Securing Medical Images using Quantum Cryptography

Nikita Bhati, Mokshada Hambir, Shivani Linganwar, Prof. Neha Patil
Department of Computer Science Engineering, AISSMS IOIT College, Pune, India

Abstract- Security is most essential thing in data as well as image security, in health care most of cases data has been hacked from unauthorized third parties. The unauthorized access should breach the privacy of data owner.For health care image security many existing systems have been proposed like watermarking, image stereography, visual cryptography as well, but each having some drawbacks related to privacy breaching. In proposed System, 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 Quantum Shor's encryption/decryption algorithm are devised based on a quantumcryptographic techniques. Numerical and simulation analyses show that the proposed quantum image encryption approach is robust, realizable, and has high efficiency compared with its classical counterpart. The Arnold scrambling has used for creating the scrambled image and logistic sine map has used for encryption index. The NEQR function creates the m*n array for scrambled image encryption with minimum time complexity. The proposed work experiment analysis also reduces the time complexity and enhance the security in untrusted cloud environment.

I. INTRODUCTION

Medical images have become an essential part of medical diagnoses and treatments. Often, many diseases are better diagnosed through medical imaging. Occasionally, there are needs to refer patients for further diagnosis and treatment without physically moving their medical records to the referred location, and these are usually transferred through network communication infrastructure such as the internet. Usually, medical images are classified information that should be treated with utmost confidentiality. Now to ensure the integrity and confidentiality of a medical image, medical professionals must properly secure these data with the network communication infrastructure in order for the patient referred location to receive the exact transferred medical image.

Nowadays, the transmission of images is a daily routine, and it is necessary to find an efficient way to transmit them over the networks. With the number of internet users on the increase every day, everything done online is under the threat of malicious intruders. The transmission of images over the internet is challenging because of the high risk of eavesdroppers and internet communication hackers. In this manner, one of the secured means of transmitting the image over the internet is cryptography.

Cryptography is a security tool that provides security in the ciphers of a message. It is also the art ofencoding and decryption messages and has existed as long as individuals have distrusted one another andsought forms of secure communication. Cryptographic algorithms use encryption keys, which arethe elements that flip a general cryptography formula into a particular methodology of cryptography.Cryptography plays a central role in itinerant communication, e-commerce, Pay-Tv, causation personal emails, and transmitting financial information, and it touches on many aspects of daily lives.There arevarious cryptologic schemes obtainable, one in every of that is that the Quantum Cryptography. QuantumCryptography, or Quantum Key Distribution (QKD), applies elementary laws of physical scienceto guarantee secure communication. It enables two legitimate users to produce a shared secret random bit string, which can be used as a key in cryptographic applications, such as message encryption(for instance, the one-time pad) and authentication. Unlike typical cryptography, whose security typically depends on trial machine assumptions, QKD guaranteessecurity supported the elemental laws of quantum physics.

Quantum Cryptography solves the problem of secret Key cryptography by providing a way for two authorized users who are in different locations to securely establish a Network secret Key. Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it.Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Since the encrypting and decrypting keys are different, it is not necessary to securely distribute a key. The security of public-key encryption depends on the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers

II. PROBLEM STATEMENT

To define the approach for the quantum image encryption of healthcare media using proposed combination of Arnold scrambled and Quantum Shores algorithm using cloud storage during the image transmission and system also eliminates and automatically recovers the different attacks from end user using security algorithms.

.

III. LITERATURE SURVEY

Yashpal singh Rajput et al.[1] Projected an encryption technique which has an advanced and enhanced adaptation of existing technique called hill cipher. The grouping of encryption strategy and block based conversion are done to secure image. By accounting such idea to blocks of an image, the correlation between the image's pixels becomes low and to understand the original image becomes hard to cryptanalysis as the quantity of blocks are fixed. Therefore, they conclude that for secure image communication the block size of an image should be small. Utmost 8 blocks are used to separate an image in the proposed strategy

C. X. Zhu et al. [2] Proposed an algorithm using the concept of encryption theory as the encryption is based on a third-order chaotic system in which the theory is defined for the RGB levels of image, because the high security is the character of a high-order chaotic system. They confused the relation between the encrypted image and the original image by means of shuffling the position and varying the RGB levels of each pixel. Finally, they have finished up their system, best case scenario.

J. Scharinger et al. [3] In this system author described a method of encryption based on chaotic Kolmogorovflow. In this method, the entire image is treated as one block and then key controlled chaotic method is use to perform permutation. In order to confuse the data, a substitution based on a shift-registered pseudo-random number generator is applied, which alters the statistical property of the cipher image. It was advocated that the scheme is computationally secure and superior to contemporary bulk encryption systems when aiming at efficient image and video data encryption.

Hossam El-din H. Ahmed et al.[4] Anticipated an encryption technique called "efficient chaos based feedback stream cipher" (ECBFSC).The method consist of logistic map and an external key. Session key concept, dividing key in 8 block used in an encryption process. Their technique's sensitivity to the plain image is also a plus to the security of the proposed ECBFSC. They have performed analysis on feedback mechanism and on Lena image to prove their proposed technique as the best and can be used in real time scenario

Rakesh S et al. [5] proposed an algorithm that breaks the correlation among the pixels position of an image so that the encrypted image can be so differ to recognize. Firstly, entropy of pixel position and pixel value is increased by applying block shuffling and chaotic series correspondingly. Then the original image is divided into blocks and by means of Arnold cat map block based shuffling is performed. Additionally a scrambled image is produced. That scrambled image is again shuffled as a whole. Lastly that image is encrypted by applying chaotic series on it. They concluded that the encrypted image has less correlation coefficient and high entropy by demonstration and analysis

Pratibha S. Ghodeet al.[6] introduced a new „keyless" (without any key) technique for encrypting lossless images. The aim of proposed work is to amplify the security level by arbitrarily distribute pixels bits over the whole image and to perk up the storage capacity of the system .The encryption and decryption algorithm is intended for lossless broadcast of an image. The author tested their technique on some other images which shows good outputs. Finally they conclude by discussing about the advantage of a keyless approach

Manish Mishra et al. [7] proposed a technique which uses Chaotic System, Wavelet Transform along with the fingerprint of the image is created by using Hash Function. All is to be transmitted to the receiver. An input image is taken on which encryption technique is applied. The method proceeds by applying the Wavelet Transform. Application of Wavelet Transform converts the image into frequency domain from where we can gather the minute details of the image. Then inverse Wavelet Transform is applied to get the image from frequency domain. Finally the image obtained is an encrypted image. Besides encryption the hash function is applied on the original image to get the fingerprint of the image. The fingerprint of the image is obtained which is used to maintain the integrity of the image.

IV. PROPOSED SYSTEM ARCHITECTURE

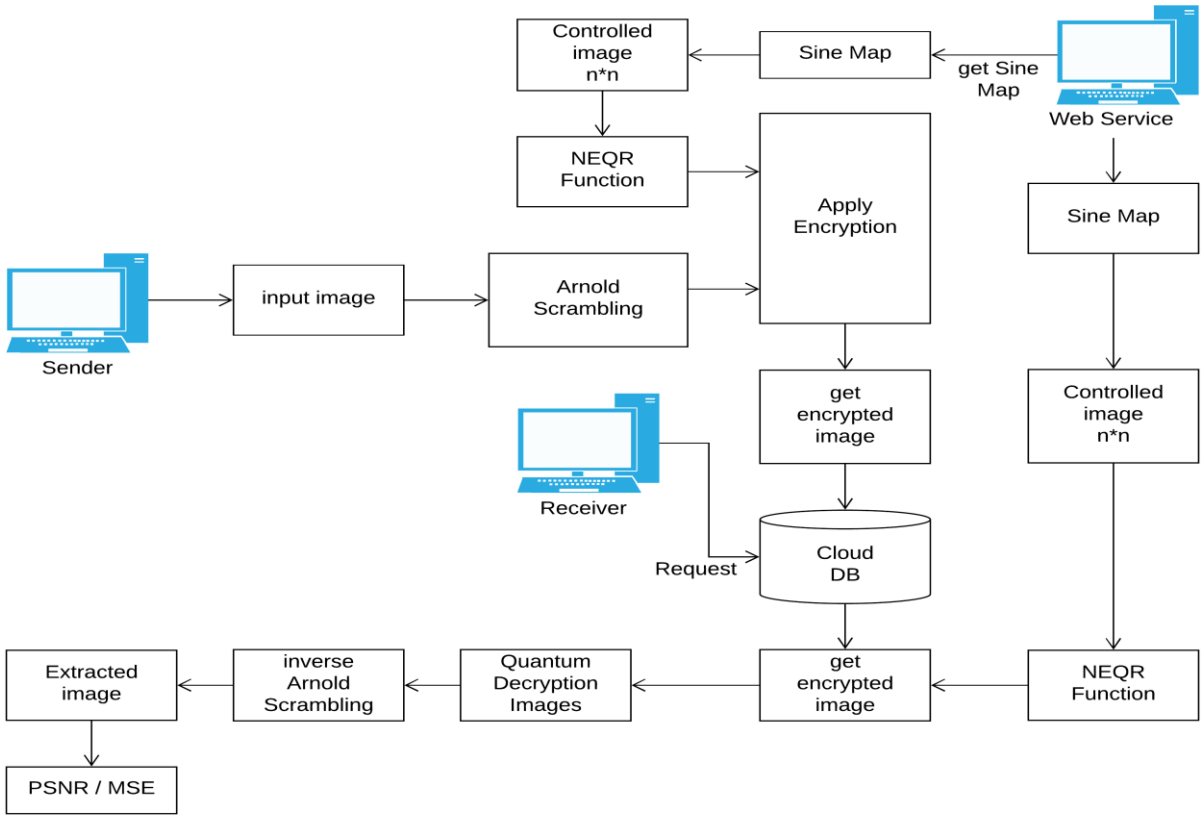

Fig.1: Proposed System Architecture

V. IMPLEMENTATION PROCEDURE

Image scrambling- In this phase any type of image can be selected for the encryption like JPEG, PNG or BMP and the input image will be scrambled using Arnold scrambling.

Image Encryption- The scrambled image will be given as a input to encryption algorithm. Encryption is the method of applying or changing some of the attributes of the original image to form a very different image. Nobody can read the exact image if he is unknown of the change done by the content owner. The logistic sine of m*n has used for image encryptionInverse Scramble - This is the action performed at the receiver side. After receiving the encrypted the main task of the receiver is to extract the original data hide behind the image. This technique is known as scramble image extraction.

Inverse Scramble -This is the action performed at the receiverside. After receiving the encrypted image, the main task of the receiver is to extract the original data hidden behind the image. This technique isknown as scramble image extraction.

Image Recovery-Image recoveryis the technique of decrypting the received image. The main task is togenerate the image same as the original image. And this is done by the reversibly perform the encryption action i.e. by using the decryption key of sine map.

Arnold Scrambling Algorithm

Step 1:Read input image [m*n]

Step 2

$$Px = \sum_{k=0}^{n} |(Col[i])\ |(Row[i])$$

Step 3:W = | Px == Th | → {1,0}

Step 4: image [i][j] =W

Step 5: return image;

Where, Px is ->Pixel Value of each block of image

Th is = this is user define threshold

W is = current weight where we stored in w it should be 0 or 1

m and n is =height and width [512*512]

Quantum N SHOR'S Factorization Algorithm

Period-Finding Subroutine: The quantum circuits used for this algorithm are designed for each choice of N and the random a used in

f(x) = ax mod N, find Q = 2q such that

N2 ≤ Q < 2N2

Which implies Q/r >*N*The input and output qubit registers have to be compelled **to** hold super positions of values from zero to Q − one, sohave Q qubits every. and so have q qubits each. Using which it may appear to be double as many qubits as necessary guarantees that there are at least N different x which produce the same f(x), even as the period approaches N/2.Proceed as follows:

Step1- Initialization of the registers to:

$$Q^{-1/2} \sum_{x=0}^{Q-1} |x\rangle|0\rangle$$

Where value of x is from 0 to Q − 1, This initial state couldbe superpositionof letter states.Step 2- Construction of the function f(x) as a quantum function and apply the same function to the above state to obtain,

$$Q^{-1/2} \sum_{x} |x\rangle|f(x)\rangle$$

this is still a superposition of Q states

Step 3- Now, By Applying the Quantum Fourier Transform to the input register. This Fourier transform (operating on a superposition of power-of-two Q = 2q states) uses a Qth root of unity

such as ω = e2πi / Q to distribute the amplitude of any given |x› state equally among all Q of the |y› states, and to do so in a different way for each different x:

$$U_{QFT|x\rangle} = Q^{-1/2} \sum_{y} w^{xy} |y\rangle$$

This leads to the final state:

$$Q^{-1} \sum_{x} \sum_{y} w^{xy} |y\rangle \ |f(x)\rangle$$

This is a superposition of much more than Q states, but many fewer than Q2 states. Although there are Q2 terms in the sum, the state

can be factored out whenever x0 and x **turn** out identical worth.Let ω = e2πi /Q, be the Qth root of unity, r be the period of f, x0 be the smallest of a set of x which yield the same given f(x) (where x0 <*r*), and b run from 0 to [(Q − x0 − 1)/r]

so that x0 + rb<*Q*.

Then ωry may be a unit vector within the advanced plane (ω may be a root of unity and r and y area unit numberand the coefficient of

Q−1|y›|f(x0)

In the final state is:

$$\sum_{x:f(x)=f(x_o)} w^{xy} = \sum_{b} w^{(x_0+rb)y} = w^{x_0 y}$$

Every value in the above equation represents a different path to the same result, and quantum interference occurs when the unit vectors ωryb point in nearly the same direction in the complex plane, which requires that ωry point to the positive real axis.

VI. RESULTS AND DISCUSSION

Table 1 summarizes the variation of PSNR (dB) with tree level L for different images. As table shows, distortion of image increases with rise in the value of L.

Table 1: Variation of PSNR (db) for different values of L

Host image 512*512	Tree level, L					
	0	1	2	3	4	5
Image1	48.8603	43.7978	39.2369	35.0450	30.6390	25.2971
Image2	48.3787	42.7184	37.3611	32.6427	28.9897	26.2350
Image3	48.4895	42.9967	37.8086	33.0630	28.7254	24.9868
Image4	49.4926	43.3546	37.0854	30.9795	25.0216	19.2101

Table 2 shows that PSNR is more when embedding is performed after dividing the image into blocks when compared with the embedding performed in a single image. Thus marked image quality increases after block division.

Table 2: Variation of PNSR (db) withbefore and image after extraction

Tree level	PSNR of Whole image	PSNR of two blocks	Average PSNR after Block Division
0	48.379	48.398	48.388
		48.378	
1	42.718	42.770	42.744
		42.718	
2	37.360	37.467	37.414
		37.361	
3	32.641	32.874	32.758
		32.642	
4	28.988	29.360	29.175
		28.989	
5	26.235	26.553	26.394
		26.235	

The below figure 2 and figure 3 also shows some additional experiments for proposed system based on the time complexity of system.

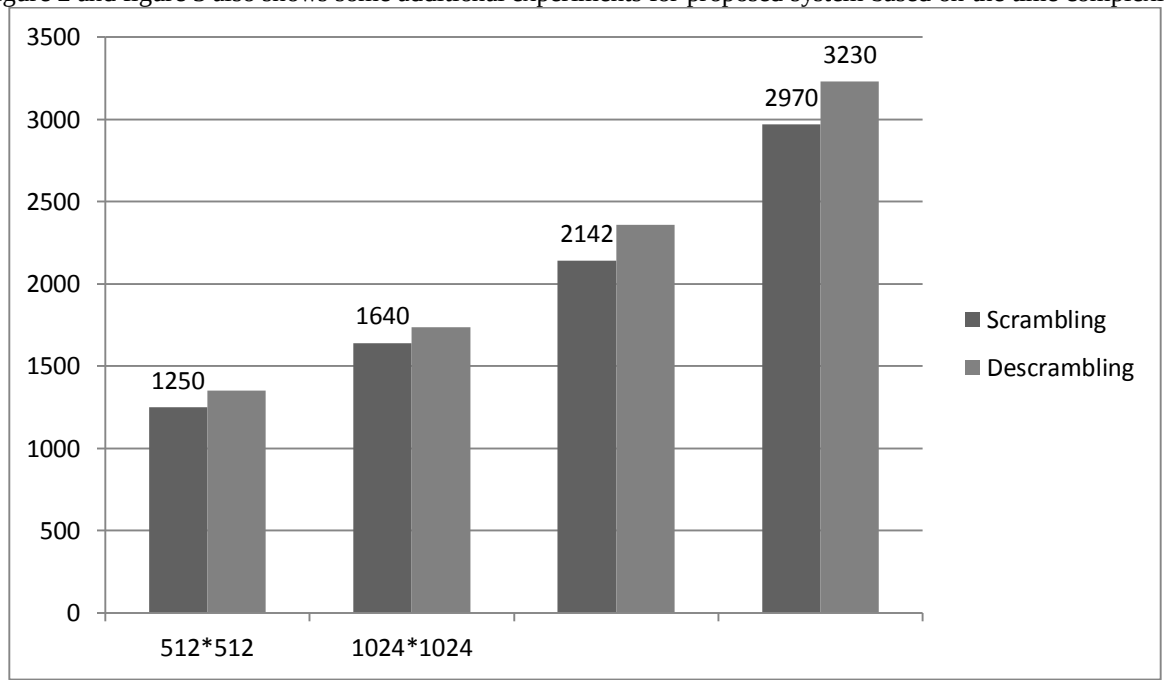

Fig.2: Time required for Arnold scrambling as well as inverse scrambling for different size of image (in milliseconds)

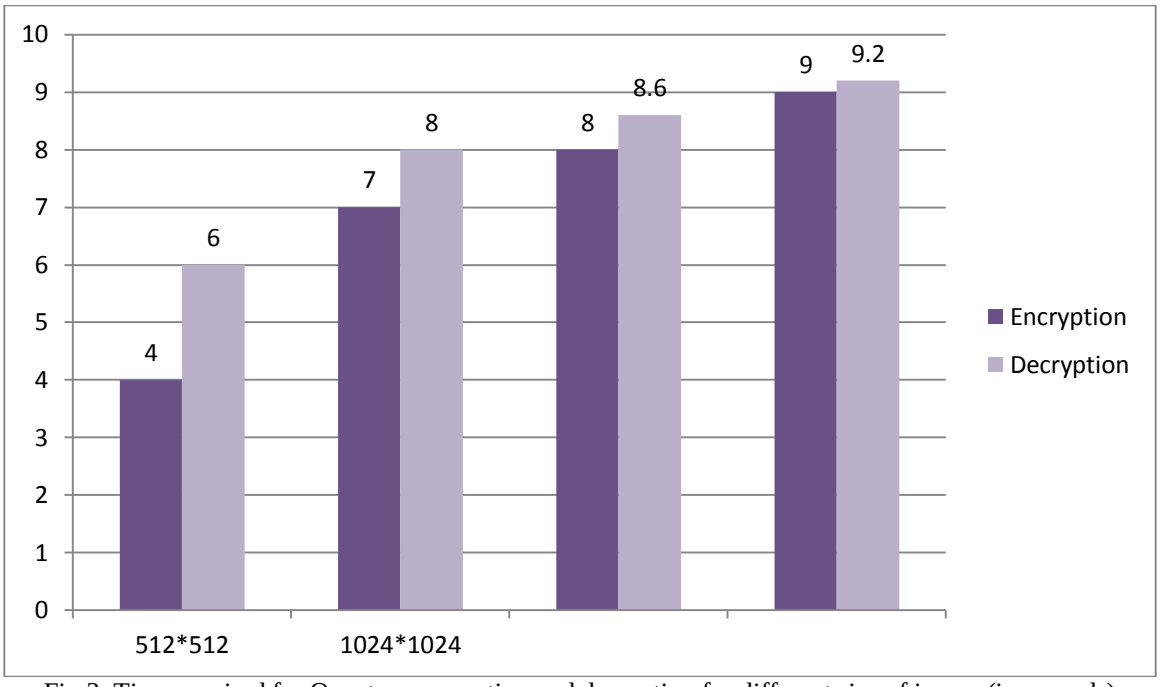

Fig.3: Time required for Quantum encryption and decryption for different size of image (in seconds)

VII. CONCLUSION

The proposed system provides the approach of security of quantum medical images in cloud environment. Basically, it is a need of healthcare industry to transmit medical images from one user to another using different communicates channels. The proposed approach can provide the security to system from external attackers.The system also reduces the losses, during the embedding as well as extraction of data and image. The experimental graphs and tables show the PSNR and MSEof each experiment.For performance analysis of the proposed approachon a classical computer, various simulations, and numerical methods were employed, such as correlation, Shannonentropy, sensitivity analysis, and histogram analysis.

VIII. REFERENCES

[1]. Yashpalsingh Rajput; A K. Gulve,A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher, International Journal of Computer Applications (0975 – 8887) Volume 95– No.4, June 2014

[2]. C. X. Zhu; Z. G. Chen; W. W. Ouyang, A new image encryption algorithm based on general Chen's chaotic system,Journal of Central South University (Science and Technology) 37 (2006) 1142.

[3]. J.Scharinger, Fast encryption of image data using chaotic Kolmo- gorov flows, J. Electron Imaging 7 (2) (1998) 318–325.

[4]. Hossam El-din H. Ahmed; Hamdy M. Kalash; Osama S. Farag Allah, An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption, Informatica 31 (2007) 121–129.

[5]. Rakesh S; Ajitkumar A Kaller; Shadakshari B C; AnnappaB,Image Encryption Using Block Based Uniform Scrambling and Chaotic Logistic Mapping, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.1,March 2012.

[6]. Pratibha S. Ghode; AbhaGaikwad,A Keyless approach to Lossless Image Encryption,International Journal of Advanced Research in Computer Science and Software Engineering 4(5), May - 2014, pp. 1459-1467.

[7]. Manish Mishra; Shraddha Fandi,Image Encryption Technique Based on Chaotic System and Hash Function,2014 IEEE International Conference on Computer Communication and Systems(ICCCS '14).