Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 13, December 2019

MEDICAL IMAGE ENCRYPTION FOR SECURE DATA TRANSMISSION: A REVIEW PAPER

Soumya K N
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: kn.soumya@jainuniversity.ac.in

Abstract

Medical images are considered as one of the most important and sensitive data in Information systems. Sending medical images over the network requires a strong encryption algorithm such that it is resistant against cryptographic attacks. Among the three security objectives for the security of information systems namely confidentiality, integrity and availability, confidentiality is the most important aspect that need to be taken much care for the secure storage and transmission of medical images. This paper presents a comparison study of the encryption of medical images and extends an obvious scene for the researchers by examining the metrics such as PSNR (Peak signal-to-noise-ratio), MSE(Mean square error) and so on for various existing encryption techniques for medical images. This also comprises the process of analyzing the level of security, requirements and purpose of medical image encryption. This survey is useful for the researchers for the comparison of different encryption techniques implemented till date.

Keywords: *Information, Medical Images, System, Telecommunication, Secure data, Safety and protection.*

I. INTRODUCTION

Telemedicine is the usage of information systems and telecommunication systems to provide distant clinical care. This has been used to overcome the barriers of distance and access in rural areas that do not have clinical center facilities. It is also used to save lives in critical and emergency situations [1]. Now a day's telehealth is becoming increasing popular for the purpose of generating, transmitting and storing large volumes of electronic patient records

and medical reports. Also different platforms for telehealth and models are evolving in which the ways provides access and use clinical health data are changing constantly.

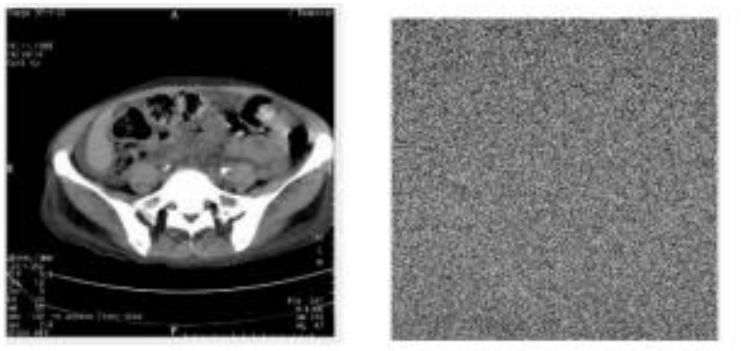

Figure 1: Illustrates the Original Image and Encrypted Image

II. MEDICAL IMAGE ENCRYPTION

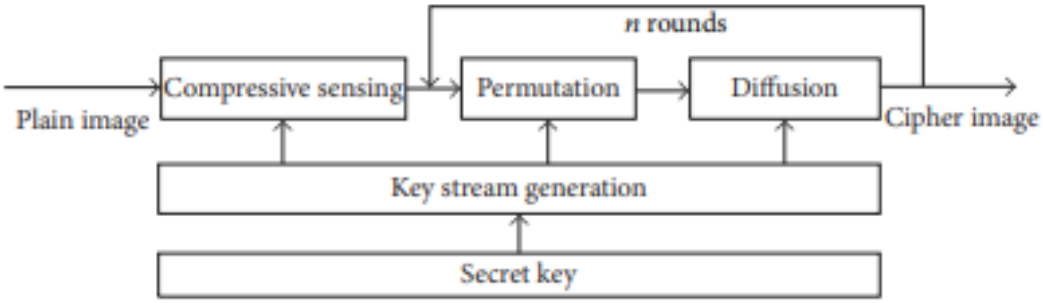

Figure 2: Illustrates the traditional picture encryption method [2]

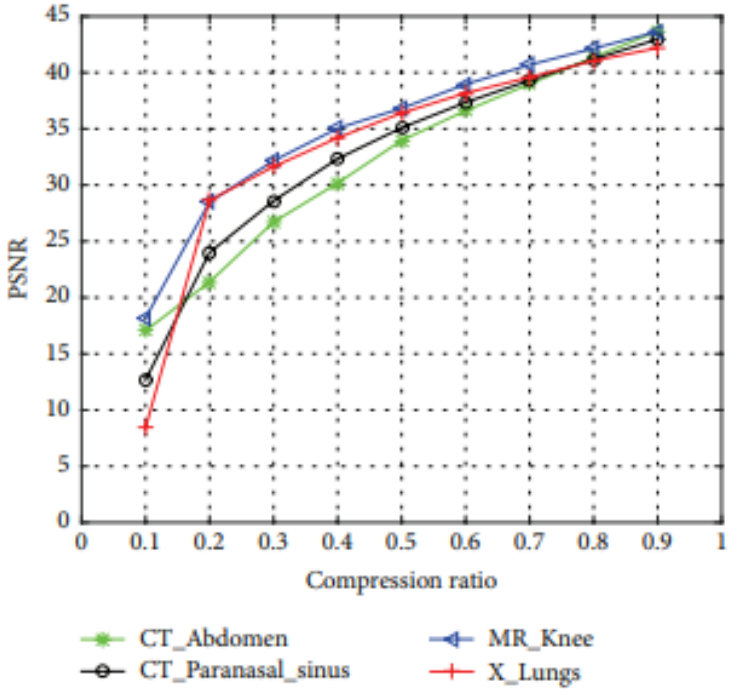

Figure 3: Illustrates the PSNR plot of diverse compression ratios [3]

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

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

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

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

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

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

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

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

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.

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

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

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

III. LITERATURE REVIEW

A symmetric image encryption scheme based on 3D chaotic cat maps was suggested by Li et al. Image encryption differs from that of texts because of certain inherent characteristics of images, such as bulk storage capability and high redundancy, which are typically difficult to handle by traditional methods. Chaos-based encryption has proposed a modern and effective

way to deal with the intractable issue of easy and highly secure image encryption, thanks to the extremely desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps. In this paper, the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme [5].

IV. DISCUSSION AND CONCLUSION

The need for medical image security is not only to ensure confidentiality and address confidentiality problems, but also to avoid the alteration of medical images that can be carried out by both approved and unauthorized users. Therefore, in terms of all the data, including medical images, there is a method to ensure security. A well-known solution that guarantees data and image protection in medical paradigms has been medical image encryption. We presented a thorough analysis of medical image encryption techniques in this paper and addressed many accompanying specifics. In different papers, several methodologies have been suggested that consider both spatial and frequency domains. There were also hiding data using Region of Interest and Region of Non Interest Segmentation. Medical care requires the highest picture quality and does not consider any changes made to the images. Thus, the medical image encryption method needs to be immune to some kind of network attack.

V. REFERENCES

[1] K. Anusudha, N. Venkateswaran, and J. Valarmathi, “Secured medical image watermarking with DNA codec,” Multimedia Tools and Applications, 2017, doi: 10.1007/s11042-015-3213-1.

[2] 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.

[3] A. M. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, “An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security,” 2017, doi: 10.1016/j.procs.2017.09.150.

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

[5] N. K. Pareek and V. Patidar, “Medical image protection using genetic algorithm operations,” Soft Computing, 2016, doi: 10.1007/s00500-014-1539-7.