Secure Transmission Model for Medical Data By using Contourlet Transform for Health-Care Systems

Ramya Rani Kalvakota, Uma Volety

Abstract: Security and Privacy are the major issues for transmission of medical data in a wireless medium. The proposed system used ConTourlet Transform 2 Level (CTT-2L) Steganography and encryption algorithms for transmission of medical data. The encryption algorithms used are Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. First, the text data is encrypted by using AES and RSA Algorithms and the data which is encrypted is embedded in a cover image using CTT-2L. The cover image is any medical image which can be either colour or grayscale image. Five statistical parameters: Peak-Signal-to-Noise-Ratio (PSNR), Mean Absolute Error (MAE), Mean Square Error (MSE), Structural Similarity (SSIM), Correlation are measured for evaluating the performance of the proposed system. The PSNR is 71.3402 and 64.7453 in colour and grayscale images respectively. The MAE is 0.0019 and 0.0045 in colour and grayscale images respectively. The MSE is 0.0026 and 0.0142 in colour and grayscale images respectively. The SSIM is 0.9999 in both colour and grayscale images. The Correlation is 1.0000 in both colour and grayscale images. The proposed system hides the data with high capacity, imperceptibility and less distortion in the received stego image as compared with the conventional methods.

Keywords CTT-2L, encryption, medical images, steganography.

I. INTRODUCTION

The remote health-care systems need transmission of medical data through a wireless medium. So, a security system is essential for protecting the diagnostic medical data transmitted through a wireless medium[1]. The proposed security system uses a combination of encryption Algorithms and steganography techniques for embedding the data in an image. In encryption, text data is converted into a format that is read only by the intended receipient and others cannot read. Encryption uses a secret key to convert the text data into human unreadable format. The intended receipient decrypts the data by using the same key which is used in the encryption. AES and RSA algorithms are used in data encryption. AES is a symmetric key algorithm[2]. The key, that is used in the encryption is also used in the decryption. AES uses different keys of length 128 bit, 192 bit and 256 bit for 10 rounds, 12 rounds, 14 rounds respectively. On the other side, RSA is an asymmetric key algorithm[2]. In encryption, a public key is used and in decryption, a private key is used. The length of the key varies from (2-2048) bits.

The technique of hiding message in an image is called Steganography. The encrypted data is hidden in an image and transmitted through the wireless medium without any suspicion. ConTourlet Transform uses a Double Filter Bank structure for Multiscale and Multidirectional decomposition of an image [3]. Multiscale Decomposition is performed by Laplacian Pyramid (LP). Multidirectional Decomposition is performed by Directional Filter Banks (DFB). The output of LP contains one low pass image and many high pass sub-bands. The low pass image is given to next level Laplacian Pyramid for further Decomposition. The high pass sub-bands are given to DFB for capturing the directional information.

II. RELATED WORKS

M.N. Do et al., [3] have proposed a ConTourlet Transform (CTT) in order to overcome the limitations of wavelets. CTT is a discrete domain multiresolution and multidirection Decomposition of an image that uses non-separable filter banks. Various experiments demonstrated the capability of CTT in various digital image applications.

Malini Mohan et al.,[4] have proposed a technique which hides data in an image by using ConTourlet Transform. The image is decomposed using CTT and data is hidden in any of the sub-bands. Statistical parameters: PSNR, Variance, Skewness are evaluated. The proposed system's PSNR value is very high.

Mohammed Elhoseny et al.,[5] have proposed a model to transmit medical data in a wireless medium. The image is decomposed using Discrete Wavelet Transform (1 Level and 2 Level) and the data which is encrypted is hidden in any of the sub-bands. The performance was evaluated using PSNR, MSE, BER, SSIM and SC. The proposed System has high PSNR and less MSE.

Miao Qiguang et al.,[6] have proposed a fusion algorithm for data hiding in an image.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author

RamyaRani Kalvakota*, Pursuing M.Tech, Digital Electronics and Communication Engineering, G. Narayanamma Institute of Technology & Science, Hyderabad.

Uma Volety , Associate Professor, Department ECE, G.Narayanamma Institute of Technology & Science, Hyderabad.

ConTourlet Transform is used in this algorithm. Discrete Wavelet Transform (DWT) cannot represent smooth contours. This is overcome by using Contourlet Transform. Based on parameter n, the fusion rules are chosen. The proposed system detects more edges than DWT.

G. Saranya et al.,[7] made a comparison between Contourlet Transform and Discrete Wavelet Transform. Different medical images are used for data embedding and extracting using Non sub-sampled Contourlet Transform (NSCT) technique. High PSNR and low MSE are obtained by these technique than DWT.

III. THE PROPOSED MODEL

The medical data is hidden in a medical cover image through the given steps: (1) The data is converted into ACSII code. (2) The code is divided into even and odd part. (3)AES Algorithm encrypts the Odd part. (4) RSA Algorithm encrypts the even part. (5) CTT-2L is used to conceal the data which is encrypted in a cover image to give a stego-image. (6) The data which is encrypted is taken out from the stego image using CTT-2L. (7) The data which is extracted is decrypted to get the ASCII code. (8) The ASCII code is converted into text data. Fig. 1. Shows the whole process.

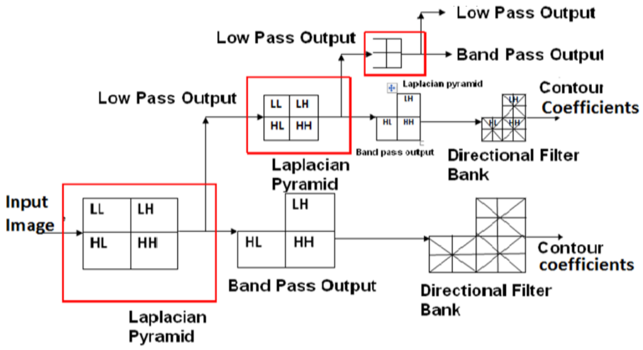

Fig. 1. Block Diagram of Proposed system.

A. Encryption Process

In the process of encryption, text data is divided into odd part and even part. AES is used to encrypt odd part by using a public key t. RSA is used to encrypt even part by using public key n. AES also encrypts the private key y for decryption of data. This is justified in the algorithm 1.

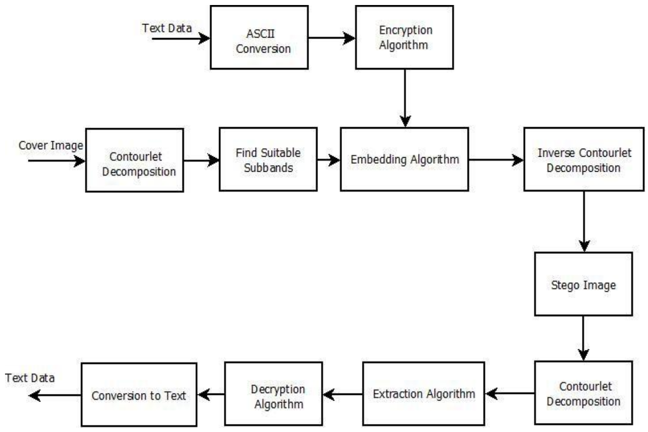

Fig. 2. Frequency Partition in CTT

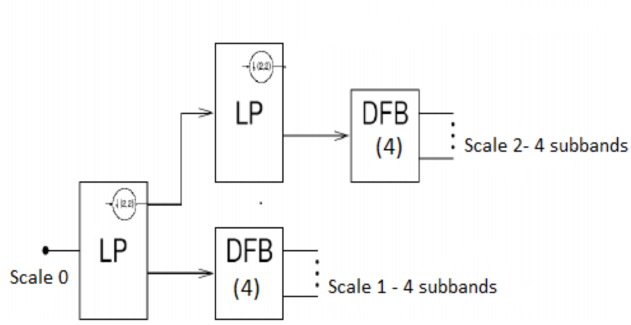

Fig. 3. Multiscale Decomposition.

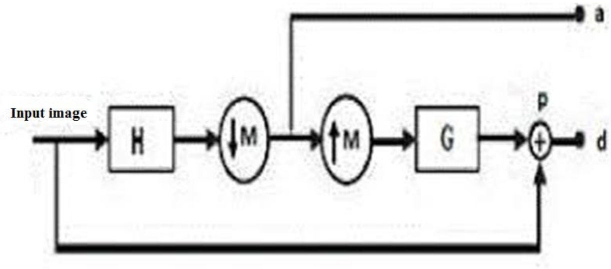

Fig. 4. Laplacian Pyramid Block Diagram.

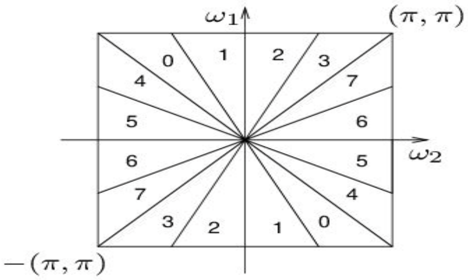

Fig. 5. Multidirectional Decomposition

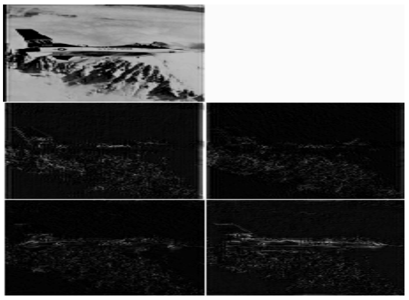

Fig. 6. Level 2 Decomposition in ConTourlet Transform.

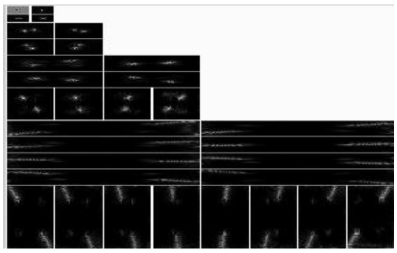

Fig. 7. Decomposition of 4 Levels in ConToulet Transform.

The algorithm for encryption is given below:

Algorithm 1:

1. The text data is divided into two parts.(Odd_Data, Even_Data)
2. Generate new key t using AES
3. Enc_Odd = AES(Odd_Data, t)
4. Generate public key n and private key y using RSA
5. Enc_Even = RSA (Even_Data, n)
6. Full_Enc_Txt is bulit by inserting both Enc_Odd and Enc_Even in their respective places.
7. Enc_Key = AES (y,t)
8. Full_Enc_Msg is compressed by converting to hashs
9. Enc_Key is compressed by converting to hashs
10. Cipher_Data = Concatenate (Full_Enc_Msg, Enc_Key)

B. Embedding Process

A CTT-2L was used to hide the data in a medical cover image. The CTT-2L is a Double Filter Bank structure that consists of a Laplacian Pyramid (LP) for multiscale Decomposition and a Directional Filter Bank (DFB) for multidirectional Decomposition. LP decomposes the image into 4 sub-bands: LL,LH, HL and HH. The algorithm for embedding is given below:

Algorithm 2:

1. ConTourlet Transform 2 Level is used to decompose the image.
2. The decomposed image consists of one low pass sub-band and four high pass sub-bands.
3. The data is embedded in any one of the selected high pass sub-band.
4. The data is converted into ASCII code before embedding in the image.
5. The code is encrypted using AES and RSA Algorithms for providing more security.
6. Least Significant Digit of the contourlet coefficient is substituted with the single digit of the data .
7. The process is repeated until whole data is embedded.

C. Extraction Process

The CTT-2L technique is used to get back the data from the cover image. The algorithm for extraction is given below:

Algorithm 3:

1. ConTourlet Transform 2 Level is used to decompose the stego-image.
2. The data is extracted from that particular sub-band in which it is hidden.
3. The digit is taken out from the Least Significant Digit of the contourlet coefficient .
4. The process is continued until whole data is extracted.

End

D. Decryption Process

Decryption is a process of converting the user unreadable format to user readable format. The same key used in the encryption is used in the decryption. The decryption algorithm is given below:

Algorithm 4:

1. Cipher_Data is divided into two parts: Hashed_Txt and Hashed_Key
2. Full_Enc_Data = Decompress (Hashed_Txt)
3. Enc_Key = Decompress (Hashed_Key)
4. y = Decrypt_AES (Enc_Key, t)
5. Enc_Odd = Split (Full_Enc_Data, odd)
6. Enc_Even = Split (Full_Enc_Data, even)
7. Odd_Data = Decrypt_ AES (Enc_Odd, t)
8. Even_Data = Decrypt_ RSA (Enc_Even, y)
9. Insert odd and even part in their respective places

IV. RESULTS AND DISCUSSION

Windows 7 operating system and Matlab 2016 were used for implementation of the proposed system. Statistical parameters are used to measure the difference between the cover image and the stego image. They are: Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE), Mean Square Error (MSE), Structural Similarity (SSIM) and Correlation. PSNR measures the standard of the reconstructed image. High value of PSNR increases the standard of the reconstructed image. It is given below:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\,\text{dB} \qquad (1)$$

Where, 255 stands for maximum gray-level value of a pixel in an image and MSE stands for Mean Square Error.MSE measures the average of the square of the difference between the cover image and the stego image. It is given below:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (2)$$

Where, m stands for no. of rows and n stands for no. of columns in the cover image, I(i,j) stands for cover image, K(i,j) stands for stego image.MAE measures the average of the difference between cover image and the stego image. It is given below:

$$\text{MAE} = \frac{1}{n}\sum_{j=1}^{n}|y_j - y_j| \qquad (3)$$

Where, n stands for no. of rows and columns in the cover image, Y_j stands for pixel value in the cover image, and Y_j stands for pixel value in the stego-image.SSIM measures the structural similarity between the cover image and the stego image. Its value lies in between −1 and 1. It is given below:

$$\text{SSIM} = \frac{2*mu1(p)mu2(p)+c1}{mu1(p^2)+mu2(p^2)+c1} * \frac{2*cov(p)+c2}{s1(p^2)+s2(P^2)+c2}$$

(4)

where, mu1(p) stands for mean of seq1 and mu2(p) stands for mean of seq2, s1(p) stands for standard deviations of seq1 and s2(p) stands for standard deviations of seq2 and the cov(p) is the covariance between seq1 and seq2. All are computed on the window XY located all over p. C1 and C2 stands for regularization constants.Correlation measures the similarity or difference in magnitude and phase between two signals or vectors when they are strongly linked together. It is given below:

$$r = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[\,n\Sigma x^2 - (\Sigma x)^2\,]\,[\,n\Sigma y^2 - (\Sigma y)^2\,]}} \qquad (5)$$

Where, n stands for no. of data pairs, X stands for cover image, and Y stands for stego image

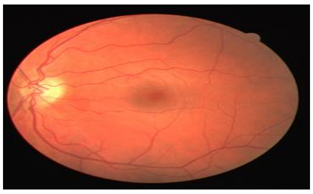

Fig. 8. Original colour image of an eye.

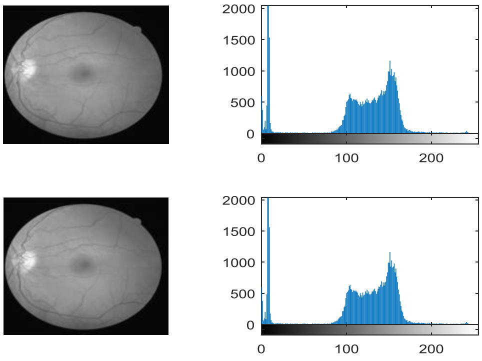

Fig. 9. Cover image and stego image with their corresponding Histograms of an eye.

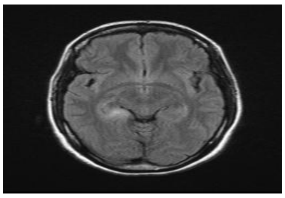

Fig. 10. Original gray-scale image of a brain.

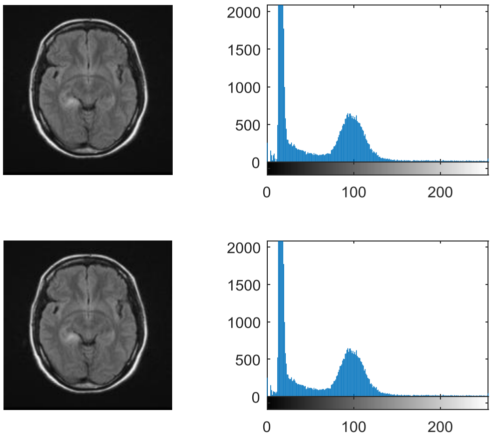

Fig. 11. Cover image and the stego image with their corresponding Histograms of a brain.

The proposed security system is compared with the MohamedElhoseny et al. method of transmission of medical data using Discrete Wavelet Transform 2 Level (DWT-2L) steganographic technique. The comparison results are shown in the table.

Table: Comparison Table

Cover Image	Parameters	Existing System	Proposed System
		DWT-2L	CTT-2L
Gray-scale image	PSNR	57.6886	64.7453
	MAE	0.0163	0.0045
	MSE	0.0554	0.0142
	SSIM	0.9999	0.9999
	Correlation	1.0000	1.0000
Colour image	PSNR	69.2114	71.3402
	MAE	0.0035	0.0019
	MSE	0.0039	0.0026
	SSIM	0.9999	0.9999
	Correlation	1.0000	1.0000

V. CONCLUSION

A secure transmission model for medical data by using CTT-2L Steganographic Technique was proposed for health-care systems. The proposed security model used AES and RSA Algorithms for encryption of data and CTT-2L for embedding the encrypted data in an image. PSNR, MAE, MSE, SSIM and Correlation were measured. The proposed system has high PSNR , less MAE and MSE as compared with other conventional methods.

REFERENCES

1. Muhammed Imran Malik et al.,"Preparing for Secure Wireless Medical Environment in 2050: A Vision". Published in IEEE Access (Volume: 6) on 7th may 2018, Electronic ISSN:2169-3536.
2. Nasrin Khanezaei et al., "A framework based on RSA and AES encryption algorithms for cloud computing services", IEEE conference, Date of conference:12-14 December 2014.
3. M. N. Do et al., "The contourlet transform: An efficient directional multiresolution image representation", IEEE Trans. On Image Processing, vol. 14, no. 6, pp. 760-769, 2005.
4. Malini Mohan et al.,"A new Algorithm for Data Hiding in images using ConTourlet Transform", IEEE 2011.
5. MohamedElhoseny et al., "Secure Medical Data Transmission Model for IOT-based Health-care Systems" Published in IEEE Access on March 21, 2018.
6. Miao Qiguang et al., "A Novel Image Fusion Method using ConTourlet Transform". Published in 2006 International Conference on Communications, Circuits and Systems, Date of Conference: 25-28 June 2006.
7. Saranya G et al., "An Approach for Embedding and Retrieving the Data in Medical Image using Contourlet Transform", International Journal of Scientific and Engineering Research, volume 3, Issue 10, Oct. 2012.

AUTHORS PROFILE

RamyaRani Kalvakota received B.Tech degree in Electronics & communication Engineering from Jyothishmathi Institute of Technological Sciences, Karimnagar and pursuing M.Tech in Digital Electronics and Communication Engineering in G. Narayanamma Institute of Technology & Science, Hyderabad. Email id: ramya.kalvakota@gmail.com.

Mrs V.Uma is working as an Associate Professor ECE department at G.Narayanamma Institute of Technology & Science, Hyderabad. She received her B.E degree from Osmania College and M.Tech form JNTU Hyderabad. She has a teaching experience of 20 years. Email id: uma.volety@gmail.com.