SCIENCE CHINA
Information Sciences

• **Supplementary File** •

A quantum image dual-scrambling encryption scheme based on random permutation

Hai-Hua Zhu[1,3], Xiu-Bo Chen[1,2*] & Yi-Xian Yang[1,2]

[1]*Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*GuiZhou University, Guizhou Provincial Key Laboratory of Public Big Data, Guizhou Guiyang,* 550025*, China;*
[3]*School of Computer and Information Technology, Nanyang Normal University, Nanyang* 473061*, China*

Appendix A Example

Example 1 (Example of Bit-plane Scrambling). When $q = 8$, a gray image (ranged in $\{0, 1, \cdots, 2^8 - 1\}$) is represented by $|I_G\rangle$. Therefore, an 8-qubit gray image has 8 bit-plane images, such as $|I_G^7\rangle$, $|I_G^6\rangle$, $\cdots$, $|I_G^0\rangle$. Each bit-plane is shown as follows.

$$\begin{cases} |I_G^7\rangle = \dfrac{1}{\sqrt{2}^{h+w}} \displaystyle\sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |C_{YX}^7\rangle |YX\rangle \\ |I_G^6\rangle = \dfrac{1}{\sqrt{2}^{h+w}} \displaystyle\sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |C_{YX}^6\rangle |YX\rangle \\ \quad\vdots \\ |I_G^0\rangle = \dfrac{1}{\sqrt{2}^{h+w}} \displaystyle\sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |C_{YX}^0\rangle |YX\rangle \end{cases}, \tag{A1}$$

$$h = \begin{cases} \lceil log_2 H \rceil, & H > 1 \\ 1, & H = 1, \end{cases}, w = \begin{cases} \lceil log_2 W \rceil, & W > 1 \\ 1, & W = 1 \end{cases},$$

where $C_{YX}^i \in \{0, 1\}$ represents the i-th binary value of the corresponding pixel position $|YX\rangle$, $i \in \{0, 1, \cdots, 7\}$.

Let $s = 10000$, the random permutation of the integers from 1 to 8 is (8 6 2 4 1 7 5 3). We can construct a series of ordered two-tuples: $(1, 8)$, $(2, 6)$, $(3, 2)$, $(4, 4)$, $(5, 1)$, $(6, 7)$, $(7, 5)$, $(8, 3)$. Then, we construct 8 gray scales with state $|0\rangle$, such as $|0^7\rangle$, $|0^5\rangle$, $|0^1\rangle$, $|0^3\rangle$, $|0^0\rangle$, $|0^6\rangle$, $|0^4\rangle$, $|0^2\rangle$. Based on these two-tuples and controlled-not gates, we can construct

$$\begin{cases} CNOT\ |C_{YX}^0, 0^7\rangle \rightarrow |C_{YX}^0, \dot{C}_{YX}^7\rangle \\ CNOT\ |C_{YX}^1, 0^5\rangle \rightarrow |C_{YX}^1, \dot{C}_{YX}^5\rangle \\ CNOT\ |C_{YX}^2, 0^1\rangle \rightarrow |C_{YX}^2, \dot{C}_{YX}^1\rangle \\ CNOT\ |C_{YX}^3, 0^3\rangle \rightarrow |C_{YX}^3, \dot{C}_{YX}^3\rangle \\ CNOT\ |C_{YX}^4, 0^0\rangle \rightarrow |C_{YX}^4, \dot{C}_{YX}^0\rangle \\ CNOT\ |C_{YX}^5, 0^6\rangle \rightarrow |C_{YX}^5, \dot{C}_{YX}^6\rangle \\ CNOT\ |C_{YX}^6, 0^4\rangle \rightarrow |C_{YX}^6, \dot{C}_{YX}^4\rangle \\ CNOT\ |C_{YX}^7, 0^2\rangle \rightarrow |C_{YX}^7, \dot{C}_{YX}^2\rangle \end{cases}, \tag{A2}$$

where, $|C_{YX}^7 C_{YX}^6 \cdots C_{YX}^0\rangle$ and $|\dot{C}_{YX}^7 \dot{C}_{YX}^6 \cdots \dot{C}_{YX}^0\rangle$ are the original gray scales in $|I_G\rangle$ and the scrambled gray scales in $|I_{GB}\rangle$, respectively.

The quantum bit-plane scrambling circuit transformation from $|I_G\rangle$ to bit-plane scrambled gray scale GQIR $|I_{GB}\rangle$ is shown in Figure A1.

When $q = 24$, a 24-qubit true color image which is based on RGB model (i.e. red, green, and blue), is represented by $|I_C\rangle$. Therefore, 24 bit-plane images of a 24-qubit true color image are represented as $|I_C^{23}\rangle$, $|I_C^{22}\rangle$, $\cdots$, $|I_C^0\rangle$. The quantum bit-plane scrambling circuit transformation from $|I_C\rangle$ to $|I_{CB}\rangle$ is similar to the case of $q = 8$.

* Corresponding author (email: flyover100@163.com)

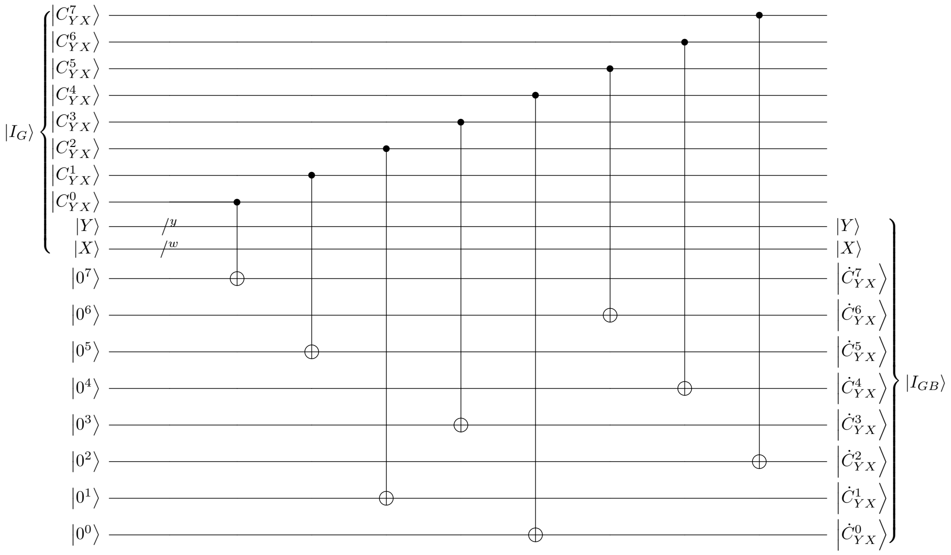

Figure A1 The quantum circuit from $|I_G\rangle$ to $|I_{GB}\rangle$

Example 2 (Example of Bit-plane Inverse Scrambling)**.** When $q = 8$, an encrypted gray image (ranged in $\{0, 1, \cdots, 2^8-1\}$) is represented by $|I_{GS}\rangle$. Therefore, a gray image has 8 bit-plane images, such as $|I^7_{GS}\rangle$, $|I^6_{GS}\rangle$, $\cdots$, $|I^0_{GS}\rangle$.

Let $s = 10000$, the random permutation of the integers from 1 to 8 is (8 6 2 4 1 7 5 3). We can construct a series of ordered two-tuples $(1, 8)$, $(2, 6)$, $(3, 2)$, $(4, 4)$, $(5, 1)$, $(6, 7)$, $(7, 5)$, $(8, 3)$. The transpositions of these two-tuples are shown as $(8, 1)$, $(6, 2)$, $(2, 3)$, $(4, 4)$, $(1, 5)$, $(7, 6)$, $(3, 8)$. Then, we construct 8 gray scales with state $|0\rangle$, such as $|0^4\rangle$, $|0^2\rangle$, $|0^7\rangle$, $|0^3\rangle$, $|0^6\rangle$, $|0^1\rangle$, $|0^5\rangle$, $|0^0\rangle$. Based on these two-tuples and controlled-not gates, we can construct

$$\begin{cases} CNOT\ |\dot{C}^0_{YX}, 0^4\rangle \rightarrow |\dot{C}^0_{YX}, C^4_{YX}\rangle \\ CNOT\ |\dot{C}^1_{YX}, 0^2\rangle \rightarrow |\dot{C}^1_{YX}, C^2_{YX}\rangle \\ CNOT\ |\dot{C}^2_{YX}, 0^7\rangle \rightarrow |\dot{C}^2_{YX}, C^7_{YX}\rangle \\ CNOT\ |\dot{C}^3_{YX}, 0^3\rangle \rightarrow |\dot{C}^3_{YX}, C^3_{YX}\rangle \\ CNOT\ |\dot{C}^4_{YX}, 0^6\rangle \rightarrow |\dot{C}^4_{YX}, C^6_{YX}\rangle \\ CNOT\ |\dot{C}^5_{YX}, 0^1\rangle \rightarrow |\dot{C}^5_{YX}, C^1_{YX}\rangle \\ CNOT\ |\dot{C}^6_{YX}, 0^5\rangle \rightarrow |\dot{C}^6_{YX}, C^5_{YX}\rangle \\ CNOT\ |\dot{C}^7_{YX}, 0^0\rangle \rightarrow |\dot{C}^7_{YX}, C^0_{YX}\rangle \end{cases} \tag{A3}$$

The quantum bit-plane inverse scrambling circuit transformation from $|I_{GS}\rangle$ to bit-plane inverse scrambled gray scale GQIR $|I_{GP}\rangle$ is shown in Figure A2.

When $q = 24$, a encrypted 24-qubit true color image which is based on RGB model (i.e. red, green, and blue), is represented by $|I_{CS}\rangle$. Therefore, 24 bit-plane images of an 24-qubit true color image are represented as $|I^{23}_{CS}\rangle$, $|I^{22}_{CS}\rangle$, $\cdots$, $|I^0_{CS}\rangle$. The quantum bit-plane scrambling circuit transformation from $|I_C\rangle$ to $|I_{CB}\rangle$ is similar to the case of $q = 8$.

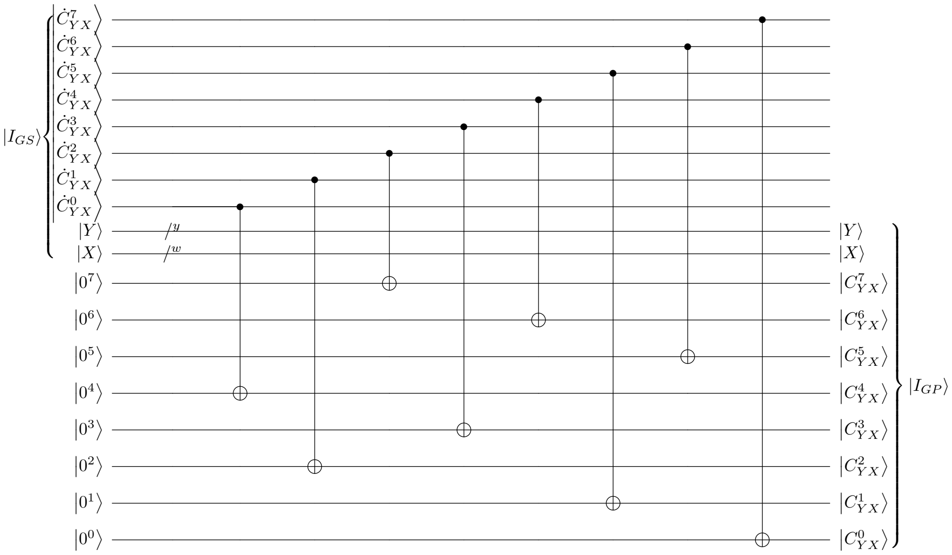

Figure A2 The quantum circuit from $|I_{GS}\rangle$ to $|I_{GP}\rangle$

Appendix B Algorithm

The pixel position scrambling algorithm is shown in **Algorithm B1**.

Algorithm B1 The pixel position scrambling algorithm

```
Input: $|I_B\rangle$. /* $|I_B\rangle$ is the GQIR of the bit-plane scrambled images with an $H \times W$ resolution. */
Initialize: $s$. /* $s$ is a random generating factor. */
Output: $|I_S\rangle$. /* $|I_S\rangle$ is the encrypted GQIR after pixel position scrambling. */

(1) the numbers of rows and columns of $|I_B\rangle \rightarrow H, W$.

(2) $s,\ H \rightarrow \{(1\ k_1),\ (2\ k_2),\ \cdots,\ (H\ k_H)\}$,
    $s,\ W \rightarrow \{(1\ t_1),\ (2\ t_2),\ \cdots,\ (W\ t_W)\}$.

(3) $\lceil log_2 H \rceil \rightarrow h$, $\lceil log_2 W \rceil \rightarrow w$

(4) for $M = 1 : H$
        $|M\rangle$, $|k_M\rangle \rightarrow (i, u_i)$, $i \in \{0, 1, \cdots, h-1\}$.
        $CNOT\ |y_i, 0_{u_i}\rangle \rightarrow |y_i, \dot{y}_{u_i}\rangle$.
    end

(5) for $N = 1 : W$
        $|N\rangle$, $|t_N\rangle \rightarrow (j, v_j)$, , $j \in \{0, 1, \cdots, w-1\}$.
        $CNOT\ |x_i, 0_{v_j}\rangle \rightarrow |x_j, \dot{x}_{v_j}\rangle$.
    end

(6) $|I_B\rangle \rightarrow |I_S\rangle$.
```

The pixel position inverse scrambling algorithm is shown in **Algorithm B2**.

Appendix C Simulation Results and Analysis

Appendix C.1 Effectiveness of The Proposed Method

Experimental results are shown in FigureC1. The histogram reflects the distribution of gray level in the image. It is clear that the color value histograms of the encrypted images are more smooth and significantly different from the color value

Algorithm B2 The pixel position inverse scrambling algorithm

```
Input: $|I_P\rangle$. /* $|I_P\rangle$ is the bit-plane inverse scrambled GQIR with an $H \times W$ resolution. */
Initialize: $s$. /* $s$ is a random generating factor. */
Output: $|I\rangle$. /* $|I\rangle$ is the decrypted GQIR after pixel position inverse scrambling. */

(1) the number of rows and columns of $|I_P\rangle \leftarrow H, W$ .
(2) $s,\ h \rightarrow (i, k_j),\ ,\ i, j \in \{1, 2, \cdots, h\}$.
(3) $s,\ H \rightarrow \{(1\ k_1),\ (2\ k_2),\ \cdots,\ (H\ k_H)\}$,
    $s,\ W \rightarrow \{(1\ t_1),\ (2\ t_2),\ \cdots,\ (W\ t_W)\}$.
(4) $\{(1\ k_1)^T,\ (2\ k_2)^T,\ \cdots,\ (H\ k_H)^T\};\ \{(1\ t_1)^T,\ (2\ t_2)^T,\ \cdots,\ (W\ t_W)^T\}$.
(5) $\lceil log_2 H\rceil \rightarrow h,\ \lceil log_2 W\rceil \rightarrow w$.
(6) for $M = 1 : H$
        $|k_M\rangle,\ |M\rangle \rightarrow (u_i, i),\ i \in \{0, 1, \cdots, h-1\}$.
        $CNOT\ |\dot{y}_{u_i}, 0_i\rangle \rightarrow |\dot{y}_{u_i}, y_i\rangle$.
    end
(7) for $N = 1 : W$
        $|t_N\rangle,\ |N\rangle \rightarrow (v_j, j),\ j \in \{0, 1, \cdots, w-1\}$.
        $CNOT\ |\dot{x}_{v_j}, 0_j\rangle \rightarrow |\dot{x}_{v_j}, x_j\rangle$.
    end
(8) $|I_P\rangle \rightarrow |I\rangle$.
```

histograms of the original images and hence, it does not provide any clues for eavesdroppers who perform statistical attack and differential attack on the encrypted image.

Correlation coefficients (CC) and SNR between original images and encrypted images are shown in Table C1. When calculating Correlation coefficient (CC), each of three color images (i.e. “Barbara”, “Cornfield” and “Flowers”) is represented in three color channels: red, green and blue. It can be seen from the formula of CC that the closer CC is to 0, the better the scrambling effectiveness will be. Table C1 shows that the five CCs are very close to 0, which indicates that five images after encryption approximate the corresponding original images. In addition, Table C1 shows that the SNRs are very small, which means that the degrees of scrambling image deviating from the original image are higher.

Table C1 Correlation coefficient and SNR between original image and encrypted image.

Image	Image resolution	Color channel	CC	$SNR\ (dB)$
“Airfield”	512 × 512	Gray	0.0014	0.1717
“Boats”	576 × 720	Gray	0.0029	0.2863
“Barbara”	576 × 720	Red	-0.0022	0.2166
		Green	0.0033	
		Blue	-0.0008	
“Cornfield”	480 × 512	Red	-0.0152	0.0777
		Green	-0.0073	
		Blue	-0.0026	
“Flowers”	362 × 500	Red	0.0036	0.1727
		Green	0.0035	
		Blue	0.0017	

The results of correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the original images and

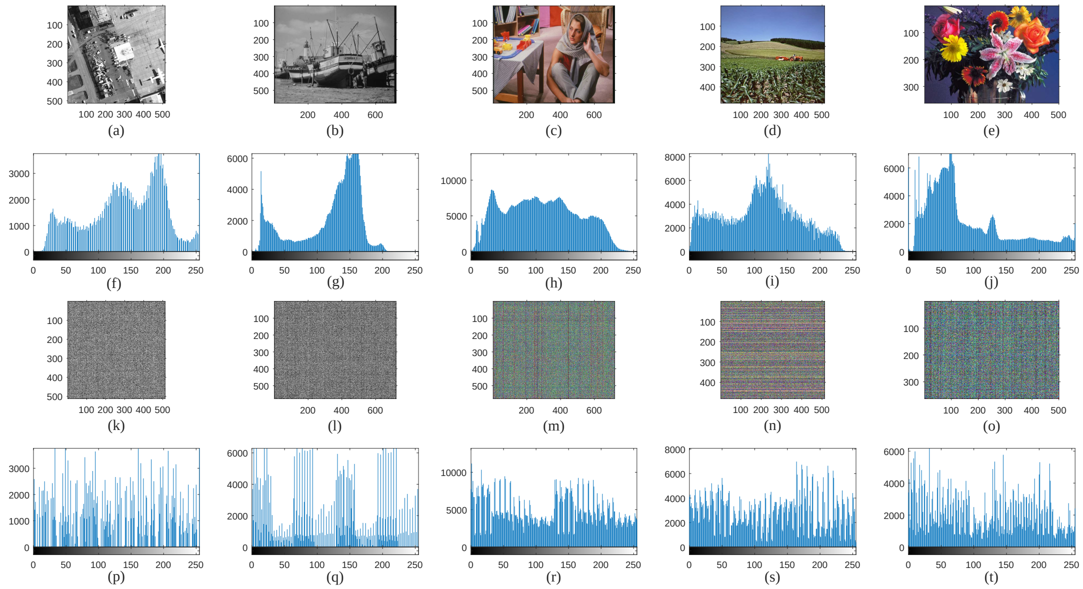

Figure C1 The experimental results. (a, b, c, d, e) original images, (f, g, h, i, j) histograms of original images, (k, l, m, n, o) encrypted images based on dual-scrambling, (p, q, r, s, t) histograms of encrypted images.

their corresponding encrypted images are given in Table C2, from which it is shown that the proposed scheme generally provides a satisfactory correlation performance.

Table C2 Correlation coefficient of adjacent pixels in original image and encrypted image.

Image	Color channel	Horizontal correlation		Vertical correlation		Diagonal correlation	
		Original image	Encrypted image	Original image	Encrypted image	Original image	Encrypted image
“Airfield”	Gray	0.9402	0.0076	0.9423	0.0078	0.9032	0.0035
“Boats”	Gray	0.9680	0.0069	0.9723	0.0168	0.9441	-0.0007
“Barbara”	Red	0.9189	0.0315	0.9619	0.0384	0.8885	0.0017
	Green	0.8974	0.0062	0.9611	0.0717	0.8730	0.0006
	Blue	0.9154	0.0023	0.9648	0.0201	0.8888	0.0040
“Cornfield”	Red	0.9228	0.2371	0.9041	0.0112	0.8371	0.0128
	Green	0.9358	0.1251	0.9128	0.0054	0.8538	0.0113
	Blue	0.9699	0.0312	0.9576	0.0009	0.9322	0.0008
“Flowers”	Red	0.9726	0.0139	0.9716	0.0296	0.9547	-0.0008
	Green	0.9516	0.0258	0.9490	0.0432	0.9210	-0.0023
	Blue	0.9532	0.0226	0.9518	0.0309	0.9248	-0.0058

To summarise, the proposed scheme can effectively scramble and encrypt quantum images.

Appendix C.2 Analysis of Key Space

As we know, the larger the key space is, the more attacks the encryption algorithm can resist. The main purpose of the dual-scrambling encryption scheme is to increase the key space. The quantum image dual-scrambling encryption scheme mainly considers the spatial scrambling methods and the spatial scrambling, which are based n pixel position and color space, severally. We set the key space of the bit-plane scrambling and the pixel position scrambling to be $\Re_1$ and $\Re_2$ respectively, then the total key space of the dual-scrambling encryption scheme is $\Re_1 \times \Re_2$.

The general quantum image dual-scrambling encryption scheme mainly includes bit-plane scrambling scheme and pixel position scrambling. Refs. [2] and [3] proposed the bit-plane scrambling algorithms respectively based on NCQI and flexible NEQR. Ref. [2] used XOR operation and XNOR operation to realize bit-plane scrambling. Theoretically, there are 2^q combinations of XOR operation and XNOR operation for q-qubit bit-plane. Ref. [3] used Gray Code to realize bit-plane scrambling. Theoretically, there are 2^q Gray Codes for q-qubit bit-plane. In practical application, the efficiency of Gray

Code is usually improved, so the cycle of Gray Code is smaller. The proposed quantum image encryption scheme is based on random permutation using the pseudo random number generator. Mersenne Twister algorithm [9] is a popular random number generator, small cycle of this algorithm in many software packages is 2^{32}. A gray image needs 8 qubits to represent the gray level. Theoretically, the scrambling space of the bit plane of the gray image is 8!, where $8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 < 2^{32}$, so the key space of the bit-plane scrambling of the gray image should be $8! = 40320$. A color image needs 24 qubits to represent the color level in RGB model. Theoretically, the scrambling space of the bit plane of the color image is 24!, where $24! = 24 \times 23 \times 22 \times \cdots \times 4 \times 3 \times 2 \times 1 > 2^{32}$, so the key space of the bit-plane scrambling of the color image should be 2^{32}. Bit-plane scrambling scheme and its key space are shown in Table C3. Obviously, the key space of the proposed scheme is the largest.

Table C3 Bit-plane scrambling scheme and its key space.

Scheme	Representation model	Image resolution	Bit-plane scrambling scheme	Key space ($\Re_1$)	
				8-qubit	24-qubit
Scheme of Ref. [2]	NCQI	Square	XOR/XNOR	2^8=256	2^{24}
Scheme of Ref. [3]	flexible NEQR	Constrained rectangle	Gray Code	2^8=256	2^{24}
Our scheme	GQIR	Arbitrary rectangle	Random permutation	8!=40320	2^{32}

Refs. [2] and [3] proposed the pixel position scrambling algorithms using XOR/XNOR operation and Gray Code, respectively. For a $2^h \times 2^h$ quantum image, XOR/XNOR operation is used for all pixels position scrambling in Ref. [2], the key space of this algorithm should be $2^h \times 2^h$. According to the flexible NEQR, a $2^h \times 2^w$ quantum image could be represented by $h+w$ qubits. Based on the theory of Gray Code, the key space of the pixel position scrambling algorithm in Ref. [3] is up to $2^h \times 2^w$. The proposed quantum image encryption scheme is based on random permutation by using the pseudo random number generator. Based on the analysis about Mersenne Twister algorithm and GQIR model, the key space of the pixel position scrambling algorithm in our quantum image encryption scheme should be min$\{\lceil log_2 H \rceil!, 2^{32}\}\times$ min$\{\lceil log_2 W \rceil!, 2^{32}\}$. Pixel position scrambling scheme and its key space are shown in Table C4. When the row number or the column number of an image is less than 8192, min$\{\lceil log_2 H \rceil!, 2^{32}\}\times$ min$\{\lceil log_2 W \rceil!, 2^{32}\}=\lceil log_2 H \rceil! \times \lceil log_2 W \rceil! > 2^h \times 2^w (flexibleNEQRmodel)$ (when $h > 4, w > 4$).Because the resolution of the practical image is usually not very high, the key space of our scheme is the largest.

Table C4 Pixel position scrambling scheme and its key space.

Scheme	Representation model	Image resolution	Position scrambling scheme	Key space ($\Re_2$)
Scheme of Ref. [2]	NCQI	$2^h \times 2^h$	XOR/XNOR	$2^h \times 2^h$
Scheme of Ref. [3]	flexible NEQR	$2^h \times 2^w$	Gray Code	$< 2^h \times 2^w$
Our scheme	GQIR	$H \times W$	Random permutation	min$\{\lceil log_2 H \rceil!, 2^{32}\}\times$ min$\{\lceil log_2 W \rceil!, 2^{32}\}$

Appendix C.3 Analysis of Computational Complexity

In quantum computers, computational complexity is often used to measure the time cost of algorithm, and its value depends on the number of basic logic gates in the constructed circuits. Because computational complexity can ignore the impact of physical devices, it is also called network complexity. The smaller the computational complexity is, the better the performance of the algorithm is.

Our dual-scrambling scheme contains two parts: bit-plane scrambling and pixel position scrambling. According to Eq. (3) in our LETTER, q $CNOT$ gates are used only once in bit-plane scrambling for q-qubit color depth quantum image. So the computational complexity is q. In pixel position scrambling, h $CNOT$ gates and w $CNOT$ gates are designed for $H \times W$ quantum image, and these gates are used only one time. So the computation complexity is $h + w$. The computational complexity of our scheme is equal to the sum of the computational complexity in two parts. Thus, computational complexity of our scheme is $q+h+w$. The quantum image dual-scrambling method based on Gray Code in Ref. [3] was used for q-qubit color depth flexible NEQR quantum image with $2^h \times 2^w$ resolution. And the circuit complexity based on $CNOT$ gate for their first method would be q and for the second one would be $h + w + q$ [2,3]. Furthermore, the authors of Ref. [3] claimed that their schemes were not restricted to square image, but the scheme mainly illustrated the constrained rectangle quantum image (i.e. the $2^h \times 2^w$ quantum image). A dual quantum image scrambling method in Ref. [2] was used for q-qubit color depth NCQI quantum image with $2^h \times 2^h$ resolution. And the circuit complexity would be $8qh + q$ [2]. Therefore, our dual-scrambling scheme is low computational complexity, and it can be applied to non-square quantum image.

References

1 N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, Q. H. Liao, Quantum image encryption based on generalized arnold transform and double random-phase encoding, Quantum Information Processing 14 (2015) 1193-1213.

2 Heidari S , Vafaei M , Houshmand M , et al. A dual quantum image scrambling method. Quantum Information Processing, 2019, 18(1).

3 R. G. Zhou, Y. J. Sun, P. Fan, Quantum image gray-code and bit-plane scrambling, Quantum Information Processing 14 (2015) 1-18.

4 G. Xu, K. Xiao, Z. P. Li, X. X. Niu, and M. Ryan. Controlled Secure Direct Communication Protocol via the Three-Qubit Partially Entangled Set of States. Cmc-Computers Materials & Continua, 2019, 58 (3): 809-827.

5 P. Q. Le, F. Dong, K. Hirota, A flexible representation of quantum images for polynomial preparation, image compression, and processing operations, Kluwer Academic Publishers, 2011.

6 Y. Zhang, K. Lu, Y. Gao, K. Xu, A novel quantum representation for log-polar images, Quantum Information Processing 12 (2013) 3103-3126.

7 J. Sang, S. Wang, Q. Li, A novel quantum representation of color digital images, Quantum Information Processing 16 (2017) 42.

8 N. Jiang, J. Wang, Y. Mu, Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio, Kluwer Academic Publishers, 2015.

9 Matsumoto M, Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Transactions on Modeling and Computer Simulation, 1998, 8(1): 3-30.