ECG Signal Steganography Using Wavelet transforms

Asha N S, Anithadevi M D, Dr.Shivakumar K B, Dr. M Z Kurian
ashans.ec@gmail.com, anumdssit@gamil.com,shivakumarkb@ssit.edu.in, mzkurianvc@yahoo.com

ABSTRACT: Today, remote PoC (Point of Care) system is widely used to reduce to traffic in the hospitals. Privacy, security and confidentiality of the patient information are the major problem in the remote health care system. In is paper, we introduced encryption process on ECG steganography using wavelet transform. In proposed method, execute the time domain steganography for transmit the proficiency to conceal the patient information in any bit location with slightest error. And also frequency steganography is implemented in which five level wavelet packet decomposition is obtained. Data hidden inside the ECG signal through shared key and scrambling matrix. In this paper we have collected the ECG signal of patient from body sensors and physionet. We have hidden the physiological parameter into biomedical signal and produced watermarked biomedical signal. We have analyzed the energies of original and watermarked ECG signal using different wavelets such as coiflet, biorthogonal and symlets wavelet. From the result we concluded that energy of encrypted ECG signal using coiflet is higher than any other wavelet transform.

Key words: Confidentiality, ECG, energy, encryption, watermarked ECG signal.

1. Introduction

Now days, patients are suffering from various diseases especially related to the heart. With large traffic in the hospital patient can not able to get the appropriate treatment in time and the chance to they may get die. In order to solve this problem health care system uses remote PoC (Point of Care) system in the hospitals. Here, collect the patient physiological signal from the patient body through body sensors. Next, the collected signals are sent to the patient PDA (Personal Digital Assistant) for further diagnosis processing. Finally, the ECG signals and patient information as well as diagnosis report are sent to hospital server via internet. Doctors can check the biomedical signals and take a possible decision in case of an emergency. By using internet as the main communication tool that introduces security, privacy as well as data integrity. According to HIPAA (Health Insurance Portability accountability Act), the information sent through the internet should be protected and secured. In this paper, encryption based steganography technique is used .This method is not enough to secure the patient information. We have applied a new technique, which is obtained by wavelet transform.

Fig.1. shows the block diagram of ECG signal steganography scenario in Point of Care (PoC) system. In this method, ECG signals are collected from the different body sensor and physionet. Physiological parameter and patient personal information have taken from patient and sends to the patient PDA via Bluetooth. Steganography technique is implemented in the patient‘s PDA device.

Send this information to the hospital server via internet. All the doctors of the hospital can see the watermarked ECG signal only the authorized doctor can extract the secret information inside the host ECG signal.

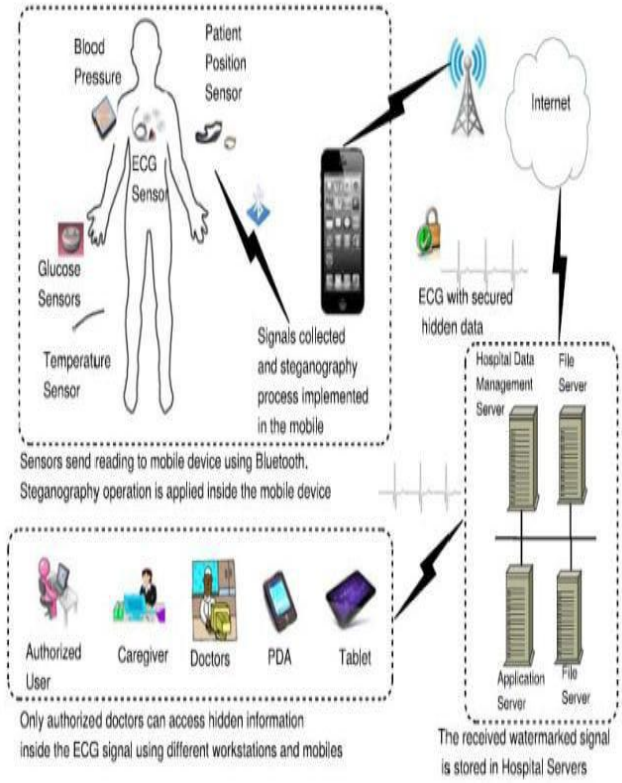

Fig.1. ECG steganography scenario in Point of Care (PoC) system where body sensors collect different readings as well as ECG signal and watermarking process implemented inside the patient‘s mobile device.

2. RELATED WORK

There are many techniques to secure the secret information. Navjot kaur and Usvir kaur proposed an audio watermarking using Arnold transformation with discrete wavelet transform (DWT) [3]. In this method, the secret information concealed inside the ECG signal by applying the DWT and DCT watermark scrambling with

Arnold transformation. After embedding extraction of secret information from ECG signal is completed. For checking the robustness, signal to noise ratio, mean square error and bit error rate is calculated. This technique was too lengthy and complexity level was high.

Nilanjan Dey, et al [4] proposed analysis of P-QRS-T components modified by blind watermarking method within the ECG signal for authentication in wireless telecardiology using DWT [4]. This method has two parts. In first parts, multi resolution wavelet transform based system is proposing for detection of P-QRS-T peaks complex from original ECG signal. P, Q, R, S, T peaks are detected and store over the whole signal. Time interval between two consecutive R-peak and rest peaks interval are measuring to check and detect abnormality of heart. To check the accuracy of P, Q, R, S, T components detection and interval measurement by processing and thresholding the original signal. The second part proposed the spread spectrum and discrete wavelet transform based watermarking. Watermarked signal is generating by DWT and compare distortion between watermarked ECG signal and original ECG signal but this method is not suitable for abnormal ECG QRS complex detection.

Golpira and Danyali [12] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this paper, medical images such as MRI are used as host signal. A 2-D wavelet transform is applied to the image. Then, the histogram of the high-frequency sub bands is determined. Next, two thresholds are selected, the first is in the beginning and the other is in the last portion of the histogram. For each threshold, a zero point is created by shifting the left histogram part of the first threshold to the left, and shifting the right histogram part of the second threshold to the right. The locations of the thresholds and zero points are used for inserting the binary watermark data. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of these algorithms is low. Moreover, no encryption key is involved in its watermarking process.

3. PROPOSED METHOD

The sender side of the proposed steganography technique consists of four integrated stages as shown in fig.2. The proposed technique is designed to ensure information hiding with minimal distortion of the host signal. Moreover, this technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.

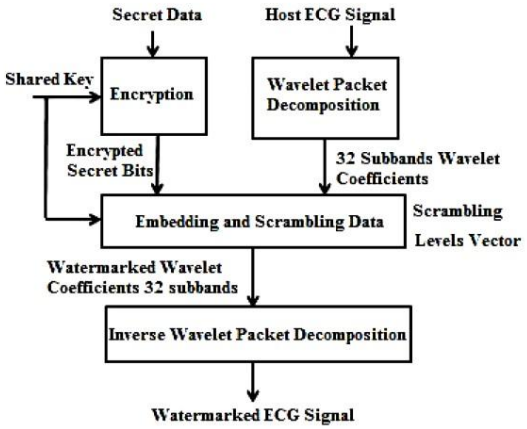

Fig.2. Blockdiagram of the sender steganography which includes encryption, wavelet decomposition, and secret data embedding.

Stage 1: Encryption

The aim of this stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons – who does not have the shared key – from accessing patient confidential data. In RSA encryption method public key is used for encrypting the patient information and private is used for decrypting the patient information.

Stage 2: Wavelet Decomposition

Wavelet transform is the process of decompose the signal into coefficients representing frequency components of the signal at a given time. Wavelet transform can be defined as follows:

C(S, P) $\int_{-\infty}^{\infty} f(t)\psi(S,P)\,dt$ (1)

Where ψ represents the wavelet function. S and P are positive integer representing transform parameters. C represents the coefficients which is a function of scale and position parameters. In most of the application we use the discrete wavelet transform (DWT). DWT decompose the signal into two using band filters. The mathematical expression is defined as:

$W(i,j)=\sum\sum X(i)\ \psi\ ij(n)$ (2)

Where W (i, j) represents the DWT coefficients, i, j shows the shift and scale parameters and ψ i,j shows wavelet basis time function. The result of the band filtering operation will be two signals, one is related to the high-frequency components and the other is related to the low-frequency components of the original signal. Low frequency component has important features of ECG signal and high frequency component contains noise. This process has implemented up to five levels.

Stage 3: Embedding Technique

Shared key and scrambling matrix is used in this stage. The patient physiological information is hide inside the host ECG signal by using scrambling matrix and private key. The Scrambling matrix can be defined as:

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

Where, S represents 128×32 matrix and s represents number from 1 to 32. Two conditions are used for making matrix.

- Same row must contain different elements.
- Row of scrambling matrix must be different.

Embedding operation is shown in fig.4. At embedding stage, shared key is converted into ASCII codes. By the sequence fetcher row is read by the scrambling matrix.. After getting the first row, patient information is embedded inside the 32 sub band wavelet coefficients. In embedding operation, 32 sub bands wavelet coefficients are converted into binary form. Secret bits are replaced by LSB bits of wavelet coefficients and produced the stego ECG signal.

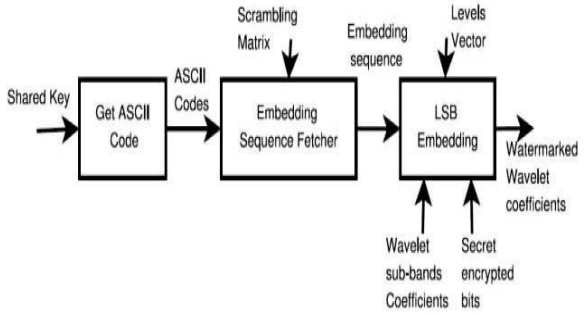

Fig.4. Block diagram showing the detailed construction of the watermark embedding operation.

Stage 4: Inverse Wavelet Decomposition

In this stage water marked wavelet coefficients are recomposed by applying inverse wavelet decomposition. After this stage, a new stego ECG signal is generated, which is similar to original ECG signal. It will be repeated until all the wavelet coefficients will be reconstructed. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain.

Therefore, the newly reconstructed stego ECG signal will be very similar to the original ECG signal.

4. EXPERIMENTAL RESULTS

First we loaded the ECG signal and output of the original ECG signal is shown in the fig.5

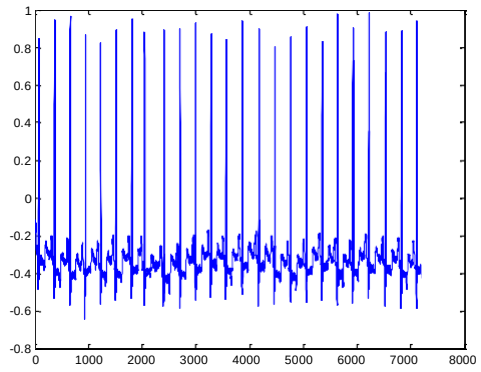

Fig.5. Host ECG signal

Afterwards, ECG signal has decomposed. Consequently, embedding process is implemented by using scrambling matrix and secret key. The bits of secret information are replaced with LSB bits of original signal. Subsequently, 32 sub bands watermarked wavelet coefficients are produced which is shown in fig.6.

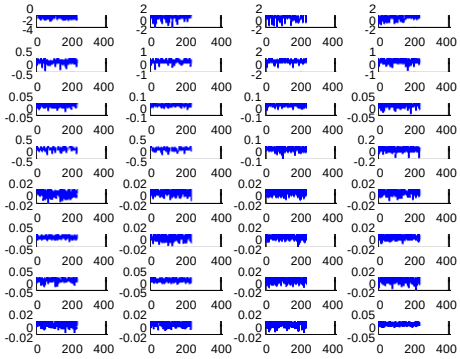

Fig.6. 32 sub band Wavelet packet coefficients

We have hidden the patient confidential information inside the ECG signal shown in fig.7.

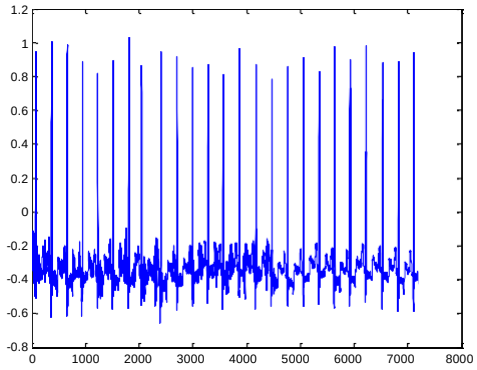

Fig.7. Data hide inside the ECG signal.

We have applied inverse wavelet packet decomposition to extract the patient information which is shown in fig. 8.

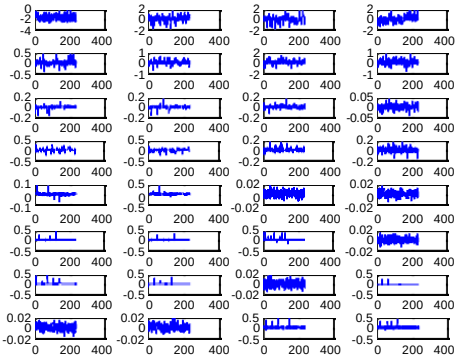

Fig.8. Inverse wavelet decomposition we get 32 sub band coefficients

Table 1 shows the energies of original ECG signal and watermarked ECG signal using different wavelets. E(original) re[resents energy of original ECG signal E(bior6.8) represents energy of encrypted ECG signal using Biorthogonal wavelet, E(sym4) represents energy of encrypted ECG signal using Symlets wavelet, E(coif5) represents energy of encrypted ECG signal using Coiflet wavelet.

Table 1

Energy of Original and watermarked ECG signal

E (original)	E (bior6.8)	E (coif5)	E (sym4)
559146 609	3.2632e+008	3.2632e+008	3.2631e+008
175010902	2.1168e+008	2.1168e+008	2.1165e+008
1.5903e+009	1.2073e+009	1.2073e+009	1.2072e+009
1.8880e+009	1.8693e+009	1.8695e+009	1.8695e+009

CONCLUSION

In the proposed method, sender steganography is implemented to encrypt the patient personal information and physiological parameters inside the ECG signal. A special range transform is implemented for shifting and scaling of the ECG signal which removes the negative value of ECG signal. Secret key is used for sending and receiving the message. Five level wavelet decomposition is applied to decompose the ECG signal. After decomposition, 32 wavelet coefficients are produced. Embedding operation is implemented by using scrambling matrix and shared key. In embedding process, secret bits of information are hidden inside LSB of cover signal. Finally 32 watermarked wavelet coefficients are produced. A new watermarked ECG signal is produced by inverse wavelet transform. The energies of original ECG signal and encrypted ECG signal are calculated by using different wavelets. We can observe that the energy of encrypted ECG signal using Coiflet Wavelet transform is higher than other wavelet transforms so Coiflet Wavelet transform can be used for encryption process in ECG steganography using wavelet transforms.

REFERENCES

[1] K. Malasri and L. Wang, ―Addressing security in medical sensor networks,‖ in *proc*. 1st *ACM SIGMOBILE Int workshop syst. Netw. Supp. Healthcare Assist. Living Environ*.,2007,p.12.

[2] H. wang, D. Peng, W. Wang, H. Sharif, H. chen, and A. Khoynezhad, ―Resource- aware secure ECG healthcare monitoring through body sensor networks,‖ *IEEE Wireless Commun., vol. 17,no. 1,pp.* 12-19, Feb. 2010.

[3] Navjot kaur and Usvir kaur, ―An audio watermarking using Arnold transformation with discrete wavelet transform (DWT) and discrete cosine transform (DCT).‖*let al/ International journal of computer science engineering* vol. 2,no 06, Nov 2013 .

[4] Nilanjan Dey, Sayantan Mukhopadhyay, Achintya, and Sheli Sinha Chaudhari, ―Analysis of P-QRS-T componenets modified by blind watermarking technique within the ECG signal for authentication in wireless telecardiology using DWT‖. *International Journal of Image, Graphics, Signal Processing*, vol.4,no 7, July 2012.

[5] AymanIbaida and Ibarhim Khalil, ―Wavelet based ECG steganography for protectingpatient confidential informationin point of care systems,‖ IEEE Trans. Biomedical Engineering, vol. 60, no. 12, December 2013

[6] Dr PrenaMahajan 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.

[7] A. Poularikas, *Transform and applications Handbook*. Boca Raton, FL, USA: CRC Press, 2006.

[8] Ganesh, G. Balasubhramanian, S.K, Jena, Pradhan,‖ Simulation results for wavelet approximation,‖ RGPA, no. 16, May 2012.
[9] Physiobank, physiotoolkit, and physionet: Components of a new research for complex physiological signals.
[10] Y. LIN. I. Jan, P. Ko, Y. Chen, J. Womg, and G. Jan, ― A wireless PDA- based physiological monitoring system for patient transpoet‖. *IEEE Trans. Inf. Telchnol. Biomed*., vol. 8, no. pp. 439-447, Dec. 2004.
[11] F. Hu, M. Jiang, M. Wanger, and D. Dong, –Privacy-preserving tele-cardiology sensor networks: Toward a low-cost portable wireless hardware/software co design‖, *IEEE Trans. Inf. Technol. Biomed.*, vol. 1.1, no.6, pp. 619-627, Nov. 2007.
[12] A. Ibaida, I. Khalil, and F. Sufi, –Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)‖, in *Proc. 5th Int. conf. Intell. Sens. Netw. Inf. Process*.., Dec. 2010, pp. 207-212.
[13] 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.
[14] I. Maglogiannis, l. Kazatzopoulos, K. Delakouridis , and S. Hadjiefthymiades, –Enabling location privacy and medical data encryption in patient telemonitoring systems‖, *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 946-954, Nov. 2009.
[15] L. Marvel, C. Boncelet, and C. Retter, –Spread spectrum image steganography‖, *IEEE Trans. IMAGE. Process.*, vol.8, no.8 pp. 1075-1083, Aug 1999.
[16] A. De la Rosa Algarim, S. Demurjian, S. Berhe, and J. Pavlich- Mariscal, –A security framework for xml schemas and documents for healthcare‖, in *Proc. IEEE Int. Conf. Biomed. Workshop*, Oct. 2012, pp. 782-789.
[17] M. Li, S. Yu, Y. Zgeng, K. REN, AND W. Lou,‖Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption‖, *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131-143, Jan. 2013.
[18] S. Kaur, R. Singhal, O. Farooq, and B. ahuja, ‖Digital watermarking of ECG data for secure wireless communication ‖, in *Proc. Int. Conf. Recent Trends Inf. Telecommun. Comput.*, Mar. 2010, pp. 140-144.
[19] H. Golpira and H. Danyali, –Reversible blind watermarking for medical images based on wavelet histogram shifting‖, *in Proc. Int. Symp. Signal Process. Inf. Technol*., Dec. 2009, pp. 31-36.
[20] K. Zheng and X. Qian, –Reversible data hiding for electrocardiogram signal based on wavelet transforms‖, *in Proc. Int. Conf. Comput. Intell. Security*, Dec. 2008, vol. 1, pp. 295-299.
[21] A. Al-Fahoum, –Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure‖, *IEEE Trans. Inf. Technol. Biomed*., vol. 10, no. 1, pp. 182-191, Jan. 2006.