IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 1, 2019, accepted April 27, 2019, date of publication April 30, 2019, date of current version May 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914184

Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model

XINGBIN LIU[1,2], DI XIAO[1], WEI HUANG[2], AND CONG LIU[3]

[1]College of Computer Science, Chongqing University, Chongqing 400044, China
[2]Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China
[3]Southwest Technology and Engineering Research Institute, Chongqing 40039, China

Corresponding author: Xingbin Liu (xbliu6@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802037, Grant 61702061, Grant 61572089, Grant 61771439, and Grant 61702469, in part by the China Postdoctoral Science Foundation under Grant 2018m640899, in part by the Chongqing Special Postdoctoral Science Foundation under Grant XmT2018032, in part by the Chongqing Research Program of Basic Research and Frontier Technology under Grant cstc2017jcyjBX0008, in part by the Chongqing Postgraduate Education Reform Project under Grant yjg183018, in part by the Chongqing University Postgraduate Education Reform Project under Grant cquyjg18219, in part by the Fundamental Research Funds for the Central Universities under Grant 106112017CDJQJ188830 and Grant 106112017CDJXY180005, and in part by the National Cryptography Development Fund under Grant MMJJ20170120.

ABSTRACT Quantum image encryption is an emerging technology for efficiently protecting visual information. A quantum block image encryption scheme is designed based on quantum Arnold transform (QArT) and lately proposed sine chaotification model (SCM) in this paper. First, in order to flexibly manipulate image blocks, a quantum block image representation (QBIR) model for block image is proposed, which encodes pixel gray values and position information of image blocks into two entangled qubit sequences. Then, QArT is applied to scramble the positions of image blocks. The final ciphertext image is obtained by quantum xor operations, which is completed with a pseudorandom sequence generated from SCM. The introduction of SCM dramatically enlarges the key space to resist brute-force attack. Moreover, the generated sequence is dependent on the original image to resist the chosen-plaintext attack. The main quantum circuits are given and the numerical simulation results demonstrate that the proposed quantum image encryption scheme is valid and reliable for quantum image protection in terms of security and computational complexity.

INDEX TERMS Quantum image representation, quantum image encryption, quantum Arnold transform, sine chaotification model, XOR operation.

I. INTRODUCTION

Due to the rapid development of information and multimedia technologies, guaranteeing the security of data storage and transmission has become increasingly important [1]–[3]. As the digital image is an important carrier of information, traditional cryptographic algorithms for protecting digital images have been intensively studied [4]–[6]. Among the proposed novel image encryption algorithms, various chaotic systems are widely used. Chai *et al.* used the memristive hyperchaotic system and a four-wing hyperchaotic system to encrypt images and obtained good encryption results [7]–[9]. Wang *et al.* proposed several novel image encryption algorithms based on one-time keys [10], bit-level permutation [11], DNA complementary rule [12] and perceptron model [13] by combining with the chaotic maps, which are robust and can resist known attacks. In addition, compressive sensing and sparse representation are also introduced in the field of traditional image encryption and they improve the efficiency of cryptographic algorithms [14], [15]. Although the mentioned traditional algorithms performance good in the protection of vital data, the efficiency and security of which are less than quantum image encryption algorithms. At present, little research has been done in the promising area of quantum image encryption as it is a burgeoning research direction [16]–[19].

The parallel computation methods generally improve the efficiency when the data volume to be processed is large. For example, Wang *et al.* proposed a fast image encryption algorithm by using parallel diffusion method [20], which greatly improves the encryption efficiency. Quantum computation exploits superposition and entanglement principles of

The associate editor coordinating the review of this manuscript and approving it for publication was Ludovico Minati.

quantum mechanics to perform parallel computation, which is more efficient for solving large scale and real-time problem than its classical counterpart. Quantum image processing attracts much attention of researchers since the pioneer works done by Shor on factorization of large numbers [21] and Grover on searching algorithm [22].

The initial task of storing and processing digital images in quantum computers is to construct a suitable representation model. To date, several quantum image representation methods have been proposed to efficiently complete different quantum image processing applications [23]–[27], among which the flexible representation for quantum images model (FRQI) [26] and the novel enhanced quantum representation model (NEQR) [27] are widely applied. The FRQI model utilizes a normalized superposition state to represent gray scale information and position information, while the NEQR model improves the representation of gray information by using basis state of qubits sequences. Although the NEQR needs more qubits to represent the same image, the original information can be accurately and easily recovered.

With the help of multiple quantum image representation models, several image encryption algorithms aimed to secure quantum information have been proposed [28]–[30]. Li and Zhao devised a simple quantum color image encryption algorithm by using controlled rotation gates to transform basic state into balanced superposition state [31]. Yang *et al.* realized quantum image encryption in quantum Fourier domain by using double random phase encoding technique [32]. Song *et al.* used restricted geometric and color transformations to realize permutation and diffusion of quantum images [33]. In quantum discrete cosine transform domain, an image compression-encryption scheme is proposed, which has high security and large key space [34]. Li *et al.* proposed a quantum image encryption scheme by devising normal arbitrary superposition state model [35]. In addition, chaotic systems are widely used in quantum image encryption schemes as they have high efficiency and the keys are easy to distribute. For instance, Ran *et al.* proposed a quantum image encryption method by generating chaotic sequences through injecting three impulse into coupled hyper-chaotic Lorenz system [36]. Based on quantum 3D Arnold transform and Zhongtang chaotic system, Zhou *et al.* suggested a multiple image encryption scheme [37]. Zhou *et al.* also proposed a quantum image encryption algorithm based on a 5D hyper-chaotic system and quantum cross-exchange operation, which improves efficiency and security [38].

Generally, to against unauthorized attacks and enhance security, image scrambling methods are adopted in quantum image encryption algorithms to transform a meaningful image into a disordered one. Jiang *et al.* extended popular traditional image scrambling techniques, such as Arnold, Fibonacci and Hilbert transforms [39], [40], to the quantum image processing field based on FRQI. Zhou *et al.* investigated a gray-code scrambling method to disorder pixels under the representation model of NEQR [41]. Recently, Heidari *et al.* proposed a dual quantum image scrambling method, which includes a bit-plane scrambler and a pixel-plane scrambler [42].

These quantum image encryption schemes mentioned above process the image by the least unit of one pixel or one bit. However, if the images to be encrypted are processed with sub-blocks, the efficiency and security will be improved. With consideration of this point, a quantum block image encryption algorithm is proposed in this paper. First of all, a block based quantum image representation model (QBIR) derived from NEQR is proposed, and the images to be encrypted are divided to sub-blocks. Next the quantum Arnold transform (QArT) is applied to the obtained sub-blocks, which scrambles the order of sub-blocks. Then a key image is generated by using recently proposed sine chaotification model (SCM). Finally, the encrypted quantum image is obtained by XOR operation between the key image and scrambled blocks. The decryption is exactly the inverse process of encryption. The original images can be accurately retrieved with correct keys and quantum measurement. Through introducing SCM into the field of quantum image encryption, not only the burden of keys transmission is reduced but also the security is improved dramatically as it is sensitive to initial values and has a large value range. Moreover, the generated key image is dependent on the original image to resist the chosen-plaintext attack. Numerical simulation results show that the proposed method is effective in protecting quantum images and the security is guaranteed by statistical analysis, key space analysis and robustness analysis.

The rest of this paper is organized as follows. In next section, some relative fundamental theories are briefly introduced, such as NEQR model, QArT, and SCM. The proposed block quantum image encryption scheme is described in Sec. III in detail, including the preparation of QBIR, encryption scheme and decryption scheme. The Sec. IV gives the numerical results and the theoretical security analysis is reported. Finally, conclusion is drawn in Sec. V.

II. PRELIMINARY KNOWLEDGE

A. NEQR MODEL FOR QUANTUM IMAGE REPRESENTATION

The NEQR model [27] is proposed by Zhang *et al.* in 2013 to represent the digital image with quantum state, which is developed from FRQI model and adopts basic state to store pixel values. For a $2^n \times 2^n$ digital image, the quantum representation using NEQR model can be expressed as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^k-1} \sum_{k=0}^{2^k-1} |C(y,x)\rangle \otimes |yx\rangle \tag{1}$$

where $|yx\rangle$ denotes the vertical position and horizontal position of the corresponding pixel and the binary sequence $|c(y,x)\rangle = \left|c_{yx}^{q-1} c_{yx}^{q-2} \cdots c_{yx}^{1} c_{yx}^{0}\right\rangle$ represents the gray value of the pixel in position (y,x) and the range of gray value

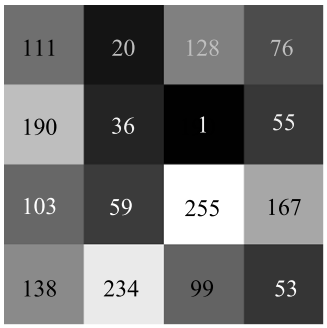


FIGURE 1. The NEQR representation of a 4 × 4 image.

is $\left[0, 2^{q-1}\right]$. Thus, a digital image I is stored into a normalized superposition state $|I\rangle$ with $2n + q$ qubits. An example of 4×4 image is shown in Fig. 1 and the corresponding NEQR representation is written as follows:

$$\begin{aligned}|I\rangle = \frac{1}{4}(&|01101111\rangle \otimes |0000\rangle + |00010100\rangle \otimes |0001\rangle \\ &+ |10000000\rangle \otimes |0010\rangle + |01001100\rangle \otimes |0011\rangle \\ &+ |10111110\rangle \otimes |0100\rangle + |00100100\rangle \otimes |0101\rangle \\ &+ |00000001\rangle \otimes |0110\rangle + |00110111\rangle \otimes |0111\rangle \\ &+ |01100111\rangle \otimes |1000\rangle + |0011011\rangle \otimes |1001\rangle \\ &+ |1111111\rangle\rangle \otimes |1010\rangle + |10100111\rangle \otimes |1011\rangle \\ &+ |10001010\rangle \otimes |1100\rangle + |1101010\rangle \otimes |1101\rangle \\ &+ |01100011\rangle \otimes |1110\rangle + |00110101\rangle \otimes |1111\rangle) \quad (2)\end{aligned}$$

B. QUANTUM ARNOLD TRANSFORM (QArT)

The classical Arnold transform is a two dimensional inverse transform, which is defined as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N), x, y = 0, 1, \ldots, N, \quad (3)$$

where N denotes the size of image to be scrambled. The symbol A is a scrambling matrix and generally it is set to $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. The coordinate information before and after transform is denoted as (x, y) and $\left(x', y'\right)$, respectively.

Therefore, the transform can be rewritten as:

$$\begin{cases} x' = (x + y) \bmod N \\ y' = (x + 2y) \bmod N. \end{cases} \quad (4)$$

It is easy to derive the inverse Arnold transform, which is deduced as follows:

$$\begin{aligned}\begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix} (\text{mod} N) \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} (\text{mod} N), \quad (5)\end{aligned}$$

i.e.,

$$\begin{cases} x = \left(2x' - y'\right) \bmod N \\ y = \left(-x' + y'\right) \bmod N. \end{cases} \quad (6)$$

The Arnold transform utilizes scrambling matrix and modulo operation to scramble image. Recently, Jiang *et al.* extended the classical Arnold transform into the field of quantum image processing. The quantum version of Arnold transform is constructed with quantum plain adder network and adder modulo N network, the detailed information of which is presented in [40]. For quantum image $|I\rangle$, the scrambled image $\left|I'\right\rangle$ can be expressed as:

$$|I'\rangle = \text{QArT}(|I\rangle) = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |C(y, x)\rangle \, \text{QArT}(|yx\rangle) \quad (7)$$

where $\text{QArT}(|yx\rangle) = \text{QArT}(|y\rangle)\, \text{QArT}(|x\rangle)$. The scrambled coordinates can be written as:

$$\begin{cases} |x^1\rangle = \text{QArT}(|x\rangle) = |x + y\rangle \bmod N \\ |y^1\rangle = \text{QArT}(|y\rangle) = |x + 2y\rangle \bmod N. \end{cases} \quad (8)$$

C. SINE CHAOTIFICATION MODEL (SCM)

As the chaotic systems have the characteristics of ergodicity, sensitive to control parameters and initial conditions, they are suitable for designing encryption systems. The common used chaotic systems include logistic map, sine map, tent map, higher order chaotic system and so on, and they are widely used in the applications to protect the security of images. The recently proposed SCM can further enhance the chaos performance of existing chaotic systems through applying a nonlinear sine function to transform the outputs of classical chaotic map into a more complex chaos sequence [43].

The SCM can be expressed as follows:

$$d_{k+1} = \sin\left(\pi f\left(p, d_k\right)\right), \quad (9)$$

where $f\left(p, d_k\right)$ denotes an existing chaotic map and p is the control parameter. The input of SCM is d_k and then the is nonlinear transformed with sine function. The advantage of this model is that it can significantly enlarge the parameter range, therefore it can be applied in encryption system to increase key space.

In this paper, the logistic map defined as follows is selected as the input chaotic map, which can be expressed as:

$$f\left(p, d_k\right) = p d_k \left(1 - d_k\right), \quad d_k \in (0, 1). \quad (10)$$

For original logistic map, the generated sequence is in chaos only if the control parameter p is within the range [3.5699456, 4]. The enhanced logistic map with SCM can be written as:

$$d_{k+1} = \sin\left(\pi p d_k \left(1 - d_k\right)\right), \quad (11)$$

where the control parameter p is in the range $(0, +\infty)$. It can be seen that the range of control parameter p is extremely enlarged if fed the logistic map into SCM. The bifurcation diagrams of logistic map and the enhanced logistic map are shown in Fig. 2. The bifurcation diagram of logistic map with parameter $p \in [1, 4]$ is shown in Fig. 2(a) and the bifurcation diagram of logistic map with parameter $p \in (0, 2000)$ is shown in Fig. 2(b).

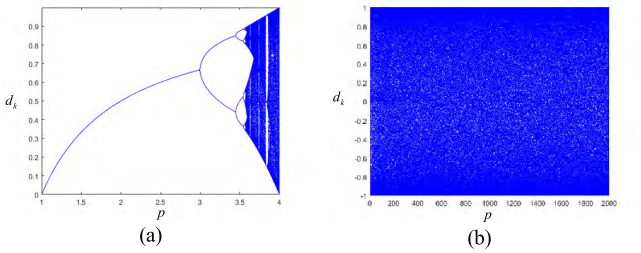


FIGURE 2. Bifurcation diagrams of (a) logistic map and (b) enhanced logistic map.

III. QUANTUM BLOCK IMAGE ENCRYPTION AND DECRYPTION SCHEME

The flowchart of proposed quantum block image encryption scheme is shown in Fig. 3. The original image is first represented with QBIR model and then the sub-blocks of original image are shuffled by the QArT. The final encrypted image is obtained after quantum XOR operations. The decryption process is the inverse of encryption process. More details of the proposed quantum image encryption scheme are presented in the following subsections.

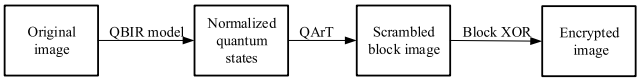


FIGURE 3. The flowchart of proposed quantum block image encryption scheme.

A. QUANTUM BLOCK IMAGE REPRESENTATION AND PREPARATION

The existing quantum image representation models can store the digital image into a quantum computer pixel by pixel efficiently. However, there is still no appropriate model for quantum block image representation. In this subsection, a quantum block image representation model QBIR is proposed and the details of representation and preparation are given.

By referring to the representation method using in NEQR, quantum superposition and basic state are utilized during the design of QBIR. Assume the image to be divided into blocks is denoted as $|I\rangle$, the size of which is $2^n \times 2^n$ and the number of blocks are set to $2^w \times 2^w$. Then the QBIR for image $|I\rangle$ can be expressed as:

$$\begin{aligned}|I\rangle &= \frac{1}{2^n}\frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{x=0}^{n-w}|C(j,t,y,x)\rangle\otimes|jtyx\rangle \\ &= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2-w}\sum_{x=0}^{n-w}|\,c_{jtyx}\,q-1\cdots c^0_{jtyx}\rangle\otimes|jt\rangle\otimes|yx\rangle\end{aligned} \tag{12}$$

where $|jtyx\rangle$ denotes position information. The $|jt\rangle$ represents the position of blocks and $|yx\rangle$ represents the position of pixels in each block. There are $2n+q$ qubits are required to represent an image with size of $2^n \times 2^n$.

FIGURE 4. The QBIR representation of a 4×4 image with 4 blocks.

Take the image shown in Fig. 1 for example, the divided blocks are shown in Fig. 4 and the corresponding QBIR expression is written as follows.

$$\begin{aligned}|I\rangle = \frac{1}{4}(&|01101111\rangle\otimes|0000\rangle+|00010100\rangle\otimes|0001\rangle \\ &+|10111110\rangle\otimes|0010\rangle+|00100100\rangle\otimes|0011\rangle \\ &+|10000000\rangle\otimes|0100\rangle+|01001100\rangle\otimes|0101\rangle \\ &+|00000001\rangle\otimes|0110\rangle+|00110111\rangle\otimes|0111\rangle \\ &+|01100111\rangle\otimes|1000\rangle+|00111011\rangle\otimes|1001\rangle \\ &+|10001010\rangle\otimes|1010\rangle+|1101010\rangle\otimes|1011\rangle \\ &+|11111111\rangle\otimes|1100\rangle+|10100111\rangle\otimes|1101\rangle \\ &+|01100011\rangle\otimes|1110\rangle+|00110101\rangle\otimes|1111\rangle).\end{aligned} \tag{13}$$

The preparation of QBIR is similar to the preparation process of NEQR, and it includes two steps. The first step is to store the position information of blocks and pixels. The identity gate $\mathbf{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$ and two dimensional Hadamard gate $\mathbf{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$ are used to transform the initial quantum state $|0\rangle^{\otimes 2n+q}$ into a superposition state. After the transform composed with $\mathbf{I}^{\otimes q}\mathbf{H}^{\otimes 2n}$, the intermediate state $|M\rangle$ can be expressed as follows.

$$\begin{aligned}|M\rangle &= \mathbf{I}^{\otimes q}\mathbf{H}^{\otimes 2n}\left(|0\rangle^{\otimes 2n+q}\right) \\ &= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{2^{n-w}-1}|0\rangle^{\otimes q}\otimes|jt\rangle\otimes|yx\rangle.\end{aligned} \tag{14}$$

The second step is to set gray information for each pixel. For pixel (Y,X) in (J,T) block, the gray information change operation R_{JTYX} can be defined as follows.

$$\begin{aligned}R_{JTYX} = \mathbf{I}\otimes\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0,jtyx\neq JTYX}^{2^{n-w}-1}&|jtyx\rangle\langle jtyx| \\ &+\Phi_{JTYX}\otimes|jtyx\rangle\langle JTYX|.\end{aligned} \tag{15}$$

where the operator Φ_{JTYX} defined as follows is used to change values of qubits.

$$\Phi_{JTYX}\left(|0\rangle^{\otimes q}\right) = |0\rangle^{\otimes q} \oplus |C(J,T,Y,X)\rangle \tag{16}$$

By utilizing the operation R_{JTYX}, the gray value of pixel (Y,X) in (J,T) block can be changed, the realization process can be described as follows.

$$\begin{aligned}
&R_{\mathrm{ITTX}}(|M\rangle)\\
&= R_{JTYX}\left(\frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n^{n-w}-12}|0\rangle^{\otimes q}|jt\rangle|yx\rangle\right)\\
&= \frac{1}{2^n}\left(\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0,j\ tyx\neq JTYX}^{2^{n-w}-1}|0\rangle^{\otimes q}|jtyx\rangle\right.\\
&\quad\left.+(|0\rangle^{\otimes q}\oplus|C(J,T,Y,X)))|JTYX\rangle\right)\\
&= \frac{1}{2^n}\left(\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0,j\ tyx\neq JTYX}^{2^{n-w}-1}|0\rangle^{\otimes q}|jtyx\rangle\right.\\
&\quad\left.+|C(J,T,Y,X)\rangle|JTYX\rangle\right)
\end{aligned} \tag{17}$$

The procedure described in Eq. (17) can only set gray information of one single pixel, and the gray values of other pixels can be set with the same operation. A total of 2^{2n} operations are needed to prepare an image, and the final quantum state can be obtained with the following operation.

$$\begin{aligned}
&\prod_{j=0}^{2^w-1}\prod_{t=0}^{2^w-1}\prod_{y=0}^{2^{n-w}-1}\prod_{x=0}^{2^{n-w}-1}R_{JTYX}(|M\rangle)\\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{2^{n-w}-1}\Phi_{JTYX}\left(|0\rangle^{\otimes q}\right)\otimes jt|\rangle\otimes|yx\rangle.\\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{2^{n-w}-1}C(j,t,y,x)\otimes|jtyx\rangle
\end{aligned} \tag{18}$$

The quantum circuit for QBIR image is illustrated in Fig. 5. The pixels in first block are shown with control-NOT gates and the other blocks are similar.

B. QArT FOR QBIR IMAGE

The proposed QBIR model encodes the digital image into quantum state block by block, and then the QArT is used to change the position information of blocks. To scramble the image blocks, the qubit sequence $|JT\rangle$ is transformed using QArT for r times. The process of shuffling blocks can be described as follows.

$$\begin{aligned}
|I'\rangle &= \mathrm{QArT}(|I\rangle)\\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{n-w}|C(j,t,y,x)\rangle\,\mathrm{QArT}(|jt\rangle)|yx\rangle
\end{aligned}$$

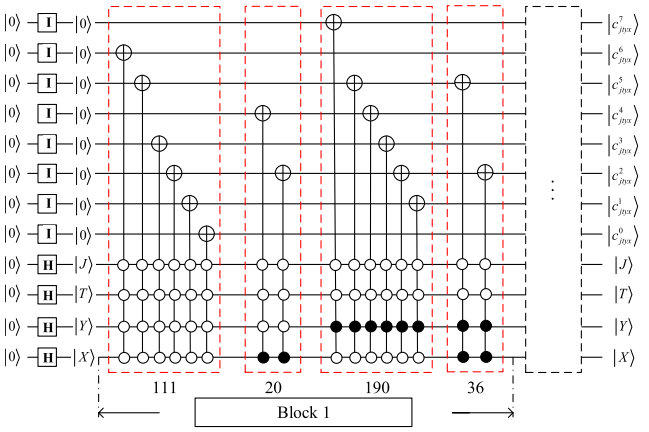


FIGURE 5. Quantum circuit for QBIR image preparation.

$$\begin{aligned}
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{x=0}^{n-w}\Big|_{x=0}^{n-w}|C(j,t,y,x)\rangle|j't'\rangle|yx\rangle\\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{x=0}^{n-w}\Big|_{x=0}^{n-w}|C'(j,t,y,x)\rangle|jt\rangle|yx\rangle,
\end{aligned} \tag{19}$$

where the $\left|j't'\right\rangle$ denotes the position of scrambled blocks.

According to the definition of QArT written in Eq. (8), the $\left|j't'\right\rangle$ can be calculated as:

$$\begin{cases}\left|j'\right\rangle = \mathrm{QArT}(|j\rangle) = |j+t\rangle \bmod 2^w\\ \left|t'\right\rangle = \mathrm{QArT}(|t\rangle) = |j+2t\rangle \bmod 2^w.\end{cases} \tag{20}$$

The inverse QArT can be easily obtained as:

$$\begin{cases}|j\rangle = \mathrm{QArT}^{-1}\left(|j'\rangle\right) = \left(2|j'\rangle - |t'\rangle\right) \bmod 2^w\\ |t\rangle = \mathrm{QArT}^{-1}\left(|t'\rangle\right) = \left(-|j'\rangle + |t'\rangle\right) \bmod 2^w.\end{cases} \tag{21}$$

The corresponding circuits for QArT is shown in Fig. 6, which is constructed with the ADDER module and ADDER-MOD module [40]. Take the image "Peppers" sized 512×512 as example, the scrambled images with block sized 16×16 and 8×8 are shown in Fig. 7(b) and Fig. 7(d), respectively. It can be seen that the position information of blocks is thoroughly scrambled and the original information cannot be obtained.

C. XOR DIFFUSION

After the position information of blocks are permutated with QArT, the gray values of blocks are also needed to be changed. In this stage, quantum XOR diffusion operation is performed to modify the gray information of all the blocks.

By utilizing the chaotic characteristic of SCM, a 2^{2n} pseudorandom sequence can be generated with Eq. (9). To resist chosen-plaintext attacks, the initial value d_0 is determined by

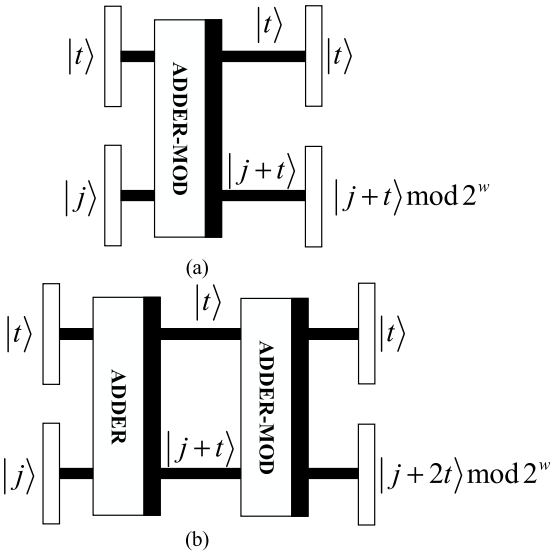


FIGURE 6. The block scrambling circuits for (a) $|j'\rangle$ and (b) $|t'\rangle$.

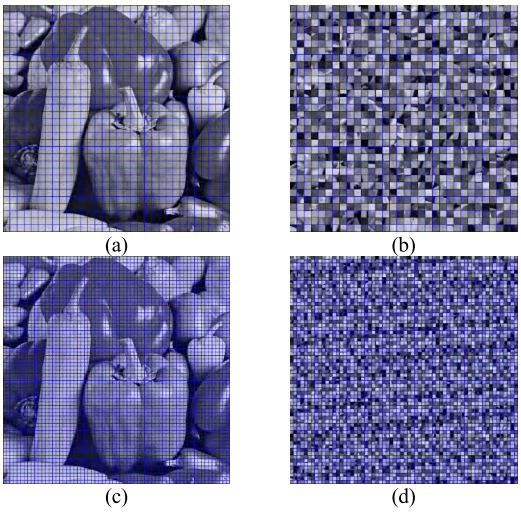


FIGURE 7. The scrambling effect of QArT for block images.

the image to be encrypted, which is calculated as:

$$d_0 = \frac{\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{2^{n-w}-1} C(j,t,y,x)}{2^{q+2n}}. \tag{22}$$

Though setting control parameter p and inputting the initial value d_0 into SCM, a sequence $\{s(l) \in (0,1), l = 1, 2\cdots 2^{2n}\}$ is obtained. Then turn the elements of sequence $\{s(l)\}$ into integer by using the following equation.

$$S(l) = \text{floor}\left(s(l) \times 10^{14}\right) \bmod \left(2^q + 1\right), \tag{23}$$

where the function floor $(\cdot)$ denotes rounded down operation.

The final ciphertext $|E\rangle$ can be obtained by performing XOR operation between scrambled quantum block image $\left|I'\right\rangle$ and pseudorandom sequence S. The sequence S can be transformed into a key image $|S\rangle$ according to Eq. (14)-(18), the block division of which is same as the original block image. The diffusion process is described as

$$\begin{aligned}
|E\rangle &= |I'\rangle \oplus |S\rangle \\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{n-w}|C'(j,t,y,x)\rangle|jtyx\rangle \\
&\oplus \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{y=0}^{n-w}|S(j,t,y,x)\rangle|jtyx\rangle \\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{x=0}^{n-w}|C'(j,t,y,x) \\
&\oplus S(j,t,y,x)\rangle|jtyx\rangle.
\end{aligned} \tag{24}$$

D. QUANTUM BLOCK IMAGE DECRYPTION SCHEME

The original image can be decrypted with inverse process of encryption, and the flowchart of decryption is illustrated in Fig. 8. The details are described as follows.

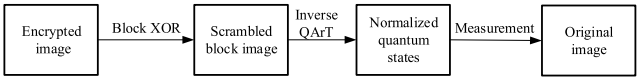


FIGURE 8. The flowchart of quantum block image decryption scheme.

Firstly, the encrypted image $|E\rangle$ is XORed with key image $|S\rangle$ generated with the same parameters as in encryption. Thus the scrambled quantum block image $\left|I'\right\rangle$ is obtained.

$$\left|I'\right\rangle = |E\rangle \oplus |S\rangle. \tag{25}$$

Then the inverse QArT expressed in Eq. (21) performs on the scrambled quantum block image $\left|I'\right\rangle$ and the original block image $|I\rangle$ is obtained.

$$\begin{aligned}
&|I\rangle \\
&= \text{QArT}^{-1}\left(|I'\rangle\right) \\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{2^{n-w}-1}\sum_{x=0}^{n-w}|C(j,t,y,x)\rangle\,\text{QArT}^{-1}\left(|j't'\rangle\right)|yx\rangle. \\
&= \frac{1}{2^n}\sum_{j=0}^{2^w-1}\sum_{t=0}^{2^w-1}\sum_{y=0}^{n-w}\sum_{x=0}^{n-w}|C(j,t,y,x)\rangle|jt\rangle|yx\rangle
\end{aligned} \tag{26}$$

IV. NUMERICAL SIMULATIONS AND THEORETICAL ANALYSIS

Since there is no quantum hardware to store and manipulate quantum image at present, the numerical simulation experiments are performed with MATLB on a classical computer. The quantum operations can be simulated by unitary matrices, and the quantum states can be represented with complex vectors. The keys in the proposed scheme include the control parameter and the initial value d_0 of SCM, and the iteration number of QArT. In the experiments, the parameters are set as: $p = 10000$, $r = 10$. The block size is set to 4×4. Six original images sized 256×256 and corresponding ciphertext

images are shown in Fig. 9. It can be seen that any of the original information cannot be recognized in the ciphertext image, which verifies the encryption scheme is effective.

A. HISTOGRAM ANALYSIS

As the image is composed of pixels with different gray values, the distribution of gray values is an important statistical feature. Histogram can intuitively reflect the gray value distribution. To resist statistical attack, the histogram of ciphertext image should be uniform. The histograms of original images and corresponding ciphertext images shown in Fig. 9 are illustrated in Fig. 10. Although the histograms of original images are totally different, the histograms of ciphertext images are relatively uniform distributed and are similar to each other.

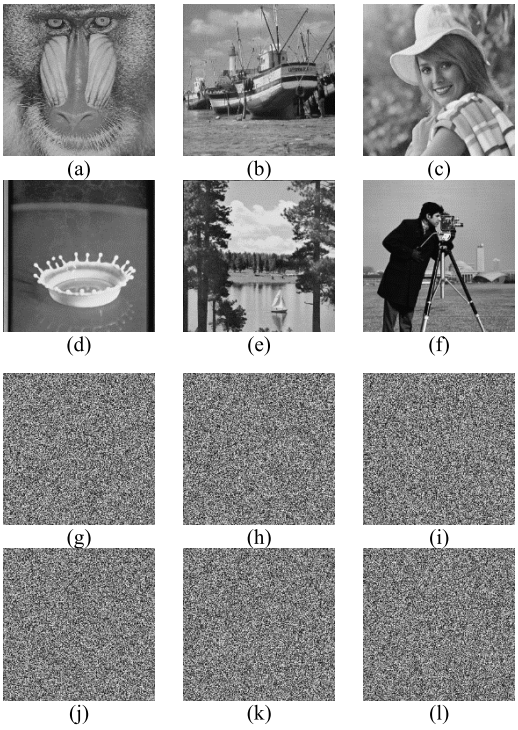


FIGURE 9. Original images (a) Baboon, (b) Boat, (c) Elaine, (d) Milkdrop, (e) Lake, (f) Cameraman, and (g)–(l) corresponding ciphertext images.

To evaluate uniformity of the encrypted images, the variance of histogram X defined as follows is used for quantity analysis [44]. The x_i and x_j represent the number of pixels with gray value equal to i and j, respectively.

$$\mathrm{var}\,(X) = \frac{1}{256 \times 256} \sum_{i=0}^{255} \sum_{j=0}^{255} \frac{1}{2} \left(x_i - x_j\right)^2 \tag{27}$$

The variance values of plaintext images and its corresponding ciphertext images are shown in Table 1, from which can be seen that the variance values of original histograms are large while the variance values of ciphertext histograms are small. The simulation results indicate that the histograms of encrypted images are uniformly distributed. In addition, we take the [46] and [47] for comparison, it can be seen that the variance values of the proposed method are smaller than other two methods. Therefore, the proposed scheme is more robust to resist the statistical attacks.

TABLE 1. Variances of histograms of original images and ciphertext images.

Image	Original	Ciphertext	Ref. [46]	Ref.[47]
Baboon	65912.5468	**269.3906**	283.3695	271.6582
Boat	96083.6875	**243.1796**	262.3589	256.0365
Elaine	35301.8359	**239.8359**	273.3698	279.3728
Milkdrop	86081.1953	**268.5859**	282.3694	276.3215
Lake	44650.5937	**282.4687**	288.3569	296.6148
Cameraman	11097.3304	**251.0078**	256.3192	266.8236

B. CORRELATION COEFFICIENT OF ADJACENT PIXELS

For a natural image, there is strong correlation between adjacent pixels. However, the pixel's correlation should be decreased in ciphertext images. The correlation coefficient (CC) defined as follows is used to measure the correlation of adjacent pixels.

$$CC = \frac{\sum_{v=1}^{2^n} (x_v - \bar{x})\,(y_v - \bar{y})}{\sqrt{\sum_{v=1}^{2^n} (x_v - \bar{x})^2 \sum_{v=1}^{N} (y_v - \bar{y})^2}}, \tag{28}$$

where x_v and y_v represents gray values of two adjacent pixels, respectively. The $\bar{x}$ and $\bar{y}$ denote corresponding mean values. If the correlation of adjacent pixels is strong, then CC value will close to 1, otherwise the CC value will close to 0.

TABLE 2. CC values of original and ciphertext images shown in Fig. 9.

Correlation coefficient	Horizontal	Vertical	Diagonal
Original Baboon	0.5776	0.6725	0.6012
Encrypted Baboon	**-0.0423**	**0.0202**	**-0.0212**
Original Boat	0.8867	0.6958	0.6846
Encrypted Boat	**-0.0110**	**-0.0661**	**0.0013**
Original Elaine	0.9634	0.9404	0.9095
Encrypted Elaine	**0.0050**	**0.0059**	**-0.0050**
Original Milkdrop	0.9742	0.8250	0.8266
Encrypted Milkdrop	**-0.0279**	**-0.0415**	**-0.0313**
Original Lake	0.9115	0.9352	0.8967
Encrypted Lake	**0.0118**	**0.0100**	**-0.0274**
Original Cameraman	0.9806	0.9832	0.9512
Encrypted Cameraman	**0.0086**	**0.0106**	**-0.0299**

The CC values of original and ciphertext images in three directions including horizontal, vertical and diagonal directions are listed in Table 2. As the CC values of ciphertext are close to 0, which indicates that the correlation is fairly weak compared with original images. In addition, 10,000 pairs of adjacent pixels in original and ciphertext image "Milkdrop" are randomly selected to analyze the correlation distribution. The distribution in three directions of original image

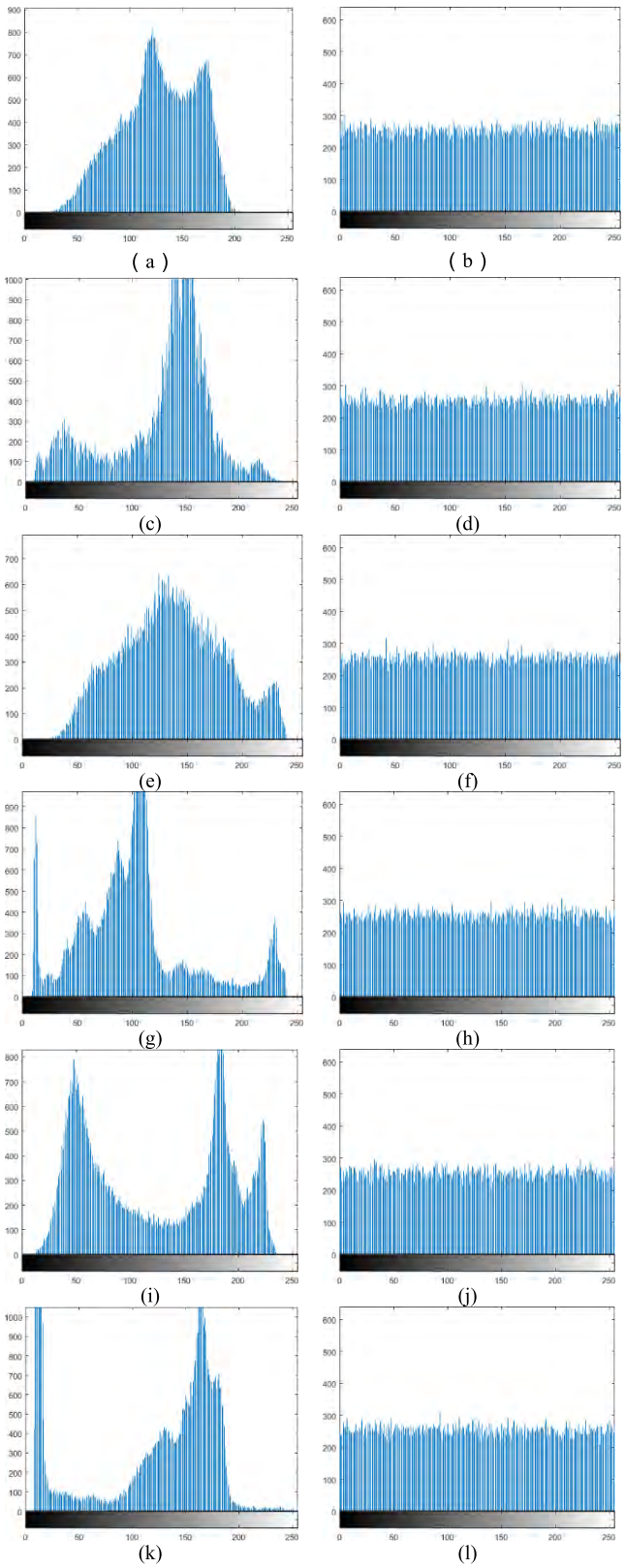


FIGURE 10. Histograms of the original images and corresponding ciphertext images.

''Milkdrop'' are plotted in Fig. 11(a)-(c), and the correlation distribution of corresponding ciphertext image are illustrated in Fig. 11(d)-(f). It is clear from Fig. 11(d)-(f) that the correlation between the adjacent pixels of ciphertext image is almost irrelevant.

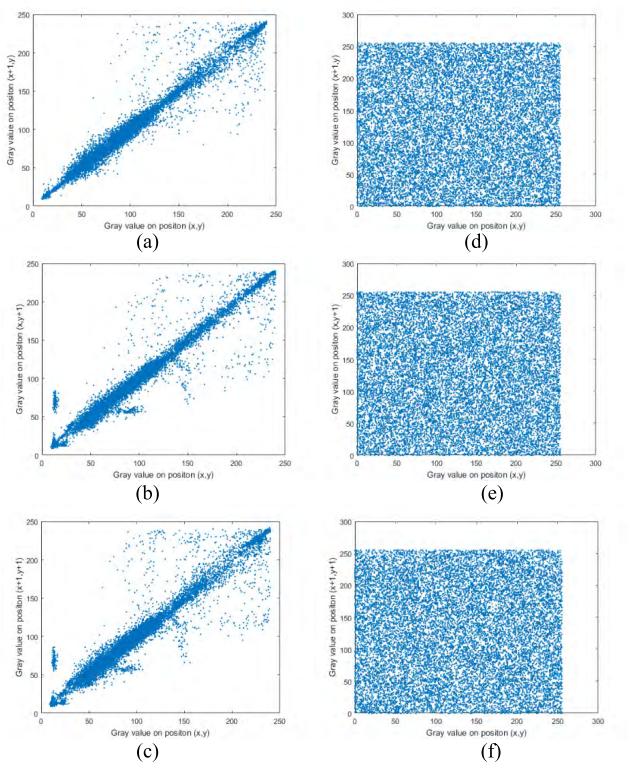


FIGURE 11. The correlation distribution of image "Milkdrop" and its ciphertext image. (a) Horizontal. (b) Vertical. (c) Diagonal. (d) Horizontal. (e) Vertical. (f) Diagonal.

C. INFORMATION ENTROPY

The information entropy (IE) is generally used to describe statistical measurement of uncertainties, which is defined with the probability of gray value in an image.

$$IE = -\sum_{h=0}^{255} P(h) \log_2 P(h), \tag{29}$$

where $P(h)$ denotes the probability of gray level h. In the ideal case, the entropy value of a truly random image encrypted image is 8. The entropy values of the original and ciphertext images are listed in Table 3, from which can be seen that the values of ciphertext images are close to the ideal value. Two other state-of-the-art methods are taken for

TABLE 3. Entropy analysis of original and ciphertext images.

Image	Original image	Ciphertext image	Ref. [48]	Ref. [49]
Baboon	7.1273	7.9970	**7.9972**	7.9969
Boat	7.1894	**7.9973**	7.9963	7.9971
Elaine	7.5046	**7.9974**	7.9962	7.9973
Milkdrop	7.2500	**7.9972**	7.9964	7.9972
Lake	7.4898	**7.9969**	7.9965	7.9968
Cameraman	7.0097	**7.9972**	7.9969	7.9972

comparison and the results indicate that the proposed method slightly surpasses others in the aspect of information entropy. Therefore, the proposed quantum block image encryption scheme can resist entropy attack.

D. KEY SENSITIVITY ANALYSIS

Key sensitivity is an important indicator to evaluate the performance of the proposed image encryption scheme, which prevents the attacker to capture original information even if a slight change of the key. To analyze the key sensitivity of the proposed scheme, correct keys and incorrect keys are used to decrypt the image ''Cameraman'' and the results are shown in Fig. 12. Fig. 12(a) shows the decrypted image with correct keys, which is the same as original image. Fig. 12(b) illustrates the decrypted image with incorrect control parameter p and other keys remain unchanged, and the deviation of p is 10^{-12}. Fig. 12(c) presents the decrypted image with incorrect initial value d_0, the deviation of which is 10^{-15}. The decrypted result with incorrect iteration number r of QArT is shown in Fig. 12(d). It can be seen from the decrypted images that the proposed image encryption scheme is extremely sensitive to keys.

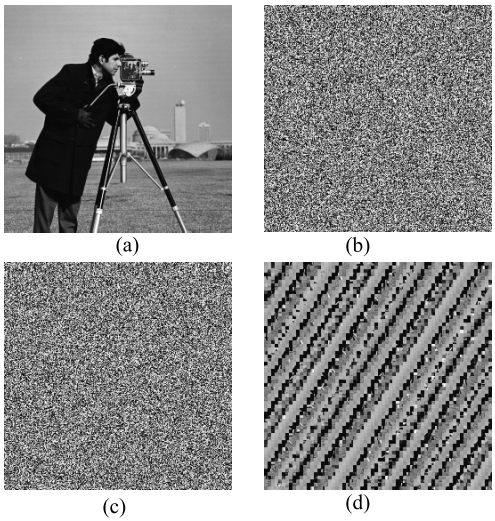


FIGURE 12. The decrypted images with correct keys and incorrect keys. (a) Correct keys. (b) Incorrect p. (c) Incorrect d_0. (d) Incorrect r.

E. KEY SPACE ANALYSIS

To resist brute-force attack, the proposed image encryption scheme should have a large key space. As the keys of the proposed scheme are independent, the key space is the product of the value range of all the parameters. According to the key sensitivity analysis, the valid precision of control parameter p , initial value d_0 and iteration number r are 10^{-12}, 10^{-15} and 1, respectively. As in the SCM, the value of control parameter p is in the range $(0, +\infty)$. Therefore, the key space is considered to be infinite. Thus the key space of the proposed scheme is large enough to frustrate brute-force attack.

TABLE 4. Results of UACI and NPCR influence.

Image	NPCR (%)	Ref. [50]	Ref.[51]
Baboon	99.5590	99.7652	99.6582
Boat	99.6445	99.7963	99.6034
Elaine	99.6078	99.7852	99.6592
Milkdrop	99.6063	99.7638	99.6389
Lake	99.6216	99.7869	99.6315
Cameraman	99.5956	99.7302	99.6215

Image	UACI (%)	Ref. [50]	Ref.[51]
Baboon	33.6197	33.5216	33.4025
Boat	33.5588	33.4716	33.4289
Elaine	33.3762	33.3940	33.4112
Milkdrop	33.4048	33.4520	33.4728
Lake	33.6030	33.3798	33.5036.
Cameraman	33.5233	33.4619	33.4960

F. UACI AND NPCR ANALYSIS

To resist the differential attack, the proposed scheme should sensitive to the original image. That's to say a slight change of the original image will cause a huge change in ciphertext image. The metrics include unified average changing intensity (UACI) and the number of pixel change rate (NPCR) are generally used to test sensitivity. Suppose the encrypted images T_1 and T_2 are obtained from the original image and a pixel change of the original image, respectively. The UACI and NPCR are defined as follows:

$$\mathrm{UACI} = \frac{1}{2^n \times 2^n} \sum_{i,j} \frac{|T_1(i,j) - T_2(i,j)|}{255} \times 100\%, \quad (30)$$

$$\mathrm{NPCR} = \frac{1}{2^n \times 2^n} \sum_{i,j} |D(i,j)| \times 100\%, \quad (31)$$

where (i, j) denotes the pixel position of the encrypted image. The value $D(i, j)$ is set to 1 if $T_1(i, j)$ is not equal to $T_2(i, j)$, otherwise the $D(i, j)$ is set to 0. The UACI and NPCR results are shown in Table 4, it can be seen that the NPCR results are close to ideal value 99.6094% and the UACI results are close to ideal value 33.4635%. In addition, two methods are taken for comparison. Although the UACI results of the proposed method is not better than [50] and [51], the NPCR results show superiority compared with the contrast methods. The results indicate that the proposed scheme performs well in the aspect of diffusion. Therefore, the differential attack is impractical.

G. ROBUSTNESS ANALYSIS AGAINST NOISE

The encrypted images are usually influenced with noises during the transmission process. For a robust image encryption algorithm, it should resist noise to some extent. Suppose the zero mean and standard deviation Gaussian random noise represented with G is added the ciphertext image E and the strength of which is denoted with k. The ciphertext image with noise is represented with $E' = E + kG$. The image Boat is used to test the influence of noise and the simulation results are shown in Fig. 13. It can be seen from the decryption results that the main information of original images can be retained.

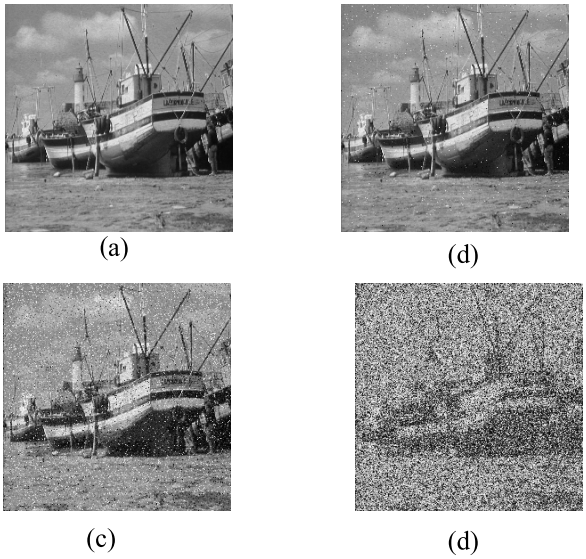


FIGURE 13. The decrypted images with different noise strength. (a) $k = 0$. (b) $k = 1$. (c) $k = 10$. (d) $k = 100$.

Thus, the proposed quantum image encryption scheme can resist noise attack.

H. RESISTANCE ATTACK ANALYSIS.

Generally, there are four kinds of attacks including ciphertext-only attack, known plaintext attack, chosen-plaintext attack and chosen ciphertext attack [42]. Among these attacks, chosen-plaintext attack is more powerful than others as the attacker can choose a plaintext and obtains its corresponding ciphertext. If the proposed algorithm resists chosen-plaintext attack, then other type attacks can also be resisted. As the initial value d_0 is determined with plaintext, and the key is related to plaintext. Therefore, the attacker cannot break the cryptosystem by encrypting and decrypting chosen plaintext images. So the proposed scheme can resist chosen-plaintext attack and other types of attack.

I. COMPUTATIONAL COMPLEXITY ANALYSIS

According to the proposed quantum block image encryption scheme, the computational complexity depends on the QArT and XOR operations. The computational complexity of quantum image processing algorithm is calculated with the number of logical elements in quantum circuits. The ADDER module and ADDER-MOD module are primary module in QArT circuits. As there are n sum modules, $2n-1$ carry modules and one control-NOT gate in the ADDER module, the complexity of which is $2n + 13(2n-1) + 1 = 28n - 12$ [29]. The ADDER-MOD module consists 5 ADDER module and therefore its complexity is about $140n$. The computational complexity of the QArT is $O(n)$. Due to the parallel characteristic of quantum computation, the XOR operation for $2^n \times 2^n$ pixels is accomplished with a $2n$-CNOT gate, which is constructed with $128n - 256$ basic gates. So the computational complexity of the QArT is $O(n)$, too. Therefore, the computational complexity of the proposed scheme is $O(n)$, which is superior compared with its classical counterpart in terms of efficiency.

V. CONCLUSION

In this paper, a quantum representation model QBIR for block images is proposed, the representation and preparation of which are detailed discussed. The chaotic system SCM is introduced into the field of quantum image encryption, which greatly enlarge the key space to infinite theoretically and simplify the keys transmission. The QArT and quantum XOR operations are respectively utilized to realize the permutation and diffusion, therefore the position information and gray values of pixels are sufficiently modified. Moreover, the bit sequence generated for XOR operation is dependent on the original image, so it can resist the chosen plaintext attack. Numerical simulation results show that the proposed quantum image encryption scheme can retrieve the original image accurately with correct keys, and the security is analyzed in the aspects of statistical, key security, UACI and NPCR. The superior efficiency in comparison with classical counterpart is also verified through computational complexity analysis.

The proposed QBIR quantum image representation model and SCM chaotic model are employed into the field of quantum image encryption and achieves good performance in security and efficiency. To research and extend the applications of QBIR model and SCM model in the aspects of color image encryption and multiple image encryption will be the directions of our future work.

REFERENCES

[1] G. Hu, D. Xiao, Y. Wang, and X. Li, "Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1305–1316, 2017.

[2] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Commun. Nonlinear Sci. Numer Simul.*, vol. 23, nos. 1–3, pp. 294–310, Jun. 2015.

[3] J. Wu, Z. Xie, Z. Liu, L. Wei, Z. Yan, and S. Liu, "Multiple-image encryption based on computational ghost imaging," *Opt. Commun.*, vol. 359, pp. 38–43, Jan. 2016.

[4] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, Apr. 2018.

[5] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[6] N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Opt. Commun.*, vol. 284, no. 13, pp. 3234–3242, 2011.

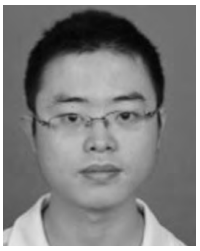
[7] X. Chai, Z. H. Gan, L. Yang, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chin. Phys. B*, vol. 25, no. 10, pp. 76–88, Aug. 2016.

[8] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.

[9] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[10] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010.

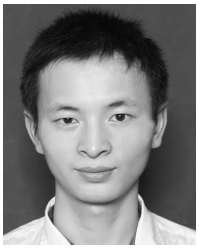
[11] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.
[12] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.
[13] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.
[14] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Opt. Commun.*, vol. 343, pp. 10–21, May 2015.
[15] N. Zhou, H. Jiang, L. Gong, and X. Xie, "Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging," *Opt. Lasers Eng.*, vol. 110, pp. 72–79, Nov. 2018.
[16] N. Abura'ed, F. S. Khan and H. Bhaskar, "Advances in the quantum theoretical approach to image processing applications," *ACM Comput. Surv.*, vol. 49, no. 4, 2017, Art. no. 75.
[17] F. Yan, A. M. Iliyasu, and P. Q. Le, "Quantum image processing: A review of advances in its security technologies," *Int. J. Quantum Inf.*, vol. 15, no. 3, 2017, Art. no. 1730001.
[18] A. M. Iliyasu, P. Q. Le, F. Dong, and K. Hirota, "Watermarking and authentication of quantum images based on restricted geometric transformations," *Inf. Sci.*, vol. 186, no. 1, pp. 126–149, 2012.
[19] P. Li, Y. Zhao, H. Xiao, and M. Cao, "An improved quantum watermarking scheme using small-scale quantum circuits and color scrambling," *Quantum Inf. Process.*, vol. 16, no. 5, p. 127, 2017.
[20] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[21] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
[22] L. K. Grover, "A fast quantum mechanical algorithm for estimating the median," in *Proc. ACM Symp. Theor. Comput.*, 1996, pp. 212–219. doi: 10.1145/237814.237866.
[23] S. E. Venegas-Andraca and S. Bose, "Storing, processing, and retrieving an image using quantum mechanics," *Proc. SPIE*, vol. 5105, pp. 1085–1090, Aug. 2003. doi: 10.1117/12.485960.
[24] J. I. Latorre. (2005). "Image compression and entanglement." Accessed: Jun. 23, 2017. [Online]. Available: https://arxiv.org/abs/quant-ph/0510031
[25] H.-S. Li, Q. Zhu, R.-G. Zhou, L. Song, and X.-J. Yang, "Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state," *Quantum Inf. Process.*, vol. 13, no. 4, pp. 991–1011, 2014.
[26] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 63–84, 2011.
[27] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: A novel enhanced quantum representation of digital images," *Quantum Inf. Process.*, vol. 12, no. 8, pp. 2833–2860, 2013.
[28] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.
[29] H. Wang, J. Wang, Y.-C. Geng, Y. Song, and J.-Q. Liu, "Quantum image encryption based on iterative framework of frequency-spatial domain transforms," *Int. J. Theor. Phys.*, vol. 56, no. 10, pp. 3029–3049, 2017.
[30] Y.-G. Yang, X. Jia, S.-J. Sun, and Q.-X. Pan, "Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding," *Inf. Sci.*, vol. 277, pp. 445–457, Sep. 2014.
[31] P. Li and Y. Zhao, "A simple encryption algorithm for quantum color image," *Int. J. Theor. Phys.*, vol. 56, no. 6, pp. 1961–1982, 2017.
[32] Y.-G. Yang, J. Xia, X. Jia, and H. Zhang, "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding," *Quantum Inf. Process.*, vol. 12, no. 11, pp. 3477–3493, 2013.
[33] X.-H. Song, S. Wang, A. A. A. El-Latif, and X. M. Niu, "Quantum image encryption based on restricted geometric and color transformations," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1765–1787, 2014.
[34] X.-Z. Li, W.-W. Chen, and Y.-Q. Wang, "Quantum image compression-encryption scheme based on quantum discrete cosine transform," *Int. J. Theor. Phys.*, vol. 57, no. 9, pp. 2904–2919, 2018.
[35] H.-S. Li, C. Li, X. Chen, and H.-Y. Xia, "Quantum image encryption algorithm based on NASS," *Int. J. Theor. Phys.*, vol. 57, no. 12, pp. 3745–3760, 2018.
[36] Q. Ran, L. Wang, J. Ma, L. Tan, and S. Yu, "A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections," *Quantum Inf. Process.*, vol. 17, no. 8, 2018, Art. no. 188.
[37] N. Zhou, X. Yan, H. Liang, X. Tao, and G. Li, "Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system," *Quantum Inf. Process.*, vol. 17, Dec. 2018, Art. no. 338.
[38] N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," *Quantum Inf. Process.*, vol. 17, no. 6, 2018, Art. no. 137.
[39] N. Jiang, L. Wang, and W.-Y. Wu, "Quantum Hilbert image scrambling," *Int. J. Theor. Phys.*, vol. 53, no. 7, pp. 2463–2484, 2014.
[40] N. Jiang, W. Y. Wu, and L. Wang, "The quantum realization of Arnold and Fibonacci image scrambling," *Quantum Inf. Process.*, vol. 13, no. 5, pp. 1223–1236, 2014.
[41] R.-G. Zhou, Y.-J. Sun, and P. Fan, "Quantum image Gray-code and bit-plane scrambling," *Quantum Inf. Process.*, vol. 14, no. 5, pp. 1717–1734, 2015.
[42] S. Heidari, M. Vafaei, M. Houshmand, and N. Tabatabaey-Mashadi, "A dual quantum image scrambling method," *Quantum Inf. Process.*, vol. 18, Jan. 2019, Art. no. 9.
[43] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.
[44] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[45] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[46] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," *Quantum Inf. Process.*, vol. 16, no. 6, 2017, Art. no. 164.
[47] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019.
[48] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9907–9927, 2017.
[49] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[50] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[51] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.



XINGBIN LIU received the Ph.D. degree from the School of Information and Electronics, Beijing Institute of Technology, in 2017. He is currently a Postdoctoral Researcher with the College of Computer Science, Chongqing University. His main research interests include image security, image fusion, and quantum information processing.

DI XIAO received the B.S. degree from Sichuan University, Chengdu, China, and the M.S. and Ph.D. degrees from Chongqing University, Chongqing, China. From 2006 to 2008, he accomplished the postdoctoral research at Chongqing University. From 2008 to 2009, he visited the Department of Computer Science, New Jersey Institute of Technology, USA. He is currently a Full Professor with the College of Computer Science, Chongqing University. His research interests include signal processing in encrypted domain, compressive sensing, quantum computation, and so on. So far, he has published more than 90 academic journal or conference papers and be successively selected as 2014–2018 Elsevier Most Cited Chinese Researchers.

WEI HUANG received the B.S. degree in mathematics and applied mathematics and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009 and 2015, respectively. He is currently a Senior Engineer with the Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum secure communication, and quantum information.



CONG LIU received the master's degree in engineering from Southwest Technology and Engineering Research Institute, Chongqing, China, in 2010. As a Senior Engineer of Southwest Technology and Engineering Research Institute, he is mainly engaged in product environmental effects and background environmental data research.