ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

Securely Data Transmission Using DWT via ECG Signal

[1] Sumedha P Awasarmol / ME, [2] Prof. Shweta Ashtekar,[3]Prof. Amruta Chintawar
[1] student, [2][3] Professor,
[1][2][3]Department of Electronics and Communication,
Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai

***Abstract*—For aged population suffering from cardiac disorders, remote ECG monitoring system is essential to be established in point of care system. Also it is essential to maintain patient confidentiality while transmitting data over public network and storing that information at hospital servers securely. This work, Secured Data Transmission via ECG Signal combines encryption and scrambling matrix technique using Discrete Wavelet Transform to protect patient confidential information. The encryption method hides patient confidential information using scrambling matrix and the shared key thereby generating watermarked ECG signal. To extract patient secret information from the ECG signal, decryption method is used using the same shared key and scrambling matrix. To evaluate diagnosability, Wavelet Weighted Percentage Residual Difference (WWPRD) and extracted WWPRD measurement would be used for analyzation.**

***Keywords*—Steganography, Encryption, Decryption, WPRD.**

I. INTRODUCTION

With the progress of civil liberties, users are becoming more concern about their confidentiality that plays a vital role in medical fields. POC and remote healthcare is an e.g. E-healthcare. Point-of-care testing allows diagnoses of patient in the physician's office, at an ambulance, at home, in the field, or in the hospital thereby resulting in timely care, and allows rapid treatment to the patient thereby reducing increasing traffic at hospitals and medical centre. However, PoC solutions provide more reliability in emergency services as patient medical information can be sent immediately to doctors. The response or appropriate action can be taken without any delay. Thus PoC and remote healthcare systems plays a crucial role for saving patient's life from cardiac diseases. Since these systems are based on wireless communication, Internet is used for transmission and reception of information. Yet internet brings threats along with convenience.

E-healthcare application faces a problem of confidentiality and reliability. Health Insurance Portability and Accountability (HIPAA) act mainly focuses on patient's confidentiality, data integrity, reliability etc. There are many methods to solve the problem of confidentiality .In the work, a safety system has been implemented to secure communication of patient private information joined with patient physiological information. A method is implemented which is based on steganography operation using Wavelet Transforms (WT). Steganography is defined as an art of secret writing that combines encryption and decryption steps which provides better performance during the transmission. In steganography method, secret information is been hidden into cover signal by using embedding technique. After embedding, a stego signal is transmitted to authorized person to extract the secret information of patient from cover signal by using shared key. In the method, ECG acts as a host signal due to larger size than any other physiological information hence it is suitable for concealing patient information. With the help of ECG signal, many cardiac diseases such as arrhythmia, ventricular fibrillation etc. can be diagnosed. The proposed method is shown in "Fig.1".

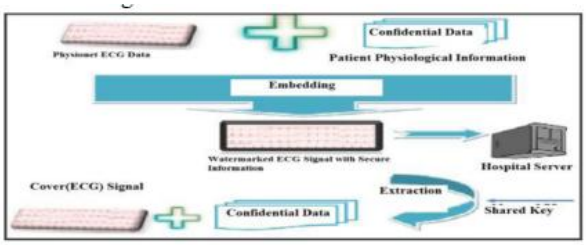

Fig.1. Block diagram of Steganography[1]

The designed method follows the HIPAA technique of wireless communication via internet for patient information but the unauthorised person cannot visualize the patient private information. The proposed method implemented a unique technique wherein ECG is collected from ECG sensors or physionet. Physiological parameters have taken of the patient at their home. Using Steganography method patient physiological parameters are embedded inside the ECG signal. This ECG signal is known as an encrypted ECG signal. Later the encrypted ECG signal is transmitted to the hospital through an internet. The size

ISSN (Online) : 2394-6849
International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

of encrypted ECG signal is similar to original ECG signal. Every individual could see the encrypted ECG signal but not the confidential information of patient except the authorized doctor having a secret key. The authorized person can only extract secret information of the patient from the biomedical signal by using secret key. This method delivers maximum protection of patient private information.

II.LITERATURE SURVEY

Several technique are involved to secure secret information.

In [7] Golpira and Danyali implemented a "Reversible blind watermarking for medical images based on wavelet histogram shifting."They applied,a two dimensional (2D) wavelet transform (WT) to the MRI images.After applying 2D WT,two frequency subbands are determined. In this process, two threshold values are selected. First threshold value was used for initial value of the histogram and second threshold value was used for last value of the histogram. First histogram value was shifted to the left part of first

thresholding which created the zero point for first threshold. Second histogram value was shifted to the right part of second thresholding which created the zero point for secondthreshold. Thereafter Binary watermark data was inserted by using threshold and zero point values. Finally, the watermark image was produced yet this method is not suitable enough for ECG signals.

In [1]Zheng and Qian proposed "Reversible data hiding for electrocardiogram signal based on wavelet transform." In this method, QRS complex was detected by using B spline WT. Haar lifting WT was used after detection of R wave to the original ECG signal. Index subscript mapping was applied and non QRS high frequency wavelet coefficients were selected. A watermarked ECG signal was produced by replacement of selected wavelet coefficients.ECG signal was recomposed by inverse wavelet decomposition. This method had low capacity because this method shifts only one bit. This method was not suitable for abnormal ECG signal.

S.Edward Jero, Palaniappan Ramu and S. Ramakrishnan proposed" Steganography in Arrhythmic Electrocardiogram Signal"[11].In this method, Edward et al. proposed an ECG steganography method for normal ECG signal using DWT-SVD watermarking algorithm. They identified the watermark embedding in high frequency band results better performance than the other frequency bands. However no work is reported on arrhythmic ECG signal using DWT-SVD steganography algorithm. The patient data is hidden inside the 2D ECG matrix of an arrhythmic ECG signal. Initially, the performance of 2D ECG matrix conversion method was evaluated and the resultant metrics showed that the deterioration due to the conversion process is negligible.DWT is one of the efficient transform to perform steganography in transform domain. The performance of ECG steganography using DWT-SVD based steganography algorithm were estimated for the 9 arrhythmic ECG signals of MIT-BIH arrhythmia database. The higher PSNR and the lowest PRD values of performance metrics appeared the better imperceptibility to the watermark and lowest deterioration of cover signal respectively. Finally,the zero BER shows that the patient data is extracted without any losses.

In [12] Ching-Yu Yang and Wen-Fong Wang proposed "Effective Electrocardiogram Steganography Based on Coefficient Alignment". The method presented lossy and reversible ECG steganography. It was divided into high quality and high-capacity ECG steganography which are capable of hiding confidential patient data in ECG signals. The reversible data hiding method apart from hiding secret messages restores the original ECG signal after bit extraction.

III. PROPOSED METHOD

The design method uses Discrete Wavelet Transform in combination with steganography. This technique contain authentication stage to prevent unauthorized user to extract the secret message.

A. Sender Steganography

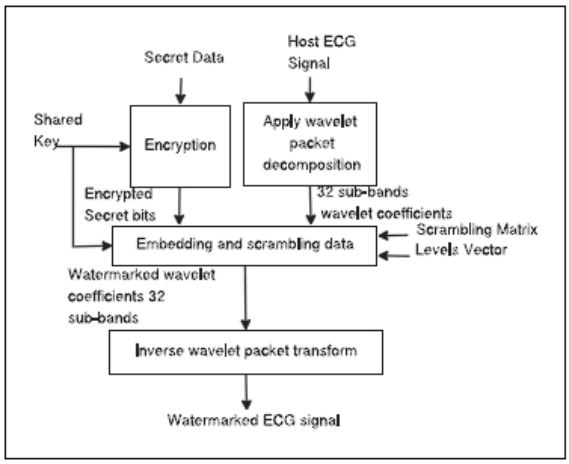

Fig.2.Block diagram of sender steganography[12]

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

The sender side of proposed technique consists of four stages:

1. Encryption:
The goal of this stage is to encrypt patient confidential information inside the Host ECG signal. The XOR ciphering technique is used with ASCII coded shared key. XOR is selected for its simplicity.

2.Wavelet Decomposition:
Wavelet transform decomposes the signal into coefficient in time frequency analysis using Band pass filter. Mathematically it is represented as:
$W(i, j) = \sum\sum X(i)\, \psi\, ij\, (n)$

Where, W (i, j) represents DWT coefficient, i represents scaling parameter, j represents shifting parameter, ψ i j (n) represents wavelet basis time function. A 5 level wavelet packet decomposition is applied to produce 32 sub bands wavelet co-efficient.

3.Embedding Operation:

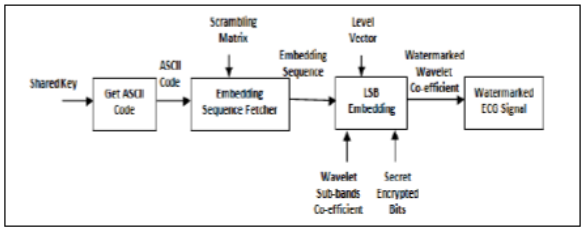

Fig.3.Block diagram of watermark Embedding Operation

In this technique a shared key and scrambling matrix is used by sender and receiver. At embedding stage row is selected by scrambling matrix using sequence row fetcher.

$$S = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,32} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,32} \\ \vdots & \vdots & \ddots & \vdots \\ s_{128,1} & s_{128,2} & \cdots & s_{128,32} \end{bmatrix}$$

Where S represents 128 x30 matrix and s represents number from 1 to 32.

4.Inverse Wavelet Decomposition
In this stage the watermark ECG signal is recomposed by adding 32 sub-bands and encrypted ECG signal is produce.

5.Insertion of Noise
During wireless transmission of a signal noise might get added. Hence in this paper Salt and Pepper noise is used to check the behavior of signal to be transmitted.

B. Receiver Steganography
Following information is required at the receiver side:
1) Shared Key.
2) Scrambling matrix.
3) Steganography level vector.
The first step is to remove noise from the received signal and then to apply five level wavelet packet decomposition to generate 32 sub-bands.Secondly by using the shared key and scrambling matrix the extraction operation starts extracting the secret bits using sequence row fetcher from scrambling matrix. Lastly the extracted secret bits are decrypted using shared key.

IV.DESIGN IMPLEMENTATION

The following flow chart is involved in implementing the design steps:

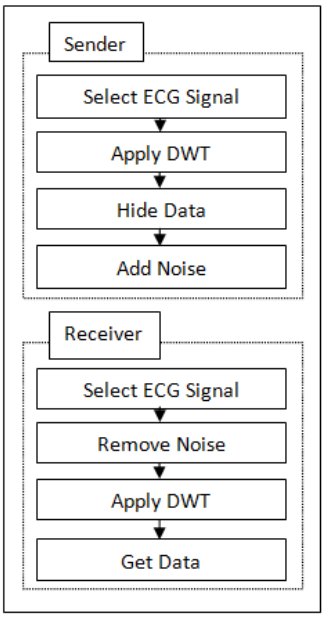

Fig.4.Flowchart of design implementation

The 32 wavelet coefficients after converting into binary bits are replaced with LSB bits of ECG signal by performing the embedding operation. Lastly, the Inverse wavelet decomposition is applied on 32 subbands wavelet coefficients to produce watermarked ECG signal is produced. After encryption, again watermarked 32 subbands wavelet coefficients are recomposed by applying wavelet decomposition. Later

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

to obtain result rearrange the secret bits from the ECG signal by using scrambling matrix and shared key. Finally, decryption process is implemented and patient secret data is extracted.

V. EXPERIMENTAL RESULTS AND ANALYSIS

Below figure 5 shows the original ECG signal collected from physionet.

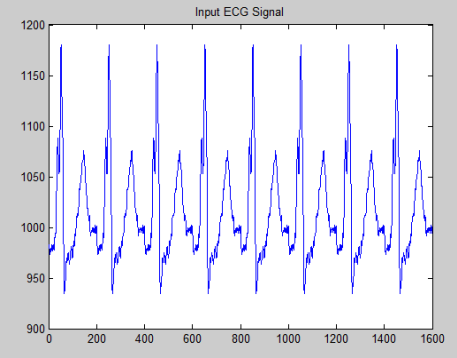

Fig.5. Original ECG Signal

Below figure 6 shows the encrypted ECG signal with embedded physiological parameters.

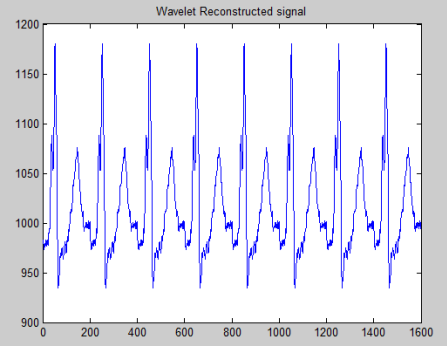

Fig.6. Encrypted ECG Signal

Below figure 7 shows Decrypted ECG Signal.

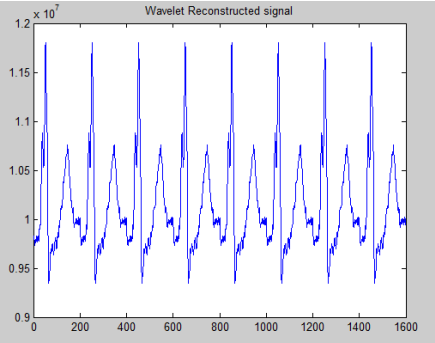

Fig.7. Decrypted ECG Signal.

Percentage Residual Difference Measurement is used to measure the difference between original host ECG signal and watermarked ECG signal. It can be represented as:

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N}(x_i^2)}}$$

where x is original ECG signal and y represents watermarked signal

To evaluate the diagnostic distortion caused by the watermark, a wavelet-based PRD (WPRD)and Weighted wavelet based PRD (WWPRD) is used. To measure distortion caused by the extraction process, WPRDE and diagnoses WWPRDE is used to calculate the difference.

The Wavelet based Percentage Residual Difference measurement can be calculated as:

$$WPRD_j = \sqrt{\frac{\sum_{i=1}^{N}(c_i - \bar{c}_i)^2}{\sum_{i=1}^{N}(c_i^2)}}$$

where c_i is the original coefficient within sub-band j and $\bar{c}_i$ is the coefficient of sub-band j for the watermarked signal.

The Weighted Wavelet based Percentage Residual Difference measurement can be calculated as:

where NL is the total number of sub-bands, ωj denotes the weight value corresponding to sub-band j, and WPRDj represents the calculated wavelet-based PRD for sub-band j.

Signal to Noise Ratio is another distortion measurement which is defined as-

SNR=40-20 log 10(Normal PRD) dB

SNR=40-20 log 10(Extracted PRD) dB

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

TABLE-I

Normal and Extracted WPRD and WWPRD measurement using db2

	Sender		Receiver	
Signal	WPRD	WWPRD	WPRDE	WWPRDE
ECG 1	0.00117238	0.00026053	999900	471357
ECG 2	0.00247577	0.00055017 2	999900	471357
ECG 3	0.00203305	0.00045178 9	999900	471357

VI. CONCLUSION

The paper represents a wavelet based secured data transmission method that collects ECG signals from Physionet. Wavelet packet decomposition is proposed for decomposing the host ECG signal. For concealing the patient private information, encryption process is implemented. Patient private information is embedded inside the host ECG signal in the form of binary bits to obtain Watermarked 32 sub-bands wavelet coefficients. Consequently, Encrypted ECG signal is produced by inverse wavelet decomposition. Later, extraction process is implemented which separates the patient private information and host ECG signal.

REFERENCES

[1]D. Awasthi and S. Madhe, "Evaluation of wavelet based ECG steganography system by using Percentage Residual Difference (PRD) measurements," Communications and Signal Processing (ICCSP), 2015 International Conference on, Melmaruvathur, 2015, pp. 0559-0563.

[2] K.Malasri and L.Wang, "Addressing security in medical sensor networks,"in proc. 1st ACM SIGMOBILE imWorkshop syst. Netw. Supp. Healthcare Assist. Living Environ. 2007, p.12.

[3] J. Garcia, I. Martinez, L. Sommo, S. Olmos, A. Mur, and P. Laguna, "Remote processing server for ECG-based clinical diagnosis support, "IEEE Trans. in! Technol.Biomed.,vol. 6,no. 4,pp.277-284,Dec.2002.

[4] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign," iEEE Trans. In!Techno!.Biomed.,vol. 11 , no. 6, pp. 619- 627, Nov. 2007.

[5] W.Lee and C. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations", IEEE Trans.Inf. Technol.Biomed. , vol. 12,no. 1,pp. 34–41,Jan. 2008.

[6] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," iEEE Trans. Imag. Process. , vol. 8, no. 8, pp. 1075-1083, Aug. 1999.

[7] H.Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting,"in Proc. iEEE int. Symp. Signal Process. Inf Technol., Dec. 2009, pp. 31 - 36.

[8] AymanIbaida and Ibrahim Khalil, "Wavelet based ECG steganography for protecting patient confidential information in point of care systems," IEEE Trans. Biomedical Engineering, vol. 60, no. 12, December 2013.

[9] Dr Prena Mahajan and Abhishek Suchdeva, "A study of encryption algorithm AES, DES , and RSA for security, "Global Journal of Computer Science and Technology Network, web and security volume 13, issue 15 version 1.0 year 2013.

[10] Masoud Nosrati, Ronak Karimi and Mehdi Hariri, "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011.

[11] S. Edward Jero, Palaniappan Ramu and S. Ramakrishnan, "Steganography in Arrhythmic Electrocardiogram Signal", 2015 IEEE 978-1-4244-9270-1/15/

[12] Ching-Yu Yang and Wen-Fong Wang, "Effective Electrocardiogram Steganography Based on Coefficient Alignment", J Med Syst (2016) 40: 66 DOI 10.1007/s10916- 015-0426-9, Department of Computer Science and Information Engineering, Springer Science Business Media New York 2015.