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

A COMPREHENSIVE REVIEW ON MEDICAL IMAGE ENCRYPTION PROCESS IN DUAL DOMAIN

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

The booming desire for e-healthcare has inflated attention to the security of cyber-attack data in today's technological era. As digital medical images are transferred through the public network, an acceptable level of security is required. Encryption, which secures medical images, is one of the most popular processes. This paper recommends DICOM image encryption based on chaotic frequency domain attractors by integer wavelet transform (IWT) and spatial domain fused with deoxyribonucleic acid (DNA) sequence. A chaotic 3D Lorenz attractor and logistic map are used in the proposed algorithm to produce pseudo-random encryption keys. Subsequent stages are involved in the algorithm, i.e. permutation, substitution, encoding, complementary and decoding. Different tests were tested for 256 × 256 DICOM images to support the resistance of the proposed algorithm by achieving an average entropy of 7.99, a larger main space of 10238 and a non-zero correlation. The overall results confirm that the algorithm proposed is robust against attacks by brute force.

Keywords: *Health care, DICOM, DNA, Encryption, Image, Medical Image, Correlation, Frequency domain.*

I. INTRODUCTION

The transmission of data via the public system is extremely vulnerable. As a result, for many years now, the world of information security has become more risky. Medical images play an indispensable role in telemedicine for various analyses of the human body [1]. For various uses, such as tele-diagnosis and tele-surgery, the use of digital medical images has been strengthened. Digital Imaging and Communications in Medicine is the most general standard for the collection, secure storage and communication of medical images (DICOM).

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

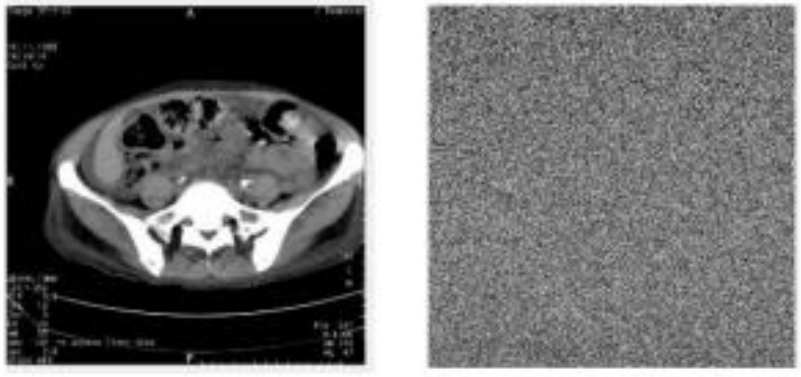

Figure 1: Illustrates the Original Image and Encrypted Image [2]

II. MEDICAL IMAGE ENCRYPTION PROCESS IN DUAL DOMAIN

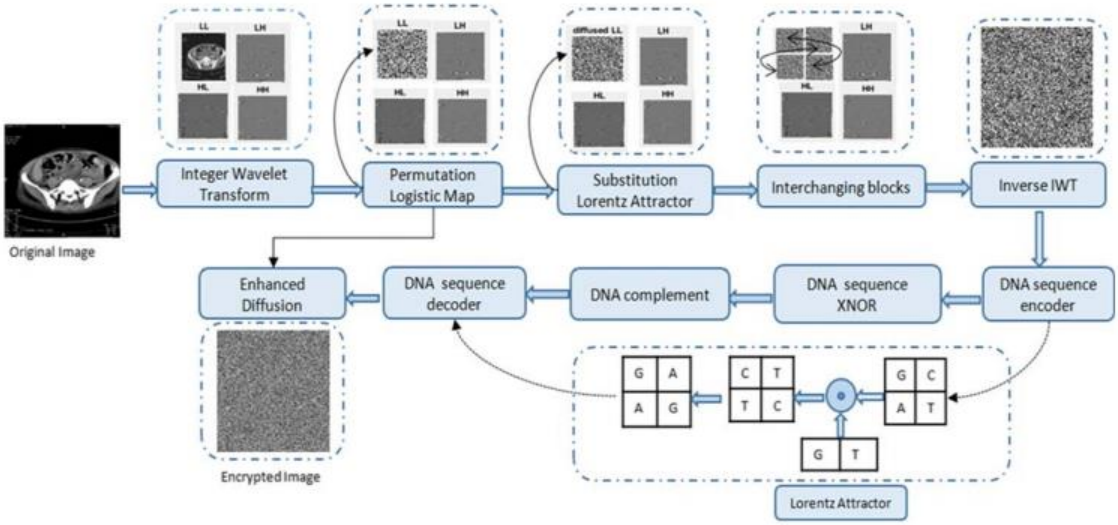

Figure 2: Illustrates the flow of the work [3]

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

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

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [5].

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

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

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

III. LITERATURE REVIEW

A research was carried out by Ravichandran et al. on the robust encryption of quantum medical pictures. For patient safety and confidentiality, medical media privacy is important. In this paper, a framework is proposed for chaos-based quantum encryption of healthcare images. Cypher photos are sent to the cloud in the system by healthcare staff in one location. In another place, the images are received from the cloud by healthcare staff. By decrypting the content of the images, the healthcare staff will support users in a secure way. In this paper, a new approach to the efficient quantum image encryption of healthcare media is also proposed. Grey code and a map that is chaotic are used in the suggested algorithm. With a grey quantum code, the quantum picture is scrambled [6].

IV. DISCUSSION AND CONCLUSION

The suggested chaos-based encryption algorithm mixed DNA to encrypt the DICOM files. Using the logistic map and Lorenz attractors accompanied by DNA sequence technique, IWT technology is used for the first degree of encryption. A BITXOR is carried out via a logistic map to obtain a final encrypted picture to intensify the security level. Several tests have been examined to determine the efficiency and robustness of the developed algorithm, such as statistical, differential, chosen-plaintext, key sensitivity, encryption quality and key space. The results obtained are also contrasted with certain current state-of-the-art designs. It has been verified by the results that the evolved chaos-DNA method based on IWT is useful for securing medical images in many real-time medical applications.

V. REFERENCES

[1] 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.

[2] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," IEEE Transactions on Information Technology in Biomedicine, 2012, doi: 10.1109/TITB.2012.2207730.

[3] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," Computers in Biology and Medicine, 2016, doi: 10.1016/j.compbiomed.2016.03.020.

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

[6] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA Chaos Blend to Secure Medical Privacy," IEEE Transactions on Nanobioscience, 2017, doi: 10.1109/TNB.2017.2780881.