Proceedings of the Federated Conference on Computer Science and Information Systems pp. 555–559
DOI: 10.15439/2017F163
ISSN 2300-5963 ACSIS, Vol. 11

# Quantum color image encryption based on multiple discrete chaotic systems

Li Li
Shenzhen Institute of Information Technology, Shenzhen, 518172, China
Email: lili_sziit2014@163.com

Bassem Abd-El-Atty, Ahmed A. Abd El-Latif
Mathematics Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
Email: {bassimeldeeb, a.rahiem}@gmail.com

Ahmed Ghoneim
Mathematics Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
Email: amghoneim@googlemail.com

***Abstract*—In this paper, a novel quantum encryption algorithm for color image is proposed based on multiple discrete chaotic systems. The proposed quantum image encryption algorithm utilize the quantum controlled-NOT image generated by chaotic logistic map, asymmetric tent map and logistic Chebyshev map to control the XOR operation in the encryption process. Experiment results and analysis show that the proposed algorithm has high efficiency and security against differential and statistical attacks.**

## I. Introduction

QUANTUM information processing is a great of current interest for computer, mathematics, and physical scientists. It is a discipline devoted to the development of novel quantum protocols/algorithms for storing, processing, and retrieving visual information [1]. It will likely lead to a new way of technological innovations in computation, communication, image processing and cryptography since the quantum computation could overcome the inefficiency on classical computers [2].

The feature of quantum parallelism is utilized in quantum image processing to speed up various processing tasks such as quantum image encryption [3-11], quantum image steganography [12, 13], quantum image watermarking [14] and so on. Quantum image encryption is widely used to assure security in the information hidden into those images [3]. The algorithms for quantum image encryption could be mainly classified into three types: quantum scrambling, quantum diffusion and combination between them. The first task of quantum image processing is to capture and store the image on quantum computers. Quantum image can be represented for flexible processing by several methods like NEQR, FRQI, NCQI, etc. [15, 16].

In 2013, a quantum image encryption algorithm based on quantum Fourier transform and double random-phase encoding is proposed in Yang et al.'s work [4]. In 2014, based on color and restricted geometric transformations, Song et al. [3] presented a new quantum image encryption algorithm. One year later, based on double random-phase encoding and generalized Arnold transform, a quantum image encryption algorithm is proposed by Zhou et al. [8]. In 2016, based on image XOR operations, Gong et al. [9] designed a quantum image encryption algorithm in which Chen's hyper-chaotic system is used to control the controlled-NOT operation. Also in the same year, Liang et al. [7] proposed a quantum image encryption algorithm based on generalized affine transform and image XOR operations controlled by logistic map. In 2017, by using iterative Arnold transforms and a hyper-chaotic system to control image cycle shift operations, a quantum image encryption algorithm is presented in Zhou et al.'s work [10]. However all quantum image encryption algorithms mentioned above used to encrypt only quantum gray-level images not quantum color images. In 2016, based on Chen's hyper-chaotic system, a quantum color image encryption algorithm is proposed in Tan et al.'s work [11]. To the best of our knowledge, in the earlier works, there is no quantum image encryption algorithm based on multiple discrete chaotic systems (e.g. logistic Chebyshev map and asymmetric tent map) for color images to increase the security of the encryption algorithm. So, the study of utilizing multiple discrete chaotic systems in quantum color image encryption algorithms is required.

In this paper, a novel quantum color image encryption algorithm is proposed based on multiple discrete chaotic maps. The proposed algorithm utilized the quantum controlled not image generated by logistic map, asymmetric tent map and logistic Chebyshev map. The quantum circuit of the proposed algorithm is devised based on NCQI [16] quantum color image representation. Based on simulations results and numerical analyses, the proposed quantum color image algorithm demonstrates the efficiency as well as security against differential and statistical attacks.

## II. Basic Recalls and Preliminary Knowledge

### A. Quantum color image representation

In this section, we give a brief overview of the novel quantum representation for color images (NCQI) [16], which is the basis of the proposed algorithm. For each pixel in an image, the NCQI model consists of color

information $|c_i\rangle$ and its corresponding position information $|i\rangle$. The representative expression of a quantum color image can be expressed as follows.

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle, |c_i\rangle = |c_i^{23}....c_i^1c_i^0\rangle, c_i^k \in \{0,1\} \quad (1)$$

For more details about NCQI representation see [16].

*B. Chaotic systems*

*1) The logistic map*

The definition of the logistic map can be seen as in Eq (2).

$$x_{i+1} = \delta x_i\left(1-x_i\right) \quad (2)$$

where $x_0 \in (0,1)$ and $\delta \in (0,4)$ are the initial value and control parameter respectively.

*2) The asymmetric tent map*

The definition of the asymmetric tent map can be seen in Eq.(3) which is the enhanced version ofthe tent map.

$$y_{i+1} = \begin{cases} \dfrac{y_i}{\beta} & for\ y_i < \beta \\ \dfrac{(1-y_i)}{(1-\beta)} & for\ y_i \geq \beta \end{cases} \quad (3)$$

where $\beta \in (0,1)$ and $y_0 \in (0,1)$ are the control parameter and initial value in the map respectively [17].

*3) The logistic Chebyshev map*

The definition of the logistic Chebyshev map [18] can be seen in Eq(4).

$$z_{i+1} = \left[\alpha z_i\left(1-z_i\right) + \frac{(4-\alpha)\cos(a\times\arccos(z_i))}{4}\right]\bmod 1 \quad (4)$$

where $z_0 \in (0,1)$ is the initial value and $\alpha \in (0,4)$ is a control parameter. $a \in N$ refers to the degree of the Chebyshev map.

## III. Proposed Quantum Image Encryption Algorithm

In this section, we introduce a quantum color image encryption algorithm utilizing quantum controlled not image which is obtained by the multiple discrete chaotic systems. In the proposed algorithm, multiple chaotic maps are used to generate the controlled not image, such as chaotic logistic map, asymmetric tent map and logistic Chebyshev map shows the quantum circuit of the proposed encryption algorithm.

The encryption procedures of the proposed algorithm are illustrated as following:

**Step 1:** select initial value for $x_i$ and value for δ where $x_0 \in (0,1)$, $3.85 \leq \delta \leq 4$ as a secrete keys in the Logistic map.

$x_{i+1} = \delta x_i\left(1-x_i\right)$, **w**here i= 0, 1, 2, ……., $2^{2n}$ , ( $2^{2n}$ is the image size).

**Step 2:** select initial value for $y_i$ and value for β where $y_0 \in (0,1)$, $\beta \in (0,1)$ as a secrete keys in the asymmetric tent map.

$$y_{i+1} = \begin{cases} \dfrac{y_i}{\beta} & for\ y_i < \beta \\ \dfrac{(1-y_i)}{(1-\beta)} & for\ y_i \geq \beta \end{cases}$$

where i= 0, 1, 2, ……., $2^{2n}$ , ( $2^{2n}$ is the image size).

**Step 3:** select initial value for $z_i$ and value for α where $z_0 \in (0,1)$, $\alpha \in (0,4)$ as a secrete key in the logistic Chebyshev map.

$$z_{i+1} = \left[\alpha z_i\left(1-z_i\right) + \frac{(4-\alpha)\cos(a\times a\cos(z_i))}{4}\right]\bmod 1$$

**w**here i= 0, 1, 2, ……., $2^{2n}$ , ( $2^{2n}$ is the image size).

**Step 4:** transform the three sequences $\{x_i\}$, $\{y_i\}$ and $\{z_i\}$ that generated from chaotic maps into integer sequences as follows:

$$x_i^* = |fix((x_i - fix(x_i))\times 10^{14})|\ mod\ 256$$
$$y_i^* = |fix((y_i - fix(y_i))\times 10^{14})|\ mod\ 256$$
$$z_i^* = |fix((z_i - fix(z_i))\times 10^{14})|\ mod\ 256$$

**Step 5:** generate the three layers of controlled color image using the three sequences $\{x_i^*\}$, $\{y_i^*\}$ and $\{z_i^*\}$ then transformation it to quantum color image.

$$|J\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle\otimes|j\rangle, |c_j\rangle = |c_j^{23}....c_j^1c_j^0\rangle, c_j^k \in \{0,1\}$$

**Step 6:** Transform the original image into quantum form as follows:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle, |c_i\rangle = |c_i^{23}....c_i^1c_i^0\rangle, c_i^k \in \{0,1\}$$

**Step 7:** The quantum color image $|I\rangle$ encrypted by applying the controlled-not operations controlled by the quantum color image $|J\rangle$ as shown in Fig. 1.

## IV. NUMERICAL RESULTS

To simulate the proposed quantum color image algorithm, a personal computer with Intel Core™ 2Duo CPU 3.00 GHz and 4 GB RAM equipped with software MATLAB R2009b (version 7.9.0.529) are used to perform operations on quantum images. Lena and baboon images of size $(256\times256)$ are used as the test images (see Figure 2). The simulation parameters as a secret keys used in logistic map are $x_0=0.321$ and $\delta=3.9842$, in asymmetric tent map $y_0=0.5678$ and $\beta=0.7$ and in logistic Chebyshev map $z_0=0.345$ , $a=222$ and $\alpha=3.2$.

### A. Correlation of adjacent pixels

In ordinary images each two pixels are highly correlated with each other, so correlation coefficients in each direction (vertical, horizontal and diagonal) close to 1 while in encrypted images using a good encryption algorithm close to 0. Table 1 stated the correlation coefficients between adjacent two pixels in each direction for the encrypted images and their corresponding original images. Figs 3, 4 and 5 show the correlations of two neighboring horizontal, vertical and diagonal pixels in red, green and blue values, respectively for Lena image. It is obviously that the correlations coefficients for the encrypted images are close to 0. So that, there is no information obtained about the original image by analysis the correlations of neighborhood pixels for encrypted image.

### B. Histogram analysis

Image histogram is an essential tool to assess the performance of any image encryption algorithm. It demonstrates the frequency distribution of pixel values in one image. The good secure encryption algorithm should resist against various brute force attacks by ensuring the uniform histograms in different encrypted images. The histograms of RGB pixel values for image Lena before and after encryption process are shown in Fig. 6. It can be seen from Fig. 6, the histograms of RGB pixel values for original image are completely different from the histograms of their corresponding encrypted image and the histograms that belong to encrypted image are very similar with each other. So we can conclude that the histogram analysis attacks can be resisted in the proposed quantum color image algorithm.

### C. Key space analysis

Key space is the space of several keys that can be used in attack process. Large key space to resist the brute-force attack is an another tool to evaluate the security for a good image encryption algorithm. The proposed algorithm has six initial values that have infinite decimals points for $x_o$, $y_o$, $z_o$, δ, β and α in addition to $a$ as a secret keys. The key space of $x_o$ only is $10^{14}$. Also $y_o$ and $z_o$ each of them have key space $10^{14}$. Thus the total key space of proposed algorithm is $10^{42}$, in addition the key spaces of δ, α and β.

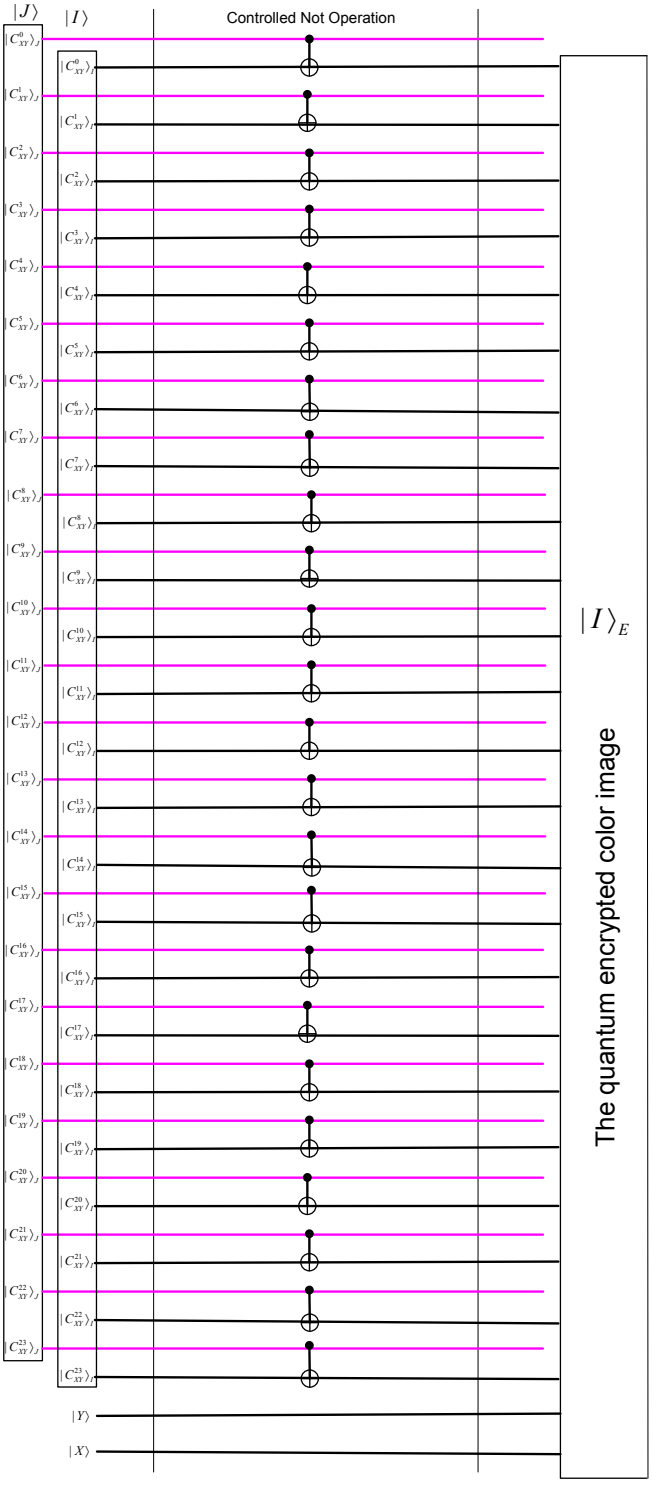
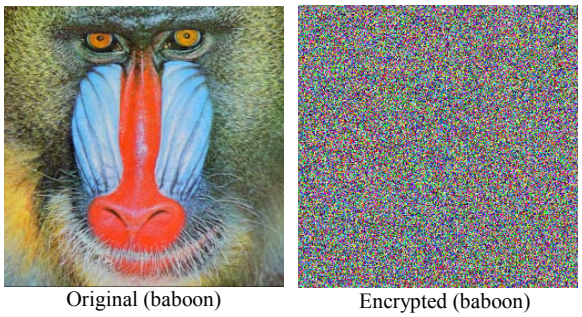



Fig. 1: the quantum circuit for the quantum color image encryption algorithm

Original (Lena) Encrypted (Lena)



Original (baboon) Encrypted (baboon)

Fig. 2: Test results of images

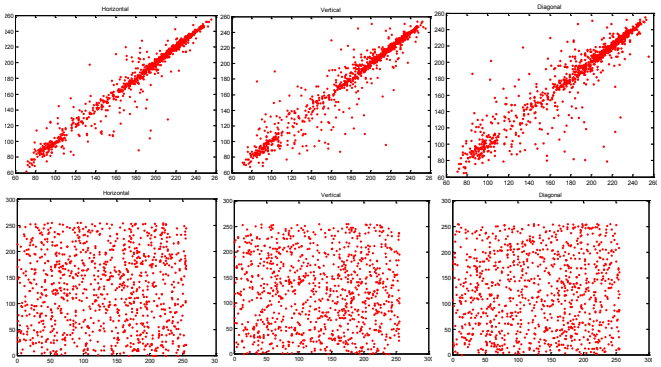


Fig. 3: Correlations of two neighboring horizontal, vertical and diagonal pixels for Lena image in red color.

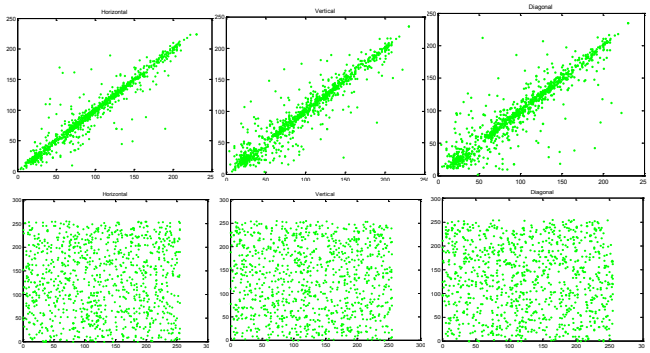


Fig. 4: Correlations of two neighboring horizontal, vertical and diagonal pixels for Lena image in green color.

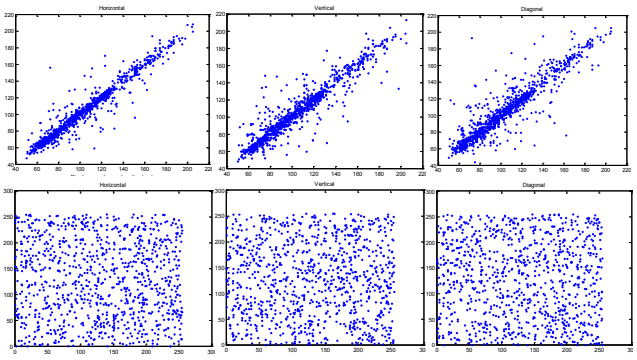


Fig. 5: Correlations of two neighboring horizontal, vertical and diagonal pixels for Lena image in blue color.

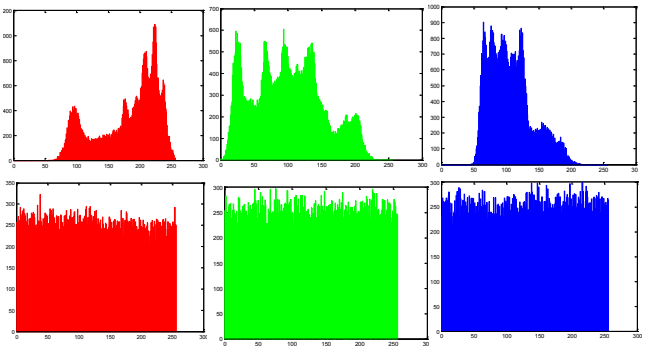
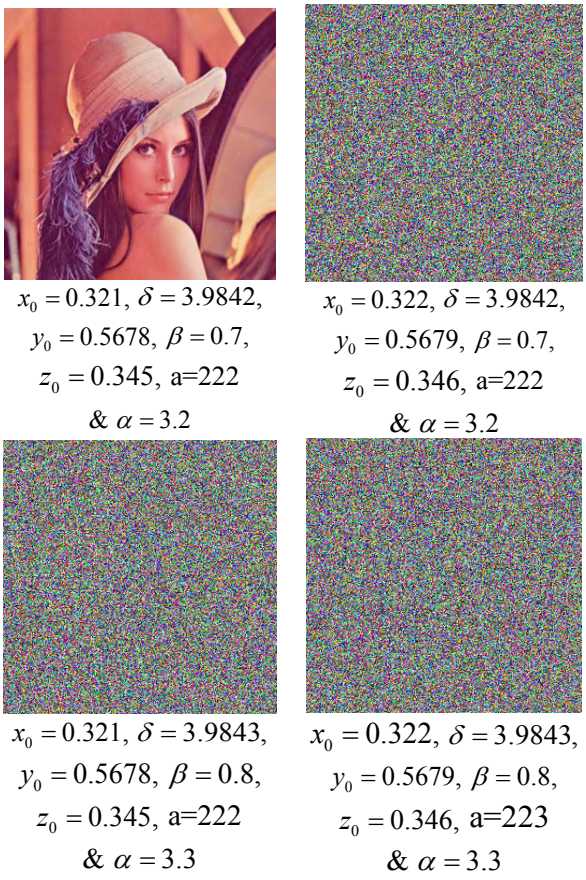


Fig. 6: Histograms of original and encrypted image Lena.



$x_0 = 0.321,\ \delta = 3.9842,$ $y_0 = 0.5678,\ \beta = 0.7,$ $z_0 = 0.345,$ a=222 & $\alpha = 3.2$

$x_0 = 0.322,\ \delta = 3.9842,$ $y_0 = 0.5679,\ \beta = 0.7,$ $z_0 = 0.346,$ a=222 & $\alpha = 3.2$

$x_0 = 0.321,\ \delta = 3.9843,$ $y_0 = 0.5678,\ \beta = 0.8,$ $z_0 = 0.345,$ a=222 & $\alpha = 3.3$

$x_0 = 0.322,\ \delta = 3.9843,$ $y_0 = 0.5679,\ \beta = 0.8,$ $z_0 = 0.346,$ a=223 & $\alpha = 3.3$

Fig. 7: Decrypted image Lena with several keys

TABLE I.
CORRELATION COEFFICIENTS OF ADJACENT PIXELS

| image | direction | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Vertical | | | Horizontal | | | Diagonal | | |
| | R | G | B | R | G | B | R | G | B |
| Original (Lena) | 0.9512 | 0.9496 | 0.9408 | 0.9796 | 0.9639 | 0.9649 | 0.9279 | 0.9179 | 0.9190 |
| Encrypted (Lena) | 0.0282 | 0.0035 | -0.0137 | -0.0348 | 0.0207 | -0.0357 | 0.0212 | -0.0464 | -0.0422 |
| Original (baboon) | 0.9460 | 0.8634 | 0.9281 | 0.9089 | 0.8582 | 0.9203 | 0.9011 | 0.7992 | 0.8876 |
| Encrypted (baboon) | -0.0088 | -0.0206 | 0.0215 | 0.0305 | 0.0296 | 0.0101 | -0.0128 | -0.0279 | 0.0146 |

### *D. Key sensitivity analysis*

Key sensitivity is known as the sensitivity of the secret key to decrypt effect which is the essential property for good image encryption algorithm. To ensure the key sensitivity in the proposed algorithm, the following tests were carried out with several keys as shown in Fig. 7.

## V. CONCLUDING REMARKS

This paper has presented a quantum color image encryption algorithm by utilizing multiple discrete chaotic maps. It used the quantum controlled not image generated by multiple maps. Based on NCQI quantum color image representation, the quantum circuit of the proposed quantum encryption algorithm for color image is devised. The simulations results and numerical analyses show that the proposed algorithm has high efficiency and security against several attacks.

## ACKNOWLEDGMENT

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at king Saud University for funding this Research group NO.(RGP#229). Also, this work is supported by Guangdong Natural Science Foundation: 2015A030310172.

## REFERENCES

[1] Michael A. Nielsen, Isaac L. Chuang ” Quantum computation and quantum information, Cambridge Series on Information and the Natural Sciences, Cambridge University press, Cambridge, (2000).

[2] S. E. Venegas-Andraca, J. L. Ball ” Processing images in entangled quantum systems”, Quantum Information Processing, February 2010, Volume 9, Issue 1, pp 1–11.

[3] Xianhua Song, Shen Wang, Ahmed A. Abd El-Latif, Xiamu Niu, “Quantum Image Encryption based on restricted geometric and color transformations” Quantum Information Processing, August 2014, Volume 13, Issue 8, pp 1765–1787.

[4] Yu-Guang Yang, Juan Xia, Xin Jia, Hua Zhang "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding" Quantum Information Processing, November 2013, Volume 12, Issue 11, pp 3477–3493.

[5] Shen Wang, Xianhua Song, and Xiamu Niu "A Novel Encryption Algorithm for Quantum Images Based on Quantum Wavelet Transform and Diffusion," . In: Pan JS., Snasel V., Corchado E., Abraham A., Wang SL. (eds) Intelligent Data analysis and its Applications, Volume II. Advances in Intelligent Systems and Computing, vol 298. Springer, Cham.

[6] Ri-Gui Zhou, Ya-Juan Sun, Ping Fan “Quantum image Gray-code and bit-plane scrambling,” Quantum Information Processing, May 2015, Volume 14, Issue 5, pp 1717–1734.

[7] Hao-Ran Liang, Xiang-Yang Tao, Nan-Run Zhou "Quantum image encryption based on generalized affine transform and logistic map," Quantum Information Processing, July 2016, Volume 15, Issue 7, pp 2701–2724.

[8] Nan Run Zhou, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, Qing Hong Liao "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," Quantum Information Processing, April 2015, Volume 14, Issue 4, pp 1193–1213 .

[9] Li-Hua Gong, Xiang-Tao He, Shan Cheng, Tian-Xiang Hua, Nan-Run Zhou "Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations," International Journal of Theoretical Physics, July 2016, Volume 55, Issue 7, pp 3234–3250.

[10] Nanrun Zhou, Yiqun Hu, Lihua Gong, Guangyong Li " Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations" Quantum Information Processing, 2017, DOI 10.1007/s11128-017-1612-0.

[11] Ru-Chao Tan,Tong Lei, Qing-Min Zhao, Li-Hua Gong, Zhi-Hong Zhou3 "Quantum Color Image Encryption Algorithm Based on A Hyper-Chaotic System and Quantum Fourier Transform, " International Journal of Theoretical Physics, 2016, DOI 10.1007/s10773-016-3157-x.

[12] Bassem Abd-El-Atty, Ahmed A. Abd El-Latif, Mohamed Amin "New quantum image steganography scheme with Hadamard transformation, " International Conference on Advanced Intelligent Systems and Informatics. Springer International Publishing, 2016, pp 342-352.

[13] Tiejun Zhang, Bassem Abd-El-Atty, Ahmed A. Abd El-Latif and Mohamed Amin " QISLSQb : A quantum image steganography scheme based on Least Significant Qubit," International Conference on Mathematical, Computational and Statistical Sciences and Engineering , 2016.

[14] X.H. Song, S. Wang, S. Liu, A.A. Abd El-Latif, X.M. Niu "A dynamic watermarking scheme for quantum images using quantum wavelet transform, " Quantum Inf. Process, 2013, Volume 12, Issue 12, pp 3689-3706.

[15] Fei Yan, Abdullah M. Iliyasu, Salvador E. Venegas-Andraca "A survey of quantum image representations," Quantum Information Processing, January 2016, Volume 15, Issue 1, pp 1–35.

[16] Jianzhi Sang, Shen Wang, Qiong Li “A novel quantum representation of color digital images,” Quantum Information Processing, February 2017, 16:42.

[17] Akram Belazi, Ahmed A. Abd El-Latif, Adrian-Viorel Diaconu, Rhouma Rhouma, Safya Belguith “Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms,” Optics and Lasers in Engineering, Volume 88, January 2017, Pages 37–50.

[18] Akram Belazi, Majid Khan, Ahmed A. Abd El-Latif, Safya Belguith “Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption,” Nonlinear Dynamics, January 2017, Volume 87, Issue 1, pp 337–361.