Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

A REVIEW PAPER ON MEDICAL IMAGE ENCRYPTION BY USING ARNOLD MAP

Shruthishree S H
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email ID: sh.shruthi@jainuniversity.ac.in

Abstract

Health staff are responsible for keeping patient records. Medical workers are not required to reveal any kind of patient-related medical information. This also refers to the medical knowledge that medical staff have discovered in connection with the patient's care. The problem of protecting confidentiality is becoming complicated with the advent of technology and its penetration into the medical sector in the form of telemedicine and e-health. Confidentiality needs to be shielded from medical image storage or image transfer from a medical database center to another center. Nowadays, in the corner of the medical photo, patient information is printed. This can be accessed by someone or even the data can be accessed and stored by the computer. Patient information can be intercepted by a third party during an electronic transfer. This could result in a major lawsuit. Apart from these security concerns, the picture should be used for situations such as medical testing, but patient information should be hidden. The patient's records should also be readily available to the medical staff for diagnostic purposes.

Keywords: *Arnold Map, Encryption, EEG, Image, Medical Image, Diagnostics, Accuracy, Confidentiality.*

I. INTRODUCTION

Secure and fast diagnosis is important in the medical field for saving the lives of people. Diagnosis involves generation of medical images. Medical images get generated using many ways like magnetic resonance imaging (MRI), radiography, ultrasound, nuclear medicine, tactile imaging, thermography, photo acoustic imaging and electroencephalography (EEG). Images are also generated during medical tests like electro cardio graph (ECG) and Magneto

Encephalography (MEG). As the size of these images is large, it requires a huge space for storage and good bandwidth for transmission in the original status [1].

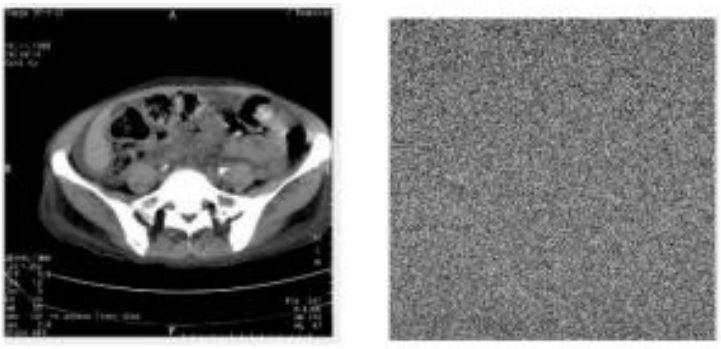

Figure 1: Illustrates the Original Image and Encrypted Image [2]

II. MEDICAL IMAGE ENCRYPTION

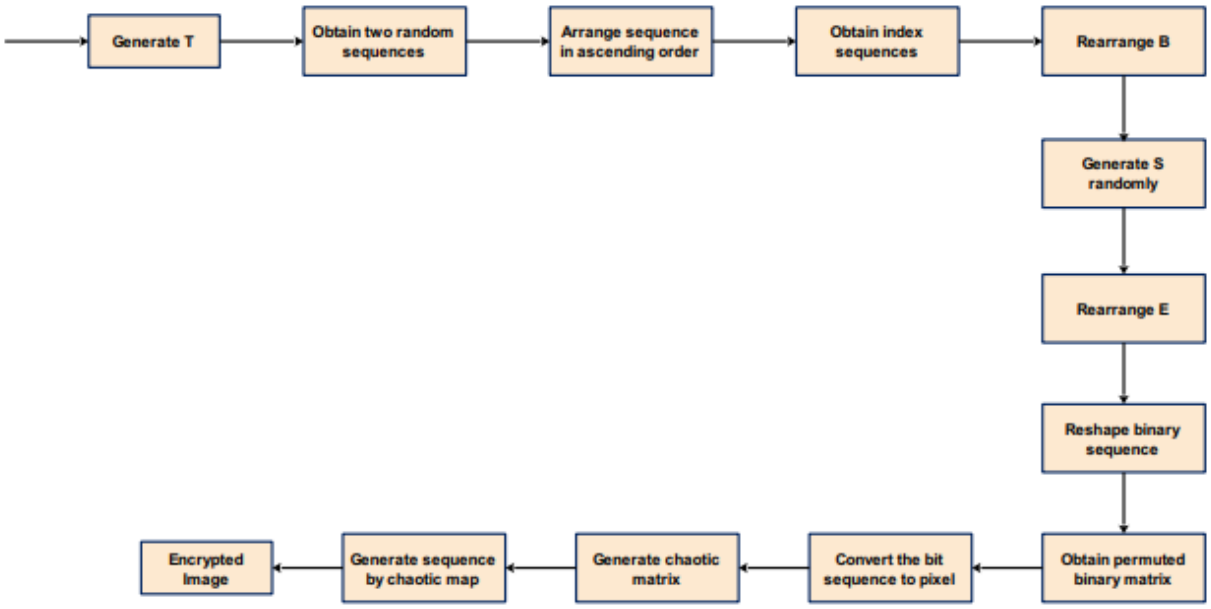

Figure 2: Illustrates the flow of the work

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$cov\ (x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\ (y_i - E(y))$$

$$r_{xy} = \frac{cov\ (x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)} \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [3].

$$r_{xy} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [4].

$$C(x,y) = \frac{\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K} \sum_{i=1}^{K} (x_i - E(x))^2$$

$$D(y) = \frac{1}{K} \sum_{i=1}^{K} (y_i - E(y))^2$$

III. LITERATURE REVIEW

A thesis on the robust encryption of quantum medical images was carried out by Abd et al. Medical media protection is essential for patient safety and confidentiality. A structure for chaos-based quantum encryption of healthcare images is proposed in this paper. Healthcare workers in one place submit cypher images to the cloud in the system. The photos are received from the cloud by the healthcare workers in another area. The healthcare workers will assist users in a safe manner by decrypting the content of the images. A new approach to the effective quantum image encryption of healthcare media is also suggested in this paper. The suggested algorithm uses grey code and a map that is chaotic. The quantum picture is scrambled with a grey quantum code [5].

IV. DISCUSSION AND CONCLUSION

In telemedicine and tele-diagnosis, patient knowledge plays a very vital role. Medical image content authentication is important as images are more and more distributed. It can be found in literature that there are many methods for medical image protection. The methods include compression, watermarking and modern secured transmission algorithms. The suggested method transforms a pixel of the image into binary bits. To obtain random numbers, the

subsequent Arnold map is used. Picture scrambling was done on the pixels' binary bits. Finally, a diffusion technique for the safe transfer of medical images was performed.

V. REFERENCES

[1] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," Signal Processing, 2017, doi: 10.1016/j.sigpro.2016.10.003.

[2] E. N. Kumar and E. S. Kumar, "A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach," 2013.

[3] H. T. Panduranga and S. K. NaveenKumar, "Selective image encryption for medical and satellite images," International Journal of Engineering and Technology, 2013.

[4] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[5] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust Encryption of Quantum Medical Images," IEEE Access, 2017, doi: 10.1109/ACCESS.2017.2777869.