A SURVEY ON SECURITY ON MEDICAL DATA AND IMAGES IN HEALTHCARE SYSTEM AND PAPER ID: 130

SWARNALI SADHUKHAN

ASSISTANT PROFESSOR OF MODERN INSTITUTE OF

ENGINEERING AND TECHNOLOGY

MAKAUT,WB

International Conference on Recent Trends in Machine Learning, IOT, Smart Cities & Applications (28th - 29th March 2020)

CONTENTS

INTRODUCTION

- The development in the field of networking technologies and telecommunications has increased the popularity of tele-medicine usage. This paper represents a technical survey on various cryptographic and watermarking processes which are applied on different medical images for secure transmission.
- As deterioration in the quality of the medical data or images at the time of transmission may endanger the treatment of patients, therefore, lossless and reversible methods need to be emphasized. In this study we have analyzed some of the most relevant existing works in this area.
- On the basis of this analysis we have tried to identify the open issues in the field of secure medical image transmission in order to provide secure transmission and ensure enhanced quality of treatment of the patients.

LITERATURE SURVEY

- A tiny change in the medical images may lead to the wrong diagnosis. Multi-layer security is explained in where DWT, DCT, and SVD are used at the time of watermark embedding and the chaotic encryption process is used to encrypt the watermark image.
- A fragile watermark is used to embed an Electronic Patient's Record (EPR) in the color image for an IoT driven healthcare system.
- A secure and hybridized medical data transmission process is proposed in an IoT based system where the data is encrypted using RSA and AES algorithm and DWT is used for watermarking.
- In a swapped Huffman tree, which is a lossless process, is used in a steganographic approach to secure and encrypt medical data and patient data.
- Determining image authenticity and self-recovery of attacked images has been done using an SVD based approach.
- The compression technique along with the cryptography algorithm for watermarking has been proposed for use in e-healthcare systems.
- A JPEG steganographic scheme is proposed where images are encrypted based on preserving inter-block dependencies.
- A Cognitive Radio (CR) technology and image encryption techniques are proposed where securely and efficiently transmit medical images.
- A chaos-based quantum encryption framework helps in securing healthcare images.
- The Quantum steganography approach is also can be used to Hides quantum secret image in a quantum cover image using.

COMPARATIVE ANALYSIS

Sl. No.	Title of the paper	Features	Advantages	Limitations & Future scope
1.	Multi-layer security of medical data through watermarking and chaotic encryption for tele-health application [1]	• DWT • DCT • SVD • Chaos based encryption	• Robust and secure • Hybrid Encryption process • improves confidentiality of patients data	• Single watermark image is used. • PSNR and MSE values can be improved • Not applied on video
2.	High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems [2]	• Generating stego RGB image using data embedder • Key is used for final encryption.	• High payload • High Imperceptibility • Detects tampering • Can be applied in real-time medical information interchange in IoT environment	• Fragile to geometric attacks

COMPARATIVE ANALYSIS

Sl. No.	Title of the paper	Features	Advantages	Limitations & Future scope
3.	Secure Medical Data Transmission Model for IOT-based Healthcare Systems [3]	• RSA • AES • DWT-2L	• High PSNR value • High imperceptibility and capacity	• Minimal deterioration
4.	Using image steganography for providing enhanced medical data security [4]	• Edge detection algorithm • Swapped Huffman tree	• Provides security and confidentiality of patients data • The imperceptibility property is maintained • Lossless encryption	• Slight variations in the peaks of the histogram.

COMPARATIVE ANALYSIS

Sl. No.	Title of the paper	Features	Advantages	Limitations & Future scope
5.	Secure and Robust Fragile Watermarking Scheme for Medical Images [5]	• SVD • Arnold Transform	• Resist VQ, addition of text, copy-paste attacks • Improves tamper localization accuracy and PSNR of self-recovered image	• Efficiency is not evaluated on non-fragile tampered images
6.	An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm [6]	• RG algorithm. • SHA-256 • Elliptical curve cryptography algorithm • Arithmetic coding algorithm.	• Better PSNR value and embedding capacity (bits) • Computational complexity is less.	• Used single watermark image • System robustness can be improved.

COMPARATIVE ANALYSIS

Sl. No.	Title of the paper	Features	Advantages	Limitations & Future scope
7.	Medical JPEG image steganography based on preserving inter-block dependencies [7]	• Calculate the non-zero AC coefficient of each sub image • Calculate cost value matrix C by cost function	• Better anti-steganalysis performance • Better results than the previous J-UNIWARD process and JPEG image steganalysis	• Time complexity is high to obtain higher security performance
8.	Transreceiving of encrypted medical image – a cognitive Approach [8]	• DNA encoding by 1D Logistic System • DNA addition and DNA subtraction by MSB manipulation • PWLCM System scrambling.	• No statistical relation between neighboring pixels • High immunity to defend statistical attacks. • Performance is increased by DNA and the chaotic map • PSNR is infinity	• Complexity is very high.

COMPARATIVE ANALYSIS

Sl. No.	Title of the paper	Features	Advantages	Limitations & Future scope
9.	Robust Encryption of Quantum Medical Images [9]	• NEQR (Novel Enhanced Quantum Representation) • Quantum controlled NOT image • Key is generated by logistic sign map and generate quantum Key by NEQR. • XOR operation is used for final encryption	• PSNR is infinity • Robust against co-relation based attacks • Secure against entropy attacks • The watermark image is exposed only by the correct secret key	• High complexity for simulating on classical computer
10.	Efficient quantum information hiding for remote medical image sharing [10]	• Steganography • Controlled "NOT" gate • Arnold's cat map	• High PSNR values and capacity of embedding and excellent visibility. • Career image is not required for extraction of the secret image.	• High complexity for simulating on classical computer

OPEN ISSUES OF MEDICAL IMAGE SECURITY

After reviewing we feel that the following are the open issues where further investigation may be done:

- Most encryption algorithms do not consider the minimal distortion or slight peak variation of histograms in medical images.
- In the cloud platforms, execution time is a very important issue. So the algorithms having high time complexity may increase the latency and response time for the users. This will cause deterioration in the Quality of Experience (QoE) for the users.
- Nowadays, research in quantum information hiding is also very popular. But for performance analysis, a classical computer is required, where simulating quantum algorithms is time consuming and costly.
- Most of the proposed schemes reviewed do not consider the time complexity. We feel that reducing the time complexity of these schemes is important and might lead to real time secure medical image transmission.

CONCLUSION AND FUTURE SCOPE

- At the time of transmission, deterioration in the quality of the medical data or images may endanger the patients, therefore, we need to secure the medical images during transmission to ensure the accuracy of medical data.
- On the basis of the review, an attempt has been made to identify the open issues in this area. These open issues provide us the future directions in which research should be conducted for achieving secure transmission and thereby ensuring enhanced quality of treatment to the patients.

REFERENCES

1. Thakur, S., Singh, A.K., Ghrera, S.P. and Elhoseny, M., 2018. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia Tools and Applications*, pp.1-14.
2. Parah, S.A., Sheikh, J.A., Ahad, F. and Bhat, G.M., 2018. High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence* (pp. 409-437). Springer, Cham.
3. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N. and Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*, *6*, pp.20596-20608.
4. Usman, M.A. and Usman, M.R., 2018, January. Using image steganography for providing enhanced medical data security. In *Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual* (pp. 1-4). IEEE.
5. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A.K., Yang, P., Huang, H. and Hou, G., 2018. Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, *6*, pp.10269-10278.
6. Aparna, P. and Kishore, P.V.V., 2018. An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm. *Journal of Intelligent Systems*, *27*(1), pp.115-133.
7. Liao, X., Yin, J., Guo, S., Li, X. and Sangaiah, A.K., 2018. Medical JPEG image steganography based on preserving inter-block dependencies. *Computers & Electrical Engineering*, *67*, pp.320-329.
8. Praveenkumar, P., Devi, N.K., Ravichandran, D., Avila, J., Thenmozhi, K., Rayappan, J.B.B. and Amirtharajan, R., 2018. Transreceiving of encrypted medical image–a cognitive approach. *Multimedia Tools and Applications*, *77*(7), pp.8393-8418.
9. El-Latif, A.A.A., Abd-El-Atty, B. and Talha, M., 2018. Robust encryption of quantum medical images. *IEEE Access*, *6*, pp.1073-1081.
10. El-Latif, A.A.A., Abd-El-Atty, B., Hossain, M.S., Rahman, M.A., Alamri, A. and Gupta, B.B., 2018. Efficient quantum information hiding for remote medical image sharing. *IEEE Access*, *6*, pp.21075-21083.

THANK YOU