and prepared via Logistic map, the CNOT operations, bit-plane scrambling and controlled perfect shuffle permutations are executed in orderly to encrypt the pixel gray value of the scrambled image. Both quantum cost and time complexity of the quantum implementation circuits are O(n) for a $2^n \times 2^n$ quantum grayscale or color images. Thus, we can infer that the investigated quantum encryption algorithm has an exponential speedup in contrast of classical counterparts with complexity no less than $\mathrm{O}\left(2^{2n}\right)$ for a $2^n \times 2^n$ digital image. Experiments are simulated on the classical computers with MATLAB environment, in which statistical and security analyses indicate that the encrypted images possess good visual effects and high security.

Author contributions All authors contributed to the study conception and design. Quantum image encryption and decryption algorithms as well as corresponding quantum implementation circuits were proposed by W-WH and R-GZ. The experimental results and numerical analysis are performed by SJ, XL and JL. The first draft of the manuscript was written by W-WH and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Appendix 1

For two n-qubit numbers A and B, $(A-B) \mod 2^n$ can be expressed as:

$$(A-B) \mod 2^n = \begin{cases} A-B, & A \geq B \\ 2^n-(B-A), & A<B \end{cases}.$$

Proof 1.1 It is obvious that $(A-B) \mod 2^n = A-B$ when $A \geq B$.

1.2 When $A < B$, it can be verified as follows:

Assume that $\overline{B} = \overline{b}_{n-1}\overline{b}_{n-2} \cdots \overline{b}_1\overline{b}_0$ denotes the inverse code of B, then we can obtain that:

$$\begin{aligned}
&B+\overline{B} \\
&= b_{n-1} \cdot 2^{n-1} + b_{n-2} \cdot 2^{n-2} + \cdots + b_1 \cdot 2^1 + b_0 \cdot 2^0 + \overline{b_{n-1}} \cdot 2^{n-1} \\
&\quad + \overline{b_{n-2}} \cdot 2^{n-2} + \cdots + \overline{b_1} \cdot 2^1 + \overline{b_0} \cdot 2^0 \\
&= \left(b_{n-1} + \overline{b_{n-1}}\right) \cdot 2^{n-1} + \left(b_{n-2} + \overline{b_{n-2}}\right) \cdot 2^{n-2} + \cdots \\
&\quad + \left(b_1 + \overline{b_1}\right) \cdot 2^1 + \left(b_0 + \overline{b_0}\right) \cdot 2^0 \\
&= 2^{n-1} + 2^{n-2} + \cdots + 2^1 + 2^0 \\
&= 2^n - 1.
\end{aligned}$$

Thus, $-B = (\overline{B}+1) - 2^n$, $\overline{B}+1 = 2^n - B$, and $(A-B) \mod 2^n$ can be deduced as follows:

$$\begin{aligned}
&(A-B) \mod 2^n \\
&= [A+(-B)] \mod 2^n = \left[A + \left(\overline{B}+1\right) - 2^n\right] \mod 2^n \\
&= \left[A + \left(\overline{B}+1\right)\right] \mod 2^n = \left[A + (2^n - B)\right] \mod 2^n \\
&= \left[2^n - (B-A)\right] \mod 2^n.
\end{aligned}$$

Since $A < B \Rightarrow [2^n - (B-A)] < 2^n$, we can obtain that:

$$\left[2^n - (B-A)\right] \mod 2^n = 2^n - (B-A),\ A < B. \qquad \square$$

References

Arnold, V.I., Avez, A.: Ergodic Problems of Classical Mechanics. Benjamin, New York (1968)

Barenco, A., Bennett, C.H., Cleve, R., et al.: Elementary gates for quantum computation. Phys. Rev. A. **52**, 3457–3488 (1995)

Dyson, F.J., Falk, H.: Period of a discrete cat mapping. Am. Math. Mon. **99**, 603–614 (1992)

Feynman, R.P.: Simulating physics with quantum computers. Int. J. Theor. Phys. **21**, 467–488 (1982)

Iliyasu, A.M.: Towards realising secure and efficient image and video processing applications on quantum computers. Entropy. **15**, 2874–2974 (2013)

Jiang, N., Dong, X., Hu, H., et al.: Quantum image encryption based on henon mapping. Int. J. Theor. Phys. **58**, 979–991 (2019)

Jiang, N., Wang, L., Wu, W.Y.: Quantum hilbert image scrambling. Int. J. Theor. Phys. **53**, 2463–2484 (2014a)

Jiang, N., Wang, L.: Analysis and improvement of the quantum Arnold image scrambling. Quantum Inf. Process. **13**, 1545–1551 (2014)

Jiang, N., Wu, W.Y., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling. Quantum Inf. Process. **13**, 1223–1236 (2014b)

Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**, 63–84 (2011)

Li, H.S., Li, C.Y., Chen, X., Xia, H.Y.: Quantum image encryption algorithm based on NASS. Int. J. Theor. Phys. **57**, 3745–3760 (2018a)

Li, H.S., Chen, X., Song, S.X., et al.: A block-based quantum image scrambling for GNEQR. IEEE Access. **7**, 138233–138243 (2019a)

Li, H.S., Chen, X., Xia, H.Y., et al.: A Quantum Image Representation Based on Bitplanes. IEEE Access **6**, 62396–62404 (2018)

Li, H.S., Fan, P., Xia, H.Y., et al.: Quantum Implementation Circuits of Quantum Signal Representation and Type Conversion. IEEE Trans Circuits Syst. I Regul. Pap. **66**, 341–354 (2019b)

Li, H.S., Fan, P., Xia, H.Y., et al.: The multi-level and multi-dimensional quantum wavelet packet transforms. Sci. Rep. **8**, 1–23 (2018c)

Li, H.S., Fan, P., Xia, H.Y., Song, S.: Quantum multi-level wavelet transforms. Inf. Sci. **504**, 113–135 (2019c)

Li, H.S., Zhu, Q.X., Zhou, R.G., et al.: Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases. Inf. Sci. **273**, 212–232 (2014)

Li L., Bassem Abd-El-Atty A.A.A.E., Ahmed G.: Quantum color image encryption based on multiple discrete chaotic systems. In: 2017 Federated Conference on Computer Science and Information Systems (2017)

Li, P., Zhao, Y.: A simple encryption algorithm for quantum color image. Int. J. Theor. Phys. **56**(6), 1961–1982 (2017)

Liang, H.R., Tao, X.Y., Zhou, N.R.: Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf. Process. **15**, 2701–2724 (2016)

Jafarizadeh, M.A., Behnia, S.: Hierarchy of chaotic maps with an invariant measure and their coupling. Phys. D Nonlinear Phenom. **159**, 1–21 (2001)

Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

Ran, Q.W., Wang, L., Ma, J., et al.: A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections. Quantum Inf. Process. **17**, 188 (2018)

Sang, J.Z., Wang, S., Li, Q.: A novel quantum representation of color digital images. Quantum Inf. Process. **16**, 42 (2017)

Stajic, J.: The future of quantum information processing. Science **339**, 1163 (2013)

Tan, R.C., Lei, T., Zhao, Q.M., et al.: Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. Int. J. Theor. Phys. **55**, 5368–5384 (2016)

Vedral, V., Barenco, A., Ekert, A.: Quantum networks for elementary arithmetic operations. Phys. Rev. A **54**, 147 (1996)

Venegas-Andraca S. B.S.: Storing, processing, and retrieving an image using quantum mechanics, In: Proceedings of SPIE Conference of Quantum Information and Computation. pp. 134–147 (2003)

Wang, L., Ran, Q., Ma, J., et al.: QRCI: a new quantum representation model of color digital images. Opt. Commun. **438**, 147–158 (2019)

Yan, F., Iliyasu, A.M., Le, P.Q.: Quantum image processing: a review of advances in its security technologies. Int. J. Quantum Inf. **15**, 1730001 (2017)

Yan, F., Iliyasu, A.M., Venegas-Andraca, S.E.: A survey of quantum image representations. Quantum Inf. Process. **15**, 1–35 (2016)

Yang, Y.G., Jia, X., Sun, S.J., Pan, Q.X.: Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. Inf. Sci. **277**, 445–457 (2014)

Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf. Process. **12**, 3477–3493 (2013)

Zhang, Y., Lu, K., Gao, Y., Wang, M.: NEQR: a novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**(8), 2833–2860 (2013a)

Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log-polar images. Quantum Inf. Process. **12**, 3103–3126 (2013b)

Zhou, N.R., Chen, W.W., Yan, X.Y., Wang, Y.Q.: Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf. Process. **17**, 137 (2018)

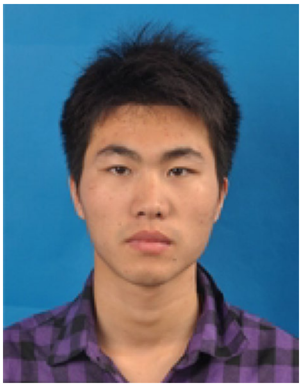
Zhou, N.R., Hua, T.X., Gong, L.H., et al.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process. **14**, 1193–1213 (2015)

Zhou, R.G., Hu, W.W., Fan, P.: Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Inf. Process. **16**, 212 (2017)

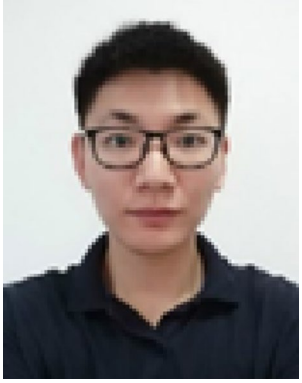
Wen-Wen Hu received the B.S. degree in mathematics and computer from Wuyi University, Fujian, China, in 2015, and the M.S. degree in computer application technology at East China Jiaotong University, Nanchang, Jiangxi, China, in 2018. At present, he is a doctoral student of Shanghai Maritime University, Shanghai, China, pursuing the Ph. D. degree in Information System. His research interests include the quantum information processing, quantum communication, digital image processing, quantum image processing.

Ri-Gui Zhou (M'12) was born on March 2, 1973. He received a B.S. degree from Shandong University, China, in 1997; an M.S. degree from the department of Computer Science and Technology of Nanchang Hangkong University, China, in 2003; and a Ph.D. degree from the department of Computer Science and Technology of Nanjing University of Aeronautics and Astronauts, China, in 2007.From 2008 to 2010, he was a Postdoctoral Fellow in Tsinghua University, China. From 2010 to 2011, he was a Postdoctoral Fellow in Carleton University, Ottawa, Canada. From 2014 to 2015, he was a Visiting Scholar at North Carolina State University, Raleigh, NC, USA. He is currently a Professor with the College of Information Engineering, Shanghai Maritime University, China. His main research interests include quantum image processing, quantum reversible logic and the quantum genetic algorithm, among others.Prof. Zhou is a senior member of the China Computer Federation (CCF) and the recipient of the New Century Excellent Talents program, Ministry of Education of China, in 2013.

She-Xiang Jiang received the M.S. degree in computer application technology at Anhui University of Science & Technology, Huainan, Anhui, China, in 2008. Currently, he is pursuing the Ph.D. degree in information system at Shanghai Maritime University, Shanghai, China. His research interests include quantum image processing, quantum communication, quantum teleportation and remote state preparation.



XingAo Liu received the B.S. degree from Nanjing University of Posts and Telecommunications in 2015. Currently, he is working toward his Ph.D. degree in information system at Shanghai Maritime University, Shanghai, China. His research interests include quantum information processing, quantum image processing, etc.



Jia Luo received the B.S. degree in information management and information system from the Shanghai Maritime University in 2016. He is currently pursuing the Ph.D. degree in information system at Shanghai Maritime University, China. His research interests include the quantum cryptography and quantum image processing.