Journal of Engineering Science and Technology
Vol. 17, No. 5 (2022) 3570 - 3582

IMPLEMENTING QUANTUM IMAGE SECURITY ALGORITHM BASED ON GEOMETRIC TRANSFORMATION AND QUANTUM RANDOM NUMBER GENERATION

ALHARITH A. ABDULLAH*, SUADAD S. MAHDI

Department of Information Security, Faculty of Information Technology,
University of Babylon, AL-Mustaqbal University College
*Corresponding Author: alharith.khafaji@yahoo.com

Abstract

Encryption is one of the techniques used for securing images, so in this study, we proposed a quantum encryption system which consists of two layers. The first layer, geometric transformations perform for the quantum bits of quantum image, while the second layer relies on encrypting these qubits by using a block quantum encryption algorithm. Quantum key distribution is used with quantum encryption algorithm for securing key exchange process between the sender and receiver. This paper presents a simulation using python programming language to convert classical bit to qubit by representing it as a quantum state and implement the quantum encryption system. Our results indicate the high level of safety secures images based on different factors such as PSNR, correlation entropy, and histogram.

Keywords: BB84, QKD, Qubit, Quantum encryption system, Quantum image.

1. Introduction

As a result of the continuous development in the field of Internet technology, which is one of the means of sending information through the network of which the image represents the most important part since it contains a lot of personal information and important data, protecting and ensuring the image's integrity and confidentiality is considered crucially important, and thus it is considered one of the important problems that requires effective solutions [1].

There are many classical encryption schemes but the rapid advance in quantum computing is a powerful threat to classical encryption systems and protocols [2]. As it is well known, the quantum computer is characterized by its ultra-high computing capacity of achieving a high degree of parallelization with the properties of superposition and entanglement [3]. Consequently, the high-speed of the quantum computing's expansion and the exploitation of quantum properties demand many encryption algorithms which are easily and extremely fast broken and they become no longer safe [4, 5]. Thus, quantum encryption has become a rather important option for achieving confidentiality and integrity of the data in many applications [6, 7].

On the other hand, quantum key distribution (QKD) is the most interesting area in the field of information security because of the exploitation of the laws of quantum physics which allow the exchange of secret keys between the two parties [5], where a series of quantum states is transmitted over a public quantum channel (such as a fiber-optic channel). The first quantum key distribution protocol was proposed by Charles H. Bennet and Gilles Brassard in 1984 called BB84 [1]. The BB84 protocol can be summarized in two stages: the first stage involves preparing the photons by using random bases specific to the sender and sending them through the quantum channel, while these photons are measured by the receiver side using its own bases. While the second stage is conducted through a classic channel which agrees on the bases that were used by the two parties.

In recent years, the encryption of quantum image has become an important researched topic, related with processing of quantum information that is employed for securing quantum images [8, 9]. There are a lot of researches that have taken care of quantum images encryption by using different ways. Wang et al. [7] presented a new algorithm for encrypting quantum images depending on transforming and diffusing of the quantum wavelet. Also, [10] shows an algorithm suggested for encrypting a quantum video relaying on various transforms. While Wang et al. [11] showed the correlative framework of quantum image encryption. Usually, using such a kind of encryption method has worked to scramble the colour information and positions of the image through various transformations.

On the hand, there is another way for encrypting the quantum image depending on the encryption which converts the image's data through using the key as in [12], where an algorithm has been proposed for encrypting quantum image depending on quantum image XOR operations. The XOR operations are performed on the quantum image using highly chaotic sequences generated by using Chen's highly chaotic control-NOT process, and they are thus used to encode information. Plus, Abdullah et al. [13] suggested quantum encryption algorithm in a new way that relies on generating quantum keys. The quantum key was generated and the quantum padding bit and the quantum block encryption algorithm were generated on the idea of a quantum half adder with introduced bit-swapping in the encryption process. While

Yan et al. [14] outlined the encryption of quantum image in general. Wang et al. 15] suggested a new algorithm for encrypting quantum image depending on the quantum key image, which has been done by using the key stream that is created through using a classic encryption algorithm. As for the encryption process, it is also the XOR process between the quantum key image and the quantum plain image. In general, the key used in this process is a key generated in a classical way and converted into quantum form. While Hu et al. [16] proposed a new quantum encryption scheme based on the chaos theory and Arnold transform, where the quantum encryption process takes place in two stages based on Arnold transform and Logistic map, the results show that the encrypted data is highly protected.

Zhou [17] relied on DNA Controlled-Not (DNA C-Not) to encrypt a quantum image, as well as they used quantum image information to obtain encryption parameters as a part of an initial key. In addition to achieving a large key space, the researcher came up with good results. Liu et al. [18] relied on three levels including block-level permutation, bit-level permutation, and pixel-level diffusion on the original image to achieve satisfactory coding results by taking advantage of the properties of quantum mechanics. The simulation results showed that the quantum image encrypting scheme proposed by the researchers has a high level of safety in comparison to its classical counterpart in terms of efficiency.

The current study presents a new quantum image security system based on geometric transformation and a quantum cryptographic algorithm by employing two quantum keys. The first key is generated through using the quantum security protocol BB84, which is one of the oldest and most important quantum protocols for generating and distributing keys and achieving authentication between the two parties through quantum properties [19], while the second key is generated through the use of QBER which is characterized by a high randomness and thus a strong key and powerful encryption are obtained by using an easy-to-implement encryption algorithm.

This paper is shown as below: Section 2 explains the quantum image representation. While, in Sections 3 deals with quantum encryption system, and Section 4 shows and analyses simulation results. Lastly, Section 5 sums up the conclusions of study.

2. Representations of Classical Data as a Quantum Data

In general, classic data is represented as a bit (binary data) to deal with in the classic domain, but in the quantum domain it is necessary to convert classic data into quantum data in format quantum state to be dealt with in quantum algorithms [20].

Our work is based on representing the classic image data (pixel) as a quantum state to be easily handled by the quantum encryption algorithm in the next stage. So, there are three stages that the classic image goes through to convert into a quantum format:

i. Converting the image to a matrix of classic data (pixels) so that each pixel represents the colour value of its location in image. Then, the binary matrix is converted to a one-dimensional array.
ii. Uploading each classical bit to a quantum bit (qubit), depending on the quantum circuit in Fig. 1.

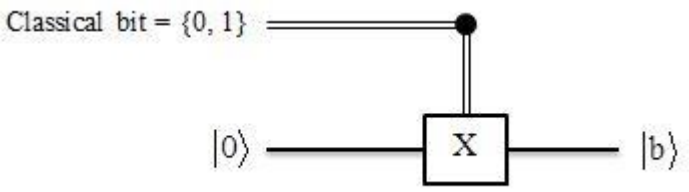

Fig. 1. Loading classical bit into the qubit quantum state.

In a circle, the classic bit is considered the controller in the circuit, where in the case of the classic bit is 0, then the x gate does not work and the output is $|\mathbf{0}\rangle$, while if the classic bit is 1, then the x gate works to invert the state of the $|\mathbf{0}\rangle$ to $|\mathbf{1}\rangle$as shown in Table 1.

Table 1. Loading classical bit {0, 1} to qubit.

Input		Output
Initial qubit	**Classical bit**	**Qubit**
$\|\mathbf{0}\rangle$	0	$\|\mathbf{0}\rangle$
$\|\mathbf{0}\rangle$	1	$\|\mathbf{1}\rangle$

iii. Finally, converting the qubits to superposition state, depending on the circle in Fig. 2 [21]. Where $\{|b1\rangle,|b2\rangle,|b3\rangle,|b4\rangle\}$ represent the classic bits loaded in qubit in previse step as in Fig. 1. While $\{a,b,g\}$ represent the superposition to store the four classical bits. This way, we can apply quantum algorithms to classic data.

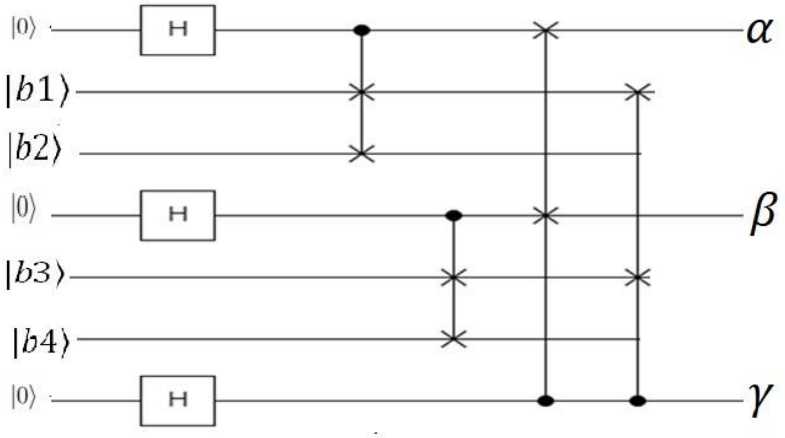

Fig. 1. Storing classical bits in the superposition state.

3. Quantum Encryption System

In terms of the approved method, this section will discuss the proposed quantum cipher system for generating quantum encryption keys and quantum encryption algorithm.

3.1. Quantum key generator

In our work, the encryption algorithm relies on two keys for the purpose of encryption , so two quantum keys (K1, K2) were generated in two different ways:

The first key is generated by BB84 quantum protocol where the protocol sends pulses of polarized light (four non-orthogonal polarized photons); each pulse contains one photon across a quantum channel to the other end [22]. And a classic public channel, such as a phone line or an Internet connection, for a solid authentication between the two parties and provide a secure connection. While the receiver receives polarized photons which are sent over a quantum channel. Eventually, the measurement bases are randomly chosen by receiver. Based on his choice, he measures the photon and stores the result right with the base used for measurement.

After sending a certain number of photons, the process of bases agreeing between sender and receiver begins information exchange over a public channel concerning their bases for each photon and ignores values that do not match the bases. After this process, both of the exchangers will get the same key value. The BB84 protocol is considered one of the most important quantum key distribution protocols [23]. Where authentication is achieved by relying on the quantum properties and the non-cloning theory of Qbits, which provides sufficient security for the secret key between the two parties [24].

While, the second key is generated using a Quantum Random Number Generator (QRNG) [25]. Probable quantum primary optic operations are used by QRNG to obtain high, unpredictable randomness [26]. In our work, qRNG library is used which is open source and written in Python language. The generated QRNG is then converted from binary form (0, 1) into quantum keys in the form:

$K2 = K_i = |0\rangle \; ; \; K2 = K_i = |1\rangle$
$K2 = Ki = \{|0\rangle, |0\rangle, |1\rangle, \dots\dots\dots\dots, i\}$

3.2. Quantum image encryption algorithm

The quantum encryption system used goes through two stages. The first stage includes the geometric transformations of the quantum state, depending on the quantum circuit in Fig. 3. Table 2 displays the results of the geometric transformation of the quantum state.

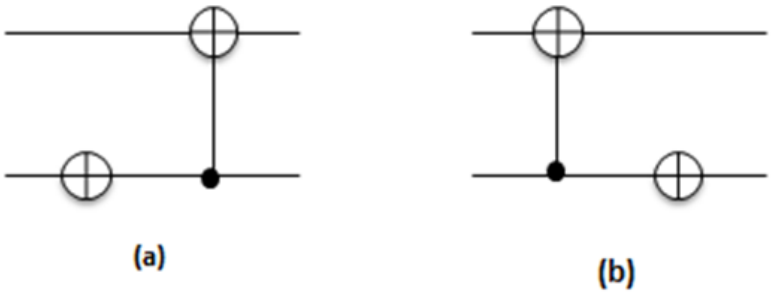

Fig. 3. The quantum circuit for the geometric transformation: (a) sender side and (b) receiver side.

Table 2. Quantum state geometric transformation in sender side.

QBits	Transformed QBits
$\|\mathbf{00}\rangle$	$\|11\rangle$
$\|\mathbf{01}\rangle$	$\|\mathbf{0}0\rangle$
$\|\mathbf{10}\rangle$	$\|\mathbf{0}1\rangle$
$\|\mathbf{11}\rangle$	$\|10\rangle$

While in the second stage, the encryption process is done through the quantum encryption algorithm. In our proposal, the quantum encryption algorithm mainly relies on the K1 and K2 keys, where the two QBits are taken from plain image to be encrypted by one of the quantum gates and depending on the keys value, based on reference [13] as shown in the Table 3.

Table 3. Unitary operation for quantum encryption.

K1	K2	Unitary Operator
$\|\mathbf{0}\rangle$	$\|0\rangle$	I
$\|\mathbf{0}\rangle$	$\|1\rangle$	H
$\|\mathbf{1}\rangle$	$\|0\rangle$	ZH
$\|\mathbf{1}\rangle$	$\|1\rangle$	X

where I, X, Z, and H are represented by the following matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

After that, the swap gate is implemented as a final step for the encryption algorithm where swap gate is represented as following:

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

In general, the quantum encryption algorithm is explained as quantum circuit in Fig. 4. Depending on the states of the keys K1 and K2, there are four states of using unitary operation gates.

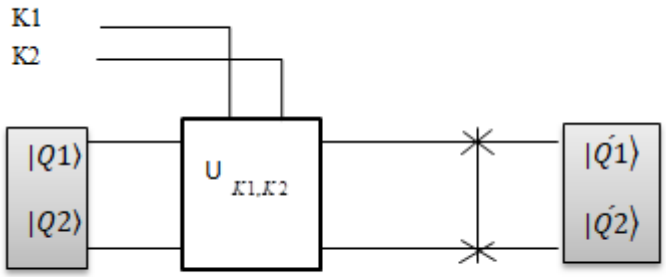

Fig. 4. Quantum encryption algorithm.

4. Experiment Results and Analysis

This section presents the results of the proposed work implementation and statistical as well as theoretical analysis. Simulation is used in the Python language on a classical computer to perform quantum image encryption operations and also to compute statistical analysis. The usual images of Lena, Peppers, and Baboon with 256×256 size is used in implementing and calculating the results of the proposed work.

4.1. Statistical analysis

In this section, we show the statistical analysis of encrypted images to verify the efficiency and effectiveness of our proposal, so we will analyse the encoded image from the following aspects: information entropy, PSNR value of images, correlation of adjacent pixel and histogram analysis.

4.1.1. Information entropy

The information entropy represents the uncertainty of the image information, and it is a basic quantity in information theory [27]. Information entropy (often only entropy) is used for measuring the units' distribution of pixels of image at each level. Entropy can be considered as the basis for cryptographic algorithms where randomness is measured. The following mathematical formula is employed for calculating the information entropy:

$$Entropy\ (S) = -\sum_{i=0}^{2^n-1} P(s_i) log_2\ P(\ s_i) \quad (1)$$

where $P(s)$ refers to the symbol s probability. Table shows the entropy values for the original image and its encrypted one. Looking at the results, we note that the closest to 8 is the encrypted image entropy, and this reflects the effectiveness and efficiency of the encryption system in providing good security to resist the attacks of information entropy.

Table 4. The information entropy of the original and encrypted images.

Images	Information Entropy (H)	
	Original Images	**Encrypted Images**
Lena	7.133765211485382	7.598861751739797
Peppers	6.7182666256346115	7.28556824529605
Baboon	7.010450983568009	7.623215504315525

4.1.2. PSNR value of images

The peak signal to noise ratio, or PSNR for short, is the important criterion for measuring image distortion [28]. Where, the value of the PSNR between the original image and its decrypted one is high, the more similar the two pictures. In general, the standard for PSNR is 30 dB and the following is the mathematical formula of PSNR:

$$PSNR = 10\ \log_2(\frac{MAX^2}{MSE}) \quad (2)$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left\|Orginal_{img} - Decrypted_{img}(i,j)\right\|^2 \quad (3)$$

where MAX refers to the image colour maximum value, MSE represents the mean squared error, i.e., the mean squared error between the original image and its

decrypted one in size N * M (N represents high of image while M represents width). The results in Table show that the PSNR values are close to 30 dB, which means that the degree of decrypted image distortion lies within the acceptable range and has a good visual effect.

Table 5. The PSNR value of decrypted images.

Images	PSNR of Decrypted Images (in dB)
Lena	28.49
Peppers	27.97
Baboon	29.29

4.1.3. NPCR and UACI randomness tests

Two of the most important measures used to evaluate the strength of the encryption algorithm to encrypt images, they are; the number of variable pixel rate (NPCR), and the uniform variable mean intensity (UACI) [29]. The high value of NPCR and UACI indicates that the encryption algorithm has a high resistance against differential attacks.

In general, NPCR counts the number of variable pixels, while UACI is the number of the average density variable between the encrypted images. The ideal values of NPCR and UACI to ensure that the encrypted image is not differentiable, so expected values of NPCR and UACI are NPCRe = 99.6094% and UAC Ie = 33.4634%. The NPCR is defined by:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (4)$$

While the UACI is realized as:

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C1(i,j) - C2\,(i,j)|}{255} \times 100\% \quad (5)$$

where W (width) and H (height) of the encrypted image, while $D\,(i, j)$ is defined as:

$$D(i,j) = \begin{cases} 0, & if\ (\ C1(i,j) = C2(i,j)) \\ 1, & if\ (\ C1(i,j) \neq C2(i,j)) \end{cases} \quad (6)$$

The values of NPCR and UACI are calculated first by encrypting the plain image, then selecting a pixel from the image randomly, then changing the value of this pixel. Then the image is encrypted after modification by the use of the same algorithm and encryption key, and finally the NPCR and UACI values are calculated. In Table 6, the results of the NPCR and UACI of the proposed encryption system are presented, and the results show the efficiency of the system against differential attacks.

Table 6. NPCR and UACI randomness test results of the proposed encryption system.

Images	NPCR (%)	UACI (%)
Lena	99.6205	33.6225
Peppers	99.4311	33.3971
Baboon	99.5809	33.4459

4.1.4. Correlation of adjacent pixel

The correlation of adjacent pixels represents strong the bonding between pixels [30]. In the normal image, the bonding strength between adjacent pixels is strong, while the bonding strength between the pixels in the encrypted image decreases. Correlation coefficient (CC) is calculated based on the following calculation:

$$CC_{xy} = \frac{\sum_{i=1}^{N}(xi-\bar{x})(yi-\bar{y})}{\sqrt{\sum_{i=1}^{N}(xi-\bar{x})^2 \sum_{i=1}^{N}(yi-\bar{y})^2}} \quad (7)$$

where, x and y represent the value of correlation for two adjacent pixels, $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} xi$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} yi$ represent equivalent mean values. The correlation of adjacent pixels is usually calculated in the horizontal, vertical, and diagonal direction of the images for the purpose of analysing and discussing the interconnection strength between the encrypted image pixels and it is usually near to or less than zero. The correlation results for the original and encrypted image are shown in Table .

Table 7. Correlation coefficients of original and encrypted images.

Images	Correlation of Original Image			Correlation of Encrypted Image		
	Horizontal Direction	Vertical Direction	Diagonal Direction	Horizontal Direction	Vertical Direction	Diagonal direction
Lena	0.8926	0.9283	0.8819	0.0021	- 0.0113	0.0019
Peppers	0.9173	0.9395	0.9518	0.0035	- 0.0075	- 0.029
Baboon	0.7939	0.8757	0.8625	- 0.0203	0.0038	0.00317

The results indicate that the correlation values between the pixels adjacent to the encrypted images are reduced. Also, our results are considered to be better compared to the results of the references [12, 15] as shown in Table 8, thus the attacker is unable to obtain the required information based on the statistical analysis.

Table 8. Comparison of correlation coefficients.

Images	Correlation of Other Works			Images	Correlation of Our Work		
	Horizontal Direction	Vertical Direction	Diagonal Direction		Horizontal direction	Vertical direction	Diagonal direction
Peppers [15]	0.014839	−0.11636	−0.002251	**Peppers**	0.0035	- 0.0075	- 0.0139
Lena [12]	−0.0013	−0.0073	0.0190	**Lena**	0.0021	- 0.0113	0.0029
Peppers [12]	−0.0085	0.0113	−0.0084	**Peppers**	0.0035	- 0.0075	- 0.0139
Baboon [12]	−0.0183	−0.0016	−0.0062	**Baboon**	- 0.0203	0.0038	0.00317

4.1.5. Histogram analysis

The histogram is considered one of the image's most essential statistical measures. It is usually used to analyse encrypted images and prove the effectiveness of the algorithm used for encryption. Through histogram, the results in Fig. 5 show that the encrypted images are flat or uniformly distributed. So it can be said that the

results are good enough to prevent the frequency analysis attack from reaching to useful information through the histograms of the encrypted images.

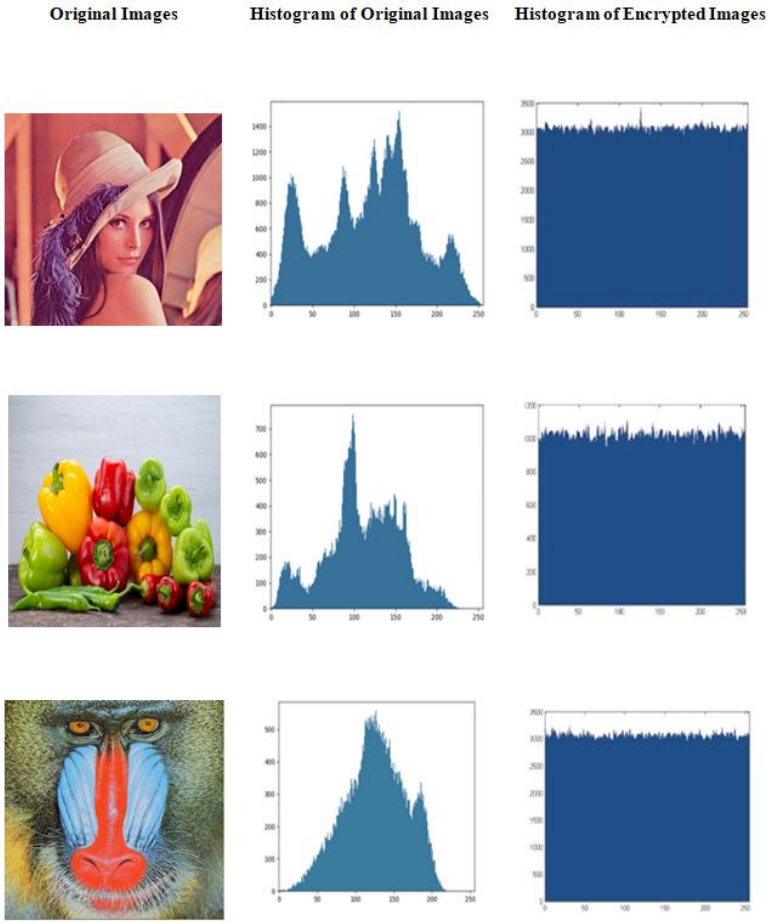

Fig. 5. Histograms of the original images and encrypted images.

4.2. Security analysis

In the present security system, the image passes through two stages; the first stage is summarized by the process of geometric transformations that takes place on the quantum bits of the image, while the second stage relies on quantum encryption based on two quantum keys.

In general, an algorithm is better if sensitive enough to the key and the key space is sufficient to hold out against a strong attack [31]. In the algorithm proposed here, two quantum keys are used with the encryption algorithm. The first key is generated by using quantum protocol BB84, while the second key is generated randomly using the QRNG function. So in case the attacker does not know the basic parameters for generating the key stream, it will depend on the space of the key and since the length of the key depends on the image size, if that size is 256 × 256 and each pixel uses 24 bit representing the colour image. Therefore, the key length is 256 × 256 × 24 and key space is $2^{256 \times 256 \times 24}$ and it is considered a great value for resist the brute force attack based on classical or quantum computer [4, 5].

On the other hand, the quantum key and the transmitted quantum photons are sensitive enough to any possible change that may occur to their quantum state depending on the rules of the mechanics of quantum, the measurement performed by eavesdropper will modify on the quantum state [3], and also cannot clone quantum state based on no-cloning theorem [24].

In Table 9 an evaluation comparison is made between the capacity of the proposed scheme and the alternative works. Commonly studied security parameters such as Entropy, NPCR, and UACI will be used to compare performance. The results indicate that the proposed scheme has a high value for NPCR and UACI indicating that the encryption algorithm has a high resistance against differential attacks. In addition to the entropy, the results are very close to 8 for the encrypted image, and this reflects the effectiveness and efficiency of the encryption system in providing good security to resist entropy information attacks.

Table 9. Comparison with other schemes.

Scheme	Paper Title	Digital Images	Entropy	NPCR	UACI
Ref. [11]	Quantum Image Encryption Based on Iterative Framework of Frequency Spatial Domain Transforms	Gray_scale	7.9627	-	-
Ref. [12]	Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations	Gray_scale	7.9993	-	-
Ref. [15]	Quantum Image Encryption Algorithm Based on Quantum Key Image	Gray_scale	7.9938	-	-
Ref. [16]	Quantum image encryption algorithm based on generalized Arnold transform and Logistic map	Color Image	7.9881	-	-
Ref. [17]	A Quantum Image Encryption Method Based on DNACNot	Gray_scale	7.1279	99.57%	33.51%
Proposed method		Color Image	7.5988	99.6205%	33.6225%

5. Conclusion

In this paper, a quantum security system for images based on geometric transformations using quantum circles was proposed as well as encrypted images with a quantum algorithm and using two different keys. The first key was generated by the BB84 quantum protocol, which is considered a security protocol to achieve the required authentication between the two parties while the other key is generated randomly.

The proposed work was simulated, and the statistical results were calculated in Python by using various quantitative and image processing libraries, such as openCV, qRNG, and others. Good results were obtained for the test image and for several statistical measures such as PSNR, entropy, pixel-adjacent relationship, and histogram. Therefore, it can be said that the proposal helps maintain the confidentiality and integrity of the information source by quantum encrypting of the images, thus preventing a quantum attack as well as a classical attack and protecting the information from new hackers. On the other hand, encryption

parameters can be transmitted through the Internet or stored in the cloud to achieve flexibility for the encryption system.

References

1. Easttom, W. (2021). *Quantum computing and cryptography*. In Modern Cryptography. Springer, Cham.
2. Stinson, D.R.; and Paterson, M.B. (2018). *Cryptography: Theory and practice*, CRC press.
3. Kumar, N.; Agrawal, A.; Chaurasia, B.K.; and Khan, R.A. (2020). *Limitations and future applications of quantum cryptography*. *IGI Global*.
4. Mavroeidis, V.; Vishi, K.; Zych, M.D.; and Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications* (*IJACSA*), 9(3), 405-414.
5. Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; and Smith-Tone, D. (2016). Report on post-quantum cryptography.. *NISTIR* 8105, US Department of Commerce, National Institute of Standards and Technology.
6. Abdullah, A.A.; Abod, Z.A.; and Abbas, M.S. (2018). An Improvement steganography system based on quantum one time pad encryption, *International Journal of Pure and Applied Mathematics*, 119(15), 263-280.
7. Wang, S.; Song, X.; and Niu, X. (2014). A novel encryption algorithm for quantum images based on quantum wavelet transform and diffusion. *Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications*, Shenzhen, China, 243-250.
8. Yan, F.; Venegas-Andraca, S.E.; and Hirota, K. (2022). Toward implementing efficient image processing algorithms on quantum computers. *Soft Computing*, 1-13.
9. Luo, Y.; Tang, S.; Liu, J.; Cao, L.; and Qiu, S. (2020). Image encryption scheme by combining the hyper-chaotic system with quantum coding. *Optics and Lasers in Engineering*, 124, 105836.
10. Yan, F.; Iliyasu, A.M.; Venegas-Andraca, S.E.; and Yang, H. (2015). Video encryption and decryption on quantum computers. *International Journal of Theoretical Physics*, 54(8), 2893-2904.
11. Wang, H.; Wang, J.; Geng, Y.-C.; Song, Y.; and Liu, J.-Q.(2017). Quantum image encryption based on iterative framework of frequency-spatial domain transforms. *International Journal of Theoretical Physics*, 56(10), 3029-3049.
12. Gong, L.-H.; He, X.-T.; Cheng, S.; Hua. T.-X.; and Zhou, N.-R. (2016). Quantum image encryption algorithm based on quantum image XOR operations. *International Journal of Theoretical Physics*, 55(7), 3234-3250.
13. Abdullah, A.A.; Al-Salih, A.M.; and Bermani, A.K. (2016). A new quantum block encryption algorithm based on quantum key generation. *Research Journal of Applied Science*, 11(10), 953-958.
14. Yan, F.; Iliyasu, A.M.; and Le, P.Q. (2017). Quantum image processing: a review of advances in its security technologies. *International Journal of Quantum Information*, 15(3), 1730001.

15. Wang, J.; Geng, Y.-C.; Han, L.; and Liu, J.-Q. (2019). Quantum image encryption algorithm based on quantum key image. *International Journal of Theoretical Physics*, 58(1), 308-322.
16. Hu, W.-W.; Zhou, R.-G.; Jiang, S.; Liu, X.; and Luo, J. (2020). Quantum image encryption algorithm based on generalized Arnold transform and Logistic map. *CCF Transactions on High Performance Computing*, 2(3), 228-253.
17. Zhou, S. (2020). A quantum image encryption method based on DNACNot. *IEEE Access*, 8, 178336-178344.
18. Liu, X.; Xiao, D.; and Liu, C. (2021). Three-level quantum image encryption based on Arnold transform and logistic map. *Quantum Information Processing*, 20(1), 1-22.
19. Kiktenko, E.O.; Malyshev, A.O.; Gavreev, M.A.; Bozhedarov, A.; Pozhar, N.O.; Anufriev, M.N.; and Fedorov, I.K. (2020). Lightweight authentication for quantum key distribution. *IEEE Transactions on Information Theory*, 66(10), 6354-6368.
20. Yan, F.; and Venegas-Andraca, S.E. (2020). Quantum image representations. *Quantum Image Processing*, 19-48.
21. Cortese, J.A.; and Braje, T.M. (2018). Loading classical data into a quantum computer. *arXiv Prepr arXiv*180301958.
22. Bennett, C.H.; and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560(P1), 7-11.
23. Mina, M.-Z.; and Simion, E. (2021). A scalable simulation of the BB84 protocol involving eavesdropping. *Innovative Security Solutions for Information Technology and Communications*.. *SecITC* 2020, Bucharest, Romania, E.U, 12596, 91-109.
24. Chen, Y.-C.; Gong, M.; Xue, P.; Yuan, H.-D.; and Zhang, C.-J. (2021). Quantum deleting and cloning in a pseudo-unitary system. *Frontiers of Physics*, 16(5), 1-7.
25. Ren, M.; Wu, E.; Liang, Y.; Jian, Y.; Wu, G.; and Zeng H. (2011). Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A*, 83(2), 23820.
26. Ma, X.; Yuan, X.; Cao, Z.; Qi, B.; and Zhang, Z. (2016). Quantum random number generation. *npj Quantum Information*, 2, 16021, 1-9.
27. Cachin, C. (1997). Entropy measures and unconditional security in cryptography. A dissertation of Doctor of Technical Sciences. Swiss Federal Institute of Technology Zurich.
28. Tanchenko, A. (2014). Visual-PSNR measure of image quality. *Journal of Visual Communication and Image Representation*, 25(5), 874-878.
29. Wu, Y.; Noonan, J.P.; and Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Journal of Selected Areas in Telecommunications* (*JSAT*), 1(2), 31-38.
30. Kaneko, S.; Murase, I.; and Igarashi, S. (2002). Robust image registration by increment sign correlation. *Pattern Recognition*, 35(10), 2223-2234.
31. Sen, J.; and Mehtab, S. (2020). *Computer and network security*. BoD-Books on Demand.