PAPER • **OPEN ACCESS**

Enhanced image encryption algorithm by quantum key distribution

To cite this article: M A Mahmoud *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1172** 012011

Enhanced image encryption algorithm by quantum key distribution

M A Mahmoud[1] ,T Mekkawy[2]and A D Elbayoumy[3]

[1] NANO Master program, Faculty of Engineering.Cairo University,Giza, Egypt
[2]Avionics Department, Military Technical Collage, Cairo, Egypt
[3]Communication Department, Military Technical Collage, Cairo, Egypt

E mail: Mohamed.khalifa84@eng1.cu.edu.eg

Abstract. Quantum Key Distribution (QKD) is one type of Quantum Cryptography (QC) which is based on quantum mechanics fundamentals such as Heisenberg's uncertainty principle and No-cloning theory. The usage of QKD warns the legitimate communicated parties to any attack attempt and this is the most interesting security parameter. Therefore, QKD provides unconditional secure communication method and supports a powerful encryption scheme. The combination between classical communication and QKD creates a new technique called semi quantum key distribution SQKD. Unfortunately, SQKD increases the schemes complexity and requires two steps for ciphering, scramble and encryption. In this paper an enhance image encryption algorithm is proposed based on QKD that eliminates most of the drawbacks of SQKD. The proposed algorithm is simpler than other encryption schemes as it exploits only one encryption step based on the power and the randomness of the generated secret key, which decreases the chance to be cracked. The correctness and efficiency of the proposed algorithm are validated by numerical simulations.

1. **Introduction**

Data encryption is one of the most important factors that used to determine the communication system quality and security. Communicated parties need their data to be ciphered to inhibit hackers from steal their data and personal information. Many schemes and algorithms were proposed to grantee data security among the last decades. Nowadays, online service takes place everywhere which increases data hacking and eavesdropping attacks attempts. Also, most of financial affairs are achieved through internet. This leads to the high requirement and the extremely need to powerful encryption schemes to save the mutual data between the service provider and the clients. Therefore, Quantum Key Distribution (QKD) [1] is adopted to improve the security performance due to its unconditional performance. The security of QKD is based on the principles of quantum mechanics, mainly, Heisenberg's uncertainty principle [2] and No-Cloning theory [3].

The quantum system sends notifications to the communicated parties for any attempt to sense or to hack the communication link. Because the measurement makes copies of the quantum states which conflicts with the No-Cloning theory, and similarly it warns the communicated parties to that eavesdropping. Quantum cryptography (QC) was introduced for the first time in 1970 [4]. It makes a great foundation for storing and transmitting the data by using linear or circular polarized photons. Moreover, when the Eavesdropper (Eve) tries to detect any information about the key that being used, the communicated parties (Alice and Bob) will notice that try immediately. In 1984, a secure communication protocol, BB84, was proposed [1]. It is based on conjugate observables and it describes photon polarized states to transmit the confidential information.

Basically, BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. These orthogonal pairs are the basis. The usual polarization state pairs are either the rectilinear basis of vertical (0°) or horizontal (90°), the diagonal basis of (45°) and (135°) or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. The usage of QKD in classical communication methods was discussed for the first time on 2007 in this technique one party is quantum (Alice) and the other party (Bob) is a classical one[5] so this algorithm named semi quantum key distribution SQKD. The first SQKD protocol [5] uses four different states. Those different states are randomly selected to be rectilinear or diagonal basis. The protocol was improved by two similar protocols were introduced in 2009[6]. The first protocol relayed on measurement and the second one was randomization dependent. A simplified SQKD protocol was employed in [7] with only three quantum states. Then, in 2011, another improved SQKD protocol was proposed [8] that was basing on entangled states, in which the qubit is more efficient by 50%, with respect to 25% of the protocol in [5]. Recently, in 2015 a new SQKD protocol was presented. The classical party in that protocol does not need the ability to measurement and needs only how to prepare, send and reorder qubits [9]. All the above SQKD protocols suppose the presence of an authenticated classical channel, which can be eliminated by pre-sharing a major secret key between two communicated parties. However, in the all mentioned SQKD protocols the classical parties are not really classical. This is because they need the ability of quantum preparing and measuring for the qubits in the computational basis, or quantum memory for the purpose of qubits reordering. In other words, the need of quantum devices for quantum operations is remaining exited. Then, Alice is supposed to be classical party and Bob is the quantum one [10].

From above literature, we observe SQKD algorithms consist of Quantum party, Classical party, Quantum channel, Classical channel, and Quantum memory. The main condition for SQKD algorithm is that the classical party can access the quantum channel otherwise no key will be shared with the communicated parties (quantum and classical). In 2016, a SQKD protocol based on a secure delegated quantum computation introduced [11], where Alice and Bob mutually transmit and receive data to third party (Charlie) to generate the secret key and it deeply requires the highest level of honesty to be in Charlie. Later in 2016, an algorithm proposed in which an integrated classical and QC scheme by using a three-party supposed to be authenticated [12]. In this scheme, three parties were involved and digital signature was added to ensure mutual authentication between the communicated parties. From the above preamble some drawbacks are concluded such as:

- Need for quantum memory.
- Need for quantum channel access for the classical party.
- The classical party is not completely classic one as he uses quantum devices for qubits measurement.
- Need for delegation of quantum computing for the third party quantum server.
- In many SQKD the key is one time pad OTP.
- Probability of the server adversary and dishonesty.
- Need for more added mutual authentication ways like digital signature.

On the other hand, image processing is a general term that represents any operation that applied to images for encryption, decryption, coding, decoding. Many researches were presented to secure images and hide their contained information between the communicated parties. On the opposite direction, attackers don't save efforts to hack communication systems and crack security keys. For example, in 2017 a scheme proposed a data transmission technique [13] by using QKD in which the data is firstly encoded by Huffman coding then the data is encrypted by QKD. This technique is limited in data size and also required a trusted third party to establish the secret key and need middle OTP coding step before data encryption and transmission.

Later in 2017, another scheme presented a robust encryption algorithm for quantum medical image [14]. In this algorithm they converted the normal medical images into quantum ones by a controlled-NOT gate then the converted images are scrambled by using quantum bit-plane and grey code and the last step is encrypting the scrambled quantum image. In 2020, an algorithm proposed for colour image encryption based on hyper chaotic map and mitochondrial DNA sequences [15] in which colour image encryption exploits an embarrassment operation that depending on a hybrid chaotic map. The first step is to separate each channel of colour images into number "n" of clusters. The second step is to create global shuffling over the total image.

The final step is to apply intra-pixel reconstructing in each cluster, which results in very non-ordered pixels in the encrypted image.

From above literature, we conclude that, QKD provides unconditional secure communication method and supports a powerful encryption scheme. The combination between classical communication and QKD creates a new technique called semi quantum key distribution SQKD. Unfortunately, SQKD increases the schemes complexity and requires two steps for ciphering, scramble and encryption. In this paper, a new enhancement for image processing algorithms is proposed. We applied QKD scheme to raise the security level to the confidential data to be transmitted over unsecure channel. The proposed scheme raises the difficulty for an attacker to hack the encrypted data. The proposed algorithm exploits the QC benefits to save images' information. Also there is no middle coding or scrambling step to reduce the algorithm complexity depending on the power of QKD. Also, the usage of the quantum channel and devices is limited to eliminate the SQKD drawbacks.

The rest of the paper is divided as follows. In section 2, an introduction to QC and OKD is presented. Section 3 explains the proposed algorithm. In section 4, results is showed and discussed. Also, a discussion is showed to compare the proposed algorithm to other algorithms [14] and [15] and finally, in section 5 the conclusion is presented.

2. Quantum cryptography and quantum key distribution

QC exploits quantum physics and quantum mechanics characteristics, which uses Heisenberg's uncertainty principle and the No-cloning theorem [2], [3]. Therefore, scientists adopted quantum mechanics to create a new branch of cryptography depending on the quantum properties. By QKD, any two communicated parties can encrypt and decrypt the messages with unique property of quantum mechanics, and the system can sense any eavesdropper. This is because the fact that the process of measuring any quantum system disturbs it. Therefore, the eavesdroppers' try will be detected easily. The first protocol of QKD is BB84 [1].

BB84 is related to its inventors "Charles H. Bennet and Gilles Brassard" in 1984. This protocol uses the polarization states of single photons to transmit a random key. Photons emerged from a light source often have a random polarization angle. To specify a selected polarization angle to the photon, a light filter is used to allow only photons that have the selected polarization angle to pass. The polarization angle is used to encode the transmitted bits.

The basis is chosen to substitute "0" and "1" without ambiguity. The first choice is rectilinear basis in which angles of 0° and 90° representing "0" and "1", respectively. The second choice is the diagonal basis; i.e., angle of 45° represents "0" and 135° represents "1". For simplicity, we denote 0°, 90°, 45° and 135° as H,V,D and A respectively. The polarization basis for H and V is denoted by + while the polarization basis for D and A is represented as ×. Table 1.shows the polarization angles for used basis in BB84 protocol.

Table 1 Polarization angles for BB84 protocol

Basis	0	1
+ (linear)	(0°) →	(90°) ↑
× (diagonal)	(45°) ↗	(135°) ↘

The data unit in QC protocols is qubit and it is defined as a physical structure defined by the quantum mechanics laws [16]. The qubit is mathematically represented by $|\psi\rangle$ [16] which is a unit vector in the two dimensional Hilbert space $|\psi\rangle \in \boldsymbol{\mathcal{H}^2}$ [16]. A qubit $|\psi\rangle$ is expressed as [16]:

$$|\psi\rangle = \alpha|p\rangle + \beta|q\rangle \quad (1)$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

Where $\alpha, \beta \in \mathbb{C}$, and $\{|p\rangle, |q\rangle\}$ is a random basis spanning $\mathcal{H}^2$[16]. The most important consequence of the vectorial nature of a qubit is that it is possible to write it in linear combination of elements of any basis. The choice of $\{|p\rangle, |q\rangle\}$ is often the orthonormal basis $\{|0\rangle, |1\rangle\}$ known as the computational basis.

In addition to the computational basis {|0⟩, |1⟩}, it is common in quantum cryptography protocols to use the diagonal basis {|+⟩, |−⟩} defined as [16]:

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \quad (3)$$

$$|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \quad (4)$$

3. Proposed algorithm

The proposed algorithm exploits QKD to generate a random key that used for image encryption operation. The key is totally random which provide a kind of difficulty to hack it. Also, the quantum mechanics principles will alarm the communicated parties for any hacking or eavesdropping attempt. The proposed algorithm is summarized as follows:

1- A QKD-based key is shared between Alice and Bob. That key has a unique property of quantum mechanics. By using BB84 protocol.
2- The confidential data is XORed with the generated key to encrypt and cipher it.
3- The encrypted data is sent through communication link.
4- At receiver, the received encrypted data is XORed again with the key to decrypt it.

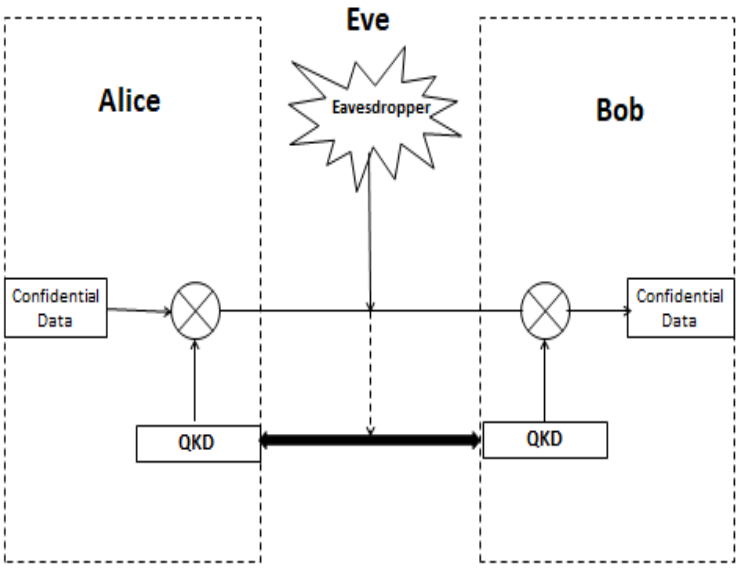


Fig.1 Schematic diagram for the proposed algorithm

The schematic diagram for the proposed algorithm is shown in Fig.1. Here Alice and Bob generate and share the quantum secret key before exchanging data. The quantum secret key and the confidential data are XORed together for data encrypting purpose before transmission. The encrypted data is transmitted through the communication link meanwhile Eve tries to hack both the communication link and QKD shared between Alice and Bob. This hacking try can be detected immediately due to the quantum mechanics properties as represented in Heisenberg's uncertainty principle and No-cloning theorem. As illustrated in Table 2, Alice and Bob use any selected QKD protocol (BB84) then the selected QKD protocol is applied for secret key establishment step.

Table 2 Random secret key extraction steps

Alice bits	1	0	1	0	1
Alice random basis	V	H	+	H	V
Random polarization	↑	→	↗	→	↑
Bob random selected polarization	V	-	V	H	V
Measuring basis	√	×	×	√	√
Bob measured basis	↑	↘	↑	→	↑
Result key	1	-	1	0	1

Where V, H, + and - represent state$|1>$, state$|0>$, state $|+>$ and state$|->$, respectively. While, the polarization angles 90°, 0°, 45° and 135° are represented as ↑ , ,↗, and , respectively. Now the resultant key is generated as "1101" after sifting the different measured basis. Once the secret key is generated Alice and Bob use this key for image encryption operation. First, Alice applies XOR process to encrypt the image. On the other hands, Bob receives the encrypted image and uses XOR operation to extract the original image.

The communication here is normal with a new feature which is the secret key is created by QC which make the following advantages:

1- Unconditional security communication system based on QKD system.
2- Ease of eavesdropping detecting.
3- Ultimate secure key generated.
4- Totally random generated key.
5- No need for a quantum server or third authenticated party.
6- No need for adding a digital signature for mutual authentication.

The expecting scenario is as follows:

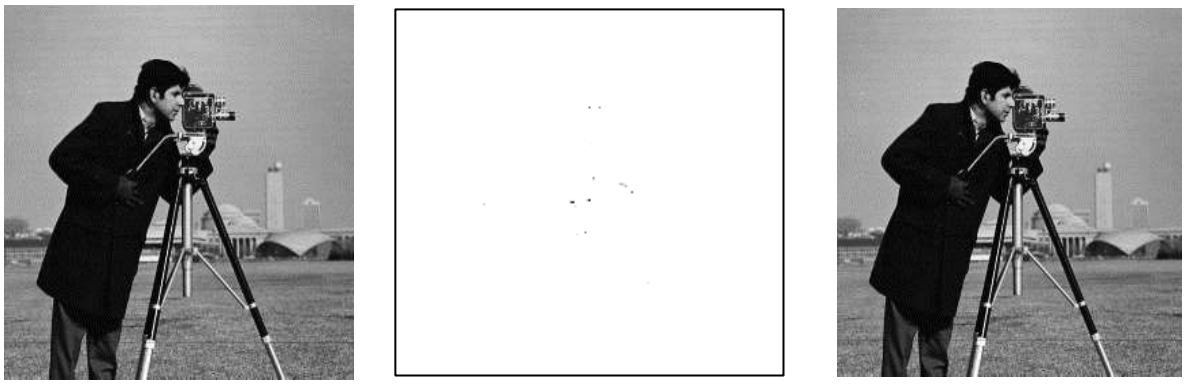
- First, Alice and Bob decide to exchange a confidential data between each other.
- Alice and Bob generate and share a completely secret random key based on QC. In other words a QKD.
- Alice prepares the confidential data to be XORed with the generated quantum key to encrypt it.
- Bob will receive the encrypted data. After eavesdropping check step he will apply XOR operation to encrypted data to decrypt it in order to extract the original confidential data.
- Any eavesdropping attempt will be discovered at once, alerts the communicated parties to that a hacker tries to steal their data then they decide to seize the communication.

4. Results and Discussions

In this section, we show the results of the proposed algorithm, by examining four datasets (Cameraman, Katrina, Aeroblk, and Honey badger images).

The key is created by QKD and then the image is XORed with the created key. As shown in Figs. 2, 3, 4, and 5, the original images are shown in Figs. 2a and 3a, and then the shared secret key which is created via QKD is XORed with the confidential dataset to encrypt it. The encrypted data is approximately hidden and has no information as shown in Figs. 2b and 3b.

On the other hand, at the receivers, the decrypted data is XORed with the shared secret key, as represented in Figs. 2c and 3c the decrypted image is rebuilt identical copy of the original dataset (image).



(a) Original image (b) Encrypted image (c) Decrypted image

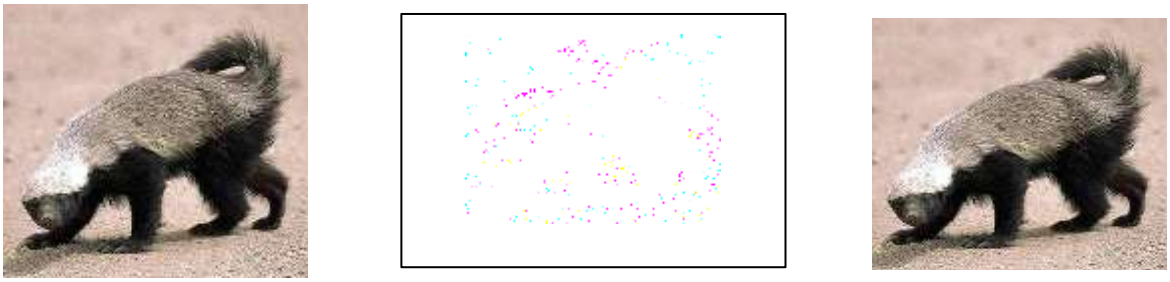
Fig.2. the proposed algorithm is applied to “cameraman” dataset

(a) Original image (b) Encrypted image (c) Decrypted image

Fig.3. the proposed algorithm is applied to “Katrina” dataset

(a) Original image (b) Encrypted image (c) Decrypted image

Fig.4. the proposed algorithm is applied to “Aeroblk” dataset



(a) Original image (b) Encrypted image (c) Decrypted image

Fig.5. the proposed algorithm is applied to "Honey badger" dataset

4.1 Simulation verification and statistical analysis

4.1.1 *Approximation quality metrics.* Approximation quality metrics are used to determine the image quality after encryption and decryption process. They consist of the Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Maximum Squared Error (MAXERR), and Ratio of Squared Norms (L2RAT), for an input image, X, and its approximation, Y. MSE is defined as the mean square error between an image, *X*, and an approximation, *Y*, is the squared norm of the difference divided by the number of elements in the signal or image N:

$$\mathrm{MSE} = \frac{\|\mathrm{X}-\mathrm{Y}\|^2}{\mathrm{N}} \tag{5}$$

Increasing MSE means the difference between the original image and the encrypted one is higher and is recommended for good encryption. PSNR is known as the peak signal-to-noise ratio in decibels (dB).

$$\mathrm{PSNR} = 20\log_{10}\frac{2^{\mathrm{B}}-1}{\sqrt{\mathrm{MSE}}} \tag{6}$$

It is recommended for PNSR to be low as possible for powerful encryption. MAXERR is the maximum absolute squared deviation of the data, X, from the approximation, Y. Higher MAXERR is better for encryption and represents good encryption algorithm. L2RAT is the ratio of the squared norm of the signal or image approximation, Y, to the input signal or image, X. The Structural Similarity (SSIM) Index quality assessment index is based on the computation of three terms, namely the luminance term, the contrast term and the structural term. The overall index is a multiplicative combination of the three terms. It measures the structural similarity between two images if it is the same, the result will be one and for different structure the better results is less than one. Naturalness Image Quality Evaluator (NIQE) no-reference image quality score calculates the no-reference image quality score for image X using the Naturalness Image Quality Evaluator NIQE. It compares X to a default model computed from images of natural scenes. Smaller score indicates better perceptual quality. If it is equality the structure of the two images is same and as it increases good encryption is achieved. The results of simulation for Cameraman and Katrina images are shown in table 3, table 4, table 5, and table 6 respectively.

Table 3.Cameraman image encryption/ decryption simulation results

	Original	Encrypted	Decrypted
PSNR	------	7.2463	Inf
MSE	------	$1.2259x10^4$	0
MAXERR	------	203	0
L2RAT	------	1.1642	1
SSIM	------	0.0822	1
NIQE	4.0994	11.2612	4.0994

Table 4.Katrina image encryption/ decryption simulation results

	Original	Encrypted	Decrypted
PSNR	------	5.4796	Inf
MSE	------	$1.8413x10^4$	0
MAXERR	------	203	0
L2RAT	------	1.3078	1
SSIM	------	-0.019843	1
NIQE	4.1943	9.1278	4.1943

Table 5.Aeroblk image encryption/ decryption simulation results

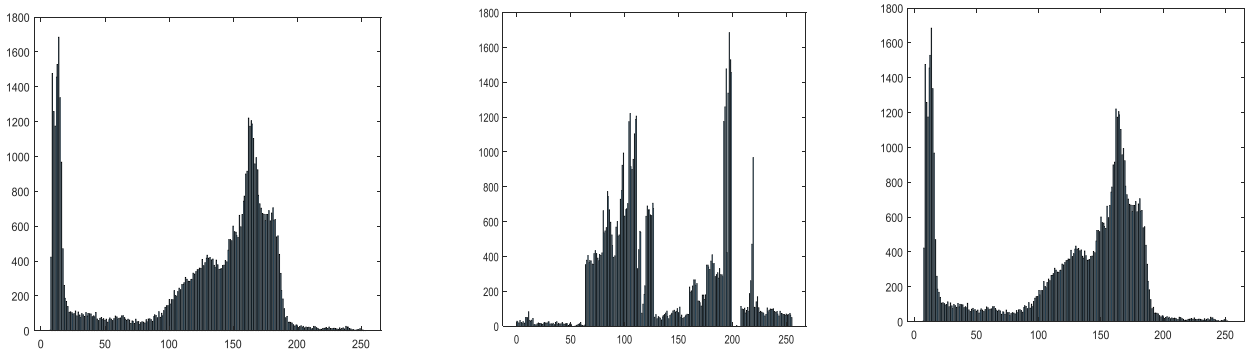
	Original	**Encrypted**	**Decrypted**
PSNR	------	3.8151e+00	Inf
MSE	------	$2.7013x10^4$	0
MAXERR	------	203	0
L2RAT	------	1.0649	1
SSIM	------	-0.016606	1
NIQE	3.2418	6.8626	3.2418

Table 6.Honeybadger image encryption/ decryption simulation results

	Original	**Encrypted**	**Decrypted**
PSNR	------	4.9242	Inf
MSE	------	$2.0925x10^4$	0
MAXERR	------	203	0
L2RAT	------	0.665546	1
SSIM	------	-0.028315	1
NIQE	4.2938	14.576	4.2938

As shown in Tables 3, 4, 5, and 6 the proposed algorithm fulfils the required conditions for a powerful algorithm. The obtained results show the powerful performance of the proposed. As shown, MSE is very high refers to a huge difference between the original data set and the encrypted one. PNSR is very low means a powerful encryption algorithm. MAXERR is extremely different between the original images and the encrypted ones points to approximately total difference between them and its value is zero compared to the decrypted images means that there is no difference between them which shows the power of the algorithm. Finally, L2RAT, SSIM, and NIQE focus how the encrypted images are different to the original ones and how the decrypted copies are the same to the original data sets.

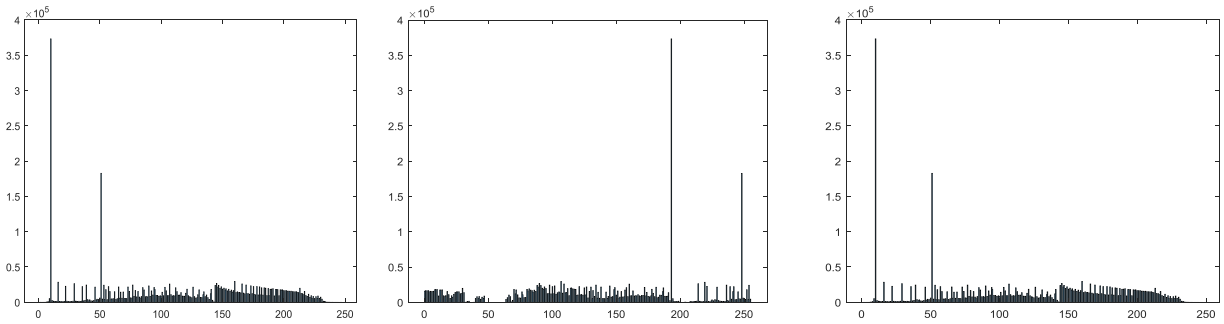
4.1.2 Histogram analysis. Histogram is a type of bar plot for numeric data that group the data into bins. Figs.6, 7, 8, and 9 show the histogram of original images of Cameraman and Katrina and the corresponding histogram of the encrypted images and decrypted ones.



(a) Original image (b) Encrypted image (c) Decrypted image

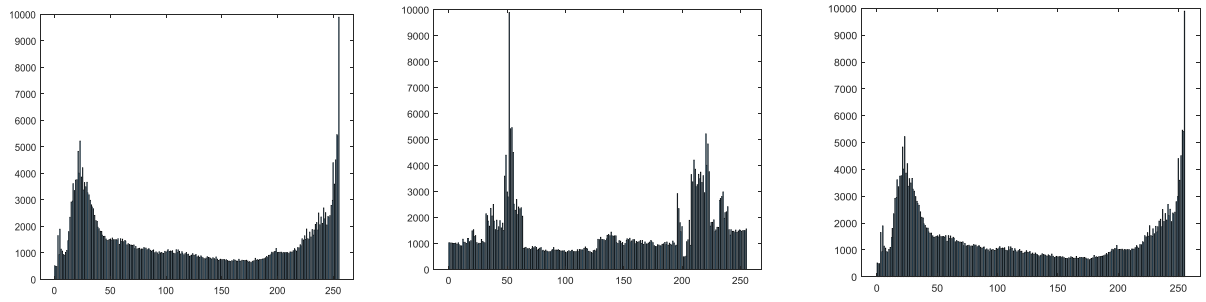
Fig.6. the histogram analysis to "cameraman" dataset

In Fig. 6, the histogram of original cameraman image, encrypted image, and decrypted image are represented in Figs. 4a, 4b and 4c, respectively. As shown, the values of the numeric plots for the encrypted image are extremely different to the values of the original image because of the applying the powerful encryption process to the original image. On the other hand, the decrypted image is the same to original one without any small change. Similarly, the same results are found in Fig.7, Fig.8, and Fig.9 for "Katrina", "Aeroblk", and"Honey badger" datasets. Obviously, the histogram of the encrypted image is totally different to the original one, which proves the effectiveness and the powerfulness of the proposed algorithm with QKD.



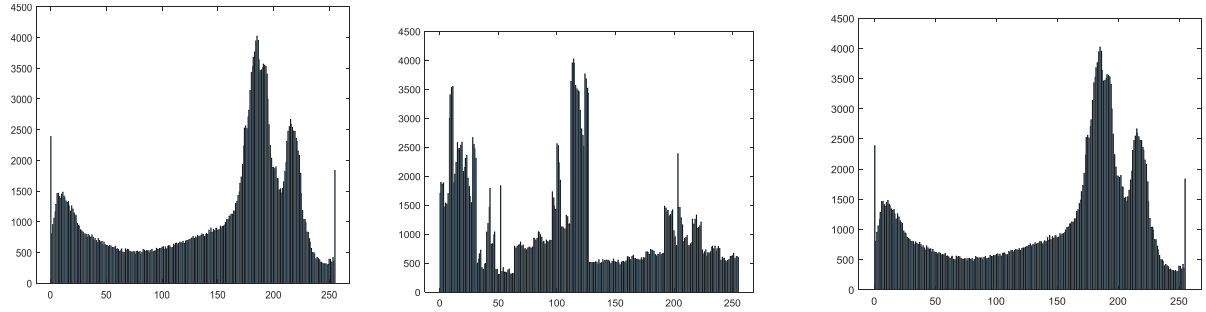
(a) Original image (b) Encrypted image (c) Decrypted image

Fig.7. the histogram analysis to "Katrina" dataset



(a) Original image (b) Encrypted image (c) Decrypted image

Fig.8. the histogram analysis to "Aeroblk" dataset



(a) Original image (b) Encrypted image (c) Decrypted image

Fig.9. the histogram analysis to "Honey badger" dataset

*4.1.3 Correlation of adjacent pixels.*The correlation between any pairs of two adjacent pixels is given by:

$$\text{coef} = \frac{\sum_{i=1}^{M}\left(k_i-\frac{1}{M}\sum_{j=1}^{M}k_j\right)\left(l_i-\frac{1}{M}\sum_{j=1}^{M}l_j\right)}{\sqrt{\sum_{i=1}^{M}\left(k_i-\frac{1}{M}\sum_{j=1}^{M}k_j\right)^2\sum_{i=1}^{M}\left(l_i-\frac{1}{M}\sum_{j=1}^{M}l_j\right)^2}} \quad (7)$$

Where M is the total number of adjacent pixels pairs in each direction and k_i, l_i are the values of adjacent pixels. Adjacent pixels in encrypted image should be de-correlated for powerful encryption algorithms. Table 7 shows the correlation of adjacent pixels for Cameraman, Katrina, Aeroblk, and Honey badger images.

Table7. Results of adjacent pixels of Cameraman, Katrina, Aeroblk, and Honey badger images

Image		**Direction**		
		Diagonal	Vertical	Horizontal
Cameraman	Original	0.908	0.959	0.939
	Encrypted	0.682	0.754	0.749
Katrina	Original	0.894	0.915	0.919
	Encrypted	0.771	0.798	0.803
Aeroblk	Original	0.968	0.98	0.982
	Encrypted	0.899	0.921	0.925
Honey badger	Original	0.911	0.919	0.944
	Encrypted	0.772	0.789	0.817

4.1.4 *Number of pixel changing rate and unified average changing intensity*. There are two quantities used to judge the power of any encryption algorithm. The first one is the number of pixel change rate (NPCR) and the second measure is unified average changing intensity (UACI). Suppose $U(i,j)$and $V(i,j)$be the (i,j)th pixel of two images U and V, respectively, Then NPCR and UACI can be expressed by using

$$\mathrm{NPCR} = \frac{1}{\mathrm{M}} \times \sum_{\mathrm{i,J}} \mathrm{D(i,j)} \times 100\% \tag{8}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{M}} \left(\sum_{\mathrm{i,j}} \frac{|\mathrm{U(i,j)} - \mathrm{V(i,j)}|}{2^{\mathrm{N}} - 1} \right) \times 100\% \tag{9}$$

Where M is the total number of image pixels' and N is the number of bits required for pixels representation and $D(i,j)$is given by:

$$\mathrm{D(i,j)} = \begin{cases} 0 \text{ if } \mathrm{U(i,j)} = \mathrm{V(i,j)} \\ 1 \text{ if } \mathrm{U(i,j)} \neq \mathrm{V(i,j)} \end{cases} \tag{10}$$

Table 8 shows the simulation NPCR and UACI results.

Table8. NPCR and UACI simulation results

Image	NPCR%	UACI%
Cameraman	99.61	33.4
Katrina	99.61	33.4
Aeroblk	99.61	33.4
Honey badger	99.61	33.4

It is preferred for powerful encryption algorithm that NPCR to be about 99% and UACI to be about 33%. As shown in Table 6, the proposed algorithm fulfils the required conditions for a powerful algorithm.

4.1.5 *Entropy analysis.* Entropy is a scalar value representing the entropy of grey scale image I. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. In other words, reflects the insecurity of image data, was denoted by E (m) of matrix m, and evaluated by:

$$\mathrm{E(m)} = -\sum_{\mathrm{i}=1}^{2^{\mathrm{L}}-1} \mathrm{p(u_i \log_2(p(u_i))} \tag{11}$$

Where $p(u_i)$ is the probability u_i. There are 2^8 probabilities for a gray scale image. The ideal entropy value is equal to 8-bit. So that the entropy value of the encrypted image should be close to 8 for efficient encryption algorithm. Table 9 shows the entropy of the proposed algorithm.

Table9. Entropy analysis

Image	Original	Encrypted
Cameraman	7.009716	7.016
Katrina	7.009716	7.016
Aeroblk	7.669	7.7273
Honey badger	7.669	7.7273

As shown in Table 9, the entropy is close to 8 which means that the proposed algorithm fulfils the required conditions for a powerful algorithm. The simulation operated with assumption of using AWGN channel. This looks like satellite communication link. So this new algorithm could be used as a secure communication link for image transmission and reception. The encrypted data is sent via Read Solomon Coded Channel (RSCC) with 255 as the total number of code symbols and 223 as the number of data symbols being encoded. This

channel is equivalent to the satellite communication channel to discuss the channel performance and bit error rate BER after add the encrypted data by means of the proposed algorithm [17].

Table10. Comparison between proposed algorithm, [14], and [15]

factor	[15]	[14]	proposed
CF(av.) "image"	0.972	0.944	0.933
CF(av.)"enc. image"	0.00336	0.0089	0.728
NPCR	99.6	99.6	99.6
UACI	33.4	36.0075	33.4
Entropy	7.99	6.42	7.009716
SSIM	--------	--------	0.0822
NIOE	--------	--------	11.2612
MSE	--------	--------	$1.23x10^4$
PSNR	--------	--------	7.2463
MAXERR	--------	--------	203
L2RAT	--------	--------	1.1642

In this proposed algorithm most of the drawbacks of SQKD are eliminated. From another point of view, comparing the simulation results of the proposed algorithm to algorithms in [14] and [15] a kind of enhancement is achieved like simplicity as there is no middle scrambling or encoding stage beside that the proposed algorithm fulfills most of the required conditions for a powerful algorithm compared with [14] and [15] despite of being simpler as represented in Table 10. In Fig.10 the comparison between the proposed algorithm and both algorithms in [14], [15] results. As represented in the figure the results are approximately equal however the proposed algorithm is simpler and quietly powered by means of QKD.

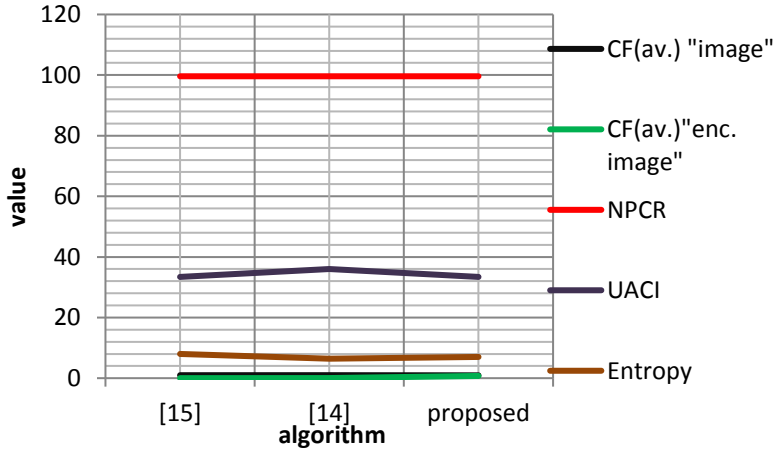


Fig.10 Comparison between proposed algorithms and [14] and [15]

5. Conclusion

In this paper a new image encryption algorithm is proposed. The proposed algorithm is based on quantum mechanics fundamentals that make it more secure as any hacking or eavesdropping try will be discovered at once. Also the generated secret key is totally random makes it very difficult to be cracked. It can be applied for any type of type of data that considered being confidential. Beside that it is a simple algorithm and does not require many complex processes and mutual authentication.

Acknowledgements

We would like to express our sincere appreciation to the reviewers for the valuable comments that have significantly enhanced the quality of this paper. The paper was introduced in the

19th International Conference on Aerospace Science and Aviation Technology ASAT-19, Military Technical Collage, Cairo, Egypt.

References

[1] Bennett, C.H. and Brassard, G., 1987. Quantum public key distribution reinvented. ACM SIGACT News, 18(4), pp.51-53.Wootters,
[2] Wootters, W.K. and Zurek, W.H., 1982. A single quantum cannot be cloned. Nature, 299(5886), pp.802-803.
[3] D'Ariano, G.M. and Yuen, H.P., 1996. Impossibility of measuring the wave function of a single quantum system. Physical review letters, 76(16), p.2832.
[4] Wiesner, S., 1983. Conjugate coding. ACM Sigact News, 15(1), pp.78-88.
[5] Boyer, M., Kenigsberg, D. and Mor, T., 2007, January. Quantum key distribution with classical Bob. In 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07) (pp. 10-10). IEEE.
[6] Boyer, M., Gelles, R., Kenigsberg, D. and Mor, T., 2009. Semiquantum key distribution. Physical Review A, 79(3), p.032341.
[7] Zou, X., Qiu, D., Li, L., Wu, L. and Li, L., 2009. Semiquantum-key distribution using less than four quantum states. Physical Review A, 79(5), p.052312.
[8] Jian, W., Sheng, Z., Quan, Z. and Chao-Jing, T., 2011. Semiquantum key distribution using entangled states. Chinese Physics Letters, 28(10), p.100301.
[9] Zou, X., Qiu, D., Zhang, S. and Mateus, P., 2015. Semiquantum key distribution without invoking the classical party's measurement capability. Quantum Information Processing, 14(8), pp.2981-2996.
[10] Lu, H. and Cai, Q.Y., 2008. Quantum key distribution with classical Alice. International Journal of Quantum Information, 6(06), pp.1195-1202.
[11] Li, Q., Chan, W.H. and Zhang, S., 2016. Semiquantum key distribution with secure delegated quantum computation. Scientific reports, 6(1), pp.1-6.
[12] Renuka, D. and Reddy, P.C., 2018. Integrated Classical and Quantum Cryptography Scheme Using Three Party Authenticated Key Distribution Protocols. Materials Today: Proceedings, 5(1), pp.1017-1023.
[13] Armanuzzaman, M., Alam, K.M.R., Hassan, M.M. and Morimoto, Y., 2017, December. A secure and efficient data transmission technique using quantum key distribution. In 2017 4th International Conference on Networking, Systems and Security (NSysS) (pp. 1-5). IEEE.
[14] Abd El-Latif, A.A., Abd-El-Atty, B. and Talha, M., 2017. Robust encryption of quantum medical images. IEEE Access, 6, pp.1073-1081.
[15] Mohamed, H.G., ElKamchouchi, D.H. and Moussa, K.H., 2020. A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences. Entropy, 22(2), p.158.
[16] Abd-El-Atty, B., Venegas-Andraca, S.E. and Abd El-Latif, A.A., 2018. Quantum information protocols for cryptography. In Quantum Computing: An Environment for Intelligent Large Scale Real Application (pp. 3-23). Springer, Cham.
[17] Samy, R. and Mahran, A., 2020. Low Complexity Viterbi Decoder for RSCC Concatenated Codes. In Journal of Physics: Conference Series (Vol. 1447, No. 1, p. 012040). IOP Publishing.