Grenze International Journal of Engineering and Technology, Jan Issue

A Review on Medical Image Encryption Techniques in Telemedicine Applications

Siyamol Chirakkarottu[1] and Dr. Sheena Mathew[2]
[1] Research Scholar, CUSAT
siyaaneeta@gmail.com
[2] Professor, CUSAT
sheenamathew@cusat.ac.in

***Abstract*—Telemedicine improves health care services in remote area by providing virtual communication between patients and medical practitioners. Most of the modern clinical diagnosis uses digital images to diagnose and examine diseases. Telemedicine requires transfer of medical images between doctors or medical experts. A patient's medical image may contain his personal information, hence it is to be kept secure. It is crucial to protect the medical images from a third person's access, during transmission. Image encryption is a convenient method to conserve the medical images. Researches are going on in the area of medical image encryption in telemedicine. This paper presents a survey on recently used image encryption techniques in telemedicine.**

***Index Terms*— telemedicine, image encryption, medical images, telesurgery, image security, cryptography.**

I. INTRODUCTION

Telemedicine involves transfer of medical information of patients from one location to another through electronic media to enhance his clinical health status. American telemedicine association (ATA) focuses on safe, effective and appropriate care for all the people whenever they need. It also promotes access to health care and health professionals through telemedicine. The most important aspect of telemedicine is the medical specialists can interact with and monitor the patients even though they are located in a remote place. Long distance health care services also can reduce the transportation cost and practical difficulty in the transportation of patient. We can also reduce the unnecessary non urgent clinical visit. Also telemedicine is an emerging area of medical education and clinical research.

There exist three types of telemedicine services.

i) Store and forward telemedicine: In store and forward telemedicine[1], also known as asynchronous telemedicine, a primary care physician can share the patient details such as images, videos or results of medical tests to a medical specialist. The technology requires secure transmission of patient details. The method is suitable for cases in which the doctor needs diagnosis from a specialist who is in another location. The specialist will reply the primary physician after evaluating the patient details.

Grenze ID: 01.GIJET.7.1.517

ii) Remote patient monitoring: Remote healthcare has many categories, all of which mean monitoring of patients outside hospital conditions by the means of technology[2]. RPM technology allows a medical practitioner to monitor the physiological data of patient such as blood pressure, sugar level, heart rate etc and consult the patient even from a distance.
iii) Real time telemedicine: The method also refers to live video consultation. Patients use live, two way communication systems such as video conferencing to hear and see the medical practitioner. The method is suitable for patients live in rural area, where medical help is not much available.

Although it may not be practical for the all clinical cases, telemedicine is widely used in medical areas such as infectious diseases, pain management, rheumatology, dermatology etc.

II. Medical Images In Telemedicine

Telemedicine services requires transfer of medical information along with medical images between patient and doctors. Medical information are to be transferred through wireless network in telemedicine services. Medical images are absolutely essential in the ongoing process of tracking the progress of many diseases. Medical imaging includes various radiological images such as CT (computed tomography), MRI (magnetic resonance imaging), ultra sound and X-ray images. In many of the diseases medical images aid the specialists to come in a better conclusion in treatment.

Telemedicine security includes problems such as authorization, authentication, integrity and accounting that are common with other information technology applications such as banking and manufacturing support[3]. Patient information security is very essential to develop a trust relationship between the health care services and the patients and thereby telemedicine services become popular. Preserving the privacy of medical data is not only an ethical but also a legal requirement[4]. HIPAA, Health Insurance Portability and Accountability Act [4], strictly instructs that a patient's medical information including images should be accessible to only the practitioners who professionally require it. Moreover, several major medical imaging communities such as American College of Radiology (ACR) and Society of Computer Applications in Radiology (SCAR) have issued guidelines and mandates for ensuring medical image security[4]. One of the feasible choice of methods to keep the images secure is encryption. Conventional encryption algorithms such as Triple-DES, AES and IDEA are not appropriate for images due to the large size and different storage formats. There exists many methods to overcome this challenge. Section III describes a review of the medical image encryption techniques used in recent telemedicine applications. Section IV gives a comparison of the methodology applied in various papers and conclusion is drawn in section V.

III. Encryption Of Medical Images – Literature Review

a) Chao based encryption for medical images: In the paper 'A Novel Medical Image Protection Scheme Using a 3-Dimensional Chaotic System'[4], Chong Ful and et.al proposed an encryption method using 3 dimensional Chen's chaotic map. The algorithm has two stages permutation and diffusion. Three dimensional Chen's chaotic map is applied in both permutation and diffusion phases. The method is proposed for teleradiology applications. The method is found to be suitable for CT, MRI and X-ray images. The patient as well as hospital details in the medical images in DICOM format, are advised to encrypt using AES and triple DES, where the proposed method is to encrypt the image in the file. The permutation performance is analyzed by comparing the permutation key of the method with that of different chaotic maps. Various performance and security analysis, key sensitivity and robustness of the method are tested and the results show that the method is well suited to real time telemedicine applications.
b) Cloud based chaotic encryption for medical images: Sefer kurnaz and Abdulrahman Ahmed jasim proposes a cloud based medical image encryption scheme in the paper 'cloud system for encryption and authentication medical images'[5]. The proposed method uses MATLAB to extract the medical image from the medical meta information in a DICOM file. The extracted image is stored as a PNG format image file. The method describes a confusion - diffusion model, in which one dimensional standard chaotic map is used as a random key stream generator. A steganography data is embedded on the image to generate stego encrypted image. The system uses well established and common methods to create a system which can authorize, authenticate and secure communications between Client and cloud and clinic, two main algorithm used in this system, chaos logistic map algorithm to encrypt medical images that extracted from DICOM file and least significant bit (LSB) for

steganography patient information inside encrypted image[6]. Quality of the method is analyzed by various metrics such as PSNR, NPCR, and SSIM.

c) Visual cryptography in telemedicine: Security of telemedicine services is a challenge because of the threats and limitations in infrastructure, sustainability, accountability and legal issues. In the paper 'Secure Authentication, Privacy and Integrity in Telemedicine using Visual Cryptography'[6], Arvind Bakshi, and Anoop Kumar Patel propose a method based on visual cryptography in telemedicine. It is a five step encryption process, in which the color image is converted in to gray scale image. Region of Interest (RONI) is obtained and it is marked. Digest algorithm[6] is applied to digest the ROI of the marked. The paper proposes an embed algorithm and share generation algorithm to embed the patient information such as patient ID, name etc and to create shares of RONI. The shares are overlapped in XOR fashion to get the encrypted image. The method is found to be suitable for medical images such as CT, MRI, X-ray etc. The results show that the explained method has a satisfactory MSE, RMSE, PSNR and SSIM.

d) Lossless encryption method using chaos and edge map: Yicong Zhou and et.al explains a lossless encryption method for medical images [7] in the paper 'A Lossless Encryption Method for Medical Images Using Edge Maps'. Author proposed an edgecrypt algorithm in which edge map of the images are obtained by any existing edge detector such as Canny, Sobel or Prewitt. Then image is split in to several binary bit planes. The edge map is encrypted by XOR operation between each pixel in the edge map and each element in a sequence generated by Logistic chaotic map. The pixels in the bit planes are shuffled and XOR operation is performed between each bit plane of the image and the encrypted edge map. The XORed bit planes are combined to form the encrypted image. MRI, CT and X-ray images are used as the test images. Sobel, Canny and Prewitt edge detectors are applied to generate the edge map for each type of test image. The method is compared with AES algorithm and from the test images it is stated that the proposed method takes very less time compared to AES encryption.

e) Medical image encryption using parallel chaotic key stream generator: A chaos based medical image encryption system is introduced in the paper 'An efficient medical image protection scheme with parallel chaotic stream generation[8]' by Wei Zhou and et.al in the year 2014. The authors proposes a permutation-diffusion architecture for medical image encryption. Arnold Cat map is applied in the permutation phase to generate the permutation key using which the image is shuffled. The diffusion phase is designed with two chaotic systems - Lorenz map and logistic chaotic map. The chaotic Logistic map is used as a parallel key stream generator which is used to encrypt the medical image. Execution time of the proposed method is compared with that of DES and the results show that the proposed algorithm 40% improvement in speed compared to traditional DES.

f) Image hiding algorithm for medical images: Yin Daia, Huanzhen Wang, Zixia Zhou and Ziyi Jin introduce an encryption method based on image hiding in the paper 'Research on medical image encryption in telemedicine system'[9] in the year 2016. The plain image is hidden in a carrier image by confusion, diffusion and information hiding. The algorithm sets a new starting point during confusion, which greatly expands the secret key space, adopts multiple iteration operations, and uses its own pixel values to execute XOR, which improves the average pixel value after diffusion[9]. The cipher image is loaded in to a carrier image to improve the security of the system. To differentiate between the cipher image and the carrier image, secondary wavelet decomposition is used. The method results in a reduced PSNR value for the test images used. Performance of the method is tested by nalyzing histograms and PSNR.

g) Encryption in EEG distribution in telemedicine: In the paper 'secure EEG distribution in telemedicine using encryption mechanism[10]', Ankita Varshney, Mukul Varshney and Jitendra Varshney describe two encryption algorithms. One is LFSR (linear feedback shift register) based security technique and other one is chaos based encryption technique. The LFSR, which is a shift register, is used as a pseudo random number generator. LFSR generates a gold sequence[11], which is the key for the encryption and decryption process. Using LFSR, two random number generators are created and the gold sequence is XORed with the second sequence. The obtained sequence is XORed with the transform EEG signal to get it encrypted. In chaos based encryption scheme, instead of LFSR, pseudo random sequences are generated by applying one dimensional quadratic chaotic map. Different initial parameters are used to generate different sequences. The results show that LFSR based encryption requires less time compared to chaotic encryption.

h) Secure telesurgery system: Yanjiang Yang and et.al proposed a method to encrypt medical images in telesurgery system in the paper 'Secure the Image-based Simulated Telesurgery System[12]' in the year 2003. In this work, the authors present an image-based simulated system for kyphoplasty surgery, categorized into telesurgery, an important kind of telemedicine service[12]. Kyphoplasty surgery is a treatment or surgical procedure for osteoporotic fractures. According to the authors, the medical images can be encrypted using any traditional symmetric encryption algorithm such as MD5 or SHA. To avoid unauthorized access and modification to the original image, image hashing functions[11] are applied to the ROI (region of interest). The work describes an application of medical image encryption in the field of telemedicine.

IV. COMPARISON

TABLE I shows the brief description of the recent medical image encryption methods used in telemedicine. From the literature review it is clear that medical image encryption in telemedicine is an emerging area, in which many research works going on. Here we can see most of the latest works are based on chaotic maps. Since chao is a non linear system and its strong dependency to its initial conditions, it is found to be suitable for image encryption.

TABLE I COMPARISON OF VARIOUS ENCRYPTION SCHEMES IN TELEMEDICINE

Sl no	Title	Methodology	Remarks
1	A Novel Medical Image Protection Scheme Using a 3-Dimensional Chaotic System[4]	A confusion – diffusion model applying three dimensional Chen map	Robust against brute force, known/chosen plain text attack, good NPCR, UACI, and minimum information entropy are obtained. Key space is 2^{149}
2	cloud system for encryption and authentication medical images[5]	A confusion _ diffusion model, applying 1D Logistic map, including steganography to generate stego encrypted image	Robustness against various attacks are not analyzed. Good NPCR, UACI, and PSNR are obtained.
3	Secure Authentication, Privacy and Integrity in Telemedicine using Visual Cryptography [6]	Visual cryptography based encryption.	Robustness against various attacks are not analysed. SSIM, MSE, and PSNR are analysed.
4	A Lossless Encryption Method for Medical Images Using Edge Maps[7]	Encryption uses edge map and one dimensional Logistic map	Encryption requires less time.
5	An efficient medical image protection scheme with parallel chaotic stream generation[8]	Arnold cat map in permutation phase and 1D logistic map in the diffusion phase.	Key space 2^{100}. Parallel chaotic system reduces time consumption in diffusion.
6	Research on medical image encryption in telemedicine system[9]	Image hiding system applying Logistic chaotic map.	Key space analysis is to be considered.
7	Secure EEG distribution in telemedicine using encryption mechanism [10]	Chaos and LFSR based encryption.	Increased speed, secure against unauthorized access.
8	Secure the Image-based Simulated Telesurgery System[11]	Medical image encryption by applying MD5 and SHA.	Security, integrity, authentication and access control of the system are analysed.

V. CONCLUSION

Telemedicine and cryptography is an emerging field which captures the attention of researchers all over the world. Since medical images are broadly used in telemedicine services, encryption is necessary to avoid unauthorized access and manipulation. The paper presents a review on various medical image encryption

techniques exist in telemedicine applications. The recent works show that researches are going on the area of encryption in remote medical consultation. The encryption scheme must be good enough to overcome unsanctioned access of personal information in medical images.

REFERENCES

[1] Dennis Bangert, Robert Doktor, 'Implementing store-and-forward telemedicine: organizational issues', Telemedicine journal and e-health: the official journal of the American Telemedicine Association, DOI:10.1089/153056200750040219 Corpus ID: 19169988

[2] Remote patient monitoring: a comprehensive study, Lakmini Malasinghe, Naeem Ramzan, Keshav Prasad Dahal, Journal of Ambient Intelligence and Humanized Computing, October 2017, DOI: 10.1007/s12652-017-0598-x

[3] Vaibhav Garg, M.S., and Jeffrey Brewer, M.S, 'Telemedicine Security: A Systematic Review', Journal of Diabetes Science and Technology, Volume 5, Issue 3, May 2011.

[4] Chong Fu1, Gao-yuan Zhang, Ou Bian, Wei-min Lei, Hong-feng Ma, 'A Novel Medical Image Protection Scheme Using a 3-Dimensional Chaotic System', PLoS ONE 9(12): e115773. doi:10.1371/journal.pone.0115773, PLOS ONE | DOI:10.1371/journal.pone.0115773 December 26, 2014.

[5] Sefer kurnaz, Abdulrahman Ahmed jasim, 'Cloud System For Encryption And Authentication Medical Images', IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. II (Jan.- Feb. 2018), PP 65-75.

[6] Arvind Bakshi, and Anoop Kumar Patel, 'Secure Authentication, Privacy and Integrity in Telemedicine using Visual Cryptography', International Journal of Advanced Science and TechnologyVol.117 (2018), pp.11-28.

[7] Yicong Zhou, Karen Panetta and Sos Agaian, 'A Lossless Encryption Method for Medical Images Using Edge Maps', 31st Annual International Conference of the IEEE EMBS, Minneapolis, Minnesota, USA, September 2-6, 2009.

[8] Wei Zhou, Wen-Qi Liu, Dong Liang Wang, Gui Xiang Zhu, Ying Jie Hu and Yong Feng Zhan, 'An efficient medical image protection scheme with parallel chaotic stream generation', Information technology journal 13(9), 1602-1611, 2014.

[9] Yin Daia, Huanzhen Wang, Zixia Zhou and Ziyi Jin, 'Research on medical image encryption in telemedicine system', Technology and Health Care 24 (2016) S435–S442 S435, DOI 10.3233/THC-161166.

[10] Ankita Varshney1, Mukul Varshney, Jitendra Varshney, 'secured EEG distribution in telemedicine using encryption mechanism', Matrix Academic International Online Journal of Engineering and Technology.

[11] Yanjiang Yang, Feng Bao, Robert Deng, 'Secure the Image-based Simulated Telesurgery System', ISCAS 2003: Proceedings of the IEEE International Symposium on Circuits and Systems, May 25-28, Bangkok, Thailand. 2, 596-599. Research Collection School Of Information Systems.