ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Secure Crypto and ECG Steganography Based Data Communication for Wireless Body Sensor Network

G Sheeba[1], M I Anju[2], K Hari Priya[3], V Monisha[4], M M Sabbana Banu[5]

Assistant Professor, Department of ECE, New Prince Shri Bhavani College of Engg. & Tech., Chennai, India [1&2]

Department of ECE, New Prince Shri Bhavani College of Engg. & Tech., Chennai, India [3,4&5]

ABSTRACT*:* The acquisition, processing and secure transmission of a patient's physiological and physical parameters to a remote location has been done by Patient Tele monitoring System (PTS). The PTS uses the wireless channel for communication of patient's data which is not secure as wireless channel is open for information being hacked by unauthorized person easily , where there is no patient's privacy thereby this project proposes the improvement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique is the chaos cryptography technique which encrypts the confidential data in to unreadable form and it is concealed in to the high frequency coefficient of the Wavelet decomposed ECG signals by the data hider. The reversible data hider technique and LSB replacement algorithm is used for concealing the secret message bits into the high frequency coefficients. In the data extraction module relevant key is used to extract the secret data and decryption keys are used to get back original information .Finally the performance of the proposed technique and existing technique is analyzed based on image, data recovery and time consumption.

KEYWORDS: ECG, Steganography, Encryption and Wavelet transform.

I. INTRODUCTION

It is of more importance to implement a security system for information to be secured and confidential being sent through the wireless channel. Patient telemonitoring system does real time monitoring of the remote patient's health for 24 x 7 there by patient's can be helped during the emergency time. For this purpose Wireless Body Sensor Network (WBSN) Architecture is been used. The wireless body sensor is deployed in to the patient's body or it can be in the wearable form like a wrist watch. This WBSN senses the temperature and heart beat of the patient and if it is abnormal the information will be sent to the patient's care taker and Patient Telemonitoring system. So that patient can be saved at time. For the transmission of the patient's status we use body sensor network and microcontroller interfaced GSM module there by message will be sent to the patient's care taker and PTS[3]. Further the PTS will send report about the patient to the doctor and patient's care taker in the wireless channel, in order to enhance the patient's privacy we propose chaos encryption system and Steganography technique for secret data transmitted over the wireless channel.

II. RELATED WORK

The patient's data is secured by using many approaches. The one such approach proposed to secure the data is done by steganography technique in which the secret information is hided inside the medical images. How much information can be stored and till to what extent the method is secured is the challenging factor faced here. What will be the resultant distortion on the original medical image or signal is finally found here.A new reversible data technique based on wavelet transform had been proposed. In their method QRS complex is detected by applying B-spline wavelet transform on the original ECG signal.Haar lifting wavelet transform is applied after the R waves have been detected.Next, the index subscript mapping is compared and applied by selecting the non QRS high frequency coefficient. The embedding of water mark is done after shifting the selected coefficient to one bit left. By applying the reverse Haar lifting wavelet transform the ECG signal is reconstructed. The embedding of watermark is done before and the Arnold transform is applied for watermark scrambling Since one bit is shifted, the capacity is low in this method. The result is that only one bit can be stored for each ECG sample value. Furthermore the user defined key has not been used and the security in this algorithm relies on the algorithm itself. Finally the normal ECG signal in which the QRS complex is detected is based on this algorithm. The algorithm will not perform well for the abnormal signal for which the QRS cannot be detected.

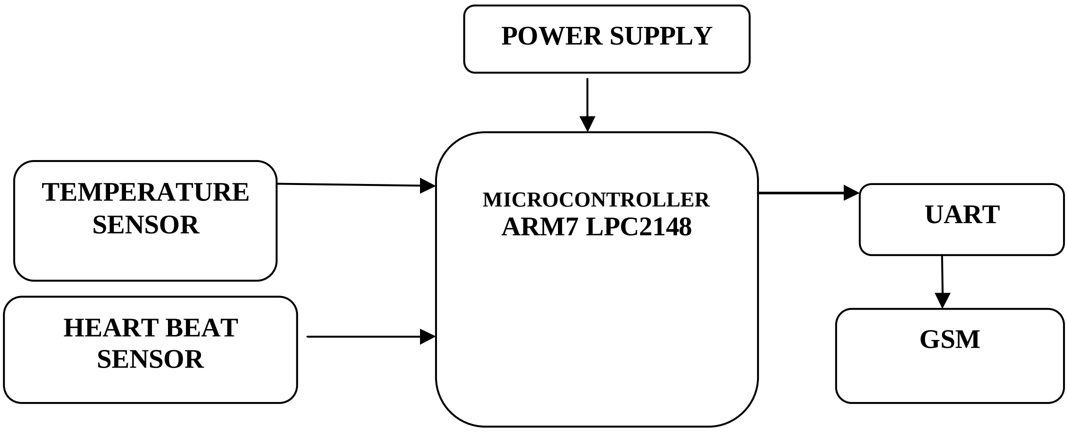

Fig.1.Hardware Unit

III.METHODOLOGY

There are four integrated stages in the sender side of the steganography technique. The stages are described below in more detail.

In the proposed technique it is ensured that there is minimal distortion in the host ECG signal which is used for hiding the confidential data in the steganography process. Moreover, in this technique authentication stage is there to prevent unauthorized users from extracting the hidden information.

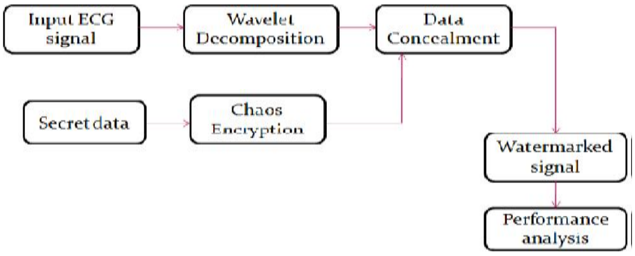

Fig.2. Block diagram for embedding process

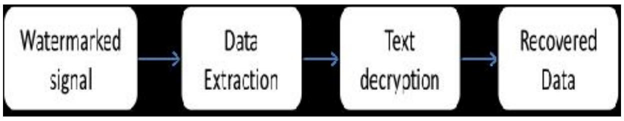

Fig.3. Block diagram for extraction process

A.STAGE 1: Chaos crypto system

Chaos crypto system is one of the advanced encryption standard for the enhancement of the privacy protection system.It encrypts the original data with the encryption key value generated from chaotic sequence with threshold function and logistic map is used for chaotic map sequence generation,which is helpful to transmit the secret inforamtion through unsecure channel securely which prevents data hacking.

B.STAGE 2:WAVELET DECOMPOSITION

Wavelet transform are used to analyze non-stationary signals whose frequency varies in time, as Fourier Transform (FT) is not suitable for such signals.Inorder to overcome the limitation of FT, Short Time Fourier Transform was proposed. The window function 'w' is chosen. It is will be considered stationary when then width of this window is equal to the segment of the signal.The wavelet transform involves projecting a signal onto a complete set of translated and dilated versions of a mother wavelet φ(t).Assuming the loose requirement that φ(t) has compact temporal and spectral support (limited by the uncertainty principle of course), upon which set of basis functions can be defined. The basis set of wavelets is generated from the mother or basic wavelet is defined as

Ψ a,b(t)=1/$\sqrt{a}$ ψ((t-b)/a);

a, b €R and a>0 -------- (1)

The variable .a. (inverse of frequency) reflects the scale (width) of a particular basis function such that its large value gives low frequencies and small value gives high frequencies. The variable .b. specifies its translation along x-axis in time. The term 1/ a is used for normalization.

Forward Lifting in IWT

Column wise processing to get H and L

H = (Co-Ce) and L = (Ce+ [H/2])

Where Co and Ce is the odd column and even column wise pixel values

Reverse Lifting scheme in IWT

Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

C. Stage 3: Adaptive LSB Embedding technique

The message information is embedded into a carrier image with virtually imperceptible modification of the image by using an ideal technique called steganographic method .The natural variations in the pixel intensities of a cover

Image to hide the secret message has been exploited by the method called Adaptive steganography. The method of embedding an additional information into the digital contents, which is undetectable to listeners is the objective of Steganography. The embedding, detecting, and coding techniques have been investigated here. The idea that have been used behind the LSB algorithm is the insertion bits of the hidden message into the least significant bits of the pixels. Several terms are used by the various groups of researchers, which includes the steganography, digital watermarking, and data hiding , since the application domain of embedding data in digital multimedia sources has been broaden.

A principle approach for detecting the least significant bit (LSB) steganography in digital signals such as images and audio has been introduced in this paper. Least Significant Bits of signal samples can be estimated with relatively high precision and the length of hidden messages which was embedded as been shown here. The stegano approach which has been newly developed is based on some statistical measures of sample pairs which are highly sensitive to LSB embedding operations. The resulting detection algorithm obtained is simple and fast. The robustness of the proposed stegano approach has been evaluated which is bounded on the estimation errors that has been developed. The counter measures and the vulnerability of the new approach to possible attacks is also assessed, and counter and are suggested. The results of the application on some sample images and the detailed algorithm is also presented here, furthermore.

D. Least Significant Bit Insertion

The concealing process uses the detailed coefficients which is obtained from the wavelet domain and second bit of the a secret message is embedded into the location of second bit and so on. The resultant watermarked signal that holds the secret message with original form and difference between the input signal and the watermarked signal is not visually perceptible to the users. The signal quality however degrades with the increase in their number of LSBs[2]. The error that has been introduced between the input and output signal, during the hiding process will be identified by mean square error and the signal quality is determined by Peak signal to noise ratio. The idea used by the LSB algorithm is the insertion of bits of the hidden message into the least significant bits of the pixels used.

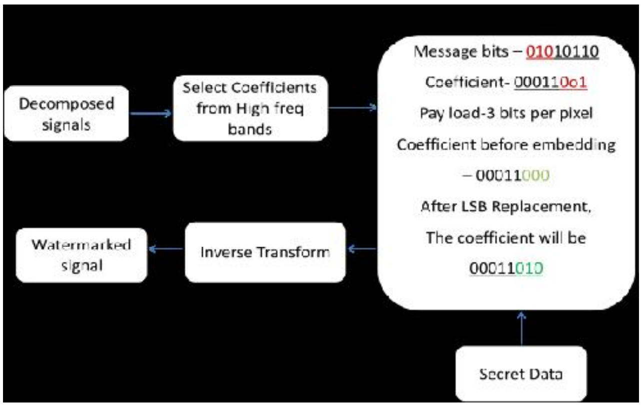

Fig.4. Block diagram for the algorithm flow of least significant bit insertion

E. Stage 4: Inverse wavelet re-composition

Inverse wavelet recomposition (IWR) is used to recompose the resultant water marked 32 subbands. A new watermark ECG signal is formed by this operation. Instead of converting the signal to time and frequency domain it is converted to time domain thus the Watermark ECG signal is similar to original unwatermarked ECG signal[1]. The algorithm starts by assigning required variable next shift will be made in the coefficient matrix to check all coefficient values are integer. Then out of 32 nodes a node is selected in each row of coefficient matrix. The value is based on scrambling matrix and key. Until the end of coefficient matrix is reached the algorithm is repeated. Then again shift is made in coefficient matrix and watermarked ECG signal is obtained by IWR.

F. Stage 5: Watermark extraction process

The information that is required at the receiver side to extract the secret bits from the Watermarked ECG signal

1 .the key value that is shared
2. Scrambling matrix
3. Steganography vector.

The 32sub band's signal is generated by applying 5level wavelet packet decomposition. The extraction operation starts by using the key value that is shared and scrambling matrix[6]. The same key value that is shared is used to extract decrypted secret bits. This process is similar to water mark embedded process where instead of changing selected nodes bit the value of the selected bit is read and reset to zero.

IV. EXPERIMENTS AND RESULTS

The medical signals is used for testing and verifying the proposed system.The proposed model is evaluated by using , the PRD (percentage residual difference) which is given as the difference between the original ECG host signal and the resulting watermarked ECG signal. The same scrambling matrix has been used in this method for obtaining the results . The same experiments and the calculated the average PRD values has been performed for different cases of scrambling matrices to generalize the results . Input signal Watermarked signal.The proposed model is evaluated by using , the PRD(percentage residual difference) which is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal as shown in Eq 3.

PRD = sqrt(sum((x – y).^2)/sum(x)) ----(3)

Where x represents the original ECG signal, and y represents the watermarked signal. Finally , the reliability of the extracted information is evaluated ,by using the bit error rate .

BER =(Berr/Btotal)× 100% -----(4)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

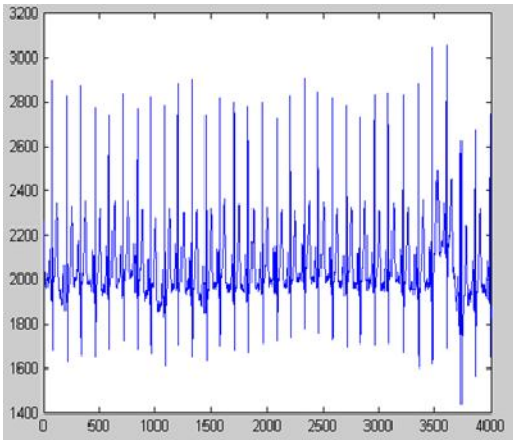

Fig.5.Input Signal

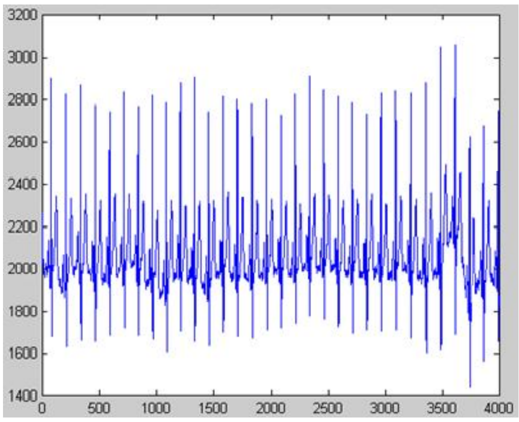

Fig.6.Watermarked Signal

Where the BER is given as the Bit Error Rate in percentage, Berr represents the total number of erroneous bits and Btotal represents the total number of bits. It is true that the removal of the watermark will have a small impact on the PRD value. As a result, the ECG signal can be still used for the diagnoses purposes , even after the removal of watermark. This encouraging result demonstrates clearly , that the watermarked ECG signals can be used for diagnoses. ECG signal types, and the resultant watermarked signals before and after the watermark extraction process has been obtained as a results . The same scrambling matrix has been used for obtaining the previous results.

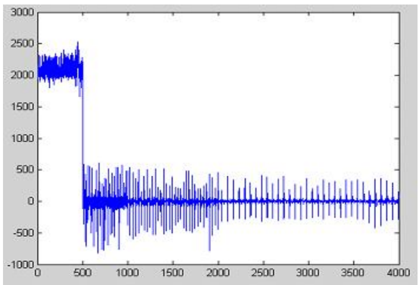

Fig.7.Wavelet Transformation signal

V. CONCLUSION

In this paper patient's detail is hided and the diagnostics information inside ECG signal algorithm is proposed using a novel steganography process. This technique will ensure the secured communication and the confidentiality in a Point-of-Care system has also been provided. Wavelet decomposition is applied here for decomposing the signal. A scrambling matrix is used to find the correct embedding sequence which is based on the user defined key. Steganography levels (i.e. number of bits to hide in the coefficients of each sub-band) are determined for each sub-band. It has been identified that the resultant watermarked ECG signal can be used for the diagnoses and the hidden data can be extracted completely.

REFERENCES

[1]Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," IEEE Transactions on information technology in biomedicine, vol. 8, no. 4,pp . 439–447, 2004.

[2] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign," IEEE Transactions on Information Technology in Biomedicine,, vol. 11, no. 6, pp. 619–627, 2007.

[3] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in 5th International Conference on Intelligent Sensors,Sensor Networks and Information Processing (ISSNIP), 2009. IEEE, 2010, pp. 207–212.

[4] W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," IEEE Transactions on Information Technology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.

[5] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments. ACM, 2007, p. 12.

[6] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," IEEE Transactions on Information Technology in Biomedicine,, vol. 13, no. 6, pp. 946–954, 2009.