SCIENCE CHINA
Information Sciences

• LETTER •

December 2019, Vol. 62 229501:1–229501:3
https://doi.org/10.1007/s11432-018-1514-y

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]*Sate Key Laboratory of Public Big Data, Guizhou University, Guiyang* 550025*, China;*
[3]*School of Computer and Information Technology, Nanyang Normal University, Nanyang* 473061*, China*

Received 21 December 2018/Revised 21 April 2019/Accepted 28 June 2019/Published online 11 November 2019

Citation Zhu H-H, Chen X-B, Yang Y-X. A quantum image dual-scrambling encryption scheme based on random permutation. Sci China Inf Sci, 2019, 62(12): 229501, https://doi.org/10.1007/s11432-018-1514-y

Dear editor,

A popular image encryption scheme is the dual-scrambling scheme that combines position transformation and bit-plane transformation. This scheme makes the image chaotic by changing the coordinate positions of image pixels and permutation of the image bit-plane. Moreover, the decrypted image is the same as the original image. Imminent scholars have proposed dual-scrambling schemes to facilitate the quantum image encryption [1–3]. This represents Arnold transformation, Gray-Code transformation or chaotic transformation. However, these schemes are based on a certain quantum image representation model in entangled quantum systems [4], such as a flexible representation of quantum images [5], a novel enhanced quantum representation [6], and a novel quantum representation of color quantum digital images [7].

However, some shortcomings in the previous studies are identified: (i) Some scrambling algorithms have periodic characteristics. The original image is periodically recovered, and the confidentiality of the image cannot be guaranteed. (ii) Owing to the limit of the selected quantum image representation, these scrambling algorithms are unsuitable for arbitrary image resolution and limited to the actual problem resolutions. (iii) When the complexity is higher, some scrambling transformations must be iterated several times for encryption efficiency.

This study aims to propose a quantum image dual-scrambling encryption scheme, which is adapted to arbitrary image resolution based on the generalized quantum image representation (GQIR) [8], and has low computational complexity. No iterative transformation is identified. In this dual-scrambling scheme, each scrambling is implemented using a permutation matrix constructed by a random permutation.

In a permutation matrix P, each row and each column of the square matrix have one and only one element 1, and the other elements are all zero. Given an $m \times n$ matrix A, the matrix $P_m A P_n$ is chaotic. Based on the properties of P, restoring the scrambled matrix $P_m A P_n$ to the matrix A is easy, i.e., $A = P_m^{\mathrm{T}} P_m^A P_n P_n^{\mathrm{T}}$. Depending on the state of the random number generator s, a random permutation refers to a permutation of the integers from 1 to n, where n is a non-negative integer and $s < 2^{32}$. When s is unchanged, the random permutation is unchanged. Therefore, we can get a fixed random permutation by controlling the random number generator s.

The dual-scrambling encryption scheme. The proposed dual-scrambling scheme is divided into encryption and decryption processes. As shown in Figure 1, the encryption process is divided into GQIR representations, bit-plane scrambling, and pixel position scrambling. Meanwhile, the decryp-

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

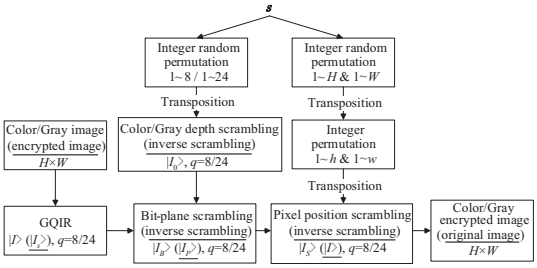

Figure 1 The encryption (decryption) processes of our dual-scrambling scheme.

tion process is the inverse of the encryption process.

An arbitrary $H \times W$ quantum image is represented as $|I\rangle$ based on GQIR model, and the bits in the same order of all pixels form a bit plane. The k-th bit-plane image $|I^k\rangle$ is represented as

$$|I^k\rangle = \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |C_{YX}^k\rangle |YX\rangle, \tag{1}$$

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

where $C_{YX}^k \in \{0, 1\}$ represents the binary value of the corresponding pixel position $|YX\rangle$, $k \in \{0, 1, \ldots, q-1\}$.

The scrambling of q bit-plane images is achieved by a series of two-tuples and controlled-not gates (CNOT). Based on the generating factor s, we obtain a random permutation of the integers from 1 to q, represented by $(k_1\ k_2\ \cdots\ k_q)$. Then, we obtain a series of two-tuples $(1\ k_1)$, $(2\ k_2)$, $\ldots$, $(q\ k_q)$. Moreover, we construct q-qubit color/gray depth of each pixel position with state $|0\rangle$, such as $|0^{k_1-1}\rangle$, $|0^{k_2-1}\rangle$, $\ldots$, $|0^{k_q-1}\rangle$. Further, the scrambling of q-qubit color/gray depth is achieved as follows:

$$\begin{cases} \text{CNOT } |C_{YX}^0, 0^{k_1-1}\rangle \to |C_{YX}^0, \dot{C}_{YX}^{k_1-1}\rangle, \\ \text{CNOT } |C_{YX}^1, 0^{k_2-1}\rangle \to |C_{YX}^1, \dot{C}_{YX}^{k_2-1}\rangle, \\ \quad \vdots \\ \text{CNOT } |C_{YX}^{q-1}, 0^{k_q-1}\rangle \to |C_{YX}^{q-1}, \dot{C}_{YX}^{k_q-1}\rangle, \end{cases} \tag{2}$$

where $|C_{YX}^{q-1} C_{YX}^{q-2} \cdots C_{YX}^0\rangle$ is the original color /gray depth, and $|\dot{C}_{YX}^{k_1-1}\rangle, |\dot{C}_{YX}^{k_2-1}\rangle, \ldots, |\dot{C}_{YX}^{k_q-1}\rangle$ represent the binary values of the corresponding pixel position $|YX\rangle$, respectively. Based on the properties of the permutation matrix, according to the order from small to large in $(k_1 - 1 \quad k_2 - 1 \quad \cdots \quad k_q - 1)$, $|\dot{C}_{YX}^{k_1-1}\rangle$, $|\dot{C}_{YX}^{k_2-1}\rangle$, $\ldots$, $|\dot{C}_{YX}^{k_q-1}\rangle$ are represented by $|\dot{C}_{YX}^{q-1} \dot{C}_{YX}^{q-2} \cdots \dot{C}_{YX}^0\rangle$, which is the scrambled color/gray depth.

We construct q bit-planes with state $|0\rangle$, such as $|I_0^{k_1-1}\rangle$, $|I_0^{k_2-1}\rangle, \ldots, |I_0^{k_q-1}\rangle$. Based on these two-tuples and controlled-not gates, the scrambling of q bit-plane images is achieved as follows:

$$\begin{cases} \text{CNOT } |I^0, I_0^{k_1-1}\rangle \to |I^0, I_B^{k_1-1}\rangle, \\ \text{CNOT } |I^1, I_0^{k_2-1}\rangle \to |I^1, I_B^{k_2-1}\rangle, \\ \quad \vdots \\ \text{CNOT } |I^{q-1}, I_0^{k_q-1}\rangle \to |I^{q-1}, I_B^{k_q-1}\rangle, \end{cases} \tag{3}$$

where $|I^{q-1} I^{q-2} \cdots I^0\rangle$ and $|I_B^{q-1} I_B^{q-2} \cdots I_B^0\rangle$ are the original and the scrambled bit-planes, respectively (Example 1 in Appendix A).

Pixel position scrambling is performed in sequence of Y and X coordinates. According to the number H of an $H \times W$ quantum image and the same generating factor s, we obtain a random permutation of the integers from 1 to H, represented by $(k_1\ k_2\ \cdots\ k_H)$. Moreover, two-tuples $(1\ k_1)$, $(2\ k_2)$, $\ldots$, $(H\ k_H)$ are achieved.

Let $(M\ k_M) \in \{(1\ k_1),\ (2\ k_2),\ \ldots,\ (H\ k_H)\}$, M and k_M represent row-numbers of original quantum image and scrambled quantum image, respectively. In this $H \times W$ quantum image, h qubits ($h = \lceil \log_2 H \rceil$) need to represent Y-coordinate, that is, $|M\rangle = |y_{h-1} y_{h-2} \cdots y_0\rangle$, and $|k_M\rangle = |\dot{y}_{h-1} \dot{y}_{h-2} \cdots \dot{y}_0\rangle$. Then, the scrambling of Y-coordinates is achieved as follows:

$$\begin{cases} \text{CNOT } |y_0, 0_{u_0}\rangle \to |y_0, \dot{y}_{u_0}\rangle, \\ \text{CNOT } |y_1, 0_{u_1}\rangle \to |y_1, \dot{y}_{u_1}\rangle, \\ \quad \vdots \\ \text{CNOT } |y_{h-1}, 0_{u_{h-1}}\rangle \to |y_{h-1}, \dot{y}_{u_{h-1}}\rangle, \end{cases} \tag{4}$$

where $|y_{h-1} y_{h-2} \cdots y_0\rangle$ and $|\dot{y}_{h-1} \dot{y}_{h-2} \cdots \dot{y}_0\rangle$ are the original and the scrambled Y-coordinates of a pixel position, respectively. The scrambling of X-coordinates is similar to that of Y-coordinates (Algorithm B1 in Appendix B).

The bit-plane inverse scrambling and pixel position inverse scrambling are performed in sequence when an encrypted image is decrypted.

Similar to the bit-plane scrambling, based on the same generation factor s, we obtain a series of two-tuples. But we need to transpose these two-tuples. Further, the inverse scrambling of q-qubit color/gray depth $|C_{YX}^{q-1} C_{YX}^{q-2} \cdots C_{YX}^0\rangle$ and the inverse scrambling of q bit-plane images $|I_P^{q-1} I_P^{q-2} \cdots I_P^0\rangle$ are achieved (Example 2 in Appendix A).

The pixel position inverse scrambling is the scrambling of the Y and X coordinates, respectively, similar to the pixel position scrambling (Algorithm B2 in Appendix B).

Simulation and analysis. To evaluate the effectiveness of our scheme, we perform simulation experiments on the classical computer using Matlab. Here s is set to 10000. Experimental results show that the color value histograms of the encrypted images are smoother and significantly different from that of the original images. Hence, the results fail to provide any clues to the statistical attack and differential attack. The correlation coefficients of the simulation are close to 0, indicating that these images after encryption approximate the corresponding original images (more details are in Appendix C.1).

The larger the keyspace is, the more attacks the encryption algorithm resists. The Mersenne Twister algorithm [9] is a popular random number generator, and the small cycle of this algorithm in many software packages is 2^{32}. A GQIR image needs q qubits to represent the gray/color level. In our scheme, the scrambling space of the bit plane is $q!$. So the keyspace of the bit-plane scrambling of a color image is $24! > 2^{32}$, larger than that of [3].

For a $2^h \times 2^w$ GQIR image, the keyspace of our pixel position scrambling algorithm is $\min\{\lceil \log_2 H \rceil !, 2^{32}\} \times \min\{\lceil \log_2 W \rceil !, 2^{32}\}$. Owing that the resolution of the practical image is usually average, particularly when the row number or the column number of an image is less than 8192, the keyspace of our scheme is larger than that of [3] (more details are in Appendix C.2).

In quantum computers, computational complexity is often used to measure the time and cost of the algorithm, and its value depends on the number of basic logic gates in circuits. Our dual-scrambling scheme contains two parts: bit-plane scrambling and pixel position scrambling. According to (3), qCNOT gates are used only once in bit-plane scrambling for q-qubit color/gray depth quantum image. In pixel position scrambling, hCNOT gates and wCNOT gates are used once for $H \times W$ quantum image. Thus, the computational complexity of our scheme is $q + h + w$, less than $8qh+q$ for $2^h \times 2^h$ image in [2]. Moreover, our scheme can be applied to the non-square quantum image (more details are in Appendix C.3).

Conclusion. A quantum image dual-scrambling encryption scheme is proposed, in which the quantum image with arbitrary resolution is gray or true color. The permutations of bit-planes, rows, and columns are uniquely generated according to the same random generator s. Based on the selected s, dual-scrambling and the corresponding inverse scrambling are executed in sequence. For bit-plane scrambling, row scrambling, and column scrambling, we can select three different generators s_b, s_h and s_w as the keys to increase the difficulty of exhaustive attack. The simulation results on the classical computer show that our encryption scheme is efficient. Compared with the existing schemes, the proposed scheme has advantages in keyspace and computational complexity.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61671087), the Fund of the Fundamental Research Funds for the Central Universities (Grant No. 2019XD-A02), and the Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 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, 2015, 14: 1193–1213
2 Heidari S, Vafaei M, Houshmand M, et al. A dual quantum image scrambling method. Quantum Inf Process, 2019, 18: 9
3 Zhou R G, Sun Y J, Fan P. Quantum image gray-code and bit-plane scrambling. Quantum Inf Process, 2015, 14: 1717–1734
4 Xu G, Xiao K, Li Z P, et al. Controlled secure direct communication protocol via the three-qubit partially entangled set of states. Comput Mater Continua, 2019, 58: 809–827
5 Le P Q, Dong F Y, Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf Process, 2011, 10: 63–84
6 Zhang Y, Lu K, Gao Y, et al. A novel quantum representation for log-polar images. Quantum Inf Process, 2013, 12: 3103–3126
7 Sang J Z, Wang S, Li Q. A novel quantum representation of color digital images. Quantum Inf Process, 2017, 16: 42
8 Jiang N, Wang J, Mu Y. Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. Quantum Inf Process, 2015, 14: 4001–4026
9 Matsumoto M, Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Trans Model Comput Simul, 1998, 8: 3–30