New Quantum Image Steganography Scheme with Hadamard Transformation

Bassem Abd-El-Atty, Ahmed A. Abd El-Latif(✉),
and Mohamed Amin

Faculty of Science, Department of Mathematics,
Menoufia University, Shibin Al Kawm 32511, Egypt
ahmed_rahiem@yahoo.com

Abstract. Based on Hadamard transformation and the novel enhanced quantum representation for quantum images (NEQR), a quantum image steganography scheme to embed a quantum text message into a quantum image is proposed. The extraction process can recover the text message with the stego image only. In the earlier works, there is no quantum image steganography algorithm to embed the quantum text message into a quantum image. The simulation results demonstrated that the proposed scheme has high-capacity, good invisibility, and high security.

Keywords: Quantum steganography · Quantum image processing · Hadamard transformation

1 Introduction

Quantum information processing has great deal of attention from both engineers and quantum scientists. The main task of quantum information is to develop new quantum algorithms for processing and storing quantum information. Quantum computer is a machine accepts input quantum states as a superposition of several inputs in another state as output quantum state [1]. Quantum steganography utilizes the effects of quantum mechanics such as quantum computation and quantum communication to achieve tasks of quantum information hiding. Quantum steganography, can be defined as the classical steganography in viewpoint of quantum mechanics, has become important researching area of quantum cryptography [2]. There are four types of quantum steganography classified as per embedding strategies [3]. The first type is information hiding of quantum data [4–10]. The second type is quantum error code [11, 12]. The third type based on the quantum cryptography protocols to hide secret messages [13, 14]. The last type, which based on quantum image processing techniques named as quantum image steganography.

The effects of quantum parallelism used in processing quantum images (PQI) to improve many processing tasks in classical image processing. The first step of PQI is to represent and store the classical images on quantum computers. There are many representations for classical images on quantum computers, such as Entangled Image [15], Real Ket [16], Multi-Channel representation of quantum image [17], log-polar representation [18], flexible representation of quantum images (FRQI) [19], which uses

A.E. Hassanien et al. (eds.), *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2016*, Advances in Intelligent Systems and Computing 533, DOI 10.1007/978-3-319-48308-5_33

number of qubits 2x + 1 to represent a gray image with size 2x × 2x and the NEQR model for represent quantum images [20]. In spite of the used qubits of NEQR increases from 2x + 1 qubits used in FRQI to 2x + q qubits, it is excellent for processing quantum image because the quantum representation is very similar to the representation of a classical image.

Recently, a number of quantum image security algorithms including encryption [21–23] and steganography based on NEQR have been proposed [24–27]. Jiang *et al.* introduced in [24] a scheme based on Moir´e Pattern, which embeds the secret binary image with size 2n × 2n into a cover gray image with size 2n × 2n. Afterward, Jiang *et al*. introduced in [25] a new quantum image steganography algorithm based on LSB, which embeds a message as binary 2n × 2n image into a cover image 2n × 2n gray image.

In the earlier works, there is no previous quantum image steganography algorithm to embed quantum secret message as a text into a quantum image. The quantum image steganography algorithms [24, 25] embed binary images or message as a binary image with maximum capacity one bit per pixel. However, quantum image steganography algorithms [24, 25] were broken to embed quantum text message into a cover image. In this paper, we will propose a quantum image steganography scheme to embed quantum text message instead of a message as an image into a quantum image. It utilizes Hadamard transformation to increase the security of embedded quantum data. Experimental results demonstrated that the maximum capacity increases from one bit per pixel to two bit per pixel in the proposed scheme and the invisibility is good [24, 25].

The rest of this paper is as follows. The Hadamard transformation and NEQR representation model are briefly reviewed in Sect. 2. Section 3 introduced the proposed quantum image steganography scheme. Section 4 gives analyses and results. The comparison with related schemes provided in Sect. 5. Finally, in Sect. 6 the conclusion is drawn.

2 Background

In this section, the NEQR model [20] for representation quantum images and Hadamard transformation are briefly reviewed, which the essentials of the proposed scheme.

2.1 NEQR Quantum Representation

By using the representation pixels idea for images in traditional computers, the NEQR representation is proposed in [20]. The NEQR model has information about the pixels color and its related position of each pixel in the image. The mathematical representation of a quantum image for an $2^n \times 2^n$ image can be expressed as follows.

$$
\begin{gathered}
|I\rangle = \tfrac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle \\
|c_i\rangle = |c_i^{q-1} \ldots c_i^1 c_i^0\rangle,\ c_i^j \in \{0,1\}, i = 0,1,\ldots,2^{2n}-1, j = 0,1,\ldots,q-1
\end{gathered}
\tag{1}
$$

where the sequence $c_i^{q-1}\ldots.c_i^1 c_i^0$ encodes the color value with range 2^q, $|i\rangle$ *for* $i = 2^{2n}-1, \ldots, 1, 0$, *are* 2^{2n} dimension computational basis quantum states. There are two parts of $|I\rangle$ as follows $|c_i\rangle$, which encodes the information about the pixels color and $|i\rangle$ which encodes the information about the related position for colors in the image.

2.2 Hadamard Transformation

The basic unite of classical informationand classicalcomputation is bit. Quantum information and quantum computation are based upon an analogue idea, quantum bit (qubit). Qubits are represented by state vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and a superposition of two states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$

To express the operation of the classical gates, we have used a truth table. For quantum gates, we use matrix representation. Hadamard transformation is represented by the following matrix.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

3 Proposed Quantum Image Steganography Scheme

We introduce a quantum image steganography scheme based on NEQR representation and Hadamard gate in this section. The proposed quantum image steganography procedures are shown in Fig. 1.

3.1 Embedding Process

The proposed quantum image steganography embedding procedures consist of two phases, which are given by the following steps.

Phase 1 Preparation of quantum states

Let the cover image $|I\rangle$ is $2^n \times 2^n$ image and the secrete message encoded into two binary matrixes with size $2^n \times 2^n$.

Note the size of the secrete text message must be less than or equal to $2^{2n-2}(2 \times 2^n \times 2^n\text{bit} = 2 \times 2^n \times 2^n/8 \text{ byte})$ characters.

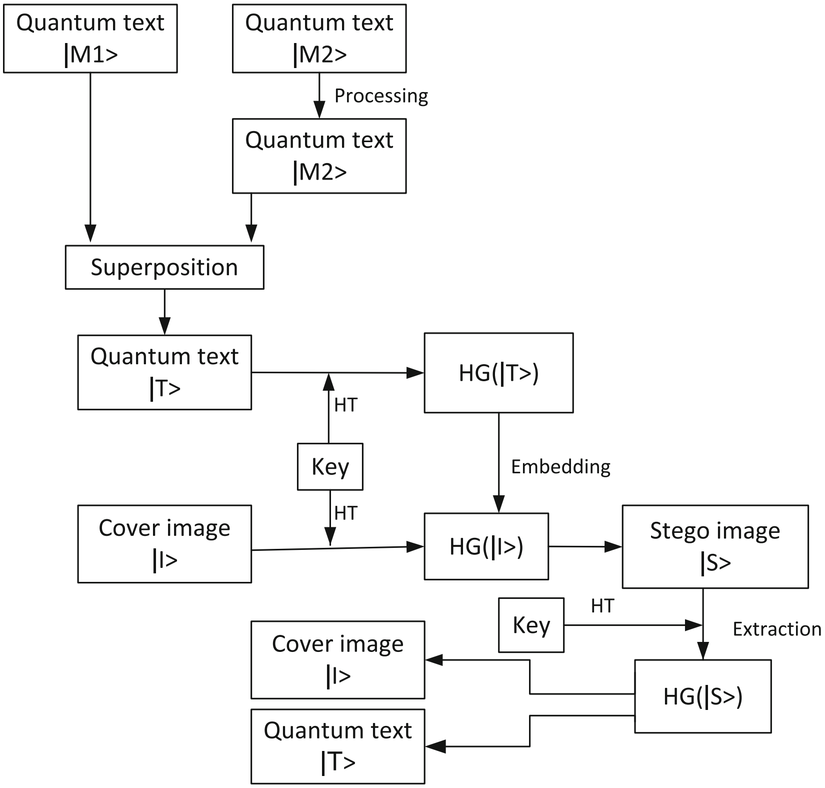


Fig. 1. Embedding and extraction procedures of the proposed quantum image steganography

The NEQR representations of $|I\rangle$, $|M1\rangle$ and $|M2\rangle$ are shown as follows:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle \otimes |i\rangle = |c_i\rangle = |c_i^{q-1}\ldots c_i^1 c_i^0\rangle,\ c_i^j \in \{0,1\} \tag{3}$$

$$|M1\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|m1_i\rangle \otimes |i\rangle,\ |m1_i\rangle = |m1_i^{q-1}\ldots m1_i^1 m1_i^0\rangle,\ m1_i^j \in \{0,1\} \tag{4}$$

$$|M2\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|m2_i\rangle \otimes |i\rangle,\ |m2_i\rangle = |m2_i^{q-1}\ldots m2_i^1 m2_i^0\rangle,\ m2_i^j \in \{0,1\} \tag{5}$$

Note that the representation of quantum text is represented only in m_i^0 and all others $m_i^j = 0$ where j = 1, 2, 3, …., q-1, according to Theorem 1.

Then shift the coefficients of vector |M2⟩ by 2^{2n+1} as follows:

$$|M2_{mod(i+2^{2n+1},2^{2n+q})}\rangle = |M2_i\rangle, i = 1, 2, \ldots, 2^{2n+q} \tag{6}$$

Then take the superposition of the two states |M1⟩ and |M2⟩ to state |T⟩.

$$|T\rangle = \frac{1}{\sqrt{2}}(|M1\rangle + |M2\rangle) \tag{7}$$

Theorem 1 Text message can be represented in quantum computation as

$$|M\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |m1_i\rangle \otimes |i\rangle, m_i \in \{0,1\} \tag{8}$$

where|M⟩ is a vector space with length 2^{2n+1} and i is the position of binary bit m_i after the representation of text message as $2^n \times 2^n$ binary matrix.

Proof To process the text message on quantum computers, the text message information at first should be represented and stored in quantum states by quantum encoding state about bits of the text message and its positions.

From NEQR representation, there are number of 2n +q qubits required to construct the representation for a $2^n \times 2^n$ image with gray range 2^q. There are two values for a bit in a text message 0 or 1 so that we need 2n + 1 qubits to represent a $2^n \times 2^n$ bit matrix for the text message.

Information about bits encoded in $|m_i\rangle$, where $m_i \in \{0, 1\}$ and $|i\rangle$ encodes the position of the related text bits. Information about the position consists of two parts: horizontal and vertical coordinates. By taking into consideration a quantum text message is a system in 2n-qubit,

$$i\rangle = |v\rangle|h\rangle = |v_{n-1}v_{n-2}, \ldots\ldots, v_0\rangle|h_{n-1}h_{n-2}, \ldots\ldots, h_0\rangle, \tag{9}$$

$$h, v \in \{0, 1, \ldots\ldots\ldots, 2^n - 1\},$$

$$|v_k\rangle, |h_k\rangle \in \{|0\rangle, |1\rangle\}, k = 0, 1, 2, \ldots\ldots, n-1,$$

here $|v_{n-1}v_{n-2}, \ldots\ldots, v_0\rangle$ encodes the first n-qubit over the vertical axis and $|h_{n-1}h_{n-2}, \ldots\ldots, h_0\rangle$ by encoding the second n-qubit over the horizontal axis. The state of quantum text message is a normalized as shown in (10),

$$\||M\rangle\| = \frac{1}{2^n}\sqrt{\sum_{i=0}^{2^{2n}-1} |m_i\rangle \otimes |i\rangle} = \frac{1}{2^n}\sqrt{2^{2n}} = \frac{1}{2^n}2^n = 1 \tag{10}$$

Phase 2 Apply unitary Hadamard transformation

Firstly, form unitary Hadamard transformation gate (HG) controlled by secrete key K in binary form where K = k_1k_2 k_3 …k_i…. K_{2n+q}, i = 2, 3, ……., 2n + q, $k_i \in \{0,1\}$, $k_1 = 1$ is to ensure the color qubit transformation.

$$HG = H \bigotimes_{i=2}^{2n+q} H^{k_i}, H^{k_i} = \{ \begin{matrix} H, k_i = 1 \\ I, k_i = 0 \end{matrix} \, i = 2,\ 3,\ \ldots\ldots,\ 2n + q \tag{11}$$

where I is identity matrix in 2-dimantional form and H is the Hadamard transformation matrix.

Then, execute HG on the quantum cover state $|I\rangle$ and quantum text state $|T\rangle$, getting vector HG($|I\rangle$) and vector HG($|T\rangle$) as follows:

$$HG(|I\rangle) = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} HG(|c_i\rangle) \otimes |i\rangle \tag{12}$$

$$HG(|T\rangle) = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} HG(|m_i\rangle) \otimes |i\rangle \tag{13}$$

Then, take the superposition of the two states HG($|I\rangle$) and HG($|T\rangle$) to the stego image state $|\mathrm{S}\rangle$.

$$|S\rangle = \frac{1}{\sqrt{2}}(HG(|I\rangle) + HG(|T\rangle)) \tag{14}$$

3.2 Extraction Operation

At the extraction operation, we utilize the secrete key to extract embedded text message from the quantum cover image. The quantum process is totally revertible, because all used transforms are unitary matrices in quantum computation.

By executing inverse of HT on the stego-image $|\mathrm{S}\rangle$, getting the cover image $|\mathrm{I}\rangle$ and the text message $|\mathrm{M}\rangle$.

$$\begin{aligned} inv(HG(|S\rangle)) &= inv(HG(\frac{1}{\sqrt{2}}(HG(|I\rangle) + HG(|T\rangle)))) \\ &= \frac{1}{\sqrt{2}}(inv(HG(HG(|I\rangle))) + inv(HG(HG(|T\rangle)))) \\ &= \frac{1}{\sqrt{2}}(|I\rangle + |T\rangle) \end{aligned}$$

4 Analyses and Results

We perform the simulation of quantum operations on the classical computer to analyses our proposed scheme. We introduce several analyzes, such as visual quality, payload capacity and security analysis.

4.1 Visual Quality

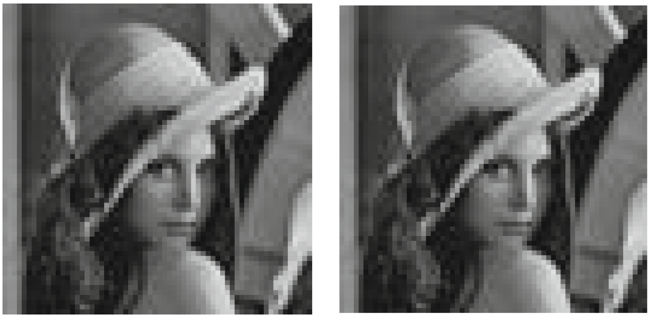
Visual quality is the amount of difference between the stego image and the original cover image in pixels values. There are many quantities to measure the difference of pixels between the stego image and the original cover image; one of the most used quantities is PSNR (peak signal to noise ratio). It is defined as the MSE (mean squared error) for two images X and Y with size i × j.

$$\mathrm{MSE} = \frac{1}{ij}\sum_{x=0}^{i-1}\sum_{y=0}^{j-1}\left[X(x,y) - Y(x,y)\right]^2 \tag{16}$$

PSNR is defined as follows.

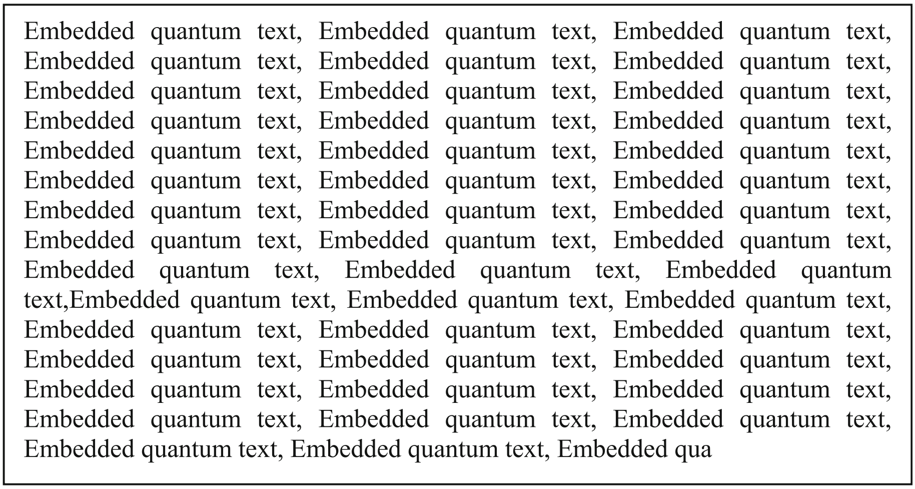
$$\mathrm{PSNR} \ = 20\log_{10}\left(\frac{\mathrm{MAX}_X}{\sqrt{\mathrm{MSE}}}\right) \tag{17}$$

Where, MAX_X is the maximum value of pixels in the cover image *X*. In this scheme, *Y* related to the stego image and *X* related to the original cover image. To simulate the proposed scheme we use images with size 64 × 64 in these experiments. The following Fig. 2 describes experimental results of our scheme and Figs. 3 and 4 describe two different text messages that embedded in the stego image and Table 1 shows the PSNR values among the original cover image and the stego image for different two text messages.



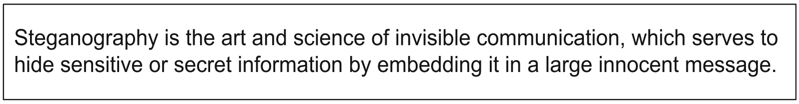
original image stego image

Fig. 2. The visual effects



Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum
text,Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded quantum text,
Embedded quantum text, Embedded quantum text, Embedded qua

Fig. 3. Text message 1 with length 1024 character



Steganography is the art and science of invisible communication, which serves to hide sensitive or secret information by embedding it in a large innocent message.

Fig. 4. Text message 2 with length 165 character

Table 1. PSNR values for different secrete text messages

Secrete message	Cover image
Message1	68.499
Message2	73.27

Obviously, from Fig. 2, human eyes can't identify the difference between the original coverimage and the stego image. From Table 1, the values of PSNR are enough. So our scheme has a good visual effect.

4.2 Payload Capacity

The steganography capacity can be stated as the ratio between the number of embedded bits of the text message and the number of pixels for cover image. The proposed scheme's capacity is given as follows:

$$C = \frac{numberofmessagebits}{numberofcoverimagepixels} = \frac{2 \times 2^n \times 2^n bit}{2^n \times 2^n pixel} = 2\,bit/pixel$$

The proposed algorithm has Payload capacity two bits per pixel, which is higher than of majority of the quantum image steganography algorithms. So we can conclude that our scheme has high-capacity.

4.3 Security Analysis

The embedded text message is same as the extracted text message so that there is no BER (Bit Error Rate) in extracted text message. The extract operation needs only quantum stego image and the binary key. The key utilized to control unitary Hadamard transformation, which is secret. Therefore, the effect of the proposed quantum image steganography scheme based on NEQR for quantum images and Hadamard transformation is excellent and has no error (error-free).

5 Comparison with Related Schemes

From the above section, the proposed algorithm has high PSNR compared to the schemes of [24, 25] based on the simulation results. The payload capacity of our scheme is two bit per pixel while the capacity of algorithms in [24, 25] are one bit per pixel. From Table 2, the proposed scheme has high-capacity, high security, good visual effect and embedding quantum text message instead of a message as an image.

Table 2. Comparison with related schemes

Items	Proposed scheme	Scheme in [24]	Scheme in [25]
Maximum capacity	2 bit/pixel	1 bit/pixel	1 bit/pixel
Security	Yes, using key	No	No
Embedding data	Quantum text message	Binary image	Message as binary image
Visual quality (PSNR) using Lena as cover image	73.27	29.2717	50.8426

6 Conclusion

A quantum image steganography scheme based on NEQR representation of quantum images and Hadamard transformation is proposed. The proposed scheme has good advantages such as the extracting operation does not require the original image or information about the embedded text message. Simulation results proved that the efficiency of the proposed scheme.

Acknowledgements. The authors would like to thank Dr. Li-Hua Gong For the valuable comments. This work was supported by Ministry of Higher Education and Scientific Research (Egypt-Tunisia Cooperation Program: 4-13 A1) and the National Natural Science Foundation of China (61462061 and 61561033).

References

1. Tseng, C.C., Hwang, T.M.: Quantum digital image processing algorithms. In: 16th IPPR Conference on Computer Vision. Graphics and Image Processing. Kinmen, ROC, pp. 827–834 (2003)
2. Xu, S.J., Chen, X.B., Niu, X.X., Yang, X.Y.: High-efficiency quantum steganography based on the tensor product of Bell states. Sci. China **56**, 1745–1754 (2013)
3. Jiang, X.S., Bo, C.X., Xin, N.X., Xian, Y.Y.: Steganalysis and improvement of a quantum steganography protocol via a GHZ4 state. Chin. Phys. B **22**, 060307 (2013)
4. Terhal, B.M., DiVincenzo, D.P., Leung, D.W.: Hiding bits in Bell states. Phys. Rev. Lett. **86**, 5807–5810 (2001)
5. Eggeling, T., Werner, R.F.: Hiding classical data in multipartite quantum states. Phys. Rev. Lett. **89**, 097905 (2002)
6. DiVincenzo, D.P., Leung, D.W., Terhal, B.M.: Quantum data hiding. IEEE Trans. Inf. Theory **48**, 580–598 (2002)
7. Hayden, P., Leung, D., Smith, G.: Multiparty data hiding of quantum information. Phys. Rev. A **71**, 062339 (2005)
8. Guo, G.C., Guo, G.P.: Quantum data hiding with spontaneous parameter down conversion. Phys. Rev. A **68**, 044303 (2003)
9. Chattopadhyay, I., Sarkar, D.: Local indistinguishability and possibility of hiding cbits in activable bound entangled states. Phys. Rev. A **365**, 273–277 (2007)
10. Matthews, W., Wehner, S., Winter, A.: Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. J. Commun. Math. Phys. **291**, 813–843 (2009)
11. Banacloche, J.G.: Hiding messages in quantum data. J. Math. Phys. **43**, 4531 (2002)
12. ShawB, A., Brun, T.A.: Quantum steganography with noisy quantum channels. Phys. Rev. A **83**, 022310 (2011)
13. Zhang, D., Li, X.: A quantum information hiding scheme using orthogonal product states. WSEAS Trans. Comput. **6**, 757–762 (2007)
14. Liao, X., Wen, Q., Sun, Y., Zhang, J.: Multi-party covert communication with steganography and quantum secret sharing. J. Syst. Softw. **83**, 1801–1804 (2010)
15. Venegas-Andraca, S.E., Ball, J.L.: Processing images in entangled quantum systems. Quantum Inf. Process. **9**, 1–11 (2010)
16. Latorre, J.I.: Image compression and entanglement. arXiv: quant-ph/, 0510031 (2005)
17. Sun, B., Le, P.Q., Iliyasu, A.M., Yan, F., Garcia, J.A., Dong, F., Hirota, K.: A multi-channel representation for images on quantum computers using the RGB a color space. In: Proceedings of the IEEE 7th International Symposiumon Intelligent Signal Processing, pp. 1–6 (2011)
18. Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log polar images. Quantum Inf. Process. **12**, 3103–3126 (2013)
19. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression and processing operations. Quantum Inf. Process. **10**, 63–84 (2011)
20. Zhang, Y., Lu, K., Gao, Y., Wang, M.: NEQR: a novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**, 2833–2860 (2013)
21. Hua, T.X., Chen, J.M., Pei, D.J., Zhang, W.Q., Zhou, N.R.: Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theor. Phys. **54**, 526–537 (2015)

22. Zhou, N.R., Hua, T.X., Gong, L.H., Pei, D.J., Liao, Q.H.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process. **14**, 1193–1213 (2015)
23. Liang, H.R., Tao, X.Y., Zhou, N.R.: Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf. Process. **15**, 1–24 (2016)
24. Jiang, N., Wang, L.: A novel strategy for quantum ımage steganography based on Moir´e pattern. Int. J. Theor. Phys. **54**, 1021–1032 (2014)
25. Jiang, N., Zhao, N., Wang, L.: LSB based quantum ımage steganography algorithm. Int. J. Theor. Phys. **55**, 107–123 (2015)
26. Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. Quantum Inf. Process. **14**, 1559–1571 (2015)
27. Wang, S., Sang, J., Song, X., Niu, X.: Least significant qubit (LSQb) ınformation hiding algorithm for quantum ımage. Measurement **73**, 352–359 (2015)