ISSN 2278-3091

Volume 10, No.2, March - April 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse161022021.pdf

https://doi.org/10.30534/ijatcse/2021/161022021

High Capacitive Secure Image Transmission Over Wireless Channels

Aparna.G[1], Dr. Kezia Joseph[2],Dr.G.Sumana[3],G. Anitha Mary[4]

[1]Research Scholar, ECE, OSMANIA UNIVERSITY, TS, India

[2] Department of ECE, Stanley Engineering College for Women, TS, India

[3]Programmer, Command Control Center, Sri Padmavati Mahila Visvavidyalayam Tirupati, India

[4]HOD, M.Sc. Data Science, Loyola Academy, Old Alwal, Secunderabad, Telangana, India

ABSTRACT

Expansion of internet connectivity and its usage globally has increased various demands of providing security for the data transmission. Telemedicine is a modern way of medical care that can be extended to any remote place across the globe. This medical care practice is a result of the deployment of communication systems and information technology into healthcare system. With this technology the diagnosed data can be shared with physician and take his consultation remarks and also physicians can access to diagnostic archive and share for medical practice and learning. However, this exchange of information is confined with several risks of data theft when they are shared in open networks and hence they are to be protected with high security algorithms. This paper provides a high capacitive security algorithm for protecting the images with hidden confidential information. The approach provides a two-way security by encrypting the clinical information initially and embedding it imperceptibly in the concerned image so that the user on other can obtain both the visual and text data at same instance.

Key words: Image transmission, Data Encryption, Data Hiding, High Capacity

1. INTRODUCTION

With the availability of high speed internet services telemedicine usage has increased and spread to many of the remote areas in the world. The telemedicine is a modern medical practice integrating information technology and communication systems. Several benefits are attained with this system like remote diagnosis, access of previous data from archive for physicians and remote distance learning [1]. However, this data transmission is often concomitant with risks when shared in open hence there is a scope to develop algorithms and approaches that secure this data [2].With the increase in the demand for secure transmission of medical data has paved a way for many international organizations to establish several special standards that intend to provide solutions to data security issues for instance, the DICOM (Digital imaging and communication in medicine) format for medical images [3].These standards provide guidelines for healthcare professionals to achieve integrity (detect tampering or alterations), confidentiality (prevent illegal access) and authenticity (verify ownership) for telemedicine services [4]. This goal is achieved with some data encryption standards and data hiding mechanisms.

Data encryption alias cryptography is the process of encoding the message such that the intruders may not able to analyze the data and can be accessed only to the authorized person. In literature there are two popular algorithms which are used for data encryption like AES (Advanced Encryption Standard) and RSA (Rivest Shamir Adleman) algorithm [5]. In AES standard the same key is used on either side of communication systems, in this standard the message block size is fixed to 128,192,256 bits; for longer messages it is divided into several these bit blocks. When the key is longer it consumes longer time to encrypt and decrypt the message however in applications like telemedicine where the clinical information is limited to several lines of text this can be treated as one of the best solution to encrypt [6], so in this paper this standard is deployed to encrypt the clinical and personal information of the patient.

Early research of hiding data into another digital data has started with steganography methods that referred as art of science that aims to hide the information within a digital data, this data may be a text, image and audio. In this work the clinical and patient's personal information is to be hided in medical image. The advantage of the steganography technique is that the message is hidden and imperceptible and this makes it not only preventing intruders from knowing the hidden information but also removes the suspicion of having hidden information. There are two aspects associated with steganography method, first is capacity and second is imperceptibility. Both the aspects inversely proportional to each other wherein the increase in the hidden data or capacity removes the property of imperceptibility so there is still demand for the method that can provide a solution for high capacity with imperceptibility [7].

2. RELATED WORKS

There are several approaches available in literature, few methods which are closely related to the current work were discussed in this section.In [2] Saheb and others have presented a paper discussing about various methods that were deployed in literature for solving the network security issues. These security requirements include authentication, Integrity and confidentiality. It also focused on discussing multiple attacks that are prevalent and their behavioral analysis is considered to treat them on threat level basis. According to this analysis, three level of threats are noticed; low-level, medium level and high or extremely high level of threats and also suggested some of the solutions to encounter these threats.

In [8] Anwar et.al have developed a technique for transmitting medical images. They have aimed to maintain the integrity of the medical information ensuring the information is only accessible to a limited number of people. At first the medical information is encrypted with AES algorithm and an ear print was created by considering the seven unique features from the ear image. The proposed approach aimed to send this information on internet and improved the security of the medical image from being accessed by unauthorized persons.

In [9], Jain and others proposed an approach for transferring the medical information by hiding it in a cover medical image which is performed using decision tree method. The coding is performed for multiple block which are evenly distributed and the secret code blocks are assigned to the cover image to insert the data using breadth first search algorithm. In this work, the medical information is encrypted using RSA algorithm before hiding it into a cover image.

In [10] Yehia et.al have surveyed healthcare applications which are based on Wireless Sensor Networks that aims to be deployed over IoT (Internet of Things) Environment. In this work, they have also discussed about the techniques that were used for handling the security issues that are pertained to health care system.

In [11], Sajjad et.al proposed a mobile cloud assisted framework for transmitting the stego-images for selective encryption.In this work the visual saliency detection model has been used for detecting the region of interest from the medical image. For embedding the information, a directed edge method is used. In another work Parah and others in [12] have proposed a high capacitive scheme for secure transmitting electronic patient record which is hidden in medical color images for IoT based health care system. Two Pseudo-random sequences like main address vector (MAV) abd Complementary Address vector (CAV) are used to address the pixel locations for embedding the data. In this approach LSB way of embedding is performed to hide the EPR data into RGB planes of the image.

In [13], Nabi et.al, proposed a crypto based watermarking approach based on AES algorithm and reversible data hiding scheme to secure the medical image. The results attained with this approach proved that the proposed approach achieves both the authenticity and integrity of the image either in both of the spatial and encrypted domains.

In [18] J.Nayak and others , proposed a compact method for storage and transmission of medical images containing the patient details. In this work, the patient information is hided in medical images and are transmitted through noisy environment in which the text data is encrypted with RSA algorithm. This approach also used cover signal like EEG and ECG which encoded with DPCM method. Forward error codes like reed Solomon is employed which has shown significant improvement in achieving low bit error rate under noisy channels.

3. PROPOSED APPROACH

Figure 1 shows the proposed approach of medical image transmission. The approach is supposed to be secure and high capacitive of hiding patient details in their respective diagnosed medical image. At first stage, the patient information details are encrypted with standard AES algorithm which is 128-bit encryption. The example of the encryption is shown in the below table 1.

In the second stage of the approach the clinical information is hidden using Integer wavelet transform and LSB transformation. The embedding algorithm is formulated as shown in algorithm:

Embedding Algorithm:

- Initially the concept of histogram modification is employed to prevent the problem of overflow and underflow that usually occurs when the pixel value changes with integer wavelet transform [14] to produce stego-image.

Table 1: Original Data and Encrypted Data

Original Data	Encrypted Data
2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy	x »(æ!* ¥ÉLöt¿#"ÊT^ Øñv¤éó ~¢zJÔ ¯Ø ¸ã*T² ôì»> 9ëÂ8j ÎV¿NôË]|è & +:&øí

- Divide the image into NxN non overlapping blocks and transform each block into Low and High frequency components with Integer wavelet transform.
- Calculate the hiding capacity of each coefficient with the following equation (1) where the term” L” represents the length of the data bits that can be hided

$$L = \begin{cases} k + 3, & if\ C \geq 2^{k+3} \\ k + 2, & if\ 2^{k+2} \leq C < 2^{k+3} \\ k + 1, & if\ 2^{k+1} \leq C < 2^{k+2} \\ k, & if\ C < 2^{k+1} \end{cases} \tag{1}$$

In the above equation (1) the term ‘k’ is minimum number of bits that can be embedded,’C’ is the absolute value of wavelet coefficient.

- In this analysis ‘LL’ sub band is used for hiding the data. Based on the idea provided in [15], in this the concept of optimum pixel adjustment is adopted. In this work, the original coefficient value in LL sub band is modified with the key (Eg: key=2) and the data is hided based on the different of the original and modified sub band block.

$$di(x,y) = p'(x,y) - p(x,y) \qquad (2)$$

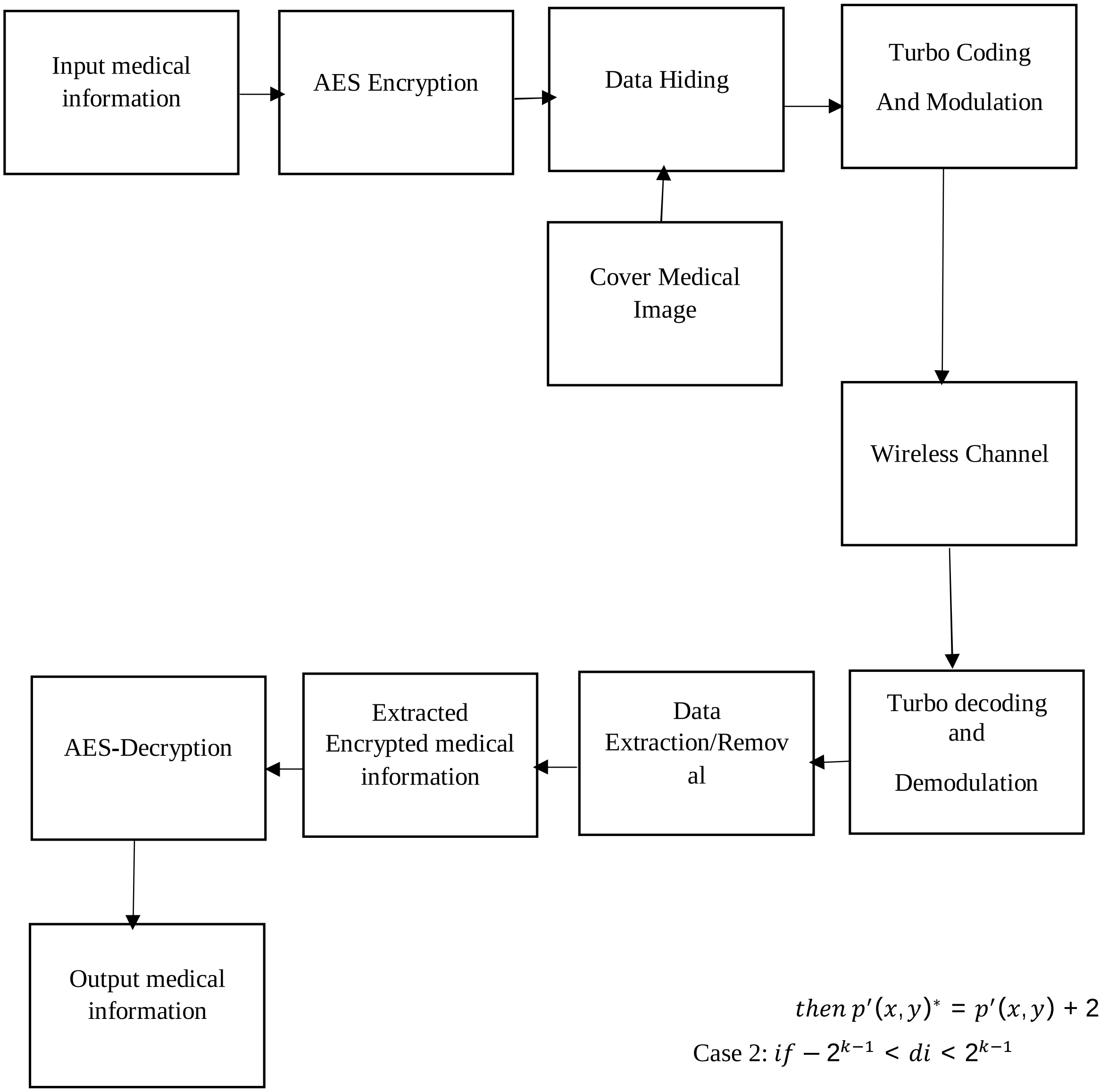

Input medical information
AES Encryption
Data Hiding
Turbo Coding And Modulation
Cover Medical Image
Wireless Channel
Turbo decoding and Demodulation
Data Extraction/Removal
Extracted Encrypted medical information
AES-Decryption
Output medical information

Figure 1: Proposed approach block diagram of encryption of medical image

In the above equation the term ‘d’ is the difference p, p’ are original and modified sub band block elements.

- The data is embedded based on these three cases of modification

Case 1: $if -2^k < di < -2^{k-1} \,\&\, if\; p'(x,y) < 256 - 2^k$

$$then\; p'(x,y)^* = p'(x,y) + 2^k$$

Case 2: $if -2^{k-1} < di < 2^{k-1}$

$$then\; p'(x,y)^* = p'(x,y)$$

Case 3: $if\; 2^{k-1} < di < 2^k \,\&\, if\; if\; p'(x,y) \geq 2^k$

$$then\; p'(x,y)^* = p'(x,y) - 2^k$$

The output of the embedding algorithm is a stego image where the important clinical information is imperceptible to human eye. This stego- image is encoded with turbo encoding which is followed with 16-Qam modulation before passing it through AWGN channel.

4. EXPERIMENTAL RESULTS

The experiments were conducted on different medical images like MR brain image, CT abdominal image and Lung X-ray image. The proposed approach is compared against the method proposed by Elhoseny and others in [17].

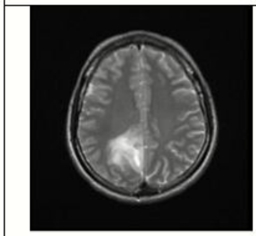
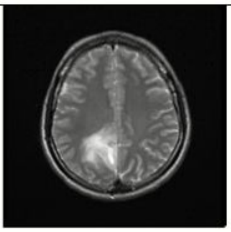
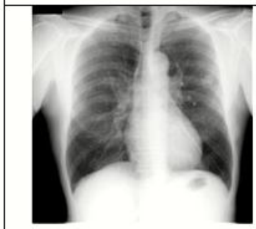
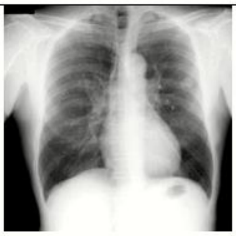
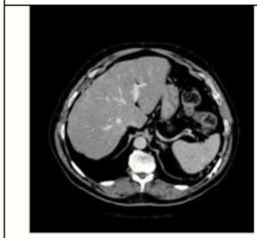
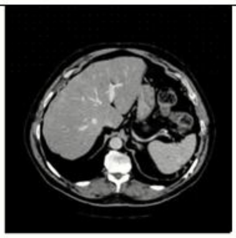
Image	Stego-Image	PSNR
		49.03
		48.46
		47.44

Figure 2: Stego- images with their respective PSNR values for different types of medical images

From the graphs and table, it can be observed that the proposed approach is able to yield high quality stego image with high capacity which is depicted in figure 2. Figure 3 depicts the BER performance different medical images when passed through AWGN channel achieves very low BER it is further reduced when turbo coding is incorporated with the model. The hiding capacity of the proposed approach is compared against the method proposed by Elhoseny in [17] and observed that the proposed approach attains high quality imperceptible images which is approximately 1.9dB improved on average.

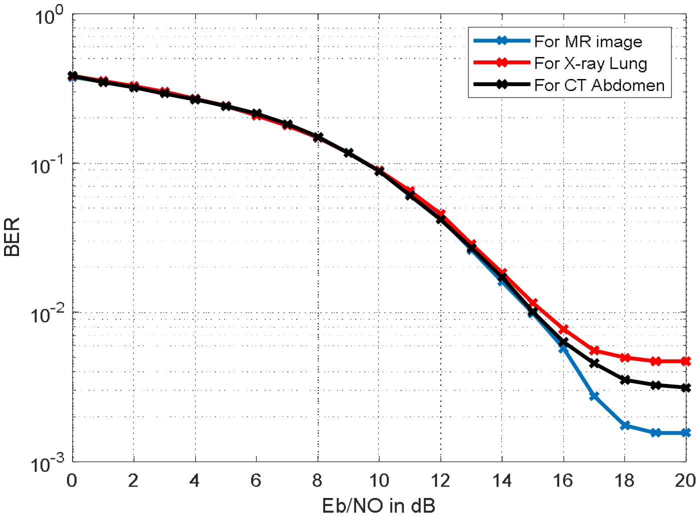


Figure 3: BER Performance of multiple medical images with varying Eb/NO under AWGN channel

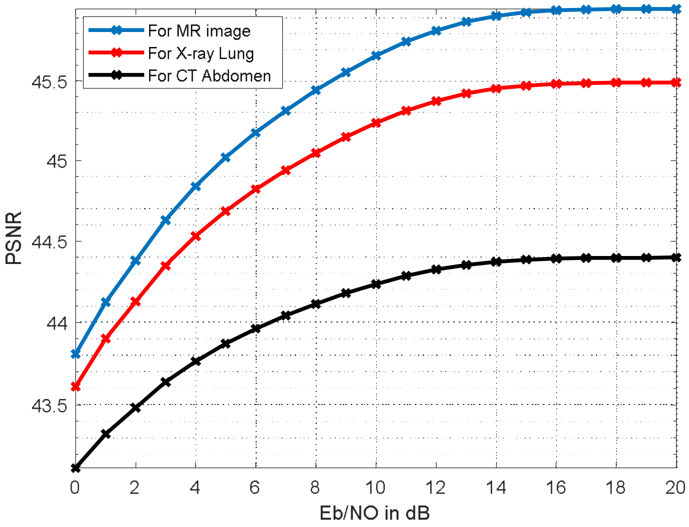


Figure 4: PSNR Performance of multiple medical images with varying Eb/NO under AWGN channel.

This remarks the objective of the current of achieving high capacity, secure and imperceptible medical image transmission model. In figure 4, PSNR analysis was conducted for different medical images in which the MRI imaging has attained higher perceptibility with PSNR of 45.8 dB.

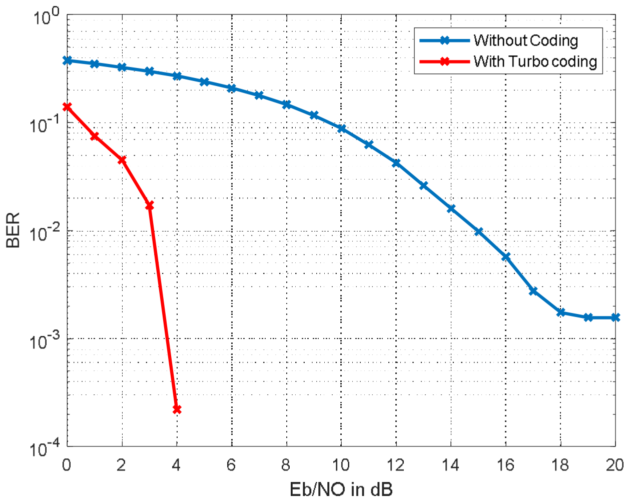


Figure 5: BER Performance of MR medical image with varying Eb/NO under AWGN channel with and with turbo coding

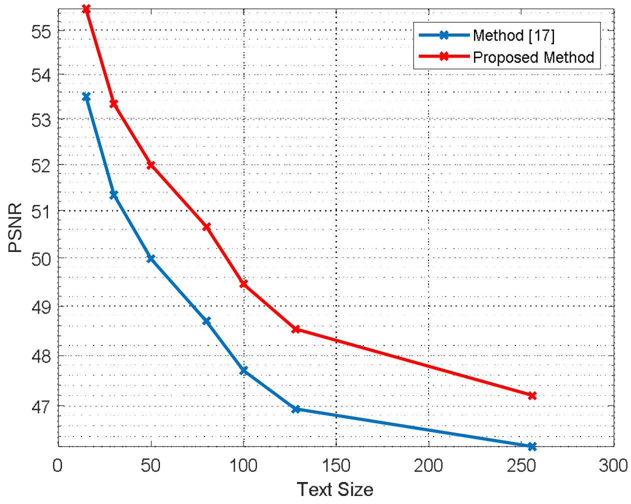
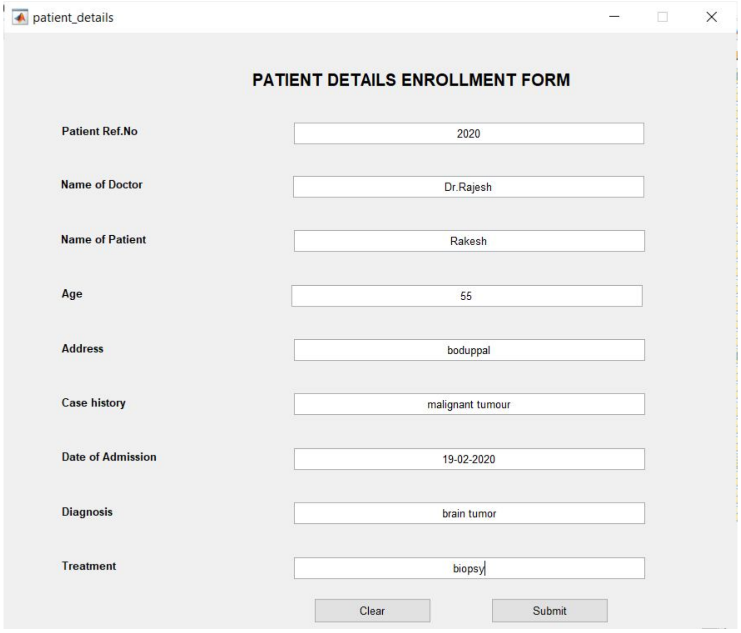


Figure 6: PSNR Performance of MR medical image with varying Text Size and comparison with method proposed in [17].

Table 2: Capacity analysis of the proposed approach

Method/ Text Size	15	30	50	80	100	128	256
Elhoseny [17]	53.5	51.2	49.3	48.4	47.5	47.1	46.2
Proposed	55.5	53.2	51.3	50.4	49.5	48.9	47.2

Figure 5 depicts the effect of turbo coding for data transmission under bursty channel. It can be observed from the graph that BER is decreased by 0.328 units when compared with the transmission without turbo coding. So it is recommended from the analysis that transmission clinical information is more accurate if it is encoded with turbo coding. Figure 6 and table 2 depicts the PSNR performance for the proposed approach to validate the property of high capacity. It can be observed from the reading that even at higher dimensions of clinical data the quality of the host image is preserved with the proposed method indicating a high capacity nature when compared with earlier method.



PATIENT DETAILS ENROLLMENT FORM

Patient Ref.No	2020
Name of Doctor	Dr.Rajesh
Name of Patient	Rakesh
Age	55
Address	boduppal
Case history	malignant tumour
Date of Admission	19-02-2020
Diagnosis	brain tumor
Treatment	biopsy

Figure 7: Entry form of Patient Clinical Information

Table 3: Clinical patient diagnostic details encryption and decryption output

Original Information	Encrypted Information	Decrypted Information
2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy	x »(æ!* ¥ÉLöt¿#"ÊT^ Øñv¤éó ~¢zJÔ ¯Ø ¸ã*T² ôì»> 9ëÂ8j ÎV¿NôË]|è & +:&øí	2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy

5.CONCLUSION

The paper proposes a secure high capacity medical image transmission model that attains high quality imperceptible stego-images which are transmitted through AWGN channel. In this work, the BER analysis was considered with and without Turbo coding and found that with coding mechanism included the BER is very low and suitable for real time application. The work mainly tries to propose a high capacitive and imperceptible mode of medical image transmission which is achieved when compared with earlier method. This work may be extended by employing customized deep networks for hiding the data in the medical images.

REFERENCES

[1] Craig, J., Patterson, V.: ‘Introduction to the practice of telemedicine’, J. Telemed. Telecare, 2005, 11, pp. 3–9

[2] A. Shehab et al., “Secure and robust fragile watermarking scheme for medical images," IEEE Access, vol. 6, pp. 10269-10278, 2018.

[3] Digital imaging and communications in medicine (DICOM) standard, DICOM’, 2006. Available at http://medical.nema.org/dicom/2006

[4] Digital imaging and communications in medicine (DICOM), part 15: security profiles ed.’, National Electrical Manufacturers Association (NEMA), 2001, PS3.15–2001

[5] S. F. Mare, M. Vladutiu, and L. Prodan, “Secret data communication system using steganography,AES and RSA," in Proc. IEEE 17th Int. Symp. Design Technol. Electron. Packag. (SIITME), Oct. 2011, pp. 339-344.

[6] S. F. Mjolsnes, Ed., A Multidisciplinary Introduction to Information Security. Boca Raton, FL, USA: CRC Press, 2011.

[7] M. S. Sreekutty and P. S. Baiju, ``Security enhancement in image steganography for medical integrity verification system," in Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT), Apr. 2017, pp. 1-5.

[8] A. S. Anwar, K. K. A. Ghany, and H. El Mahdy, ``Improving the security of images transmission," Int. J. Bio-Med. Inform. e-Health, vol. 3, no. 4, pp. 7-13, 2015.

[9] M. Jain, R. C. Choudhary, and A.Kumar, ``Secure medical image steganography with RSA cryptography using decision tree," in Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I), Dec. 2016, pp. 291-295

[10] L. Yehia, A. Khedr, and A. Darwish, ``Hybrid security techniques for Internet of Things healthcare applications," Adv. Internet Things, vol. 5, pp. 21-25, Jul. 2015

[11] M. Sajjad et al., ``Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," Multimedia Tools Appl., vol. 76, no. 3, pp. 3519-3536, 2017.

[12] S. A. Parah, J. A. Sheikh, F. Ahad, and G. M. Bhat, ``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. Cham, Switzerland: Springer, 2018, pp. 409-437

[13] H. Abdel-Nabi and A. Al-Haj, ``Efficient joint encryption and data hiding algorithm for medical images security," in Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS), Apr. 2017, pp. 147-152.

[14] Ahmad Shaik, V. Thanikaiselvan, Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification, Journal of King Saud University - Computer and Information Sciences, 2018

[15] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in changes Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[16] C. Y. Liu and S. Lin, "Turbo encoding and decoding of Reed-Solomon codes through binary decomposition and self-concatenation," in IEEE Transactions on Communications, vol. 52, no. 9, pp. 1484-1493, Sept. 2004

[17] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018

[18] Nayak, Jagadish & Bhat, P. & Kumar, M. & Acharya, U Rajendra. (2005). Reliable and robust transmission and storage of medical images with patient information. 91-95.