Medical Image Security - the State-of-the-Art

C. Devi Parameswari, K. Shankar

Abstract: In clinical diagnosis, the medical images act as a significant role and also in therapy, research and teaching and so on, Medical imaging is assumed as a biological imaging part, that had been build from 19th century. For each year, the medical image-based researches have increased at a standard rate of 3%-5%, the need for data-storage has hiked by 10%-25% majorly. To preserve the medical data of patient, the Health Insurance Portability and Accountability Act (HIPAA) needs insurance companies and medical providers to execute some policies and processes. The present standard based on numerous relative studies is done in this paper.

Keywords : Medical Image, Cloud, Security, Encryption.

I. INTRODUCTION

Imaging technology has assumed a critical job in the improvement of medicinal services area. Actually, examining medical pictures is a significant wellspring of important organic data [1]. Different diseases have been distinguished utilizing picture handling techniques and hence have given early stage identification and helped the doctors to fix the ailment. For instance, the need of quick and secure diagnosis is fundamental in the medical world [2]. These days, the transmission of visual information is an everyday schedule and it is important to locate an effective method to transmit them over systems. When imparting the medical pictures to persistent data we ought to give high security (Integrity, Authentication, Confidentiality) to the substance exhibits in the covering picture. To diminish inner security dangers, numerous solutions dependent on various techniques are proposed to advance cloud computing in social insurance space [3]. As needs be, medicinal services associations are roused to move to the cloud stockpiling to exploit this new worldview. Sadly, the usage of cloud stockpiling raises a few difficulties, including security and protection issues [4]. Medicinal services units may require a few tasks to be performed on the information put away in the cloud and they approach the cloud specialist organizations. Outsider access to those records can be permitted by scrambling the first message utilizing cryptographic algorithms [5]. Visual cryptography is an advanced cryptographic technique which is utilized to the mystery picture is shared safely and furthermore its data is kept up with most extreme

Confidentiality. A sender transmits the mystery picture which is partitioned into offers and it holds concealed data. At the point when these offers are adjusted and stacked together, they will in general uncover the mystery picture data to the collector. When the offers are made, it is encoded independently by scrambled algorithms [6]. In encryption, the plaintext is changed over into cipher text utilizing a mystery key. The picture can likewise be changed over to encoded structure utilizing the mystery key. The scrambled picture is then sent at unbound medium towards the goal. At accepting end, the encoded picture is decoded utilizing a similar key of sender side [7]. Aside from this, there are still an excessive number of territories which require further improvements like increasingly productive algorithms can be created which can expand the security level in the cloud computing. These challenging concerns motivated us to do research in the medial image security domain.

II. REVIEW OF LITERATURE

The security for the medical pictures has turned out to be very critical since the correspondence of specific patients data is transmitted over the open system. The security issue is increasing rapidly with developed tools for hacking the image data. Many types of research proposed solutions for the security issue but they were failed to get complete security over the insecure network. In medical domain an enormous measure of information is accessible yet individuals are not ready to separate the significant data about the variables that reason some infection. A difficult undertaking in the medical business is to give successful medicines to patients and to analyze the infection accurately. The pros and Cons of the researches are explained as underneath table:

III. PROBLEM IMPORTANCE

Deriving a medical classification with conventional techniques is a complex task, nowadays not much research has been done to address the complete task of medical data. Due to these, human services experts depend intensely on these advanced records to improve diagnosis and treatment of diseases. In current prescription, these records are viewed as the key parts in the clinical decision-making. Another noteworthy necessity of this picture classification technique is the low computational speed. Despite the fact that many computerized techniques are accessible, machine intelligence techniques are holding a noteworthy position as a result of its predominant presentation measures.

Medical Image Security-the state-of-the-Art

Despite the fact that it is promising, how to secure information protection and at the same time keep up the executives of the picture stays testing. Medical pictures might be scrambled to guarantee security and integrity. As known, the quality of numerous encryption algorithms lies in the encryption key and its length, which is a noteworthy plan issue. The encryption plan is said to be computationally secure on the off chance that it meets a few criteria. To conquer the difficulties of medical picture security the proposed model takes a decent solution.

Table- I: Review of Literature

Author name	Year	Method	Imaging modalities	Pros and Cons
Shankar K and Eswaran P [8]	2015	Visual cryptography AES algorithm	Leena and Baboon image	▪ High security to share data fast execution speed ▪ Minimized PSNR value is needed
Ming Yang et al. [9]	2010	Discrete Cosine Transform (DCT) The region of Interest (ROI) RSA encryption algorithm	Skull image	▪ In these techniques transmitted the patient information into two different files ▪ Securely protects patient information in scenarios such as electronic transmission and medical imaging research. ▪ Vulnerable to attacks by cropping
Marwan et al. [10]	2017	multi-cloud environment segmentation and watermarking mechanisms	Medical image	▪ High security and performance ▪ Increase in operating expenses
FouadKhelif et al. [11]	2018	Embedded Block Coding with Optimized Truncation algorithm, AES	Digital images	▪ Protects the image content in a more reliable way ▪ Higher data insertion capacity
Mbarek Marwan et al. [12]	2018	SVM, FCM	medical images	▪ Classify image pixels more efficiently ▪ Prevent the potential disclosure of confidential data ▪ Achieve fast and accurate results
Yufeng Wang et al. [13]	2018	Artificial intelligence	3D reconstruction based on medical imaging, 3D printing	▪ Uniqueness model ▪ Facial ID was deemed impractical in real life
Fatma E.-Z. A. Elgamal et al. [14]	2013	Spatial embedding techniques Cryptographic algorithm	Electronic Patients' Records	▪ Fast and require less processing time. ▪ Dynamic embedding algorithm to increase the visibility of the shared images.
NesrineKaaniche and MarylineLaurent [15]	2017	Cloud Service Provider cryptographic mechanism dual encryption scheme	Electronic Health Records, Virtual Machines	▪ Cryptography provides an interesting solution ▪ Does not offer complete solutions
Wei Pan et al. [16]	2015	medical image sharing partial-encryption watermarking	Medical Image	▪ Achieve a higher degree of security ▪ The solution becomes flexible and scalable
George C. Kagadis et al. [17]	2013	Cloud computing ICT encryption technique	medical imaging	▪ Improve manageability, accessibility, and storage availability
Suguna et al. [18]	2017	Elliptic Curve Cryptography algorithm AES-GCM	DICOM images	▪ Provides the confidentiality, authenticity, integrity (CIA) for both the header and the pixel data. ▪ Consumes less time for both encryption and decryption process.
Arunkumar et al. [19]	2018	Deep Belief network multiclass SVM classifier	Retinal image	▪ An efficient system for the classification of common characteristic datasets. ▪ The training time becomes slower due to the very large number of parameters.
Veeramuthu et al. [20]	2016	Multi-Level Discrete Wavelet Transform PNN-RBF training and classification method Fisher Discriminant Ratio (FDR)	Brain image	▪ Increase the classification accuracy in tumor functional brain images. ▪ The efficient method to diagnosis the tumor region in early stage itself ▪ The classification is not significantly affected by the randomized initialization of the weights of the neural network.
PhilomenaJees et al. [21]	2016	AES encryption algorithm	DICOM image	▪ Medical images are securely outsourced to cloud with a high degree of protection more effective ▪ AES makes the cryptanalysis difficult
Kirti Dhiman et al. [22]	2017	Visual Cryptography technique	True color images	▪ Increase the security and to avoid the suspicion ▪ Lossless in nature and are less complex.
Hsiang-Cheh et al. [23]	2016	visual secret sharing	Color images	▪ Better performance, ease of implementation. ▪ Ownership of progressively transmitted image can be assured

Kalaivani Pachaiyappan et al. [24]	2014	Visual cryptography (Visual Secret Sharing)	Binary secret images	▪ Quality of the image is perfect. ▪ Without any loss of generality.
Elavarasi et al. [25]	2017	Color Visual Secret Sharing	Digital medical image	▪ Provide satisfactory security level. ▪ Proves the security, effectiveness, and robustness ▪ Difficult to decipher the secret image
K.Shankar and Eswaran [26]	2015	Visual Secret Share (VSS) Creation Scheme Elliptic Curve Cryptography GWO algorithm	Secret image	▪ The original image is shared securely and its information is maintained with confidentiality. ▪ High mean square error value.
K. Shankar and P. Eswaran [27]	2016	Elliptic curve cryptography Cuckoo Search (CS) algorithm	Secret image	▪ Optimal PSNR value ▪ Low performance
K. Shankar and P. Eswaran [6]	2015	Elliptic curve cryptography	Secret image	▪ Effective encryption and decryption ▪ MSE needs to be improved ▪ Low performance of low peak signal to noise ratio
K. Shankar and P. Eswaran [28]	2018	Homomorphic Encryption (HE) Ant Lion Optimization (ALO)	Digital image	▪ Great strength ▪ Fitness function as max entropy the best-encrypted image is characterized
XuehuYan et al.[29]	2019	Visual Cryptography Scheme (VCS)	Digital image	▪ Its has no pixel expansion and codebook design, which is therefore studied as well. ▪ Security Levels corresponding to typical VSS schemes are theoretically analyzed and classified
Xi Yang et al. [30]	2019	Convolutional neural network	Terahertz (THz) security screening cameras (TSSCs)	▪ The accuracy was promoted because of the decrease in false positives, and the efficiency was improved because of the reduction of the computation domain.

IV. EXISTING SOLUTION

Consequently, the difficulties of medical image examination model development come from the complexity of image data, the information captured by medical imaging modalities not usually clear and complete. This issue is because of absence of imaging process and technology which create incompetent resolution and artifacts. A common issue in medical imaging examination is validating data. Measurements by human are not accurate absolutely. The technique of medical imaging needs a actual fact standard to verify their result.

V. CONCLUSION

The major purpose of this research is to model a secure structure for securing patients' information. This can be achieved by reducing the disadvantages created by the existing solutions and by providing new techniques which incorporate some of the existing solutions. The main focus of the study is improving the security of medical images by using various optimization algorithms in the way of several steps. The proposed model assumes that encryption using new method can be done effective than other methods with the very small delay but it attains strong security of images and no illegal activities will acquire. The results will show that the proposed sharing scheme gives the image confidentiality, integrity, and reliability. Performance analysis proves the security, effectiveness, and robustness of the proposed algorithm. The proposed solution can be increased the accuracy rate compared to the existing solution. This paper helps the research activity in the domain of medical image processing and security processes. .

REFERENCES

1. Mohamed Elhoseny, K.Shankar, "Optimal Bilateral Filter and Convolutional Neural Network based Denoising Method of Medical Image Measurements", Measurement, Volume 143, Pages 125-135, September 2019.
2. K. Shankar, Mohamed Elhoseny, E. Dhiravida chelvi, SK. Lakshmanaprabu, Wanqing Wu, "An Efficient Optimal Key Based Chaos Function for Medical Image Security", IEEE Access, Vol.6, Issue.1, page(s): 77145-77154, December 2018.
3. Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things", Neural
4. Computing and Applications - Springer, October 2018. (Impact Factor: 4.213) DOI: https://doi.org/10.1007/s00521-018-3801-x
5. K. Karthikeyan, R. Sunder, K. Shankar, S. K. Lakshmanaprabu, V. Vijayakumar, Mohamed Elhoseny, Gunasekaran Manogaran, "Energy consumption analysis of Virtual Machine migration in cloud using hybrid swarm optimization (ABC–BA)", The Journal of Supercomputing - Springer, September 2018.
6. K. Shankar, Mohamed Elhoseny, R. Satheesh Kumar, S. K. Lakshmanaprabu, Xiaohui Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique", Journal of Ambient Intelligence and Humanized Computing, December 2018. (Impact Factor: 1.423) https://doi.org/10.1007/s12652-018-1161-0
7. Shankar, K., and P. Eswaran. "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography." China Communications 14, no. 2 2017): 118-130.
8. K. Shankar, SK. Lakshmanaprabu, Deepak Gupta, Ashish Khanna, Victor Hugo C. de Albuquerque, "Adaptive Optimal Multi Key Based Encryption for Digital Image Security", Concurrency and Computation: Practice and Experience, December 2018. (Impact Factor: 1.133). DOI: https://doi.org/10.1002/cpe.5122
9. Shankar, K., and P. Eswaran. "Sharing a secret image with encapsulated shares in visual cryptography." Procedia Computer Science 70 (2015): 462-468.
10. Yang, Ming, Monica Trifas, Lei Chen, Lei Song, D. B. Aires, and JaleesaElston. "Secure patient information and privacy in medical imaging." J. Syst. Cybern. Inf 8, no. 3 (2010): 63-66.
11. Marwan, M., A. Kartit, and H. Ouahmane. "Design a Secure Framework for Cloud-Based Medical Image Storage." In Proceedings of the 2nd International Conference on Big Data, Cloud and Applications, (2017), pp. 1-6.

12. Khelifi, Fouad, TaharBrahimi, Jungong Han, and Xuelong Li. "Secure and privacy-preserving data sharing in the cloud based on lossless image coding." Signal Processing, Vol.148 (2018): pp.91-101.

13. Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security Enhancement in Healthcare Cloud using Machine Learning." Procedia Computer Science, Vol.127 (2018): pp.388-397.

14. Wang, Yufeng, Liwei Wang, and Chang-aoXue. "Medical information security in the era of artificial intelligence." Medical hypotheses, pp.115 (2018): pp.58-60.

15. Fatma, E-ZA Elgamal, Noha A. Hikal, and F. E. Z. Abou-Chadi. "Secure medical images sharing over cloud computing environment." IJACSA) International Journal of Advanced Computer Science and Applications, Vol.4, no. 5 (2013).

16. Kaaniche, Nesrine, and Maryline Laurent. "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms." Computer Communications, Vol.111 (2017): pp.120-141.

17. Pan, Wei, GouenouCoatrieux, DalelBouslimi, and Nicolas Prigent. "Secure public cloud platform for medical images sharing." In MIE, pp. 251-255. 2015.

17. Kagadis, George C., Christos Kloukinas, Kevin Moore, Jim Philbin, Panagiotis Papadimitroulas, Christos Alexakos, Paul G. Nagy, DimitrisVisvikis, and William R. Hendee. "Cloud computing in medical imaging." Medical physics 40, no. 7 (2013).

18. Suguna, D., and G. Vallathan. "Security Analysis of Medical Images Transmission over Wireless Network." Asian Journal of Applied Science and Technology (AJAST) 1, no. 3 (2017): 301-303.

19. Arunkumar, R., and NagarajBalakrishnan. "Medical Image Classification for Disease Diagnosis by DBN Methods." Pak. J. Biotechnol, Vol. 15, No. 1 (2018): 107-110.

20. Veeramuthu, A., S. Meenakshi, and V. PriyaDarsini. "Brain image classification using learning machine approach and brain structure analysis." Procedia Computer Science 50 (2015): 388-394.

21. Jees, Philomina, and T. Diya. "Medical Image Protection in Cloud System." matrix, Vol.2 (2016): pp.3.

22. Dhiman, Kirti, and Singara Singh Kasana. "Extended visual cryptography techniques for true color images." Computers & Electrical Engineering (2017).

23. Huang, Hsiang-Cheh, Yuh-Yih Lu, and Jiun Lin. "Ownership protection for progressive image transmission with reversible data hiding and visual secret sharing." Optik-International Journal for Light and Electron Optics 127, no. 15 (2016): 5950-5960.

24. Pachiappan, K. A. L. A. I. V. A. N. I., S. Annaji, and N. I. T. H. Y. A. Jayakumar. "Security in medical images using enhanced visual secret sharing scheme." Int j sciengtechnol res 3, no. 9 (2014): 1642-1645.

25. Elavarasi, G., and M. Vanitha. "A Novel Method for Securing Medical Image Using Visual Secret Sharing Scheme.", 2017.

26. Shankar, K. and Eswaran, P., 2015. A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique. Australian Journal of Basic & Applied Science, 9(36), pp.150-163.

27. Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique." Journal of Circuits, Systems and Computers 25, no. 11 (2016): 1650138.

28. Shankar, K., and S. K. Lakshmanaprabu. "Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm." International Journal of Engineering & Technology 7, no. 1.9 (2018): 22-27.

29. Yan, X., Liu, L., Lu, Y. and Gong, Q., 2019. Security analysis and classification of image secret sharing. Journal of Information Security and Applications, 47, pp.208-216.

30. Yang, X., Wu, T., Zhang, L., Yang, D., Wang, N., Song, B. and Gao, X., 2019. CNN with spatio-temporal information for fast suspicious object detection and recognition in THz security images. Signal Processing, 160, pp.202-214.

AUTHORS PROFILE

Dr. K. Shankar. received the M.C.A., M.Phil., and Ph.D. degrees in computer science from Alagappa University, Karaikudi, India. He is currently Post Doc Fellow in the Alagappa University, Karaikudi, India. He has several years of experience in research, academia, and teaching. Collectively, Dr. K. Shankar authored/co-authored over 38 ISI Journal articles (with total Impact Factor 99.636) and 107 Scopus Indexed Articles. Dr. K. Shankar guest-edited several special issues at many journals published by Inderscience and MDPI. He has been a part of various seminars, paper presentations, research paper reviews, and conferences as a convener and a session chair, a guest editor in journals. He has authored or co-authored many research papers in reputed journals and conferences. He serves as the reviewer in some SCI indexed Journals like IEEE, Elsevier, Springer and the IEEE conferences. He displayed vast success in continuously acquiring new knowledge and applying innovative pedagogies and has always aimed to be an effective educator and have a global outlook. His current research interests include Secret Image Sharing Scheme, Digital Image Security, Cryptography, Internet of Things, Healthcare applications and Optimization algorithms**.**

C.Devi Parameswari received her B.Sc and M.Sc (Computer Science) from Madurai Kamaraj University in 2013 and 2018 respectively. Now, she is a Research Scholar in the Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India. Her current research areas include cryptography, secret image sharing scheme, Image security.