IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 10, Issue 1, Ser. I (Jan. - Feb. 2020), PP 44-48
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Multilayered Information Security in Quantum Image

Kalaiarasi G[1], StanelyKarunakaran W[2]
[1](Electronics And Communication Engineering, Mam College Of Engineering, Trichy)
[2](Associate Professor /Ece Department, Mam College Of Engineering, Trichy)

Abstract: *The internet users are regularly increasing day by day. After the launching of the 4G or IMT-Advanced services, communication over internet increased drastically. People across all the communities like social, economic, business, financial, etc. are doing communication or exchanging their valued documents over internet. The demand for securing the data in efficient way has been increased. As, cryptography is the best way to secure the communication. This work implements the chaotic algorithm which guarantees the security of the information. The proposed encryption/decryption algorithm is devised based on NEQR quantum image representation. Simulation analysis shows that the proposed quantum image encryption approach is robust, realizable, and has high efficiency compared with its classical counterpart.*
Keywords: *chaotic systems, cryptography, Quantum Image, Qubits, NEQR*

I. Introduction

Protecting the information content in digital imagesis essential today for diverse purposes, from military to healthcare systems. 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 communication channel or IOT network is important for patient confidentiality[7]. Therefore, for health-care 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[2]: 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 diffusion component can be verified in the 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 confusion and diffusion in the plain images to obtain secure cipher images.

Quantum mechanics lead to the creation of quantum computation and later quantum computers to solve problem that cannot be efficiently solved in traditional computers. In 1982, Feyman introduced the idea of quantum computers, a novel computation model which involves aphysical machine that accept input states as a superposition of many different inputs in another state as output state[3]-[6]. In quantum computes, an image is captured and stored by suitable representation models. The literature offers various models for quantum images, such as Real ket[5]; Entangled Image[9]; Multi-Channel representation of quantum image(MCRQCI); log-polar[10]; Flexible representation of quantum images(FRQI)[11], which used 2^{n+1}qubits to represent a $2^n * 2^n$grey image; and the novel enhanced quantum representation(NEQR)[12] which uses 2^{n+q}qubits to represent a $2^n * 2^n$ grey image. Although NEQR requires 2^{n+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 are 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[12].

Researchers have developed a lot of cryptographic algorithms, but most algorithms are intended to encrypt messages in text form. Although conventional encryption algorithms such as DES, AES, Blowfish, Serpent, RC4, RSA, ElGammal, Rabin can also encrypt images but the algorithm is safe enough to be applied. This is due to the image have different characteristics with textual data. An Image generally has a large data capacity, so the image encryption requires large computational volume. Some application that have a need for real-time such as teleconferencing, live streaming, and others, obviously require high computing speed that the conventional algorithm is obviously not suitable for encrypting image.

Arnold's Cat Map algorithm(ACM) is one of the cryptographic algorithm used to encrypt the image. The concept of the algorithm is continuously rotate the image so that it becomes a form that is not visible and random so that the image cannot be seen by the naked eye but can still be recognized by the system for image file(image) of the same.

II. Proposed Work

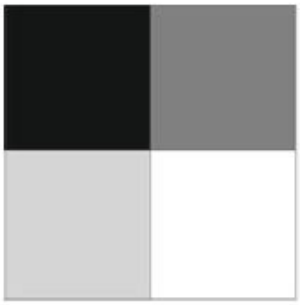
The proposed work consists of the given discussed phases.

1.Quantum Image Representation

The transformation process of an image from classical into quantum form is the first step in the quantum image processing. The grey scale image can be represented in the quantum state by several models such as NEQR representation[12], which contains the color and corresponding position information of every pixel in the image. The representative expression of the NEQR model for a $2^n * 2^n$ image can be expressed as follows:

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

Where $|ci\rangle$ is the color value, and $|i\rangle$ is the information about the corresponding position.



$$|I\rangle = \frac{1}{2}(|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle + |255\rangle \otimes |11\rangle)$$
$$= \frac{1}{2}(|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle)$$

Fig 2.1 A 2*2 example and it representative expression in NEQR

The obvious is that NEQR utilizes the basis state of qubit sequence to represent the grey scale of pixels instead of probability amplitude of a single qubit in FRQI. Different grey scales can be distinguished in NEQR because different basis states of qubit sequence are orthogonal. Fig 2.1 illustrates a 2*2 gray scale image and its representative expression in NEQR. In this figure, because the grey scale ranges between 0 and 255, eight qubits are needed in NEQR to store the grey-scale information for the pixels. Therefore NEQR needs q+2n bits to represent a $2^n * 2^n$ image with gray range 2^q.

2. Quantum Cryptography

Chaos is a common technique used in the random number generator[4], it's happening because this technique is faster and easier to use in the process stream object both in terms of storage and process objects only a few functions (chaotic maps) and some parameters (initial conditions) were quite good used if the process takes quite a long time[4]. Arnold's cat map chaotic two dimensions that can be used to change position of the pixel without removing any information from the image[8], pixel image can be assumed by $S = \{(x, y) |\ x, y = 0,1,2, \dots \dots N-1\}$. Two dimensional image of Arnold's cat map can be written by the following equations:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix} \text{ (mod n)} \quad (2)$$

$$\begin{pmatrix} 1 & p \\ q & q+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ (mod n)} \quad (3)$$

Where p and q are positive integers, the determinant (A) = 1. (x', y') is the new position of the original pixel position (x,y) when Arnold's cat map algorithm performed once. Results after application of Arnold's cat map to the number of iterations R will be a random drawing that contains all the values of the same pixel of the original image. The number of iterations R to complete depending on the parameters p, q and N size of the original image. So Arnold's cat map algorithm has parameters p, q and the number of iterations R, all can be used as a secret key[8].

3. Framework Implementation

The image to be secured is initially converted into quantum image using the NEQR quantum representation algorithm. The quantum image is then encrypted using the Arnold's cat map algorithm and then is decrypted using the same to obtain the original secret image. Here are the steps how algorithms work

1. Read the Image file
2. Convert the image into grey scale image
3. Identify each pixels and position of the image.
4. Convert it into quantum image using NEQR algorithm.
5. Read the color pixel RGB.
6. Calculate the position X, Y pixel in the image to be encrypted.
7. Rotation (iteration) RGB pixels to the image to be random and cannot be recognized.

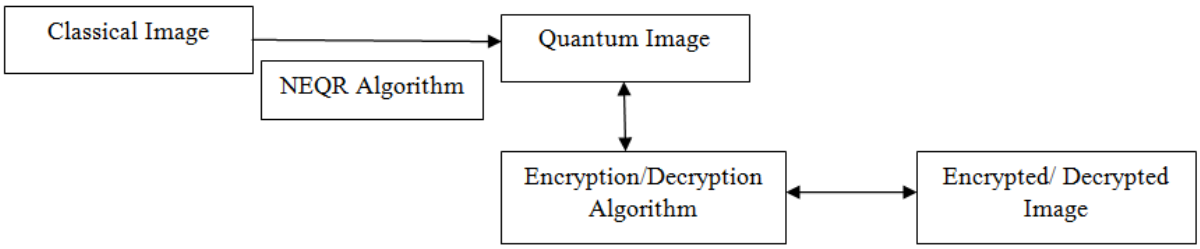


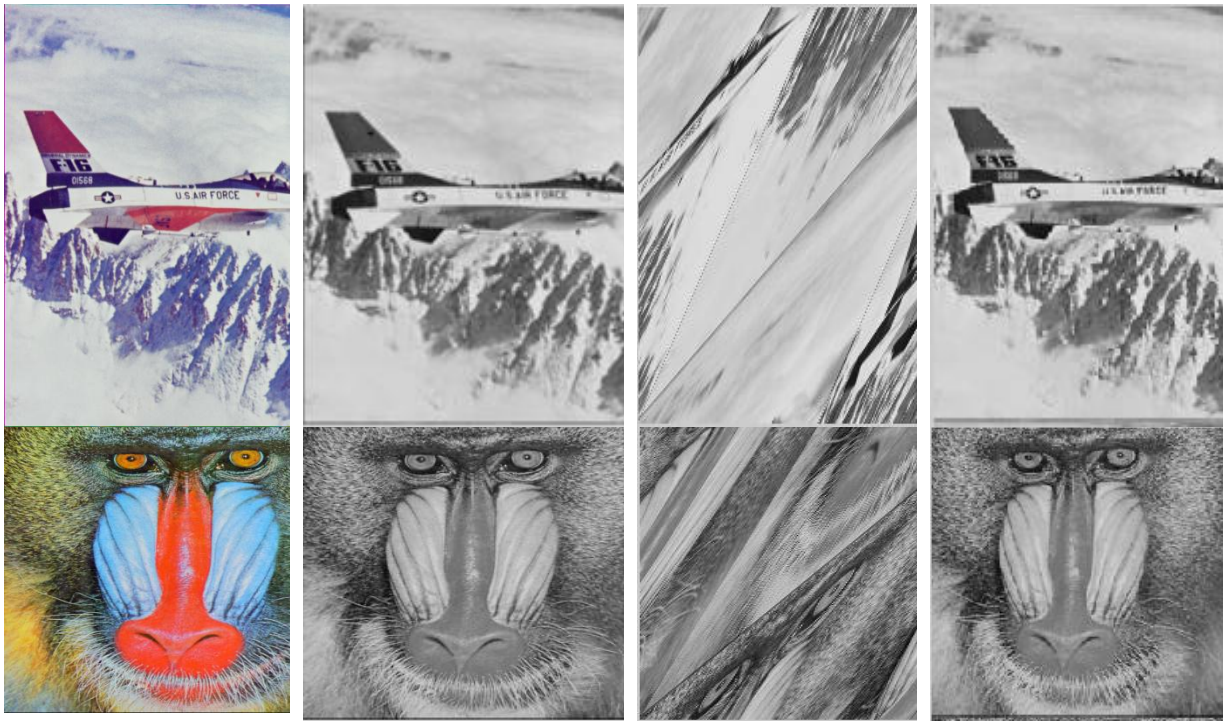
Fig 2.2 Process Flow

III. Experiment and Result

To analyze the proposed approaches, a laptop with 6 GB RAM and Intel core CPU equipped with MATLAB R2014a is utilized to perform quantum operations on quantum images. Fig 3.1 shows the simulation result of the image converted into quantum image and the encrypted image using Arnold's cat map algorithm as well the image is decrypted to get the original image. Image of different size is taken as the input image and the following simulation results are discussed as below.

The difference between the original image and the encrypted image is compared and found to be of minimal difference with no loss in image information. The entropy of the quantum and original image is compared and found to be equal. Entropy of an image is the measure of image information content, which is interpreted as the average uncertainty of information source.

Original Image	Quantum Image	Encrypted Image	Decrypted Image



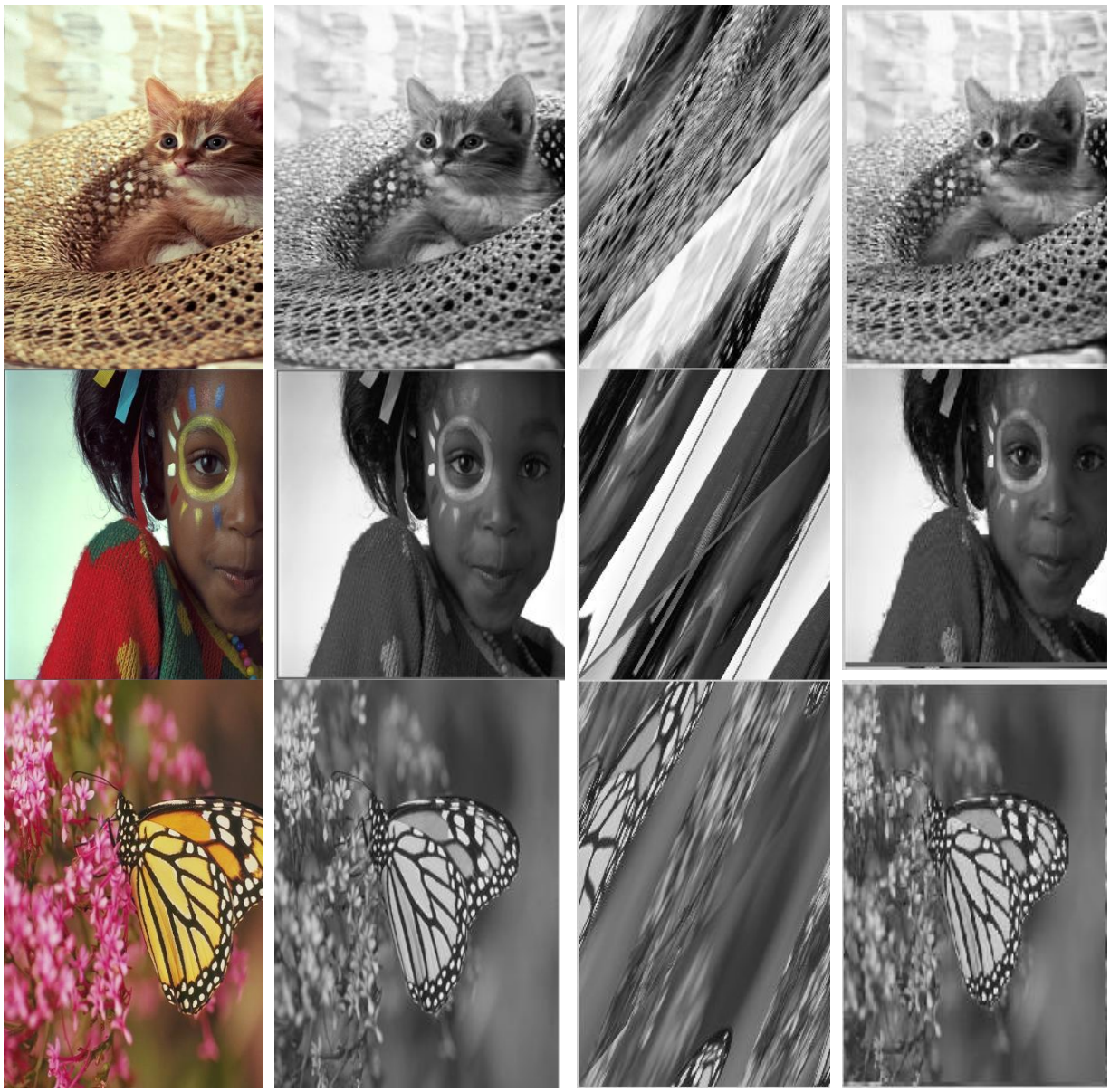


Fig 3.1 Simulation result

In Image, Entropy is defined as corresponding states of intensity level which individual pixels can adapt. Table 3.1 represents the entropy comparison of the original image and quantum image. These values are compared to be more or less equal.

Original Image	Quantum Image
7.6783	7.2297
7.9269	7.8753
7.5227	7.1613
7.5338	7.4748
6.6798	6.7311

Table 3.1 Entropy comparison of original and quantum image

IV. Conclusion

A highly secure quantum image cryptography approach is shown in this work. Arnold's cat map encryption is good enough to secure a digital image, especially in the security pixel mostly algorithm cryptography secures files or specific to text, berdeda with other algorithms Arnold's cat map could safeguard the image of a well without reducing the value or information of a digital image that is secured and this is one of the advantages of this algorithm is the author of the analysis of this study.

References

[1]. B. Sun *et al.*, ``A multi-channel representation for images on quantum computers using the RGBacolor space," in *Proc. IEEE 7th Int. Symp.Intell. Signal Process.*, Sep. 2011, pp. 1_6.

[2]. C. E. Shannon," Communication theory of secrecy systems", *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656_715, Oct. 1949.

[3]. 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.

[4]. E. AVAROĞLU , "Pseudo Random Number Generator Based on Arnold's Cat Map and Statistical Analysis," Turkey, 2011.

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

[6]. M. A. Nielsen and I. L. Chuang, ``Quantum computation," in *Quantum Information*, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, 2010,pp. 13_211

[7]. M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Alamri. "Toward end-to-end biometrics based security for IoT infrastructure" *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44_51, Oct. 2016.

[8]. P. Gupta, S. Singh and I. Mangal, "Image Encryption Based On Arnold Cat Map and S-Box," IJARCSSE, vol. IV, no. 8, pp. 807-812, 2014.

[9]. 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.

[10]. 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, 2013.

[11]. P. Q. Le, F. Dong, and K. Hirota, ``A _exible representation of quantumimages for polynomial preparation, image compression, and processingoperations," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 63_84, Feb. 2011.

[12]. Y. Zhang, K. Lu, Y. Gao, and M. Wang, ``NEQR: A novel enhancedquantum representation of digital images," *Quantum Inf. Process.*, vol. 12,no. 8, pp. 2833_2860, Aug. 2013.