Secure Medical Data Transmission Model by using Steganography Technique

K.Srinivasa Rao[1], Marada Kalyani[2], Putti Pooja Yasaswini[3], Velpula Kousalya[4]
[1]Assistant Professor, [2,3,4]B.Tech Students
Department of ECE, Andhra Loyola Institute of Engineering and Technology,Vijayawada,A.P.,India.

Abstract **-** Over the years, owing to the internet, downloading data from world wide web is now at tips. Eventually, data copying, theft and backup of digital content is not a big deal in the world of multimedia.Therefore, authentication of data, copyright and ownership of the content is diminishing.So, security of digital data is the basic requirement in today's digital world.A lot of concerns have been brought up in maintaining the security for the information transmitted or put away over open channels particularly at the level of text and picture information. The novel method start by encrypting the secret medical data by using hybrid encryption scheme, built by using a combination of Rivest, Shamir and Adlemann(RSA) and Advanced Encryption Standard(AES) and then hide the results in a cover image by using Integer Wavelet Transform(IWT) technique and later on receiver will decrypt the data.So,no one apart from authorized sender and receiver will be aware of the secret data that is being existed.The performance of the proposed system was evaluated based on the statistical parameters such as peak signal-to-noise ratio (PSNR) and Mean square error (MSE).Compared to the state-of-art methods, the proposed model proved its ability to hide confidential patients health data in an image.

Keywords **-** *AES, IWT, Mean square error, RSA, Steganography, Peak Signal to Noise Ratio.*

I. INTRODUCTION

Innovation of technology and fast internet make information to distribute all over the world very easily and economically [1]. With the rapid development, in use of data communication in the mobile networks and in the internet realized the need of secure data transfer, which in turn present the new challenges for protecting the information from the unauthorized access[2].So the art of hiding data have an importance due to the ever increasing need of prevention methods against illegal copyright, tampering, optimal use of available bandwidth for data transmission and reception,authentication etc.,.Data hiding has been used for the purpose of concealing information and communication from one place to another. While sending or storaging a data, it may be under threat because any unauthorized user can access it, modify it, so there is need to provide security for the data.A data is secure, if it fulfills conditions such as Availability, Accuracy, Authenticity, Confidentiality, Integrity [3]. Steganography is derived from the greek origin means "concealed writing" where "stegano" means "secret or hidden", and "graphy" means "writing". Steganography is a method of hiding secret messages into an cover media known as stegogramme such that an unintended observer will not be aware of existence of the hidden messages [4][5]. Therefore, it is necessary to develop an efficient model to ensure the security and integrity of medical data transmitted and received.

This paper aims to improve the security for the medical data based on the integration between hybrid encryption scheme and steganography technique.

This paper is organized into Seven sections including this section.Section 2 illustrates the related works, Section 3 explains the proposed model, Section 4 explains the proposed model algorithms ,Section 5 provides the evaluation parameters, Section 6 provides results and Section 7 summarizes the main conclusions.

II. RELATED WORKS

M.Elhoseny et al.[6],developed a secure medical data transmission model for IoT –based healthcare systems and able to hide the confidential patient's data into a transmitted cover image by integrating DWT technique with a proposed hybrid(RSA and AES) encryption scheme.

Jain et al. [7], proposed a technique for transferring patient's information into the medical cover image by hiding the data using decision tree concept. Insert the data by the mapping mechanism based on breadth-first search.RSA algorithm was used to encipher the data before embedding.

Prerna and Girish [8],made a comparative study of there digital image watermarking techniques(DWT,DWT-SVD,IWT-SVD) have been elaborated .The comparative study is based on the values of PSNR and NCC. At last,it has been observed that IWT-SVD gives comparable results faster than the DWT and DWT-SVD.

Sreekurty and Baiju [9],proposed a medical integrity verification system to improve the security of medical image using 2D Haar DWT. Through the verification stage, the extraction algorithm is applied to retrieve the original cover image and secret data.

III. PROPOSED SYSTEM

This paper proposes a security model for securing a medical data transmission over the media.The proposed model comprises of four phases.So here,in our proposed model the continuous process is as follows:

a) Data Encryption Phase - Confidential patient's data(medical text) is divided into even and odd

characters.Even characters are given to the RSA algorithm and odd characters are given to the AES algorithm.So the data is encrypted using a hybrid encryption scheme(RSA & AES) and generate the cipher text as an output in the data encryption phase.

b) Embedding Phase - The encrypted data nothing but the cipher text is being concealed in a cover image using a steganography technique IWT and produces a stego-image as the output of the embedding phase.Stego-image physically visibles like cover image but they both are different.

c) Transmission Phase - The transmission phase is one of the important section for sending the data to the destination securely.The encryption section generates the stego-image which defines that the data is embedded or hidden in an cover image.This image is secured using the secret key.Usually, we are using e-mail for transferring the data.If the person hacks the e-mail and obtain the image, the secret key helps from unauthorized notification.

d) Extraction phase - The embedded data inside the stego-image which is transferred using the e-mail is retrieved using a secret key and extracts the data hidden using inverse IWT and produces the cipher text as an output.

e) Data Decryption Phase - The decryption phase is reverse operation of the encryption phase. The extracted data nothing but the cipher data is decrypted to retrieve the original medical data that is transmitted.

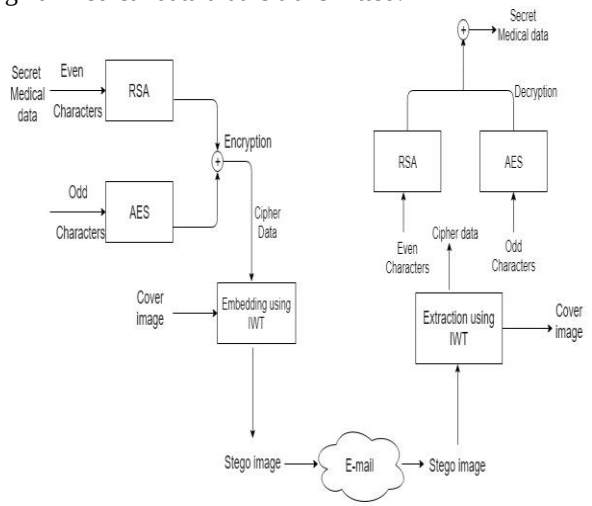

Figure 1: The proposed frame work for securing the medical data transmission

IV. ALGORITHMS

a) RSA Algorithm - RSA stands for Rivest, Shamir, Adleman developed in the year 1977.The RSA algorithm is used in the public key or asymmetric encryption as well as in digital signature[7].It is the most widely used public key algorithm in the world, used to encrypt a message without need to exchange a secret key separately.It allows the sender to encrypt the message using public key and decrypt the message using private key by the receiver.So,the security will be high if we use RSA in public key encryption.It's security is based on the difficulty of factoring large integers.It provides confidentiality, integrity and authentication for our data.RSA function depend upon the large prime numbers of public and private keys.

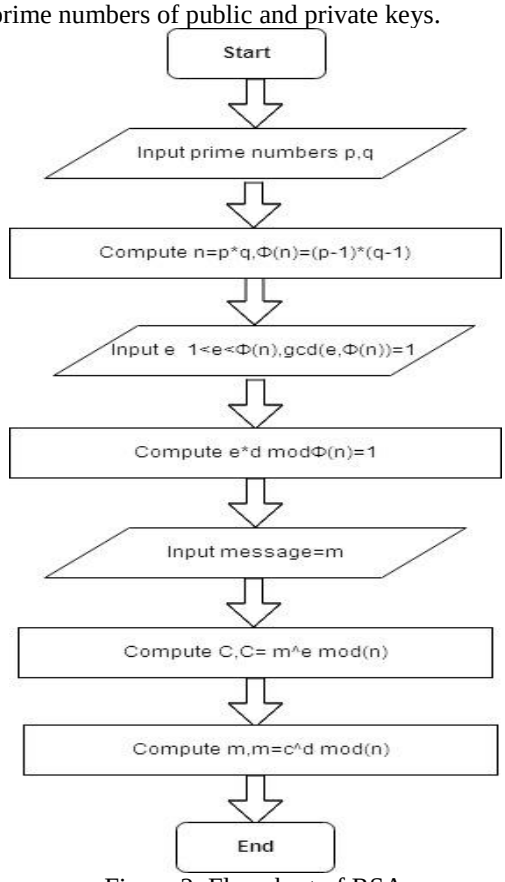

Figure 2: Flowchart of RSA

b) AES Algorithm - AES stands for Advanced Encryption Standard algorithm developed in the year 1997 and also known as Rijndael algorithm.It is an encryption standard choosen by Joan Daemon and Vincent Rijment. AES is a symmetric key encryption where same key is used for both encryption and decryption. AES takes a block of size 128 bits as input and produces the output block of same size.Plain text is processed in number of rounds(10 rounds) to get a cipher text.AES supports different key sizes like 128,192 and 256-bit keys.Each and every round we have to use separate sub-key.Each encryption key size will change the number of bit and also the complexity of the cipher text[6].It consists of 4 Transformations:

i). **Add Round Key** - In this step, each byte of the state is XOR-ed with the corresponding element of the key matrix.

ii). **Sub-bytes** - A non-linear substitution step where each byte is replaced with another element according to the look up table(s-box matrix) written in hexa-decimal system.The generating function used in this is GF(2^8) means 256 values are possible.

iii). **Shift Rows** - A transposition step where rows of the blocks are cylindrically shift in left direction.The first row is untouched,the second by one shift,third by two and fourth by three.

iv). Mix Columns - A linear mixing operation which operates on the columns of the state,combining four bytes in each column.It causes flips of bits spread all over the block.

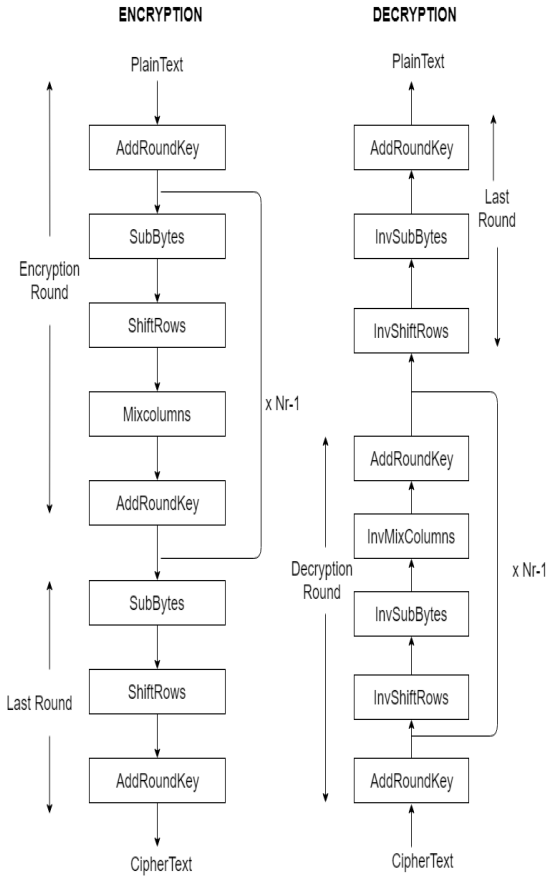

Figure 3: Flowchart of AES

c) Integer Wavelet Transform(IWT) - The IWT maps the integers to integers having importance in lossless coding applications and are derived from the linear wavelet functions which support invertibilty in finite precision arithmetic with less computational.The problem of encoding the original signal can therefore be transferred to encode wavelet coefficients,which provide a time-frequency description of the original signal.Makes the implementation considerations very attractive and easy regarding the size of the variables to be used .It is utilized to solve rounded error problem.IWT is generated using an efficient algorithm known as Lifting Scheme[8].The main advantage of this approach is reduction in the number of operations needed to perform the wavelet transform.An additional advantage is that it don't require an extra memory to store the resulting coefficients and also intoduces the feasibility of a reversible integer-to-integer wavelet transform with slight modification of the usual floating-point representation. Lifting scheme is an effective way of implementation of the wavelet filtering operation and it is divided into three stages:Split,Predict and Update.

i). Split - At this stage,main signal is divided into two samples even and odd sets.

ii). Predict:In this phase,odd samples are predicted from the even samples.This step is also called as Dual Lifting.

iii). Update:In this step,new even samples are generated by adding the original even samples to the predicted odd samples.This is also known as primal lifting.

Inverse Lifting Transform is also carried out with the difference that its signs are reversed.

V. EVALUATION PARAMETERS

a) Peak Signal-to-Noise Ratio(PSNR) - It calculates the imperceptibility of the stego-image.The higher the value of the PSNR of the stego-image reveals a higher quality of the stego-image or a higher imperceptibility of hidden message.The PSNR is calculated accotding to the following equation-

$$PSNR = 10\log_{10}[\frac{K^2}{MSE}]$$

Where K represent the maximum possible value of the pixel in an image (e.g:for a gray-scale image the maximum value is 255) and MSE is the mean square error.

b) Mean Square Error(MSE) - It calculates the magnitude of the average error between the original image and the stego-image.The MSE is computed below:

$$MSE = \frac{1}{[R*C]^2}\sum_{i=0}^{n}\sum_{j=1}^{m}[X(i,j) - Y(i,j)]^2$$

Where,R and C are the number of rows and columns in the cover image, X(i,j) is the intensity of X(i,j) the pixel in the cover image and Y(i,j) is the intensity of Y(i,j) the pixel in the stego-image.

VI. RESULTS

The performance of our model was compared with another technique developed by M.Elhoseny et. al.[6] on 256*256 pixel medical gray-scale image using 15-byte text size.

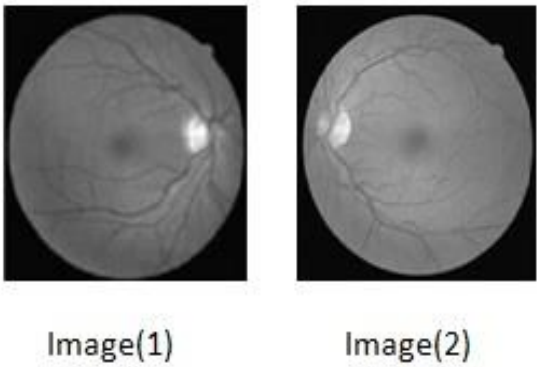

Figure 4: Gray Format of the Data Set

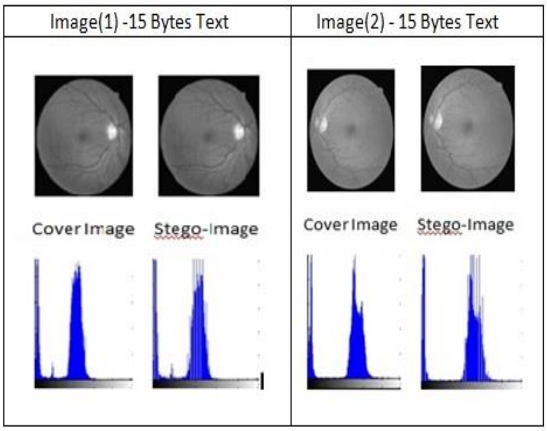

Figure 5:Histograms of the cover image and stego-image for the proposed model with text size of 15 bytes.

Table 1: Results of PSNR and MSE values for the gray-scale images for M.Elhoseny et.al Model and ProposedModel.

Cover Image	Text Size (15 Bytes)	PSNR			MSE		
		M.Elhoseny et.al [6]		Proposed Model	M.Elhoseny et.al [6]		Proposed Model
		DWT-2L	DWT-1L	IWT	DWT-2L	DWT-1L	IWT
Image(1)	15	56.04	55.43	56.73	0.16	0.18	0.045
Image(2)	15	56.05	55.43	57.34	0.16	0.18	0.039

VII. CONCLUSION

Information Security is greatly essential over the unsecured shared medium.So,the image transforms are essential for achieving efficient compression of the image to successfully transmit accurate medical data.A secure medical data transmission model using gray-scale images as a cover image based on the steganography technique has been proposed. Here the selection of a specific transform thus become vital,to maximize performance and results.We use different metrics such as PSNR and MSE to evaluate an error between the original image and the stego-image.From the results it is observed that,IWT gives efficient results when compared with the DWT-2L and DWT-1L.Thus,IWT is mostly recommended for critical medical applications because of its perfect reconstruction of the data without any loss of information along with low complexity and generates minimum error too.Unlike DWT,IWT increases the speed, regularity, stability and robustness with respect to the DWT.Further more,the execution time and computational complexity is 25% less as compared with DWT,which is suitable for the need of telemedicine.

VIII. REFERENCES

[1]. Information Hiding In Images Using SteganographyTechnique,RamadhanJ.Mstafa,Christian Bach,March2013, ASEE Conference, DOI:10.13140/RG.2.1.1350.9360

[2]. Security Algorithms In Cloud Computing , T.Ramaporkalai,IJCST–Volume:5,Issue:2,Mar – Apr 2017, ISSN: 2347-8578.

[3]. Adaptive Steganography Scheme Using More Surrounding Pixels, Masoud Afrakhteh & Subariah Ibrahim, June 2010,paper published in 2010 International Conference on Computer Design and Applications by IEEE,DOI-10.1109/ICCDA.2010.5541442.

[4]. Secret Key Estimation in Sequential Steganography, Trivedi.S, Chandramouli.R, IEEE,DOI:10.1109/TSP.2004.839925,volume:5,Issue:2,Feb.2005.

[5]. Image Steganography Using Hybrid Method LWT-DWT-SVD, Shallu Vohra, Binay Binod Kumar,Vol. 6, Issue 8, August 2017, DOI:10.15680/IJIRSET.2017.0608122

[6].]Secure Medical Data Transmission Model for IoT based-Health care systems,Elhoseny DOI:10.1109/ACCESS.2018.2817615,IEEE Access 2018.

[7]. Secure Medical Image Steganography with RSA Cryptography Using Decision Tree, M. Jain, R.C.Choudhary and Anil Kumar, published in 2016 2nd International Conference on Contemporary Computing and Informatics, DOI:10.1109/IC3I.2016.7917977,IEEE.

[8]. A Comparative Study of DWT ,DWT-SVD and IWT-SVD, Prerna Gupta and Girish Parmar IJEECS,Volume :6,Issue :7,2017,ISSN 2348-117X.

[9]. Security Enhancement in Image Steganography for Medical Integrity Verification System, M.S.Sreekutty & P.S.Baiju, ICCPCT, April,DOI:10.1109/ICCPCT.2017.8074197, IEEE Access,2017.

[10].