IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 30, 2017, accepted November 22, 2017, date of publication November 27, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2777869

Robust Encryption of Quantum Medical Images

AHMED A. ABD EL-LATIF[1], BASSEM ABD-EL-ATTY[1], AND MUHAMMAD TALHA[2]
[1]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[2]Deanship of Scientific Research, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Ahmed A. Abd El-Latif (a.rahiem@gmail.com)

This work was supported by the Deanship of Scientific Research at King Saud University through the Research Group under Grant RG-1437-037.

ABSTRACT Security of medical media is important for patient safety and confidentiality. This paper proposes a framework for the chaos-based quantum encryption of healthcare images. In the framework, healthcare staff in one location send cipher images to the cloud. The healthcare staff in another location receives the images from the cloud. By decrypting the content of the images, the healthcare staff can assist users in a secure manner. This paper also proposes a novel approach for the efficient quantum image encryption of healthcare media. The proposed algorithm utilizes gray code and a chaotic map. The quantum image is scrambled by quantum gray code. Then, the scrambled quantum image is encrypted using a quantum XOR operation based on a key generator controlled by the logistic-sine map. The circuits of the proposed encryption/decryption algorithm are devised based on an NEQR quantum image representation. Numerical and simulation analyses show that the proposed quantum image encryption approach is robust, realizable, and has high efficiency compared with its classical counterpart.

INDEX TERMS Quantum image encryption, chaotic systems, healthcare.

I. INTRODUCTION

Protecting the information content in digital images is essential today for diverse purposes, from military to healthcare systems [1]–[4], [33]. Advanced encryption techniques for the secure transmission, storage, and retrieval of quantum images are increasingly required for a variety of image-processing applications, especially for medical images. The encryption of patient or user information before its transference over a communications channel or IoT network is important for patient confidentially [5]. Therefore, for healthcare applications, it is quite important to improve suitable approaches to protect medical quantum images.

Indeed, a well-designed healthcare image security method should satisfy the two criteria identified by Shannon [6]: confusion and diffusion. Confusion means the indistinguishability of the cipher image and inability to trace the secret key or plain image from the cipher image. Diffusion means that any changes in either the key or the plain image lead to large changes in the cipher image. The substitution box (S-box) is a nonlinear component many encryption approaches employ to ensure the confusion property [7]. The diffusion property can be verified in chaotic dynamic systems. In fact, chaotic systems or maps have various ultimate features, such as ergodicity, sensitivity to preliminary conditions, and exhibition of random behavior, which can induce both confusion and diffusion in the plain images to obtain secure cipher images.

Quantum mechanics led to the creation of quantum computation and later quantum computers to solve problems that cannot be efficiently solved on traditional computers. In 1982, Feynman introduced the idea of quantum computer, a novel computation model which involves a physical machine that can accept input states as a superposition of many different inputs in another state as output state [8]–[12]. In quantum computers, an image is captured and stored by suitable representation models. The literature offers various representation models for quantum images, such as Real Ket [13]; Entangled Image [14]; Multi-Channel representation of quantum image (MCRQI) [15]; log-polar [16]; flexible representation of quantum images (FRQI) [17], which uses $2n+1$ qubits to represent a $2^n \times 2^n$ gray image; and the novel enhanced quantum representation (NEQR) [18], which uses $2n+q$ qubits to represent a $2^n \times 2^n$ gray image. Although NEQR requires $2n+q$ qubits, which is greater than the qubits required for FRQI, it is good for quantum-image processing, because the quantum color coding is very similar to the color coding in classical images

Recent intensive research efforts are underway around the world to investigate a number of quantum technologies, such as quantum teleportation, quantum cryptography, and

quantum steganography, among many others, which could lead to more powerful quantum computers in the near future. Medical images derived from quantum healthcare systems and transferred into the public cloud present substantial risks to patient safety and confidentiality. Therefore, they should be encrypted or hidden from malicious behavior before sending them to the cloud [3], [19].

Quantum image encryption has attracted considerable attention from both scientists and engineers in recent years. A short overview of the main recently proposed quantum image encryption approaches is given hereafter. Jiang *et al.* [20] introduced quantum scrambling based on the realization of Arnold and Fibonacci transformations. Also, Jiang *et al.* [21] proposed quantum scrambling based on the Hilbert scanning matrix. Zhou *et al.* [22], proposed quantum scrambling for images based on Gray code and the bit-plane. Yang *et al.* [23] introduced a quantum image-encryption algorithm based on double, random-phase encoding and a generalized Arnold transform. Song *et al.* [24], proposed a strategy in which pixel positions are scrambled by restricted geometric transformations and then permutated by restricted color transformations. Zhou *et al.* [25], introduced a quantum encryption algorithm that uses double random-phase operations to encode color information and an Arnold transform to scramble pixel positions. Gong *et al.* [26] proposed an algorithm based on quantum XOR operations generated with a chaotic system to encode gray-level information. Very recently, Liang *et al.* [27] introduced a quantum algorithm based on quantum XOR operations generated with the logistic map to encrypt gray-level information, while the generalized affine transform is used to encode position information. In addition, several papers have been introduced regarding the security of healthcare media [28]–[31]

This paper introduces a new framework for the secure quantum encryption of healthcare images. The healthcare staff on one side send the quantum cipher images to the cloud, while the medical staff on the receiving side retrieves the images from the cloud. Decrypting the content inside the received unintelligible images with the correct keys, staff can securely assist patients. This paper also presents a novel, chaos-based, quantum encryption approach based on gray code and a chaotic logistic-sine map. The quantum image is scrambled using the quantum gray-code. Then, the scrambled quantum image is encrypted using XOR operations based on a key generator controlled by the logistic-sine map. Simulation analyses show that the proposed quantum image encryption approach is robust, realizable, and has higher efficiency than its classical counterpart. In addition, it is fast and suitable for secure images in healthcare systems.

The rest of this paper is organized as follows. Preliminary work for the proposed approach is presented in Section 2. Section 3 offers the framework for secure healthcare media encryption. Section 4 introduces a novel, chaos-based approach to quantum image encryption and decryption. Section 5 analyzes the numerical simulations on a classical computer. Finally, Section 6 concludes.

II. PRELIMINARY KNOWLEDGE

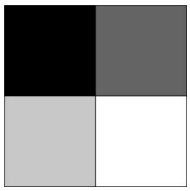
A. NOVEL ENHANCED QUANTUM REPRESENTATION (NEQR)

The NEQR [18] model contains the color information and corresponding position information for every pixel in an image. The mathematical representation of an image in a quantum scenario for $2^n \times 2^n$ is as follows:

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

Where the sequence $c_i^{q-1}....c_i^1 c_i^0$ encodes the color value with color range 2^q , $|i\rangle$ for $i = 0, 1, \ldots, 2^{2n} - 1$ with 2^{2n} dimension computational basis. The two parts in the NEQR: $|c_i\rangle$ and $|i\rangle$ encodes information about the colors and their related positions in the image, respectively.

Figure 1 shows 2×2 NEQR image model.



$$|I\rangle = \frac{1}{2}(|0\rangle\otimes|00\rangle + |100\rangle\otimes|01\rangle + |200\rangle\otimes|10\rangle + |255\rangle\otimes|11\rangle)$$
$$= \frac{1}{2}(|00000000\rangle\otimes|00\rangle + |01100100\rangle\otimes|01\rangle + |11001000\rangle\otimes|10\rangle + |1111111\rangle\otimes|11\rangle)$$

FIGURE 1. An example of 2 × 2 image and its representative expression in NEQR.

B. GRAY CODE

Gray code is a signal coding method and commonly used in the digital conversions. The mathematical formula of the gray code is given by:

$$g_i = t_i \oplus t_{i+1}, i = 0, 1, ..., q - 1 \quad (2)$$
$$g_q = t_q \quad (3)$$

Where t is a positive integer with binary code $t = (t_q t_{q-1}.....t_1 t_0)$

A simple example is shown in Fig. 2.

C. BIT-PLANE

The collection of bits corresponding to a particular bit position of each pixel value of an image is known as a bit plane. For example, the range of pixel values of an image is [0, 255]. Binary form represents this as 8-bit data, so the image has eight bit planes: the eight bit plane contains the least significant bit, and the first contains a collection of the most significant bits. An illustrated example of bit planes of a baboon image is shown in Figure 3.

D. CONTROLLED-NOT OPERATION

In quantum computation, the analogue of the classical XOR gate is the controlled-NOT gate, which has two-inputs:

b3	b2	b1	b0	g3	g2	g1	g0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	1	0
0	1	0	1	0	1	1	1
0	1	1	0	0	1	0	1
0	1	1	1	0	1	0	0
1	0	0	0	1	1	0	0
1	0	0	1	1	1	0	1
1	0	1	0	1	1	1	1
1	0	1	1	1	1	1	0
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	0	0	1
1	1	1	1	1	0	0	0

FIGURE 2. A simple example of gray code.

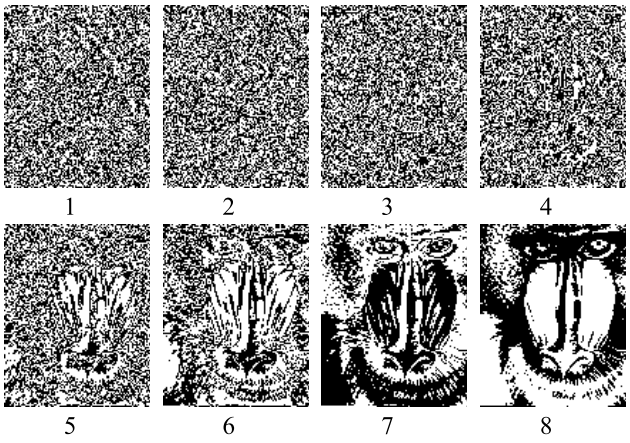


FIGURE 3. Bit-planes of baboon image from 1 to 8.

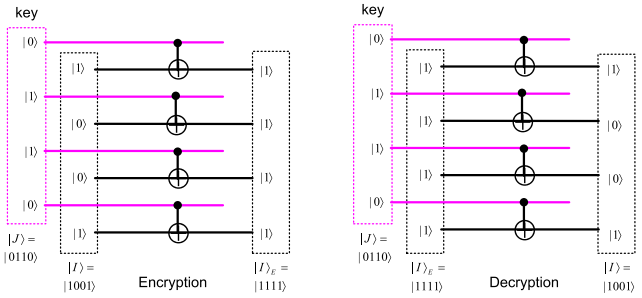


FIGURE 4. An illustrated example of controlled-NOT encryption and decryption.

the target qubit and the control qubit. The gate flips the target qubit if the control qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$. We can encrypt the quantum image (target qubit) utilizing the secret key as the control qubit. An illustrated example is given in Figure 4. The gate is represented by the unitary matrix.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

E. THE CHAOTIC MAP

The logistic-sine map is a one-dimensional, discrete chaotic map [32], designed as follows

$$k_{i+1} = \left(\psi(k_i - k_i^2) + (4 - \psi)\sin(\pi k_i)/4\right) \mod 1 \quad (4)$$

Where ψ is the control parameter $\psi \in [0, 4]$, and k_0 is the initial value. Fig. 5 shows the bifurcation, which reveals the strong attractor in the selected map.

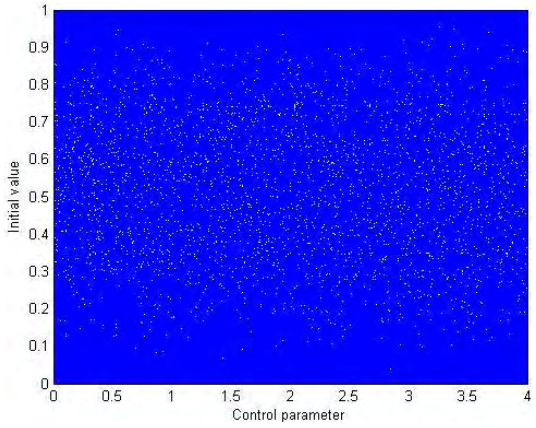


FIGURE 5. Bifurcation of the map [32] (the figure is drawn by MATLAB program to illustrate the bifurcation of the map).

III. FRAMEWORK FOR THE PROPOSED SECURE QUANTUM ENCRYPTION OF HEALTHCARE MEDIA

Fig. 6 shows the framework for the proposed secure encryption of health care media. Patients and healthcare staff in one location encrypt important medical images via the proposed quantum encryption scheme, sending the cipher images to the cloud. The health care staff in another location accesses the images from the cloud, decrypting the content via the proposed decryption method. The proposed quantum encryption system ensures high confidentiality for patients and users of the health care system.

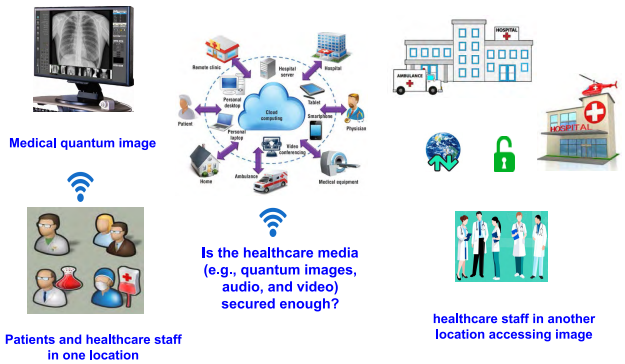


FIGURE 6. The proposed secure encryption framework for healthcare media.

A. PROPOSED APPROACH

We present a new quantum encryption approach for healthcare images based on quantum bit-plane arrangements,

gray code, quantum image controlled-not gates, and quantum images representing using NEQR. The proposed quantum algorithm is illustrated in Fig. 7, and the circuit for the proposed algorithm is shown in Fig. 8.

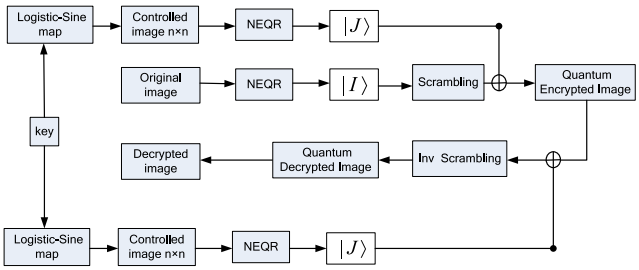


FIGURE 7. The proposed quantum algorithm.

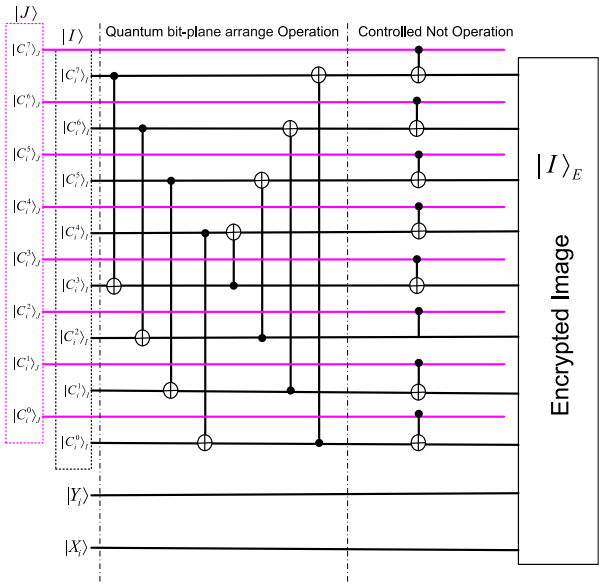


FIGURE 8. Quantum circuit for encryption algorithm.

B. ENCRYPTION PROCESS

The encryption procedures of the proposed algorithm consist of three phases, which illustrated as follows:

Phase 1: Prepare quantum image controlled-NOT

The creation of the controlled–NOT image given by the following steps.

Step 1: Choose k_i and ψ, where $k_0 \in (0, 1)$, $\psi \in [0, 4]$ are secrete keys in the map.

$$k_{i+1} = \left(\psi(k_i - k_i^2) + (4 - \psi)\sin(\pi k_i)/4\right) \mod 1$$

Where $i = 0, 1, 2, \ldots, 2^{2n}$, (2^{2n} is the size of an image).

Step 2: Transform the sequence $\{k_i\}$ into an integer sequence:

$$k_i^* = |fix((k_i - fix(k_i)) \times 10^8)| mod 256$$

Step 3: Transform k_i^* sequence into quantum image representation using NEQR.

$$|J\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes |j\rangle, |c_j\rangle = |c_j^7 \ldots c_j^1 c_j^0\rangle, c_j^k \in \{0, 1\}$$

Step 4: Transform the original medical image into the quantum one by:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, |c_i\rangle = |c_i^7 \ldots . c_i^1 c_i^0\rangle, c_i^k \in \{0, 1\}$$

Phase 2: Scrambling for quantum image $|I\rangle$

The quantum image $|I\rangle$ scrambled using quantum bit-plane and gray code as shown in Fig. 9.

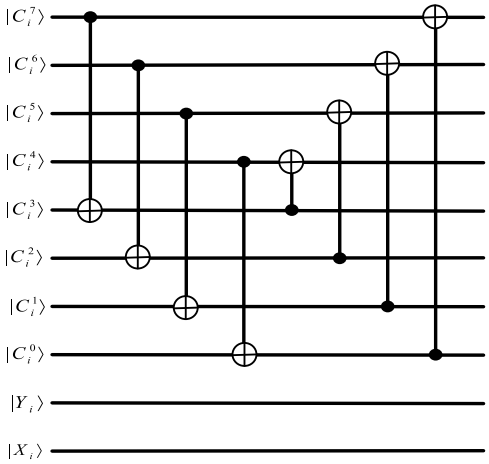


FIGURE 9. The bit-plane and its circuit.

Phase 3: Encryption the scrambled quantum image $|I\rangle_S$

The quantum image $|I\rangle$ is encrypted by adapting the controlled-not operations on the scrambled image $|I\rangle_S$, which is then controlled by the quantum image $|J\rangle$ as displayed in Fig. 8.

C. DECRYPTION PROCESS

The keys involved in the encryption process are the initial parameters k_0 and Ψ. The decryption process is the inverse process of encryption, as shown in Fig. 10. It can be implemented as follows.

Phase 1: Prepare quantum image controlled-not.

Set the key values for k_0 and Ψ to get the quantum image $|J\rangle$

$$|J\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes |j\rangle, |c_j\rangle = |c_j^7 \ldots c_j^1 c_j^0\rangle$$

Phase 2: Controlled-NOT process

By implementing the controlled-NOT operations on the ciphered quantum image $|I\rangle_E$ controlled by the quantum image $|J\rangle$, we get the scrambled quantum image $|I\rangle_S$

Phase 3: Descrambling quantum image $|I\rangle_S$

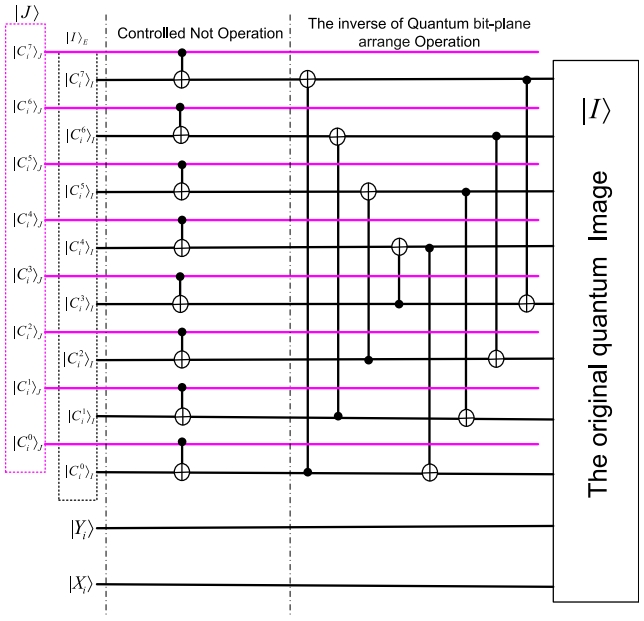


FIGURE 10. Quantum circuit for decryption algorithm.

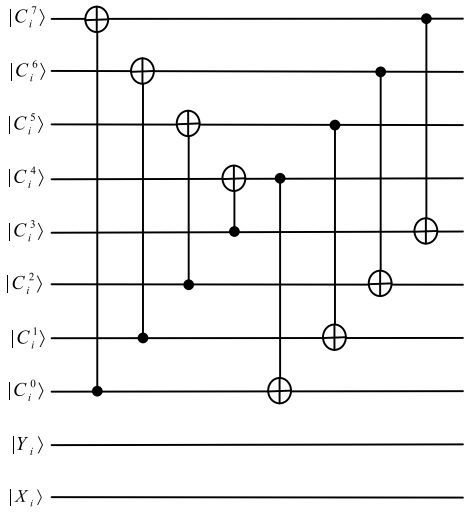


FIGURE 11. The inverse of the bit-plane and its circuit.

The quantum image $|I\rangle_S$ is descrambled using the quantum bit-plane and gray code to obtain the original image $|I\rangle$ as shown in Figure 11.

IV. NUMERICAL SIMULATIONS USING CLASSICAL COMPUTERS

The proposed algorithm was verified by a set of simulation analyses on a personal computer with an Intel Core^{TM}2 Duo CPU 3.00 GHz and 4GB RAM. MATLAB R2009b (version 7.9.0.529) was used to perform the operations for the proposed quantum encryption of healthcare images. Some selected medical images of size (128 × 128) were used as the original images, as shown in Fig. 12. The simulation parameters, used as secret keys in the chaotic map, were $k_0 = 0.34$ and $\Psi = 3.98421$.

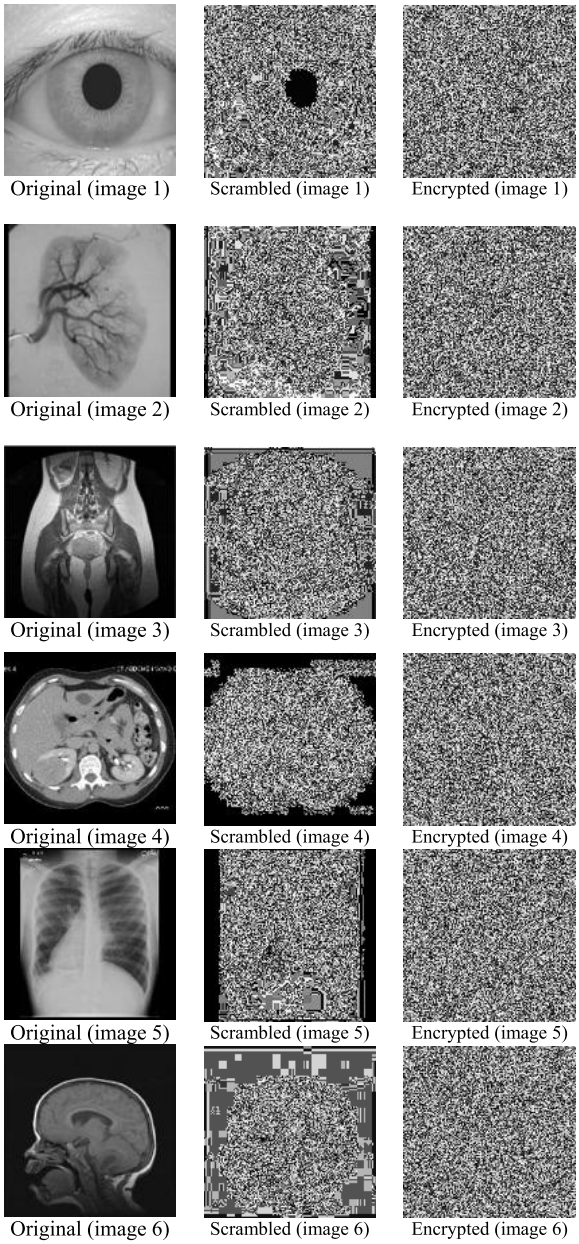


FIGURE 12. Results of the proposed quantum encryption scheme.

A. CORRELATION OF ADJACENT PIXELS

In plain images, the value of a pixel is very close to the values of horizontally, vertically, and diagonally adjacent pixels, with high correlations close to 1. A cryptanalyst can capitalize on this to break the cipher. Therefore, adjacent pixels in ciphered images must be de-correlated, with close to zero correlation. The correlations between each pair of two adjacent pixels is given by

$$corr_{kl} = \frac{\sum_{i=1}^{M}\left(k_i - \frac{1}{M}\sum_{j=1}^{M}k_j\right)\left(l_i - \frac{1}{M}\sum_{j=1}^{M}l_j\right)}{\sqrt{\sum_{i=1}^{M}\left(k_i - \frac{1}{M}\sum_{j=1}^{M}k_j\right)^2 \sum_{i=1}^{M}\left(l_i - \frac{1}{M}\sum_{j=1}^{M}l_j\right)^2}} \quad (5)$$

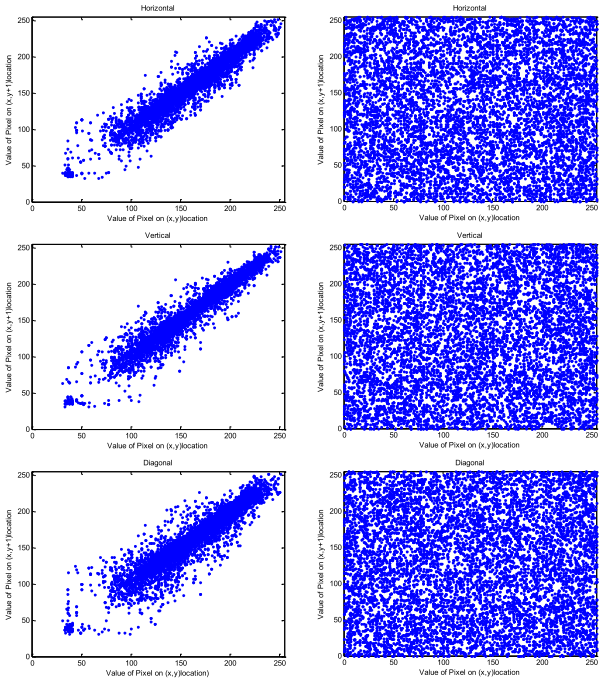


FIGURE 13. Correlations of two neighboring horizontal, vertical and diagonal pixels for image 1. The first column is the original image and the second column is the encrypted image.

TABLE 1. Results of Correlation of adjacent pixels.

image	direction		
	Horizontal	Vertical	Diagonal
Original (image 1)	0.9744	0.9760	0.9550
Encrypted (image 1)	-0.0020	-0.0095	-0.0015
Original (image 2)	0.9799	0.8973	0.8837
Encrypted (image 2)	0.0037	-0.0069	-0.0100
Original (image 3)	0.9672	0.9520	0.9277
Encrypted (image 3)	-0.0152	-0.0201	-0.0098
Original (image 4)	0.9375	0.9467	0.9131
Encrypted (image 4)	0.0073	-0.0187	0.0008
Original (image 5)	0.9714	0.9703	0.9438
Encrypted (image 5)	-0.0104	-0.0155	-0.0070
Original (image 6)	0.9249	0.9013	0.8506
Encrypted (image 6)	0.0007	-0.0008	-0.0044

Where M is the total number of adjacent pixel pairs in each direction and k_i, l_i are the values of adjacent pixels. The results of correlation coefficients in each neighboring direction for two pixel pairs of the original and cipher images are shown in Table 1 and Fig. 13. As may be seen, the proposed approach fulfills the zero-correlation requirement and has high privilege against correlation-based attacks.

B. NUMBER OF PIXEL CHANGE RATE

To examine the influence of changing pixels in the plain image on the encrypted image there are two measures used, the first one is the number of pixel change rate (NPCR) and the second measure is unified average changing intensity (UACI) [32]. Let $U(i,j)$ and $V(i,j)$ be the $(i,j)th$ pixel of two images U and V, respectively. The NPCR and UACI can be expressed by using. (6) and (7), respectively [32].

$$NPCR = \frac{1}{M} \times \sum_{i;j} D(i,j) \times 100\% \tag{6}$$

$$UACI = \frac{1}{M}\left(\sum_{i,j} \frac{|U(i,j) - V(i,j)|}{2^N - 1}\right) \times 100\% \tag{7}$$

Where M is the total number of pixels in the image, N is the total bits used to represent the pixel value and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0 & if\ U(i,j) = V(i,j) \\ 1 & if\ U(i,j) \neq V(i,j) \end{cases}$$

From Table 2, the average NPCR value is 99.63% for all tested images. Thus, the proposed approach is very sensitive to any tiny changes in the pixel of the images.

TABLE 2. NPCR and UACI

Image	NPCR%	UACI%
Image 1	99.6643	28.9754
Image 2	99.6765	28.1845
Image 3	99.5483	37.2495
Image 4	99.6704	36.0075
Image 5	99.5727	33.4553
Image 6	99.6582	37.1384

C. HISTOGRAM ANALYSIS

The image histogram is a very important statistical analysis tool to evaluate the performance of image encryption algorithms, reflecting the frequency distribution of pixels in an image. An effective encryption scheme can improve resistance against statistical cryptanalysis by ensuring uniform peakiness of different encrypted images. Fig. 14 shows histograms of several plain and their corresponding encrypted images. The histograms of quantum-encrypted images are almost uniform. Thus, we conclude that the proposed quantum encryption approach is robust against a statistical attack based on histogram analysis.

D. SHANNON ENTROPY ANALYSIS

The statistical measure of the distribution of image pixels for each level is known as information entropy. The information entropy of an image can be calculated using the following equation

$$Entropy = -\sum_{i=1}^{2^L-1} p(u_i) \log_2 (p(u_i)) \tag{8}$$

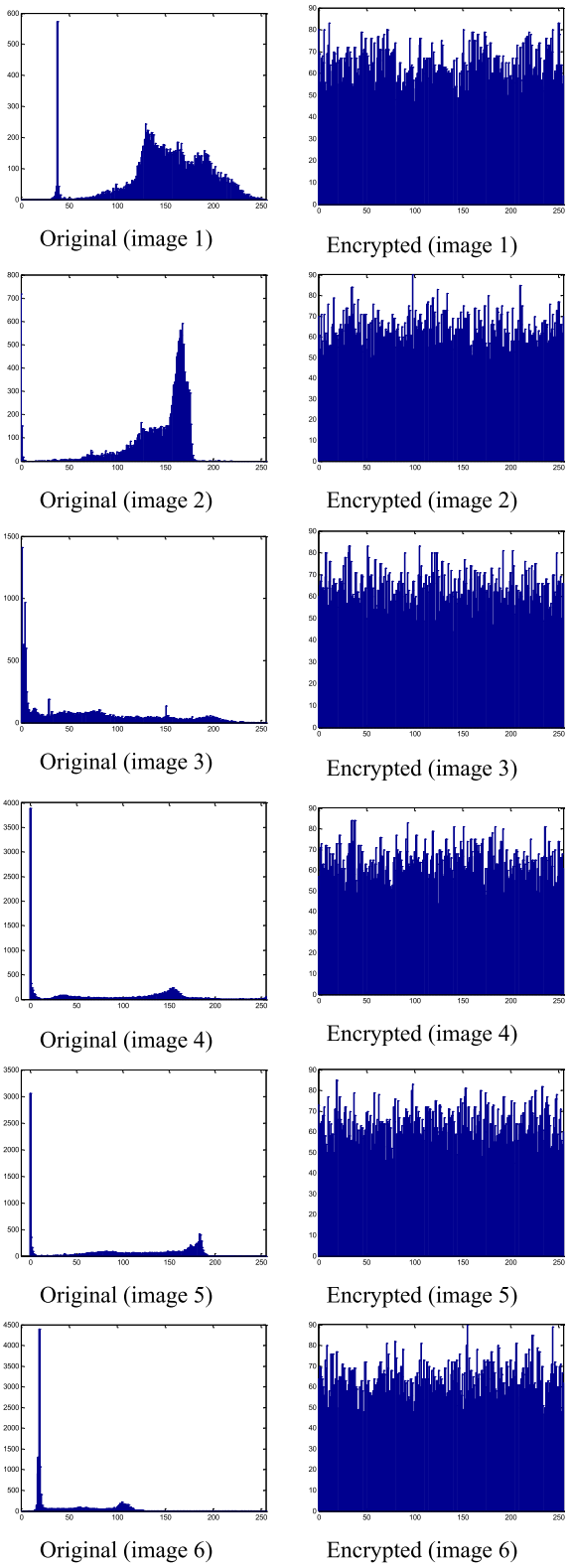


FIGURE 14. Histograms of original and encrypted images.

Where $p(u_i)$ represents the probability u_i. There are 2^8 (range of [0,255]) possible values for a grayscale image. The ideal entropy value is equal to 8-bit. Consequently, the entropy value of the encrypted image should be close to 8 to confirm the efficiency of the proposed algorithm. Table 3 states the information entropy values of original and their related encrypted images. The information entropy of all encrypted images is obviously close to eight bits, showing that the proposed encryption approach is secure against entropy attack.

TABLE 3. Entropy analysis.

Image	Original image	Encrypted image
Image 1	7.1024	7.9878
Image 2	6.3134	7.9899
Image 3	6.9879	7.9898
Image 4	6.4286	7.9896
Image 5	6.5169	7.9893
Image 6	5.3849	7.9884

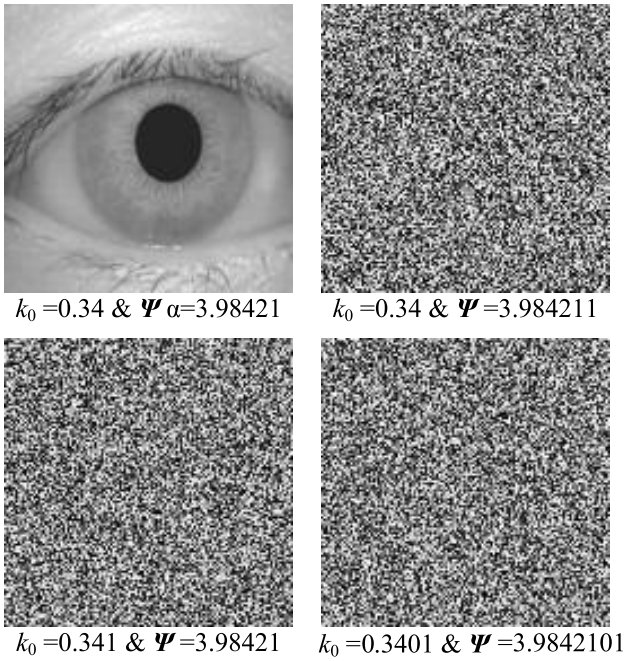


FIGURE 15. Decrypted images (the correct keys are $k_0 = 0.34$ and $\Psi = 3.98421$).

E. KEY SENSITIVITY ANALYSIS

Key sensitivity means that small changes in the secret key should lead to significant modifications in the cipher image. To evaluate key sensitivity, different images are encrypted with one fixed, correct secret key. Decryption is performed with different, slightly changed keys. The resulting images, decrypted with the wrong key—even if only slightly different from the secret key—should reveal no information about the secret data and appear totally different. Fig. 15 shows four different images decrypted with the correct and wrong keys, showing that the secret information is revealed only with the exactly correct secret key.

V. CONCLUSION

This paper proposed a new framework for the secure quantum encryption of healthcare images. In this framework, patient images in one location are first transformed into an NEQR representation before being encrypted with the proposed encryption approach and sent to the cloud. The health care staff on the receiving side accesses the images from the cloud, decrypting the content using the proposed decryption approach. For performance analysis of the proposed approach on a classical computer, various simulations, and numerical methods were employed, such as correlation, Shannon entropy, sensitivity analysis, and histogram analysis.

REFERENCES

[1] N. A. Loan, S. A. Parah, J. A. Sheikh, J. A. Akhoon, and G. M. Bhat, "Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications," *J. Biomed. Inform.*, vol. 73, pp. 125–136, Sep. 2017.

[2] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Medical data sheet in safe havens—A tri-layer cryptic solution," *Comput. Biol. Med.*, vol. 62, pp. 264–276, Jul. 2015.

[3] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Comput. Med. Imag. Graph.*, vol. 27, nos. 2–3, pp. 185–196, Mar./Jun. 2003.

[4] M. S. Hossain, "Cloud-supported cyber-physical localization framework for patients monitoring," *IEEE Systems J.*, vol. 11, no. 1, pp. 118–127, Mar. 2017.

[5] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44–51, Oct. 2016.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[7] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Opt.-Int. J. Light Electron Opt.*, vol. 130, pp. 1438–1444, Feb. 2017.

[8] M. A. Nielsen and I. L. Chuang, "Quantum computation," in *Quantum Information*, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 13–211

[9] H.-K. Lo, *Quantum Cryptology*, vol. 77. Singapore: World Scientific, 1998, pp. 7–20.

[10] C. P. Williams, "Quantum computing and quantum communications," in *Proc. 1st NASA Int. Conf. QCQC*, vol. 1509. Palm Springs, CA, USA, Feb. 1998, pp. 200–217.

[11] C. C. Tseng and T. M. Hwang, "Quantum digital image processing algorithms," in *Proc. 16th IPPR Conf. Comput. Vis., Graph. Image Process.*, 2003, pp. 827–834.

[12] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985.

[13] J. I. Latorre. (2005). "Image compression and entanglement." [Online]. Available: https://arxiv.org/abs/quant-ph/0510031

[14] S. E. Venegas-Andraca and J. L. Ball, "Processing images in entangled quantum systems," *Quantum Inf. Process.*, vol. 9, no. 1, pp. 1–11, Feb. 2010.

[15] B. Sun *et al.*, "A multi-channel representation for images on quantum computers using the RGBa color space," in *Proc. IEEE 7th Int. Symp. Intell. Signal Process.*, Sep. 2011, pp. 1–6.

[16] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," *Quantum Inf. Process.*, vol. 12, no. 9, pp. 3103–3126, Sep. 2013.

[17] 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, Feb. 2011.

[18] 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, Aug. 2013.

[19] M. S. Hossain, A. Alamri, A. El Saddik, "A biologically inspired framework for multimedia service management in a ubiquitous environment," *Concurrency Comput., Pract. Exper.*, vol. 21, no. 11, pp. 1450–1466, Aug. 2009.

[20] 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, May 2014.

[21] N. Jiang, L. Wang, and W.-Y. Wu, "Quantum Hilbert image scrambling," *Int. J. Theor. Phys.*, vol. 53, no. 7, pp. 2463–2484, Jul. 2014.

[22] 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, May 2015.

[23] 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, Nov. 2013.

[24] 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, Aug. 2014.

[25] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1193–1213, Apr. 2015.

[26] L.-H. Gong, X.-T. He, S. Cheng, T.-X. Hua, and N.-R. Zhou, "Quantum image encryption algorithm based on quantum image XOR operations," *Int. J. Theor. Phys.*, vol. 55, no. 7, pp. 3234–3250, Jul. 2016.

[27] H.-R. Liang, X.-Y. Tao, and N.-R. Zhou, "Quantum image encryption based on generalized affine transform and logistic map," *Quantum Inf. Process.*, vol. 15, no. 7, pp. 2701–2724, Jul. 2016.

[28] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT)—Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016.

[29] M. S. Hossain and G. Muhammad, "Healthcare big data voice pathology assessment framework," *IEEE Access*, vol. 4, pp. 7806–7815, 2016.

[30] L. Hu, M. Qiu, J. Song, M. S. Hossain, and A. Ghoneim, "Software defined healthcare networks," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 67–75, Dec. 2015.

[31] Y. Hu, K. Duan, Y. Zhang, M. S. Hossain, S. M. M. Rahman, and A. Alelaiwi, "Simultaneously aided diagnosis model for outpatient departments via healthcare big data analytics," in *Multimedia Tools and Applications*. 2016, pp. 1–15.

[32] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[33] M. S. Hossain and G. Muhammad, "Cloud-assisted speech and face recognition framework for health monitoring," *Mobile Netw. Appl.*, vol. 20, no. 3, pp. 391–399, Feb. 2015.

AHMED A. ABD EL-LATIF received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, Harbin, China, in 2013. He is currently a lecturer of computer science at Menoufia University. He is an author and a co-author of many publications, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He is a referee of many referred international repute journals and conferences. His areas of interests are multimedia content encryption, secure wireless communication, IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He is a fellow of the Academy of Scientific Research and Technology, Egypt. He received many awards, the State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt; the Best Ph.D. Student Award from the Harbin Institute of Technology, China, in 2013; and the Young Scientific Award from Menoufia University, in 2014.

BASSEM ABD-EL-ATTY was born in Menoufia, Egypt, in 1989. He received the B.S. degree in physics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2010 and 2017, respectively, where he is currently pursuing the Ph.D. degree in quantum information processing with the Faculty of Science, School of Mathematics and Computer Science. His research interests include quantum information processing and image processing.

MUHAMMAD TALHA received the Ph.D. degree in computer science from the Faculty of Computing, University of Technology, Malaysia. He is currently with the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia. He is an author of numerous papers published in local and international journals. His research interests are image processing, medical imaging, features extraction, and classification and machine learning techniques.